Contents

Plan Your Deployment .................................................................................................................. 1

Get Started with Tableau Server on Linux .................................................................................. 1

Server Administrator Overview .................................................................................................. 2

Architectural overview .................................................................................................................. 3

Tableau and your data .................................................................................................................... 4

User access .................................................................................................................................. 5

Where should I install Tableau Server in my network? ............................................................... 5

Sizing and scalability .................................................................................................................... 6

Tableau Server management model ............................................................................................... 7

Management tools ........................................................................................................................ 8

Security ........................................................................................................................................ 9

Tableau Services Manager Overview ............................................................................................ 9

Functionality ................................................................................................................................ 9

Components ................................................................................................................................ 10

TSM Authentication ...................................................................................................................... 10

Custom PAM service definition .................................................................................................... 11

Connecting TSM clients ............................................................................................................... 11

Infrastructure Planning ................................................................................................................. 12

Before you install... ....................................................................................................................... 12

Hardware recommendations ......................................................................................................... 13
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Configuration</td>
<td>30</td>
</tr>
<tr>
<td>Two Node Installation - Specialized for flow environments</td>
<td>33</td>
</tr>
<tr>
<td>Server Configuration</td>
<td>34</td>
</tr>
<tr>
<td>High Availability Installations (HA)</td>
<td>37</td>
</tr>
<tr>
<td>Recommendations</td>
<td>37</td>
</tr>
<tr>
<td>Server Configuration</td>
<td>37</td>
</tr>
<tr>
<td>Virtual Machines and Public Cloud Deployments</td>
<td>40</td>
</tr>
<tr>
<td>Beyond Baseline Configurations</td>
<td>40</td>
</tr>
<tr>
<td>Disaster Recovery Considerations</td>
<td>40</td>
</tr>
<tr>
<td>Tableau Server Scalability</td>
<td>41</td>
</tr>
<tr>
<td>Identity Store</td>
<td>42</td>
</tr>
<tr>
<td>Local identity store</td>
<td>42</td>
</tr>
<tr>
<td>External identity store</td>
<td>42</td>
</tr>
<tr>
<td>LDAP bind</td>
<td>44</td>
</tr>
<tr>
<td>LDAP with GSSAPI (Kerberos) bind</td>
<td>44</td>
</tr>
<tr>
<td>LDAP over SSL</td>
<td>44</td>
</tr>
<tr>
<td>System user and groups</td>
<td>46</td>
</tr>
<tr>
<td>User</td>
<td>46</td>
</tr>
<tr>
<td>Groups</td>
<td>47</td>
</tr>
<tr>
<td>Authenticating clients</td>
<td>47</td>
</tr>
<tr>
<td>User Management in Active Directory Deployments</td>
<td>48</td>
</tr>
<tr>
<td>Active Directory user authentication and Tableau Server</td>
<td>48</td>
</tr>
</tbody>
</table>
Install the Tableau Server package ...........................................86
Initialize TSM ........................................................................88
Next step ..............................................................................90
Activate and Register Tableau Server ......................................91
Prerequisite ............................................................................91
Use the TSM web interface .....................................................91
Use the TSM CLI .....................................................................94
Log in to Tableau Services Manager .......................................94
Activate Tableau Server .........................................................94
Register Tableau Server ........................................................95
Next step ..............................................................................96
Offline Activation When Installing Tableau Server .......................96
Offline activation overview and prerequisites ..............................96
In this article .........................................................................97
Log in to Tableau Services Manager .......................................100
Step 1 - Generate an offline activation request file ......................101
Step 2 - Upload the offline activation request to Tableau ..............102
Step 3 - Initialize or activate your license ..................................102
First time license activation ....................................................102
Subsequent license activation ................................................103
Deactivate Tableau Server Offline ...........................................103
Configure Initial Node Settings ...............................................104
Prerequisite .............................................................................................................. 104
Use the TSM web interface .................................................................................... 104
Identity store settings ............................................................................................ 106
Gateway port ........................................................................................................... 110
Sample workbook installation ................................................................................ 110
Use the TSM CLI ..................................................................................................... 111
Configure identity store settings ........................................................................... 111
Configure gateway settings (optional) .................................................................... 112
Configure sample workbook installation (optional) .............................................. 112
Apply pending configuration changes .................................................................... 112
Verify LDAP configuration (Optional) ..................................................................... 113
Initialize and start Tableau Server ....................................................................... 113
Next Step ................................................................................................................ 114
Configuration File Example ................................................................................... 114
Entities vs keys ....................................................................................................... 115
Add an Administrator Account .............................................................................. 116
Prerequisites ........................................................................................................... 117
Use web UI .............................................................................................................. 117
Use tabcmd CLI ...................................................................................................... 117
Next steps ............................................................................................................... 118
Validate Installation ............................................................................................... 118
Prerequisites ........................................................................................................... 119
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install PostgresSQL driver and validate installation</td>
<td>119</td>
</tr>
<tr>
<td>Initial Node Installation Defaults</td>
<td>119</td>
</tr>
<tr>
<td>Jump-start Installation</td>
<td>121</td>
</tr>
<tr>
<td>Before you begin</td>
<td>121</td>
</tr>
<tr>
<td>Step 1: Install Tableau Server package and start Tableau Services Manager</td>
<td>122</td>
</tr>
<tr>
<td>Step 2: Activate and register Tableau Server</td>
<td>123</td>
</tr>
<tr>
<td>Step 3: Configure local identity store</td>
<td>124</td>
</tr>
<tr>
<td>Step 4: Finalize installation</td>
<td>124</td>
</tr>
<tr>
<td>Step 5: Install PostgreSQL drivers</td>
<td>125</td>
</tr>
<tr>
<td>Configure Local Firewall</td>
<td>125</td>
</tr>
<tr>
<td>Single-node configuration</td>
<td>126</td>
</tr>
<tr>
<td>Multi-node cluster configuration</td>
<td>127</td>
</tr>
<tr>
<td>Before you begin</td>
<td>127</td>
</tr>
<tr>
<td>Step 1: Configure initial node.</td>
<td>127</td>
</tr>
<tr>
<td>Step 2: Configure additional nodes</td>
<td>129</td>
</tr>
<tr>
<td>Automated Installation of Tableau Server</td>
<td>130</td>
</tr>
<tr>
<td>Benefits of using the automated installer</td>
<td>130</td>
</tr>
<tr>
<td>Before you begin</td>
<td>131</td>
</tr>
<tr>
<td>How to use the automated installer</td>
<td>132</td>
</tr>
<tr>
<td>Configure Tableau Server for a forward proxy</td>
<td>133</td>
</tr>
<tr>
<td>Perform an unattended installation</td>
<td>134</td>
</tr>
<tr>
<td>Step 1: Install the automated installer</td>
<td>134</td>
</tr>
</tbody>
</table>
Tableau Server on Linux Administrator Guide

Step 2: Create files to provide additional configuration information required to run the automated install ......................................................... 135
Step 3: Run the automated install .......................................................... 136

Install Tableau Server in a Disconnected (Air-Gapped) Environment .............. 137

Prerequisites ......................................................................................... 138

Installing Tableau Server on an Air-Gapped Computer Running Linux ............ 138

Activating Tableau Server in an Air-Gapped Environment ............................. 141

Step 1. Transcribe data from your air-gapped system into an activation request template. ........................................................................... 141
Step 2. Initialize or activate your license .................................................. 143
First time license activation ...................................................................... 143
Subsequent license activation .................................................................... 144

Displaying Maps in an Air-Gapped Environment ....................................... 144

Install Tableau Server in the Cloud ......................................................... 145

Post Installation Tasks ........................................................................... 146

Security Hardening Checklist .................................................................. 146

1. Update to the current version ............................................................ 146
2. Configure SSL/TLS with a valid, trusted certificate .............................. 146
3. Disable older versions of TLS ............................................................ 146
4. Disable Triple-DES cipher suite ......................................................... 147
5. Configure SSL encryption for internal traffic .................................... 148
6. Enable firewall protection .................................................................. 148
7. Restrict access to the server computer and to important directories ........ 149
8. Generate fresh secrets and tokens ................................................. 149
9. Disable services that you’re not using ........................................... 149

REST API ..................................................................................... 150
JMX Service .................................................................................. 150

10. Verify session lifetime configuration .............................................. 150
11. Configure a server safelist for file-based data sources ..................... 151
13. Disable Guest access ................................................................. 153

Change List ................................................................................. 154

Configure SMTP Setup ..................................................................... 154
Use the TSM web interface ............................................................ 154
Use the TSM CLI ............................................................................ 155
Configuration file reference ............................................................ 156

Files and Permissions in TSM ........................................................... 159
Setting permissions for individual files ............................................ 160
Setting permissions for directories .................................................. 161

Configure Server Event Notification ................................................. 162
Use the TSM web interface ............................................................ 162
Use the TSM CLI ............................................................................ 165
Set notification values individually .................................................. 165
Set all notification values with a single json file .............................. 167
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Data Cache</td>
<td>167</td>
</tr>
<tr>
<td>Database Drivers</td>
<td>168</td>
</tr>
<tr>
<td>Install drivers in a cluster</td>
<td>169</td>
</tr>
<tr>
<td>Server Crash Reporter</td>
<td>169</td>
</tr>
<tr>
<td>Configure Server Crash Reporter</td>
<td>170</td>
</tr>
<tr>
<td>Use the TSM web interface</td>
<td>170</td>
</tr>
<tr>
<td>Use the TSM CLI</td>
<td>171</td>
</tr>
<tr>
<td>Crash reporter settings</td>
<td>172</td>
</tr>
<tr>
<td>Configuration template</td>
<td>172</td>
</tr>
<tr>
<td>Configuration file reference</td>
<td>172</td>
</tr>
<tr>
<td>Navigate the Admin Areas of the Tableau Web Environment</td>
<td>174</td>
</tr>
<tr>
<td>Access based on site role and number of sites</td>
<td>174</td>
</tr>
<tr>
<td>Server administrator</td>
<td>174</td>
</tr>
<tr>
<td>Site administrator</td>
<td>175</td>
</tr>
<tr>
<td>Server administrator tasks</td>
<td>176</td>
</tr>
<tr>
<td>Site administrator tasks</td>
<td>177</td>
</tr>
<tr>
<td>Migrate to New Hardware</td>
<td>177</td>
</tr>
<tr>
<td>Tableau Server product key activation</td>
<td>179</td>
</tr>
<tr>
<td>Enable and Configure Tableau Prep Conductor on Tableau Server</td>
<td>179</td>
</tr>
<tr>
<td>Who can do this?</td>
<td>180</td>
</tr>
<tr>
<td>Server Topology</td>
<td>180</td>
</tr>
<tr>
<td>Next step:</td>
<td>182</td>
</tr>
</tbody>
</table>
Step 1 (New Install): Install Tableau Server with Tableau Prep Conductor ……. 182

Who can do this? .............................................................................................................. 183

Before you install ............................................................................................................. 183

Install Tableau Server and enable Tableau Prep Conductor ............................. 183

Configure public gateway settings ................................................................. 184

Verify Tableau Prep Conductor is enabled and running ............................. 184

Dedicate a node for Tableau Prep Conductor .................................................. 186

Next step .................................................................................................................... 187

Step 1 (Existing Install): Enable Tableau Prep Conductor ..................... 187

Who can do this? .............................................................................................................. 188

Before you upgrade ................................................................................................... 188

Prepare for upgrade: ................................................................................................. 188

Configure public gateway settings ................................................................. 188

Tableau Server Installations using User-Based licenses ..................... 189

Tableau Server single-node installations ....................................................... 189

Tableau Server multi-node installations ......................................................... 191

Tableau Server Installations using Core-Based licenses ..................... 194

Tableau Server single-node installations ....................................................... 194

Tableau Server multi-node installations ......................................................... 197

Next step .................................................................................................................... 201

Step 2 - Configure Flow Settings for your Tableau Server ..................... 201

Who can do this? .............................................................................................................. 201
Creating a distributed Tableau Server installation ........................................ 214
Creating a highly available (HA) Tableau Server installation .......................... 214
Recover from an initial node failure ............................................................. 216
Configure Coordination Service ensemble on additional nodes ...................... 216
Tableau Server service license check ......................................................... 216
Distributed Requirements .............................................................................. 217
Hardware ........................................................................................................ 217
Hardware Guidelines for High Availability ..................................................... 217
Software ......................................................................................................... 218
Installation location ........................................................................................ 218
Networking and Ports .................................................................................... 219
Best Practices .................................................................................................. 219
SSL .................................................................................................................. 220
Distributed Installation Recommendations ...................................................... 220
Recommendations for all installations ............................................................ 221
Install and Configure Additional Nodes .......................................................... 222
Use the TSM web interface ............................................................................. 222
Generate the node bootstrap file ...................................................................... 223
Install and initialize an additional node ............................................................ 223
Configure the additional node with Cluster Controller ...................................... 226
Use the TSM CLI .............................................................................................. 228
Generate the node bootstrap file ...................................................................... 228
Install and initialize an additional node .......................................................... 229
Configure the additional node ....................................................................... 231
Install drivers ................................................................................................. 233
Drivers and administrative views ................................................................. 233
Database Drivers ............................................................................................ 233
Install drivers in a cluster .............................................................................. 234
Example: Install and Configure a Three-Node HA Cluster ............................ 234
A Single Server System .................................................................................. 234
A Three-Node System .................................................................................... 236
Configuration steps ....................................................................................... 237
Before you begin ........................................................................................... 238
Use the TSM web interface ............................................................................ 238
Step 1: Install the initial node ................................................................. 238
Step 2: Generate a bootstrap file for the additional nodes ............................. 238
Step 3: Install and initialize an additional node ........................................... 239
Step 4: Install and initialize a second additional node ................................. 242
Step 5: Configure the new node with a minimum topology ......................... 244
Step 6: Deploy a Coordination Service ensemble ...................................... 245
Step 7: Configure processes for the second node ....................................... 250
Step 8: Configure processes for third node ................................................ 251
Use the TSM CLI ........................................................................................... 252
Step 1: Install the initial node ................................................................. 252
Step 2: Generate a bootstrap file for the additional nodes .......................... 252
Step 3: Install an additional node ................................................................. 253
Step 4: Install a second additional node ....................................................... 255
Step 5: Add a process to the additional nodes .............................................. 258
Step 6: Deploy a Coordination Service ensemble ......................................... 258
Step 7: Configure processes for the second node ....................................... 262
Step 8: Configure processes for third node .................................................. 264
Step 9: Configure firewall rules (optional) ................................................... 265
Add a Load Balancer ....................................................................................... 265
Add a Load Balancer ....................................................................................... 265
Configure Tableau Server to work with a load balancer .............................. 266
   Load balancer configuration key-value pairs .............................................. 266
   Configuration template example ............................................................... 268
Deploy a Coordination Service Ensemble ................................................... 269
Hardware requirements .................................................................................. 269
The Coordination Service Quorum ............................................................... 270
   Number of Coordination Service instances to use .................................... 270
Deploy a new Coordination Service ensemble ......................................... 271
Configure Client File Service ....................................................................... 275
Configure CFS on additional nodes ............................................................ 276
Repository Failover ....................................................................................... 276
Automatic repository failover ..................................................................... 276
Use the TSM CLI  .......................................................... 297
Add a new instance of the repository.  .................................. 297
Remove an instance of the repository.  .................................. 298
Move the File Store Process  .................................................. 298
Use the TSM web interface  .................................................. 298
Adding a second instance of File Store  .................................. 299
Decommissioning and removing an instance of file store ............ 299
Use the TSM CLI  .......................................................... 300
Adding a second instance of file store  .................................. 300
Decommissioning and removing an instance of File Store .......... 301
Remove a Node  .................................................................. 302
Prerequisites for removing a node .......................................... 302
Use the TSM web interface  .................................................. 303
Use the TSM CLI  .......................................................... 304
Configure Tableau Server for High Availability with Coordination Service-Only Nodes .................................................. 305
Prerequisite  ......................................................................... 305
Deploy an ensemble on Coordination Service-only nodes .......... 306
Add a Load Balancer  .......................................................... 310
Configure Tableau Server to work with a load balancer .............. 311
Load balancer configuration key-value pairs ............................ 311
Configuration template example ............................................. 313
Migrate Tableau Server from Windows to Linux .................................................. 314

Step 1: Plan your migration .............................................................................. 315

Step 2: Create a backup .................................................................................. 316

Migrate from 2018.1 or earlier ........................................................................ 316

Migrate from 2018.2 or later ........................................................................... 317

Step 3: Install Tableau Server on Linux and restore the Windows backup .......... 318

Step 4: Test Tableau Server on Linux .............................................................. 319

Step 5: Install Tableau Server on Linux in your production environment and
restore the Windows backup ......................................................................... 321

Test Workbook Performance ........................................................................ 321

Set up your test environment ....................................................................... 322

Capture performance metrics and analyze ................................................... 322

Troubleshoot performance issues ................................................................. 323

Capture the conclusions and results from your testing ............................... 326

Migrate from Tabadmin to the TSM CLI ...................................................... 326

Tabadmin commands with a corresponding TSM CLI command ................ 326

Tabadmin commands with no corresponding TSM CLI command ............ 331

Uninstall Tableau Server ............................................................................. 333

Uninstalling and completely removing Tableau Server ............................. 333

Uninstall a Tableau Server package ........................................................... 334

Reinstall a Tableau Server package that was accidentally uninstalled ....... 335

Remove Tableau Server from Your Computer ......................................... 336
What tableau-server-obliterate does .................................................. 337
Running the tableau-server-obliterate script ........................................ 338
To completely remove Tableau Server without removing server licensing: . 338
To completely remove Tableau Server and licensing: .............................. 339
Upgrade Tableau Server Overview ....................................................... 340
Upgrade Tableau Server on Linux ....................................................... 341
Research the Upgrade .......................................................................... 341
What's New in Tableau Server .............................................................. 344
What's new in version 2019.1 .............................................................. 344
Web authoring auto recovery ............................................................... 345
Option to install to non-default location on RHEL-distros ....................... 345
Microservice Container Processes ...................................................... 345
Pluggable Authentication Modules (PAM) ........................................... 346
TSM client authentication ................................................................. 346
Ask Data and Elastic Server Processes ................................................. 346
Tableau Prep Conductor Server Process .............................................. 346
Tableau Data Management Add-On ................................................... 347
Node roles for Backgrounder Process ............................................... 347
SSL connection to Rserve external service ......................................... 347
Added in previous versions .................................................................. 347
Materialize calculations in extracts already published to Tableau Server .......................... 348
Secure extract data at the row level .................................................... 348
Improved content browsing (in-release beta) .................................................. 349
Support for Content Security Policy ............................................................... 349
Improved support for LDAP ............................................................................. 349
Connections to external services support SSL .................................................. 349
SAML now supports PKCS#8 key files .............................................................. 350
Improved key and secrets refresh process ....................................................... 350
Backup without compression (added in version 2018.3.2) ............................ 350
Include colleagues on data conversations with @mentions ................................ 351
Create a support case from the TSM UI or CLI ............................................... 351
Manage Dashboard Extensions in Tableau Server .......................................... 352
Automated daemon port configuration ........................................................... 352
Amazon Linux 2 now supported ..................................................................... 352
Resize headers on the web .............................................................................. 353
Streamline discussion threads by deleting comments ...................................... 353
New user-based term licenses are now available ........................................... 353
New and renamed site roles are now available .............................................. 354
Improved support for managing web data connectors .................................. 354
Optimized server performance for data alerts ............................................... 355
Nested projects ............................................................................................. 355
Filtered search hidden by default .................................................................. 355
Tableau Data Engine with Hyper ................................................................... 356
Extracts use the new .hyper format ............................................................... 356
Changes to the way values are computed .................................................... 356

Tableau Services Manager ............................................................................. 357

Hot topology support ..................................................................................... 357

Lightweight Directory Access Protocol (LDAP) support .............................. 357

What’s Changed - Things to Know Before You Upgrade ................................. 358

Install to non-default locations (RHEL-like distributions only) ...................... 358

High-resolution thumbnails ........................................................................... 359

Project card images ....................................................................................... 359

Floating worksheet captions become transparent ....................................... 360

Changes to some Data Engine tsm configuration set options ......................... 360

SSL Off-loading and SAML ............................................................................ 360

Moving the repository in a two-node cluster not supported .......................... 361

Updates to Tableau Server Apache Logs ....................................................... 361

The Read Only site role is now deprecated .................................................. 362

The tabcmd initialuser command prompts for password ............................ 362

New ports added ............................................................................................ 363

  Automatic port assignment ........................................................................ 363

  Manual port assignment .......................................................................... 363

  Ports added in 2018.2 ............................................................................. 363

Removed tabadmin command options .......................................................... 364

Updated tsm commands .............................................................................. 364

Updated upgrade-tsm script ....................................................................... 365
Tableau Server configuration changes ........................................... 366
Changes to extracts ................................................................. 366
Version compatibility ............................................................... 367
Viewer (can publish) and Unlicensed (can publish) site roles removed ... 367
Nested projects and content navigation ........................................ 367
Nested projects and tabcmd ....................................................... 368
Filtered search hidden by default .............................................. 368
Minimum Hardware Requirements and Recommendations for Tableau Server ........................................................................... 369
Minimum Hardware Requirements for Testing and Prototyping ........ 370
Minimum Hardware Recommendations for Production .................... 371
Prepare for the Upgrade ............................................................ 373
Gather custom configuration information ....................................... 373
Gather the environment configuration ......................................... 375
Copy the setup files to a local file share ....................................... 375
Update tabcmd ........................................................................ 376
Back up Tableau Server data ..................................................... 376
Generate asset keys file before uninstalling Tableau Server for Windows 2018.1.x or earlier .......................................................... 377
Locating an existing asset keys file .............................................. 377
Restoring a pre-2018.2 Tableau Server for Windows backup along with asset keys ................................................................. 377
Check your product maintenance status ...................................... 378
Run TSM commands ................................................................. 398
Migrate 10.5.x to single user ..................................................... 399
Upgrade to 2018.x .................................................................... 399
Related topics ......................................................................... 400

Troubleshoot Tableau Server Install and Upgrade ......................... 401

General Troubleshooting Steps .................................................. 401

Common Tableau Server Install Issues ...................................... 401
Installation logs location ......................................................... 401
Unable to log into TSM or Tableau Server (sign in screen redisplayed after entering credentials) ........................................... 402
Multiple install attempts fail ..................................................... 402
Install fails due to hardware requirements ................................... 403

Common Tableau Server Upgrade Issues ................................. 403
Upgrade logs location ............................................................... 403
Upgrade multi-node, initializing additional node fails with "Enter your credentials again" error ............................................... 403
Upgrading fails due to lack of disk space .................................... 404

Starting Tableau Server ............................................................ 405
Tableau Server cannot determine if it fully started ....................... 405
Tableau Server doesn't start ..................................................... 405

Reindexing Tableau Server Search & Browse .......................... 405
Problems that can be solved by rebuilding Search & Browse index 405
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronize all Active Directory groups on demand</td>
<td>462</td>
</tr>
<tr>
<td>View synchronization activity</td>
<td>463</td>
</tr>
<tr>
<td>Set the minimum site role for users in an Active Directory group</td>
<td>463</td>
</tr>
<tr>
<td>What happens when users are removed in the source Active Directory?</td>
<td>465</td>
</tr>
<tr>
<td>Improving group synchronization performance</td>
<td>465</td>
</tr>
<tr>
<td>Quick Start: Synchronize All Active Directory Groups on a Schedule</td>
<td>465</td>
</tr>
<tr>
<td>1 Set a minimum site role for synchronization</td>
<td>466</td>
</tr>
<tr>
<td>2 Set the schedule</td>
<td>467</td>
</tr>
<tr>
<td>3 Run synchronization on-demand (optional)</td>
<td>467</td>
</tr>
<tr>
<td>4 View the status of synchronization tasks</td>
<td>468</td>
</tr>
<tr>
<td>Delete Groups</td>
<td>469</td>
</tr>
<tr>
<td>Dashboard-based Custom Portals</td>
<td>470</td>
</tr>
<tr>
<td>Sketch out a portal design</td>
<td>471</td>
</tr>
<tr>
<td>Gather images for logos and navigation elements</td>
<td>471</td>
</tr>
<tr>
<td>Lay out text, images, and selected sheets on a dashboard</td>
<td>472</td>
</tr>
<tr>
<td>Link dashboard elements to content</td>
<td>472</td>
</tr>
<tr>
<td>Publish, test, and refine your portal</td>
<td>473</td>
</tr>
<tr>
<td>Data Connection Authentication</td>
<td>474</td>
</tr>
<tr>
<td>More information</td>
<td>474</td>
</tr>
<tr>
<td>Enable Kerberos Delegation</td>
<td>474</td>
</tr>
<tr>
<td>Supported data sources</td>
<td>474</td>
</tr>
<tr>
<td>Requirements</td>
<td>475</td>
</tr>
</tbody>
</table>
Configuration process ............................................................................ 475
See also ................................................................................................. 478
OAuth Connections .................................................................................. 478
Overview of the OAuth process ............................................................... 478
Access tokens for data connections ....................................................... 480
Access tokens for authentication from approved clients ....................... 480
Configure the Server for OAuth Support .............................................. 480
Preparing for Configuring OAuth Support ........................................... 480
Configure Settings for Your Data Provider .......................................... 481
Set up OAuth for Google ........................................................................ 481
Obtain a Client ID and Enable Google APIs ........................................ 482
Configure Tableau Server for Google OAuth ........................................ 484
Create and edit Google data source ..................................................... 484
Managing access tokens ....................................................................... 485
Set up OAuth for Salesforce.com ......................................................... 485
Create a Connected Salesforce App ..................................................... 485
Configure Tableau Server for Salesforce.com OAuth ............................. 487
Managing access tokens ....................................................................... 488
Set up OAuth for QuickBooks Online .................................................. 488
Create a Connected Intuit App .............................................................. 488
Configure Tableau Server for QuickBooks Online ................................. 489
Managing access tokens ....................................................................... 489
Allow users who can publish to edit, save changes to, and download new workbooks, but not overwrite existing workbooks ........................................ 500

Allow explorers to download workbooks ........................................ 500

See also .......................................................................................... 501

Configure Projects, Groups, and Permissions for Managed Self-Service .... 501

Create a project team and adopt a permissions strategy ....................... 502

Steps to coordinate projects and groups ............................................ 502

1. Plan your permissions .................................................................. 503

   Use a closed permissions model for managed content ................... 504

2. Remove permissions that will cause ambiguities ............................ 504

3. Create groups ............................................................................ 506

4. Assign permissions to the groups ................................................. 507

   Set permissions templates .......................................................... 507

   Example ..................................................................................... 508

5. Create projects and adjust permissions ....................................... 509

   Example project structure .......................................................... 509

   Help project leaders manage content and users find it ................. 511

6. Lock permissions in each project ................................................. 512

   Automate working with groups and projects .............................. 512

   Next steps .................................................................................. 513

   Learn how Tableau and some of our customers address governance and self-service ...................................................... 514
Use Projects to Manage Content Access ...................................................... 514
Why use projects ......................................................................................... 515
When to create project hierarchies (example) ........................................... 516
Why not use sites? ....................................................................................... 517
Project-level administration ......................................................................... 517
Project ownership and project leader access in project hierarchies ............ 518
Actions project-level administrators can take on projects ........................ 518
How the Default project acts as a permissions template ............................ 519
Prevent publishers from changing permissions on content they own .......... 520
Next steps .................................................................................................... 520
Add Projects and Move Content Into Them ............................................... 520
Add a top-level or child (nested) project ..................................................... 521
Move a content resource to another project .............................................. 522
How moving projects affects Project Leader permissions ........................ 523
Delete a project ............................................................................................ 524
Required access level for moving content ................................................... 524
  Required site role .................................................................................... 525
  Required permissions for the project that users move content to ............... 525
  Required permissions for the project that users move content from ........... 525
Set Project Default Permissions and Lock the Project ................................. 526
Prerequisites ................................................................................................. 526
Set the default permissions for a project or multiple projects .................... 526
Lock or unlock permissions on a top-level project ........................................ 531
Permissions roles you can set at the project level ........................................ 533
Capabilities you can set for a project ......................................................... 534
See also ....................................................................................................... 535
Permissions in Project Hierarchies ............................................................... 535
Project permissions states: locked and managed by owner ......................... 536
When to use each state ............................................................................... 536
How permissions are evaluated in project hierarchies ............................... 537
How permissions are applied in locked project hierarchies ....................... 538
How permissions are applied in unlocked project hierarchies ................. 539
See also ....................................................................................................... 539
Add a Project Image .................................................................................... 539
Set a project image ..................................................................................... 540
Content Permissions and Ownership .......................................................... 543
What makes up a user’s permissions ........................................................... 544
Who can set permissions ........................................................................... 544
Quick Start: Permissions ............................................................................ 545
1 Add users to groups ................................................................................ 545
2 Open a project’s permissions settings ..................................................... 546
3 Create a permissions rule ....................................................................... 547
4 View a user’s effective permissions ....................................................... 548
Site roles .................................................................................................... 549
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permissions evaluation</td>
<td>549</td>
</tr>
<tr>
<td>Manage Content Ownership</td>
<td>551</td>
</tr>
<tr>
<td>Who can change or be given ownership, by content type</td>
<td>551</td>
</tr>
<tr>
<td>Considerations for changing content ownership</td>
<td>552</td>
</tr>
<tr>
<td>Change the owner of a content resource</td>
<td>553</td>
</tr>
<tr>
<td>View or Edit Permissions</td>
<td>554</td>
</tr>
<tr>
<td>View or edit a permissions rule for a selected content resource</td>
<td>555</td>
</tr>
<tr>
<td>How the permissions rules settings work together</td>
<td>557</td>
</tr>
<tr>
<td>What determines users’ effective permissions</td>
<td>558</td>
</tr>
<tr>
<td>Set Permissions on Individual Content Resources</td>
<td>559</td>
</tr>
<tr>
<td>Capabilities you can set on data sources</td>
<td>560</td>
</tr>
<tr>
<td>Permission role templates for data sources</td>
<td>561</td>
</tr>
<tr>
<td>Capabilities you can set on workbooks and views</td>
<td>561</td>
</tr>
<tr>
<td>Editing view-level permissions</td>
<td>561</td>
</tr>
<tr>
<td>Permission role templates for workbooks and views</td>
<td>562</td>
</tr>
<tr>
<td>Capabilities you can set on flows</td>
<td>562</td>
</tr>
<tr>
<td>Set permissions on a content resource</td>
<td>563</td>
</tr>
<tr>
<td>See also</td>
<td>566</td>
</tr>
<tr>
<td>How Permissions are Evaluated</td>
<td>566</td>
</tr>
<tr>
<td>Notes on permissions</td>
<td>568</td>
</tr>
<tr>
<td>The order of precedence in which Tableau evaluates permissions</td>
<td>568</td>
</tr>
<tr>
<td>Permissions Reference</td>
<td>569</td>
</tr>
</tbody>
</table>
How certification helps users find trusted data ................................................. 587
Create guidelines for selecting data sources to certify ........................................ 589
Who can certify data sources ........................................................................... 589
Certify a data source ......................................................................................... 590
Keep Data Fresh ............................................................................................... 590
Manage Refresh Tasks ....................................................................................... 590
See also ............................................................................................................ 591
Refresh Data on a Schedule .............................................................................. 591
Quick Start: Refresh Extracts on a Schedule ..................................................... 593
1 Set up a schedule on the server ...................................................................... 594
2 Enable scheduled extract refreshes and failure emails ..................................... 594
3 Publish a workbook with an extract ............................................................... 595
4 Monitor refresh performance ....................................................................... 596
Automate Refresh Tasks ................................................................................... 597
Handle Extract Refresh Alerts ......................................................................... 597
Resolving Extract Refresh Problems ............................................................... 599
Edit Connections on Tableau Server ............................................................... 600
Authentication types for Google, Salesforce, and WDC data ......................... 602
Google authentication options ....................................................................... 603
Salesforce.com authentication options ............................................................. 603
Monitor progress ............................................................................................. 604
Cube Data Sources .......................................................................................... 605
<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>616</td>
</tr>
<tr>
<td>618</td>
</tr>
<tr>
<td>619</td>
</tr>
<tr>
<td>619</td>
</tr>
<tr>
<td>620</td>
</tr>
<tr>
<td>620</td>
</tr>
<tr>
<td>620</td>
</tr>
<tr>
<td>621</td>
</tr>
<tr>
<td>621</td>
</tr>
<tr>
<td>623</td>
</tr>
<tr>
<td>624</td>
</tr>
<tr>
<td>626</td>
</tr>
<tr>
<td>626</td>
</tr>
<tr>
<td>627</td>
</tr>
<tr>
<td>627</td>
</tr>
<tr>
<td>627</td>
</tr>
<tr>
<td>627</td>
</tr>
<tr>
<td>627</td>
</tr>
<tr>
<td>627</td>
</tr>
<tr>
<td>627</td>
</tr>
<tr>
<td>630</td>
</tr>
<tr>
<td>632</td>
</tr>
</tbody>
</table>
See also ................................................................................................................. 632

Use Dashboard Extensions .................................................................................. 632

Add an extension to a dashboard ........................................................................ 633

Configure a dashboard extension ....................................................................... 634

Reload a dashboard extension ............................................................................. 635

Ensure that extensions run on Tableau Online or Tableau Server .................. 635

Data security and dashboard extensions ............................................................. 636

Allow or deny data access to an extension .......................................................... 636

Enable JavaScript ............................................................................................... 637

Get support for dashboard extensions .................................................................. 637

Manage Server .................................................................................................... 639

Security ................................................................................................................ 640

Authentication ...................................................................................................... 640

Client authentication compatibility ................................................................. 642

Local authentication ........................................................................................... 643

External authentication solutions ........................................................................ 643

NTLM and SSPI .................................................................................................... 643

Kerberos ............................................................................................................... 644

SAML .................................................................................................................... 644

OpenID Connect .................................................................................................. 644

Mutual SSL .......................................................................................................... 644

Trusted authentication ........................................................................................ 645
LDAP ........................................................................................................ 645
Other authentication scenarios ................................................................. 646
Data access and source authentication ....................................................... 646
SAML ........................................................................................................ 646
SAML Requirements ............................................................................... 648
Certificate and identity provider (IdP) requirements .............................. 649
SSL Off-loading ..................................................................................... 650
Using SSL certificate and key files for SAML ........................................ 650
User management requirements .............................................................. 651
SAML compatibility notes and requirements .......................................... 652
Using SAML SSO with Tableau client applications ................................. 654
Redirecting authenticated users back to Tableau clients ......................... 655
XML data requirements ........................................................................ 655
Configure Server-Wide SAML ................................................................. 658
Before you begin .................................................................................... 659
Use the TSM web interface .................................................................. 659
Use the TSM CLI .................................................................................... 663
Before you begin .................................................................................... 663
Configure return URL, SAML entity ID, and specify certificate and key files ........................................ 663
Generate Tableau Server metadata and configure the IdP ......................... 664
Match assertions ..................................................................................... 665
Optional: Disable client types from using SAML .................................... 666
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test the configuration</td>
<td>667</td>
</tr>
<tr>
<td>Configure SAML with AD FS on Tableau Server</td>
<td>668</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>668</td>
</tr>
<tr>
<td>Step 1: Verify SSL connection to AD FS</td>
<td>668</td>
</tr>
<tr>
<td>Step 2: Configure SAML on Tableau Server</td>
<td>669</td>
</tr>
<tr>
<td>Step 3: Configure AD FS to accept sign-in requests from Tableau Server</td>
<td>669</td>
</tr>
<tr>
<td>Step 4: Provide AD FS metadata to Tableau Server</td>
<td>673</td>
</tr>
<tr>
<td>Use SAML SSO with Kerberos Database Delegation</td>
<td>674</td>
</tr>
<tr>
<td>Overview of the process</td>
<td>675</td>
</tr>
<tr>
<td>Configure Tableau Server for SAML with Kerberos</td>
<td>676</td>
</tr>
<tr>
<td>Configure Site-Specific SAML</td>
<td>676</td>
</tr>
<tr>
<td>Prerequisites for enabling site-specific SAML</td>
<td>676</td>
</tr>
<tr>
<td>Server-wide settings related to site-specific SAML</td>
<td>677</td>
</tr>
<tr>
<td>Configure the server to support site-specific SAML</td>
<td>678</td>
</tr>
<tr>
<td>About the commands</td>
<td>678</td>
</tr>
<tr>
<td>Configure SAML for a site</td>
<td>679</td>
</tr>
<tr>
<td>Troubleshoot SAML</td>
<td>683</td>
</tr>
<tr>
<td>SAML and Enable Automatic Logon</td>
<td>684</td>
</tr>
<tr>
<td>HTTP Status 500 error when configuring SAML</td>
<td>684</td>
</tr>
<tr>
<td>Signing In from the Command Line</td>
<td>684</td>
</tr>
<tr>
<td>Login fails: failed to find the user</td>
<td>685</td>
</tr>
<tr>
<td>Login fails: SSL offloading</td>
<td>685</td>
</tr>
</tbody>
</table>
Tableau Mobile app clients ........................................... 702
OS- and browser-specific notes ........................................ 702
Note 1: Internet Explorer or Chrome on Windows desktop ................. 703
Note 2: Firefox on Windows or Mac OS X desktop .......................... 704
Note 3: Chrome on Mac OS X desktop .................................... 705
Note 4: Mobile Safari or Tableau Mobile on Mac iOS ....................... 706
Note 5: Android platform .................................................. 706
  Troubleshoot Kerberos ................................................... 706
  Single sign-on to Tableau Server ........................................ 706
Troubleshooting sign-in errors on the client computer ....................... 707
Troubleshooting sign-in errors on the server ................................ 709
Verify Kerberos configuration script ...................................... 710
  Data source SSO .......................................................... 710
Delegated data source access failures ..................................... 710
Kerberos delegation multi-domain configuration .......................... 711
Cross-domain constrained delegation ...................................... 712
  Configure Mutual SSL Authentication .................................. 713
  Use the TSM web interface .............................................. 713
  Use the TSM CLI .......................................................... 715
    Step 1: Require SSL for external server communication ................. 715
    Step 2: Use mutual SSL ............................................... 715
  Additional options for mutual SSL ..................................... 716
Fallback authentication .......................................................... 716
User name mapping ............................................................. 716
Certificate Revocation List (CRL) .......................................... 717
Mapping a Client Certificate to a User During Mutual Authentication ....... 717
User-name mapping options .................................................. 717
Change the certificate mapping .............................................. 718
Address user-name mapping ambiguity in multi-domain organizations .... 719
OpenID Connect .................................................................. 720
Authentication overview ....................................................... 720
How Tableau Server Works with OpenID Connect ....................... 723
Requirements for Using OpenID Connect .................................. 723
IdP account ....................................................................... 723
Local authentication ........................................................... 724
IdP claims: mapping users .................................................... 724
Default: using email claim to map users ................................... 724
Ignoring the domain name ..................................................... 725
Using custom claims to map users .......................................... 726
Changing the sub claim ....................................................... 727
Configure the Identity Provider for OpenID Connect ..................... 728
Configure the IdP .................................................................. 728
Redirect URL ...................................................................... 729
Example IdP process ........................................................... 729
Test Trusted Authentication ............................... 749
Step 1: Add a test user ........................................ 749
Step 2: Create a test HTML page ......................... 750
Step 3: Retrieve a trusted ticket from Tableau Server ............................... 751
Step 4: Test access with trusted ticket ....................... 752
Troubleshoot Trusted Authentication ......................... 753
Ticket Value of -1 Returned from Tableau Server .............. 753
HTTP 401 - Not Authorized .................................... 755
HTTP 404 - File Not Found .................................... 755
Invalid User (SharePoint or C#) ............................ 755
Attempting to Retrieve the Ticket from the Wrong IP Address ............ 756
Cookie Restriction Error ..................................... 756
An error occurred communicating with the server (403) .......... 757
Data Connection Authentication ............................. 757
More information ............................................. 757
Enable Kerberos Delegation .................................. 757
Supported data sources ..................................... 758
Requirements ............................................. 758
Configuration process ..................................... 758
See also ............................................. 761
OAuth Connections ........................................................................................................ 761
Overview of the OAuth process ...................................................................................... 762
Access tokens for data connections ................................................................................. 763
Access tokens for authentication from approved clients ........................................... 763
Configure the Server for OAuth Support .................................................................... 763
Preparing for Configuring OAuth Support ................................................................. 764
Configure Settings for Your Data Provider .............................................................. 764
Set up OAuth for Google ............................................................................................. 764
Obtain a Client ID and Enable Google APIs ............................................................. 765
Configure Tableau Server for Google OAuth .......................................................... 767
Create and edit Google data source ............................................................................. 768
Managing access tokens ............................................................................................... 768
Set up OAuth for Salesforce.com ................................................................................ 768
Create a Connected Salesforce App .......................................................................... 769
Configure Tableau Server for Salesforce.com OAuth ............................................... 771
Managing access tokens ............................................................................................... 771
Set up OAuth for QuickBooks Online ......................................................................... 772
Create a Connected Intuit App ................................................................................... 772
Configure Tableau Server for QuickBooks Online ................................................... 773
Managing access tokens ............................................................................................... 773
Allow Saved Access Tokens ...................................................................................... 774
Managing credentials centrally ................................................................................... 775
Import and export configuration information .............................................. 794
Securing secrets for import and export operations ..................................... 794
Cluster nodes ................................................................................................. 797
Secrets storage event logging ......................................................................... 797
Managing secrets ............................................................................................. 797
Updating secrets ............................................................................................... 797
Retrieving passwords ....................................................................................... 798

Extension Security - Best Practices for Deployment ..................................... 800
Security for extensions in Tableau ................................................................. 800
Potential security risks ..................................................................................... 801
Mitigating the security threats .......................................................................... 801
Manage extensions using Tableau ................................................................. 802
Recommendations for Tableau Desktop ......................................................... 802
Selectively enable extensions on Tableau Desktop ........................................ 803
Recommendations for Tableau Server and Tableau Online .......................... 804
Trust extensions on the safe list ....................................................................... 804
Checklist for the safe list: ............................................................................... 805
Add extensions to the safe list: ....................................................................... 805
Block specific extensions from running on Tableau Server ......................... 805
Turn off extensions for a site ............................................................................ 805
Show or hide user prompts to run extensions ............................................... 806
Turn off the default behavior for extensions ............................................... 806
Network Security .......................................................... 806
Client to Tableau Server ................................................. 807
Client access from the Internet ........................................ 807
Clickjack Protection ....................................................... 808
Tableau Server to your database ...................................... 808
Tableau Server to the Internet ......................................... 808
Communication with the repository ................................. 809
Server component communication in a cluster .................. 809
Clickjack Protection ....................................................... 809
Effects of clickjack protection ........................................ 810
Disabling clickjack protection ........................................ 811
Content Security Policy .................................................. 811
Configure and enable CSP .............................................. 812
   Step 1: Set default directives ...................................... 812
   Step 2: Add additional directives (optional) ...................... 814
   Step 3: Specify report-only directives (optional) ............... 815
   Step 4: Enable CSP on Tableau Server ......................... 815
   Step 5: Run tsm pending-changes apply ....................... 816
View CSP report .......................................................... 816
SSL ............................................................................. 817
Configure SSL for External HTTP Traffic to and from Tableau Server .... 817
   SSL certificate requirements ..................................... 818
Option for repository-ssl enable ................................................................. 831
Cluster environments ........................................................................... 831
Configure Postgres SSL to Allow Direct Connections from Clients ........ 832
Configure Mutual SSL Authentication .................................................... 833
Use the TSM web interface ................................................................ 833
Use the TSM CLI .................................................................................. 835
Step 1: Require SSL for external server communication ....................... 835
Step 2: Use mutual SSL ....................................................................... 835
Additional options for mutual SSL ....................................................... 836
Fallback authentication ........................................................................ 836
User name mapping ............................................................................ 837
Certificate Revocation List (CRL) ........................................................ 837
Mapping a Client Certificate to a User During Mutual Authentication ...... 837
User-name mapping options ................................................................ 838
Change the certificate mapping ............................................................ 839
Address user-name mapping ambiguity in multi-domain organizations .... 840
How Mutual SSL Authentication Works ............................................... 840
System User, sudo Privileges, and systemd .......................................... 841
Privilege separation ........................................................................... 842
sudo privileges ................................................................................. 842
systemd user service ....................................................................... 843
Running systemctl commands ......................................................... 843
Security Hardening Checklist .......................................................... 844
1. Update to the current version ....................................................... 844
2. Configure SSL/TLS with a valid, trusted certificate ..................... 844
3. Disable older versions of TLS ...................................................... 844
4. Disable Triple-DES cipher suite .................................................. 845
5. Configure SSL encryption for internal traffic ............................... 846
6. Enable firewall protection ........................................................... 846
7. Restrict access to the server computer and to important directories .... 847
8. Generate fresh secrets and tokens ................................................ 847
9. Disable services that you’re not using ........................................... 847

   REST API .................................................................................. 847
   JMX Service ............................................................................. 848

10. Verify session lifetime configuration ............................................ 848
11. Configure a server safelist for file-based data sources ................... 849
12. Enable HTTP Strict Transport Security for web browser clients ...... 850
13. Disable Guest access ................................................................... 850

Change List ................................................................................... 851

Manage Licenses ............................................................................ 852

Licensing Overview ......................................................................... 852
License metric: User-Based or Core-Based ....................................... 852
User-Based licenses ...................................................................... 853
Data Management Add-On .............................................................. 854
Tableau Server licenses and site roles after an upgrade ......................... 854
Tableau Server product key activation ............................................. 855
Tableau Server licensing and virtual machines (VMs) ............................ 855
View Server Licenses ........................................................................ 855
Viewing licenses from the Tableau Server web UI ................................. 856
Use the TSM web interface ............................................................... 856
Use the TSM CLI ............................................................................ 857
Refresh Expiration Date for the Product Key ...................................... 858
Before you begin ............................................................................. 859
Use the TSM web interface ............................................................... 859
Use the TSM CLI ............................................................................ 860
Add Capacity to Tableau Server .......................................................... 860
Use the TSM web interface ............................................................... 861
Use the TSM CLI ............................................................................ 864
Activate Tableau Server Offline - Adding a License .............................. 865
In this article ............................................................................... 866
Offline activation overview and prerequisites ..................................... 866
Log in to Tableau Services Manager ................................................ 871
Step 1 - Generate an offline activation request file ............................... 871
Step 2 - Upload the offline activation request to Tableau ..................... 872
Step 3 - Initialize or activate your license ......................................... 872
First time license activation .............................................................. 872
Tableau Server on Linux Administrator Guide

Navigate the Admin Areas of the Tableau Web Environment .................................................. 886
Access based on site role and number of sites ................................................................. 886
Server administrator ........................................................................................................ 886
Site administrator ............................................................................................................. 887
Server administrator tasks .............................................................................................. 888
Site administrator tasks .................................................................................................. 889
Sign in to Tableau Services Manager Web UI ............................................................... 889
Requirements .................................................................................................................. 890
Sign in to the TSM web UI ............................................................................................... 891
Customize Your Server ..................................................................................................... 892
Language and Locale for Tableau Server .......................................................................... 893
Supported Languages ....................................................................................................... 893
Default Settings ................................................................................................................ 893
How Language and Locale are Determined ...................................................................... 893
Use Custom Fonts in Tableau Server ................................................................................ 895
Manage Sites ..................................................................................................................... 895
Sites Overview .................................................................................................................. 895
What is a site ...................................................................................................................... 896
Authentication and sign-in credentials ............................................................................. 896
The Default site ................................................................................................................ 896
Why or why not add sites ............................................................................................... 897
Administrator-level access to sites .................................................................................... 898
Licensing and user limits ................................................................. 899

Add or Update Sites ...................................................................... 900

Add a site ..................................................................................... 900

Export or Import a Site ................................................................. 905

Site migration options ................................................................. 905

What information is or isn’t preserved in a site export ............... 906

Prepare the source and target sites ............................................. 907

Tips for importing to a target with fewer users or schedules than the source site .......................................................... 911

1. Export a site ............................................................................. 912

2. Generate the import mapping files ........................................... 912

3. Verify that site settings are mapped correctly ......................... 913

   To verify mapping files ........................................................... 914

4. Import the correctly mapped files to the target site ............... 914

Mapping file content reference .................................................. 915

   CSV file name: mappingsDomainMapperForGroups ................ 915

   CSV file name: mappingsScheduleMapper .............................. 916

   CSV file name: mappingsSiteMapper ....................................... 917

   CSV file name: mappingsSystemUserNameMapper .................. 917

   CSV file name: MappingsScheduleRecurrenceMapperWithAutoCreation . 918

Delete Sites .................................................................................. 918

Site Availability .......................................................................... 919
To activate or suspend a site ................................................................. 920

Allow Users to Save Revision History ................................................. 920

Notes ................................................................................................. 921

Permissions users need to work with revision history ......................... 921

Enable revision history and set the number of revisions allowed .......... 921

Clear all revisions ............................................................................ 922

Security for previewing and restoring workbooks ................................ 922

See also ............................................................................................ 922

Extract Refresh Schedules ................................................................. 922

Before refreshing extracts ................................................................. 923

Setting up refresh schedules ............................................................. 923

Refreshing extracts manually ............................................................. 924

Refreshing extracts from Tableau Desktop ......................................... 924

Enable Extract Refresh Scheduling and Failure Notification ............... 925

Managing schedules from the server .................................................. 926

How refresh failure emails work ....................................................... 926

How the last successful refresh date is determined ............................. 927

Create or Modify a Schedule ............................................................... 927

To create a new schedule .................................................................. 927

To modify an existing schedule ......................................................... 929

See also ............................................................................................ 930

Enable Custom Schedules for Subscriptions ...................................... 930
Enable custom schedules ................................................................. 930

How Scheduled Server Jobs are Prioritized ....................................... 931

Jobs and Tasks ........................................................................... 931

Priority Rules for Jobs .................................................................. 932

Configure Workbook Performance after a Scheduled Refresh ............... 933

Determine the performance impact .................................................. 933

Turn off workbook caching for the server ........................................ 934

Turn off workbook caching for a site .............................................. 934

Configure the workbook caching threshold ....................................... 935

Ensure Access to Subscriptions and Data-Driven Alerts ..................... 935

Set Up a Site for Subscriptions ....................................................... 936

Prerequisite: Configure the server to send subscription emails .......... 936

Enable subscriptions ..................................................................... 937

Test subscriptions in a site ............................................................ 938

Manage all user subscriptions ........................................................ 939

Suspended Subscriptions ............................................................... 939

Resume suspended subscriptions .................................................. 939

See also ...................................................................................... 940

Set Up for Data-Driven Alerts ......................................................... 940

Configure email for data-driven alerts ............................................ 941

Manage all data-driven alerts in a site ............................................ 941

Disable data-driven alerts for a site .............................................. 941
Control how often the server checks data-driven alerts ........................................... 942
Track the server’s alert-checking process ................................................................. 942
Identify and fix failing alerts .................................................................................... 942
Administrative Views ................................................................................................. 944
Navigating to administrative views ............................................................................ 944
Pre-built Administrative Views .................................................................................. 945
Performance of Views ................................................................................................. 945
Performance of Flow Runs ......................................................................................... 947
Traffic to Views ........................................................................................................... 948
Traffic to Data Sources ............................................................................................... 949
Actions by All Users .................................................................................................. 950
Actions by Specific User ............................................................................................. 952
Actions by Recent Users ............................................................................................. 953
Background Tasks for Extracts .................................................................................... 954
Understand this view ................................................................................................... 955
Status ......................................................................................................................... 955
See details about a task ............................................................................................... 956
Background Tasks for Non Extracts ............................................................................. 956
Upgrade Thumbnails Job ............................................................................................ 957
Troubleshooting ......................................................................................................... 959
Background Task Delay .............................................................................................. 959
Stats for Load Times ................................................................................................. 961
Stats for Space Usage ................................................................. 962
Server Disk Space ................................................................. 964
Desktop License Usage .......................................................... 966
Who has used Tableau in the last <nn> days? ........................... 967
What licenses have not been used in the last <nn> days ............... 968
Desktop License Expiration .................................................... 968
Create Custom Administrative Views ....................................... 970
Performance ........................................................................... 971
Tableau Server Performance Overview .................................... 971
General Performance Guidelines ............................................. 972
Hardware and Software .......................................................... 972
Configuration ......................................................................... 972
Server Resource Manager (SRM) .............................................. 973
Performance Monitoring Overview ......................................... 973
Collect Data with the Tableau Server Repository ...................... 974
Enable access to the Tableau Server repository ......................... 975
Connect to the Tableau Server repository ................................. 976
Performance Tuning ............................................................... 978
Optimize for User Traffic ......................................................... 978
When to optimize for user traffic ............................................. 979
Slow load times for views ....................................................... 979
High resource usage corresponding to user traffic ................... 980
Ways to optimize for user traffic ................................................................. 982
Adjust the number of VizQL server processes ........................................ 982
Adjust the number of other processes ...................................................... 982
Adjust the VizQL session timeout limit .................................................. 983
Refresh the cache less often ..................................................................... 983
Assess view responsiveness ..................................................................... 983
About Client-Side Rendering ................................................................... 984
Requirements ......................................................................................... 984
Configure the complexity threshold for computers and mobile devices ....... 984
Disable client-side rendering .................................................................... 985
Testing with the URL Parameter ............................................................... 986
Optimize for Extracts .............................................................................. 986
When to optimize for extracts ................................................................. 986
High CPU usage corresponds to extract schedules .................................. 986
Extracts fail or run slowly ......................................................................... 988
Ways to optimize for extracts ................................................................. 989
Adjust the extract refresh schedule ......................................................... 989
Speed up specific extracts ....................................................................... 990
Configure the execution mode for extract refreshes ................................. 990
Increase the number of backgrounder processes .................................... 991
Isolate processes ..................................................................................... 991
Optimize for Query Heavy Environments ................................................. 991
When to use this configuration ................................................................. 991
When not to use this configuration .......................................................... 992
Configuration ......................................................................................... 993
General configuration notes ................................................................. 994
Special configuration notes ................................................................. 994
Performance Benefits ........................................................................... 995
Additional Benefits .............................................................................. 995
When to Add Nodes and Reconfigure ....................................................... 996
Performance Tuning Examples ............................................................... 997
Performance Recording ......................................................................... 997
Create a Performance Recording ............................................................ 997
Start a Performance Recording for a View ............................................. 998
View a Performance Recording .............................................................. 999
Interpret a Performance Recording ......................................................... 999
Timeline ............................................................................................... 1000
Events ................................................................................................. 1000
Query .................................................................................................... 1002
Performance Monitoring Tools ............................................................... 1002
About Client-Side Rendering ................................................................. 1004
Requirements ....................................................................................... 1005
Configure the complexity threshold for computers and mobile devices ........ 1005
Disable client-side rendering ............................................................... 1006
Back up Tableau Server data .............................................................. 1026
Backup and Disk Space Usage ......................................................... 1027
Create a backup using the TSM command line interface (CLI) .............. 1028
Create a pre-upgrade backup .......................................................... 1028
Script the backup process ............................................................... 1029
Remove log files and clear temporary folders ..................................... 1029
Run the backup ............................................................................. 1029
Copy the backup file to another computer ........................................ 1030
Restore from a backup ..................................................................... 1030
Restore Tableau Server from a backup file ........................................ 1031
Server Maintenance ....................................................................... 1032
View Server Process Status ............................................................ 1033
Tableau Services Manager (TSM) Status page .................................... 1033
Tableau Server Status page ............................................................. 1035
Access Status Remotely .................................................................. 1036
Get Process Status as XML .............................................................. 1037
Status values in the XML ............................................................... 1039
Troubleshoot Server Processes ....................................................... 1040
Cluster Controller .......................................................................... 1040
File Store ....................................................................................... 1041
Repository ..................................................................................... 1043
VizQL Server .................................................................................. 1044
Clear Saved Data Connection Passwords ........................................ 1044

To clear saved data connection passwords for all server users: ......... 1045

Synchronize All Active Directory Groups on the Server .................. 1045

Before you begin ............................................................................. 1046

Synchronize Active Directory groups on a schedule ...................... 1046

Synchronize all Active Directory groups on demand ..................... 1047

View synchronization activity ......................................................... 1047

Set the minimum site role for users in an Active Directory group .... 1048

What happens when users are removed in the source Active Directory? .... 1049

Improving group synchronization performance .............................. 1049

Set the Default Start Page for All Users ....................................... 1050

To set the default start page for all users .................................... 1050

Disable Automatic Client Authentication ...................................... 1051

Remove Unneeded Files .................................................................. 1052

Server Settings (General) ............................................................... 1052

Stop or Restart the Tableau Server Computer ................................. 1055

tsm Command Line Reference ...................................................... 1056

Using the tsm CLI ............................................................................ 1057

Viewing help content in the shell .................................................. 1057

Synopsis ...................................................................................... 1057

Commands .................................................................................... 1058

Categories ................................................................................... 1058
tsm authentication ................................................................. 1058

tsm authentication kerberos <commands> ................................. 1059
Synopsis ................................................................. 1059
Options for kerberos configure ........................................... 1060

tsm authentication list ....................................................... 1060
Synopsis ................................................................. 1060
Options ................................................................. 1060

tsm authentication mutual-ssl <commands> ............................. 1060
Synopsis ................................................................. 1060
Options ................................................................. 1061

tsm authentication openid <commands> .................................. 1062
Synopsis ................................................................. 1062
Options for openid configure .............................................. 1062
Options for openid map-claims ........................................... 1064

tsm authentication saml <commands> .................................... 1065
Available commands ...................................................... 1065

tsm authentication saml configure ....................................... 1065
Synopsis ................................................................. 1065
Options ................................................................. 1065
Example ................................................................. 1068

tsm authentication saml enable and saml disable ...................... 1068
Synopsis ................................................................. 1068
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Examples</td>
<td>1142</td>
</tr>
<tr>
<td>tsm maintenance reindex-search</td>
<td>1142</td>
</tr>
<tr>
<td>Synopsis</td>
<td>1142</td>
</tr>
<tr>
<td>Option</td>
<td>1142</td>
</tr>
<tr>
<td>tsm maintenance reset-searchserver</td>
<td>1143</td>
</tr>
<tr>
<td>Synopsis</td>
<td>1143</td>
</tr>
<tr>
<td>Option</td>
<td>1143</td>
</tr>
<tr>
<td>tsm maintenance restore</td>
<td>1143</td>
</tr>
<tr>
<td>Synopsis</td>
<td>1143</td>
</tr>
<tr>
<td>Options</td>
<td>1143</td>
</tr>
<tr>
<td>tsm maintenance send-logs</td>
<td>1145</td>
</tr>
<tr>
<td>Synopsis</td>
<td>1145</td>
</tr>
<tr>
<td>Options</td>
<td>1145</td>
</tr>
<tr>
<td>tsm maintenance validate-resources</td>
<td>1146</td>
</tr>
<tr>
<td>Synopsis</td>
<td>1146</td>
</tr>
<tr>
<td>Options</td>
<td>1146</td>
</tr>
<tr>
<td>tsm maintenance ziplogs</td>
<td>1147</td>
</tr>
<tr>
<td>Synopsis</td>
<td>1147</td>
</tr>
<tr>
<td>Options</td>
<td>1147</td>
</tr>
<tr>
<td>Global options</td>
<td>1149</td>
</tr>
<tr>
<td>tsm pending-changes</td>
<td>1150</td>
</tr>
<tr>
<td>tsm pending-changes apply</td>
<td>1150</td>
</tr>
<tr>
<td>Command</td>
<td>Page</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------</td>
</tr>
<tr>
<td>tsm sites import-verified</td>
<td>1175</td>
</tr>
<tr>
<td>Synopsis</td>
<td>1175</td>
</tr>
<tr>
<td>Options</td>
<td>1175</td>
</tr>
<tr>
<td>tsm sites unlock</td>
<td>1176</td>
</tr>
<tr>
<td>Options</td>
<td>1176</td>
</tr>
<tr>
<td>Global options</td>
<td>1176</td>
</tr>
<tr>
<td>tsm start</td>
<td>1177</td>
</tr>
<tr>
<td>Synopsis</td>
<td>1178</td>
</tr>
<tr>
<td>Option</td>
<td>1178</td>
</tr>
<tr>
<td>Global options</td>
<td>1178</td>
</tr>
<tr>
<td>tsm status</td>
<td>1179</td>
</tr>
<tr>
<td>Synopsis</td>
<td>1179</td>
</tr>
<tr>
<td>Options</td>
<td>1179</td>
</tr>
<tr>
<td>Global options</td>
<td>1180</td>
</tr>
<tr>
<td>tsm stop</td>
<td>1181</td>
</tr>
<tr>
<td>Synopsis</td>
<td>1181</td>
</tr>
<tr>
<td>Option</td>
<td>1181</td>
</tr>
<tr>
<td>Global options</td>
<td>1182</td>
</tr>
<tr>
<td>tsm topology</td>
<td>1183</td>
</tr>
<tr>
<td>tsm topology cleanup-coordination-service</td>
<td>1183</td>
</tr>
<tr>
<td>Synopsis</td>
<td>1184</td>
</tr>
<tr>
<td>Option</td>
<td>1184</td>
</tr>
<tr>
<td>Command</td>
<td>Synopsis</td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
</tr>
<tr>
<td><code>tsm user-identity-store set-connection</code></td>
<td><code>Options</code></td>
</tr>
<tr>
<td><code>tsm user-identity-store set-group-mappings</code></td>
<td><code>Options</code></td>
</tr>
<tr>
<td><code>tsm user-identity-store set-user-mappings</code></td>
<td><code>Options</code></td>
</tr>
<tr>
<td><code>tsm user-identity-store verify-group-mappings</code></td>
<td><code>Options</code></td>
</tr>
<tr>
<td><code>tsm user-identity-store verify-user-mappings</code></td>
<td><code>Options</code></td>
</tr>
<tr>
<td><code>tsm version</code></td>
<td><code>Global options</code></td>
</tr>
<tr>
<td><code>tsm File Paths</code></td>
<td><code>Default locations for files</code></td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>LDAP GSSAPI bind options</td>
<td>1228</td>
</tr>
<tr>
<td>LDAP simple bind options</td>
<td>1229</td>
</tr>
<tr>
<td>Shared LDAP options</td>
<td>1229</td>
</tr>
<tr>
<td>identityStoreSchemaType options</td>
<td>1230</td>
</tr>
<tr>
<td>kerberosSettings Entity</td>
<td>1233</td>
</tr>
<tr>
<td>Configuration template</td>
<td>1233</td>
</tr>
<tr>
<td>Configuration file reference</td>
<td>1234</td>
</tr>
<tr>
<td>mutualSSLSettings Entity</td>
<td>1234</td>
</tr>
<tr>
<td>Configuration template</td>
<td>1235</td>
</tr>
<tr>
<td>Configuration file reference</td>
<td>1236</td>
</tr>
<tr>
<td>openIDSettings Entity</td>
<td>1239</td>
</tr>
<tr>
<td>Configuration template</td>
<td>1239</td>
</tr>
<tr>
<td>Configuration file reference</td>
<td>1240</td>
</tr>
<tr>
<td>samlSettings Entity</td>
<td>1243</td>
</tr>
<tr>
<td>Template categories and definitions</td>
<td>1244</td>
</tr>
<tr>
<td>samlSettings configuration template</td>
<td>1244</td>
</tr>
<tr>
<td>SAML configuration entity reference</td>
<td>1245</td>
</tr>
<tr>
<td>Pass the configuration file to Tableau Server</td>
<td>1251</td>
</tr>
<tr>
<td>See also</td>
<td>1251</td>
</tr>
<tr>
<td>sapHanaSettings Entity</td>
<td>1251</td>
</tr>
<tr>
<td>SAP HANA SAML settings</td>
<td>1252</td>
</tr>
<tr>
<td>Configuration template</td>
<td>1252</td>
</tr>
<tr>
<td>Configuration file reference</td>
<td>1253</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------</td>
</tr>
<tr>
<td>trustedAuthenticationSettings Entity</td>
<td>1254</td>
</tr>
<tr>
<td>Configuration template</td>
<td>1254</td>
</tr>
<tr>
<td>Configuration file reference</td>
<td>1255</td>
</tr>
<tr>
<td>web-data-connector-settings Entity</td>
<td>1257</td>
</tr>
<tr>
<td>Web data connector settings</td>
<td>1258</td>
</tr>
<tr>
<td>Configuration template</td>
<td>1258</td>
</tr>
<tr>
<td>Configuration file reference</td>
<td>1259</td>
</tr>
<tr>
<td>tabcmd</td>
<td>1260</td>
</tr>
<tr>
<td>Install tabcmd</td>
<td>1260</td>
</tr>
<tr>
<td>How to use tabcmd</td>
<td>1263</td>
</tr>
<tr>
<td>Examples</td>
<td>1263</td>
</tr>
<tr>
<td>tabcmd Commands</td>
<td>1264</td>
</tr>
<tr>
<td>addusers group-name</td>
<td>1265</td>
</tr>
<tr>
<td>Options</td>
<td>1265</td>
</tr>
<tr>
<td>Global options</td>
<td>1266</td>
</tr>
<tr>
<td>creategroup group-name</td>
<td>1268</td>
</tr>
<tr>
<td>Global options</td>
<td>1268</td>
</tr>
<tr>
<td>createproject project-name</td>
<td>1271</td>
</tr>
<tr>
<td>Options</td>
<td>1271</td>
</tr>
<tr>
<td>Global options</td>
<td>1271</td>
</tr>
<tr>
<td>createsite site-name</td>
<td>1274</td>
</tr>
<tr>
<td>Page</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td></td>
</tr>
<tr>
<td>Options .................................................................................................................. 1274</td>
<td></td>
</tr>
<tr>
<td>Global options ........................................................................................................ 1275</td>
<td></td>
</tr>
<tr>
<td>createsiteusers filename.csv ............................................................................... 1277</td>
<td></td>
</tr>
<tr>
<td>Local authentication .............................................................................................. 1278</td>
<td></td>
</tr>
<tr>
<td>Active Directory authentication ............................................................................ 1278</td>
<td></td>
</tr>
<tr>
<td>Options .................................................................................................................. 1279</td>
<td></td>
</tr>
<tr>
<td>Global options ........................................................................................................ 1280</td>
<td></td>
</tr>
<tr>
<td>createsiteusers filename.csv ............................................................................... 1283</td>
<td></td>
</tr>
<tr>
<td>Local authentication .............................................................................................. 1283</td>
<td></td>
</tr>
<tr>
<td>Active Directory authentication ............................................................................ 1283</td>
<td></td>
</tr>
<tr>
<td>Options .................................................................................................................. 1284</td>
<td></td>
</tr>
<tr>
<td>Global options ........................................................................................................ 1285</td>
<td></td>
</tr>
<tr>
<td>delete workbook-name or datasource-name ......................................................... 1288</td>
<td></td>
</tr>
<tr>
<td>Options .................................................................................................................. 1288</td>
<td></td>
</tr>
<tr>
<td>Global options ........................................................................................................ 1288</td>
<td></td>
</tr>
<tr>
<td>deletegroup group-name ...................................................................................... 1291</td>
<td></td>
</tr>
<tr>
<td>Global options ........................................................................................................ 1291</td>
<td></td>
</tr>
<tr>
<td>deleteproject project-name .................................................................................. 1293</td>
<td></td>
</tr>
<tr>
<td>Option ..................................................................................................................... 1294</td>
<td></td>
</tr>
<tr>
<td>Global options ........................................................................................................ 1294</td>
<td></td>
</tr>
<tr>
<td>deletesite site-name ............................................................................................... 1296</td>
<td></td>
</tr>
<tr>
<td>Global options ........................................................................................................ 1297</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Global options</td>
<td>1329</td>
</tr>
<tr>
<td>login</td>
<td>1331</td>
</tr>
<tr>
<td>Options</td>
<td>1333</td>
</tr>
<tr>
<td>logout</td>
<td>1335</td>
</tr>
<tr>
<td>publish filename.twb(x), filename.tds(x), or filename.hyper</td>
<td>1337</td>
</tr>
<tr>
<td>Options</td>
<td>1338</td>
</tr>
<tr>
<td>Global options</td>
<td>1341</td>
</tr>
<tr>
<td>publishsamples</td>
<td>1343</td>
</tr>
<tr>
<td>Description</td>
<td>1343</td>
</tr>
<tr>
<td>Syntax</td>
<td>1343</td>
</tr>
<tr>
<td>Options</td>
<td>1344</td>
</tr>
<tr>
<td>Global options</td>
<td>1344</td>
</tr>
<tr>
<td>refreshextracts workbook-name or datasource-name</td>
<td>1347</td>
</tr>
<tr>
<td>Options</td>
<td>1347</td>
</tr>
<tr>
<td>Global options</td>
<td>1349</td>
</tr>
<tr>
<td>removeusers group-name</td>
<td>1351</td>
</tr>
<tr>
<td>Options</td>
<td>1351</td>
</tr>
<tr>
<td>Global options</td>
<td>1352</td>
</tr>
<tr>
<td>runschedule schedule-name</td>
<td>1354</td>
</tr>
<tr>
<td>Global options</td>
<td>1354</td>
</tr>
<tr>
<td>set setting</td>
<td>1357</td>
</tr>
</tbody>
</table>
Cannot start Tableau Server after installation ........................................... 1371

Cannot create initial administrator account with multiple Active Directory (AD) domains ................................................................. 1372

Fonts ................................................................................................. 1372

Support for Asian character sets ...................................................... 1373

Initializing Tableau Server ............................................................... 1373

TSM initialization fails because the tableau user account exists but is not a member of the group tableau ........................................... 1373

Error initializing Tableau Server on unsupported system locale ........... 1374

Error initializing Tableau Server when en_US.utf8 is not included in locale list .............................................................................. 1374

Error: status 10 - initializing Tableau Server when data directory path includes a period .................................................................. 1374

Error initializing Tableau Server after reinstallation ........................... 1375

Activating Tableau Server ............................................................... 1375

Tableau Server license activation fails .............................................. 1375

Reindexing Tableau Server Search & Browse .................................... 1376

Problems that can be solved by reindexing Search & Browse .............. 1376

Restarting Tableau Server ............................................................... 1376

Restarting Tableau Server or applying changes fails ........................ 1376

Error restarting Tableau Server after adding or configuring a node ...... 1377

Backup/Restore .................................................................................. 1377

File locations ..................................................................................... 1378
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changing basefilepath does not change the location of an existing file</td>
<td>1378</td>
</tr>
<tr>
<td>TSM commands</td>
<td>1379</td>
</tr>
<tr>
<td>TSM command line does not show progress for long-running tasks</td>
<td>1379</td>
</tr>
<tr>
<td>Opening Firewall ports</td>
<td>1379</td>
</tr>
<tr>
<td>Manually opening firewall ports on Ubuntu</td>
<td>1379</td>
</tr>
<tr>
<td>OpenID fails on first sign-in attempt</td>
<td>1379</td>
</tr>
<tr>
<td>Administrative views do not display</td>
<td>1380</td>
</tr>
<tr>
<td>Changing locale on view</td>
<td>1380</td>
</tr>
<tr>
<td>Work with Log Files</td>
<td>1380</td>
</tr>
<tr>
<td>Investigating Tableau Server Issues</td>
<td>1381</td>
</tr>
<tr>
<td>Server Log File Locations</td>
<td>1383</td>
</tr>
<tr>
<td>Tableau Server Log and Configuration File Locations</td>
<td>1383</td>
</tr>
<tr>
<td>Logs not included in the ziplog archive</td>
<td>1383</td>
</tr>
<tr>
<td>Bash script logging</td>
<td>1384</td>
</tr>
<tr>
<td>System information</td>
<td>1384</td>
</tr>
<tr>
<td>Log Archive File Locations (unzipped archive)</td>
<td>1384</td>
</tr>
<tr>
<td>Log File Snapshots (Archive Logs)</td>
<td>1394</td>
</tr>
<tr>
<td>Use the TSM web interface</td>
<td>1394</td>
</tr>
<tr>
<td>Uploading log snapshots for Tableau Support</td>
<td>1396</td>
</tr>
<tr>
<td>Use the TSM CLI</td>
<td>1397</td>
</tr>
<tr>
<td>Sending log archives to Tableau Support</td>
<td>1398</td>
</tr>
<tr>
<td>Change Logging Levels</td>
<td>1399</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Logging Levels</td>
<td>1399</td>
</tr>
<tr>
<td>Change Logging Levels</td>
<td>1400</td>
</tr>
<tr>
<td>Reset Logging Levels</td>
<td>1401</td>
</tr>
<tr>
<td>Troubleshoot Tableau Server Install and Upgrade</td>
<td>1402</td>
</tr>
<tr>
<td>General Troubleshooting Steps</td>
<td>1402</td>
</tr>
<tr>
<td>Common Tableau Server Install Issues</td>
<td>1403</td>
</tr>
<tr>
<td>Installation logs location</td>
<td>1403</td>
</tr>
<tr>
<td>Unable to log into TSM or Tableau Server (sign in screen redisplayed after entering credentials)</td>
<td>1403</td>
</tr>
<tr>
<td>Multiple install attempts fail</td>
<td>1403</td>
</tr>
<tr>
<td>Install fails due to hardware requirements</td>
<td>1404</td>
</tr>
<tr>
<td>Common Tableau Server Upgrade Issues</td>
<td>1404</td>
</tr>
<tr>
<td>Upgrade logs location</td>
<td>1404</td>
</tr>
<tr>
<td>Upgrade multi-node, initializing additional node fails with &quot;Enter your credentials again&quot; error</td>
<td>1405</td>
</tr>
<tr>
<td>Upgrading fails due to lack of disk space</td>
<td>1405</td>
</tr>
<tr>
<td>Starting Tableau Server</td>
<td>1406</td>
</tr>
<tr>
<td>Tableau Server cannot determine if it fully started</td>
<td>1406</td>
</tr>
<tr>
<td>Tableau Server doesn't start</td>
<td>1406</td>
</tr>
<tr>
<td>Reindexing Tableau Server Search &amp; Browse</td>
<td>1406</td>
</tr>
<tr>
<td>Problems that can be solved by rebuilding Search &amp; Browse index</td>
<td>1406</td>
</tr>
<tr>
<td>Activating Tableau Server</td>
<td>1407</td>
</tr>
</tbody>
</table>
Tableau Server license activation fails .............................................. 1407
Confirm you can access the licensing server ..................................... 1407
Verify the date and time ................................................................. 1408
Force the product key to be read again ........................................... 1408
Send the contents of trusted storage to Tableau Support ................. 1409
Troubleshoot Server Sign in Problems ............................................. 1409
Troubleshooting scenarios ............................................................. 1410
Unable to log into TSM or Tableau Server (sign in screen redisplayed after entering credentials) ....................................................... 1410
Troubleshoot Licensing .................................................................. 1411
Handle an unlicensed server ........................................................... 1411
Unlicensed User-Based Server ....................................................... 1411
Unlicensed Core-Based Server ....................................................... 1411
Troubleshoot user-based licensing .................................................. 1412
A user or administrator is unlicensed due to license expiration .......... 1412
Server Administrator site role is unchanged when using a Creator license ................................................................. 1414
Licenses are not immediately available ......................................... 1414
A user with a Viewer license cannot open Tableau Server or Tableau Online workbooks from Tableau Desktop ......................... 1414
Handle an Unlicensed VizQL Server Process ................................... 1414
Tableau Services Manager (TSM) Command Timeout .................... 1415
Tableau Services Manager (TSM) Backup Timeout ......................... 1416
Troubleshoot Performance of Workbooks with Calculations

Scenario: You upgraded your Tableau Server recently. You are experiencing slow response times and the majority of your extracts have not been refreshed, so they are still in .tde format.

Scenario: You upgraded your Tableau Server recently. You are experiencing slow response times and a majority of your extracts have been refreshed and upgraded from .tde to .hyper.

Scenario: You upgraded your Tableau Server a while ago and you are experiencing slow response times. It is not practical for you to roll back using the backup you made prior to upgrade because your workbooks have changed since the upgrade, and the extracts have been upgraded to .hyper format.
Tableau Server Processes ................................................................. 1428
Licensed processes ........................................................................ 1428
Process workflow ........................................................................... 1441
Tableau Server Coordination Service ................................................ 1442
Configuration for the Coordination Service ...................................... 1443
The Coordination Service Quorum .................................................... 1443
Number of Coordination Service instances to use ............................ 1444
  If you reduce the number of nodes ................................................. 1444
Viewing Coordination Service Status .............................................. 1445
Tableau Server Data Engine ............................................................. 1446
Memory and CPU usage .................................................................. 1446
CPU usage ....................................................................................... 1446
Memory usage ................................................................................ 1447
Server configuration, Scalability, and Performance .............................. 1448
  Scalability: .................................................................................. 1448
  Performance: ............................................................................... 1449
Performance benefits ...................................................................... 1449
Tableau Server File Store .................................................................. 1450
  The decommission Command ....................................................... 1451
Tableau Server Gateway Process ...................................................... 1451
  Port assignment ......................................................................... 1452
  Log files for the gateway process ............................................... 1452
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway processes in a cluster</td>
<td>1453</td>
</tr>
<tr>
<td>Additional information</td>
<td>1453</td>
</tr>
<tr>
<td>Tableau Server Repository</td>
<td>1454</td>
</tr>
<tr>
<td>Preferred active repository</td>
<td>1454</td>
</tr>
<tr>
<td>The failoverrepository Command</td>
<td>1455</td>
</tr>
<tr>
<td>Tableau Server Microservice Containers</td>
<td>1455</td>
</tr>
<tr>
<td>Viewing Microservice Container Status</td>
<td>1456</td>
</tr>
<tr>
<td>Microservice Container Status</td>
<td>1456</td>
</tr>
<tr>
<td>Use the TSM web interface</td>
<td>1456</td>
</tr>
<tr>
<td>Use the TSM CLI</td>
<td>1457</td>
</tr>
<tr>
<td>Tableau Prep Conductor</td>
<td>1459</td>
</tr>
<tr>
<td>Overview</td>
<td>1459</td>
</tr>
<tr>
<td>Performance and Scale Recommendations</td>
<td>1460</td>
</tr>
<tr>
<td>Topology and Configuration</td>
<td>1460</td>
</tr>
<tr>
<td>Enabling Tableau Prep Conductor on Tableau Server</td>
<td>1461</td>
</tr>
<tr>
<td>Tableau Server Dynamic Topology Changes</td>
<td>1461</td>
</tr>
<tr>
<td>Example Scenarios</td>
<td>1462</td>
</tr>
<tr>
<td>Making dynamic topology changes</td>
<td>1462</td>
</tr>
<tr>
<td>Impact of dynamic topology changes</td>
<td>1463</td>
</tr>
<tr>
<td>Best practices</td>
<td>1463</td>
</tr>
<tr>
<td>Automating dynamic topology changes</td>
<td>1463</td>
</tr>
<tr>
<td>Additional information</td>
<td>1464</td>
</tr>
</tbody>
</table>
Step 1: Back up Tableau Server ........................................1498
Step 2: Remove Tableau Server .......................................1498
Step 3: Reinstall Tableau Server with new authentication type ....1498
LDAP Configuration Reference .........................................1499
Calculated configKeys ....................................................1512
Unsupported configKeys ..................................................1513
Plan Your Deployment

Get Started with Tableau Server on Linux ............................................................. 1
Server Administrator Overview ............................................................................. 2
Tableau Services Manager Overview ................................................................. 9
Infrastructure Planning ....................................................................................... 12

Get Started with Tableau Server on Linux


Plan

<table>
<thead>
<tr>
<th>Server Administrator Overview</th>
<th>Before you install...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure Planning</td>
<td>Security</td>
</tr>
<tr>
<td>Tableau Services Manager Overview</td>
<td>Planning a Site</td>
</tr>
</tbody>
</table>

Deploy

<table>
<thead>
<tr>
<th>Install and Configure Tableau Server</th>
<th>Install Drivers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed and High Availability Tableau Server Installations</td>
<td>Install Tableau Server in the Cloud</td>
</tr>
<tr>
<td>Jump-start Installation</td>
<td>Migrate Tableau Server from Windows to Linux</td>
</tr>
<tr>
<td>Tableau Mobile Deployment Guide</td>
<td>Tableau Desktop and Tableau Prep Deployment Guide</td>
</tr>
</tbody>
</table>
Manage Server

<table>
<thead>
<tr>
<th>tsm Command Line Reference</th>
<th>Extract Refresh Schedules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add or Update Sites</td>
<td>Add Users to Tableau Server</td>
</tr>
</tbody>
</table>

Manage Sites

<table>
<thead>
<tr>
<th>What is a site</th>
<th>Manage Users and Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Content Access</td>
<td>Manage Data</td>
</tr>
</tbody>
</table>

Automate and Extend

<table>
<thead>
<tr>
<th>Tableau Developer Tools</th>
<th>Tableau Tools and Samples on GitHub</th>
</tr>
</thead>
<tbody>
<tr>
<td>REST API</td>
<td>tsm Command Line Reference</td>
</tr>
<tr>
<td>Web Data Connector (WDC)</td>
<td>Extract API</td>
</tr>
<tr>
<td>Manage Dashboard Extensions in Tableau Server</td>
<td></td>
</tr>
</tbody>
</table>

Server Administrator Overview

Tableau Server on Linux integrates with a number of components in your IT infrastructure to provide a unique self-service data analytics culture for your users. It's important that you, as a server administrator, understand how Tableau Server fits into your IT infrastructure.

The topics in this section provide information on planning, deploying, tuning, and managing Tableau Server.

If you are new to Tableau Server, and you want to deploy it in your organization, we encourage you to deploy Tableau Server as a single server in a test environment first. The easiest
Tableau Server on Linux Administrator Guide

way to do a single-server installation and to understand the essential requirements is to follow the steps in Everybody’s Install Guide.

This topic provides a brief overview of how to think about Tableau Server and how it interacts with your existing IT infrastructure.


Architectural overview

Tableau Server is a collection of processes that work together to provide a full self-service analytic platform for your users. The following diagram shows a high-level architectural view of Tableau Server.

Multiple server processes (shown in blue above) work together to provide services at various tiers. The Gateway process is the component that redirects traffic from all Tableau clients to the available server nodes in a cluster.
Data Services is a logical grouping of services that provide data freshness, shared metadata management, governed data sources, and in-memory data. The underlying processes that power Data Services are the Backgrounder, Data Server and Data Engine processes.

Analytics Services, composed of the VizQL and Cache Server processes, provide user-facing visualization and analytics services and caching services.

Sharing and Collaboration, and Content Management Service are powered by the Application Server process. Core Tableau Server functionality such as user login, content management (projects, sites, permissioning, etc.) and administration activities are provided by the Application Server process.

All of the above services use and rely on the Repository process, which contains structured relational data like metadata, permissions, workbooks, data extracts, user info, and other data. The File Store process enables data extract file redundancy across the cluster and ensures extracts are locally available on all cluster nodes. Under heavier loads, extract files are available locally across the cluster for faster processing and rendering.

Tableau’s architecture is flexible, allowing you to run the platform just about anywhere. You can install Tableau Server on-premises, in your private cloud or data center, on Amazon EC2, on Google Cloud Platform, or on MS Azure. Tableau analytics platform can also run atop virtualization platforms. We recommend you follow the best practices for each virtualization platform to ensure the best performance from Tableau Server.

Tableau and your data

When you install Tableau Server into your organization, it becomes a core component of the analytics pipeline to the data your users need. It's important to understand how Tableau Server interacts with your business data. Specifically, Tableau Server can store extracts of data in your organization. It can also connect to live data sources. How you choose to provide the data to your Tableau users is informed by a number of variables: data source type, user scenario, performance and access requirements, and infrastructure conditions.
Tableau Server has not been architected as a data warehouse server where static, native data files are housed. In fact, using Tableau Server as a traditional data warehouse is a poor use of your investment. Rather, when it comes to data storage, we recommend hosting optimized data extracts on Tableau Server. While a data extract is often a subset of a larger data source in your organization, you can also create extracts for data sources that are overtaxed during work hours by scheduling the extract refresh for off-hours.

Extracts are also useful for modeling data or to enable highly-performant visualization authoring. For example, to improve visualization authoring and interaction performance you may optimize extracts by filtering the source data to the essential fields for a given department or project.

Tableau Server also provides direct, authorized access to live data sources, allowing users to build and run complex filtered queries against a variety of connected data sources. For this scenario, Tableau requires highly performant network access to the data sources in your organization and to those in the cloud. Tableau Server and the target data sources also need to be properly sized to handle the processing load required by high-volume, complex data operations.

**User access**

Tableau Server is also a web-based collaboration platform, where users connect to share, view, and interact with data visualizations and data sources from a variety of devices. This means that Tableau Server must be accessible to Tableau users within your local protected network. You can also extend access to data visualizations to desktop, mobile, and authenticated web users outside your organization.

Tableau Server integrates with the following user authentication solutions: Active Directory, SAML, OpenId, and Kerberos.

**Where should I install Tableau Server in my network?**

Because of the highly-sensitive nature of most data that organizations manage with Tableau Server, and because Tableau Server requires access to internal data stores, Tableau
Server must be run inside a protected network. Authenticated access from the internet is configured to connect to Tableau Server through a reverse proxy or a VPN solution.

Some organizations embed Tableau views in public webpages, or, for internal users, on generic web servers on the internal network.

Tableau Server can be configured to support such scenarios with either authenticated or anonymous access. For authorized access, where users can only view underlying data to which they have permission, you can configure trusted tickets with a generic web server. In this scenario, Tableau Server authorizes access to the underlying data in an embedded view. This scheme enables you to host interactive data visualizations on a web server in a DMZ or outside the protected network.

Anonymous access to embedded Tableau views requires that you enable "guest user" for Tableau Server. Guest user also requires that you license Tableau Server according to the number of cores you are running, rather than a named-user (interactor) model.

**Sizing and scalability**

Depending on the size and data usage in your organization, you can scale Tableau Server up or out. As you scale your server, you can also selectively allocate resources to meet your data needs and user needs.
Tableau Server on Linux Administrator Guide

When you scale up Tableau Server, you add hardware resources to a single server. For example, you might increase the memory and processing power of the computer running Tableau Server.

When you scale out Tableau Server, you add computers (or nodes). To create a highly available deployment with failover, you need at least three nodes. For example, you might run most CPU-intensive server processes on two nodes and use the third node for the gateway and coordination controller services.

Whether you scale up or scale out, you can selectively allocate resources by configuring the number and type of server processes that run. If your organization has a lot of data and creates a lot of data extracts, you can increase the number of processes that are dedicated to refreshing and storing extracts. Alternatively, if your organization wants to optimize for heavy user loads, you can increase the number of processes dedicated to responding to user requests. Additionally, you can integrate Tableau Server into industry-standard network load balancers to further optimize your server for user requests.

Tableau Server management model

Tableau Server has been designed to support a management scheme with two high-level administrators: server administrator and site administrator. In small organizations, these roles may be assumed by the same person or team, but in larger organizations, the roles often diverge.

In this model, server administrators are IT professionals who maintain and deploy heterogeneous server solutions. Essential areas for server administrators may include networking, hardware tuning and maintenance, security and access, and managing users and directory services. The tools and documentation that we deliver with Tableau Server for the server administrator support these core server IT areas.

Site administrator, on the other hand, is an administrative role specific to Tableau Server or Tableau Online deployments. The Tableau site administrator is fundamentally concerned with data content. The site administrator manages users and their access to projects, work-
books, and data sources. To learn about sites and how to plan your deployment for them, see What is a site

Management tools

Tableau Server includes a number of toolsets for managing the system:

- **Tableau Server administrator page**: This is the web-based administrative site that is installed on each Tableau Server instance. Tasks performed on the administrator page are day-to-day tasks for both server and site administrators. Server-related tasks include creating sites and site administrator accounts, optionally importing users, setting up synchronization with directory services, setting up extract refresh schedules, monitoring server performance and usage, and other global settings.

  Site-related tasks include managing content and assign permissions, running extract refreshes, create groups and projects, monitoring site activity, optionally adding users, and other content-related tasks.

  See Navigate the Admin Areas of the Tableau Web Environment.

  Permissions required for the Tableau Server administrator page are based on site roles. The site roles are generated and managed by Tableau Server.

- **tsm Command Line Reference**: This is the primary interface for server-wide configurations. The configurations made with TSM CLI are rarely revisited after initial configuration. For example: SSL, subscriptions, data caching, service account, SMTP alerting, user authentication, and single-sign on configuration are all performed with TSM CLI.

- **tabcmd**: You can use the tabcmd command-line utility on a Windows or Linux computer to create scripts to automate administrative tasks on your Tableau Server sites. For example, use tabcmd for creating or deleting users, projects, and groups.

- **REST API**: With the Tableau Server REST API you can manage and change Tableau Server resources programmatically, via HTTP. The API gives you simple access to the functionality behind the data sources, projects, workbooks, site users, and sites on a Tableau server. You can use this access to create your own custom applications or to script interactions with Tableau Server resources.
Security

As an application server connecting to data that may be highly-sensitive, Tableau Server supports and implements a number of industry security standards. Our server administration documentation includes best practices and implementation for user authentication, authorization, data security, and network security. While our default installation is secure by design, we also recommend following the security hardening checklist to further lock down your deployment.

For more information about security audit compliance, vulnerability reporting, and other security resources, visit http://www.tableau.com/security.

Tableau Services Manager Overview

This article provides an overview of Tableau Services Manager (TSM), which you can use to configure and administer Tableau Server. The TSM CLI was introduced with Tableau Server on Linux, version 10.5. Beginning with version 2018.2, the TSM Web UI is available.

- Functionality
- Components
- Authentication
- Connecting

Functionality

TSM gives server administrators command-line and web-based options for configuring and maintaining Tableau Server, including performing administrative task like backing up server data, restoring backups, creating log archives, and managing multi-node clusters. For example, you use TSM to perform the following tasks:

- Initial configuration of Tableau Server after installation
- Ongoing configuration management, including editing settings and changing the server topology
- Running administrative tasks such as backup, restore, and ziplogs
For administrators familiar with earlier versions of Tableau Server, TSM replaces the following tools from previous versions of Tableau Server:

- Tableau Server Configuration utility
- tabadmin command line utility
- Tableau Server Monitor

Components

TSM consists of services (called processes in this documentation) and clients. TSM processes are administrative services which manage Tableau Server processes. TSM processes run continuously after TSM is initialized, even when the rest of Tableau Server is offline.

TSM processes that run, even when Tableau Server is stopped include:

- Administration Agent
- Administration Controller
- Client File Service
- Coordination Service (based on Apache Zookeeper™)
- Service Manager
- Licensing Service

For more information about TSM processes and Tableau Server processes, see Tableau Server Processes.

TSM Authentication

Whether you use the TSM Web UI, the command line interface, or the TSM API, you need to authenticate to Tableau Server before you can perform administrative tasks. This user account is distinct from Tableau Server user accounts, including Tableau Server administrators and site administrators.

TSM delegates authentication of users to the underlying operating system. On Linux, this means that authentication is handled using Pluggable Authentication Modules (PAM). PAM is the standard on all Linux distributions on which Tableau Server is supported. If your
organization has configured PAM to authenticate with your directory service (Active Directory, LDAP), then you can authorize any user from that directory service to access TSM. In this scenario, any authenticated PAM user that is a member of the tsmadmin group is authorized to access TSM.

In the 2019.1 release, TSM authentication process uses PAM directly and then falls back to an authentication scheme using substitute user (su) if PAM fails or is not configured with a directory service. If PAM is not configured with a directory service then local accounts must be managed on the Linux computer. In these cases, TSM will use the su method of authentication: passing the user-provided credentials to run the true command in the /bin directory. If that command succeeds, then authentication is verified. Therefore, if the user is a member of the tsmadmin group, then the authenticated user is granted access to TSM.

Custom PAM service definition

TSM uses the standard PAM login service to authenticate. You can further customize TSM authentication behavior by creating a tableau PAM service file in /etc/pam.d. If this file exists, then it will be consulted instead of the PAM login service.

Connecting TSM clients

As a security measure, you can only connect to TSM with clients (CLI, Web UI, Rest API) over HTTPS. This is because TSM allows you to perform administrative tasks and to connect to TSM from other computers.

When you are connecting with a TSM client, you must connect to the Tableau Server instance running the TSM Administration Controller service.

TSM HTTPS connections rely on a self-signed certificate generated by the Tableau Server installer. This certificate is the Tableau installation CA certificate that signs the SSL certificates Tableau creates for encrypting traffic over HTTP. The Tableau installation CA certificate must be trusted by the systems connecting to TSM Administration Controller.

The TSM CLI client validates certificate trust from a different store than the TSM Web UI uses. The TSM CLI client refers to the trusted store in the local Java keystore to validate trust
for CA certificates. Since the TSM Web UI must establish connection with a web browser, trust is validated with the operating system's trusted keystore. The difference in how CA certificates are stored determines different trust configuration scenarios as outlined here:

- For TSM CLI communications on Tableau Server, the certificate trust is configured by default as part of the installation, node bootstrap, and upgrade processes. The Tableau installation CA certificate is added to the trusted store in the Java keystore. This allows you to access TSM using the CLI from any computer in the cluster without additional configuration. However, when accessing TSM Web UI, the browser will prompt you to trust the host running TSM Administration Controller service.
- For TSM CLI connections from remote computers, you will be prompted to trust the Tableau installation CA certificate the first time you connect to the Tableau Server running TSM Administration Controller. You can choose to trust the CA certificate, in which case you will not be prompted again on that computer until the certificate expires (default is 3 years). Or you can connect with a one-time trust by running your TSM command with the \(--trust-admin-controller-cert flag\).
- For TSM Web UI connections from remote computers, the browser will prompt you to trust the host running TSM Administration Controller service.

**Infrastructure Planning**

**Before you install...**

*Note:* You can find additional information about technical specifications for Tableau Server on the Tableau web site, [here](#).

This topic includes requirements and recommendations that you must consider before you install Tableau Server into a production environment.

If you want to install a single server, or if you want to do a minimal installation for test purposes, refer to our single-server installation guide, [Everybody's Install Guide](#).
If you are deploying Tableau Server in a distributed cluster, review Distributed Requirements in addition to the requirements and recommendations described in this topic.

Hardware recommendations

The following list describes the minimum hardware recommendations for a single-node installation of Tableau Server:

- 8 core, 2.0 GHz or higher processor
- 64-bit processor architecture
- 32 GB memory
- 50 GB disk space available, with a minimum of 15 GB allocated to the /opt directory, and the remainder allocated to the /var directory for data storage. See the section, Data directory, below.

Important: The disk space requirement cannot be checked until you initialize TSM. If you don’t have enough space, you won’t be told this until after you install the Tableau Server package.

To see the full list of recommendations and to see the minimum requirements, see Minimum Hardware Requirements and Recommendations for Tableau Server.

For public cloud deployments on Amazon Web Services and Google Cloud Platform, their “vCPU” is actually a CPU hyper-thread, and not a full CPU core. When sizing cloud instances, you will need twice as many vCPU as the Tableau Server CPU core requirements given (4 vCPU for a minimum trial installation, 16 vCPU for a recommended installation).

Operating system requirements

The following distributions of Linux are supported:
Red Hat Enterprise Linux (RHEL) 7.3 and higher, CentOS 7.3 and higher, Oracle Linux 7.3 and higher, and Amazon Linux 2.

These distributions are collectively referred to in this documentation as RHEL-like.

RHEL 8 is not supported.

The latest versions of Ubuntu 16.04 and 18.04 LTS only.

Non-LTS releases are not supported

Previous versions of CentOS and Ubuntu are not supported because Tableau Server requires systemd for process management.

Custom kernels are not supported.

In a multi-node installation of Tableau Server, all of the computer nodes where you are installing Tableau must run Linux and the same distribution of Linux.

**Note:** All nodes in a multi-node cluster must have the same type of operating system. You cannot install a multi-node instance of Tableau Server on a combination of Linux and Windows nodes.

**Installation directory**

The core Tableau Server bits are installed in the `/opt` directory by default.

- The directory where you install Tableau Server must have at least 15 GB of free disk space allocated to it. If you attempt to install Tableau Server on a computer that does not have enough space, the Tableau Server package will install, but you will be unable to continue with setup.
- You can specify a non-default install location on RHEL-like systems, but cannot change the location on Ubuntu.
- Do not specify a symbolic link or a directory location on a Network File System (NFS) volume when specifying a non-default install location on RHEL-like systems.
Data directory

By default, Tableau Server will create a data directory for all content and extracts that are managed by Tableau. The directory is created at /var/opt/tableau/tableau_server.

You can specify a different directory for data (extract) storage during installation. If you plan to use a different directory, do not create the directory. Instead, let Tableau Server setup create the directory. The data directory requires specific permissions that are set during the installation process.

To change the data directory, you must pass a flag along with the data directory path when you run the initialize-tsm script. See Help Output for initialize-tsm Script.

If you are changing the default data directory:

- Do not specify a symbolic link or a data directory location on a Network File System (NFS) volume.
- Do not specify a data directory location with a path that includes a period or space. If there is a period or space in the path, initialization will fail.

**Important:** You cannot change the data directory location after you’ve run initialize-tsm. The data directory location will persist for the life of the deployment, including subsequent upgrades.

Tableau Prep Conductor

Tableau Prep Conductor is one of the process on Tableau Server. It runs a flow, checks connection credentials, and sends alerts if a flow fails. Tableau Prep Conductor leverages the scheduling and tracking functionality of Tableau Server so you can automate running flows to update the flow output instead of logging into Tableau Prep Builder to manually run individual flows as your data changes.
Tableau Prep Conductor is licensed separately and is available through the Data Management Add-on license. For more information on Tableau Prep Conductor licensing, see Licensing Tableau Prep Conductor.

It is recommended that you enable Tableau Prep Conductor on a dedicated node. It is recommended that you enable Tableau Prep Conductor on a dedicated node to run flows. For more information:

- If you are installing a new Tableau Server, see Installing Tableau Server with Prep Conductor.
- If you are adding Tableau Prep Conductor to an existing installation of Tableau Server, see Add Tableau Prep Conductor to your Tableau Server Installation.

Additional requirements

Make sure that your environment also meets the following additional requirements:

Hostname

- Tableau Server must be able to resolve the hostname to an IP address either using the domain name server (DNS) or with a local host file on the computer running Tableau Server. By default, host files are stored at /etc/hosts.
- The hostname of the server must not change after you start Tableau Services Manager during the setup process. For example, this might happen if you use the cloud-init package to initialize a virtual machine, and you install Tableau Server on that virtual machine.
- Hostnames that include underscores (_) are not supported by Tableau Server on Linux.

Static IP address

The computer where you install Tableau Server must have a static IPv4 or IPv6 address.

Database drivers

To connect to specific data sources, the computer where you install Tableau Server must have the correct database drivers installed. For more information, see Database Drivers.
Available ports

TSM and Tableau Server each require an available TCP port in order for you to access them. TSM defaults to port 8850, and the Tableau Server Gateway service defaults to port 80. We strongly recommend that you ensure that both port 8850 and 80 are not in use on your system before installing Tableau Server. If those ports are not available, the TSM and gateway ports may be dynamically remapped to different port numbers, and there is currently no interface for displaying which port they have been remapped to.

See Tableau Services Manager Ports.

Local firewall configuration

If you are running a firewall on the computer where you will be installing Tableau Server, then you will need to open the following default ports for Tableau Server traffic. All port numbers, except 443 can be changed.

<table>
<thead>
<tr>
<th>Port</th>
<th>TCP/UDP</th>
<th>Used by ...</th>
<th>TYPE OF INSTALLATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP</td>
<td>Gateway</td>
<td>X</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>SSL. When Tableau Server is configured for SSL, the application server redirects requests to this port. Do not change this port.</td>
<td>X</td>
</tr>
<tr>
<td>8850</td>
<td>TCP</td>
<td>Tableau Services Manager.</td>
<td>X</td>
</tr>
<tr>
<td>8060</td>
<td>TCP</td>
<td>PostgreSQL database.</td>
<td>X</td>
</tr>
<tr>
<td>8061</td>
<td>TCP</td>
<td>PostgreSQL backup verification port</td>
<td>X</td>
</tr>
<tr>
<td>8000-</td>
<td>TCP</td>
<td>Range of ports reserved by default for</td>
<td>X</td>
</tr>
</tbody>
</table>
### System user and groups

Tableau Server on Linux uses one unprivileged user, and two groups for proper operation. Tableau will create the default account and groups during setup. Alternatively, you can specify existing accounts. See System user and groups.

### Sudo and root access

All installation tasks and administrative tasks for Tableau Server must be run as root. Often this is accomplished using the sudo command, but running the commands directly as the root user is also possible.

To install Tableau Server with the root account, you must specify a user account during installation. The account will be used for managing TSM. Specify the account by running the initialize-tsm script with the `-a` option. See Help Output for initialize-tsm Script.

### Account password

See Tableau Services Manager Ports and Configure Local Firewall.

<table>
<thead>
<tr>
<th>Port</th>
<th>TCP/UDP</th>
<th>Used by ...</th>
<th>TYPE OF INSTALLATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>9000</td>
<td></td>
<td>dynamic mapping of Tableau processes</td>
<td></td>
</tr>
<tr>
<td>27000-27009</td>
<td>TCP</td>
<td>Range of ports used by Tableau Server for License service. This range must be open on the node running the License service and accessible from other nodes. By default, the initial node runs the License service.</td>
<td>X</td>
</tr>
</tbody>
</table>
The user account that you use to install and administer Tableau Server must be able to authenticate with a password. That is, the user must not use another means of authenticating (for example public key authentication).

If the account you are using to install and initialize Tableau Server does not have a password, you can set one using the `passwd` command:

```
sudo passwd $USER
```

**Port access requirements**

If you want to install Tableau Server remotely, for example by means of SSH, ensure that the following ports are open:

- **8850.** The port used for the Tableau Services Manager (TSM) web interface. You can use this interface to configure Tableau Server.
- **80.** The port used for the main Tableau Server web interface.

The Tableau Server installer attempts to open these ports during the installation process, but it can only open these ports for the `firewalld` firewall. If your computer runs another firewall, you must open the ports before you install.

**Virtual Container environments**

Installation of Tableau Server in virtual container environments such as Docker have not been tested and are not supported. Tableau Server on Linux will not function as expected if installed in these environments.

**Package requirements**

**Systemd**

Tableau Server requires `systemd` to manage services. This package is installed by default on CentOS 7 and Ubuntu 16. If you decide to test Tableau Server on a modified version of these distributions, you can run the following command to confirm that `systemd` is installed:
If `systemd` is installed, the installation location is displayed. For example, you might see the following output:

```
whereis systemd
```

```
systemd: /usr/lib/systemd /etc/systemd /usr/share/systemd /usr/share/man/man1/systemd.1.gz
```

If you have systemd installed but the Tableau installer is failing requirements checks for systemd, it's likely that systemd is not running. To verify that systemd is running, run the following command:

```
ls /run/systemd
```

The output will be a list of files and directories. If systemd is running, the output will include `system`. If `system` is not in the output, then systemd is not running.

*Continue to the next step: Install and Configure Tableau Server.*

**Disk Space Requirements**

In general, when estimating the amount of additional disk space to allocate for Tableau Server for day-to-day usage, you must consider whether or not extracts will be published to Tableau Server, and consider the number of workbooks that you expect to publish to Tableau Server. If you anticipate using extracts, Tableau recommends that you begin with a few hundred gigabytes (GB). If you do not anticipate using extracts, you may only need around 50 GB to fulfill your usage needs.

Looking for Tableau Server on Windows? See [Disk Space Requirements](#).

Here are the factors that affect disk space requirements:
Publishing extracts to Tableau Server

Consider the number of extracts that will be published to Tableau Server and the size of each extract. Test your needs by publishing several extracts to Tableau Server, and then checking the disk space used. You can use this amount of disk space to help you figure out how many extracts will be published to Tableau Server over time as well as how each existing extract will increase in size.

Refreshing extracts

Consider the space needed by the temp directory during an extract refresh. The temp directory, which is where an extract is stored to during a refresh, may require up to three times the final file size of the extract.

While there may be some cases where .hyper extracts become bigger after an extract upgrade, there are other cases when .hyper extracts become smaller after an extract upgrade. In general, the overall disk size requirements should be the same for .hyper extracts as it was for .tde extracts.

Creating many workbooks

If using workbooks, consider the number of workbooks that will be published to Tableau Server. Individual workbooks tend to take up a small amount of disk space. However, if you anticipate thousands of workbooks being published, you may want to allocate additional disk space to accommodate those workbooks.

Logging

To assist with daily management and troubleshooting, Tableau Server creates log files as a part of its normal operations. Depending on the level at which the logging is configured, it can significantly impact the amount of disk space necessary on the Tableau Server computer.
Backing up and Restoring Tableau Server

You must have adequate disk space for database backup and restore processes to run successfully. In addition to the amount of space needed for the backup file, you need temporary disk space roughly 10 times the size of the backup file (so if your backup is 4 GB, you should have about 40 GB of temporary disk space available). Similarly you will need adequate temporary disk space for restoring from a backup.

When calculating disk space, be aware that background tasks for cleaning up old extracts are temporarily paused. This means that, for the duration of the backup, extract refreshes will leave extra files in place, adding to disk space usage. If your backup takes a long time, or if your organization uses many extracts that are regularly updated, this can result in a significant amount of temporary disk space usage. These old files will be removed after the backup is complete.

Recommended Baseline Configurations

Determining the topology (number of nodes, number of Tableau Server processes) of your Tableau Server deployment requires you to consider these variables: your environment, sources of data and management to provide self-service data access, workload, and usage. However you may not have enough information about these variables when you deploy Tableau Server for the first time. This topic describes three baseline architectures that can be used as starting points for your Tableau Server installations.

Hardware Recommendations

The hardware recommendations seen below are based on the hardware that the Tableau team uses to test Tableau Server scalability. We suggest that you use these recommendations as starting points for your production deployments. For proof-of-concept deployments, see Minimum Hardware Requirements and Recommendations for Tableau Server.

<table>
<thead>
<tr>
<th>Install Type</th>
<th>Processor</th>
<th>CPU</th>
<th>RAM</th>
<th>Free Disk Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Server</td>
<td>64-bit</td>
<td>8 physical cores</td>
<td>64 GB</td>
<td>500 GB - 1 TB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(16vCPUs), 2.0</td>
<td>(8GB/physical)</td>
<td></td>
</tr>
</tbody>
</table>
### Install Type

<table>
<thead>
<tr>
<th>Install Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
</tr>
<tr>
<td>CPU</td>
</tr>
<tr>
<td>RAM</td>
</tr>
<tr>
<td>Free Disk Space</td>
</tr>
</tbody>
</table>

| GHz or higher | Core) |

If you are adding Tableau Prep Conductor to your Tableau Server installation, it is recommended to add a second node and dedicate this to running Tableau Server Prep Conductor. This node should have a minimum or 4 physical cores (8 vCPUs), and 16 GB of RAM.

Multi-node and enterprise deployments

Nodes must meet or exceed the minimum hardware recommendations, except in the following scenarios where a node can be configured with 4 physical cores (8 vCPUs):

- Dedicated node for Backgrounder.
- Dedicated node for Tableau Prep Conductor.
- Move all the licensed process from the initial node to additional nodes.

**Note:** For deployments using virtual machines, Tableau recommends dedicated CPU affinity. If you are running Tableau Server in a virtual environment, use your VM host's best practices for vCPU allocation in relation to the number of physical CPU cores on the VM host. Typically 2 vCPUs = 1 physical core for Tableau Server. For example, for AWS installations, the 4 core minimum recommendation is equivalent of 8 AWS vCPUs. Similarly, follow the best practices provided by your virtual infrastructure provider to make sure Tableau Server has access to the appropriate compute, memory, and data resources. If you are installing Tableau Server in a virtual environment or a cloud-based deployment, see Virtual Machines and Public Cloud Deployments section later in this topic.

#### Estimating Disk Space

There are several factors that affect disk space requirements, including whether or not you will be publishing extracts, flows, and the number of workbooks to Tableau Server. For more...
Baseline Configurations

- Single Server Installations
- Two Node Installation - Specialized for extract heavy environments
- Two Node Installation - Specialized for flow environments
- High Availability Installations (HA)

Single Server Installations

Recommendations

We recommend using a single machine to install your Tableau Server for initial deployments with limited usage and are not mission critical. Single Server installations can also be expanded to multi-node installation as your workloads grow.

Here are some instances when a single server installation may not be right for you:

- If your system is considered mission critical and needs to be highly available. High availability is about minimizing the system downtime. It is achieved by eliminating single points of failure, and having a reliable failover mechanism. Tableau Server requires a minimum of a three-node configuration to provide redundancy and eliminate the single points of failure. This is one of the primary reasons to move to a multi-node configuration.

- If you have a lot of active users and a lot of extract refreshes, the two types of loads may be competing for the same resources on the machine. In such a scenario, a single server configuration may not be the right option as you may need additional specialized nodes to isolate the difference workloads.
Note: Active users represent the interactive, concurrent requests made to Tableau Server, including consuming dashboards on a laptop or mobile device, web authoring, and connecting to and querying Published Data Sources.
Server Configuration
Tableau Server on Linux Administrator Guide

Stand-alone Tableau Server node

- Gateway
- Search & Browse
- Application Server (VizPortal) x2
- VizQL Server x2
- Data Server x2
- Ask Data
- Elastic Server
- Cache Server x2
- Backgrounder x2
- Interactive Microservice container
- Non-Interactive Microservice Container
- Data Engine
- File Store
- Repository
- Licensing
- Cluster Controller
- Coordination Service
• Stand-alone single server node with all the processes installed on one machine.

• Below are the number of processes for an 8 core machine:
  - VizQL Server: Set to 2 instances (Number of physical cores divided by 4, up to a maximum of 4).
  - Backgrounder, Cache Server, and Data Server: Set to 2 instances.
  - All other processes, only one instance of the process is installed, regardless of hardware.

Note: One instance of Tableau Prep Conductor is automatically configured with Backgrounder, when you have the Data Management Product Key activated on your server. However, It is recommended that you have a dedicated node for Tableau Prep Conductor. If you plan to have flows on your Tableau Server, it is recommended that you use two or more nodes and dedicated one of these nodes to run only flows. The example configuration described above does not include Tableau Prep Conductor since it is a single node server.

Multi-Node Installations

Running Tableau Server on more than one machine is called a multi-node installation, or a cluster. There are various reasons why you might want to have a multi-node installation. For example, you may have heavy extract environments which can mean dedicating some hardware resources to Backgrounder process. For systems that have high availability requirements, you need a multi-node environment that has at least three nodes.

Two Node Installation - Specialized for extract heavy environments

Recommendations

Start with a two node configuration when the following conditions apply to you:
• **Extract heavy environment:** Majority of your data sources are extracts. Having just a few, extremely large extracts could put your deployment in this category, as would having very many small extracts.

• **Frequent extract refreshes:** Refreshing an extract is a CPU-intensive task. Deployments where extracts are frequently refreshed (for example, several times a day during business hours) are often helped by more emphasis on the background process, which handles refresh tasks.

**Important:** Two-node configurations do not meet the minimum requirements for high availability. If you need a system that is highly available, see High Availability Installations (HA).
Server Configuration
Tableau Server on Linux Administrator Guide

Tableau Server Initial Node
On the initial node, install all the processes except for the backgrounder. Below is the number of instances of the processes for an 8 core machine:

- VizQL Server: Set to 2 instances. (default calculation: Number of physical cores divided by 4, up to a maximum of 4).

- Cache Server, and Data Server: Set to 2 instances. One instance of Ask Data is automatically configured on the node that has Data Server.

- Elastic Server: Should be configured on the initial node. Elastic Server memory is configured to 256MB by default and can be configured to improve performance by using the elasticsearcherver.vmopts TSM configuration option. For more information, see tsm configuration set Options.

- All other processes, only one instance of the process is installed, regardless of hardware. One instance of Interactive Microservice Container is installed on a node that has Application Server enabled, and one instance of Non-Interactive Microservice Container is installed on a node that has Backgrounder enabled.

- Isolate backgrounder on the additional node. To calculate the minimum number of backgrounder processes to run on this node, divide the computer’s total number of physical cores by 4. To calculate the maximum number, divide the computer's total physical cores by 2. In the example shown above, both the nodes are on machines with 8 physical cores. When you install the backgrounder, Tableau Server automatically installs one instance of the Data Engine.

Note: This configuration assumes that you do not have Tableau Prep Conductor enabled on your Tableau Server. If are using Tableau Prep Conductor to schedule and manage flows, and have an extract heavy environment, we recommend that you have at least 3 nodes and use the 3 node configuration described later in this topic.

As you monitor and gather data about the performance and usage, you can fine tune and configure the number of instances for these processes. For example, on the node where it
is dedicated to running backgrounder, initially, you can set the number of backgrounder processes to minimum (total number of cores divided by four), and increase the number of backgrounder processes later if you find that:

- Extract refreshes are taking a long time to complete
- Subscriptions and alerts are not completing on time

For more information on performance tuning, see Performance Tuning topic.

Two Node Installation - Specialized for flow environments

Start with a two node configuration if you are planning to publish, schedule, and manage flows on your Tableau Server.

**Important:** Two-node configurations do not meet the minimum requirements for high availability. If you need a system that is highly available, see High Availability Installations (HA).
On the initial node, install all the processes. Below is the number of instances of the processes for an 8 core machine:

- VizQL Server: Set to 2 instances. (default calculation: Number of physical cores divided by 4, up to a maximum of 4).

- Cache Server, and Data Server: Set to 2 instances. One instance of Ask Data is automatically configured on the node that has Data Server.

- Backgrounder: Minimum 2, maximum 4. The diagram above shows the maximum for an 8 core node. Tableau Prep Conductor is automatically configured on the node where you have backgrounder installed. On the initial node, set the Backgrounder node role to run all job types including flows using the \texttt{tsm topology set-node-role tsm} configuration. For more information, see \texttt{tsm topology set-node-role}

- Elastic Server: Should be configured on the initial node. Elastic Server memory is configured to 256MB by default and can be configured to improve performance by using the \texttt{elasticsearch.vmopts} TSM configuration option. For more information, see \texttt{tsm configuration set Options}.

- All other processes, only one instance of the process is installed, regardless of hardware. One instance of Interactive Microservice Container is installed on a node that has Application Server enabled, and one instance of Non-Interactive Microservice Container is installed on a node that has Backgrounder enabled.

- Isolated the backgrounder on the additional node to run only flows. Use the \texttt{tsm topology set-node-role tsm} configuration to configure this setting. For more information, see \texttt{tsm topology set-node-role}

Note: If you have both a heavy extract environment, and schedule and manage flows on your server, we recommend that you use the 3 node configuration described below.
High Availability Installations (HA)

Recommendations

A highly available installation of Tableau Server is a distributed installation that is designed to maximize the availability of Tableau Server. High availability basically means that the system is available with minimal amount of downtime. To build in redundancy for HA related items such as repository, file redundancy, and failover, you need a minimum of three nodes. The tolerance for downtime will vary for each organization and depends on the SLAs you have established in your organization.

High availability is achieved by eliminating single points of failure and detecting failures and setting up a reliable failover system. HA in Tableau Server is mainly achieved by:

- File redundancy with multiple File Store/Data Engine instances.

- Active/Passive Repository across two nodes.

- Adding an external load balancer to make sure your installation is robust to Gateway failures and make sure that requests only get routed to functioning Gateway processes.

Server Configuration

Three-node configuration:
To build in redundancy, you need to add additional nodes to host instances of the repository and File Store/Data Engine processes. You can add instances of other processes, including multiple instances of a process on a node.

To build redundancy for the type of backgrounder jobs, have one of the nodes (initial
node in this example) run all type of jobs. Backgrounders run all types of jobs by
default. On one of the additional nodes, set the backgrounder to run only flows, and
the other additional node to run all jobs except for flows.

- The successful functioning of Tableau Server depends on a properly functioning
  Coordination Service. For server installations of three or more nodes, we recommend
  that you add additional instances of the Coordination Service by deploying a new
  Coordination Service ensemble. This provides redundancy and improved availability
  in the event that one instance of the Coordination Service has problems. For more
  information, see Deploy a Coordination Service Ensemble.

- Elastic Server cannot be configured to have redundancy and should only configured
  on the initial node in a three-node configuration. Elastic Server memory is configured
  to 256MB by default and can be configured to improve performance by using the
  elasticserver.vmopts TSM configuration option. For more information, see
  tsm configuration set Options.

- To reduce the system’s vulnerability, you can run multiple gateways and additional
  instances of some of the server processes. The fewest number of computers required
  to achieve this configuration is three.

- A second, passive instance of the repository has been added to one of the new nodes.

- One instance of Interactive Microservice Container is installed on a node that has
  Application Server enabled, and one instance of Non-Interactive Microservice Con-
  tainer is installed on a node that has Backgrounder enabled.

NOTE: In certain circumstances you may want to limit the processes running on your ini-
tial node. Reasons for doing this include wanting to run as few processes as possible on
the node to limit processing requests on the node. You might also remove licensed
Tableau Server processes from the node if you have a core-based license and do not
want the initial node cores to count against your core use. When considering this, be
aware that there can be performance implications for backup and restore when the
repository and File Store are moved off the initial node. For more information on Tableau Server licensed processes, see Tableau Server Processes. For additional information about the potential benefit of locating the repository and File Store on the initial node, see tsm maintenance backup.

Virtual Machines and Public Cloud Deployments

In general, the considerations and recommendations described in this topic apply to virtual environment and cloud deployments.

If you are running Tableau Server in a virtual environment, use your VM host's best practices for vCPU allocation in relation to the number of physical CPU cores on the VM host. Typically 2 vCPUs = 1 physical core for Tableau Server. For example, for AWS installations, the 4 core minimum recommendation is equivalent of 8 AWS vCPUs.

For more information on cloud-based deployments, see:

- Install Tableau Server in the Cloud.

Beyond Baseline Configurations

Disaster Recovery Considerations

While HA configurations reduce downtime, you may still encounter failures in case of a disaster or hardware failures. In addition to the above considerations, you should evaluate the importance of disaster recovery in your organization and plan for a deployment that helps you meet your disaster recovery goals and objectives.

When planning for disaster recovery (DR) in your Tableau environment, there are two main factors to consider:

- Recovery Time Objective (RTO), a measure of how much downtime your business can accept before a full recovery.
Influences how often you restore your backups to an alternative cluster and the amount of infrastructure investment.

- Recovery Point Objective (RPO), a measure of how much data loss your business can tolerate.
  - Influences how often you will need to take backups of your system.
  - For Tableau Server the RPO cannot be shorter than the time it takes to complete a full backup of your server.

The diagram below illustrates how to plan for a range of RTO requirements:

![Diagram showing RTO requirements](image)

Tableau Server Scalability

These baseline configurations may not be enough as your needs change and grow, and you might need to scale your Tableau Server beyond these configurations. Like other enterprise platforms, Tableau Server scales up by adding processor, memory, and disk to existing node, and scales out by adding more nodes to a cluster. However, scalability and per-
formance are heavily dependent on external systems and user activity. The configuration of your Tableau Server can be different depending on your requirements and variables:

<table>
<thead>
<tr>
<th>ENVIRONMENT</th>
<th>DATA</th>
<th>WORKLOAD</th>
<th>USAGE</th>
</tr>
</thead>
</table>
| • Physical of VM  
• Hardware and OS  
• Network  
• HA and DR | • Size  
• Live of Extract  
• Refresh Frequency  
• Latency | • # of Workbooks  
• Workbook Efficiency  
• Total Users  
• Peak Traffic | • Active Users  
• Interaction Type  
• User Geography  
• Internet Scale |

For more information on Tableau Server scalability and the variables affecting scalability, see Tableau Server Scalability whitepaper.

Identity Store

Tableau Server requires an identity store to manage user and group information. There are two kinds of identity stores: local and external. When you install Tableau Server you must configure either a local identity store or an external identity store.

For information about configuration options for the identity store, see identityStore Entity and LDAP Configuration Reference.

Local identity store

When you configure Tableau Server with a local identity store, all user and group information is stored and managed in the Tableau Server repository. In the local identity store scenario, there is no external source for users and groups.

External identity store

When you configure Tableau Server with an external store, all user and group information is stored and managed by an external directory service. Tableau Server must synchronize with the external identity store so that local copies of the users and groups exist in the
Tableau Server repository, but the external identity store is the master source for all user and group data.

If you have configured the Tableau Server identity store to communicate with an external LDAP directory, then all users (including the initial admin account) that you add to Tableau Server must have an account in the directory.

When Tableau Server is configured to use an external LDAP directory for authentication, you must first import user identities from the external directory to the identity store. When users sign in to Tableau Server, their credentials are passed to the external directory, which is responsible for authenticating the user; Tableau Server does not perform this authentication. However, the Tableau user names stored in the identity store are associated with rights and permissions for Tableau Server. Therefore, after authentication is verified, Tableau Server manages user access (authorization) for Tableau resources.

Active Directory is an example of an external user store. Tableau Server is optimized to interface with Active Directory. For example, when you install Tableau Server on an Active Directory domain-joined computer using the Configure Initial Node Settings, Setup will detect and configure most Active Directory settings. If, on the other hand, you are using TSM CLI to install Tableau Server, you must specify all the Active Directory settings. In this case, be sure to use the LDAP - Active Directory template to configure identity store.

If you are installing into Active Directory, we recommend that you review User Management in Active Directory Deployments before you deploy.

For all other external stores, Tableau Server supports LDAP as a generic way to communicate the identity store. For example, OpenLDAP is one of several LDAP server implementations with a flexible schema. Tableau Server can be configured to query the OpenLDAP server. To do so, the directory administrator must provide information about the schema. During setup, you must use Configure Initial Node Settings to configure a connection to other LDAP directories.
LDAP bind

Clients that wish to query a user store using LDAP must authenticate and establish a session. This is done by binding. There are multiple ways to bind. Simple binding is authenticating with a username and password. For organizations that connect to Tableau Server with simple bind, we recommend configuring an SSL encrypted connection, otherwise the credentials are sent over the wire in plaintext. Another type of binding Tableau Server supports is GSSAPI binding. GSSAPI uses Kerberos to authenticate. In Tableau Server’s case, Tableau Server is the client and the external user store is the LDAP server.

LDAP with GSSAPI (Kerberos) bind

We recommend binding to LDAP directory with GSSAPI. To bind with GSSAPI you will need a keytab file specifically for the Tableau Server service.

If you are installing into Active Directory, and the computer where you are installing Tableau Server is already joined to the domain, then the computer may already have a configuration file and a keytab file. In this case, the Kerberos files are for the operating system functionality and authentication. Strictly speaking, you can use these files for GSSAPI bind, but we don’t recommend using them. Instead, contact your Active Directory administrator and request a keytab specifically for the Tableau Server service. See Understanding Keytab Requirements.

Assuming your operating system has a properly configured keytab for authentication to the domain, then the Kerberos keyfile for GSSAPI bind is all you need for the base installation of Tableau Server. If you plan to use Kerberos authentication for users, then configure Kerberos for user authentication and Kerberos delegation to data sources after installation is complete.

LDAP over SSL

By default, LDAP with simple bind is not encrypted. If you are configuring LDAP with simple bind, we strongly recommend that you enable LDAP over SSL (LDAPS).
If you already have certificates installed for LDAP on the computer running Tableau Server, then LDAPS should work with minimal configuration during the installation process.

**Note:** If you are running Tableau Server in a distributed deployment, then you must manually copy the SSL certificate to each node in the cluster. Copy the certificate only to those nodes where the Tableau Server Application Server process is configured. Unlike other shared files in a cluster environment, the SSL certificate used for LDAP will not be automatically distributed by the Client File Service.

Specifically, if you have installed Tableau Server, and you have valid certificates installed in the Tableau keystore (/etc/opt/tableau/tableau_server-/tableauservicesmanagerca.jks), then you can specify SSL when you configure the identity store.

The password for the Java keystore is changeit. (Do not change the password for the Java keystore).

If you do not have certificates already in place on your computer that are configured for the LDAP server then you must obtain a SSL certificate for the LDAP server and import it into the Tableau system keystore.

Use the "keytool" Java tool to import certificates. In a default installation, this tool is installed with Tableau Server at /opt/tableau/tableau_server-/packages/respository.<installer version>/jre/bin/keytool.

The following command (for RHEL-like distributions) imports the certificate:

```
sudo "$PROGRAMFOLDER"/packages/repository*/jre/bin/keytool -import -file "$CERTSDIR" -alias "$OPENLDAPSSLSERVER" -keystore /etc/opt/tableau/tableau_server/tableauservicesmanagerca.jks -storepass changeit -noprompt
```
System user and groups

Tableau Server on Linux uses one user, and two groups for proper operation. The user and
groups can be local or from an LDAP directory service.

User

Tableau Server requires a service account. This account is an unprivileged user with nor-
mal login privileges.

LDAP/AD

If you want to use an existing user account in your LDAP directory, or if you want to create a
new user account in your LDAP directory for Tableau Server then you must disable account
and group creation during installation.

Specifically, you will need to set the `--disable-account-creation` and `--g` flags
when you run the initialize-tsm script. If you are not going to use the default names, then you
will also need to specify user and group names with the `--unprivileged-user` and the
`--tsm-authorized-group` flags. See Help Output for initialize-tsm Script for more
details.

The user account should be an unprivileged user with normal login privileges. Configure the
account with the following characteristics:

- Shell set to `/bin/bash`.

- For convenience, consider setting the home directory to the data directory path. The
  account must have ownership and write privileges to the home directory.

Local

If you want to use local users and groups, the `initialize-tsm` script can automatically
create them during installation. By default, the unprivileged account is named `tableau`. If
an account named `tableau` already exists, the Tableau will use it. To specify a different
account, see Help Output for initialize-tsm Script.
Groups

Tableau Server requires two groups for operation.

In a default installation, the local `tableau` account belongs to a primary group named `tableau`. However, if you specify an alternate unprivileged user during installation, then the primary group for that alternate account will be used. As a convenience, any account can be added to this group to be able to read the Tableau Server log files (without becoming root).

The second group is used to authorize which users are authorized to authenticate to Tableau Services Manager (TSM). Any user in this group will be able to send commands to TSM, so it should be restricted to Tableau Server administrators. By default, this group is named `tsadmin`.

If there is an existing LDAP group that matches these criteria, it can be used. Otherwise, a new LDAP group could be created, and all Tableau Server administrators can be added to this new group. Note that at least one administrator must be in this group in order to successfully initialize Tableau Server.

Authenticating clients

Basic user authentication in Tableau Server is by username and password sign-in for both local and external user stores. In the local case, user passwords are stored as a hashed password in the repository. In the external case, Tableau Server passes the credentials to the external user store and awaits a response as to whether the credentials are valid. External user stores can also handle other kinds of authentication like Kerberos or SSPI (Active Directory only), but the concept is still the same, Tableau Server delegates the credentials or user to the external store and awaits a response.

You can configure Tableau Server such that username-password sign-in is disabled. In these scenarios other authentication methods, such as trusted authentication, OpenID, or SAML can be used. See Authentication.
User Management in Active Directory Deployments

This topic describes important technical details that you should be familiar with if you use Active Directory to authenticate users for Tableau Server. This topic assumes that you are familiar with Active Directory user management and basic Active Directory schema and domain concepts.

**Note:** If you run Tableau Server on Linux, all external directory communication is configured and managed with a LDAP identity store. In the context of user and group synchronization, Tableau Server configured with LDAP identity store is equivalent to Active Directory. Active Directory synchronization features in Tableau Server function seamlessly with properly configured LDAP directory solutions.

Active Directory user authentication and Tableau Server

Tableau Server stores all user names in the Tableau Server identity store, which is managed by the repository. If Tableau Server is configured to use Active Directory for authentication, you must first import user identities from Active Directory to the identity store. When users sign in to Tableau Server, their credentials are passed to Active Directory, which is responsible for authenticating the user; Tableau Server does not perform this authentication. (By default, NTLM is used for authentication, but you can enable Kerberos or SAML for single sign-on functionality—however, in all these cases, authentication is left to Active Directory.) However, the Tableau user names stored in the identity store are associated with rights and permissions for Tableau Server. Therefore, after authentication is verified, Tableau Server manages user access (authorization) for Tableau resources.

Active Directory user name attributes and Tableau Server

Active Directory uniquely identifies user objects using several attributes. (For details, see [User Naming Attributes](https://msdn.microsoft.com) on the MSDN website.) Tableau Server relies on two Active Directory user naming attributes:
sAMAccountName. This attribute specifies the logon name that was originally designed for use with older versions of Windows. In many organizations, this name is combined with the NetBIOS name for authentication, using a format like example\jsmith, where example is the NetBIOS name and jsmith is the sAMAccountName value. Due to the original design in Windows, the sAMAccountName value must be less than 20 characters.

In the Windows Active Directory Users and Computers administrative console, this value is in the field labeled User logon name (pre-Windows 2000) on the Account tab of the user object.

userPrincipalName (UPN). This attribute specifies a user name in the format jsmith@example.com, where jsmith is the UPN prefix and @example.com is the UPN suffix.

In the Windows Active Directory Users and Computers administrative console, the UPN is a concatenation of two fields on the Account tab of the user object: the User logon name field, and the domain drop-down list next to it.

Adding users from Active Directory

You can add users individually from Active Directory, either by typing them in the server environment or by creating a CSV file and importing the users. You can also add Active Directory users by creating a group via Active Directory and importing all of the group's users. The result can be different depending on which approach you're using.

Adding user groups

If you import an Active Directory user group, Tableau will import all users from the group using the sAMAccountName.

Sync behavior when removing users from Active Directory

Users cannot be automatically removed from Tableau Server through an Active Directory sync operation. Users that are disabled, deleted, or removed from groups in Active Directory
remain on Tableau Server so that you can audit and reassign the user's content before removing the user's account completely.

However, Tableau Server will act upon user objects differently based how the status of that user object changes in Active Directory. There are two scenarios: deleting/disabling users in Active Directory or removing users from synchronized groups in Active Directory.

When you delete or disable a user in Active Directory and then synchronize that user's group on Tableau Server, the following occurs:

- The user is removed from the Tableau Server group you synchronized.
- The user's role is set to "unlicensed."
- The user will still belong to the All Users group.
- The user is unable to sign in to Tableau Server.

When you remove a user from a group in Active Directory and then synchronize that group on Tableau Server, the following occurs:

- The user is removed from the Tableau Server group you synchronized.
- The user's role is retained: it is not set to "unlicensed."
- The user will still belong to the All Users group.
- The user will still have permission to the Tableau Server with access to everything that the All Users group is granted permission to use.

In both instances, to remove a user from Tableau Server, the server administrator must delete the user from the Server Users page in Tableau Server.

**Domain nicknames**

In Tableau Server, domain nickname is equivalent to the Windows NetBIOS domain name. In a Windows Active Directory forest, a fully qualified domain name (FQDN) can have an arbitrary NetBIOS name. The NetBIOS name is used as the domain identifier when a user logs in to Active Directory.

For example, the FQDN `west.na.corp.lan` might be configured with a NetBIOS name (nickname) of `SEATTLE`. The user `j smith` in that domain could log on to Windows using either of the following user names:
Tableau Server on Linux Administrator Guide

- west.na.corp.example.com\jsmith
- SEATTLE\jsmith

If you want your users to sign in to Tableau Server with a NetBIOS name instead of the FQDN, then you'll need to verify that the nickname value for each domain where users log in is set. See editdomain for information on how to view and set the nickname value for each domain.

Support for multiple domains

You can add users from a domain that's different from the domain of the Tableau Server computer in these cases:

- Two-way trust has been established between the server's domain and the users' domain.

- The server's domain trusts the users' domain (one-way trust). See Domain Trust Requirements.

The first time you add a user from the non-server domain, use the fully-qualified domain name with the user name. Any additional users you add from that domain can be added using the domain's nickname, provided the nickname matches the NetBIOS name.

Duplicate display names

If user display names are not unique across multiple domains, then managing users with the same display name in Tableau can be confusing. Tableau Server will display the same name for two users. For example, consider an organization with two domains, example.lan and example2.lan. If user John Smith exists in both domains, then adding that user to groups and other administrative tasks will be confusing in Tableau Server. In this scenario, consider updating the display name in Active Directory for one of the users to differentiate the accounts.
Sign in to Tableau Server with NetBIOS name

Users can sign in to Tableau Server using the domain nickname (NetBIOS name), for example, SEATTLE\jsmith.

Tableau Server cannot query for NetBIOS name for a given FQDN. As a result, Tableau sets the nickname of a given FQDN according to the first entry in the namespace. For example, given the FQDN west.na.corp.lan, Tableau sets the nickname to west.

Therefore, you might need to update the domain nickname on Tableau Server before users can sign in using the nickname. If you do not update the nickname, users will have to sign in using a fully qualified domain name. For more information, see Users From New Domain Unable to Log In and Do Not Appear in User List in the Tableau Knowledge Base.

Domain Trust Requirements

When you run Tableau Server in an Active Directory environment across multiple domains (either in the same Active Directory forest or in different forests), some Tableau functionality is dependent on the trust relationship between the domains. For example, some administrators manage users in domains that are separate from where they deploy server applications, such as Tableau Server. In other organizations, a Tableau Server deployment might be shared with external partners or with different partners in the organization. Finally, Windows-authenticated data sources, such as SQL Server, MSAS, or Oracle, that Tableau Server connects to may also be in other domains.

If it’s feasible, we recommend configuring two-way trust between all domains that interact with Tableau Server. If this is not possible, Tableau Server can be configured to support user authentication where a one-way trust has been configured. In this case, a one-way trust between domains is supported when the domain in which Tableau Server is installed is configured to trust the domain where user accounts reside.

The following illustration shows one-way trust between the domain where Tableau Server is installed and the domain where user accounts reside:
In this scenario, Tableau Server is in the dev.local domain, and users from the users.lan Active Directory domain are imported into Tableau Server. A one-way trust is required for this scenario; specifically, the dev.local domain is configured to trust the users.lan domain. Users in the users.lan domain can access Tableau Server in the dev.local with their normal Active Directory credentials. However, you may need to update the domain nickname on Tableau Server before users log on with the nickname. Refer to the Tableau Knowledge Base for more information.

When you configure Tableau Server for this scenario, specify the user domain during installation. See Configure Initial Node Settings.

Kerberos single sign-on is supported in this one-way trust scenario.

Review User Management in Active Directory Deployments to understand how multiple domains, domain naming, NetBIOS, and Active Directory user name format influence Tableau user management.

Connecting to live data in one-way trust scenarios

In the one-way trust scenario, users connecting to Tableau Server can connect to live data that's hosted in the cloud or on any other data source on premises that does not rely on Windows authentication.
Data sources that require Windows-authentication might have additional authentication requirements that complicate the scenario, or that can even prevent Tableau Server users from connecting. This is because Tableau Server uses a service account for authentication with such data sources. If you are running Tableau Server in a different domain than data sources that use Windows authentication, verify that the service account that is used for Tableau Server can access the data source.

Communicating with the Internet

In most enterprises, Tableau Server needs to communicate with the internet. Tableau Server was designed to operate inside a protected internal network. Do not set up Tableau Server directly on the internet or in a DMZ. Instead, communications between your network and the internet should be mediated using proxy servers. If the computer running Tableau Server cannot access the internet directly, then you may need to deploy forward proxy servers to mediate traffic from inside the network to targets on the internet. Tableau Server doesn't support pass-through or manual proxy authentication.

For inbound traffic, we recommend running Tableau Server behind reverse proxy servers.

How Tableau communicates with the internet

Tableau Server requires outbound access to the internet for these scenarios:

- Working with maps. Tableau uses map data that is hosted externally.

  Tableau Server needs to connect to maps.tableausoftware.com using port 443. If it cannot make this connection, maps may fail to load. You can test connectivity by accessing the Miami and Havana (blue water) map.

  This is the URL:

  https://maps.tableausoftware.com/tile/d_Mode=named|from=tableau1_2_base/-mode=named|from=tableau1_2_admin0_borders_mode=named|from=tableau1_2_place_
• Connecting to the Tableau send-logs server.

You can upload log files to Tableau when working with Support. See `tsm maintenance send-logs`. To successfully upload files to Tableau, your Tableau Server must be able to communicate with the send-logs server on port 443:

`report-issue.tableau.com:443`

• Licensing. Tableau products connect to the internet to activate product keys. Unless you activate Tableau software with the Offline Activation Tool, all Tableau products must have access to the internet to validate licenses. Specifically Tableau requires internet access during the following licensing operations: activation, deactivation, and on the refresh maintenance date. For more information about these operations, see Manage Licenses.

Tableau Server needs to connection to the following internet locations for licensing purposes:

• `licensing.tableau.com:443`

• `atr.licensing.tableau.com:443`

• `o.ss2.us`

• `ocsp.rootg2.amazontrust.com`

• `ocsp.rootca1.amazontrust.com`

• `ocsp.sca1b.amazontrust.com`

• `crt.sca1b.amazontrust.com`

• `crt.rootca1.amazontrust.com`
Requests to the above domains may be on port 80 or 443.

If Tableau Server cannot make a connection while attempting to activate its license, you will be prompted to do an offline activation.

- Working with external or cloud-based data.

Tableau Server needs to connect to the following internet location for Box, Dropbox, and OneDrive services:

`galop.connectors.tableau.com:443`

Tableau Server can run without internet access. For more information about deploying Tableau Server in organizations without access to the internet, see Install Tableau Server in a Disconnected (Air-Gapped) Environment.

In many enterprises, users also need to access Tableau Server from outside the network (that is, from the internet). For example, in many enterprises, users want to be able to reach Tableau Server from their mobile devices in order to interact with views that are stored on
the server. To configure access to Tableau Server from the internet or from mobile devices, you should use a reverse proxy. See Configuring Proxies for Tableau Server.

**Configuring Proxies for Tableau Server**

In most enterprises, Tableau Server needs to communicate with the internet. Tableau Server was designed to operate inside a protected internal network. Do not set up Tableau Server directly on the internet or in a DMZ. Instead, communications between your network and the internet should be mediated using proxy servers. Forward proxy servers mediate traffic from inside the network to targets on the internet. Reverse proxy servers mediate traffic from the internet to targets inside the network.

**Who should read this article?**

This article is for IT professionals who are experienced with general networking and gateway proxy solutions. The article describes how and when Tableau requires internet access, and describes how to configure your network and Tableau to use forward and reverse proxy servers for access to and from the internet. There are many third-party proxy solutions available, so some of the content in the article is necessarily generic.

Before you configure a proxy server, see Communicating with the Internet.

**Configure a forward proxy server**

To enable communication from Tableau Server to the internet, deploy Tableau Server behind a forward proxy server. When Tableau Server needs access to the internet, it doesn't send the request directly to the internet. Instead, it sends the request to the forward proxy, which in turn forwards the request. Forward proxies help administrators manage traffic out to the internet for tasks such as load balancing, blocking access to sites, etc.

If you use a forward proxy, you must configure the computers that run Tableau Server inside the network to send traffic to the forward proxy. Tableau Server doesn't support pass-through or manual proxy authentication.
Configuring Tableau Server on Linux to work with a forward proxy

We recommend configuring Tableau Server to work with your forward proxy solution as part of the installation process. Specifically, configure Tableau Server when you run ./initialize-tsm as described in Install and Initialize TSM, or as part of Automated Installation of Tableau Server.

The procedure below describes how to create a forward proxy configuration file for Tableau Server on Linux.

The configuration file is stored in the following directory:

~<unprivileged_user>/.config/systemd/tableau_server.conf.d

By default, Tableau Server creates the unprivileged user, tableau. Therefore, the default path to the configuration directory is:

~tableau/.config/systemd/tableau_server.conf.d

The proxy configuration file name in this topic and in the configuration file below is referred to as 20-proxy.conf. You can name this file according to your own convention, but it must use the .conf extension. systemd will process files stored in the tableau_server.conf.d directory in lexical order according to file name.

1. Run the tsm stop command.

2. Start a session as the unprivileged user. By default, tableau, is the unprivileged user created by Tableau Server during installation. Run the following command:

   sudo su -l tableau

3. Create or open the 20-proxy.conf file in the tableau_server.conf.d directory. If you configured forward proxy during setup, then the 20-proxy.conf file has already been created.
Create the file. Run the following command:

```
touch .config/systemd/tableau_server.conf.d/20-proxy.-conf
```

Open the `20-proxy.conf` file in a text editor.

4. Copy the **Proxy configuration file contents** into the file. If you are editing an existing file, take care not to delete the configuration. The **Proxy configuration file contents** include instructions on how to set forward proxy configurations. After you have edited and saved the file go to Step 5.

**Proxy configuration file contents**

```
# Always edit this file on Tableau Server as the unprivileged user. By default, tableau, is the unprivileged user created by Tableau Server during installation.
# Set environment variables http_proxy and https_proxy to point to your proxy host.
# For example, to set the proxy to example-host for ports 80 and 443, run the following commands:
#
http_proxy=http://example-host:80/
https_proxy=http://example-host:443/
#
# Take care to use 'http' when you specify the URL for the
https_proxy environmental variable.
# Do not specify the 'https' protocol for the value of the
https_proxy environmental variable.
#
# To bypass the proxy server, specify exceptions in the no_proxy variable. Use this variable if your proxy server does
```
not route internal addresses.
# You must also add exceptions to this proxy configuration
to guarantee that all communications within a local
Tableau Server cluster (if you have one now or will have
one later) do not route to the proxy server.
# Enter both the host name and the IP address for each com-
puter. Additionally, include the cannonical host name (loc-
alhost) and IP address (127.0.0.1) for the local computer.
# For example, to specify exceptions for a three-node
cluster:
#
no_proxy-
="lo-
calhost,127.0.0.1,hostname1,hostname2,hostname3,IP1,IP2,IP3"
#
# Where "hostname1" is the actual hostname of node 1, and
"IP1" is the actual IP address of node 1, etc.

5. Restart the TSM services. Run the following commands:

```bash
systemctl --user restart tabadmincontroller_0
systemctl --user restart appzookeeper_0
systemctl --user restart clientfileservice_0
systemctl --user restart fnplicenseservice_0
systemctl --user restart licenseservice_0
systemctl --user restart tabadminagent_0
systemctl --user restart tabsvc_0

tsm restart
```
How a reverse proxy works with Tableau Server

A reverse proxy is a server that receives requests from external (internet) clients and forwards them to Tableau Server. Why use a reverse proxy? The basic answer is security. A reverse proxy makes Tableau Server available to the internet without having to expose the individual IP address of that particular Tableau Server to the internet. A reverse proxy also acts as an authentication and pass-through device, so that no data is stored where people outside the company can get to it. This requirement can be important for organizations that are subject to various privacy regulations such as PCI, HIPAA, or SOX.

The following diagram illustrates the communication path when a client makes a request to Tableau Server that is configured to work with a reverse proxy server.

1. An external client initiates a connection to Tableau Server. The client uses the public URL that's been configured for the reverse proxy server, such as https://tableau.example.com. (The client doesn't know that it's accessing a reverse proxy.)

2. The reverse proxy maps that request in turn to a request to Tableau Server. The reverse proxy can be configured to authenticate the client (using SSL/TLS) as a precondition to passing the request to Tableau Server.

3. Tableau Server gets the request and sends its response to the reverse proxy.

4. The reverse proxy sends the content back to the client. As far as the client is concerned, it just had an interaction with Tableau Server, and has no way to know that the communication was mediated by the reverse proxy.
Proxy servers and SSL

For better security, you should configure reverse proxy servers to use SSL for any traffic that's external to your network. This helps to ensure privacy, content integrity, and authentication. Unless you’ve deployed other security measures to protect traffic between your internet gateway and Tableau Server, we also recommend configuring SSL between the gateway proxy and Tableau Server. You can use internal or self-signed certificates to encrypt traffic between Tableau Servers and other internal computers.

Mobile access

Tableau Server adds an X-header to all HTTP responses for Tableau Mobile sessions. By default, most proxy solutions will preserve X-headers. If your proxy solution does not preserve X-headers, then you will need to configure your proxy server to preserve the following header to all HTTP responses for Mobile client sessions: X-Tableau: Tableau Server.

If you have configured authentication at the proxy server gateway, then your proxy server must respond to Tableau Mobile HTTP requests with a HTTP 302 response. The 302 must include a redirect to the identity provider login page. To view a diagram that describes the 302 authentication sequence, see Tableau Mobile Authentication Sequence in the Tableau Community.

Reverse proxy and user authentication

Tableau Server will always authenticate users. This means that even if you are authenticating inbound connections at the gateway for your organization, Tableau Server will still authenticate the user.

However, not all clients will support user authentication with a reverse proxy:

- For supported web browsers, you can use SAML, OpenID Connect, Kerberos, Trusted Tickets or manual authentication with a reverse proxy. However, we recommend a transparent scenario where user requests are not prompted for authentication at
the gateway. This recommendation doesn't prohibit using SSL for client/server system-level authentication at the gateway proxy, in fact, we strongly recommend SSL system-level authentication.

- Tableau Mobile supports SAML or manual authentication with a reverse proxy. The iOS version of Tableau Mobile additionally supports Kerberos with a reverse proxy. The same recommendation above applies.

- Tableau Desktop does not support authentication with a reverse proxy. To support remote access with Tableau Desktop, use a VPN solution or configure your reverse proxy to route traffic from Tableau Desktop directly to Tableau Server for authentication.

If your organization is authenticating with Active Directory:

- Active Directory with Enable automatic logon (SSPI) is not supported with a reverse proxy.
- Tableau Server must be configured for reverse proxy before configuring Tableau Server for Kerberos. For more information, see Configure Kerberos.

### Configure Tableau Server to work with a reverse proxy server

Before you configure Tableau Server, you'll need to collect the following information about the proxy server configuration. To configure Tableau Server, you use the `tsm configuration set` command. The information you need to collect corresponds to options you'll need when you run `tsm`.

Most of the following `tsm` options are also used to configure Tableau Server deployments that operate behind a load balancer. For more information, see Add a Load Balancer.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Corresponding <code>tsm configuration set</code> option</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address or CNAME</td>
<td>You can either enter an IP address or a CNAME for this option.</td>
<td><code>gateway.trusted</code></td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
<td>Corresponding tsm configuration set option</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
<td>Corresponding tsm configuration set option</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
<td>Corresponding tsm configuration set option</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
<td>Corresponding tsm configuration set option</td>
</tr>
</tbody>
</table>
Tableau Server on Linux Administrator Guide

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Corresponding tsm configuration set option</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>An example would be a proxy server bigbox.example.com and CNAME entries of ftp.example.com and <a href="http://www.example.com">www.example.com</a>.</td>
<td></td>
</tr>
<tr>
<td>Ports</td>
<td>Port numbers for traffic from the client to the reverse proxy server.</td>
<td>gateway.public.port</td>
</tr>
</tbody>
</table>

If you are using a distributed installation of Tableau Server, then run the following tsm commands on the initial node in your cluster.

1. Enter the following command to set the FQDN that clients will use to reach Tableau Server through the proxy server, where name is the FQDN:

   tsm configuration set -k gateway.public.host -v 'name'

   For example, if Tableau Server is reached by entering https://tableau.example.com in the browser, enter this command:

   tsm configuration set -k gateway.public.host -v 'tableau.example.com'

2. Enter the following command to set the address or the CNAME of the proxy server, where server_address is the IPv4 address or CNAME value:

   tsm configuration set -k gateway.trusted -v 'server_ip_address'

   If your organization uses multiple proxy servers, enter multiple IPv4 addresses, separating them with commas. IP ranges are not supported. To improve start up and initialization of Tableau Server, minimize the number of entries for gateway.trusted.

3. Enter the following command to specify alternate names for the proxy server, such as
its fully qualified domain name, any not fully qualified domain names, and any aliases. If there's more than one name, separate the names with a comma.

```
tsm configuration set -k gateway.trusted_hosts -v 'name1, name2, name3'
```

For example:

```
tsm configuration set -k gateway.trusted_hosts -v 'proxy1.example.com, proxy1, ftp.example.com, www.example.com'
```

4. If the proxy server is using SSL to communicate with the internet, run the following command, which tells Tableau that the reverse proxy server is using port 443 instead of port 80:

```
tsm configuration set -k gateway.public.port -v 443
```

**Note:** If the proxy server is using SSL to communicate with Tableau Server, SSL must be configured and enabled on Tableau Server.

5. Enter the following command to commit the configuration change:

```
tsm pending-changes apply
```

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

**Configure the reverse proxy server to work with Tableau Server**

When a client accesses Tableau Server through a reverse proxy, specific message headers have to be preserved (or added). Specifically, all proxy servers in the message chain must
be represented in the `gateway.trusted` and `gateway.trusted_hosts` settings.

The following graphic shows example headers for a single-hop message chain, where the proxy server is communicating directly with Tableau Server:

The following graphic shows example headers for a multiple-hop message chain, where the message traverses two proxy servers before connecting to Tableau Server:

The following table describes what these headers are and how they relate to the configuration settings on Tableau Server:

<table>
<thead>
<tr>
<th>Headers</th>
<th>Description</th>
<th>Related Tableau Server settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>REMOTE_ADDR</code> and <code>X-FORWARDED-FOR</code> (XFF)</td>
<td>Tableau Server needs these headers to determine the IP address of origin for requests. <code>X-FORWARDED-FOR</code> header must present IP address chain to Tableau Server in the order the connections have occurred.</td>
<td>The IP address that you set in <code>gateway.trusted</code> must match the IP presented in <code>REMOTE_ADDR</code>. If you sent multiple addresses in <code>gateway.trusted</code>, one of...</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td><strong>HOST and X-FORWARDED HOST (XFH)</strong></td>
<td>These headers are used to generate absolute links to Tableau Server when it replies to the client. <strong>X-FORWARDED-HOST</strong> header must present host names to Tableau Server in the order the connections have occurred. The host names that are presented in <strong>X-FORWARDED-HOST</strong> header must be included in the host names that you specify in <code>gateway.trusted_hosts</code>.</td>
<td></td>
</tr>
<tr>
<td><strong>X-FORWARDED-PROTO (XFP)</strong></td>
<td>This header is required if SSL is enabled for traffic from the client to the proxy, but not for traffic from the proxy to Tableau Server. The <strong>X-FORWARDED-PROTO</strong> headers are important for scenarios where HTTP or HTTPS is not maintained along each hop of the message route. For example, if the reverse proxy requires SSL for outside requests, but traffic between the reverse proxy and Tableau Server is not configured to use SSL, <strong>X-FORWARDED-PROTO</strong> headers are required. Some proxy solutions add the <strong>X-FORWARDED-PROTO</strong> headers automatically, while others do not. Finally, depending on your proxy solution, you might have to configure port forwarding to trans-Port configuration on reverse proxy (inbound connections from client and outbound connections to Tableau Server) must be specified in the corresponding parameter: <code>gateway.public.port</code>, which is the port clients use to connect to the proxy. If the proxy server is using SSL to communicate with Tableau Server, SSL must be configured and enabled on Tableau Server.</td>
<td></td>
</tr>
</tbody>
</table>
Validate reverse proxy setup

To validate your reverse proxy setup, publish workbooks and datasources using Tableau Server web authoring or Tableau Desktop. If you are connecting with a web browser to Tableau Server from the internet, verify that you are using a recommended browser. Publish and view workbooks that use existing datasources as well as a datasource that you’ve published. Use the links below to familiarize yourself with connecting with Tableau Server as an end-user.

<table>
<thead>
<tr>
<th>Task</th>
<th>Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of web authoring.</td>
<td>Use Tableau on the Web</td>
</tr>
<tr>
<td>Log in to Tableau Server from Tableau Desktop or a web browser.</td>
<td>Sign in to Tableau Server or Online</td>
</tr>
<tr>
<td>Publish a workbook to Tableau Server.</td>
<td>Publish a Workbook</td>
</tr>
<tr>
<td>Publish a data source.</td>
<td>Publish a Data Source</td>
</tr>
<tr>
<td>Open workbook from Tableau Server.</td>
<td>Opening Workbooks from the Server</td>
</tr>
<tr>
<td>Log out Server (with Desktop).</td>
<td>Sign in to Tableau Server or Online</td>
</tr>
<tr>
<td>Download workbook from a web browser.</td>
<td>Download Workbooks</td>
</tr>
<tr>
<td>Check to make sure tabcmd (from a non-server client)</td>
<td>tabcmd</td>
</tr>
</tbody>
</table>
works.

Related topics

- Tableau Desktop Internet Access Requirements
- Tableau Community: Cannot Create Firewall Rules to Access Mapping Servers
- Add a Load Balancer
Deploy

The topics in this section provide information on installing, configuring, and upgrading Tableau Server on Linux.

Looking for Tableau Server on Windows? See Install and Configure Tableau Server

Install and Configure Tableau Server .............................................. 71
Automated Installation of Tableau Server ........................................ 130
Install Tableau Server in a Disconnected (Air-Gapped) Environment ........ 137
Install Tableau Server in the Cloud .................................................. 145
Post Installation Tasks .................................................................. 146
Enable and Configure Tableau Prep Conductor on Tableau Server ........ 179
Distributed and High Availability Tableau Server Installations .............. 212
Migrate Tableau Server from Windows to Linux ................................ 314
Uninstall Tableau Server ............................................................... 333
Upgrade Tableau Server Overview ................................................. 340

Install and Configure Tableau Server

The topics referenced at the bottom of this page describe the steps to install and configure Tableau Server. If you are installing a distributed deployment (cluster), use the steps in this topic to install the initial node, then, to install additional nodes, see Distributed and High Availability Tableau Server Installations.
After you run the installation, you must then continue setup by activating a license, registering Tableau Server, and configuring various settings including authentication.

Other installation methods

There are a few alternative methods that you can use to install Tableau Server.

- If you want a quick start procedure to install Tableau Server in a non-production environment, see Jump-start Installation.
- Automated Installation of Tableau Server.
- If you are installing Tableau Server in an environment without a connection to the internet, see Install Tableau Server in a Disconnected (Air-Gapped) Environment.
- You can also install Tableau Server onto various cloud platforms. See Install Tableau Server in the Cloud.
- For single-server installations in departments or small businesses, see Everybody’s Install Guide.

Before you begin

To install Tableau Server you must have a computer that satisfies the hardware requirements. You will get an informational message if your computer meets the minimum requirements but does not satisfy the recommended minimum requirements. In this case, your computer hardware can handle a trial installation of Tableau but is not adequate for a production environment. For more information, see Before you install....

Installation steps

The following steps describe how to install Tableau Server on a single computer. Use the steps to install Tableau Server in a single server deployment. Use the steps to install the initial node in a multi-node Tableau Server deployment. Run the steps sequentially.
1. Install and Initialize TSM

2. Activate and Register Tableau Server

3. Configure Initial Node Settings

4. Add an Administrator Account

5. Validate Installation

**Before you install...**

*Note:* You can find additional information about technical specifications for Tableau Server on the Tableau web site, [here](#).

This topic includes requirements and recommendations that you must consider before you install Tableau Server into a production environment.

If you want to install a single server, or if you want to do a minimal installation for test purposes, refer to our single-server installation guide, *Everybody's Install Guide.*

If you are deploying Tableau Server in a distributed cluster, review Distributed Requirements in addition to the requirements and recommendations described in this topic.

**Hardware recommendations**

The following list describes the minimum hardware recommendations for a single-node installation of Tableau Server:

- 8 core, 2.0 GHz or higher processor
- 64-bit processor architecture
- 32 GB memory
- 50 GB disk space available, with a minimum of 15 GB allocated to the /opt directory, and the remainder allocated to the /var directory for data storage. See the section, Data directory, below.

**Important:** The disk space requirement cannot be checked until you initialize TSM. If you don’t have enough space, you won’t be told this until after you install the Tableau Server package.

To see the full list of recommendations and to see the minimum requirements, see Minimum Hardware Requirements and Recommendations for Tableau Server.

For public cloud deployments on Amazon Web Services and Google Cloud Platform, their “vCPU” is actually a CPU hyper-thread, and not a full CPU core. When sizing cloud instances, you will need twice as many vCPU as the Tableau Server CPU core requirements given (4 vCPU for a minimum trial installation, 16 vCPU for a recommended installation).

**Operating system requirements**

The following distributions of Linux are supported:

- Red Hat Enterprise Linux (RHEL) 7.3 and higher, CentOS 7.3 and higher, Oracle Linux 7.3 and higher, and Amazon Linux 2.

  These distributions are collectively referred to in this documentation as RHEL-like.

  RHEL 8 is not supported.

- The latest versions of Ubuntu 16.04 and 18.04 LTS only.

  Non-LTS releases are not supported

Previous versions of CentOS and Ubuntu are not supported because Tableau Server requires systemd for process management.

Custom kernels are not supported.
In a multi-node installation of Tableau Server, all of the computer nodes where you are installing Tableau must run Linux and the same distribution of Linux.

Note: All nodes in a multi-node cluster must have the same type of operating system. You cannot install a multi-node instance of Tableau Server on a combination of Linux and Windows nodes.

Installation directory

The core Tableau Server bits are installed in the `/opt` directory by default.

- The directory where you install Tableau Server must have at least 15 GB of free disk space allocated to it. If you attempt to install Tableau Server on a computer that does not have enough space, the Tableau Server package will install, but you will be unable to continue with setup.
- You can specify a non-default install location on RHEL-like systems, but cannot change the location on Ubuntu.
- Do not specify a symbolic link or a directory location on a Network File System (NFS) volume when specifying a non-default install location on RHEL-like systems.

Data directory

By default, Tableau Server will create a data directory for all content and extracts that are managed by Tableau. The directory is created at `/var/opt/tableau/tableau_server`.

You can specify a different directory for data (extract) storage during installation. If you plan to use a different directory, do not create the directory. Instead, let Tableau Server setup create the directory. The data directory requires specific permissions that are set during the installation process.

To change the data directory, you must pass a flag along with the data directory path when you run the `initialize-tsm` script. See Help Output for initialize-tsm Script.

If you are changing the default data directory:
- Do not specify a symbolic link or a data directory location on a Network File System (NFS) volume.
- Do not specify a data directory location with a path that includes a period or space. If there is a period or space in the path, initialization will fail.

**Important:** You cannot change the data directory location after you’ve run `initialize-tds`. The data directory location will persist for the life of the deployment, including subsequent upgrades.

**Tableau Prep Conductor**

Tableau Prep Conductor is one of the processes on Tableau Server. It runs a flow, checks connection credentials, and sends alerts if a flow fails. Tableau Prep Conductor leverages the scheduling and tracking functionality of Tableau Server so you can automate running flows to update the flow output instead of logging into Tableau Prep Builder to manually run individual flows as your data changes.

Tableau Prep Conductor is licensed separately and is available through the Data Management Add-on license. For more information on Tableau Prep Conductor licensing, see Licensing Tableau Prep Conductor.

It is recommended that you enable Tableau Prep Conductor on a dedicated node. It is recommended that you enable Tableau Prep Conductor on a dedicated node to run flows. For more information:

- If you are installing a new Tableau Server, see Installing Tableau Server with Prep Conductor.
- If you are adding Tableau Prep Conductor to an existing installation of Tableau Server, see Add Tableau Prep Conductor to your Tableau Server Installation.

**Additional requirements**

Make sure that your environment also meets the following additional requirements:
Hostname

- Tableau Server must be able to resolve the hostname to an IP address either using the domain name server (DNS) or with a local host file on the computer running Tableau Server. By default, host files are stored at /etc/hosts.
- The hostname of the server must not change after you start Tableau Services Manager during the setup process. For example, this might happen if you use the cloud-init package to initialize a virtual machine, and you install Tableau Server on that virtual machine.
- Hostnames that include underscores (_) are not supported by Tableau Server on Linux.

Static IP address

The computer where you install Tableau Server must have a static IPv4 or IPv6 address.

Database drivers

To connect to specific data sources, the computer where you install Tableau Server must have the correct database drivers installed. For more information, see Database Drivers.

Available ports

TSM and Tableau Server each require an available TCP port in order for you to access them. TSM defaults to port 8850, and the Tableau Server Gateway service defaults to port 80. We strongly recommend that you ensure that both port 8850 and 80 are not in use on your system before installing Tableau Server. If those ports are not available, the TSM and gateway ports may be dynamically remapped to different port numbers, and there is currently no interface for displaying which port they have been remapped to.

See Tableau Services Manager Ports.

Local firewall configuration

If you are running a firewall on the computer where you will be installing Tableau Server, then you will need to open the following default ports for Tableau Server traffic. All port numbers, except 443 can be changed.
### Tableau Server on Linux Administrator Guide

<table>
<thead>
<tr>
<th>Port</th>
<th>TCP/UDP</th>
<th>Used by ...</th>
<th>TYPE OF INSTALLATION</th>
<th>Distributed / High Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP</td>
<td>Gateway</td>
<td>All</td>
<td>X</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>SSL. When Tableau Server is configured for SSL, the application server redirects requests to this port. Do not change this port.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>8850</td>
<td>TCP</td>
<td>Tableau Services Manager.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>8060</td>
<td>TCP</td>
<td>PostgreSQL database.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>8061</td>
<td>TCP</td>
<td>PostgreSQL backup verification port</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>8000-9000</td>
<td>TCP</td>
<td>Range of ports reserved by default for dynamic mapping of Tableau processes</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>27000-27009</td>
<td>TCP</td>
<td>Range of ports used by Tableau Server for License service. This range must be open on the node running the License service and accessible from other nodes. By default, the initial node runs the License service.</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

See Tableau Services Manager Ports and Configure Local Firewall.

### System user and groups

Tableau Server on Linux uses one unprivileged user, and two groups for proper operation. Tableau will create the default account and groups during setup. Alternatively, you can specify existing accounts. See System user and groups.

### Sudo and root access
All installation tasks and administrative tasks for Tableau Server must be run as root. Often this is accomplished using the sudo command, but running the commands directly as the root user is also possible.

To install Tableau Server with the root account, you must specify a user account during installation. The account will be used for managing TSM. Specify the account by running the initialize-tsm script with the \texttt{--a} option. See Help Output for initialize-tsm Script.

**Account password**

The user account that you use to install and administer Tableau Server must be able to authenticate with a password. That is, the user must not use another means of authenticating (for example public key authentication).

If the account you are using to install and initialize Tableau Server does not have a password, you can set one using the \texttt{passwd} command:

\begin{verbatim}
  sudo passwd $USER
\end{verbatim}

**Port access requirements**

If you want to install Tableau Server remotely, for example by means of SSH, ensure that the following ports are open:

- \texttt{8850}. The port used for the Tableau Services Manager (TSM) web interface. You can use this interface to configure Tableau Server.
- \texttt{80}. The port used for the main Tableau Server web interface.

The Tableau Server installer attempts to open these ports during the installation process, but it can only open these ports for the firewalld firewall. If your computer runs another firewall, you must open the ports before you install.

**Virtual Container environments**
Installation of Tableau Server in virtual container environments such as Docker have not been tested and are not supported. Tableau Server on Linux will not function as expected if installed in these environments.

Package requirements

**Systemd**

Tableau Server requires systemd to manage services. This package is installed by default on CentOS 7 and Ubuntu 16. If you decide to test Tableau Server on a modified version of these distributions, you can run the following command to confirm that systemd is installed:

```
whereis systemd
```

If systemd is installed, the installation location is displayed. For example, you might see the following output:

```
systemd: /usr/lib/systemd /etc/systemd /usr/share/systemd /usr/share/man/man1/systemd.1.gz
```

If you have systemd installed but the Tableau installer is failing requirements checks for systemd, it's likely that systemd is not running. To verify that systemd is running, run the following command:

```
ls /run/systemd
```

The output will be a list of files and directories. If systemd is running, the output will include `system`. If `system` is not in the output, then systemd is not running.

*Continue to the next step: Install and Configure Tableau Server.*
Minimum Hardware Requirements and Recommendations for Tableau Server

The following minimum hardware requirements and recommendations apply to all computers running Tableau Server, including physical hardware and virtual machines (VMs):

- **Minimum requirements for testing and prototyping** are the minimum hardware your computer must have in order to install Tableau Server. If your computer does not meet these requirements, the Setup program will not install Tableau Server. These requirements are appropriate for testing and prototyping, but are not appropriate for most production environments.

- **Minimum recommendations for production** go beyond minimum requirements, and represent the minimum hardware configuration you should use for a production installation of Tableau Server. If your computer meets the minimum requirements but does not meet these recommendations, the Setup program will warn you, but you can continue the installation.

In addition, Tableau Server should not be installed on a physical computer or on a VM instance that is also running resource-intensive applications such as databases or application servers.

**Note:** If you install Tableau Server on a computer that meets the minimum requirements but does not have at least 8 cores and 16 GB of system memory, the default number of all processes installed is reduced to one of each process by design. For more information about processes, see Server Process Limits.

Minimum Hardware Requirements for Testing and Prototyping

The computer on which you are installing or upgrading Tableau Server must meet the minimum hardware requirements. If the Setup program determines that your computer does not meet the following requirements, you will not be able to install Tableau Server.

These minimum requirements are appropriate for a computer that you use for prototyping and testing of Tableau Server. They apply to single-node installations and to each computer in a distributed installation.

<table>
<thead>
<tr>
<th>Processor CPU</th>
<th>RAM Free</th>
<th>Disk Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>64-bit 2-core</td>
<td>8 GB</td>
<td>15 GB</td>
</tr>
</tbody>
</table>

**Minimum Hardware Requirements**

**Note:** These minimum requirements are not recommended for use in production environments. For production minimum recommendations, see Minimum Hardware Recommendations for Production.

For the requirements:

- Free disk space is calculated after the Tableau Server Setup program is unzipped. The Setup program uses about 1 GB of space. You may need to allocate additional disk space depending on various factors like whether you will be using extracts. For more information, see Disk Space Requirements.

The core Tableau Server bits must be installed in a directory with at least 15 GB of free disk space. If you attempt to install Tableau Server on a computer that does not have enough space, the Tableau Server package will install, but you will be unable to continue with setup. By default the install location is the `/opt` directory. You can change the installation path for Tableau Server on RHEL distros. For more information, see Option to install to non-default location on RHEL-distros.
If you plan to make heavy use of extracts then you may need to allocate additional disk space. You can specify a different directory for data (extract) storage during installation. See Install and Initialize TSM.

- Core count is based on "physical" cores. Physical cores can represent actual server hardware or cores on a virtual machine (VM). Hyper-threading is ignored for the purposes of counting cores.

### Minimum Hardware Recommendations for Production

For production use, the computer on which you install or upgrade Tableau Server should meet or exceed the minimum hardware recommendations. These recommendations are general. Actual system needs for Tableau Server installations can vary based on many factors, including number of users and the number and size of extracts. If the Setup program determines that your computer does not meet the following recommendations, you will get a warning, but you can continue with the setup process. The minimum recommendations listed here are intended as general guidance. However the recommendations for your environment may vary. For more information, see the Hardware recommendations section of the Recommended Baseline Configurations topic.

<table>
<thead>
<tr>
<th>Install Type</th>
<th>Processor</th>
<th>CPU</th>
<th>RAM</th>
<th>Free Disk Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single node</td>
<td>64-bit</td>
<td>8-core, 2.0 GHz or higher</td>
<td>32 GB</td>
<td>50 GB</td>
</tr>
</tbody>
</table>

If you are adding Tableau Prep Conductor to your Tableau Server installation, it is recommended to add a second node and dedicate this to running Tableau Server Prep Conductor. This node should have a minimum of 4 cores (8 vCPUs), and 16 GB of RAM.

**Multi-node and enterprise deployments**

Contact Tableau for technical guidance.

Nodes must meet or exceed the minimum hardware recommendations, except:

- Nodes running backgrounder, where 4 cores may be acceptable.
Install Type | Processor | CPU | RAM | Free Disk Space
--- | --- | --- | --- | ---
- | | | | Dedicated node for Tableau Prep Conductor: Minimum of 4 cores (8 vCPUs), and 16 GB of RAM.

For the recommendations:

- Free disk space is calculated after the Tableau Server Setup program is unzipped. The Setup program uses about 1 GB of space. You may need to allocate additional disk space depending on various factors like whether you will be using extracts. For more information, see Disk Space Requirements.

The core Tableau Server bits must be installed in a directory with at least 15 GB of free disk space. If you attempt to install Tableau Server on a computer that does not have enough space, the Tableau Server package will install, but you will be unable to continue with setup. By default the install location is the `/opt` directory. You can change the installation path for Tableau Server on RHEL distros. For more information, see Option to install to non-default location on RHEL-distros.

If you plan to make heavy use of extracts then you may need to allocate additional disk space. You can specify a different directory for data (extract) storage during installation. See Install and Initialize TSM.

- Core count is based on "physical" cores. Physical cores can represent actual server hardware or cores on a virtual machine (VM). Hyper-threading is ignored for the purposes of counting cores.

- RAM shown is the minimum recommended for a single-node installation. Your installation may function better with more RAM, depending on activity, number of users, and background jobs, for example. For hardware specifications Tableau uses internally for testing scalability, see Hardware Recommendations.

For hardware recommendations for Tableau Server in the cloud, see the following:
Install and Initialize TSM

This topic guides you through the process of installing Tableau Server and initializing Tableau Services Manager (TSM).

**Important:** Do not install a beta version of Tableau Server in your production environment. You should also never restore a production Tableau Server installation using a backup of a beta version.

Prerequisites

Before proceeding, review the topic, Before you install....

Review optional initialization parameters

Before you install and initialize TSM, it is critical that you review the parameters that you may optionally set as part of the initialization operation. You can only run `initialize-tsm` once, so be sure to run it with all of the options that your organization needs. Some options, such as non-default system user and group can only be configured as part of the initialization operation. Other configurations, such as forward proxy and dynamic port settings can be manually set after you run initialization, but doing so is a much more labor-intensive process.

For a complete list of optional parameters, see Help Output for initialize-tsm Script.

Some common scenarios where optional initialization parameters are used:
• Configuring Tableau Server to work with a forward proxy server. See Optional: common initialize-tsm parameters, later in this topic, to configure Tableau Server during installation. You can also configure Tableau Server after you install, see Configuring Tableau Server on Linux to work with a forward proxy.
• Specifying dynamic port mapping. By default, most ports needed by Tableau Server are assigned (mapped) dynamically from a predefined range of ports. The port assignments are made for each service or process during installation. If you want to modify port mapping, we recommend configuring this during installation, see Controlling port remapping with initialize-tsm.
• Specifying non-default system user or group This configuration change can only be performed during initialization. See System user and groups.
• Specifying a non-default data directory. This configuration change can only be performed during initialization. See Data directory.

Install Tableau Server

Install Tableau Server with your distribution’s package manager, then run a script to initialize TSM. The script is included with the installed package.

**Important:** The hostname of the server must not change after you start TSM. For example, this might happen if you use the cloud-init package to initialize a virtual machine, and you install Tableau Server on that virtual machine.

Install the Tableau Server package

By default, Tableau Server is installed in the `/opt` directory. On RHEL-like distributions you can specify a different install location.

1. Log on as a user with `sudo` access to the computer where you want to install Tableau Server.
2. Download the `.rpm` or `.deb` installer package from the Tableau Server Downloads and Release Notes page.
3. Navigate to the directory where you copied the `.rpm` or `.deb` package.
4. Use the package manager to install the Tableau Server package.

Do not install to a location using a symbolic link or to a directory on a Network File System (NFS) volume.

- On RHEL-like distributions, including CentOS, you have the option to install Tableau to a non-default location. If you choose to do so, you need to take extra steps.

  - **Default location**—To install to the default location (/opt/tableau/tableau_server), run the following commands:
    
    ```
    sudo yum update
    sudo yum install tableau-server-<version>.x86_64.rpm
    ```

  - **Non-default location**—To install to a non-default location, you must use `rpm -i`. You will also need to install all dependent packages. See the note below.

    Run the following command:

    ```
    sudo rpm -i --prefix /preferred/install/path tableau-server.rpm
    ```

**Note:** When you use `yum` to install Tableau Server, all dependent packages are automatically downloaded and installed. This is the preferred method for installing Tableau. If you want to install to a non-default location, or your organization does not allow you to use `yum` and you must install using `rpm -i`, you must also install all dependent packages separately. For information about installing dependent packages, see Installing Tableau Server on an Air-Gapped Computer Running Linux.
On Ubuntu, run the following commands:

```bash
sudo apt-get update
sudo apt-get upgrade
sudo apt-get -y install gdebi-core
sudo gdebi -n tableau-server-<version>_amd64.deb
```

Initialize TSM

You can specify a separate location for data (extracts and extract metadata) storage, whether or not you install Tableau to the default location.

Do not specify a symbolic link or a directory location on a Network File System (NFS) volume.

1. **Navigate to the scripts directory:**
   
   ```bash
   cd /opt/tableau/tableau_server/packages/scripts.<version_code>/
   ```

2. **Run the following script to start TSM:**
   
   ```bash
   sudo ./initialize-tsm --accepteula --<optional_parameters>
   ```

   The only required parameter for the `initialize-tsm` script is `--accepteula`. You must include this parameter to accept the Tableau Server End User License Agreement (EULA). The EULA is available in the following location:

   ```bash
   /opt/tableau/tableau_server/packages/docs.<version_code>/Commercial_EULA.txt
   ```

   However, review the following common parameters before running the script.

**Optional: common initialize-tsm parameters**

There are a number of parameters (also referred to as, *flags*) that you can set when
you run initialize-tsm. Common flags are listed below. For a complete list, run the command, `sudo ./initialize-tsm -h`, or see Help Output for initialize-tsm Script.

- The `-a` flag to specify a user to be added to the tsmadmin and tableau groups instead of the user running this script. If you are installing with the root account, you must specify the `-a` flag.

- The `--unprivileged-user` flag to set a different service account. By default a new user called `tableau` will be created. This account is an unprivileged service account under which most Tableau process run. We recommend creating a different user only in the case where a `tableau` user account already exists on the computer.

- The `-d` flag to specify a non-default location of the "data directory" where Tableau Server stores extracts, information about extracts, and more.

By default, Tableau Server uses the following location for the directory:

```
/var/opt/tableau/tableau_server
```

When you set this flag, the `initialize-tsm` script will create and apply permissions to the directory that you specify. There are important restrictions that apply to changing the default directory path. See Data directory.

- The `--debug` flag for troubleshooting. This option displays each command in the script as it is run and can make it easier to troubleshoot issues. Use of this option results in extensive output to the screen.

- We recommend configuring Tableau Server for a forward proxy solution during installation.

To do so, include the `--http_proxy` and/or `--https_proxy` flags to specify the forward proxy server. Specify the URL with the port, for example:
--http_proxy=http://proxy.example.lan:80/

--https_proxy=http://1.2.3.4:443/

Take care to use http when you specify the URL for the https_proxy environmental variable. Do not specify the https protocol for the value of the https_proxy environmental variable.

To configure Tableau Server to bypass the forward proxy, include the --no_proxy flag. You should also add exceptions to this proxy configuration to guarantee that all communications within a local Tableau Server cluster (if you have one now or will have one later) do not route to the proxy server. For example:

--no_proxy=
y=localhost,127.0.0.1,localaddress,.localdomain.com.

- If you want to manually manage port assignment for TSM and Tableau Server processes, you may need to use one or more port-related switches with initialize-tsm. For more information, see Controlling port remapping with initialize-tsm.

3. Log off and log on again to the terminal before you configure Tableau Server.

When you log on again, you create a new session in which group membership changes have taken effect. The new session also has access to the environment variables added by the initialize-tsm script.

Alternatively, you can run the following command to update your path for the current session (but not to update your group membership):

source /etc/profile.d/tableau_server.sh

Next step

- Activate and Register Tableau Server
Activate and Register Tableau Server

This topic describes how to activate and register Tableau Server.

Tableau Server requires at least one product key that both activates the server and specifies the number of license levels you can assign to users. You can access your product keys from the Customer Portal.

If you need to activate Tableau Server on a computer that is offline, see Activate Tableau Server Offline - Adding a License. If you need to activate additional product keys to add capacity to an existing Tableau Server installation, see Add Capacity to Tableau Server.

Prerequisite

Before proceeding with the procedures in this topic, complete the following prerequisites as outlined in Install and Configure Tableau Server:

- Install and Initialize TSM
- TSM uses port 8850. If you are running a local firewall, open port 8850. See Configure Local Firewall.

Use the TSM web interface

1. Sign in to Tableau Services Manager Web UI.

2. On the **Activate** page, Enter or paste your product key and click **Activate License**.
3. On the Register page, enter your information into the fields and click **Register**.
Register with Tableau. All fields are required.

Contact Information
- First Name
- Last Name
- Phone Number
- Email

Company Information
- Organization
- Industry
- Department
- Job Role

Region Information
- City
- Postal Code
- Country/Region
- State/Province

Register
Use the TSM CLI

Log in to Tableau Services Manager

Before you can proceed you must log in to Tableau Services Manager (TSM).

To log in to TSM, run the following command:

`tshm login -u <username>

What if I can't log in?

The account that you use to configure the rest of the installation must be a member of the tsmadmin group that was created during initialization. To view the user accounts in the tsmadmin group, run the following command:

`grep tsmadmin /etc/group

If the user account is not in the group, run the following command to add the user to the tsmadmin group:

`sud0 usermod -G tsmadmin -a <username>

After you have added the user to the tsmadmin group, run the tsm login command.

Activate Tableau Server

To activate Tableau Server for production use, you must have a product key.

To activate a product key, run the following command:

`tsm licenses activate -k <product key>

To activate a two-week trial, run the following command:

`tsm licenses activate -t

If you are unable to activate Tableau, for example, if you get an error like this:

License Server not available
Register Tableau Server

After activation, you need to register Tableau Server. To do this, create a registration file and then pass it as an option with the `tsm register` command.

1. Generate a template that you can edit by running the following command:

   ```bash
   tsm register --template > /path/to/<registration_file>.json
   ```

2. Edit the template file to create your completed registration file.

   Here is an example of a registration file in the required format:

   ```json
   {
     "zip" : "97403",
     "country" : "USA",
     "city" : "Springfield",
     "last_name" : "Simpson",
     "industry" : "Energy",
     "eula" : "yes",
     "title" : "Safety Inspection Engineer",
     "phone" : "5558675309",
     "company" : "Example",
     "state" : "OR",
     "department" : "Engineering",
     "first_name" : "Homer",
     "email" : "homer@example.com"
   }
   ```

3. After saving changes to the file, pass it with the `--file` option to register Tableau Server:

   ```bash
   tsm register --file /path/to/<registration_file>.json
   ```
For example:

tsm register --file /usr/share/tableau-reg-file.json

If you have a product key for Data Management Add-on license, and plan to enable Tableau Prep Conductor, see Install Tableau Server with Prep Conductor.

Next step

- Configure Initial Node Settings

Offline Activation When Installing Tableau Server

When you install Tableau Server, you have to activate at least one product key. Doing this activates the server, and specifies the number of license levels you can assign to users. There are also times you may need to activate licenses after Tableau Server is installed, for example, if you add capacity to your server, or get a new product key. If you don't have your product key, you can get it from the Tableau Customer Account Center.

In most cases, you can activate your key directly from Tableau, either during installation, or later, using the Tableau Services Manager (TSM) Licenses page, but there are some circumstances that don't allow you to do this. If your computer is not connected to the internet for example, or has a firewall that restricts access outside your intranet. In these cases you need to do an offline activation.

- Offline activation when adding a license—To complete an offline activation when you are adding a license to Tableau Server, see Activate Tableau Server Offline - Adding a License.
- Offline activation of licenses during install—To complete an offline activation when you are installing Tableau Server, follow the steps below.

Offline activation overview and prerequisites

Offline activation of Tableau Server involves several steps. If you have never activated a product key before on your computer, you need to run through the steps twice, once to initialize licensing on the computer, and a second time to activate the key. If you have had a license on the computer in the past, you run through the steps only once.
Offline activation steps:

1. Generate an offline activation request file (offline.tlg).
2. Upload the offline activation request to Tableau and download the resulting activation file (activation.tlf).
3. Upload the activation file to Tableau Server.

If this is the first time a Tableau product key has been activated on the computer, you repeat these three steps a second time.

Use the TSM web interface

If you are unable to do an activation of your product key from within the TSM Setup UI, you can do an offline activation. This might be necessary if you are installing on a machine that is isolated without internet access. If you attempt to activate your product key and see a dialog that says online activation is unavailable, you can activate the key offline. Click Activate License Offline.
Instructions for a five-step process display.


Create an offline file you will upload to Tableau. If your license key is not pre-filled in the form, enter your key and click **Create Offline File** to generate an offline file (*offline.tlq*) on the local computer.
Tableau Server on Linux Administrator Guide

Leave the Tableau Server install program open and copy the offline.tlq file to a computer with internet access. You need to upload this file to Tableau to generate an activation file.

2. Upload and submit the offline file.

On the computer where you copied the offline.tlq file, open a browser and go to http://www.tableau.com/support/activation to open the Tableau Support Activation page. You will upload and submit the offline.tlq file to Tableau. This automatically generates an activation file (activation.tlf) that you can download and copy back to the Tableau Server computer.

   a. On the Offline Activation page, click Choose File to select the offline.tlq file.
   b. Click Upload Activation File to submit the file to Tableau.
   c. Click the here link to download the activation.tlf file to your computer.

   **Offline Activation**

   The activation was successful. Please click here to download your activation file.

   For help creating the offline activation file, see Activate Tableau Desktop Offline or Activate Tableau Server Offline. (Linux)

   d. Copy the downloaded activation.tlf file to the computer where Tableau Server is installed.

3. Upload the activation file.

   On the Tableau Server computer, click Upload Activation File to upload the file to Tableau Server.
4. Create, upload, and submit a second offline file.

If this is the first Tableau license activated on the computer, then you will need to activate again.

Perform Steps 1 and 2 again: create a new `offline.tlq` file, submit it to Tableau, and download another `activation.tlf` file.

5. Upload the second activation file.

On the Tableau Server computer, upload the second `activation.tlf` file. When you do this successfully, the **Activate License** option is enabled.

6. Click **Activate License** to complete the offline activation and continue with the installation process.

**Use the TSM CLI**

Log in to Tableau Services Manager
Before you can proceed you must log in to Tableau Services Manager (TSM).

To log in to TSM, run the following command:

```
tsm login -u <username>
```

**What if I can't log in?**

The account that you use to configure the rest of the installation must be a member of the `tsmadmin` group that was created during initialization. To view the user accounts in the `tsmadmin` group, run the following command:

```
grep tsmadmin /etc/group
```

If the user account is not in the group, run the following command to add the user to the `tsmadmin` group:

```
sudo usermod -G tsmadmin -a <username>
```

After you have added the user to the `tsmadmin` group, run the `tsm login` command.

Step 1 - Generate an offline activation request file

1. On the initial node, open a terminal session.

2. Type this command to get your offline activation file:

   ```
ts freshwater get-offline-activation-file -k <product-key> -o <target-directory>
   ```

   You can get your product key from the Tableau Customer Portal. The target directory must already exist.

3. Copy the offline activation file (`offline.tlq`) from the target directory to a computer that has internet access.
Step 2 - Upload the offline activation request to Tableau

1. On the computer that has internet access, go to the Tableau Product Activations page.

2. Complete the instructions to upload your offline.tlq file.

   This creates an activation file, activation.tlf.

3. Download the resulting activation file from Tableau.

Step 3 - Initialize or activate your license

1. Copy the activation file (activation.tlf) to a location accessible from your Tableau Server computer.

2. Run the following command:

   tsm licenses activate -f <path-and-activation-file>

3. Restart the server for licensing changes to take effect:

   tsm restart

First time license activation

If this is the first Tableau license activated on the computer, you will see this message:

Your license has been initialized. To complete the activation, we need one more exchange. Generate and send to Tableau a second activation request file.

Repeat steps 1 through 3 above to activate your license. You need to generate a second offline.tlq file, upload it to Tableau, and download the resulting activation.tlf file, then use that file to activate your license.

If you are not sure whether you need to repeat the steps, you can run this command:

   tsm licenses list

If you see a message like this one you need to repeat the steps above:
No licenses are currently activated.

Subsequent license activation

If this is not the first Tableau license activated on the computer, or if you have completed the steps above two times, you should see a success message:

Activation successful.

Tableau Server is activated. If you need additional assistance, contact Tableau Technical Support.

Deactivate Tableau Server Offline

If Tableau Server does not have Internet access, you can use the instructions in this topic to deactivate Tableau Server. You will need to use a second computer that is able to access the Internet to complete this activation process.

Note: These instructions require you to save a file that you will use for deactivation. You must complete these steps using a browser other than Microsoft Edge, such as Google Chrome. If you use Edge, the product key return file used for deactivation is not created.

1. On the Tableau Server initial node, create a directory to store the offline deactivation file that is created in the next step.

2. Log in to TSM using a Tableau Administrator account, and then run the following command:

   tsm licenses get-offline-deactivation-file -k <productkey> -o <deactivation-file-directory>

3. Move the deactivate.tlg file from the deactivation file directory that you specified in the previous command to a trusted computer that has Internet access.
4. On the trusted computer that has Internet access, open a web browser and visit the Tableau Product Activations page. Follow the instructions on that page to submit your deactivate.tlg file.

5. When prompted, save the product key return file (return.tlr) from the Product Activations page.

6. Move the product key return file (return.tlr) from the trusted computer that has Internet access to the Tableau Server initial node that runs the Licensing Server service.

7. Log in to TSM using a Tableau Administrator account, and then run the following command:

```
 tsm licenses deactivate -f <path-to-license-key-return-file>
```

Configure Initial Node Settings

This topic describes how to configure essential server settings as part of the initial Tableau Server installation process.

Prerequisite

Before proceeding with the procedures in this topic, complete the following prerequisites as outlined in Install and Configure Tableau Server:

- Install and Initialize TSM
- Activate and Register Tableau Server

You may also need to configure your local firewall for Tableau Server traffic. See Configure Local Firewall.

Use the TSM web interface
Tableau Server on Linux Administrator Guide

After you have activated and registered Tableau Server, the installation program will display the Setup page.

**Note:** If you need to configure Tableau Server to connect to an LDAP directory that is not Active Directory, then you must use the TSM CLI.
Identity store settings

You must configure the identity store settings for the Tableau Server computer. The identity store manages Tableau Server accounts. You can configure the identity store to synchronize with an external directory (for example, OpenLDAP or Active Directory) or you can configure the identity store to manage and store accounts on Tableau Server. If you will be
using a single sign on solution (OpenID, SAML, Kerberos, etc) then review the following topics before configuring the identity store:

- Identity Store
- Authentication

**Important:** After you have configured and applied settings for the identity store, it cannot be changed.

If you select **Active Directory**, Tableau Server will populate the **Domain** and **NetBIOS** fields from the computer on which you are running Setup. In some cases, Setup may not display these attributes. For more information about how Tableau Server connects and communicates with Active Directory, see User Management in Active Directory Deployments.

Tableau Server requires read access to Active Directory. You can use simple bind or GSSAPI bind to authenticate Tableau Server with Active Directory.

**LDAP simple bind**
If you are using simple bind to authenticate with Active Directory, enter a domain account and password. We recommend using LDAPS to connect. See LDAP over SSL.

**LDAP GSSAPI bind**
Identity Store

You cannot change the identity store after initializing.

- Local
- Active Directory

<table>
<thead>
<tr>
<th>Domain</th>
<th>NetBIOS (Nickname)</th>
</tr>
</thead>
<tbody>
<tr>
<td>example.lan</td>
<td>example</td>
</tr>
</tbody>
</table>

Hostname (Optional)  Port (Optional)

Tableau Server requires read access to Active Directory. Specify how Tableau Server will authenticate with Active Directory.

- LDAP simple bind
- LDAP GSSAPI bind

Specify a user principal name (UPN) and upload the Kerberos configuration file Tableau Server will use to authenticate to the Identity Store.

UPN
tabserv@example.lan

Configuration file [Select File]

Specify and configure the method Tableau Server will use to authenticate to Active Directory.

- Keytab file
- Username and password

Keytab file [Select File]

Username            Password
We recommend binding to LDAP directory with GSSAPI. To bind with GSSAPI you will need a keytab file specifically for the Tableau Server service. See Understanding Keytab Requirements.

Gateway port

The default port for web access to Tableau Server (via HTTP) is port 80. If the installation program determines that port 80 is in use when you first install Tableau Server, an alternate port (for example 8000) is used and shown in the Port number box.

You may need to change the port for other networking needs, for example, if you have a hardware firewall or proxy in front of the Tableau Server host, this might make running a back-end system on port 80 undesirable.

Sample workbook installation

By default, Tableau Server will install sample workbooks in the Default site when you initialize the server.

Alternatively, you can publish samples after installation by using the publishsamples tabcmd command.
After you have configured the options on this page, click **Initialize**.

The initialization process can take a while. When initialization is complete the following page is displayed:

![Initialize Progress](image)

**Initialization Complete**

You will need to create a Tableau Server Administrator account.

Continue

---

**Use the TSM CLI**

First, configure identity store, gateway settings, and sample workbook installation. Then apply the changes, optionally verify your LDAP connection, and then initialize Tableau Server.

Configure identity store settings

You must configure the identity store settings for the Tableau Server computer.

**Important:** After you have configured and applied settings for the identity store, it cannot be changed.
Use the json template in the identityStore Entity to create a json file. After you have filled in the options with the appropriate values, you can then pass the json file with this command:

```
tsm settings import -f path-to-file.json.
```

Configure gateway settings (optional)

Depending on your network requirements, you may need to configure the gateway settings for the Tableau Server computer. For example, if you are enabling SSL or configuring access to Tableau Server with a reverse proxy, you may need to configure gateway settings. See gatewaySettings Entity for more information.

Use the json template in the gatewaySettings Entity to create a json file. After you have filled in the options with the appropriate values, you can then pass the json file with this command:

```
tsm settings import -f path-to-json-file.json.
```

Configure sample workbook installation (optional)

By default, Tableau Server will install sample workbooks in the Default site when you initialize the server.

If you do not want to install sample workbooks during installation, run the following command:

```
tsm configuration set -k install.component.samples -v false
```

You can publish samples after installation by using the publishsamples tabcmd command.

Apply pending configuration changes

Now that you’ve created and set initial configuration, you must apply them. When you apply configuration changes, tsm will verify the settings you’ve set before committing them.

To apply configuration changes to Tableau Server, run this command:

```
tsm pending-changes apply
```
The pending-changes apply command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the --ignore-prompt option, but this does not change the restart behavior. For more information, see tsm pending-changes apply.

Once this command has completed, TSM processes are running, and Tableau Server is configured but is not running.

Verify LDAP configuration (Optional)

If your identity store uses Active Directory or OpenLDAP, then we recommend verifying LDAP connectivity before proceeding.

To do so, run the following commands before you initialize the server:

tsm user-identity-store verify-user-mappings -v <user name>

tsm user-identity-store verify-group-mappings -v <group name>

User and group names must be valid names that exist in the LDAP server that you are connecting to. If your LDAP connection is set up correctly, then the user or group attributes will be returned to the shell. If your connection is not set up correctly, then an error will be returned.

Initialize and start Tableau Server

- To initialize and start Tableau Server, use the --start-server option:

  
  tsm initialize --start-server --request-timeout 1800

  This saves time by starting the server running after initialization.

- If you are going to reconfigure Tableau Server after initialization, leave the --start-server option off:
tsm initialize --request-timeout 1800

This stops the server after initialization.

Start Tableau Server. If you did not use the --start-server option during initialization and are finished configuring Tableau Server, use this command to start the server:

tsm start --request-timeout 900

**Note:** If you experience timeouts when installing or configuring Tableau Server, you may need to specify a longer timeout. For more information, see Install fails due to timeouts.

---

Next Step

After initialization is complete, create the Tableau Server administrator user account. See Add an Administrator Account.

Configuration File Example

This article provides an example of a complete JSON configuration file, with gatewaySettings and identityStore entities specified. In addition, a configuration key sets the gateway timeout to 900 seconds.

Your configuration file will look different depending on the options you need to set.

You might set multiple .json configuration files during installation. To set the values for each file in Tableau Server, you run the following command, once for each configuration file:

```
tsm settings import -f path-to-file.json
```

After you set the configuration files, run tsm pending-changes apply to apply the changes from all of the .json files you’ve set.
As shown in the example above, there are two classes of configuration parameters: configEntities and configKeys.

**configEntities**

Certain types of configuration are done through entity sets that map to specific scenarios, such as the identity store and gateway configurations. When you pass a set of configEntities with the `tsm settings import -f path-to-file.json` command, TSM validates the configuration. If values passed are invalid, TSM will provide an error. This enables you to make changes during the configuration process, rather than experience a configuration failure at initialization or run time.
Entities can be set only by including a `configEntities` block in a `.json` file.

**Important:** All files that are referenced in `configEntities` must be located on the local computer. Do not specify UNC paths.

`configKeys`  
Entities cover only a small portion of the configuration values that can be set. Hundreds of keys correspond to parameters stored in `.yml` files. Tableau Server uses these parameters to store all of the configuration information for all services.

You can set individual keys with the `tsm` configuration command. But during deployment, setting them along with other configuration scenarios in JSON files, as shown above, is more convenient.

Unlike `configEntities`, `configKeys` are not validated.

**Note:** We do not recommend setting parameters that are not documented in `tsm` configuration set Options.

**Add an Administrator Account**

The final step in activating Tableau Server is to add the initial administrator account. The administrator will have all access to the server including the ability to manage users, groups, and projects.

The server must be running when you create the initial admin user.

If you have configured the Tableau Server identity store to use LDAP or Active Directory, then the initial administrative user that you specify must be an account in the directory. The initial administrative user is generally distinct from the user account on the Tableau Server computer that you use to run `tsm`.
However, these accounts can be the same if you have configured the Tableau Server identity store to use LDAP or Active Directory and the initial admin user is a member of the tsmadmin group on the Tableau Server computer.

Prerequisites

Before proceeding with the procedures in this topic, complete the following prerequisites as outlined in Install and Configure Tableau Server:

- Install and Initialize TSM
- Activate and Register Tableau Server
- Configure Initial Node Settings

Use web UI

After Tableau Server is finished initializing, the installation program will display a page to create the Tableau Server administrator.

- If you configured a local identity store during setup, then specify a name and password that you want to use.

- If you configured a LDAP or Active Directory identity store during setup, then you must specify a user account that is a member of the directory.

If you are installing remotely, then you must sign in to TSM on the physical computer where Tableau Server is installing, or you can access the computer remotely and run the tabcmd initialuser command from a shell.

Use tabcmd CLI

You must create the initial administrative account for Tableau Server.
If you configured a local identity store during setup, then specify a name and password that you want to use.

If you configured a LDAP or Active Directory identity store during setup, then you must specify a user account that is a member of the directory.

To create the initial user, run the following `tabcmd` command:

```
tabcmd initialuser --server http://localhost --username '"<new-admin-username>"'
```

For example:

```
tabcmd initialuser --server http://localhost --username '"tableau-admin"'
```

If you are running the HTTP protocol on a port other than 80, specify the port after the host name, for example: `--server http://localhost:8080`.

After you run the command, the shell will prompt for an administrative password.

Next steps

After you have created the Tableau Server administrator account, continue your deployment by working through the configuration topics at Post Installation Tasks.

**Important:** You must install the PostgreSQL driver if you want to use the built-in administrative views. You can find driver links and installation instructions for all the supported connectors on the [Driver Download page](#).

Validate Installation

To validate that Tableau Server is installed and running properly and to review the built-in administrative views, you must install the PostgreSQL driver.
Prerequisites

Before proceeding with the procedure in this topic, complete the following prerequisites as outlined in Install and Configure Tableau Server:

- Install and Initialize TSM
- Activate and Register Tableau Server
- Configure Initial Node Settings
- Add an Administrator Account

Install PostgreSQL driver and validate installation

To validate installation:

1. Download PostgreSQL drivers from the Driver Download page.

2. Install the drivers on your Tableau Server computer:
   - On CentOS and RHEL, download the .rpm file and then run the following command:
     
     ```
     sudo yum install tableau-postgresql-odbc-9.5.3-1.x86_64.rpm
     ```
   - On Ubuntu, download the .deb file and then run the following command:
     
     ```
     sudo dpkg -i tableau-postgresql-odbc_9.5.3_amd64.deb
     ```

3. To validate that the drivers installed, navigate to the Administrative Views in Tableau Server.

Initial Node Installation Defaults

By default, the Tableau Server installer configures the number of process instances that Tableau Server runs based on the hardware detected by the installer. The default con-
configuration applies to single-server installations and to the initial server of a multi-node installation.

You can calculate the default configuration based on the following rules for each process, where the number of cores refers to the number of logical CPU cores:

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Number of Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>VizQL Server</td>
<td>Equal to the number of cores divided by four, up to a maximum of four process instances.</td>
</tr>
<tr>
<td>Backgrounder</td>
<td>Set to two unless the number of cores is fewer than eight.</td>
</tr>
<tr>
<td>Cache Server</td>
<td>Set to two unless the number of cores is fewer than eight.</td>
</tr>
<tr>
<td>Data Server</td>
<td>Set to two unless the number of cores is fewer than eight.</td>
</tr>
</tbody>
</table>

For all other process types, the number of process instances is set to one, regardless of the hardware.

Here’s an example default configuration for a computer with 16-cores:

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Number of Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>VizQL Server</td>
<td>4</td>
</tr>
<tr>
<td>Application Server</td>
<td>1</td>
</tr>
<tr>
<td>Backgrounder</td>
<td>2</td>
</tr>
<tr>
<td>Cache Server</td>
<td>2</td>
</tr>
<tr>
<td>Data Server</td>
<td>2</td>
</tr>
<tr>
<td>File Store</td>
<td>1</td>
</tr>
<tr>
<td>Data Engine</td>
<td>1</td>
</tr>
</tbody>
</table>
Jump-start Installation

This topic provides all of the steps required to perform a basic, quick-start installation of Tableau Server using the command line. The purpose of the configuration described here is to provide the quickest, simplest path to a Tableau Server installation on a computer running the CentOS 7.3 (and higher) or Ubuntu distribution of Linux. Use this procedure as practice, to try out the Tableau Server installation, management, and user experience before your actual server deployment.

**Important:** Do not use this procedure as a stand-alone resource for deploying Tableau Server into a production environment. To deploy Tableau Server into a production environment, refer to the content at Install and Configure Tableau Server.

The procedures in this topic will install an instance of Tableau Server for Linux with the following characteristics:

- Operating system: CentOS 7.3 (and higher) or Ubuntu
- Identity store: local authentication
- Gateway port: 80
- Tableau Server administrator account: admin

Before you begin

Review the topic, Before you install.... The procedure below assumes that you have installed Linux on conforming hardware and according to the environmental requirements specified in that topic.

Note that the computer you install on must meet the minimum hardware requirements specified in Minimum Hardware Requirements and Recommendations for Tableau Server. The setup program will not install Tableau Server onto systems that do not meet the minimum hardware requirements.
Step 1: Install Tableau Server package and start Tableau Services Manager

Install Tableau Server with your distribution’s package manager, then run a script to initialize Tableau Services Manager (TSM). Tableau Services Manager is the management toolset used to install, configure, and manage Tableau services.

The initialize script is included with the installed package. For more details, see Install and Initialize TSM.

1. Log on as a user with sudo access to the computer where you want to install Tableau Server.

2. Navigate to the directory where you copied the Tableau Server installation package.

3. Use the package manager to install the Tableau Server package.

Do not install to a location using a symbolic link or to a directory on a Network File System (NFS) volume.

- On RHEL-like distributions, including CentOS, run the following commands:

  
  ```bash
  sudo yum update

  sudo yum install tableau-server-<version>.x86_64.rpm
  ```

  **Note:** When you use `yum` to install Tableau Server, all dependent packages are automatically downloaded and installed. This is the preferred method for installing Tableau. If your organization does not allow you to use `yum` and you must install using `rpm -i`, you must also install all dependent packages separately.

- On Ubuntu, run the following commands:
sudo apt-get update
sudo apt-get upgrade
sudo apt-get -y install gdebi-core
sudo gdebi -n tableau-server-<version>_amd64.deb

4. Navigate to the scripts directory:

    cd /opt/tableau/tableau_server/packages/scripts.<version_code>/

5. Run the following script to start TSM:

    sudo ./initialize-tsm --accepteula

6. After initialization is complete, close the terminal session:

    exit or logout

Step 2: Activate and register Tableau Server

Before you can configure Tableau Server you must activate a license and register. For more details, see Activate and Register Tableau Server.

1. Log on as a user with sudo access and log in to TSM. Run the following command:

    tsm login -u <username>

2. Activate the Tableau Server license. Run the following command:

    tsm licenses activate -k <license_key>

3. Register Tableau Server. Generate a template that you can edit by running the following command:

    tsm register --template > /path/to/registration_file.json

4. Open a text editing program, fill in the registration file, save it, then pass it with the fol-
lowing command:

```
tsm register --file /path/to/registration_file.json
```

### Step 3: Configure local identity store

You must configure the identity store settings. This procedure simplifies installation setting identity store to local authentication. Workbook examples are installed by default. For more details on customizing these defaults, see Configure Initial Node Settings.

- Pass the configuration file with the following command:

```
tsm settings import -f /opt/tableau/tableau_server-/packages/scripts.<version_code>/config.json
```

### Step 4: Finalize installation

The final steps of installation are to apply changes, initialize and start TSM, and then to create the administration account. More details about these steps are at Configure Initial Node Settings.

1. **Apply the configurations you made in the previous steps.** Run the following command:

   ```
tsm pending-changes apply
   ```

2. **Initialize and start Tableau Server.** Run the following command:

   ```
tsm initialize --start-server --request-timeout 1800
   ```

3. **Create the Tableau Server administrator account.** Run the following command:

   ```
tabcmd initialuser --server 'localhost:80' --username 'admin' --password '<password>'
   ```

   Where '<password>' is a strong password. Enclose the password and other arguments in single quotes.
Use the admin account that you created to access the Tableau Server admin web pages. See Sign in to the Tableau Server Admin Area.

Step 5: Install PostgreSQL drivers

To validate that Tableau Server is installed and running properly and to review the built-in administrative views, you must install the PostgreSQL driver.

1. Download PostgreSQL drivers from the Driver Download page.

2. Install the drivers on your Tableau Server computer:
   - On CentOS and RHEL, download the .rpm file and then run the following command:
     
     ```bash
     sudo yum install tableau-postgresql-odbc-9.5.3-1.x86_64.rpm
     ```
   
   - On Ubuntu, download the .deb file and then run the following command:
     
     ```bash
     sudo dpkg -i tableau-postgresql-odbc_9.5.3_amd64.deb
     ```

3. To validate that the drivers installed, navigate to the Administrative Views in Tableau Server.

Configure Local Firewall

This topic explains how to configure the firewall on the computer running Tableau Server.

A local firewall should be enabled on the operating system to protect Tableau Server in single and multi-node deployments. In a distributed (multi-node) installation of Tableau Server, communication between nodes does not use secure communication. Therefore, you should enable firewalls on the computers that host Tableau Server.

We recommend that you configure the firewall so that only two ports are accessible to external traffic: the gateway port and the tabadmincontroller port. By default, these are ports 80 and 8850 respectively. Additionally, if you are running in a distributed deploy-
ment, then you will need to open the port range, 27000-27009, so licensing can communicate across nodes.

The gateway port is used for HTTP connection to Tableau Server. We recommend that you use SSL for the gateway port. If you will be using SSL, then the port must be 443 because Tableau Server does not support other ports for SSL. The procedures below describe how to configure the firewall for the gateway port. Configure the Tableau Server gateway (Configure Initial Node Settings) to match the port you set here.

The examples below describe how to configure the firewall on single and multi-node deployments of Tableau Server running on RHEL/CentOS distributions. The examples use Firewalld, which is the default firewall on CentOS.

**Single-node configuration**

1. Open a bash shell and run the following TSM command to retrieve the port number for the tabadmincontroller port:

   ```
tsm topology list-ports
   ```

   Make a note of the tabadmincontroller port. By default, this port is 8850.

2. Start firewalld:

   ```
sudo systemctl start firewalld
   ```

3. Verify that the default zone is a high-security zone, such as public. If it is not, we recommend changing it to a high-security zone.

   ```
sudo firewall-cmd --get-default-zone
   sudo firewall-cmd --set-default-zone=public
   ```

4. Add ports for the gateway port and the tabadmincontroller port. In the example below we use the default ports (80 and 8850).

   ```
sudo firewall-cmd --permanent --add-port=80/tcp
   ```
sudo firewall-cmd --permanent --add-port=8850/tcp

5. Reload the firewall and verify the settings.

   sudo firewall-cmd --reload
   sudo firewall-cmd --list-all

Multi-node cluster configuration

In addition to enabling ports, configuring the firewall on a multi-node cluster requires additional steps to ensure that nodes can communicate with each other.

Before you begin

You will need the IP address for each node in the cluster. The example here uses <node1IP> as a placeholder for the initial node IP address, and <node2IP> and <node3IP> as placeholders for the IP addresses of two additional nodes.

Step 1: Configure initial node.

   1. Open a bash shell and run the following TSM command to retrieve the port number for the tabadmincontroller port:

      tsm topology list-ports

      Make a note of the tabadmincontroller port. By default, this port is 8850.

   2. Run the following commands to determine the range of port numbers that TSM may dynamically select. You will specify this range later in this procedure. Make a note of the port range.

      tsm configuration get -k ports.range.min
      tsm configuration get -k ports.range.max

      A typical range is 8000 to 9000.

   3. Start firewalld:
sudo systemctl start firewalld

4. Verify that the default zone is a high-security zone, such as public. If it is not, we recommend changing it to a high-security zone.

```
failsafe-cmd --get-default-zone
```

```
sudo failsafe-cmd --set-default-zone=public
```

5. Add ports for the gateway port and the tabadmincontroller port. In the example below we use the default ports (80 and 8850). You must also add a port range (27000-27010) to enable licensing communication between nodes.

```
sudo failsafe-cmd --permanent --add-port=80/tcp
```

```
sudo failsafe-cmd --permanent --add-port=8850/tcp
```

```
sudo failsafe-cmd --permanent --add-port=27000-27010/tcp
```

6. Configure the firewall to allow all traffic from the other nodes in the cluster. For the ports option, specify the range you noted in Step 2. Run the command for each of the additional nodes in your cluster. For example:

```
sudo failsafe-cmd --permanent --add-rich-rule='rule family=ipv4 source address=<node2IP>/32 port port=8000-9000 protocol=tcp accept'
```

```
sudo failsafe-cmd --permanent --add-rich-rule='rule family=ipv4 source address=<node3IP>/32 port port=8000-9000 protocol=tcp accept'
```

7. Reload the firewall and verify the settings.

```
sudo firewall-cmd --reload
```

```
failsafe-cmd --list-all
```
Step 2: Configure additional nodes

Each node in the cluster must be able to communicate with the initial node and with the other nodes.

Run this procedure on each additional node in the cluster. In this example, the node at IP address, <node2IP>, communicates with the initial node at <node1IP> and a third node at <node3IP>.

1. Start firewall:

   sudo systemctl start firewalld

2. Verify that the default zone is a high-security zone, such as public. If it is not, we recommend changing it to a high-security zone.

   firewall-cmd --get-default-zone

   sudo firewall-cmd --set-default-zone=public

3. Configure the firewall to allow gateway and tabadmincontroller access from the other nodes in the cluster. For example:

   sudo firewall-cmd --permanent --add-rich-rule='rule family=ipv4 source address=<node1IP>/32 port port=80 protocol=tcp accept'

   sudo firewall-cmd --permanent --add-rich-rule='rule family=ipv4 source address=<node1IP>/32 port port=8000-9000 protocol=tcp accept'

   sudo firewall-cmd --permanent --add-rich-rule='rule family=ipv4 source address=<node3IP>/32 port port=80 protocol=tcp accept'
sudo firewall-cmd --permanent --add-rich-rule="rule family=ipv4 source address=<node3IP>/32 port port=8000-9000 protocol=tcp accept"

In this example, since the tabadmincontroller port (8850) is included in the port range, it is not explicitly specified in a command.

4. Reload the firewall and verify the settings.

sudo firewall-cmd --reload

firewall-cmd --list-all

Automated Installation of Tableau Server

Tableau provides an automated-installer script to automate an install of Tableau Server. The script is community supported. You can download the script and use it as written, or modify it for your specific needs.

Benefits of using the automated installer

- With a single command, you can install, configure and get to a working instance of Tableau Server.

- The command can be run without user input making it suitable for automation.

- The configuration can be set once and used for all your installations, making this a repeatable process.

When not to use the automated installer:

- If you are installing for the first time, we recommend that you manually test the installation before automating the process. Any issues that block installation are easier to resolve interactively, and after you have resolved these issues, you can use the automated installer.
Tableau Server on Linux Administrator Guide

- If you are testing or trying new configuration parameters such as authentication methods, we recommend that you manually run the installation first. TSM validates configuration entities and rejects configuration parameters that are not valid. Once you have the correct parameters identified, you can use the automated installer.

- If you are unable to or do not want to enter passwords into the secrets file, using the automated installer might not be an option for you.

Before you begin

Review the Before you install... topic to make sure you have installed Linux on a computer that meets the operating system requirements and the minimum hardware requirements for Tableau Server.

Note: If you are installing Tableau Server in a production environment, review the minimum hardware recommendations. The recommendations represent the minimum hardware configuration you should use for a production installation of Tableau Server.

To perform an automated installation, you have to use the automated installer package, which uses the Tableau Server install package as an input. We recommend that you download both of these packages before you begin as follows:

1. Download both the automated installer package and the Tableau Server installer package:
   a. Download the automated installer package from GitHub for the distribution you are using. The automated installer packages can be found in the packages sub directory.

      Note: The version of automated installer package you use must match the version of the Tableau Server installer package. For example, use 10.5.0 version of the automated installer package with 10.5.0 version of the Tableau Server installer package.

   b. Select and download the appropriate Tableau Server installer package from
the Tableau Server Product Downloads and Release Notes page. The one you choose depends on which Linux distribution you are using. For example, for RHEL like systems, tableau-server-<version>.x86_64.rpm.

2. Copy the packages and templates to a location on or accessible from the computer where you are going to install Tableau Server.

How to use the automated installer

The automated installer installs the Tableau Server installer package, creates the directories, sets the permissions required to run Tableau Server, and starts the Tableau Services Manager (TSM) setup. After the TSM setup is completed, the automated installer runs tsm commands to install, configure, and start Tableau Server. By default, during installation, the automated installer activates a trial license. If you have an actual product key, you can provide the product key at the command line or activate the product key after you run the script. Most of the command line options in the automated installer are the same as the options used by the tsm initialize command.

To run the automated installer without user input, you must provide the following required command line options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s &lt;secrets-file&gt;</td>
<td>The name of the secrets file. The secrets file should have the user names and passwords for TSM administrator and the Tableau Server administrator accounts.</td>
</tr>
</tbody>
</table>

**Note:** Providing the password in the secrets file is optional. However, if passwords are not found in the secrets file, you will be prompted to provide them during installation.
The automated installer package includes the template for the secrets file.

- `f <config-file>`
  The name of the configuration JSON file. The automated installer package includes the template for the configuration file.

- `r <registration-file>`
  The name of the registration file. The automated installer package includes the template for the registration file.

--accepteula
Indicates that you have accepted the End User License Agreement.

<package-file>
The rpm or deb Tableau Server installer.

Use the `-h` option to see a full list of all the required command line options.

Configure Tableau Server for a forward proxy

If your organization uses a forward proxy solution to access the internet, then configure Tableau Server to use the proxy server. Tableau Server must access the internet for map data and for default licensing functionality.

We recommend configuring Tableau Server for a forward proxy solution during installation.

To configure proxy server during unattended installation, include the `--http_proxy` and/or `--https_proxy` flags to specify the forward proxy server.

Specify the URL with the port, for example:

```
--http_proxy=http://proxy.example.lan:80/ --https_proxy=yt=http://1.2.3.4:443/
```

Take care to use `http` when you specify the URL for the `https_proxy` variable. Do not specify the `https` protocol for the value of the `https_proxy` variable.

To configure Tableau Server to bypass the forward proxy, include the `--no_proxy` flag. You should also add exceptions to this proxy configuration to guarantee that all
communications within a local Tableau Server cluster (if you have one now or will have one later) do not route to the proxy server. For example:

```
--no_proxy=localhost,127.0.0.1,localaddress,.localdomain.com.
```

If you do not configure the forward proxy during installation, then refer to Configuring Tableau Server on Linux to work with a forward proxy, after you have installed.

Perform an unattended installation

Step 1: Install the automated installer

1. Log onto the computer as a user with sudo access.

2. Use the package manager to install the script package:

   - ON RHEL-like distributions, including CentOS, run the following command:
     
     ```
     sudo yum install /path/to/tableau-server-automated-installer-<version>.noarch.rpm
     ```

   - On Ubuntu, run the following commands:
     
     ```
     sudo apt-get update
     sudo apt-get -y install gdebi-core
     sudo gdebi -n /path/to/tableau-server-automated-installer-<version>.deb
     ```

The automated installer package download includes templates for the configuration file (config.json), registration file (reg_templ.json) and the secrets (secrets) file that you can use to modify for your requirements as described in the next step. The installer script, and the templates for the initial node configuration, Tableau Server registration, and secrets file are installed to:
Step 2: Create files to provide additional configuration information required to run the automated install

Since the automated installer is meant to run without user interaction, you must provide the following additional information:

1. Run the following command to copy the templates, config.json, reg_templ.json, and secrets, to another directory like your home directory. We don't recommend that you edit the template files directly:

   cp /opt/tableau/tableau_server_automated_installer/automated-installer.<version>/
   {config.json,reg_templ.json,secrets} ~

2. Edit the configuration template, config.json, to provide the initial node configuration settings. You must provide identity store settings for the Tableau Server computer. Depending on your network requirements, you may need to also provide the gateway settings. The caching option is set to cache and reuse data for as long as possible. Sample workbooks are installed by default. The template includes the minimum required information, so the template is a starting point. For more information on configuration settings, see Configure Initial Node Settings.

3. Edit the registration file reg_templ.json to provide the information needed to register Tableau Server. For more information, see Activate and Register Tableau Server.

4. Edit the secrets file using the secrets template with the user name and password for the TSM administrator and Tableau Server administrator accounts.

   - The TSM administrator account should be the same user as the sudo admin running the script. If you do not want to specify the password in the secrets file, you can leave it blank, and you will be prompted to provide the password during
The Tableau Server administrator account is the initial account that is created by the installer and is used to administer Tableau Server.

Step 3: Run the automated install

1. Log onto the computer as a user with sudo access.

ON RHEL-like distributions, including CentOS, run the following command:

```bash
sudo /opt/tableau/tableau_server_automated_installer-automated-installer.<version>/automated-installer -s /path/to/secrets -f /path/to/config.json -r /path/to/reg_templ.json --accepteula /path/to/tableau-server-<version>.x86_64.rpm
```

On Ubuntu, run the following command:

```bash
sudo /opt/tableau/tableau_server_automated_installer-automated-installer.<version>/automated-installer -s /path/to/secrets -f /path/to/config.json -r /path/to/reg_templ.json --accepteula /path/to/tableau-server-<version>_amd64.deb
```

**Important:** You must specify `--accepteula` key to acknowledge and accept the end user license agreement (EULA) in the command that you use the run the script. The EULA is available in the following location: `/opt/tableau/tableau_server/packages/docs.<version_code>/EULA.rtf`. 
Install Tableau Server in a Disconnected (Air-Gapped) Environment

You can install Tableau Server in a disconnected environment that has no outside network access of any kind. Such disconnected environments, commonly referred to as air-gapped, are used when high security is needed to prevent data breaches or to guard against hacking. Air-gapped environments have no internet access, no outside network access, no outside wireless access, etc. The only means of getting software and data into or out of an air-gapped environment is by using removable media such as USB sticks or writeable optical CDs or DVDs.

Installing Tableau Server in an air-gapped environment is an advanced task for IT administrators who are familiar with the security considerations, best practices, and pitfalls of installing software in air-gapped environments.

The following Tableau Server features will be unavailable or will have reduced functionality in an air-gapped environment:

- **Maps** – Tableau Server uses externally hosted map data. Maps are unavailable in an air-gapped environment unless you also install a map server in your air-gapped environment. You can use the following workarounds.

- **Licensing** – Tableau Server needs to connect to the internet in order to activate product keys. However, you can manually activate the product keys.
• **External data** – Any data located outside your air-gapped environment is unavailable.

Prerequisites

In order to install Tableau Server in an air-gapped environment, you’ll need the following:

• Trusted computer with limited access to the internet that you can use to download the installation packages and resources required by Tableau Server. A trusted computer has been scanned and cleared of any viruses and malware.

• Trusted removable media that you can use to transfer the downloaded software to your air-gapped environment. Trusted removable media is removable media that is new and previously unused and comes from a reputable or known source. Trusted removable media has been scanned and verified that it does not contain any viruses or malware.

• Air-gapped environment with computers and storage that meet the requirements for installing Tableau Server.

Installing Tableau Server on an Air-Gapped Computer Running Linux

The easiest way to install Tableau Server on a computer in an air-gapped environment is to do so before the computer is placed into the air-gapped environment. If that’s not possible you’ll need to download the required packages to a trusted computer outside the air gap:

1. On a trusted computer outside the air gap with internet access, download the Tableau Server installation package.

2. Extract the list of dependent packages:

   **On Ubuntu:**
dpkg --field <debfile> Depends (where <debfile> is the name of the .deb package you downloaded from Tableau).

Example command:

dpkg --field tableau-server-linux-1.deb Depends

Example output:

cacertificates, fontconfig, net-tools, bash-completion, cacertificates-java, freeglut3, libegl1-mesa, libfreetype6, libgssapi-krb5-2, libxcomposite1, libxrender1, libxslt1.1, lsb-core

On RHEL and RHEL-like Linux distributions:

yum -q deplist <RPM file> (where <RPM file> is the .rpm package you downloaded from Tableau).

Example command:

yum -q deplist tableau-server-linux_1.rpm

Example output:

package: tableau-server-10400.17.0703.1600.x86_64 10400-17.0703.1600
dependency: /bin/sh
provider: bash.x86_64 4.2.46-21.el7_3
dependency: bash-completion
provider: bash-completion.noarch 1:2.1-6.el7
dependency: cacertificates
provider: cacertificates.noarch 2017.2.14-70.1.el7_3
3. Download each of the dependent packages:

On Ubuntu:
apt-get download <package1> <package2>...

On RHEL and RHEL-like Linux distributions:

yumdownloader <package1> <package2>...

4. Transfer the packages to your removable media.

5. On your air-gapped computer, insert the removable media containing the Tableau Server installation package and dependent packages, and then run the installer.

6. After installation is complete, you can activate the Tableau Server product keys. For more information, see Activating Tableau Server in an Air-Gapped Environment.

Activating Tableau Server in an Air-Gapped Environment

Because an air-gapped computer is not connected to the internet, you’ll need to perform the Tableau Server activation process manually.

Step 1. Transcribe data from your air-gapped system into an activation request template.

1. On your Tableau Server in the air-gapped environment, use TSM to obtain the offline activation file. At a command prompt:

   tsm licenses get-offline-activation-file -k <product-key> -o <target-directory>

   The <target-directory> must exist. You can obtain your product key in the Tableau Customer Portal.

2. On a trusted computer that is connected to the internet and is capable of sending files via email, right-click and choose Save link as to download either the server_first-pass_linux.tlq or the server_secondpass_linux.tlq file. The firstpass template is used when the computer has never had Tableau Server installed on it before.

3. Open both the offline.tlq file from the disconnected computer, and the
appropriate server_firstpass_linux.tlq or server_secondpass_linux.tlq file in an XML text editor such as Notepad++ on the trusted computer that has Internet access. You'll need to write down the values from the disconnected computer in order to copy them to the computer that has Internet access.

4. Update the following XML elements in the appropriate .tlq file (server_firstpass_linux.tlq or server_secondpass_linux.tlq) with the values for the same elements in offline.tlq on the disconnected computer. The template file has X's where you need to change the values. Do not change anything other than the values below.

All the Machine / Hash values in the .tlq files are Hex values. The only valid characters are 0 - 9 and A - F. Use all caps for any letters.

Line 2 - <EntitlementId>

Line 5 - <ClientVersion>

Line 5 - <RevisionType> (This value is only present in the server_secondpass_linux.tlq file.)

Line 5 - <MachineIdentifier> (This value is only present in the server_secondpass_linux.tlq file.)

Line 11 - <Value> (If the value is not present, remove the "X" place holder, leaving <Value></Value>.)

Line 12 - <Value> (If the value is not present, remove the "X" place holder, leaving <Value></Value>.)

Line 13 - <Value> (If the value is not present, remove the "X" place holder, leaving <Value></Value>.)

Line 15 - <SequenceNumber>
5. Upload the edited template (offline.t1q) to the Tableau Offline Activation website.

6. The website should say The activation was successful. Please click here to download your activation file.

   Download the activation.tlf file and transfer it to your Tableau Server.

Step 2. Initialize or activate your license

1. Move the activation file (activation.tlf) to your disconnected computer using trusted removable media.

2. Run the following command:

   tsm licenses activate -f <path-and-activation-file>

First time license activation

If this is the first Tableau license activated on the computer, you will see this message:

Your license has been initialized. To complete the activation, we need one more exchange. Generate and send to Tableau a second activation request file.

You need to follow the steps below to activate your license. If you are not sure whether you need to repeat the steps, you can run this command:

   tsm licenses list

   If you see a message like this one you need to repeat the steps above:

   No licenses are currently activated.
Subsequent license activation

If this is not the first Tableau license activated on the computer, or if you have completed the steps above two times, you should see the message "Activation successful," which indicates that Tableau Server is activated.

**Note:** You may have to perform offline activation twice to completely activate your air-gapped Tableau Server. The first offline activation sets up Trusted Storage on the computer if Tableau has never been licensed on it before. The second offline activation propagates the licensing information into Trusted Storage. If you’re upgrading an existing install of Tableau Server, right-click and choose Save link as to download the server_secondpass_linux.tlq file. It will match all the places to put the values from the generated .tlq file.

Displaying Maps in an Air-Gapped Environment

In an air-gapped environment, maps in Tableau Server will be unavailable due to the lack of internet access in the air-gapped environment. You can use the following workarounds to display maps in an offline environment:

- **Option 1** – Use the offline background maps

  To use the offline background map select Map > Background maps > Offline. For more information, see Select Background Maps.

  **Note:** Due to size limitations with the offline map, zooming in too deep may result in errors as the images for the more close-up maps are not stored offline.

- **Option 2** – Use a map as a background image

  Locate the desired map online and save it as an image file, or copy a map from another location. Set this map image as a static background image in Tableau Desktop. For more information, see Use Background Images in Your Views.
Note: Zooming in and out will not work with background images.

- Option 3 – Use a local GeoServer

For more information, see Use Web Map Service (WMS) Servers.

Install Tableau Server in the Cloud

Even if you don’t have your own infrastructure and server hardware, you can deploy an enterprise-level Tableau Server installation in the cloud. Building a cloud-based solution has many benefits over an on-premises installation. For example, the overall total cost of ownership for building a Tableau Server solution in the cloud is normally much less than a similar on-premises solution because you don’t have to buy all of the expensive hardware. In addition, the cloud can provide better uptime, reliability, and fault-tolerance, especially if you deploy your solution across different regions and availability zones.


You can build and scale your Tableau environment in the following cloud environments:

- **Tableau Online** - If you don’t want to install software or purchase hardware, you can choose analytics as a service with Tableau Online, the Tableau-hosted environment in the cloud. For more information, see Tableau Online.

- **Amazon Web Services** - You install and manage Tableau Server on Amazon Web Services (AWS). For more information, see Install Tableau Server in the AWS Cloud.

- **Google Cloud Platform** - You install and manage Tableau Server on the Google Cloud Platform. For more information, see Install Tableau Server on the Google Cloud Platform.

- **Microsoft Azure** - You install and manage Tableau Server on Microsoft Azure. For more information, see Install Tableau Server on Microsoft Azure.
Post Installation Tasks

Security Hardening Checklist

The following list provides recommendations for improving the security ("hardening") of your Tableau Server installation.

1. Update to the current version

We recommend that you always run the latest version of Tableau Server. Additionally, Tableau periodically publishes maintenance releases of Tableau Server that include fixes for known security vulnerabilities. (Information regarding known security vulnerabilities can be found on the Security Bulletins page.) We recommend that you review maintenance release notifications to determine whether you should install them.

To get the latest version or maintenance release of Tableau Server, visit the Customer Portal page.

2. Configure SSL/TLS with a valid, trusted certificate

Secure Sockets Layer (SSL/TLS) is essential for helping to protect the security of communications with Tableau Server. Configure Tableau Server with a valid, trusted certificate (not a self-signed certificate) so that Tableau Desktop, mobile devices, and web clients can connect to the server over a secured connection. For more information, see SSL.

3. Disable older versions of TLS

Tableau Server uses TLS to authenticate and encrypt many connections between components and with external clients. External clients, such as browsers, Tableau Desktop, Tableau Mobile connect to Tableau using TLS over HTTPS. Transport layer security (TLS) is an improved version of SSL. In fact, older versions of SSL (SSL v2 and SSL v3) are no longer considered to be adequately secure communication standards. As a result, Tableau
Server does not allow external clients to use SSL v2 or SSL v3 protocols to connect. We recommend that you only allow external clients to connect to Tableau Server with TLS v1.2.

Specifically, we recommend that you disable TLS v1 and TLS v1.1 on Tableau Server. However, before you disable a specific version of TLS, verify that the browsers that your users connect to Tableau Server with support TLS v1.2. In some cases, you may need to preserve support for TLSv1.1.

The following tsm command enables TLS v1.2 (using the "all" parameter) and disables SSL v2, SSL v3, TLS v1, and TLS v1.1 (by prepending the minus [-] character to a given protocol).

```
tsm configuration set -k ssl.protocols -v 'all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1'
```

```tsm pending-changes apply```

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see tsm pending-changes apply.

4. Disable Triple-DES cipher suite

The Triple-DES cipher suite is no longer considered adequate to encrypt sessions on the internet. Specifically, running Triple-DES ciphers leaves the Tableau Server vulnerable to information disclosure and denial of service attacks. You can learn more at the National Vulnerability Database webpage for CVE-2016-2183.

Triple-DES is enabled by default on the version of OpenSSL that is running on Tableau Server. However, other deprecated cipher suites (MD5 and RC4) are disabled. To add Triple-DES to the list of disabled ciphers, run the following commands. (The `!aNULL` parameter forces clients to use a legitimate cipher.)
tsm configuration set -k ssl.ciphersuite -v
'HIGH:MEDIUM:!aNULL:!MD5:!RC4:!3DES'

tsm pending-changes apply

5. Configure SSL encryption for internal traffic

Configure Tableau Server to use SSL to encrypt all traffic between the Postgres repository and other server components. By default, SSL is disabled for communications between server components and the repository. We recommend enabling internal SSL for all instances of Tableau Server, even single-server installations. Enabling internal SSL is especially important for multi-node deployments. See Configure SSL for Internal Postgres Communication.

6. Enable firewall protection

Tableau Server was designed to operate inside a protected internal network.

**Important:** Do not run Tableau Server, or any components of Tableau Server on the internet or in a DMZ. Tableau Server must be run within the corporate network protected by an internet firewall. We recommend configuring a reverse proxy solution for internet clients that need to connect to Tableau Server. See Configuring Proxies for Tableau Server.

A local firewall should be enabled on the operating system to protect Tableau Server in single and multi-node deployments. In a distributed (multi-node) installation of Tableau Server, communication between nodes does not use secure communication. Therefore, you should enable firewalls on the computers that host Tableau Server. See Configure Local Firewall.

To prevent a passive attacker from observing communications between nodes, configure a segregated virtual LAN or other network layer security solution.
See Tableau Services Manager Ports to understand which ports and services Tableau Server requires.

7. **Restrict access to the server computer and to important directories**

Tableau Server configuration files and log files can contain information that is valuable to an attacker. Therefore, restrict physical access to the machine that is running Tableau Server. In addition, make sure that only authorized and trusted users have access to the Tableau Server files in the `/var/opt/tableau/tableau_server/` directory.

8. **Generate fresh secrets and tokens**

Any Tableau Server service that communicates with repository or the cache server must first authenticate with a secret token. The secret token is generated during Tableau Server setup. The encryption key that internal SSL uses to encrypt traffic to Postgres repository is also generated at during setup.

We recommend that after you install Tableau Server, you generate new encryption keys for your deployment.

These security assets can be regenerated with the `tsm security regenerate-internal-tokens` command.

Run the following commands:

```bash
tsm security regenerate-internal-tokens
tsm pending-changes apply
```

9. **Disable services that you're not using**

To minimize the attack surface of the Tableau Server, disable any connection points that are not needed.
REST API

The REST API interface is enabled by default. If no applications will make REST API calls to your installation of Tableau Server 9.3 (or later), disable it by using the following commands:

```
tsm configuration set -k api.server.enabled -v false

 tsm pending-changes apply
```

Important: Tableau Prep uses REST API to access Tableau Server. If your organization uses Tableau Prep, do not disable REST API.

JMX Service

JMX is disabled by default. If it's enabled but you're not using it, you should disable it by using the following:

```
tsm configuration set -k service.jmx_enabled -v false

 tsm pending-changes apply
```

10. Verify session lifetime configuration

By default, Tableau Server does not have an absolute session timeout. This means that client sessions can remain open indefinitely if the Tableau Server inactivity timeout is not exceeded. (The default inactivity timeout is 240 minutes.)

If your security policy requires it, you can set an absolute session timeout. Be sure to set your absolute session timeout in a range that allows the longest-running extract or publishing operations in your organization. Setting the session timeout too low may result in extract and publishing failures for long-running operations.

To set the session timeout run the following commands:
Tableau Server on Linux Administrator Guide

tsm configuration set -k wgserver.session.apply_lifetime_limit -v true

tsm configuration set -k wgserver.session.lifetime_limit -v value, where value is the number of minutes. The default is 1440, which is 24 hours.

tsm configuration set -k wgserver.session.idle_limit -v value, where value is the number of minutes. The default is 240.

tsm pending-changes apply

11. Configure a server safelist for file-based data sources

By default, Tableau Server allows authorized Tableau Server users to build workbooks that use files on the server as file-based data sources (such as spreadsheets). In this scenario, files are accessed by the tableau system account.

To prevent unwanted access to files, we recommend that you configure safelist (sometimes referred to as “whitelist”) functionality. This lets you limit tableau account access to just the directory paths where you host data files.

1. On the computer running Tableau Server, identify the directories where you will host data source files.

   Important Make sure the file paths you specify in this procedure exist on the server. If the paths do not exist when the computer starts, Tableau Server will not start.

2. Run the following commands:

   tsm configuration set -k native_api.allowed_paths -v "path" , where path is the directory to add to the safelist. All subdirectories of the specified
path will be added to the safelist. If you want to specify multiple paths, separate them with a semicolon, as in this example:

```
tsm configuration set -k native_api.allowed_paths -v
"/datasources;/HR/data"
```

tsm pending-changes apply

### 12. Enable HTTP Strict Transport Security for web browser clients

HTTP Strict Transport Security (HSTS) is a policy configured on web application services, such as Tableau Server. When a conforming browser encounters a web application running HSTS, then all communications with the service must be over a secured (HTTPS) connection. HSTS is supported by major browsers.

For more information about how HSTS works and the browsers that support it, see The Open Web Application Security Project web page, [HTTP Strict Transport Security Cheat Sheet](https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet).

To enable HSTS, run the following commands on Tableau Server:

```
tsm configuration set -k gateway.http.hsts -v true
```

By default, HSTS policy is set for one year (31536000 seconds). This time period specifies the amount of time in which the browser will access the server over HTTPS. You should consider setting a short max-age during initial roll-out of HSTS. To change this time period, run `tsm configuration set -k gateway.http.hsts_options -v max-age=<seconds>`. For example, to set HSTS policy time period to 30 days, enter `tsm configuration set -k gateway.http.hsts_options -v max-age-e=2592000`.

```
tsm pending-changes apply
```
13. Disable Guest access

Core-based licenses of Tableau Server include a Guest user option, which allows any user in your organization to see and interact with Tableau views embedded in web pages.

Guest user access is enabled by default on Tableau Servers deployed with core-based licensing.

Guest access allows users to see embedded views. The Guest user cannot browse the Tableau Server interface or see server interface elements in the view, such as user name, account settings, comments, and so on.

If your organization has deployed Tableau Server with core licensing and Guest access is not required, then disable Guest access.

You can disable Guest access at the server or site level.

You must be a server administrator to disable the Guest account at either the server or the site level.

To disable Guest access at the server level:

1. In the site menu, click Manage All Sites and then click Settings > General.

2. For Guest Access, clear the Enable Guest account check box.

3. Click Save.

To disable Guest access for a site:

1. In the site menu, select a site.

2. Click Settings, and on the Settings page, clear the Enable Guest account check box.

For more information, see Guest User.
Tableau Server on Linux Administrator Guide

Change List

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 2017</td>
<td>Ported and updated for Tableau Services Manager and Linux platform.</td>
</tr>
<tr>
<td>May 2018</td>
<td>Added clarification: Do not disable REST API in organizations that are running Tableau Prep.</td>
</tr>
</tbody>
</table>

Configure SMTP Setup

Tableau Server can email server administrators about system failures, and email server users about subscribed views and data-driven alerts. First, however, you need to configure the SMTP server that Tableau Server uses to send email. After configuring SMTP, complete the steps to configure notifications (Configure Server Event Notification), then when you start or restart the server, it will trigger an email notification, which confirms that you have set up notifications correctly.

Encrypted SMTP connections are not supported for notifications or subscriptions.

Configuring SMTP requires that you restart Tableau Server services.

Use the TSM web interface

1. Open TSM in a browser:
   https://<tsm-computer-name>:8850. For more information, see Sign in to Tableau Services Manager Web UI.

2. Click Notifications on the Configuration tab and click Email Server.

3. Enter the SMTP configuration information for your organization:
4. Click **Save Pending Changes** after you've entered your configuration information.

5. Click **Pending Changes** at the top of the page:

6. Click **Apply Changes and Restart**.

**Use the TSM CLI**

For the initial configuration of SMTP, we recommend that you use the configuration file template below to create a json file. You can also set any single configuration key listed below with the syntax described in tsm configuration set.

1. Copy the following json template to a file. Fill in the key values with your SMTP configuration. See the reference section that follows for more information about SMTP key options.

```json
{
```

Tableau Server on Linux Administrator Guide
"configKeys": {  
  "svcmonitor.notification.smtp.server": "SMTP server url",  
  "svcmonitor.notification.smtp.send_account": "SMTP user name",  
  "svcmonitor.notification.smtp.port": 25,  
  "svcmonitor.notification.smtp.password": "SMTP server password",  
  "svcmonitor.notification.smtp.ssl_enabled": false,  
  "svcmonitor.notification.smtp.from_address": "From email address",  
  "svcmonitor.notification.smtp.target_addresses": "To email address1,address2",  
  "svcmonitor.notification.smtp.canonical_url": "Tableau Server URL"
}

2. Run the `tsm settings import -f file.json` to pass the json file with the appropriate values to Tableau Services Manager to configure Tableau Server for SMTP. Tableau Services Manager will validate the entity values.

3. Run the `tsm pending-changes apply` command to apply the changes. See `tsm pending-changes apply`.

Configuration file reference

This table lists all of the options that can be used to configure SMTP.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>svc-</code></td>
<td>Address of SMTP server.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>mon-itor.notification.smtp.server</td>
<td>Example: &quot;svc-mon-itor.notification.smtp.server&quot;: &quot;mail.example.com&quot;</td>
</tr>
<tr>
<td>svc-mon-itor.notification.smtp.send_account</td>
<td>User name for SMTP account.</td>
</tr>
<tr>
<td>svc-mon-itor.notification.smtp.port</td>
<td>Port number for SMTP server. The default is 25.</td>
</tr>
<tr>
<td>svc-mon-itor.notification.smtp.password</td>
<td>Password for SMTP server account. Example: &quot;svc-mon-itor.notification.smtp.password&quot;: &quot;password&quot;</td>
</tr>
<tr>
<td>svc-mon-itor.notification.smtp.ssl_enabled</td>
<td>Specifies whether the connection to the SMTP server is encrypted. The default is false. <em>Note: This should be left as false. Encrypted SMTP connections are not supported for notifications or subscriptions.</em></td>
</tr>
</tbody>
</table>
| svc-mon-itor.notification.smtp.from | Email address that will send an notification if there's a system failure. The email address must have valid syntax (for example, ITalerts@bigco.-
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>com or noreply@mycompany), but it does not have to be an actual email account on Tableau Server. (Some SMTP servers may require an actual email account, however.)</td>
</tr>
</tbody>
</table>

**Note:** You can override the system-wide email address on a per-site basis. For more information, see What is a site.

Example:

"svc-monitor.notification.smtp.from_address": "donot-reply@example.com"

| svc-monitor.notification.smtp.target_addresses | Email address to receive notifications. If email notifications are enabled, you need to include at least one address. Separate multiple addresses with commas. |

Example:

"svc-monitor.notification.smtp.target_addresses": "iluvdata@example.com"

| svc-monitor.notification.smtp.canonical_url | URL of the Tableau Server. Enter http:// or https://, followed by the name or IP address of the Tableau server. Used in the footer of subscription email. |
Files and Permissions in TSM

This topic covers the permissions requirements needed for Tableau Services Manager (TSM) to access and use files. This information is intended for server administrators. This topic does not address permissions used for managing users and content within Tableau Server (permissions for content and users). For information related to these permissions, see Content Permissions and Ownership.

During installation of TSM and Tableau Server, an unprivileged user (tableau) is created and added to a server authorized group (tableau). This user account enables the work done by TSM and Tableau Server processes. You can change the user and group during installation. For more information, see Identity Store.

Permissions requirements for TSM apply to both files, and to the directories in which the files are placed. When TSM creates and manages files, the files get put into specific default locations with the necessary permissions and you don't need to worry about setting permissions. When you create, copy, or move files yourself, or when you put files into non-default locations, you need to be aware of permission requirements so that TSM can properly access the files. Common cases (For information about using non-default locations, see tsm File Paths.)

General rules for permissions and TSM are:
Files—If the tableau group has access to a file (if it is the group owner and has read access to the file), the users in the group have access to the file. An alternate approach is to give "other" read access.

Directories—If the tableau group has read and execute access to the directory that contains a file, and any parent directories of that directory, the users in the group have access to the file.

Situations that may require you to adjust permissions include server backup files and site import archives that you copy from a different computer or to a non-default location, customization files such as logos or images, and security certificates such as SSL certificates.

For example, if you migrate from Tableau Server on Windows to Tableau Server on Linux, you use a backup created in Windows to restore data to your Linux server. Because this backup file isn't created by TSM, it may not have the correct permissions for the restore process to access it. You need to make sure the backup file and the directory structure you copy it into have the proper permissions. Similarly, if you are copying files like certificates to additional nodes in a cluster, you need to make sure the files and the directories you copy them into have the permissions the tableau user needs in order to access them.

Setting permissions for individual files

If you are using a file you copy to one of the default locations created by TSM, you need to make sure the ownership and permissions on the file allow TSM access by giving the tableau user read access. You can do this in one of two ways:

- You can give the tableau user read access by giving the tableau group (in a default installation) read and execute access to a file using the chgrp and chmod commands. For example:

  chgrp tableau <backup>.tsbak
  chmod g+rx <backup>.tsbak
Alternately, you can give world read and execute access to the file:

```
chmod o+rx <backup>.tsbak
```

**Setting permissions for directories**

In addition to setting the proper permissions on the files themselves, TSM also needs permissions for the directory that contains the file, as well as any parent directories. If you are using a non-default location for files that TSM will access, you will need to make sure permissions for the parent directory or directories that contain the file allow read and execute access.

You can address this issue in a couple of ways:

- Change group ownership of the directory to the *tableau* group, and add group read and execute permission to the directory. Doing this makes files in the directory more available to the *tableau* user.

  ```
  chgrp tableau <directory-name>
  chmod g+rx <directory-name>
  ```

- Alternatively, you can add world read and execute permission to the directory. This makes files in the directory more available to all users on the system. This approach may require additional steps to ensure security of other files in the directory. For example, you may want to make sure other files in the directory are not world readable so other users cannot read them.

  ```
  chmod o+rx <directory-name>
  ```

**Hint:** You can use `namei -mo` command to list an entire permissions tree. This can make it easier to see what directories need to have permissions adjusted to allow access by the *tableau* group. You can find more information on the internet.
Configure Server Event Notification

A Tableau Services Manager (TSM) administrator can configure Tableau Server to allow notifications for the following events:

- Content updates
  - Extract failures (enabled by default)
  - Subscription views for users (disabled by default)
- Server health monitoring
  - Server status changes (disabled by default)
  - License reporting (disabled by default)
- Drive space
  - Email alerts when space crosses or remains below pre-configured thresholds (disabled by default)
  - Recording usage history (enabled by default)

**Note:** You need to configure SMTP before you can configure subscriptions or notifications. For more information, see Configure SMTP Setup.

Use the TSM web interface

1. Open TSM in a browser:

   https://<tsm-computer-name>:8850.

   For more information, see Sign in to Tableau Services Manager Web UI.

2. Click **Notifications** on the **Configuration** tab and click **Events**.

3. Configure notification settings for your organization:
   - Content updates

     - **Send emails for extract refresh failures**

       When this option is enabled (the default), a server administrator can configure email notifications to be sent when extract refreshes fail. These
messages are configured at the site level, so even if this option is enabled, messages are not sent unless the Send email to data source and workbook owners when scheduled refreshes fail option is enabled for a site (this is enabled by default). For details, see Enable Extract Refresh Scheduling and Failure Notification.

- **Allow users to receive email for views that they have subscribed to**

  When this option is enabled (by default is it disabled), a server administrator can configure a site to send subscription email. These email messages are configured at the site level and can only be configured when this option is enabled. For details, see Set Up a Site for Subscriptions.

  When users subscribe to a workbook or view, a snapshot of the view is emailed to them on a scheduled basis, so they can see the latest updates without having to sign into Tableau Server.

- **Server health monitoring**

  - **Send emails for Tableau Server process events (up, down, and failover)**

    Tableau Server sends an email message when the data engine, repository, or gateway server processes stop or restart, or when the initial Tableau Server node stops or restarts.

    If you are running a single-server installation (all processes on the same computer), health alerts are only sent when Tableau Server is up. No "down" alerts are sent. If you are running a distributed installation that's configured for failover, a DOWN alert means that the active repository or a data engine instance has failed and the subsequent UP alert means that the passive instance (repository) or second instance (data engine) of that process has taken over.
• **Send emails for Tableau Server license reporting**

License reporting is generated at Tableau Desktop and sent to Tableau Server.

• **Drive space**

Enable notifications for remaining drive space on your Tableau Server.

• **Send emails when unused drive space drops below thresholds**

You can configure Tableau Server to send email alerts when disk space usage on any node crosses a threshold, or remains below the threshold. And you can configure how often threshold alerts are sent.

There are two thresholds you must set, **Warning threshold** and **Critical threshold**. Thresholds are expressed in percentage of disk space remaining. The critical threshold must be less than the warning threshold.

You also specify the **Send threshold alert every** option. This determines how often, in minutes, warning and critical alerts should be sent. The default value is 60 minutes.

• **Record disk space usage information and threshold violations for use in custom administrative views**

When you configure Tableau Server to record disk space usage, information about free disk space is saved in the repository and you can view the usage history using the Administrative Views.

4. Click **Save Pending Changes** after you’ve entered your configuration information.

5. Click **Pending Changes** at the top of the page:
6. Click **Apply Changes and Restart**.

**Use the TSM CLI**

The various notification values described above can be set individually with the tsm configuration set command. Alternatively, you can construct a json file and pass all configuration values in one operation. Both methods are described in this section.

Set notification values individually

The following table shows the key/value pairs that map to the notification events described earlier in this topic. Use the tsm configuration set command with the following syntax to set a single key/value pair:

```
tsm configuration set -k <config.key> -v <config_value>
```

For example, to enable job failure notifications, run the following command:

```
tsm configuration set -k backgrounder.notifications_enabled -v true
```

<table>
<thead>
<tr>
<th>Notification option</th>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extract failures or Flow run failures</td>
<td>backgrounder.notifications_enabled</td>
<td>true</td>
</tr>
<tr>
<td>Enable subscription views for user</td>
<td>subscriptions.enabled</td>
<td>true</td>
</tr>
<tr>
<td>Server status changes</td>
<td>svcmonitor.notification.smtp.enabled</td>
<td>true</td>
</tr>
<tr>
<td>License reporting</td>
<td>features.DesktopReporting</td>
<td>true</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Remaining space thresholds: enable email notifications</td>
<td>storage.monitoring.email_enabled</td>
<td>true</td>
</tr>
<tr>
<td>Remaining space thresholds: warning percentage</td>
<td>storage.monitoring.warning_percent</td>
<td>integer value, for example, 20</td>
</tr>
<tr>
<td>Remaining space thresholds: critical percentage</td>
<td>storage.monitoring.critical_percent</td>
<td>integer value, for example, 15</td>
</tr>
<tr>
<td>Set email interval</td>
<td>storage.monitoring.email_interval_min</td>
<td>integer value, in minutes, for example, 25</td>
</tr>
<tr>
<td>Record usage history</td>
<td>storage.monitoring.record_history_enabled</td>
<td>true</td>
</tr>
</tbody>
</table>

After you are done setting values, you must run the following command:

```bash
tsm pending-changes apply
```

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`. 
Set all notification values with a single json file

To make all notifications settings with a single configuration, you can pass a json file.

Copy and edit the following template to create a file for your configuration.

```json
{
  "configKeys": {
    "backgrounder.notifications_enabled": true,
    "subscriptions.enabled": true,
    "svc-monitor.notification.smtp.enabled": true,
    "features.DesktopReporting": true,
    "storage.monitoring.email_enabled": true,
    "storage.monitoring.warning_percent": 20,
    "storage.monitoring.critical_percent": 15,
    "storage.monitoring.email_interval_min": 25,
    "storage.monitoring.record_history_enabled": true
  }
}
```

After you have saved the file, pass it with the following command:

```bash
tsm settings import -f <path-to-file.json>
```

To apply changes, run the following command:

```bash
tsm pending-changes apply
```

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

Configure Data Cache

Views published to Tableau Server are interactive and sometimes have a live connection to a database. As users interact with the views in a web browser, the data that is queried gets stored in a cache. Subsequent visits will pull the data from this cache if it is available. By default, Tableau Server will cache and reuse data for as long as possible. You can change
this behavior by configuring the caching option using the `tsm data-access caching set` command.

1. Log in to TSM:

   `tsm login -u <name>`

2. Run this command:

   `tsm data-access caching set -r <value>`

   Where `<value>` is one of these options:

   - **low or empty string ("")**. This is the default value and indicates that Tableau Server should configure cache and always use cached data when available.
   - `<value>"<value>"` specifies the maximum number of minutes data should be cached.
   - **always** or 0 (zero). These values indicates that Tableau Server should always get the latest data and that the cache should be refreshed each time a page is reloaded.

3. Apply changes with the `tsm pending-changes apply` command. This will restart Tableau Server.

### Database Drivers

Tableau connectors require a driver to talk to the database. Before you can connect to data sources from Tableau Server, you must install drivers for the data sources you want to connect to. You can find information about supported data sources for Tableau Server on Linux on the [Tableau Server tech specs page](https://www.tableau.com/support/linux-admin-technical-specs). You can find driver links and installation instructions for all the supported connectors on the [Driver Download page](https://www.tableau.com/support/linux-driver-download).

**Important**: You must install the PostgreSQL driver if you want to use the built-in administrative views.
Install drivers in a cluster

You need to install the drivers for your data sources on the initial node in a Tableau Server cluster. If you install Tableau Server on multiple nodes, you must also install drivers on any node that runs any of the following processes:

- Application Server (Vizportal)
- Backgrounder
- Data Server
- VizQL Server

Server Crash Reporter

The Tableau Server administrator can enable an option to allow logs and related files to be sent to Tableau when the server has an issue that results in a crash. These files are used by Tableau to identify and address issues that cause crashes. By default this option is disabled, and it should only be enabled in organizations that are not subject to regulations related to data privacy.

**Important:** Do not enable crash reporting if your data is subject to privacy regulations.

If Tableau Server has a problem that results in a crash, log files and dump files are generated. If the crash data upload feature is enabled, these files are automatically gathered and zipped into an encrypted package that is sent in the background, at the scheduled time. The encrypted package is sent in small pieces to limit impact to network performance. Only one crash report is packaged and uploaded at a time (a new crash report is not packaged until the previous package has been uploaded) and is sent in a "first in, first out" order. You can schedule the sending for a low-use window to further reduce any impact to your users.

The encrypted package is made up crash dump files and logs that include the following:

- Crash/core dump files
- Error log files related to the crash
- Manifest files related to the crash

The files can contain data that includes:

- Machine-specific information (for example: hardware, operating system, domain).

- A snapshot of the contents of memory at the time of the crash, including application activity details like information about data connections, actions taken by the user in Tableau, and data being worked on in Tableau.

- Tableau information including customer-identifiable information.

Configure Server Crash Reporter

Server crash reporting is disabled by default. This topic describes how to enable and configure server crash reporting. Crash reports are encrypted and sent to Tableau. See Server Crash Reporter for more information.

**Important:** Do not enable crash reporting if your data is subject to privacy regulations.

Use the TSM web interface

1. Open TSM in a browser:

   https://<tsm-computer-name>:8850. For more information, see Sign in to Tableau Services Manager Web UI.

2. Click the **Maintenance** tab.

3. Under Other Maintenance Tasks, in Server Crash Reporter, select **Enable crash reporting**:
4. Specify the scheduled time of day to upload the crash reports to Tableau.

5. When you are finished, click **Pending Changes**, and then click **Apply Changes and Restart**.

Use the TSM CLI

Use the configuration file template below to create a json file. After you have filled in the options with the appropriate values, pass the json file and apply settings with the following commands:

```bash
tsm settings import -f path-to-file.json
tsm pending-changes apply
```

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

Because the configuration file is using configKey class, the values that you pass are not validated by TSM as they are when you use configEntities class. You can verify and set individual options by using the tsm configuration commands.
Crash reporter settings

The crash reporter settings in the template below specify a range of options for configuring Tableau Server to send crash reports to Tableau.

Configuration template

Use this template to configure the gateway settings.

For more explanation about configuration files, entities, and keys see Configuration File Example.

```json
{
    "configKeys": {
        "servercrashupload.enabled": "true",
        "servercrashupload.scheduled_time": "1:00:00 UTC",
        "servercrashupload.proxy_server_host": "",
        "servercrashupload.proxy_server_port": "",
        "servercrashupload.proxy_server_username": "",
        "servercrashupload.proxy_server_password": "",
        "servercrashupload.preserve_upload_packages": "false",
        "servercrashupload.delete_completed_dumps": "false"
    }
}
```

Configuration file reference

This table includes keys that you can set to configure crash reporting.

servercrashupload.enabled

Default: false.

Set to true to enable crash reporting.

servercrashupload.scheduled_time

Default: 1:00:00 UTC
Specifies the scheduled time that crash uploads will begin. Enter time of day in 24 hour format.

**servercrashupload.proxy_server_host**

If your organization uses a proxy server to communicate with the internet, specify the host name.

**servercrashupload.proxy_server_port**

If your organization uses a proxy server to communicate with the internet, specify the port number.

**servercrashupload.proxy_server_username**

If your proxy server requires authentication, specify the user name with this key.

**servercrashupload.proxy_server_password**

If your proxy server requires authentication, specify the password with this key.

**servercrashupload.preserve_upload_packages**

Default: false.

To save all packages that are created for a crash reporting, set this key to true.

By default, packages are saved to /var/opt/tableau/tableau_server-/data/tabsvc/clustercontroller/tabcrashreporter.

**servercrashupload.delete_completed_dumps**

Default: false.

To delete all dumps after they are sent, set this key to true.
Navigate the Admin Areas of the Tableau Web Environment

As an administrator on Tableau Server or Tableau Online, you can access admin settings that aren’t available to other users to configure sites, users, projects, and to do other content-related tasks.

The settings in this article refer to the Tableau web environment. Tableau Server administrators with appropriate credentials can also change server settings such as processor, caching, authentication, distributed deployment, and related configurations using the TSM web environment. For information, see Sign in to Tableau Services Manager Web UI.

Access based on site role and number of sites

The menus you get when you sign in to Tableau Server or Tableau Online depend on the following conditions:

- Whether you’re a site or server administrator.

  Site administrator access is available on Tableau Online and Tableau Server. Server administrator access is only on Tableau Server.

- Whether you have access to only one site or to multiple sites.

Server administrator

In a multi-site environment, menus at the top enable you to modify a specific site or all sites, and to configure users, groups, schedules, tasks, and server settings.

On a single-site server, the site selector does not appear, and all other menus are the same.

To access server administrator settings that affect all sites, open the site menu, and then select Manage All Sites.
To return to the site administration menus, select All Sites, and then select the site you want to manage.

Site administrator

If you are a site administrator for Tableau Online or Tableau Server, and you have access to multiple sites, you’ll get menus for selecting which site to manage, and for managing that site’s content, users, groups, schedules, and tasks, and for monitoring its status.

The site selector displays the name of the current site. To go to another site, select the site menu, and then select the site name.
If you have access to only one site, the site selector does not appear, but all other menus are the same.

Server administrator tasks

Server administrators (available with Tableau Server Enterprise only) can do the following:

- Monitor server status and activity.
- Generate log files.
- Add sites and edit site settings. Only server administrators can add sites to the server.
- Add users to the server, and assign users to sites.
- Add and manage site groups.

To manage settings only for a specific site, you must first navigate to the site. Within each site, you can do the following:

- Administer content: Create projects, move content from one project to another, assign permissions, change ownership of a content resource, and so on.
- Manage schedules for extract refreshes and subscriptions.
- Monitor site activity and record workbook performance metrics.
- Manage storage space limits for content published by users.
- Allow web authoring.
- Enable revision history.
- Allow site administrators to add and remove users.
- Allow users to subscribe to workbooks and views, and allow content owners to subscribe others to workbooks and views.
- Enable offline snapshots for favorites (iOS only).
Site administrator tasks

A site administrator on Tableau Online or Tableau Server can do the following tasks:

- Administer content: Create projects, move content from one project to another, assign permissions, change ownership of a content resource, and so on.
- View, manage, and manually run schedules for extract refreshes and subscriptions.
- Add and manage site users (if allowed by the server administrator; see Add or Update Sites).
- Add and manage site groups.
- Monitor site activity.

Migrate to New Hardware

Use the following procedure to migrate Tableau Server from one computer to another. You might do this if you are upgrading the computer hardware that Tableau is running on.

Specifically, these steps describe how to move Tableau Server data from your in-production computer to a new computer where Tableau Server is installed. Before you start, make sure you have followed the steps in Prepare for the Upgrade, including creating a backup and gathering any assets that require manual actions. For details, see Perform a Full Backup and Restore of Tableau Server. You'll need these to restore your Tableau Server data and configuration.

**Note:** This operation includes steps that you may need to perform using the TSM command line.

1. Deactivate your product key on your original installation of Tableau Server. You need to do this so you can activate it on the new computer. For more information, see "Tableau Server product key activation" below.
2. Install Tableau Server on the new computer. For details, see Install and Initialize TSM.

3. Copy your backup file `.tsbak` to the folder location specified by the `base-filepath.backuprestore` variable. By default this is: `/var/-opt/tableau/tableau_server/data/tabsvc/files/backups`.

**Note:** You can change the location for the backup file. For more information, see tsm File Paths.

4. Next, stop Tableau Server:

   ```
   tsm stop
   ```

5. Restore your in-production data to your new Tableau Server installation using the `tsm maintenance restore` command:

   ```
   tsm maintenance restore -f <filename>
   ```

   where `<filename>` is the name of the `.tsbak` file you copied in step 3.

   For more information about restoring Tableau Server data, see Restore from a backup.

6. Start the server:

   ```
   tsm start
   ```

7. **Distributed installations only:** Install Tableau Server on the new computers you want to add to your new Tableau Server cluster. See Install and Configure Additional Nodes for steps.

8. If you have not deactivated your product key on the old computer, do that after you test your new Tableau Server installation and confirm that it’s ready for production.
For details, see "Tableau Server product key activation" below.

**Note:** If you do not have an internet connection, you are prompted to create an off-line activation file to complete the deactivation process. See Activate Tableau Server Offline - Adding a License for steps.

### Tableau Server product key activation

You can activate the same Tableau Server product key up to three times. This allows you to test Tableau Server (in a sandbox or QA environments, for example), as well as use Tableau in production. To maximize your activations, you should deactivate your product key when you remove Tableau Server from a computer, unless you will be reinstalling Tableau on the same computer. Doing this gives you the opportunity to use the activation on a different computer. For example, if you move Tableau Server from one computer to another, deactivate the product key, then remove Tableau from the original computer. When you install Tableau on the new computer, you can activate the key there without any conflict. If you are removing Tableau Server to reinstall it on the same computer, you don’t need to deactivate the key. Tableau will use the key when reinstalled. For example, if you are moving Tableau from one drive on a computer to a different drive on the same computer. For information on how to deactivate a product key, see tsm licenses deactivate.

### Enable and Configure Tableau Prep Conductor on Tableau Server

Tableau Prep Conductor is supported only on Tableau Server versions 2019.1 or later.

Tableau Prep Conductor is licensed through the Data Management Add-on, on a per Deployment basis, which is may be User-Based or Core-Based. A Deployment includes a licensed production Tableau Server installation and licensed non-production Tableau Server installations that support the production installation. For more information on Deployment, see the [EULA Documentation](#).
Who can do this?

Server administrators can install Tableau Server and enable Tableau Prep Conductor.

Server-level settings can be configured by Tableau Server administrators, and site-level settings can be configured by Tableau Server and Site administrators.

Server Topology

When you install Tableau Server and enable Tableau Prep Conductor, using the Data Management product key, Tableau Prep Conductor is automatically enabled by default by the setup program.

For multi-node installations, by default, one instance of Tableau Prep Conductor is enabled on any node that has backgrounder installed. In the example below, Tableau Prep Conductor is enabled on node 2 and 3 where the backgrounders are also enabled, but not on node 1, 4, and 5.
The topics in this section will walk you through the process of the steps you need to take to enable and configure Tableau Prep Conductor.

Below is a visual representation of that work-flow:
Next step:

New Tableau Server Installations: Step 1 (New Install): Install Tableau Server with Tableau Prep Conductor

Existing Tableau Server Installations: Step 1 (Existing Install): Enable Tableau Prep Conductor

Step 1 (New Install): Install Tableau Server with Tableau Prep Conductor

This topic describes how to Tableau Prep conductor on a new installation of Tableau Server.

Tableau Prep Conductor is supported only on Tableau Server versions 2019.1 or later.
Tableau Prep Conductor is licensed through the Data Management Add-on, on a per Deployment basis, which is may be User-Based or Core-Based. A Deployment includes a licensed production Tableau Server installation and licensed non-production Tableau Server installations that support the production installation. For more information on Deployment, see the EULA Documentation.

Who can do this?

Server administrators can install Tableau Server and enable Tableau Prep Conductor.

Before you install

The recommended topology for a production Tableau Server installation is a dedicated node for running flows. If you currently have a single node Tableau Server installation it is recommend that you add a second node and dedicate it to run flows.

- Review the hardware recommendations for Tableau Server and Tableau Prep conductor.
  - Minimum Hardware Requirements and Recommendations for Tableau Server installation on Windows.
  - Minimum Hardware Requirements and Recommendations for Tableau Server installation on Linux.

Install Tableau Server and enable Tableau Prep Conductor

Windows:

Use the instructions provided in the Install Tableau Server topic to install Tableau Server. When you get to the Activate step, use the product keys to activate Tableau Server, and enable Tableau Prep Conductor. The Data Management product key specifically enables Tableau Prep Conductor. All product keys are available through the Customer Portal.

Linux:
Use the instructions provided in the Install Tableau Server topic to install Tableau Server. When you get to the Activate step, use the product keys to activate Tableau Server, and enable Tableau Prep Conductor. The Data Management product key specifically enables Tableau Prep Conductor. All product keys are available through the Customer Portal.

Configure public gateway settings

If your Tableau Server is set up with one of the following:

- Load balancer to distribute requests across gateways.
- Reverse proxy to authenticate external (internet) client requests and offloading SSL-based encryption.

You must configure the following public gateway settings:

$ tsm configuration set -k gateway.public.host -v <name> (This should be the url that your users are using to access Tableau Server)

$ tsm configuration set -k gateway.public.port -v 443

For more information on configuring gateway settings, see Configuring Proxies for Tableau Server.

Verify Tableau Prep Conductor is enabled and running

When you activate the Data Management product key, a single instance of Tableau Prep Conductor is automatically enabled on any node that has Backgrounder enabled.

**Use the following steps to verify that it is enabled and running:**

1. Open a browser and enter the Tableau Server URL, and append the dedicated TSM web UI port. Here are some examples of what the URL might look like:

   https://localhost:8850/ (if you're working directly on the server computer)

   https://MarketingServer:8850/ (if you know the server's name)

   https://10.0.0.2:8850/ (if you know the server's IP address)
In the sign-in page that appears, enter your administrator user name and password.

**Note:** Tableau Server creates and configures a self-signed certificate during the installation process. This certificate is used to encrypt traffic to the TSM Web UI. Because it's a self-signed certificate, your browser will not trust it by default. Therefore, your browser will display a warning about the trustworthiness of the certificate before allowing you to connect.

2. In the Tableau Services Manager web interface, click the **Status** tab to see the status.

- If Tableau Prep Conductor is enabled and running, you should see Tableau Prep Conductor in the list of processes and show as **Active** on at least one node. If Tableau Prep Conductor is not enabled, you will see Tableau Prep Conductor in the list of process, but with no status information for any of the nodes.

**Tableau Prep Conductor not enabled:**
Tableau Prep Conductor enabled and running. In the image below, Tableau Prep Conductor is enabled on node1 and node3:

Dedicate a node for Tableau Prep Conductor

On the node you are planning to dedicate to running flows, enable Backgrounder process if it is not already enabled. It is recommended that you do not run other processes like VizQL server on this node.

Since you are dedicating this node to running flows, you must change configure Backgrounder to run only flow tasks. By default, the Backgrounder process runs tasks of all types, including flows, extract refreshes, and subscriptions. For more information, see Node Roles in Tableau Server.

Run the following tsm commands on that dedicated node to run only flow tasks:
Tableau Server on Linux Administrator Guide

1. Run the following command to allow Backgrounders on this node to run only flow tasks.

   tsm topology set-node-role -n node1 -r flows

2. Apply the changes and restart Tableau Server:

   tsm pending-changes apply

If you have more than 2 nodes in your Tableau Server installation, you can choose to configure other nodes to run all tasks other than flows:

1. Restrict a node to not allow flows. This command removes Tableau Prep Conductor from this node and Backgrounders on this node will not run flow tasks.

   tsm topology set-node-role -n node1 -r no-flows

2. Apply the changes and restart Tableau Server:

   tsm pending-changes apply

Next step

Step 2 - Configure Flow Settings for your Tableau Server

Step 1 (Existing Install): Enable Tableau Prep Conductor

This topic describes how to enable Tableau Prep conductor on your existing installation of Tableau Server.

Tableau Prep Conductor is supported only on Tableau Server versions 2019.1 or later. If you are using Tableau Server 2018.3 or earlier, you must first upgrade your Tableau Server to 2019.1 before enabling Tableau Prep Conductor on your Tableau Server installation.

Tableau Prep Conductor is licensed through the Data Management Add-on, on a per Deployment basis, which is may be User-Based or Core-Based. A Deployment includes a licensed production Tableau Server installation and licensed non-production Tableau Server
installations that support the production installation. For more information on Deployment, see the EULA Documentation.

This topic describes how to enable Tableau Prep conductor on your existing installation of Tableau Server.

Who can do this?

Tableau Server Administrators can install or upgrade Tableau Server, and enable Tableau Prep Conductor on Tableau Server.

Before you upgrade

Prepare for upgrade:

- Know before you upgrade
- Licensing Tableau Prep Conductor
- Tableau Server Hardware Requirements and Recommendations

Configure public gateway settings

If your Tableau Server is set up with one of the following:

- Load balancer to distribute requests across gateways.
- Reverse proxy to authenticate external (internet) client requests and offloading SSL-based encryption.

You must configure the following public gateway settings:

```
tsm configuration set -k gateway.public.host -v <name> (This should be the url that your users are using to access Tableau Server)
```

```
tsm configuration set -k gateway.public.port -v 443
```

For more information on configuring gateway settings, see Configuring Proxies for Tableau Server.
Tableau Server on Linux Administrator Guide

Tableau Server Installations using User-Based licenses

The recommended topology for a production Tableau Server installation is a dedicated node for running flows. For more information, see Minimum Hardware Requirements and Recommendations for Tableau Server.

Tableau Server single-node installations

If you currently have a single node Tableau Server installation, it is recommended that you add a second node and dedicate it to running flows.

1. Run upgrade on your current Tableau Server installation using the information in the topics below:
   - Windows
   - Linux

2. Activate the Data Management product key. This will enable Tableau Prep Conductor on your node. The Data Management product key, like your other server keys, are available through the Customer Portal.
   - In the Tableau Services Manager web interface, click Licensing on the Configuration tab and click Activate License.
   - Enter or paste your new product key and click Activate.
   - On the Register page, enter your information into the fields and click Register.

3. You will be prompted to restart the server. Restart the server and verify that Tableau Prep Conductor is enabled and running.
   - In the Tableau Services Manager web interface, click the Status tab to see the status. If Tableau Prep Conductor is enabled and running, you should see Tableau Prep Conductor in the list of processes and show as Active. If Tableau Prep Conductor is not enabled, you will see Tableau Prep Conductor in the list
of process, but with no status information.

**Tableau Prep Conductor not enabled:**

![Tableau Prep Conductor not enabled](image1)

**Tableau Prep Conductor enabled and running:**

![Tableau Prep Conductor enabled and running](image2)

4. Add a second node to your Tableau Server installation. The installer will enable certain required processes like the Cluster Controller. Enable Backgrounder process on it as it is required to run scheduled flow tasks. When you enable the Backgrounder process, the installer automatically enables a single instance of Data Engine on the node. Do not add any other processes on this node.

5. Run the following commands to dedicate this node to do only flow tasks. This will
enable Tableau Prep Conductor on your new node. For more information on node roles, see Node Roles in Tableau Server.

- Get the nodeID for your dedicated node to see the list of services on each node:
  
  tsm topology list-nodes -v.

- Set the node role for the dedicated node using the nodeID that you got from running the command described above:
  
  tsm topology set-node-role -n <nodeID> -r flows.

- Apply the changes, and restart the server:
  
  tsm pending-changes apply.

- Review the status to ensure that all the processes are up and running and configured correctly:
  
  tsm status -v.

You have successfully added Tableau Prep Conductor to your Tableau Server installation.

Tableau Server multi-node installations

1. Run upgrade on your current Tableau Server Installation using the information in the topics below:

   - Windows

   - Linux

2. Activate the Data Management product key. This will enable Tableau Prep Conductor on the nodes where you already have the Backgrounder process enabled. The Data Management product key, like your other server keys, are available through the Customer Portal.
In the Tableau Services Manager web interface, click **Licensing** on the **Configuration** tab and click **Activate License**.

- Enter or paste your new product key and click **Activate**.

- On the **Register** page, enter your information into the fields and click **Register**.

3. You will be prompted to restart the server. Restart the server and verify that Tableau Prep Conductor is enabled and is running.

- In the Tableau Services Manager web interface, click the **Status** tab to see the status of all the processes. If Tableau Prep Conductor is enabled and running, you should see Tableau Prep Conductor in the list of processes and show as **Active**. If Tableau Prep Conductor is not enabled, you will see Tableau Prep Conductor in the list of processes, but with no status information.

**Tableau Prep Conductor not enabled:**

![Tableau Services Manager Status page](image)
4. Add a new node to your Tableau Server installation. The installer will enable certain required processes like the Cluster Controller. Enable Backgrounder process on it as it is required to run scheduled flow tasks. When you enable the Backgrounder process, the installer automatically enables a single instance of Data Engine on the node. Do not add any other processes on this node.

**Note:** The dedicated note counts towards to total count of the Coordination Service ensemble. You may need to deploy a Coordination Service on the new node depending on the total number of nodes you have in your cluster including the new dedicated node. For more information, see [Deploy a Coordination Service Ensemble](#).

5. Run the following command to dedicate this node to only doing flow related
operations. This will enable Tableau Prep Conductor on your new node. For more information on node roles, see Node Roles in Tableau Server.

- Get the nodeID for your dedicated node to see the list of services on each node:
  - `tsm topology list-nodes -v`.
- Set the node role for the dedicated node using the nodeID that you got from running the command described above:
  - `tsm topology set-node-role -n <nodeID> -r flows`.
- Apply the changes and restart the server:
  - `tsm pending-changes apply`.
- Review the status to ensure that all the processes are up and running and configured correctly:
  - `tsm status -v`.

6. At this stage, you may have Tableau Prep Conductor enabled on other nodes. By default, the Backgrounder process on a node performs all tasks of all types including flow tasks. To isolate Tableau Prep Conductor and flow tasks to only certain nodes, you can configure the Backgrounders to do one of the following:

- **To run only flow tasks**: `tsm topology set-node-role -n <nodeID> -r flows`.
- **To run all other tasks except flows**: `tsm topology set-node-role -n <nodeID> -r no-flows`.

You have successfully added Tableau Prep Conductor to your Tableau Server installation.

Tableau Server Installations using Core-Based licenses

The recommended topology for a production Tableau Server installation is a dedicated node for running flows. For more information, see Minimum Hardware Requirements and Recommendations for Tableau Server.

The Data Management Add-on for Core-Based licenses includes two product keys: Data Management product key which enables Tableau Prep Conductor, and Resource Core product key that comes in units of four. The resource key should be applied to the node ded-
Tableau Server on Linux Administrator Guide

icated to running the flows. These product keys, like your other server keys, are available through the Customer Portal.

Tableau Server single-node installations

If you currently have a single node Tableau Server installation, it is recommended that you add a second node and dedicate it to running flows.

1. Run upgrade on your current Tableau Server Installation using the information in the topics below:
   - Windows
   - Linux

2. Activate the product keys. This will enable Tableau Prep Conductor on the nodes where you already have the Backgrounder process enabled.
   - In the Tableau Services Manager web interface, click Licensing on the Configuration tab and click Activate License.
   - Enter or paste your new product key and click Activate.
   - On the Register page, enter your information into the fields and click Register.

3. You will be prompted to restart the server. Restart the server and verify that Tableau Prep Conductor is enabled and is running.
   - In the Tableau Services Manager web interface, click the Status tab to see the status. If Tableau Prep Conductor is enabled and running, you should see Tableau Prep Conductor in the list of processes and show as Active. If Tableau Prep Conductor is not enabled, you will see Tableau Prep Conductor in the list of process, but with no status information.

Tableau Prep Conductor not enabled:
4. Add a second node to your Tableau Server installation. The installer will enable certain required processes like the Cluster Controller. Enable Backgrounder process on it as it is required to run scheduled flow tasks. When you enable the Backgrounder process, the installer automatically enables a single instance of Data Engine on the node. Do not add any other processes on this node.
Important: The number of physical cores on this machine must be equal to, or less than the Resource Core units you purchased. For example, if you purchased four units, your node can have up to four physical cores.

5. Run the following commands to dedicate this node to only doing flow tasks. This will enable Tableau Prep Conductor on your new node. For more information on node roles, see Node Roles in Tableau Server.

   - Get the nodeID for your dedicated node to see the list of services on each node:

     \[\text{tsm\ topology\ list-nodes\ -v}\.\]

   - Set the node role for the dedicated node using the nodeID that you got from running the command described above:

     \[\text{tsm\ topology\ set-node-role\ -n\ <nodeID>\ -r\ flows}\.\]

   - Apply the changes and restart the server: \text{tsm\ pending-changes\ apply}\.

   - Review the status to ensure that all the processes are up and running and configured correctly:

     \[\text{tsm\ status\ -v}\.\]

You have successfully added Tableau Prep Conductor to your Tableau Server installation.

Tableau Server multi-node installations

1. Run upgrade on your current Tableau Server installation using the information in the topics below:

   - Windows

   - Linux

2. Activate the product keys. This will enable Tableau Prep Conductor on the nodes where you already have the Backgrounder process enabled.
In the Tableau Services Manager web interface, click **Licensing** on the **Configuration** tab and click **Activate License**.

- Enter or paste your new product key and click **Activate**.
- On the **Register** page, enter your information into the fields and click **Register**.

3. You will be prompted to restart the server. Restart the server and verify that Tableau Prep Conductor is enabled and is running.

- In the Tableau Services Manager web interface, click the **Status** tab to see the status. If Tableau Prep Conductor is enabled and running, you should see Tableau Prep Conductor in the list of processes and show as **Active**. If Tableau Prep Conductor is not enabled, you will see Tableau Prep Conductor in the list of process, but with no status information.

**Tableau Prep Conductor not enabled:**

![Tableau Prep Conductor status](image)
4. Add a new node to your Tableau Server installation. A dedicated node to run flow related operations is recommended for production Tableau Server installations. The installer will enable certain required processes like the Cluster Controller. Enable Backgrounder process on it as it is required to run scheduled flow tasks. When you enable the Backgrounder process, the installer automatically enables a single instance of Data Engine on the node. Do not add any other processes on this node.

**Note:** The dedicated note counts towards to total count of the Coordination Service ensemble. You may need to deploy a Coordination Service on the new node depending on the total number of nodes you have in your cluster including the new dedicated node. For more information, see [Deploy a Coordination Service Ensemble](#).
Important:
The number of physical cores on this machine must be equal to, or less than the Resource Core units you purchased. For example, if you purchased four units, your node can have up to four physical cores.

5. Run the following commands to dedicate this node to only doing flow tasks. This will enable Tableau Prep Conductor on your new node. For more information, see Node Roles in Tableau Server.

   - Get the nodeID for your dedicated node to see the list of services on each node:
     
     tsm topology list-nodes -v.

   - Set the node role for the dedicated node using the nodeID that you got from running the command described above:
     
     tsm topology set-node-role -n nodeID -r flows.

   - Apply the changes and restart the server:
     
     tsm pending-changes apply.

   - Review the status to ensure that all the processes are up and running and configured correctly:
     
     tsm status -v.

6. At this stage, you may have Tableau Prep Conductor enabled on other nodes that have the Backgrounder process. By default, the Backgrounder process on a node performs all tasks of all types including flow tasks. To isolate Tableau Prep Conductor and flow operations to only certain nodes, you can configure the backgrounders to do one of the following:
To run only flow tasks:

```
  tsm topology set-node-role -n <nodeID> -r flows.
```

To run all other tasks except flows:

```
  tsm topology set-node-role -n <nodeID> -r no-flows.
```

Next step

Step 2 - Configure Flow Settings for your Tableau Server.

Step 2 - Configure Flow Settings for your Tableau Server

This topic described the various flow settings that you can configure for your Tableau Server.

Who can do this?

Tableau Server Administrators can configure server and site level settings. Tableau Site Administrator can configure site level settings.

Publishing, Scheduling, and Credential Settings

When you activate Tableau Prep Conductor using the Data Management product key, Tableau Prep Conductor is enabled for the entire Tableau Server installation. You can further modify and customize the setting for sites.

Use the following instructions to configure settings related to flows for all your sites or for individual sites:

Use the following instructions to sign in to Tableau Server Admin pages:

- Windows: Tableau Server Admin Pages.
- Linux: Tableau Server Admin Pages.

Configure whether publishing and scheduling flow should be allowed for a site:
1. **Enable users to publish and schedule flows:** This setting is enabled by default when you enable Tableau Prep Conductor. If you have multiple sites, you can selectively turn off Tableau Prep for Server for individual sites. If you disable this setting for a site that once allowed flows, see Implication of disabling Tableau Prep Conductor section later in this topic to learn more.

On the **General** page under **Settings**, scroll to the **Flows** setting and clear the **Allow user to publish and schedule flows** check box to turn off Tableau Server for the site.

2. **Embed Credentials**

   - **Allow publishers to embed credentials in a data source, flow or workbook:** This setting allows publishers to attach passwords to published flows that will automatically authenticate web users.
- Allow publishers to schedule flow runs and data extract refreshes: This option is only available if setting above is enabled. When this setting is enabled, publishers will see scheduling options in the Publish dialog box.

Implication of disabling Tableau Prep Conductor

If you disable Tableau Prep Conductor after using it for a while, you will not be able to see the flows, schedules, task, and other things related to flows. The following table gives you more information on what you can and cannot see when you disable Tableau Prep for Server completely or only for specific sites:

<table>
<thead>
<tr>
<th></th>
<th>Prep not enabled at Server level</th>
<th>Prep enabled at Server level, but disabled for a site</th>
<th>Prep enabled for both Server and site</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show flows</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Show tasks/schedules in Server view</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Show tasks/schedules in Site view</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Show Site setting (only for Server Admins)</td>
<td>Yes (disabled)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Show TSM status</td>
<td>Yes (Tableau Prep Conductor is not shown)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Show TSM settings</td>
<td>Yes (disabled)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Important: Scheduled tasks will continue to run even when Tableau Prep Conductor is disabled for that site, but will fail.
Configure notifications for flow failures

You can configure Tableau Server to send email notifications for flow run failures. The notifications are sent for failures that occur when running the flows through either a scheduled task or a manual run using Run now menu option. You must first enable the server-wide setting, and then configure at the site-level.

To enable the server-wide email notification

You can either use the Tableau Services Manager (TSM) web interface or TSM CLI as described below:

Use the TSM web interface

1. Open TSM in a browser:

   https://<tsm-computer-name>:8850.

2. Click Notifications on the Configuration tab and click Email Server.

3. Enter the email server information.

4. Click the Events tab.

5. Under Content Updates, select Send emails for extract refresh failures and flow run failures if not already turned on by default.

6. Click Save Pending Changes after you've entered your configuration information.

7. Click Apply Changes and Restart.

Use the TSM CLI

The notification values can be set individually with tsm configuration set command:
Windows: tsm configuration.

Linux: tsm configuration.

Set notification values

Use the tsm configuration set command with the following syntax to

to enable flow failure notifications, run the following command:

```
tsm configuration set -k backgrounder.notifications_enabled -v true
```

**Note:** This will enable email notification for both extract refresh failures and flow failures.

After you are done setting values, you must run the following command:

```
tsm pending-changes apply
```

The pending-changes apply command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in the case there is no restart. You can suppress the prompt using the --ignore-prompt option, but this does not change the restart behavior.

To configure email notification for a site:

On the **General** page under **Settings**, scroll to the **Flow Run and Refresh Failure Notifications** setting and clear the **Send email to data source, flow, and workbook, when flow runs and scheduled refreshes fail** check box to turn off refresh failure and flow run notifications.
Next step

Step 3- Create Schedules for Flow Tasks

Who can do this?

Tableau Server Administrators can create and modify schedules. Schedules are created at the server level and apply across all the sites on a server.
Create a new schedule:

1. On the Schedules tab, click New Schedule.

2. Enter the following information in the New Schedule dialog box and click Create.

   - **Name:** Enter a descriptive name for the schedule. Typically, this includes the description of the schedule frequency.

   - **Task Type:** Select Flow as the task type.

   - **Default Priority:** You can define a default priority from 1 to 100, where 1 is the highest priority. This value will be assigned to the tasks by default. If two tasks are pending in the queue, the one with the higher priority runs first.

   - **Execution:** Choose whether a schedule will run in parallel or serially. Schedules that run in parallel run on all available backgrounder processes so that they can complete faster.
**Frequency:** You can define an hourly, daily, weekly, or monthly schedule.

Next step

Step 4 - Safe list Input and Output locations

**Step 4 - Safe list Input and Output locations**

This topic describes the rules that apply to this feature and how to safe list the directories on your network.

Flow input and output connections may need to connect to databases or files in the directories on your network. You must safe list the directories you want to allow access to. Input and Output connections will only be allowed to connect to data in the safe listed locations. By default, no connections are allowed. You can still publish the flows and any data that is embedded in the flow file (tflx) to Tableau Server.
Who can do this?

Tableau Server Administrators who also are a member of the `tsadmin` group can configure settings using `tsm` commands.

How to safelist input and output locations

The following rules apply and must be considered when configuring this setting:

- The directory paths should be accessible by Tableau Server. These paths are verified during server startup and at flow run time and is **not** verified at the time of publishing the flow to Tableau Server.

- Network directory paths have to be absolute and cannot contain wildcards or other path traversing symbols. For example, `\\myhost\myShare*` or `\\myhost\myShare*` are invalid paths and would result in all the paths as disallowed. The correct way to safelist any folder under `myShare` would be `\\myhost\myShare`, `\\myhost\myShare\`, or `\\myhost\myShare\myShare`.

  **Note:** The `\\myhost\myShare` configuration will not allow `\\myhost\myShare1`. In order to safelist both of these folders safelist them as `\\myhost\myShare`; `\\myhost\myShare1`.

- **Windows:**

  - The value can be either `*`, to allow any network directory, or a specified list of network directory paths, delimited by a semicolon (`;`). If the path contains spaces or special characters you will have to either use single or double quotes. Whether you use single or double quotes depends on the shell that you are using.

  - No local directory paths are allowed even when the value is set to `*`.

- **Linux:**
The value can be either * meaning that any path, including local (with the exception of some system paths configured using "native_api.internal_disallowed_paths"), or a list of paths, delimited by a semicolon (;).

You must be using a kernel version of equal to or later than 4.7. Safe listing is not supported on kernel version earlier than 4.7. To check the kernel version, in the Linux terminal, type the command `uname -r`. This will display the full version of the kernel you are running on the Linux machine.

**Note:** If a path is both on the flows allowed list and internal_disallowed list, **internal_disallowed** takes precedence.

Use the following commands to create a list of allowed network directory paths:

**For input connections:**

```bash
tsm configuration set -k maestro.input.allowed_paths -v your_networkdirectory_path_1;your_networkdirectory_path_2

tsm pending-changes apply
```

**For output connections:**

```bash
tsm configuration set -k maestro.output.allowed_paths -v your_networkdirectory_path_1;your_networkdirectory_path_2

tsm pending-changes apply
```

**Important:**
These commands overwrite existing information and replace it with the new information you provided. If you want to add a new location to an existing list, you must provide a list of all the locations, existing, and the new one you want to add. Use the following commands to see the current list of input and output locations:

```bash
tsm configuration get -k maestro.input.allowed_paths

tsm configuration get -k maestro.output.allowed_paths
```
Step 5 - Optional Server Configurations

The options described in this topic are not required to enable flow publishing and scheduling flows on Tableau Server. They can be used to customizing your environment according to your requirements.

Who can do this?

Tableau Server administrators can make changes to server configurations.

Set the timeout period for flows

You can set time limits for how long a flow can run to make sure that subsequent tasks are not held up due to stalled tasks. The following two tsm command options determine how long a flow task can run before the flow background task is canceled. These two commands together determine the total timeout value for flow tasks.

Use the following tsm commands to change the default timeout period of 4 and half hours:

```
backgrounder.extra_timeout_in_seconds
```

(Default value: 14400 seconds or 4 hours)

```
backgrounder.default_timeout.run_flow
```

(Default value: 1800 seconds or 30 minutes)

Set the threshold for suspended flow tasks

By default, a subscription is suspended after 5 consecutive flow tasks failures. To change the threshold number of flow task failures that can occur before they are suspended, use the following tsm configuration set command:
tsm configuration set -k backgrounder.flow_failure_threshold_for_run_prevention -v <number>

This sets the threshold for the number of consecutive failed flow tasks necessary before suspending the tasks. This is a server-wide setting.

Distributed and High Availability Tableau Server Installations

The most basic way to run Tableau Server is to install a single node. With this type of installation you have a fully functional Tableau Server, with all Tableau Services Manager (TSM) and Tableau Server processes running on that single node, but this may not be the optimal way to use Tableau Server. You can decide how to install Tableau based on your organization's needs, and your resources, adding additional nodes and configuring Tableau for high availability. Your installation options include:

- **Single-node installation**—This type of installation is reasonable for testing, running trials, and for environments that can handle occasional downtime and system availability due to lack of redundancy. All server processes are running on a single machine. There is less redundancy and fewer safeguards in the event of a problem with one of the server processes. You also need to make sure the computer you install Tableau Server on has adequate resources to handle the processes and the demands of users and data.

- **Distributed installation**—This type of installation is also called a multi-node installation and requires multiple computers so you can install and run server processes on those distributed nodes. Spreading the server processes out over multiple nodes can extend the reliability and efficiency of Tableau Server by providing redundancy and additional computing power. With the right configuration, a distributed installation can also provide you with automatic repository failover. For more information on failover, see Repository Failover.

- **Highly available (HA) installation**—An HA installation of Tableau Server is a
special type of multi-node installation with a minimum of three nodes and multiple instances of key processes (the Repository, File Store/Data Engine (Hyper), and Coordination Service) on different computers. With an HA installation, there is built-in redundancy of those key processes, including multiple File Stores, and automatic Repository failover. The goal is to minimize system downtime by eliminating single points of failure, and enabling detection of failures with failover where possible.

The first computer you install Tableau on, the "initial node," has some unique characteristics. Two processes run only on the initial node and cannot be moved to any other node except in a failure situation, the License service (License Manager) and TSM Controller (Administration Controller). Tableau Server includes a script that automates moving these two processes to one of your other existing nodes so you can get complete access back to TSM and keep Tableau Server running.

Two other processes are initially included on the initial node but can be added or moved to additional nodes, the CFS (Client File Service) and the Coordination Service. Depending on how your installation was configured with CFS and Coordination Service, you may also need to take steps to redeploy these.

For information about moving the License service and TSM Controller from the initial node to another node, see Recover from an initial node failure below.

Prerequisite

These instructions assume that your cluster meets the Distributed Requirements.

**Note:** All nodes in a multi-node cluster must have the same type of operating system. You cannot install a multi-node instance of Tableau Server on a combination of Linux and Windows nodes.
Licensing

You must have a valid Tableau Server product key. The type of license you have may determine how many nodes you can install Tableau on. You cannot use a trial license key for a distributed Tableau Server installation. For more information on licensing, see Licensing Overview.

Creating a distributed Tableau Server installation

These are the general steps you follow to create a distributed installation of Tableau Server:

1. Begin by installing Tableau Server on your initial node.
   For details, see Install and Configure Tableau Server.

2. Generate a node configuration (bootstrap) file on the initial node.
   For details, see Generate the node bootstrap file.

3. Install Tableau Server on an additional node using the node bootstrap file.
   For more information, see Install and initialize an additional node.

4. Configure your additional node with the processes you want to run on it.
   For more information, see Configure the additional node.

5. Repeat Steps 3 and 4 for any additional nodes you want to install.

6. Deploy a new Coordination Service ensemble.
   For more information, see Deploy a Coordination Service Ensemble.

Creating a highly available (HA) Tableau Server installation

A high availability Tableau Server installation is a special type of distributed installation, designed to accommodate failure in key server components without loss of complete server
To create an HA installation, follow the same steps you take to create a distributed deployment but include additional steps to make the deployment highly available. These additional steps include adding at least two additional nodes (for a minimum of three nodes in the cluster), adding a second instance of the repository, and second instances of the data engine/file store, adding additional gateway processes, and deploying a Coordination Service ensemble. You can also add a load balancer to distribute requests among the gateways.

At a high level, these are the steps you follow to create a highly available installation of Tableau Server:

1. Begin by installing Tableau Server on your initial node.
   
   For details, see Install and Configure Tableau Server.

2. Generate a node configuration (bootstrap) file on the initial node.
   
   For details, see Generate the node bootstrap file.

3. Install Tableau Server on at least two additional nodes using the node bootstrap file.
   
   For more information, see Install and initialize an additional node.

4. Configure each additional node with the processes you want to run on it. These must include a second copy of the Tableau Server repository, and a second copy of the data engine and file store, as well as additional instances of the gateway.
   
   For more information, see Configure the additional node.

5. Deploy a Coordination Service ensemble.
   
   For more information, see Deploy a Coordination Service Ensemble.

6. (Optional) Configure a load balancer.
   
   For more information, see Add a Load Balancer.
For details on how to create a three-node HA installation, see Example: Install and Configure a Three-Node HA Cluster.

Recover from an initial node failure

With a Tableau Server installation, the initial node includes two services that are only installed on that node, the License service, and the TSM Controller. If there is a problem with the initial node, Tableau Server may not continue to function, even when configured for high availability. To recover from a situation where the initial node fails, you can move the TSM Controller and the License service to one of your already configured nodes. This allows you to recover from the failure while using resources you already have in the cluster. You do not have to configure a standby initial node in case the initial node fails.

For details on how to recover from a failure on the initial node, see Recover from an Initial Node Failure.

Configure Coordination Service ensemble on additional nodes

Configuring a Coordination Service on multiple nodes provides additional duplication of processes and so reduces the possibility of server downtime due to an issue with one of the Coordination Service nodes. For details on how to deploy a Coordination Service ensemble on your cluster, see Deploy a Coordination Service Ensemble.

Tableau Server service license check

A number of processes are installed when you install Tableau Server. Some of these processes are dependent on the existence of a valid Tableau Server license while other installed processes are not. The subset of Tableau Server that require a valid Tableau Server license are considered "licensed processes."

When a licensed process starts or restarts, the process checks with the Tableau Server License Manager service on the initial node to verify there is a valid license. When the
License Manager validates the license, the process is fully functional and able to respond to requests from other Tableau Server processes. Once a licensed process has received confirmation from the License Manager, the process does not need to reconfirm the license for 72 hours, or until the process restarts. If the process is not able to verify that it is licensed (if the primary node is unavailable, for example) it cannot run, but it continues to check for a valid license until it confirms the license. To see when the last licensing check occurred, look at the log files in the `/var/opt/tableau/tableau_server-data/tabsvc/logs/licenseservice` directory. For more information about licensed processes, see Licensed processes.

Distributed Requirements

Before you start to configure a Tableau Server cluster, make sure you meet the following requirements.

Hardware

While the computers you use in your cluster must meet the requirements described in Before you install..., they do not need to be identical.

Hardware Guidelines for High Availability

Here are some guidelines for the systems you use for failover and high availability:

- **Failover—three computers**: To configure a cluster that provides failover support for the file store and repository processes, you need at least three computers or VMs: one for the initial Tableau Server node and two for additional nodes.

- **Multiple gateways—three computers and a load balancer**: Adding multiple Gateway processes to your Tableau Server installation and using a load balancer to automatically distribute requests to those gateways enhances the reliability of Tableau further. To configure a cluster that provides failover support and multiple gateways,
you need to add a load balancer to front your three-node cluster.

- **Failover & multiple gateway support—three computers and a load balancer:** To configure a cluster that provides the above plus support for multiple gateways, you need at least three computers or VMs, and a load balancer to front the cluster.

- **High availability—three computers and a load balancer:** To configure for high availability, you need the resources described above.

- **Initial computers:** If you configure for high availability, the initial Tableau Server node may be running few or no Tableau Server processes. Therefore, the computer that serves as the initial node does not need as many cores as the ones running your additional nodes. You will, however, need adequate disk space for backups because the initial computer is used during the database backup and restore processes. In addition to the amount of space needed for the backup file, you need temporary disk space roughly 10 times the size of the backup file (so if your backup is 4 GB, you should have about 40 GB of temporary disk space available).

**Software**

- All nodes in a distributed installation must be running the same version of Tableau Server.

- All nodes must be running the same distribution of Linux.

**Installation location**

When you start Tableau Services Manager (TSM) you can specify a non-default location for the data directory. This location must be the same on all nodes in your distributed Tableau Server installation.
Networking and Ports

- **Ports**: As with any distributed system, the computers or VMs you use need to be able to communicate with one another. For information on how Tableau Services Manager handles port mapping, see Tableau Services Manager Ports.

- **Same subnet**: Do not install a distributed system across multiple subnets. Latency between subnets can cause problems with Tableau server, so all nodes in the cluster should be installed on the same subnet.

  **Note**: When installing a cluster on AWS, this requirement does not apply. For details, see "Install Tableau on Amazon Web Services" in the Tableau Server Help.

- **Static IP addresses**: Any computer running Tableau Server, whether it’s a single server installation or part of a cluster, must have a static IP address.

- **Discoverable**: Each node in the cluster must be discoverable from other node computers using DNS or a local host file.

- **Time zone and time**: Each node in the cluster must be in the same timezone, with their system clocks synchronized. This may happen automatically. For example, if your nodes are all in the Active Directory domain, the domain controller usually handles this. If you are not sure your cluster meets this requirement, consult with your internal IT experts.

**Best Practices**

Here are some things to keep in mind before you start to install and configure:

- **IP addresses or computer names**: As mentioned above, each computer in the cluster must use a static IP address.
• **Backup:** It’s a best practice to create a backup prior to making significant system changes. See Back up Tableau Server data for steps.

**SSL**

If you are planning to configure SSL for a highly available Tableau Server cluster with multiple gateways and a load balancer ([learn more](#)), make sure that the SSL certificate you use was issued for the load balancer’s host name. See Configure SSL for External HTTP Traffic to and from Tableau Server for other details.

**Distributed Installation Recommendations**

When you add nodes to a Tableau Server installation, you must decide how many processes to run on each computer. This page provides some general recommendations that are intended only as a starting point.

In addition to these general recommendations, you should also:

- Understand how your organization uses Tableau Server and tune your configuration for your use case—for example, whether you want to optimize for user response or for extract refreshes.

- Perform thorough performance testing to identify the best places to adjust process configuration.

For more information on tailoring a Tableau Server installation to your organization’s needs, see Performance Tuning Examples.

For more information on the requirements for a distributed installation and for information on configuring additional nodes, see Distributed and High Availability Tableau Server Installations.
Recommendations for all installations

Although the computers that make up a Tableau Server cluster do not need to have identical hardware, they must all meet the same minimum system requirements. The recommendations on this page assume that the computers where you install Tableau Server have eight cores or more.

The following recommendations apply to all server configurations:

- Run Backgrounder processes on a dedicated computer if you plan on refreshing extracts frequently. Backgrounder processes are generally the most CPU intensive and can slow down other processes on the same computer.

  **Note:** In versions earlier than 10.5, the backgrounder process spun up temporary instances of Data Engine when refreshing extracts. In 10.5, a single instance of Data Engine is installed with the backgrounder during setup. The backgrounder uses this running instance of Data Engine when refreshing extracts.

- If you plan to refresh extracts frequently or if you plan to refresh large extracts, increase the number of processes for Backgrounder processes.

- Run VizQL processes on a different computer than Backgrounder processes. Having them on the same machine means that extract refreshes can affect user views.

- The instance of Data Engine installed on the node where File Store is installed is used for querying data for view requests. Consider separating the File Store process from the backgrounder processes to help minimize the backgrounder tasks from affecting user views.

- Locating the repository (pgsql) and the File Store on the same node as the Administration Controller can reduce the length of time it takes to back up Tableau Server. The Administration Controller is usually on the initial node, unless you have had an initial node failure and had to move the controller to another node.
When the repository is co-located with the controller it eliminates or greatly reduces the need to compress and transfer data between nodes during the backup process. This is also true with the File Store, especially if your organization uses extracts heavily.

**Note:** In a distributed installation with three or more nodes, you can have a maximum of two repository instances (active and passive). You can also run Tableau Server with one repository, but doing this means there is no failover available for the repository. For more information, see Tableau Server Repository.

### Install and Configure Additional Nodes

After you install Tableau Server on one computer (or node), the server is functional and ready for use, but it has no redundancy. If there is a problem with a process or a problem with the computer, Tableau Server may be unavailable. In addition, all processes are running on a single computer, so there can be contention for resources on that computer.

You can extend your Tableau Server installation by adding Tableau to additional nodes, creating a distributed installation. This article describes the general steps for installing Tableau Server on additional nodes and assumes you have already installed Tableau on an initial node. For more information on installing Tableau on the initial node, see Install and Initialize TSM.

If you are installing Tableau Server on multiple nodes, you should install and configure one node at a time. This makes it easier to troubleshoot any issues you might run into.

**Important:** You should add and configure additional nodes when you can fully complete the process by applying pending changes. Adding a node without finishing by applying pending changes can result in users being unable to log into Tableau Server.

**Use the TSM web interface**
Generate the node bootstrap file

1. Open TSM in a browser:

   https://<tsm-computer-name>:8850

   For more information, see Sign in to Tableau Services Manager Web UI.

2. Click the **Configuration** tab, and in the Add a Node box, click **Download Bootstrap File**.

   ![Add a Node Screenshot]

   The bootstrap file is created and copied to your local computer.

Install and initialize an additional node

Before you begin, verify that your node bootstrap file is recent. For example, if you have run `tsm security regenerate-internal-tokens` after you generated a bootstrap file, then initialization will fail.
1. Copy the original installer you used on the first computer along with the bootstrap file you generated and put them in a location accessible from the new computer you are adding Tableau Server to. This could be a mounted network share, or directly on the new computer.

2. If you are running a local firewall, then you need to configure firewall rules for all the nodes in the cluster. For more information, see Configure Local Firewall.

3. On the new node, run the Tableau Server Setup program:

   Use the package manager to install the Tableau Server package.

   Do not install to a location using a symbolic link or to a directory on a Network File System (NFS) volume.

   - On RHEL-like distributions, including CentOS, you have the option to install Tableau to a non-default location. If you choose to do so, you need to take extra steps.

   - **Default location**—To install to the default location (/opt/tableau/tableau_server), run the following commands:

     ```
     sudo yum update
     
     sudo yum install tableau-server-<version>.x86_64.rpm
     ```

   - **Non-default location**—To install to a non-default location, you must use `rpm -i`. You will also need to install all dependent packages. See the note below.

     Run the following command:

     ```
     sudo rpm -i --prefix /preferred/install/path tableau-server.rpm
     ```
Note: When you use `yum` to install Tableau Server, all dependent packages are automatically downloaded and installed. This is the preferred method for installing Tableau. If you want to install to a non-default location, or your organization does not allow you to use `yum` and you must install using `rpm -i`, you must also install all dependent packages separately. For information about installing dependent packages, see Installing Tableau Server on an Air-Gapped Computer Running Linux.

- On Ubuntu, run the following commands:

  ```bash
  sudo apt-get update
  sudo apt-get upgrade
  sudo apt-get -y install gdebi-core
  sudo gdebi -n tableau-server-<version>_amd64.deb
  ```

4. To initialize communications between your new node and the initial node, run the initialize-tsm script that is installed when you install Tableau Server.

Navigate to the `scripts` directory:

```bash
cd /opt/tableau/tableau_server/packages/scripts.<version_code>/
```

5. Run the initialize-tsm script:

```bash
sudo ./initialize-tsm -b /path/to/<bootstrap>.json -u
<admin-user-on-first-node> --accepteula
```

- Use the `-b` flag to provide the path to the bootstrap file that you copied to the computer. If you have encrypted the bootstrap file, then you must pipe the file as described in Securing secrets for import and export operations.

- Use the `-u` flag to enter the user name of the administrative user on the initial
node. This is the name of an administrative user on the computer, not the Tableau Server administrator. You will be prompted for the user password.

- **Important:** You must enter the credentials of the same user that you used during the installation process on the initial node.

- The `--accepteula` flag accepts the Tableau Server End User License Agreement (EULA). The EULA is available in the following location:

  `/opt/tableau/tableau_server/packages/docs.<version_code>/EULA.rtf`

Configure the additional node with Cluster Controller

1. Open TSM in a browser:

   https://<tsm-computer-name>:8850

   For more information, see Sign in to Tableau Services Manager Web UI.

2. Click the **Configuration** tab. A message should tell you that the new node was added.

   ![Configuration Tab](image)

   Click **Continue** to dismiss the message.
3. Cluster Controller is part of the minimum topology and is already selected. Each node must run Cluster Controller.

If you only want to set the minimum topology for the node, go to Step 4 below. You might do this if you will be adding additional nodes and are not ready to configure this node beyond the minimum.

If you want to add additional processes to the minimum topology, specify the processes that should run on the node. Do this by selecting the processes you want, or specifying the number of processes that should run on the node.

For example, to add a Gateway and two instances of the Backgrounder on the node:

   a. Select **Gateway**.

   b. Set the **Backgrounder** count to 2.

     Adding Backgrounder to a node will also add an instance of Data Engine if one is not already on the node.

The specific processes and process counts you set will depend on your organizational environment and needs. Some processes are added automatically when you add another process. For more information, see Configure Nodes and Tableau Server Processes.

**Note:** The TSM Web UI limits you to a maximum of 8 instances of processes that allow you to select the number of instances. To configure more instances than this, use the command line and the `TSM topology set-process` command. For more information, see `tsm topology set-process`.

4. Click **Pending Changes** at the top of the page:
If you are configuring a cluster with three or more nodes, a Coordination Service ensemble warning displays. You can continue. You will deploy a Coordination Service ensemble in a separate step.

5. Click **Apply Changes and Restart** and **Confirm** to confirm a restart of Tableau Server.

After Tableau Server restarts, the node is included with the minimum topology necessary and any additional processes you configured.

**Use the TSM CLI**

**Generate the node bootstrap file**

To install Tableau Server on additional computers you use the same installer you did for the initial node, along with a "bootstrap" file you generate on the initial node.

**Important**: The bootstrap file contains a copy of the master keystore file used for encrypting the configuration secrets. We strongly recommend that you take additional measures to secure the bootstrap file using mechanisms as described in Securing secrets for import and export operations.

1. After installing Tableau Server on the initial node, generate the node bootstrap file.

2. On the initial node, open a terminal session.

3. Type this command to generate the bootstrap file:

   ```
   tsm topology nodes get-bootstrap-file --file <path\-file>.json
   ```
Tableau Server on Linux Administrator Guide

Install and initialize an additional node

1. Copy the original installer you used on the first computer along with the bootstrap file you generated and put them in a location accessible from the new computer you are adding Tableau Server to. This could be a mounted network share, or directly on the new computer.

2. If you are running a local firewall, then you need to configure firewall rules for all the nodes in the cluster. For more information, see Configure Local Firewall.

3. On the new node, run the Tableau Server Setup program:

Use the package manager to install the Tableau Server package.

Do not install to a location using a symbolic link or to a directory on a Network File System (NFS) volume.

- On RHEL-like distributions, including CentOS, you have the option to install Tableau to a non-default location. If you choose to do so, you need to take extra steps.
  - **Default location**—To install to the default location (/opt/tableau/tableau_server), run the following commands:

    ```
sudo yum update

    sudo yum install tableau-server-<version>.x86_64.rpm
    ```

  - **Non-default location**—To install to a non-default location, you must use `rpm -i`. You will also need to install all dependent packages. See the note below.

    Run the following command:
sudo rpm -i --prefix /preferred/install/path
tableau-server.rpm

**Note:** When you use *yum* to install Tableau Server, all dependent packages are automatically downloaded and installed. This is the preferred method for installing Tableau. If you want to install to a non-default location, or your organization does not allow you to use *yum* and you must install using *rpm* -i, you must also install all dependent packages separately. For information about installing dependent packages, see Installing Tableau Server on an Air-Gapped Computer Running Linux.

- On Ubuntu, run the following commands:

  ```bash
  sudo apt-get update
  sudo apt-get upgrade
  sudo apt-get -y install gdebi-core
  sudo gdebi -n tableau-server-<version>_amd64.deb
  ```

4. To initialize communications between your new node and the initial node, run the initialize-tsm script that is installed when you install Tableau Server.

   **On the new node:**

   Navigate to the `scripts` directory:

   ```bash
   cd /opt/tableau/tableau_server/packages/scripts.<version_code>/
   ```

5. Run the initialize-tsm script:

   ```bash
   sudo ./initialize-tsm -b /path/to/<bootstrap>.json -u
   <admin-user-on-first-node> --accepteula
   ```
Use the -b flag to provide the path to the bootstrap file that you copied to the computer. If you have encrypted the bootstrap file, then you must pipe the file as described in Securing secrets for import and export operations.

Use the -u flag to enter the user name of the administrative user on the initial node. This is the name of an administrative user on the computer, not the Tableau Server administrator. You will be prompted for the user password.

**Important:** You must enter the credentials of the same user that you used during the installation process on the initial node.

The --accepteula flag accepts the Tableau Server End User License Agreement (EULA). The EULA is available in the following location:

```
/opt/tableau/tableau_server/packages/docs.<version_code>/EULA.rtf
```

Configure the additional node

**Note:** This basic example illustrates how to set the topology on a node. For a more detailed, working multi-node example, see Example: Install and Configure a Three-Node HA Cluster.

On the initial (original) node, set the topology for the newly added node. The topology specifies which processes should run on the node, and how many instances of each process should run. The topology for the node will depend on your environment and organizational needs. The below are just examples of setting the topology.

1. On the new node, open a terminal session.

2. Get the node-id for the new node:

   ```
   tsm topology list-nodes -v
   ```
The -v option lists the nodes and the processes they are currently running. You can identify the newly added node because it will not have any processes on it.

3. **Specify the individual processes that should run on this node.**

Do this with the following command:

```bash
tsml topology set-process -n <nodeID> -pr <processname> -c <n>
```

You must add an instance of the Cluster Controller to each node.

For example, to add the Cluster Controller, two instances of the Backgrounder, and a Gateway to node2:

```bash
tsml topology set-process -n node2 -pr clustercontroller -c 1
ntsml topology set-process -n node2 -pr backgrounder -c 2
ntsml topology set-process -n node2 -pr gateway -c 1
```

The specific processes and process counts you set will depend on your organizational environment and needs. Some processes are added automatically when you add another process. For more information, see Configure Nodes and Tableau Server Processes.

4. **Apply the node configuration.** The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

```bash
tsml pending-changes apply
```

A warning about deploying a Coordination Service ensemble displays if you have deployed a three- or five-node cluster. If this is the only warning, you can safely over-
Tableau Server on Linux Administrator Guide

ride it using the --ignore-warnings option to apply the configuration changes in spite of the warning.

    tsm pending-changes apply --ignore-warnings

Install drivers

You need to install drivers so that Tableau Server can connect to data and run extracts. Install these drivers on nodes that are running any of the following processes:

- VizQL Server (vizqlserver)
- Application Server (vizportal)
- Data Server (dataserver)
- Backgrounder (backgrounder)

Drivers and administrative views

If you want to use the built-in administrative views in Tableau Server, you also need to install the PostgreSQL driver on any nodes running any of the above processes.

For more information, see Database Drivers.

Database Drivers

Tableau connectors require a driver to talk to the database. Before you can connect to data sources from Tableau Server, you must install drivers for the data sources you want to connect to. You can find information about supported data sources for Tableau Server on Linux on the Tableau Server tech specs page. You can find driver links and installation instructions for all the supported connectors on the Driver Download page.

Important: You must install the PostgreSQL driver if you want to use the built-in administrative views.
Install drivers in a cluster

You need to install the drivers for your data sources on the initial node in a Tableau Server cluster. If you install Tableau Server on multiple nodes, you must also install drivers on any node that runs any of the following processes:

- Application Server (Vizportal)
- Backgrounder
- Data Server
- VizQL Server

Example: Install and Configure a Three-Node HA Cluster

A multi-node high availability installation of Tableau Server can help to maximize the efficiency and availability of Tableau Server. When configuring a multi-node Tableau Server deployment, the steps you perform are designed to build in redundancy, helping to reduce your potential downtime. In addition to simply improving efficiency by moving or adding server processes to additional nodes, you can create a highly available (HA) installation of Tableau Server by satisfying these requirements:

- Add additional nodes for a total of at least three nodes
- Deploy a Coordination Service ensemble on at least three nodes
- Add a second instance of the File Store on one of the additional nodes (Data Engine will be installed automatically, if it is not already on the node)
- Add a second instance of the Repository (pgsql) on one of the additional nodes

A Tableau Server installation that includes these additions will have built-in redundancy and can support failover in the event of a problem with the repository. This example shows how to do this, and more.

A Single Server System

After installing Tableau Server on an initial node, you have a system that is running everything it needs to function. It has at least one instance of all server processes and is the most basic configuration of Tableau Server. It has no redundancy. The server topology looks like this (some TSM-specific processes are not shown):
Stand-alone Tableau Server node

- Gateway
- Search & Browse
- Application Server (VizPortal) x2
- VizQL Server x2
- Data Server x2
- Ask Data
- Elastic Server
- Cache Server x2
- Backgrounder x2
- Interactive Microservice container
- Non-Interactive Microservice Container

- Data Engine
- File Store

- Repository

- Licensing
- Cluster Controller
- Coordination Service
A Three-Node System

To build in redundancy, you need to add additional nodes to host instances of the repository and the data engine and file store processes. You can add instances of other processes, including multiple instances of a process on a node. In addition, to reduce the system’s vulnerability, you can run multiple gateways and additional instances of some of the server processes. The fewest number of computers required to achieve this configuration is three.

In the diagram below, the file store process has been added to both additional nodes. A second, passive instance of the repository has also been added to one of the other new nodes. Finally, the server processes (shown in blue) have been added to the additional nodes to provide redundancy.
Configuration steps

This procedure describes how to configure a three-node HA Tableau Server cluster with two repository instances and two file store/data engine instances on the additional nodes as
Before you begin

Before you install Tableau Server on any additional nodes, ensure that each additional node meets the distributed requirements. See Distributed Requirements for details.

Use the TSM web interface

**Note:** This operation includes steps that you may need to perform using the TSM command line.

Step 1: Install the initial node

See Install and Configure Tableau Server.

Step 2: Generate a bootstrap file for the additional nodes

1. Open TSM in a browser:

   https://<tsm-computer-name>:8850

   For more information, see Sign in to Tableau Services Manager Web UI.

2. Click the **Configuration** tab, and in the Add a Node box, click **Download Bootstrap File**.
The bootstrap file is created and copied to your local computer.

Step 3: Install and initialize an additional node

1. Copy the original installer you used on the first computer along with the bootstrap file you generated and put them in a location accessible from the new computer you are adding Tableau Server to. This could be a mounted network share, or directly on the new computer.

2. If you are running a local firewall, then you need to configure firewall rules for all the nodes in the cluster. For more information, see Configure Local Firewall.

3. On the new node, run the Tableau Server Setup program:

   Use the package manager to install the Tableau Server package.

   Do not install to a location using a symbolic link or to a directory on a Network File System (NFS) volume.
On RHEL-like distributions, including CentOS, you have the option to install Tableau to a non-default location. If you choose to do so, you need to take extra steps.

- **Default location**—To install to the default location (/opt/tableau/tableau_server), run the following commands:

  ```
  sudo yum update
  sudo yum install tableau-server-<version>.x86_64.rpm
  ```

- **Non-default location**—To install to a non-default location, you must use `rpm -i`. You will also need to install all dependent packages. See the note below.

  Run the following command:

  ```
  sudo rpm -i --prefix /preferred/install/path
  tableau-server.rpm
  ```

**Note:** When you use `yum` to install Tableau Server, all dependent packages are automatically downloaded and installed. This is the preferred method for installing Tableau. If you want to install to a non-default location, or your organization does not allow you to use `yum` and you must install using `rpm -i`, you must also install all dependent packages separately. For information about installing dependent packages, see Installing Tableau Server on an Air-Gapped Computer Running Linux.

- On Ubuntu, run the following commands:

  ```
  sudo apt-get update
  sudo apt-get upgrade
  ```
Tableau Server on Linux Administrator Guide

```
sudo apt-get -y install gdebi-core
sudo gdebi -n tableau-server-<version>_amd64.deb
```

4. To initialize communications between your new node and the initial node, run the `initialize-tsm` script that is installed when you install Tableau Server.

**Navigate to the scripts directory:**

```
cd /opt/tableau/tableau_server/packages/scripts.<version_code>/
```

5. Run the `initialize-tsm` script:

```
sudo ./initialize-tsm -b /path/to/<bootstrap>.json -u <admin-user-on-first-node> --accepteula
```

- Use the `-b` flag to provide the path to the bootstrap file that you copied to the computer. If you have encrypted the bootstrap file, then you must pipe the file as described in Securing secrets for import and export operations.

- Use the `-u` flag to enter the user name of the administrative user on the initial node. This is the name of an administrative user on the computer, not the Tableau Server administrator. You will be prompted for the user password.

**Important:** You must enter the credentials of the same user that you used during the installation process on the initial node.

- The `--accepteula` flag accepts the Tableau Server End User License Agreement (EULA). The EULA is available in the following location:

```
/opt/tableau/tableau_server/packages/docs.<version_code>/EULA.rtf
```
Step 4: Install and initialize a second additional node

1. Copy the original installer you used on the first computer along with the bootstrap file you generated and put them in a location accessible from the new computer you are adding Tableau Server to. This could be a mounted network share, or directly on the new computer.

2. If you are running a local firewall, then you need to configure firewall rules for all the nodes in the cluster. For more information, see Configure Local Firewall.

3. On the new node, run the Tableau Server Setup program:

   Use the package manager to install the Tableau Server package.

   Do not install to a location using a symbolic link or to a directory on a Network File System (NFS) volume.

   • On RHEL-like distributions, including CentOS, you have the option to install Tableau to a non-default location. If you choose to do so, you need to take extra steps.

     • **Default location**—To install to the default location (/opt/tableau/tableau_server), run the following commands:

       ```
       sudo yum update
       sudo yum install tableau-server-<version>.x86_64.rpm
       ```

     • **Non-default location**—To install to a non-default location, you must use `rpm -i`. You will also need to install all dependent packages. See the note below.

       Run the following command:
sudo rpm -i --prefix /preferred/install/path tableau-server.rpm

**Note:** When you use `yum` to install Tableau Server, all dependent packages are automatically downloaded and installed. This is the preferred method for installing Tableau. If you want to install to a non-default location, or your organization does not allow you to use `yum` and you must install using `rpm -i`, you must also install all dependent packages separately. For information about installing dependent packages, see Installing Tableau Server on an Air-Gapped Computer Running Linux.

- On Ubuntu, run the following commands:

  ```
sudo apt-get update
sudo apt-get upgrade
sudo apt-get -y install gdebi-core
sudo gdebi -n tableau-server-<version>_amd64.deb
  ```

4. To initialize communications between your new node and the initial node, run the `initialize-tsm` script that is installed when you install Tableau Server.

   **Navigate to the scripts directory:**

   ```
cd /opt/tableau/tableau_server/packages/scripts.<version_code>/
  ```

5. Run the `initialize-tsm` script:

   ```
sudo ./initialize-tsm -b /path/to/<bootstrap>.json -u <admin-user-on-first-node> --accepteula
  ```

   - Use the `-b` flag to provide the path to the bootstrap file that you copied to the computer. If you have encrypted the bootstrap file, then you must pipe the file as described in Securing secrets for import and export operations.
• Use the `-u` flag to enter the user name of the administrative user on the initial node. This is the name of an administrative user on the computer, not the Tableau Server administrator. You will be prompted for the user password.

**Important:** You must enter the credentials of the same user that you used during the installation process on the initial node.

• The `--accepteula` flag accepts the Tableau Server End User License Agreement (EULA). The EULA is available in the following location:

```
/opt/tableau/tableau_server/packages/docs.<version_code>/EULA.rtf
```

Step 5: Configure the new node with a minimum topology

To complete the process of adding new nodes to your cluster, you need to configure them with a minimum topology. With a minimum topology, the only pending change will be the addition of Cluster Controller, which is required on each node. If you want other processes on the nodes you can add most of them at the same time. This example only configures the nodes with Cluster Controller.

1. Open TSM in a browser:

   `https://<tsm-computer-name>:8850`

   For more information, see Sign in to Tableau Services Manager Web UI.

2. Click the **Configuration** tab. A message should tell you that new nodes were added.
Click **Continue** to dismiss the message.

3. Click **Pending Changes** at the top of the page:

   If you are configuring a cluster with three or more nodes, a Coordination Service ensemble warning displays. You can continue. You will deploy a Coordination Service ensemble in a separate step.

4. Click **Apply Changes and Restart** and **Confirm** to confirm a restart of Tableau Server.

   When Tableau Server restarts, the nodes are included with the minimum topology necessary.

Step 6: Deploy a Coordination Service ensemble

If you install a total of three or more nodes, you should also deploy a Coordination Service ensemble. If you do not, you will get a warning message every time you make changes to the server configuration or topology. You can ignore this message, but as a best practice you should deploy a multi-node Coordination Service ensemble.
When you install Tableau Server, a single instance of the Coordination Service is installed on the initial node. TSM and Tableau Server depend on the Coordination Service to function properly, so to provide redundancy and ensure availability on multi-node installations, configure additional instances of the Coordination Service by deploying a Coordination Service ensemble. Coordination Service ensembles are installed with one, three, or five instances of the Coordination Service. In a three-node installation of Tableau Server, the recommended number of Coordination Service instances is three, one on each node.

Do not attempt to deploy a Coordination Service ensemble if there are other changes pending. Discard or apply any pending changes before deploying a new Coordination Service ensemble.

**Note:** This operation includes steps that you may need to perform using the TSM command line.

The following steps illustrate how to deploy a new Coordination Service ensemble on an existing three-node Tableau Server cluster and clean up the old ensemble.

1. On the initial node, open a terminal session.

2. Type this command to sign in to Tableau Server as a TSM administrator:

   ```
   tsm login -u <username>
   ```

   You will be prompted for your password.

3. Type this command to stop Tableau Server:

   ```
   tsm stop
   ```

   Some TSM processes will continue to run, including the Administration Controller and Administration Agent.

4. Confirm there are no pending changes:
If there are pending changes, you need to either discard the changes or apply them. Applying pending changes will take some time:

- **Discard the changes**
  
  tsm pending-changes discard

  or

- **Apply the changes**
  
  tsm pending-changes apply

Wait until the command completes and you are returned to the system prompt.

5. Get the node IDs for each node in the cluster:

   tsm topology list-nodes -v

6. **Use the `tsm topology deploy-coordination-service` command to add a new Coordination Service ensemble by adding the Coordination Service to specified nodes.** You must specify the node(s) that the Coordination Service should be added to. The command also makes the new ensemble the "production" ensemble (the ensemble in use).

   For example, deploy the Coordination Service to all three nodes of a three-node cluster, where the nodes are node1, node2, and node3:

   tsm topology deploy-coordination-service -n node1,node2,node3

7. **Wait until the new Coordination Service ensemble is running and the server is ready for the next step.**
**Important.** If you attempt to clean up the old Coordination Service ensemble before the server is in the proper state, you can put the server into an unrecoverable state and may need to completely reinstall Tableau.

a. Check the status of the server:

   ```
   tsm status -v
   ```

   If the deployment is not complete, you may see processes showing as running when they are not, and the Coordination Service showing a status of "unavailable" while the service is synchronizing between nodes on the cluster. Tableau Server may show as being in an error state while this is happening. You may also get an error message: "Could not connect to TSM Controller at '<host>:8850'." This is normal when the server is returning to a valid state.

b. Check the status of the server periodically until you are prompted to sign in again.

c. When you are prompted, sign in to TSM and continue to check the server status until you see a status of "STOPPED" for each node. If the status of a node shows as "ERROR" you need to wait. When each node status is "STOPPED" you should also see the following services running:

   On the initial node:

   - Two instances of the Coordination Service on the initial node, both with a status of "running".
   - The Administration Controller with a status of "running". (The Administration Controller is only installed on the initial node.)
   - The Administration Agent with a status of "running".
Tableau Server on Linux Administrator Guide

- Additional services on the initial node, all with a status of "running": Service Manager, License Manager, Client File Service.

On the additional nodes:

- One or more instance of the Coordination Service on each additional node you specified when you deployed the new ensemble, all with a status of "running". If you are deploying a new ensemble to nodes that already had Coordination Service running, you will see two instances of the service.

- The Administration Agent on every node, with a status of "running".

If you do not see a status of "running" for all of the above, wait a few minutes and run the status command again.

**Note:** If there is a problem with an instance of the Coordination Service (if it shows as stopped for example), you can toggle back to your previous Coordination Service ensemble using the `tsm topology toggle-coordination-service` command. To do this, the rest of the services should be in the state described above, including Administration Controller and Agent. You can toggle back to the previous ensemble only if you have **not** run the `cleanup-coordination-service` command. Tableau Server cannot be running when you use this command.

8. Remove the old ensemble. This step is **required**. You cannot run Tableau Server with multiple Coordination Service ensembles configured.

   ```
   tsm topology cleanup-coordination-service
   ```

   Tableau Server must be stopped when you use this command, but some TSM services will be running (see above).

9. Start Tableau Server:
For more information and details on deploying a new Coordination Service ensemble, see Deploy a Coordination Service Ensemble.

Step 7: Configure processes for the second node

1. Open TSM in a browser:

   https://<tsm-computer-name>:8850

   For more information, see Sign in to Tableau Services Manager Web UI.

2. Click the Configuration tab.

3. Specify the processes and number of instances that should run on the first additional node.

   In this example:

   a. Select Gateway.

   b. Set the Application Server (vizportal) count to 2.

   c. Set the VizQL Server count to 2.

   d. Set the Cache Server count to 2.

   e. Select Search & Browse.

   f. Set the Backgrounder count to 2.

      Adding Backgrounder to a node will also add an instance of Data Engine if one is not already on the node.

   g. Set the Data Server count to 2.
h. Select **File Store**.

i. Select **Repository** (pgsql).

The specific processes and process counts you set will depend on your organizational environment and needs. Some processes are added automatically when you add another process. For more information, see Configure Nodes and Tableau Server Processes.

**Note:** The TSM Web UI limits you to a maximum of 8 instances of processes that allow you to select the number of instances. To configure more instances than this, use the command line and the `TSM topology set-process command`. For more information, see `tsm topology set-process`.

Step 8: Configure processes for third node

1. In TSM, on the **Configuration** tab, specify the processes and number of instances that should run on the second additional node.

   In this example:

   a. Select **Gateway**.

   b. Set the **Application Server** (vizportal) count to 2.

   c. Set the **VizQL Server** count to 2.

   d. Set the **Cache Server** count to 2.

   e. Select **Search & Browse**.

   f. Set the **Backgrounder** count to 2.

   Adding Backgrounder to a node will also add an instance of Data Engine if one is not already on the node.
g. Set the **Data Server** count to 2.

h. Select **File Store**.

2. Click **Pending Changes** at the top of the page:

   ![Pending Changes](image)

   The Pending Changes list displays.

3. Click **Apply Changes and Restart** and **Confirm** to confirm a restart of Tableau Server.

**Use the TSM CLI**

**Step 1: Install the initial node**

See Install and Configure Tableau Server.

**Step 2: Generate a bootstrap file for the additional nodes**

To install Tableau Server on additional computers you use the same installer you did for the initial node, along with a "bootstrap" file you generate on the initial node.

**Important:** The bootstrap file contains a copy of the master keystore file used for encrypting the configuration secrets. We strongly recommend that you take additional measures to secure the bootstrap file using mechanisms as described in Securing secrets for import and export operations.

1. After installing Tableau Server on the initial node, generate the node bootstrap file.

2. On the initial node, open a terminal session.

3. Type this command to generate the bootstrap file:
Tableau Server on Linux Administrator Guide

```
tsm topology nodes get-bootstrap-file --file <path\-file>.json
```

Step 3: Install an additional node

1. Copy the original installer you used on the first computer along with the bootstrap file you generated and put them in a location accessible from the new computer you are adding Tableau Server to. This could be a mounted network share, or directly on the new computer.

2. If you are running a local firewall, then you need to configure firewall rules for all the nodes in the cluster. For more information, see Configure Local Firewall.

3. On the new node, run the Tableau Server Setup program:

   Use the package manager to install the Tableau Server package.

   Do not install to a location using a symbolic link or to a directory on a Network File System (NFS) volume.

   - On RHEL-like distributions, including CentOS, you have the option to install Tableau to a non-default location. If you choose to do so, you need to take extra steps.

     - **Default location**—To install to the default location (/opt/tableau/tableau_server), run the following commands:

       ```
sudo yum update

       sudo yum install tableau-server-<version>.x86_64.rpm
       ```

     - **Non-default location**—To install to a non-default location, you must use `rpm -i`. You will also need to install all dependent packages. See the note below.
Run the following command:

```bash
sudo rpm -i --prefix /preferred/install/path
tableau-server.rpm
```

**Note:** When you use `yum` to install Tableau Server, all dependent packages are automatically downloaded and installed. This is the preferred method for installing Tableau. If you want to install to a non-default location, or your organization does not allow you to use `yum` and you must install using `rpm -i`, you must also install all dependent packages separately. For information about installing dependent packages, see Installing Tableau Server on an Air-Gapped Computer Running Linux.

- On Ubuntu, run the following commands:

  ```bash
  sudo apt-get update
  sudo apt-get upgrade
  sudo apt-get -y install gdebi-core
  sudo gdebi -n tableau-server-<version>_amd64.deb
  ```

4. To initialize communications between your new node and the initial node, run the `initialize-tsm` script that is installed when you install Tableau Server.

   **On the new node:**

   Navigate to the `scripts` directory:

   ```bash
   cd /opt/tableau/tableau_server/packages/scripts.<version_code>/
   ```

5. Run the `initialize-tsm` script:

   ```bash
   sudo ./initialize-tsm -b /path/to/<bootstrap>.json -u <admin-user-on-first-node> --accepteula
   ```
Use the -b flag to provide the path to the bootstrap file that you copied to the computer. If you have encrypted the bootstrap file, then you must pipe the file as described in Securing secrets for import and export operations.

Use the -u flag to enter the user name of the administrative user on the initial node. This is the name of an administrative user on the computer, not the Tableau Server administrator. You will be prompted for the user password.

**Important:** You must enter the credentials of the same user that you used during the installation process on the initial node.

The --accepteula flag accepts the Tableau Server End User License Agreement (EULA). The EULA is available in the following location:

/opt/tableau/tableau_server/packages/docs.<version_code>/EULA.rtf

Step 4: Install a second additional node

Install Tableau Server on the second additional node:

1. Copy the original installer you used on the first computer along with the bootstrap file you generated and put them in a location accessible from the new computer you are adding Tableau Server to. This could be a mounted network share, or directly on the new computer.

2. If you are running a local firewall, then you need to configure firewall rules for all the nodes in the cluster. For more information, see Configure Local Firewall.

3. On the new node, run the Tableau Server Setup program:

   Use the package manager to install the Tableau Server package.

   Do not install to a location using a symbolic link or to a directory on a Network File System (NFS) volume.
On RHEL-like distributions, including CentOS, you have the option to install Tableau to a non-default location. If you choose to do so, you need to take extra steps.

- **Default location**—To install to the default location (/opt/tableau/tableau_server), run the following commands:

  ```
  sudo yum update
  sudo yum install tableau-server-<version>.x86_64.rpm
  ```

- **Non-default location**—To install to a non-default location, you must use `rpm -i`. You will also need to install all dependent packages. See the note below.

  Run the following command:

  ```
  sudo rpm -i --prefix /preferred/install/path tableau-server.rpm
  ```

  **Note:** When you use `yum` to install Tableau Server, all dependent packages are automatically downloaded and installed. This is the preferred method for installing Tableau. If you want to install to a non-default location, or your organization does not allow you to use `yum` and you must install using `rpm -i`, you must also install all dependent packages separately. For information about installing dependent packages, see Installing Tableau Server on an Air-Gapped Computer Running Linux.

- On Ubuntu, run the following commands:

  ```
  sudo apt-get update
  sudo apt-get upgrade
  ```
sudo apt-get -y install gdebi-core
sudo gdebi -n tableau-server-<version>_amd64.deb

4. To initialize communications between your new node and the initial node, run the initialize-tsm script that is installed when you install Tableau Server.

On the new node:

Navigate to the scripts directory:

cd /opt/tableau/tableau_server/packages/scripts.<version_code>/

5. Run the initialize-tsm script:

```
sudo ./initialize-tsm -b /path/to/<bootstrap>.json -u <admin-user-on-first-node> --accepteula
```

- Use the `-b` flag to provide the path to the bootstrap file that you copied to the computer. If you have encrypted the bootstrap file, then you must pipe the file as described in Securing secrets for import and export operations.

- Use the `-u` flag to enter the user name of the administrative user on the initial node. This is the name of an administrative user on the computer, not the Tableau Server administrator. You will be prompted for the user password.

**Important:** You must enter the credentials of the same user that you used during the installation process on the initial node.

- The `--accepteula` flag accepts the Tableau Server End User License Agreement (EULA). The EULA is available in the following location:

```
/opt/tableau/tableau_server/packages/docs.<version_code>/EULA.rtf
```
Step 5: Add a process to the additional nodes

1. On the initial node, configure a cluster controller instance on each additional node:

   tsm topology set-process -n <nodeID_second-node> -pr
   clustercontroller -c 1

   tsm topology set-process -n <nodeID_third-node> -pr
   clustercontroller -c 1

2. Apply the node configuration changes:

   tsm pending-changes apply --ignore-warnings

   A warning about deploying a Coordination Service ensemble displays because you have deployed a three-node cluster. Use the --ignore-warnings option to apply the configuration changes in spite of the warning. You will deploy a new Coordination Service ensemble in the next step.

Step 6: Deploy a Coordination Service ensemble

If you install a total of three or more nodes, you should also deploy a Coordination Service ensemble. If you do not, you will get a warning message every time you make changes to the server configuration or topology. You can ignore this message, but as a best practice you should deploy a multi-node Coordination Service ensemble.

When you install Tableau Server, a single instance of the Coordination Service is installed on the initial node. TSM and Tableau Server depend on the Coordination Service to function properly, so to provide redundancy and ensure availability on multi-node installations, configure additional instances of the Coordination Service by deploying a Coordination Service ensemble. Coordination Service ensembles are installed with one, three, or five instances of the Coordination Service. In a three-node installation of Tableau Server, the recommended number of Coordination Service instances is three, one on each node.

Do not attempt to deploy a Coordination Service ensemble if there are other changes pending. Discard or apply any pending changes before deploying a new Coordination Service ensemble.
Note: This operation includes steps that you may need to perform using the TSM command line.

The following steps illustrate how to deploy a new Coordination Service ensemble on an existing three-node Tableau Server cluster and clean up the old ensemble.

1. On the initial node, open a terminal session.

2. Type this command to sign in to Tableau Server as a TSM administrator:

   `tsm login -u <username>`

   You will be prompted for your password.

3. Type this command to stop Tableau Server:

   `tsm stop`

   Some TSM processes will continue to run, including the Administration Controller and Administration Agent.

4. Confirm there are no pending changes:

   `tsm pending-changes list`

   If there are pending changes, you need to either discard the changes or apply them. Applying pending changes will take some time:

   - Discard the changes
     `tsm pending-changes discard`
     
     or
Apply the changes:

```bash
tsm pending-changes apply
```

Wait until the command completes and you are returned to the system prompt.

5. Get the node IDs for each node in the cluster:

```bash
tsm topology list-nodes -v
```

6. Use the `tsm topology deploy-coordination-service` command to add a new Coordination Service ensemble by adding the Coordination Service to specified nodes. You must specify the node(s) that the Coordination Service should be added to. The command also makes the new ensemble the "production" ensemble (the ensemble in use).

For example, deploy the Coordination Service to all three nodes of a three-node cluster, where the nodes are node1, node2, and node3:

```bash
tsm topology deploy-coordination-service -n node1,node2,node3
```

7. Wait until the new Coordination Service ensemble is running and the server is ready for the next step.

**Important.** If you attempt to clean up the old Coordination Service ensemble before the server is in the proper state, you can put the server into an unrecoverable state and may need to completely reinstall Tableau.

a. Check the status of the server:

```bash
tsm status -v
```

If the deployment is not complete, you may see processes showing as running when they are not, and the Coordination Service showing a status of
"unavailable" while the service is synchronizing between nodes on the cluster. Tableau Server may show as being in an error state while this is happening. You may also get an error message: "Could not connect to TSM Controller at '<host>:8850'." This is normal when the server is returning to a valid state.

b. Check the status of the server periodically until you are prompted to sign in again.

c. When you are prompted, sign in to TSM and continue to check the server status until you see a status of "STOPPED" for each node. If the status of a node shows as "ERROR" you need to wait. When each node status is "STOPPED" you should also see the following services running:

On the initial node:

- Two instances of the Coordination Service on the initial node, both with a status of "running".
- The Administration Controller with a status of "running". (The Administration Controller is only installed on the initial node.)
- The Administration Agent with a status of "running".
- Additional services on the initial node, all with a status of "running": Service Manager, License Manager, Client File Service.

On the additional nodes:

- One or more instance of the Coordination Service on each additional node you specified when you deployed the new ensemble, all with a status of "running". If you are deploying a new ensemble to nodes that already had Coordination Service running, you will see two instances of the service.
- The Administration Agent on every node, with a status of "running".
If you do not see a status of "running" for all of the above, wait a few minutes and run the status command again.

**Note:** If there is a problem with an instance of the Coordination Service (if it shows as **stopped** for example), you can toggle back to your previous Coordination Service ensemble using the `tsm topology toggle-coordination-service` command. To do this, the rest of the services should be in the state described above, including Administration Controller and Agent. You can toggle back to the previous ensemble only if you have **not** run the `cleanup-coordination-service` command. Tableau Server cannot be running when you use this command.

8. Remove the old ensemble. This step is **required**. You cannot run Tableau Server with multiple Coordination Service ensembles configured.

```
 tsm topology cleanup-coordination-service
```

Tableau Server must be stopped when you use this command, but some TSM services will be running (see above).

9. Start Tableau Server:

```
 tsm start
```

For more information and details on deploying a new Coordination Service ensemble, see Deploy a Coordination Service Ensemble.

**Step 7: Configure processes for the second node**

1. On the initial node, set the topology for the second node. The topology specifies which processes should run on the node, and how many instances of each process should run. For details about configuring nodes, see Configure Nodes. Data engine will be added automatically when you add other processes. For details on when data
engine is added, see Tableau Server Processes.

a. Get the node-id for the new node:  
   tsm topology list-nodes -v

b. Specify individual processes that will run on the new node:

   tsm topology set-process -n <node-id> -pr gateway -c 1
   tsm topology set-process -n <node-id> -pr vizqlserver -c 2
   tsm topology set-process -n <node-id> -pr vizportal -c 2
   tsm topology set-process -n <node-id> -pr backgrounder -c 2
   tsm topology set-process -n <node-id> -pr cacheserver -c 2
   tsm topology set-process -n <node-id> -pr searchserver -c 1
   tsm topology set-process -n <node-id> -pr dataserver -c 2
   tsm topology set-process -n <node-id> -pr filestore -c 1
   tsm topology set-process -n <node-id> -pr pgsql -c 1

2. Apply the node configuration changes. You will be prompted with a message that Tableau Server will restart.

   tsm pending-changes apply
Step 8: Configure processes for third node

On the initial node, set the topology for the new node. The topology specifies which processes should run on the node, and how many instances of each process should run. Data engine will be added automatically when you add other processes. For details on when data engine is added, see Tableau Server Processes.

1. Get the node-id for the new node:

   tsm topology list-nodes -v

2. Specify individual processes that will run on the new node:

   tsm topology set-process -n <node-id> -pr gateway -c 1
   tsm topology set-process -n <node-id> -pr vizqlserver -c 2
   tsm topology set-process -n <node-id> -pr vizportal -c 2
   tsm topology set-process -n <node-id> -pr backgrounder -c 2
   tsm topology set-process -n <node-id> -pr cacheserver -c 2
   tsm topology set-process -n <node-id> -pr searchserver -c 1
   tsm topology set-process -n <node-id> -pr dataserver -c 2
   tsm topology set-process -n <node-id> -pr filestore -c 1

3. Apply the node configuration. You will be prompted with a message that Tableau Server will restart.

   tsm pending-changes apply

4. Start the server:

   tsm start
Step 9: Configure firewall rules (optional)

If you are running a local firewall, then you need to configure firewall rules for all the nodes in the cluster. For more information, see Configure Local Firewall. For more information, see Local firewall configuration.

Add a Load Balancer

At this point, all three nodes have gateways, which are used to route requests to available server processes. All gateways are active, but to further reduce the potential for downtime in the cluster, you can configure a load balancer. For more information, see Add a Load Balancer.

Add a Load Balancer

You can enhance the reliability of Tableau Server by running gateways on multiple nodes, and configuring a load balancer to distribute requests across the gateways. Unlike the repository process, which can be active or passive, all gateway processes are active. If one gateway in a cluster becomes unavailable, the load balancer stops sending requests to it. The load balancer algorithm you choose determines how the gateways will route client requests.

Note: If you will be using Kerberos authentication, you need to configure Tableau Server for your load balancer before you configure Tableau Server for Kerberos. For more information, see Configure Kerberos.

Note the following as you configure your load balancer to work with Tableau Server:

- **Tested load balancers**: Tableau Server clusters with multiple gateways have been tested with Apache and F5 load balancers.

  If you are using an Apache load balancer and creating custom administrative views, you need to connect directly to the Tableau Server repository. You cannot connect through the load balancer.
• **Tableau Server URL**: When a load balancer is in front of a Tableau Server cluster, the URL that’s accessed by Tableau Server users belongs to the load balancer, not the initial Tableau Server node.

• **Trusted host settings**: The computer running the load balancer must be identified to Tableau Server as a trusted host. See the procedure below for how to configure Tableau Server.

• **Proxy server configurations**: The settings used to identify a load balancer to Tableau Server are the same ones that are used to identify a proxy server. If your Tableau Server cluster requires both a proxy server and a load balancer, both must use a single external URL defined in `gateway.public.host` and all proxy servers and load balancers must be specified in `gateway.trusted` and `gateway.trusted_hosts`. For more information, see Configuring Proxies for Tableau Server.

**Configure Tableau Server to work with a load balancer**

Use the following key-value pairs to configure Tableau Server for a load balancer. You can set the values individually with the `tsm configuration set` command.

Or, use the configuration file template example at the end of this topic to create a configKey json file. After you have filled in the options with the appropriate values, pass the json file and apply settings with tsm commands.

**Load balancer configuration key-value pairs**

The key-value pairs described in this section can be set with the `tsm configuration set` command. After you have set all values, run the following command:

```
  tsm pending-changes apply
```

```
gateway.public.host
  Value: name
```
The value, name is the URL that will be used to reach Tableau Server through the load balancer.

For example, if Tableau Server is reached by entering tableau.example.com in a browser address bar, enter this command:

```bash
tsm configuration set -k gateway.public.host -v "tableau.example.com"
```

gateway.public.port

**Value:** port_number

By default, Tableau assumes that the load balancer is listening on port 80 for external communications. Use this key to specify a different port.

For example, if your load balancer is configured for SSL and listening on port 443, enter the following command:

```bash
tsm configuration set -k gateway.public.port -v "443"
```

gateway.trusted

**Value:** server

Specify the load balancer(s) IPv4 address or computer name.

The value for server can be a comma-separated list, for example:

```bash
tsm configuration set -k gateway.trusted -v "10.32.139.45, 10.32.139.46, 10.32.139.47"
```

or

```bash
tsm configuration set -k gateway.trusted -v "proxy1, proxy2, proxy3"
```

gateway.trusted_hosts

**Value:**
Specify alternate names for the load balancer(s), such as its fully-qualified domain name, any non-fully-qualified domain names, and any aliases. These are the names a user might type in a browser. Separate each name with a comma:

```
tsm configuration set -k gateway.trusted_hosts -v "name1, name2, name3"
```

For example:

```
tsm configuration set -k gateway.trusted_hosts -v "lb.example.com, lb, ftp.example.com, www.example.com"
```

Configuration template example

You can configure all of the settings in one operation by customizing the following configuration template example and creating a configKey json file.

Refer to the key-value pair descriptions above to customize the values for your organization.

```
{
  "configKeys": {
    "gateway.public.host": "tableau.example.com",
    "gateway.public.port": "443",
    "gateway.trusted": "proxy1, proxy2, proxy3",
    "gateway.trusted_hosts": "lb.example.com, lb, ftp.example.com, www.example.com"
  }
}
```

When you are finished, save the json file.

Pass the json file with tsm to set the configuration, and then apply settings by running the following commands:

```
tsm settings import -f /path/to/file.json

 tsm pending-changes apply
```
For more information about using configKey schemes, see Configuration File Example.

**Deploy a Coordination Service Ensemble**

The Coordination Service is built on Apache ZooKeeper, an open-source project, and coordinates activities on the server, guaranteeing a quorum in the event of a failure, and serving as the source of "truth" regarding the server topology, configuration, and state. The service is installed automatically on the initial Tableau Server node, but no additional instances are installed as you add additional nodes. Because the successful functioning of Tableau Server depends on a properly functioning Coordination Service, we recommend that for server installations of three or more nodes, you add additional instances of the Coordination Service by deploying a new Coordination Service ensemble. This provides redundancy and improved availability in the event that one instance of the Coordination Service has problems.

- Hardware requirements
- The Coordination Service Quorum
- Deploy a new Coordination Service ensemble

**Hardware requirements**

The hardware you use for Tableau Server can have an effect on how well the Coordination Service runs. In particular:

- **Memory.** The Coordination Service maintains state information in memory. By design, the memory footprint is small, and is typically not a factor in overall server performance.

- **Disk speed.** Because the service stores state information on disk, it benefits from fast disk speed on the individual node computers.

- **Connection speed** between nodes. The service communicates continuously between cluster nodes; a fast connection speeds between nodes helps with efficient synchronization.
Because the Coordination Service is I/O intensive, if you are running Tableau Server on computers that meet or just exceed the minimum hardware requirements, you may want to configure a Coordination Service ensemble that puts the service on nodes that are not being used for other server processes. This reduces the chance of delays due to I/O contention between server processes. For information on how to deploy an ensemble on dedicated Coordination Service-only nodes, see Configure Tableau Server for High Availability with Coordination Service-Only Nodes.

The Coordination Service Quorum

To ensure that the Coordination Service can work properly, the service requires a quorum—a minimum number of instances of the service. This means that the number of nodes in your installation impacts how many instances of the Coordination Service you want to configure in your ensemble.

Number of Coordination Service instances to use

The maximum number of Coordination Service instances you can have in an ensemble on Tableau Server depends on how many Tableau Server nodes you have in your deployment. Configure a Coordination Service ensemble based on these guidelines:

<table>
<thead>
<tr>
<th>Total number of server nodes</th>
<th>Recommended number of Coordination Service nodes in ensemble (must be 1, 3, or 5)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-2 nodes</td>
<td>1 node</td>
<td>This is the default and requires no changes unless you want to move the Coordination Service off your initial node and onto your additional node.</td>
</tr>
<tr>
<td>3-4 nodes</td>
<td>3 nodes</td>
<td></td>
</tr>
<tr>
<td>5 or</td>
<td>5 nodes</td>
<td>Five is the maximum number of Coordination</td>
</tr>
<tr>
<td>Total number of server nodes</td>
<td>Recommended number of Coordination Service nodes in ensemble (must be 1, 3, or 5)</td>
<td>Notes</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>more nodes</td>
<td></td>
<td>Service instances you can install.</td>
</tr>
</tbody>
</table>

**Deploy a new Coordination Service ensemble**

If you install a total of three or more nodes, you should also deploy a Coordination Service ensemble. If you do not, you will get a warning message every time you make changes to the server configuration or topology. You can ignore this message, but as a best practice you should deploy a multi-node Coordination Service ensemble.

When you install Tableau Server, a single instance of the Coordination Service is installed on the initial node. TSM and Tableau Server depend on the Coordination Service to function properly, so to provide redundancy and ensure availability on multi-node installations, configure additional instances of the Coordination Service by deploying a Coordination Service ensemble. Coordination Service ensembles are installed with one, three, or five instances of the Coordination Service. In a three-node installation of Tableau Server, the recommended number of Coordination Service instances is three, one on each node.

Do not attempt to deploy a Coordination Service ensemble if there are other changes pending. Discard or apply any pending changes before deploying a new Coordination Service ensemble.

**Note:** This operation includes steps that you may need to perform using the TSM command line.
The following steps illustrate how to deploy a new Coordination Service ensemble on an existing three-node Tableau Server cluster and clean up the old ensemble.

1. On the initial node, open a terminal session.

2. Type this command to sign in to Tableau Server as a TSM administrator:

```bash
tsm login -u <username>
```

You will be prompted for your password.

3. Type this command to stop Tableau Server:

```bash
tsm stop
```

Some TSM processes will continue to run, including the Administration Controller and Administration Agent.

4. Confirm there are no pending changes:

```bash
tsm pending-changes list
```

If there are pending changes, you need to either discard the changes or apply them. Applying pending changes will take some time:

- Discard the changes

```bash
tsm pending-changes discard
```

or

- Apply the changes:

```bash
tsm pending-changes apply
```

Wait until the command completes and you are returned to the system prompt.

5. Get the node IDs for each node in the cluster:

```bash
tsm topology list-nodes -v
```
6. **Use the `tsm topology deploy-coordination-service` command to add a new Coordination Service ensemble by adding the Coordination Service to specified nodes. You must specify the node(s) that the Coordination Service should be added to. The command also makes the new ensemble the "production" ensemble (the ensemble in use).**

For example, deploy the Coordination Service to all three nodes of a three-node cluster, where the nodes are node1, node2, and node3:

```
 tsm topology deploy-coordination-service -n node1,node2,node3
```

7. **Wait until the new Coordination Service ensemble is running and the server is ready for the next step.**

**Important.** If you attempt to clean up the old Coordination Service ensemble before the server is in the proper state, you can put the server into an unrecoverable state and may need to completely reinstall Tableau.

a. **Check the status of the server:**

```
 tsm status -v
```

If the deployment is not complete, you may see processes showing as running when they are not, and the Coordination Service showing a status of "unavailable" while the service is synchronizing between nodes on the cluster. Tableau Server may show as being in an error state while this is happening. You may also get an error message: "Could not connect to TSM Controller at '<host>:8850'." This is normal when the server is returning to a valid state.

b. **Check the status of the server periodically until you are prompted to sign in again.**
c. When you are prompted, sign in to TSM and continue to check the server status until you see a status of "STOPPED" for each node. If the status of a node shows as "ERROR" you need to wait. When each node status is "STOPPED" you should also see the following services running:

On the initial node:

- Two instances of the Coordination Service on the initial node, both with a status of "running".
- The Administration Controller with a status of "running". (The Administration Controller is only installed on the initial node.)
- The Administration Agent with a status of "running".
- Additional services on the initial node, all with a status of "running": Service Manager, License Manager, Client File Service.

On the additional nodes:

- One or more instance of the Coordination Service on each additional node you specified when you deployed the new ensemble, all with a status of "running". If you are deploying a new ensemble to nodes that already had Coordination Service running, you will see two instances of the service.
- The Administration Agent on every node, with a status of "running".

If you do not see a status of "running" for all of the above, wait a few minutes and run the status command again.

**Note:** If there is a problem with an instance of the Coordination Service (if it shows as **stopped** for example), you can toggle back to your previous Coordination Service ensemble using the `tsm topology toggle-`
coordination-service command. To do this, the rest of the services should be in the state described above, including Administration Controller and Agent. You can toggle back to the previous ensemble only if you have not run the cleanup-coordination-service command. Tableau Server cannot be running when you use this command.

8. Remove the old ensemble. This step is required. You cannot run Tableau Server with multiple Coordination Service ensembles configured.

   tsm topology cleanup-coordination-service

   Tableau Server must be stopped when you use this command, but some TSM services will be running (see above).

9. Start Tableau Server:

   tsm start

Configure Client File Service

The Client File Service (CFS) manages most shared files in a multinode cluster. For example, authentication related certificates, keys, and files (OpenID, mutual SSL, SAML, and Kerberos), and customization files are managed by CFS.

A single instance of CFS is configured on the initial node when you first install Tableau Services Manager (TSM) and Tableau Server. You can configure additional instances on other nodes, using these limitations and recommendations:

- There must be at least one instance of CFS for any Tableau Server installation. You cannot remove all instances of CFS.
- We recommend you do not configure more than one instance on any one node. Additional instances would not provide any benefit and would be a waste of resources.
- We recommend you configure a CFS instance on each node where you deploy the Coordination Service.
This article explains how to add or remove an instance of CFS. You cannot configure CFS from the Web UI. You must use the CLI to add or remove CFS. The procedure is the same one you use for adding a process to a node.

Configure CFS on additional nodes

1. On the initial node, open a terminal session.

2. Find the node ID for the node you are updating:

   ```
   tsm topology list-nodes -v
   ```

3. Add CFS on the node by specifying the process and a single instance.
   
   For example, this command adds one instance of CFS to node1:

   ```
   tsm topology set-process -n node1 -pr clientfileservice -c 1
   ```

4. Apply the changes:

   ```
   tsm pending-changes apply
   ```

Repository Failover

In a Tableau Server installation, the repository (pgsql) database is one of the key required processes. The Tableau Server repository stores information about Tableau Server users, groups and group assignments, permissions, projects, data sources, and extract metadata and refresh information. Because it is critical to the server functioning, Tableau Server has a built-in automatic "failover" for the repository when server is installed in a distributed environment that meets certain requirements.

Automatic repository failover

Automatic repository failover means that if there is a problem with the active Tableau Server repository, the server will automatically switch to using the passive repository. This does not
happen immediately, to protect against momentary issues with the repository that don’t justify a switch, but if the repository is unavailable for more than five minutes, failover occurs.

For automatic repository failover to work, your Tableau Server installation needs:

- A minimum of three nodes
- Two instances of the repository installed

Optional but highly recommended:

- A multi-node Coordination Service ensemble deployed

With these conditions satisfied, repository failover will occur if the active repository becomes unavailable, either due to a problem with the process, or a problem with the node the process is running on. If the original repository becomes available again (if, for example, the node is restarted and all processes come up properly), it is made the passive repository, available for failover if necessary.

Manual repository failover

There may be reasons you want to shift back to the original repository after failover occurs. One reason would be if that instance of the repository is installed on a computer with more resources. To do this, use the `tsm topology failover-repository` command to manually switch back to the original repository. For more information, see `tsm topology failover-repository`.

Preferred active repository

When you configure Tableau Server you have the option to specify a node as the preferred active repository. When Tableau Server is configured for repository failover, the preferred active repository node is the one used for the active repository. This is an optional step, and if you do not specify a preferred active repository node, Tableau Server will select the active repository node on startup.
To configure the preferred active repository, use the `tsm configuration set` command to configure the `pgsql.preferred_host` option:

```
  tsm configuration set -k pgsql.preferred_host -v "<host_name>"
```

**Note:** The `host_name` is case-sensitive and must match the node name shown in the output of `tsm status -v`.

Configure a preferred active repository node if you want Tableau Server to select a specific node on startup. You might want to do this if you have a particular server you want to use for your active repository (a computer with more disk space or memory for example), or if you are using custom administrative views. Custom administrative views have embedded connection information that refers to the repository for which you created the views. For more information on connecting to the Tableau Server repository, see Collect Data with the Tableau Server Repository

**Recover from an Initial Node Failure**

The first computer you install Tableau on, the "initial node," has some unique characteristics. Two processes run only on the initial node and cannot be moved to any other node except in a failure situation, the License service (License Manager) and TSM Controller (Administration Controller). Tableau Server includes a script that automates moving these two processes to one of your other existing nodes so you can get complete access back to TSM and keep Tableau Server running.

Two other processes are initially included on the initial node but can be added or moved to additional nodes, the CFS (Client File Service) and the Coordination Service. Depending on how your installation was configured with CFS and Coordination Service, you may also need to take steps to redeploy these.

If there is a problem with the initial node and you have redundant processes on your other nodes, Tableau Server can continue to run for up to 72 hours before the lack of the licensing service impacts other processes. Your users can continue to sign in and see and use their
content after the initial node fails, but you will not be able to reconfigure Tableau Server because you won’t have access to the Administration Controller. This means you should make a point of moving the two unique processes to another of your running nodes as soon as possible. If your initial node fails for reasons that are recoverable in a relatively short amount of time (for example, a hardware failure you can correct), you should first attempt to bring the node back up without using the procedure below.

**Note:** The steps in this article require server downtime and can be disruptive, and should only be used in the event of a catastrophic failure of the initial node. If you are unable to get your initial node running again, use the following steps to move key TSM processes to another node in your cluster.

**General requirements**

- If the initial node was running the only instance of the Client File Service (CFS), you need to add that process to another node. Tableau Server requires at least one instance of the CFS. For more information, see Configure Client File Service.
- As part of the process for setting up a multi-node Tableau Server installation you should have deployed a Coordination Service ensemble. The process below assumes there was a Coordination Ensemble deployed before there was a problem with the initial node. For more information about deploying a Coordination Service ensemble, see Deploy a Coordination Service Ensemble.

**Note:** This operation includes steps that you may need to perform using the TSM command line.

**Move the TSM Controller and License Service to another node**

If there is a problem with the initial node, the TSM Controller and the Licensing Service need to be started on another node. Follow these steps to use the provided `move-tsm-controller` script and get the Controller and Licensing Service working on another node.
1. On a node that is still working, run the Controller recovery script. At a terminal prompt on a working node, type the following command:

   sudo /opt/tableau/tableau_server-/packages/scripts.<version_code>/move-tsm-controller -n <nodeID>

   where "nodeID" is the ID for the node you want the TSM Controller to run on. For example:

   sudo /opt/tableau/tableau_server-/packages/scripts.10400.17.0802.1319/move-tsm-controller -n node2

2. Verify the Administration Controller is running on the node:

   tsm status -v

3. Stop Tableau Server:

   tsm stop

4. Add the License Service to the node:

   tsm topology set-process -pr licenseservice -n <nodeID> -c 1

5. Remove the old License Service from the original node, where "nodeID" is the initial node that has failed:

   tsm topology set-process -pr licenseservice -n <nodeID> -c 0

6. If the initial node had been running the only instance of CFS, add CFS to this node:
7. (Optional) You can also add other processes that had been running on the initial node but are not running on this node. For instance, to add a cache server:

```
tsm topology set-process -pr cacheserver -n node2 -c 1
```

8. Apply the changes:

```
tsm pending-changes apply
```

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

9. Restart the TSM Administration Controller (as `tableau` system account):

```
sudo su -l tableau -c "systemctl --user restart tabadmincontroller_0.service"
```

**Note:** It may take a few minutes for tabadmincontroller to restart. If you attempt to apply pending changes in the next step before the controller has fully restarted, TSM will not be able to connect to the controller. You can verify that the controller is running by using the `tsm status -v` command. Tableau Server Administration Controller should be listed as "is running".

10. Apply pending changes (there may not appear to be any, but this step is required):

```
tsm pending-changes apply
```

11. Activate the Tableau Server license on the new Controller node:
12. Verify the license is properly activated:

   tsm licenses list

13. If the initial node was running the Coordination Service, you need to deploy a new Coordination Service ensemble that does not include that node. If you have a three node cluster and the initial node was running the Coordination Service, you must deploy a new, single-instance Coordination Service ensemble on a different node and clean up the old ensemble. In this example, a single instance of the Coordination Service is being deployed to the second node:

   tsm topology deploy-coordination-service -n <nodeID2>

   Wait until the server is completely switched over to the new ensemble.

14. When the server has switched over to the new ensemble, clean up the old ensemble.

   Important: Do not do this too soon. You must wait until the server has completely switched to the new ensemble before running the cleanup command or you can permanently break Tableau. For more information about deploying a Coordination Service ensemble, including detailed instructions for determining that the server is ready to clean up the old ensemble, see Deploy a Coordination Service Ensemble.

   tsm topology cleanup-coordination-service

15. If the initial node was running a File Store instance, you need to remove that instance:

   tsm topology filestore decommission -n <nodeID> --delete-filestore

   Where nodeID is the initial node that has failed.
16. Apply pending changes, using the `--ignore-warnings` flag if the new Coordination Service ensemble you deployed above is a single node ensemble:

```
 tsm pending-changes apply --ignore-warnings
```

17. Remove the initial node, where `nodeID` is the initial node that has failed:

```
 tsm topology remove-nodes -n <nodeID>
```

18. Apply pending changes, using the `--ignore-warnings` flag if the new Coordination Service ensemble you deployed above is a single node ensemble:

```
 tsm pending-changes apply --ignore-warnings
```

19. Start Tableau Server:

```
 tsm start
```

At this point your server should start, and you will be able to use TSM to configure it. The next step is to replace your initial node so your cluster has the original number of nodes. How you do this depends on whether or not you want to reuse the node that failed. We recommend that you only reuse that node if you are able to identify the reason it failed, and take steps to keep the failure from recurring.

20. If you plan to reuse the original node, you first need to completely remove Tableau from it. Do this by running the `tableau-server-obliterate` script. For details on doing this, see Remove Tableau Server from Your Computer.

21. On a fresh computer, or on your original computer after completely removing Tableau, install Tableau using your original Setup program and a bootstrap file generated from the node that is now running the Administration Controller and Licensing Service. This creates an additional node you can configure as part of your cluster. For details on how to add the node, see Install and Configure Additional Nodes.
A best practice is to configure any processes you lost when the original node failed, to make sure your cluster is fully redundant. You may want to move processes from your new initial node to the newly added additional node to duplicate your original configuration. For example, if your initial node was only running gateway and File Store, you may want to configure the new initial node the same way.

22. You should also redeploy a new Coordination Service ensemble, once you have your nodes up and running the way you want. For details, see Deploy a Coordination Service Ensemble.

Recover from a Node Failure

If there is a problem with one of your server nodes, and you have redundant processes on your other nodes, Tableau Server can continue to run. Your users can continue to sign in and see and use their content after the node fails, but they may experience performance degradation as a result of the failed node. In addition, your server will be at greater risk of catastrophic failure if the bad node was running processes that are no longer redundant. This means you should make a point of removing the bad node and replacing it as soon as you can. If your node fails for reasons that are recoverable in a relatively short amount of time (for example, a hardware failure you can correct), you should first attempt to bring the node back up without using the procedure below.

**Note:** If the failed node is your initial node, there are larger implications for your Tableau Server installations. For details on how to recover from the failure of an initial node, see Recover from an Initial Node Failure.

General requirements

- There is still at least one functioning node with an instance of the File Store on it.
- There is still at least one functioning node with a Repository on it.
Removing a Failed Node

To remove a failed node from a Tableau Server cluster:

1. Stop Tableau Server:

   tsm stop

2. Identify the failed node:

   tsm status -v

   The failed node will have a status of "ERROR" and processes will show as unavailable. The node ID is listed as "node<n>" with the machine name following it. For example, node3:

   node3: WIN-00915SFASVH
   Status: ERROR
   'Tableau Server Gateway 0' status is unavailable.

3. Determine any key processes that were running on the node:

   - If the failed node was running the Coordination Service, you need to deploy a new ensemble and clean up the old one before you can remove the node. Do this while Tableau Server is stopped. For detail steps, see Deploy a Coordination Service Ensemble.

   - If the failed node was running File Store, you need to force-decommission File Store and remove it before you can remove the node.
4. If the cluster was a three-node cluster and there are repositories on the remaining working nodes, you need to either remove one repository, or add a new node. This is because you are limited to a single instance of the repository when you have fewer than three nodes.

To remove one repository:
```
tsm topology set-process -n <nodeID> -pr pgsql -c 0
```

5. Run the command to remove the failed node. This adds the change to the pending changes list:
```
tsm topology remove-nodes -n <nodeID>
```

6. Verify the node removal is pending:
```
tsm pending-changes list
```

7. Apply pending changes to remove the node:
```
tsm pending-changes apply
```

8. Start Tableau Server:
```
tsm start
```

9. Install Tableau Server on a new node and configure the node with the processes that the old, failed node had been running.

10. On a fresh computer, or on your original computer after completely removing
Tableau, install Tableau using your original Setup program and a bootstrap file generated from the initial node. For details on how to do this, see Install and Configure Additional Nodes.

A best practice is to configure any processes you lost when the original node failed, to make sure your cluster is fully redundant.

11. You should also redeploy a new Coordination Service ensemble, once you have your nodes up and running the way you want. For details, see Deploy a Coordination Service Ensemble.

Configure Nodes

Use the Tableau Services Manager (TSM) Web UI or CLI commands to configure the topology of a node. The initial node is configured with a default that includes all the processes used by TSM and Tableau Server. When you add additional nodes you need to specify which processes will run on those nodes, and how many instances of those processes will run. You may also want to change the topology of the initial node, either adding instances of existing processes, or moving some of those processes to your additional nodes (this is common when setting up a distributed installation of Tableau Server).

**Note:** You cannot remove the File Store or Repository (pgsql) if this is the only instance of that process in your cluster. You must have at least one instance of each of the processes in your Tableau Server installation, and you must add the second instance and allow it to synchronize with the first before you remove the process on the original node. For more information see Move the Repository Process and Move the File Store Process.

Use the TSM web interface
In most cases, you can make multiple changes to your server configuration. Exceptions are if you are moving or removing a File Store instance or the Repository.

To configure your Tableau Server nodes using the TSM web interface, do the following:

1. Open TSM in a browser:

   https://<tsm-computer-name>:8850

   For more information, see Sign in to Tableau Services Manager Web UI.

2. Click the **Configuration** tab.

   Your next steps depend on the configuration changes you want to make.

   - **Add processes**—Add processes to a node by specifying the number of instances you want on the node, or selecting the box for the process.

     For example, to add four instances of the Backgrounder and a Gateway to a node:

     a. Select the **Gateway** box:

        ![Gateway Box](image)

     b. Set the **Backgrounder** count to 4:
Adding Backgrounder to a node will also add an instance of Data Engine if one is not already on the node.

**Note:** The TSM Web UI limits you to a maximum of 8 instances of processes that allow you to select the number of instances. To configure more instances than this, use the command line and the `TSM topology set-process` command. For more information, see `tsm topology set-process`.

- **Change process count**—Change the number of processes on a node by specifying the new number, or selecting the box for the process.

- **Remove a process completely**—Remove all instances of a process from a node by clearing the box for the process, or setting the count to 0 (zero).

In most cases you move a process from one node to another by setting the process instance count on the first node to 0 (zero), and setting the count to a non-zero value on the second node.

If you are attempting to make a configuration that is not allowed (if, for example, you try to remove a File Store that has not been decommissioned), a message displays to let you know this.

3. Click **Pending Changes** at the top right, and **Apply Changes and Restart** to
commit the changes and restart Tableau Server.

Use the TSM CLI

- Adding processes to a node
- Changing the number of processes on a node
- Removing all instances of a process from a node
- Moving all instances of a process from one node to another node

To configure nodes, run commands from the initial node and use the node ID to specify which node you are configuring. To determine the node ID, use the `tsm topology list-nodes` command. Use the `tsm topology set-process` command to add, update or remove a process on a node. You need to specify the node you are configuring, the process you are adding, updating, or removing, and the number of instances of the process. After setting the topology for a node you need to apply the changes to Tableau Server.

Apply changes using the `tsm pending-changes apply` command. After the changes are applied, Tableau Server is returned to the state it was in before the command was run. This means that if it was running, it will be restarted, and if it was stopped it will remain stopped after pending changes have been applied. In most cases, if Tableau Server is running when you apply pending changes, the server is stopped so that changes can be applied, and then restarted. The exception is if you are changing the number of instances of Backgrounder, or VizQL Server on an existing node. With changes to those processes on an existing node, Tableau Server does not have to be stopped if it is running.

You need the node ID for a node in order to configure the node. To determine the node ID, use this command:

```
tsm topology list-nodes -v
```
Note: Examples here show some process names. For a complete list, see Tableau Server Processes.

Adding processes to a node

Use the `tsm topology set-process` command to add a process to a node. You need to specify the node you are configuring, the process you are adding, and the number of instances of the process.

1. On the initial node, open a terminal session.
2. Find the node ID for the node you are changing:
   
   ```
   tsm topology list-nodes -v
   ```
3. Add processes on the node by specifying the process and the number of instances.
   
   For example, this command adds two instances of backgrounder to node1:
   
   ```
   tsm topology set-process -n node1 -pr backgrounder -c 2
   ```
4. Apply the changes:
   
   ```
   tsm pending-changes apply
   ```

Changing the number of processes on a node

Change the number of processes on a node by specifying an already configured process and providing a new value for the number of instances.

1. On the initial node, open a terminal session.
2. Find the node ID for the node you are changing:
   
   ```
   tsm topology list-nodes -v
   ```
3. Change the number of processes on the node by specifying an already configured
process and providing a new value for the number of instances.

For example, on a node (node1) that is already running backgrounder, this command changes the number of instances to four:

```
tsm topology set-process -n node1 -pr backgrounder -c 4
```

4. Apply the changes:

```
tsm pending-changes apply
```

Removing all instances of a process from a node

1. On the initial node, open a terminal session.

2. Find the node ID for the node you are changing:

```
tsm topology list-nodes -v
```

3. Remove a process from a node by specifying a count of 0 instances for that process on the node.

   For example, this command removes the backgrounder process from node1:

   ```
tsm topology set-process -n node1 -pr backgrounder -c 0
```

4. Apply the changes:

```
tsm pending-changes apply
```

Moving all instances of a process from one node to another node

In most cases you move a process from one node to another by setting the process instance count on the first node to zero, and setting the count to a non-zero value on the second node.

1. On the initial node, open a terminal session.

2. Find the node ID for the node you are changing:
Move a process from one node to another node by specifying a count of 0 instances for that process on the first node and specifying a count of 1 or greater to the second node.

For example, these commands remove Backgrounder from node0 and add two instances of it to node1:

```
tsm topology set-process -n node0 -pr backgrounder -c 0
```

```
tsm topology set-process -n node1 -pr backgrounder -c 2
```

4. Apply the changes:
```
tsm pending-changes apply
```

**Node Roles in Tableau Server**

The Backgrounder process runs server tasks, including extract refreshes, subscriptions, flow tasks, ‘Run Now’ tasks, and tasks initiated from tabcmd. Starting in 2019.1, you can configure the type of tasks that a backgrounder can perform on a node. This applies to Tableau Server installations that have more than one node where backgrounder is enabled.

The following node roles are useful if you have a Tableau Prep Conductor license for your Tableau Server Deployment. For more information, see Tableau Prep Conductor.

By default, Backgrounder is set to perform server tasks of all types. You can customize it to only run flow tasks, or run all tasks other than flows: For more information, see tsm topology.

**Install Tableau Server on a Two-Node Cluster**

When you install Tableau Server on a two-node cluster, you can install server processes on one or both nodes. A two-node cluster can improve the performance of Tableau Server, because the work is spread across multiple machines.

Note the following about two-node clusters:
• A two-node cluster does not provide failover or support for high availability.

• You can’t install more than one instance of the repository on a two-node cluster, and the repository must be on the initial node.

If you need failover or high availability, or want a second instance of the repository, you must install Tableau Server on a cluster of at least three computers. In a cluster that includes at least three nodes, you can configure two instances of the repository, which gives your cluster failover capability.

Maintain a Distributed Environment

After you set up an initial node and one or more additional nodes for a distributed installation, you can perform all subsequent configuration and updates from the initial node, using the TSM CLI, or from any computer using a browser and the TSM Web interface.

When you install additional nodes, they are added by computer name. If the computer name of a node changes, you will need to remove and reinstall the node. For details on removing a node, see Remove a Node.

You can monitor the status of the Tableau Server cluster on the TSM Status page. See View Server Process Status for details.

Additional actions you may need to maintain your distributed environment include:

Move the Repository Process

Tableau Server relies on the PostgreSQL repository to store server data. There must always be at least one active instance of the repository in any Tableau Server installation, and you can have a maximum of two instances (one active, one passive) if you have at least three nodes in your installation. You cannot remove a repository instance if it is the only instance.

This means that if you want to move the only instance of your repository from one node to another node, you need to add a second instance and synchronize the new repository with
the old one before you remove the old one. Synchronize repository instances by starting server. If you’ve added a new repository, it will automatically synchronize with the existing instance.

If you are deleting a node from your server cluster and that node is hosting the only instance of the repository, you must add a second instance of the repository and synchronize the instances before removing the node.

If you are also moving the file store, you can move the repository at the same time. See Move the File Store Process.

Before making a change to the repository, create a full backup of Tableau Server. For more information, see tsm maintenance backup.

**Important:** You cannot add a second repository instance and remove the first one in the same step. You must have both running so the contents of the first is synchronized with the second, before you remove the original instance.

The steps for moving the repository are:

1. Add a new instance of the repository to another node, start server, and wait for it to synchronize with the first repository.

2. Remove the instance of the repository from the original node.

Use the TSM web interface

To move a repository you need to first add a second instance on a second node, and then after the two instances have synchronized all the data in the original repository, remove the original instance. These steps must be done separately to allow for the synchronization of content between the two instances.
Add a new instance of the repository.

1. **Open TSM in a browser:**

   `https://<tsm-computer-name>:8850`

   For more information, see Sign in to Tableau Services Manager Web UI.

2. **Click the Configuration tab.**

3. **For the node you are adding the repository to:**

   Select **Repository** (pgsql).

4. **Click Pending Changes at the top of the page:**

   The Pending Changes list displays.

   If you are configuring a three- or five-node cluster and have not deployed a Coordination Service ensemble, a warning will display. You can continue, and deploy a Coordination Service ensemble in a separate step. For details on deploying a Coordination Service ensemble, see Deploy a Coordination Service Ensemble.

5. **Click Apply Changes and Restart and Confirm** to confirm a restart of Tableau Server.

6. **After Tableau Server has restarted, on the Status tab, verify that all processes are active.**

Remove an instance of the repository.

1. **In TSM, on the Status tab, verify that all processes are active. When both repositories show as Active, you can remove the first one.**

2. **Click the Configuration tab.**
3. For the node you’re removing the repository from, clear the Repository box.

4. Click Pending Changes at the top of the page.

   If you are configuring a three- or five-node cluster and have not deployed a Coordination Service ensemble, a warning will display. You can continue, and deploy a Coordination Service ensemble in a separate step. For details on deploying a Coordination Service ensemble, see Deploy a Coordination Service Ensemble.

5. Click Apply Changes and Restart and Confirm to confirm a restart of Tableau Server.

Use the TSM CLI

To move a repository you need to first add a second instance on a second node, and then after the two instances have synchronized all the data in the original repository, remove the original instance. These steps must be done separately to allow for the synchronization of content between the two instances.

Add a new instance of the repository.

1. Add the repository (pgsql) to another node:

   ```
   tsm topology set-process -n <nodeID> -pr postgresql -c 1
   ```

2. Apply the changes. The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

   ```
   tsm pending-changes apply
   ```

3. Wait for the new repository on the second node to synchronize with the repository on the first node.
```
tsm status -v
```

Wait until the new repository status shows as "passive".

Remove an instance of the repository.

Once the new instance of the repository is fully synchronized and shows as "passive" you can remove the original instance:

1. Remove the repository from the first node by setting the process count to 0 (zero):
   ```
tsm topology set-process -n <nodeID> -pr psql -c 0
   ```
2. Apply the change. The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.
   ```
tsm pending-changes apply
   ```

**Move the File Store Process**

You cannot remove an instance of File Store if it is the only instance on the server. You cannot run Tableau Server without at least one instance of File Store. This means if you need to move the File Store, or if you are deleting a server node that is hosting the only instance of the File Store, you must first move File Store to another node.

Moving the File Store is a two-part process:

- Adding a second instance of File Store (if there is not an existing second instance).
- Decommissioning and removing the original instance of File Store.

This article assumes you have installed Tableau Server on an initial node and at least one additional node. For more information on adding nodes to Tableau Server, see Install and Configure Additional Nodes.

Use the TSM web interface
Adding a second instance of File Store

This procedure assumes you have added an additional node. For more information on adding nodes to Tableau Server, see Install and Configure Additional Nodes.

1. Open TSM in a browser:

   https://<tsm-computer-name>:8850

   For more information, see Sign in to Tableau Services Manager Web UI.

2. Click the **Configuration** tab.

3. For the node you want to add an instance of File Store on, select **File Store**.

   Adding File Store to a node will also add an instance of Data Engine if one is not already on the node.

4. Click **Pending Changes** at the top of the page:

   ![](image)

   The Pending Changes list displays.

   A Coordination Service ensemble warning displays because you are configuring a three-node cluster. You can continue. You will deploy a Coordination Service ensemble in an upcoming step.

5. Click **Apply Changes and Restart** and **Confirm** to confirm a restart of Tableau Server.

Decommissioning and removing an instance of file store

1. In TSM, on the **Status** tab, verify that all processes are active.

2. Click the **Configuration** tab.

3. For the node you’re removing File Store from, clear the **File Store** box.
This will generate a warning about decommissioning the File Store before removing it. You cannot remove an instance of File Store unless it has been decommissioned. Click OK to decommission and remove the file store. Data Engine will also be removed unless an instance of one of these processes is installed on the node: VizQL Server, Application Server (Vizportal), Data Server, or Backgrounder.

4. Click the Status tab to see the status of the decommission. When the instance of File Store is marked "Ready for removal" you can continue.

![File Store Status](image)

5. Click Pending Changes at the top of the page.

   Note: If you are configuring a three- or five-node cluster, a Coordination Service ensemble warning will display. You can continue to apply pending changes and deploy a Coordination Service ensemble in a separate step. For information on deploying a Coordination Service ensemble, see Deploy a Coordination Service Ensemble.

6. Click Apply Changes and Restart and Confirm to confirm a restart of Tableau Server.

   Use the TSM CLI

Adding a second instance of file store

1. Create a full backup of Tableau Server. For more information, see Back up Tableau Server data.

2. Add the File Store to a second node.

   tsm topology set-process -n <nodeID> -pr filestore -c 1
The File Store is automatically added. Data engine is also added if it is not already on the node.

Apply the configuration changes:

tsm pending-changes apply

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `-ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

3. Check the status of the new file store instance.

   tsm status -v

   Wait for the new File Store to synchronize with the File Store on the first node. When synchronization is complete the new File Store has a status of "running" instead of "synchronizing".

Decommissioning and removing an instance of File Store

Once you have a second instance of File Store installed and synchronized you can decommission and remove the original instance. You must decommission the original instance before you remove it. Doing this guarantees that any unique files on the File Store node are duplicated to another file store node.

1. Decommission the original File Store:

   tsm topology filestore decommission -n <nodeID> --override

2. When the decommission command completes, remove the File Store from the node by applying the pending configuration changes. The File Store is automatically removed. Data Engine is also removed unless an instance of one of these processes is installed on the node: VizQL Server, Application Server (Vizportal), Data Server, or
Backgrounder.

```
tsm pending-changes apply
```

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

Remove a Node

If your Tableau Server installation includes a node you no longer need, you can remove it to simplify your installation, and to free up the hardware resources on that node.

Prerequisites for removing a node

There are prerequisites you must satisfy before you can remove a node from your Tableau Server cluster. If your node has one of a number of limitations, you need to address these before you can remove the node. The limitations include confirm that the node has been added with at least one process, and that the node does not include any process that is not also installed on another node.

If one of the following configuration limitations applies, you must take action before you can remove the node:

- If the node was just added using the Web UI, you need to apply pending changes before you can remove it. If you added it using the command line, you need to configure it with at least one process before you can remove it.

- If the node includes the only Repository instance, you need to move the Repository to another node. See Move the Repository Process.

- If the node is running the only instance of the File Store, you need to move the File Store to another node. See Move the File Store Process.

- If the node is running an instance of the Coordination Service, you must deploy a new
Coordination Service ensemble that does not include the node. See Deploy a Coordination Service Ensemble.

**Important:** Do not use the `tableau-server-obliterate` script to remove a node. First remove the node using the TSM UI or the `tsm topology remove-nodes` command. This leaves the rest of the cluster in a good state. Later, if you want to re-add the node to the cluster, run the `tableau-server-obliterate` script on the node to completely remove Tableau. After removing Tableau from the node, restart the computer and then re-add the node using the normal steps for adding and configuring a node. For details on running the script, see Remove Tableau Server from Your Computer.

Use the TSM web interface

1. Open TSM in a browser:

   https://<tsm-computer-name>:8850

   For more information, see Sign in to Tableau Services Manager Web UI.

2. Click the **Configuration** tab and, under the node you want to remove, click **Remove Node**:

   ![Remove Node Button]

   If a configuration limitation does not allow you to remove the node (if, for example, it includes a File Store that must first be decommissioned), a message will display letting you know this. See **Prerequisites** above for more information.
3. Click **Pending Changes** at the top right, and **Apply Changes and Restart**.

Use the TSM CLI

Use the `tsm topology remove-nodes` command to remove a node from a cluster.

To remove a node from a cluster it must have been configured with a process at some point in the past. If you added a node using the CLI and want to remove it but have not configured any processes, you must add a process on it, run the `tsm pending-changes apply` command, and then remove the node. For example, you might add one instance of Cluster Controller to the node:

```
 tsm topology set-process -n <nodeID> -pr clustercontroller -c 1.
```

If you are removing a node you added using the Web UI, the Cluster Controller process is automatically added so you do not need to add it before removing the node.

1. On the initial node, open a terminal session.

2. Find the node ID for the node you are changing:

   ```
   tsm topology list-nodes -v
   ```

3. Remove a node using the `remove-nodes` command.

   For example, to remove `node2` from an existing cluster:

   ```
   tsm topology remove-nodes --node-names "node2"
   ```

   If a configuration limitation does not allow you to remove the node (if, for example, it includes a File Store that must first be decommissioned), a message will display letting you know this. See **Prerequisites** above for more information.
4. Apply the changes:

```
tsm pending-changes apply
```

Configure Tableau Server for High Availability with Coordination Service-Only Nodes

The Coordination Service is built on Apache ZooKeeper, an open-source project, and coordinates activities on the server, guaranteeing a quorum in the event of a failure, and serving as the source of "truth" regarding the server topology, configuration, and state. The service is installed automatically on the initial Tableau Server node, but no additional instances are installed as you add additional nodes. Because the successful functioning of Tableau Server depends on a properly functioning Coordination Service, we recommend that for server installations of three or more nodes, you add additional instances of the Coordination Service by deploying a new Coordination Service ensemble. This provides redundancy and improved availability in the event that one instance of the Coordination Service has problems.

The Coordination Service can generate a large amount of I/O as it communicates with other components of the server, so if you are running Tableau Server on computers that meet or just exceed the minimum hardware requirements, you may want to install Tableau Server in a configuration that uses Coordination Service-only nodes. This means installing Coordination Service on nodes that run no other server processes, and removing Coordination Service from any nodes that are running other server processes. This procedure explains how to do this. You can also run the Coordination Service ensemble on the same nodes running other Tableau Server processes. For details on how to do that, see Deploy a Coordination Service Ensemble.

Prerequisite

Before proceeding with the procedures in this topic, complete the following prerequisites:

- Install and Configure Tableau Server - Install Tableau on your initial node.

- Install and Configure Additional Nodes - Install Tableau on at least two additional
nodes.

**Note:** This operation includes steps that you may need to perform using the TSM command line.

Deploy an ensemble on Coordination Service-only nodes

One way to accommodate the high I/O impact of the Coordination Service is to deploy an ensemble on nodes that only run the Coordination Service and the Cluster Controller. The following steps illustrate how to deploy a Coordination Service ensemble on an existing multi-node Tableau Server cluster.

**Note:** For a core-based Tableau Server license, Coordination Service-only nodes do not count against the total count of licensed cores.

1. Add additional nodes to your cluster.

   See Install and Configure Additional Nodes.

2. If you added the new nodes using the TSM CLI, you need to configure the nodes with Cluster Controller (this step is not necessary if you added the nodes using the TSM Web UI because Cluster Controller is automatically added when you add a node with the Web UI).

   On the initial node, open a terminal session.

3. Type this command to sign in to Tableau Server as a TSM administrator:

   ```
   tsm login -u <username>
   ```

   You will be prompted for your password.

4. From the initial node of the cluster, configure the new nodes with an instance of the
Cluster Controller:

```bash
tsm topology set-process -pr clustercontroller -n <node4> -c 1

 tsm topology set-process -pr clustercontroller -n <node5> -c 1

 tsm topology set-process -pr clustercontroller -n <node6> -c 1
```

5. **Apply the configuration changes.** The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

```bash
tsm pending-changes apply
```

A warning about deploying a Coordination Service ensemble displays because you have deployed a multi-node cluster. If this is the only warning, you can safely override it using the `--ignore-warnings` option to apply the configuration changes in spite of the warning.

```bash
tsm pending-changes apply --ignore-warnings
```

6. **Confirm that all nodes are up and running:**

```bash
tsm status -v
```

7. **On the initial node of the cluster, open a terminal session and type this command to stop Tableau Server:**

```bash
tsm stop
```

8. **Get the node IDs for each node in the cluster:**
Use the `tsm topology deploy-coordination-service` command to add a new Coordination Service ensemble by adding the Coordination Service to specified nodes. You must specify the node(s) that the Coordination Service should be added to. The command also switches Tableau Server to use the new ensemble.

For example, deploy the Coordination Service to three nodes of a six-node cluster:

```
  tsm topology deploy-coordination-service -n <node4,node5,node6>
```

Wait until the new Coordination Service ensemble is running and the server is ready for the next step. **This is important.**

**Important.** If you attempt to clean up the old Coordination Service ensemble before the server is in the proper state, you can put the server into an unrecoverable state and may need to completely reinstall Tableau.

a. Check the status of the server:

```
  tsm status -v
```

If the deployment is not complete, you may see processes showing as running when they are not, and the Coordination Service showing a status of "unavailable" while the service is synchronizing between nodes on the cluster. Tableau Server may show as being in an error state while this is happening. You may also get an error message: "Could not connect to TSM Controller at '<host>:8850'." This is normal when the server is returning to a valid state.

b. Check the status of the server periodically until you are prompted to sign in again.

c. When you are prompted, sign in to TSM and continue to check the server
status until you see a status of "STOPPED" for each node. If the status of a node shows as "ERROR" you need to wait. When each node status is "STOPPED" you should also see the following services running:

On the initial node:

- Two instances of the Coordination Service on the initial node, both with a status of "running".
- The Administration Controller with a status of "running". (The Administration Controller is only installed on the initial node.)
- The Administration Agent with a status of "running".
- Additional services on the initial node, all with a status of "running": Service Manager, License Manager, Client File Service.

On the additional nodes:

- One or more instance of the Coordination Service on each additional node you specified when you deployed the new ensemble, all with a status of "running". If you are deploying a new ensemble to nodes that already had Coordination Service running, you will see two instances of the service.
- The Administration Agent on every node, with a status of "running".

If you do not see a status of "running" for all of the above, wait a few minutes and run the status command again.

**Note:** If there is a problem with an instance of the Coordination Service (if it shows as stopped for example), you can toggle back to your previous Coordination Service ensemble using the `tsm topology toggle-coordination-service` command. To do this, the rest of the services...
should be in the state described above, including Administration Controller and Agent. You can toggle back to the previous ensemble only if you have **not** run the `cleanup-coordination-service` command. Tableau Server cannot be running when you use this command.

11. When the new ensemble is running properly, remove the old ensemble. This step is *required*. You cannot run Tableau Server with multiple Coordination Service ensembles configured.

    `tsm topology cleanup-coordination-service`

    Tableau Server must be stopped when you use this command.

12. Start Tableau Server:

    `tsm start`

**Add a Load Balancer**

You can enhance the reliability of Tableau Server by running gateways on multiple nodes, and configuring a load balancer to distribute requests across the gateways. Unlike the repository process, which can be active or passive, all gateway processes are active. If one gateway in a cluster becomes unavailable, the load balancer stops sending requests to it. The load balancer algorithm you choose determines how the gateways will route client requests.

**Note:** If you will be using Kerberos authentication, you need to configure Tableau Server for your load balancer before you configure Tableau Server for Kerberos. For more information, see Configure Kerberos.

Note the following as you configure your load balancer to work with Tableau Server:
Tested load balancers: Tableau Server clusters with multiple gateways have been tested with Apache and F5 load balancers.

If you are using an Apache load balancer and creating custom administrative views, you need to connect directly to the Tableau Server repository. You cannot connect through the load balancer.

Tableau Server URL: When a load balancer is in front of a Tableau Server cluster, the URL that's accessed by Tableau Server users belongs to the load balancer, not the initial Tableau Server node.

Trusted host settings: The computer running the load balancer must be identified to Tableau Server as a trusted host. See the procedure below for how to configure Tableau Server.

Proxy server configurations: The settings used to identify a load balancer to Tableau Server are the same ones that are used to identify a proxy server. If your Tableau Server cluster requires both a proxy server and a load balancer, both must use a single external URL defined in gateway.public.host and all proxy servers and load balancers must be specified in gateway.trusted and gateway.trusted_hosts. For more information, see Configuring Proxies for Tableau Server.

Configure Tableau Server to work with a load balancer

Use the following key-value pairs to configure Tableau Server for a load balancer. You can set the values individually with the tsm configuration set command.

Or, use the configuration file template example at the end of this topic to create a configKey json file. After you have filled in the options with the appropriate values, pass the json file and apply settings with tsm commands.

Load balancer configuration key-value pairs

The key-value pairs described in this section can be set with the tsm configuration set command. After you have set all values, run the following command:
tsm pending-changes apply

gateway.public.host

Value: name

The value, name is the URL that will be used to reach Tableau Server through the load balancer.

For example, if Tableau Server is reached by entering tableau.example.com in a browser address bar, enter this command:

    tsm configuration set -k gateway.public.host -v "tableau.example.com"

gateway.public.port

Value: port_number

By default, Tableau assumes that the load balancer is listening on port 80 for external communications. Use this key to specify a different port.

For example, if your load balancer is configured for SSL and listening on port 443, enter the following command:

    tsm configuration set -k gateway.public.port -v "443"

gateway.trusted

Value: server

Specify the load balancer(s) IPv4 address or computer name.

The value for server can be a comma-separated list, for example:

    tsm configuration set -k gateway.trusted -v "10.32.139.45, 10.32.139.46, 10.32.139.47"

or
Tableau Server on Linux Administrator Guide

tsm configuration set -k gateway.trusted -v "proxy1, proxy2, proxy3"

gateway.trusted_hosts

Value:

Specify alternate names for the load balancer(s), such as its fully-qualified domain name, any non-fully-qualified domain names, and any aliases. These are the names a user might type in a browser. Separate each name with a comma:

tsm configuration set -k gateway.trusted_hosts -v "name1, name2, name3"

For example:

tsm configuration set -k gateway.trusted_hosts -v "lb.example.com, lb, ftp.example.com, www.example.com"

Configuration template example

You can configure all of the settings in one operation by customizing the following configuration template example and creating a configKey json file.

Refer to the key-value pair descriptions above to customize the values for your organization.

{  
  "configKeys": {  
    "gateway.public.host": "tableau.example.com",  
    "gateway.public.port": "443",  
    "gateway.trusted": "proxy1, proxy2, proxy3",  
    "gateway.trusted_hosts": "lb.example.com, lb, ftp.example.com, www.example.com"  
  }  
}

When you are finished, save the json file.
Pass the json file with tsm to set the configuration, and then apply settings by running the following commands:

```bash
tsm settings import -f /path/to/file.json
tsm pending-changes apply
```

For more information about using configKey schemes, see Configuration File Example.

**Migrate Tableau Server from Windows to Linux**

Customers running Tableau Server on Windows can migrate to Linux by taking a backup of their existing Tableau installation and restoring it to a fresh installation on Linux. This topic describes the steps necessary to do this migration. You cannot migrate or upgrade from a beta version of Tableau Server to an officially released version.

The basic steps to migrate from Tableau Server on Windows to Tableau Server on Linux include:

1. **Step 1: Plan your migration**—Plan for your migration, including gathering all the information you'll need to be successful. During this step you should familiarize yourself with potential differences between Tableau Server on Windows and Tableau Server on Linux.

2. **Step 2: Create a backup**—Create a backup of Tableau Server on Windows.

3. **Step 3: Install Tableau Server on Linux and restore the Windows backup**—Install a fresh instance of Tableau Server on Linux in a test environment so you can test out the migration, then restore your Windows backup. The restore of your Windows backup will restore the Tableau content (users, projects, sites, workbooks and data sources), but will not restore customizations, so you will need to spend some time configuring Tableau Server on Linux to match the expectations in your organization. If
you have a multi-node installation you will need to add nodes and configure them separately.

4. **Step 4: Test Tableau Server on Linux**—Try Tableau Server on Linux to make sure content is there as you expect, and users are able to perform all the actions they do on Windows. Look specifically at any changes identified as potential differences between Tableau Server on Windows and Tableau Server on Linux. Include key stakeholders in the testing both to leverage their knowledge and to help communicate the upcoming changes.

5. **Step 5: Install Tableau Server on Linux** in your production environment and restore the Windows backup—Once you’re satisfied that Tableau Server on Linux gives you the functionality you need, install Tableau in your production Linux environment and restore the Windows backup.

**Step 1: Plan your migration**

A successful migration from Windows to Linux requires some preparation beforehand. You will need to satisfy the following requirements:

- **Identity store**: You can only restore from a backup that has the same type of identity store as the running server. For example, a backup from a server using local authentication can be restored to a Tableau Server initialized with local authentication, but a backup from a server using Active Directory authentication cannot be restored to a server initialized with local authentication. To change the identity store from a local identity store to an external identity store, see Changing the Identity Store.

- **Server administrator**: You must have password for at least one of the user accounts with Server Administrator privileges from the Tableau Server source (Windows) deployment. You must use the same user as the Server Administrator in the migrated deployment to Linux.

- **Clean installation of Tableau Server for Linux**: When you install Tableau Server on Linux later in this topic, be sure to use the same identity store type as you are using
on Windows, and do not create users or content. When you restore the Windows backup file to the Linux deployment of Tableau Server, all user data and content will be replaced from the Windows backup file.

- **Differences between Windows and Linux**: Review the differences between Tableau Server on Windows and on Linux so you are aware of them and can investigate in your test environment.

  - If you are migrating from a version of Server on Windows prior to 10.5, approach the migration like an upgrade and familiarize yourself with any changes between your existing version and 10.5 by reading What's Changed in the Server on Windows help.

  - Any custom fonts you use may need to be installed on your Linux computer, and may render differently there than on Windows.

  - Connection options for Linux are a subset of those available for Tableau Server on Windows. Review the connection types that are available and make sure the ones you need are supported.

  - TSM replaces tabadmin. Understand the TSM commands and how they compare to older tabadmin commands. For a list of tabadmin commands and their TSM equivalents, see Migrate from Tabadmin to the TSM CLI.

**Step 2: Create a backup**

The steps to create a backup depend on what version of Tableau Server on Windows you are running. If you have version 2018.1.x or earlier, you need to use tabadmin to create your backup. If you are running version 2018.2.0 or later, you use TSM to create the backup.

**Migrate from 2018.1 or earlier**

If you are migrating from Tableau Server on Windows version 2018.1.x or earlier:
Tableau Server on Linux Administrator Guide

1. Log on to the computer running Tableau Server on Windows.

2. Open a command prompt as an administrator.

3. Navigate to the bin directory. For example:

   ```
   cd "C:\Program Files\Tableau\Tableau Server\10.4\bin"
   ```

   Run the following command:

4. `tabadmin backup tabserver -v -d`

   Include the `-v` flag to verify the integrity of the backup. Include the `-d` flag to include the date in the file name. In the example, `tabserver` will be used as the base file name of the resulting backup file. The date of the backup will be appended to the file name, for example `tabserver-2017-12-20.tsbak`.

For more information, see Back Up Tableau Server Data in the Tableau Server on Windows help (version 2018.1).

Migrate from 2018.2 or later

If you are migrating from Tableau Server on Windows version 2018.2.0 or later:

1. Log on to the computer running Tableau Server on Windows.

2. Open a command prompt as an administrator.

3. Run the following command:

   ```
   tsm maintenance backup -f <filename> -d
   ```

   Include the `-d` flag to include the date in the backup file name.

For more information, see Back up Tableau Server data in the Tableau Server on Windows help.
Step 3: Install Tableau Server on Linux and restore the Windows backup

In a test environment, install Tableau Server on Linux:

- Install Tableau Server for Linux according to the procedure, Install and Configure Tableau Server. Use the same identity store as on your Windows deployment, and do not create users or content.

Restore the Tableau Server on Windows backup:

1. Copy the Windows backup file to the computer running Tableau Server on Linux. By default the restore process will look for the file in this location:

/var/opt/tableau/tableau_server/data/tabsvc/files/backups/

You can change the location. For more information, see tsm File Paths.

2. Run the following command to stop Tableau Server:

   tsm stop

3. Run the following command to restore from the backup file:

   tsm maintenance restore -f <filename.tsbak>

   Where <filename.tsbak> is the name of your backup file, for example, tabserver-2017-10-20.tsbak.

   For more information, see tsm maintenance restore

4. Run the following command to start Tableau Server:

   tsm start

After restoring your Tableau content, you may need to configure Tableau Server. For example, if you are migrating from a multi-node installation, you will need to add and configure the additional nodes. You will also need to configure any customizations you made on Windows, including copying over image or logo files if applicable.
Step 4: Test Tableau Server on Linux

Once you've installed Tableau Server on Linux and restored your Windows backup, you can test the new version of Tableau Server. Because the restore process only restores content to Tableau, you may need to update configuration, topology (adding additional nodes for example), and any customizations you have on your Windows installation.

You'll want to be familiar with the known differences between Windows and Linux, as well as any potential problem areas. Test basic functionality, along with any special aspects of server that your organization relies on. For example, there may be key data sources that your organization uses with Tableau. Test these to make sure you're seeing what you expect.

These are some areas of testing to consider:

- **User access.** Confirm that Tableau Server users, including administrators, can sign in. Test your normal user sign in process. Have some of your users participate in the testing to make sure they are able to sign in as expected, and that they can get to the same content that they have access to in your production environment.

- **Viewing built-in administrative views.** With this release of Tableau Server on Linux, you must install PostgreSQL drivers manually, and the administrative views depend on these. Confirm that you have installed the drivers necessary by accessing the built-in administrative views. For more information, see Administrative Views.

- **Data source availability.** Tableau Server on Linux supports a subset of the data sources on Tableau Server on Windows. You need to confirm that the data sources used by your organization are supported on Linux, and install any drivers required. For details on which data sources are supported, see the Tableau Server tech specs. For information about installing drivers, see Database Drivers.

- **Access to file-based data sources on shared drives.** Data sources such as Excel files on network drives will require special actions in order to be accessible from Linux. You or your IT department will need to mount the drives and update any workbooks
using these data sources. For more information on connecting to network drives, see the Tableau Community.

- **Viewing published workbooks.** Have users who are familiar with the content try to view published workbooks to make sure they appear as expected. Test views embedded in web pages (for example, in SharePoint pages). Be especially aware of how fonts may differ between Windows and Linux, and some custom fonts may need to be added to your Linux computer, or replaced with other fonts if they are not available on Linux. Dashboard layouts may appear different as well, due to differences in fonts.

- **Server processes.** Sign in to Tableau Server as a server administrator, and then open the Server Status page to confirm that all services and processes are running as expected. Be aware of intentional changes due to changes in version 10.5. For more information, see Tableau Server Data Engine.

- **Publishing workbooks and data sources.** Have users publish workbooks and data sources from Tableau Desktop to make sure this goes as you expect. You may need to install drivers to support the data source connections you are using. See Database Drivers.

- **Subscriptions and extract refreshes.** Manually run some extract refreshes to confirm that they complete successfully. Run some key scheduled extract refreshes to confirm that they complete as expected.

- **Permissions.** Confirm that permissions are still set as expected for users and content.

- **Command-line utilities and APIs.** If applicable, test the command line utilities (tsm and tabcmd) and programmatic access via APIs. With Tableau Server on Linux, tabadmin is replaced by TSM. For more information, see Migrate from Tabadmin to the TSM CLI.
Step 5: Install Tableau Server on Linux in your production environment and restore the Windows backup

When you have completed testing and have identified those areas that require additional changes on your part, or communication to your users, you are ready to install Tableau Server on Linux in your production environment and restore the Windows backup. To do this, follow the same steps described above.

**Important:** If you are migrating from Tableau Server version 2018.1 or earlier on Windows - You can take a backup from Tableau Server on Linux and restore that backup to Tableau Server on Windows version 2018.2 or later, but you cannot restore that backup to Tableau Server on Windows version 2018.1 or earlier. This means that if you migrate to Linux, you cannot easily switch back to Tableau Server on Windows version 2018.1 or earlier. Keep this in mind as you test your migration, and consider keeping your installation on Windows until you are certain that you no longer need it.

**Test Workbook Performance**

In most cases, you can expect to see similar or better performance after upgrading your Tableau Server from versions 10.4 or earlier to 10.5 or later. However, for workbooks that use complex calculations, you may see performance issues after you upgrade. This article describes how to test performance and troubleshoot these performance issues before you upgrade your production Tableau Server from versions 10.4 and earlier to 10.5 or later.

If you have already upgraded your production Tableau Server to 10.5 or later, and you are seeing performance issues for workbooks that have calculations and use extracts as the data source, see Troubleshoot Performance of Workbooks with Calculations.

Since Linux was first released in 10.5, this only applies when you are migrating from Tableau Server versions 10.4 or earlier on Windows to Linux 10.5 or later.
To make sure your workbook performance is same or better after your upgrade to Tableau 10.5 or later, we strongly recommend that you set up a test environment and do performance testing before you upgrade your production Tableau Server.

Use the following sequence of steps for testing workbook performance:

1. **Set up your test environment**
2. **Capture performance metrics and analyze**
3. **Troubleshoot performance issues**
4. **Capture the conclusions and results**

**Set up your test environment**

1. Create a test environment that mirrors your production environment as closely as possible.
   
   Follow the steps described in Migrate Tableau Server from Windows to Linux.

2. Disable any automated or scheduled extract refresh schedules.

**Capture performance metrics and analyze**

1. Run Tabjolt or any other tool of your choice to capture performance metrics on your current version of Tableau Server to set a baseline. Use workbooks that have calculations and use extracts as the data source for testing. For more information about how install and use Tabjolt, see the Tabjolt Installation Guide.

2. Perform a full backup to capture the metrics from the first step.

3. Upgrade your test environment to 10.5.3 or later. We are recommending 10.5.3 as the minimum version since the settings you need to enable in order to resolve performance issues later on are only available in 10.5.3 or later versions of Tableau.

4. **Checkpoint:** Run Tabjolt to compare workbook performance before and after
If you see performance degradation after upgrade at this step, it may be due to other Tableau Server issues and might require further investigations. For more information, see Record and Analyze Workbook Performance.

If you see no difference in performance before and after upgrade, continue to the next step.

5. Select a subset of workbooks and run a full refresh of the extracts. Doing a full refresh will upgrade the extracts from .tde to .hyper.

6. **Checkpoint:** Run the tool again to compare the performance of your workbooks between step 4 and step 6 which is essentially before and after doing extract refreshes. Specifically, check for workbooks with slower response times or failure to load.

**Troubleshoot performance issues**

If you find that you are unable to test due to performance issues, or you find that VizQL server is consuming all or most of the available memory on the machine while viewing them, follow **steps 1 through 3**.

For workbooks that load successfully, but have slower response after upgrade, follow **steps 4 and 5**.

1. Enable the following setting that checks the number of query nodes required for Tableau to generate the workbook and displays an error when the set limit is exceeded. This helps prevent VizQL process from consuming the memory resources on the machine that might result in critical Server issues:

   Use TSM CLI to run the following commands:

   ```bash
   tsm configuration set -k native_api.node_limit_checker_pre_rewrite_disable -v false
   tsm pending-changes apply
   ```
2. Test the workbooks by viewing or interacting with them. You should see an error message informing you about exceeding the node limits on workbooks that have performance issues - The error message might say something like: "Logical Query tree has 2348182 nodes, maximum number allowed is 1000000...."

3. Use Tableau Desktop to troubleshoot your workbook performance. Run this command to enable the node limit check in your Tableau Desktop:

```cmd
tableau.exe -DNodeLimitCheckerPreRewriteDisable=false
```

**Note:** This setting is only available in Tableau Desktop 10.5.3 or later.

In Tableau Desktop, download and open the workbooks that displayed the error message about high node limits in step 2. Try optimizing the performance of workbooks using methods described in the Best Practices for Creating Calculations in Tableau topic. If successful, then publish them to Tableau Server. If you are still experiencing performance issues, continue to the next step.

4. For workbooks that load successfully, but the overall response times is slower after upgrade, materialize calculations for your extract:

**Using Tabcmd:**

```bash
tabcmd refreshextracts --workbook "My Workbook" --addcalculations
```

For more information, Compute Calculations Now option.
5. If you have a large number of workbooks that fall under the above category (overall response times is slower after upgrade), consider enabling the server wide setting to retain materialized calculations for all extracts when they are upgraded from .tde to .hyper:

**Using TSM CLI:**

```bash
 tsm configuration set -k native_api.preserve_calculations_on_hyper_refresh_conversion -v true
 tsm pending-changes apply
```

**Considerations for turning on this setting:**

Turn this setting on only if majority of your workbooks require calculations to be materialized. There are resource and time costs associated with this setting, as described below:

- When this setting is set to true, the extract file size will increase, affecting the overall disk space.

- Extracts with materialized calculations take a longer time to refresh than extracts without materialized calculations.

This setting only affects extracts that are not yet upgraded to .hyper. Extracts already upgraded to .hyper before turning on this setting will not have the calculations materialized. This setting will also not affect workbooks and extracts published from Tableau Desktop, or any new extract refreshes published to Tableau Server that do not use the **Compute Calculations Now** option.

**Note:** This setting is only available in Tableau Server 10.5.3 or later.

6. Enable the extract refresh schedules and monitor the performance of your workbooks to make sure that your workbooks are performing as expected.
Capture the conclusions and results from your testing

Make a note of the settings and steps that helped resolve the performance issues to use them to prevent performance degradation when you upgrade your Production Tableau Server.

For example, if during your testing, you found that you needed to set the `native_api.preserve_calculations_on_hyper_refresh_conversion` setting to true, remember to disable your extract refreshes just before you upgrade your production Tableau Server.

After upgrade, set the `native_api.preserve_calculations_on_hyper_refresh_conversion` setting to true, and then re-enable your extract refreshes after you have confirmed that you are not experiencing slow response times after upgrade.

Migrate from Tabadmin to the TSM CLI

The Tableau Services Manager (TSM) command-line interface (CLI) replaces the tabadmin CLI in Tableau Server on Linux, and in Tableau Server on Windows version 2018.2. This page maps tabadmin commands to TSM commands to help you to migrate to the TSM CLI.

To learn more about the TSM CLI, see tsm Command Line Reference.


Tabadmin commands with a corresponding TSM CLI command

The following table shows which tabadmin commands correspond to commands available in the TSM CLI.

<table>
<thead>
<tr>
<th>Command Description</th>
<th>Tabadmin Command(s)</th>
<th>Comparable TSM CLI Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function</td>
<td>Command 1</td>
<td>Command 2</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>----------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Activate a license</td>
<td><code>tabadmin activate --activate</code></td>
<td><code>tsm licenses activate</code></td>
</tr>
<tr>
<td>Deactivate licenses</td>
<td><code>tabadmin activate --return</code></td>
<td><code>tsm licenses deactivate</code></td>
</tr>
<tr>
<td>Activate a trial license</td>
<td><code>tabadmin activate --trial</code></td>
<td><code>tsm licenses activate --trial</code></td>
</tr>
<tr>
<td>Create a backup of the data managed by Tableau Server</td>
<td><code>tabadmin backup</code></td>
<td><code>tsm maintenance backup</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>A backup created using TSM does not include any server configuration data. There is no option to include server configuration data.</td>
</tr>
<tr>
<td>Clear the server cache</td>
<td><code>tabadmin clearcache</code></td>
<td><code>tsm maintenance cleanup -r</code></td>
</tr>
<tr>
<td>Clean up temporary files and old log files</td>
<td><code>tabadmin cleanup</code></td>
<td><code>tsm maintenance cleanup</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> This command was added in version 10.5.1</td>
</tr>
<tr>
<td>Update the server configuration with any changes you’ve made</td>
<td><code>tabadmin configure</code></td>
<td><code>tsm pending-changes apply</code></td>
</tr>
<tr>
<td>Customize the server name and logos</td>
<td><code>tabadmin customize</code></td>
<td><code>tsm customize</code></td>
</tr>
<tr>
<td>Enable access to the repository</td>
<td><code>tabadmin dbpass</code></td>
<td><code>tsm data-access repository-access enable</code></td>
</tr>
<tr>
<td>Task</td>
<td>Command Line</td>
<td>TSM Command</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Disable access to the repository</td>
<td><code>tabadmin dbpass --disable</code></td>
<td><code>tsm data-access repository-access disable</code></td>
</tr>
<tr>
<td>Set a file store instance to read-only mode</td>
<td><code>tabadmin decommission</code></td>
<td><code>tsm topology filestore decommission</code></td>
</tr>
<tr>
<td>Delete one or more Web Data Connectors (WDCs) from Tableau Server</td>
<td><code>tabadmin delete_web-dataconnector</code></td>
<td><code>tsm data-access web-data-connectors delete</code></td>
</tr>
<tr>
<td>Add a Web Data Connector (WDC) to Tableau Server</td>
<td><code>tabadmin import_web-dataconnector</code></td>
<td><code>tsm data-access web-data-connectors add</code></td>
</tr>
<tr>
<td></td>
<td>and</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>tabadmin whitelist_web-dataconnector</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> TSM does not support importing WDCs, instead it lets you add WDCs to a safe list (or &quot;whitelist&quot;). To learn more, see Web Data Connectors in Tableau Server.</td>
<td></td>
</tr>
<tr>
<td>List Web Data Connectors (WDCs) used by Tableau Server</td>
<td><code>tabadmin list_web-dataconnectors</code></td>
<td><code>tsm data-access web-data-connectors list</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>To learn more, see Web Data Connectors in Tableau Server.</td>
</tr>
<tr>
<td>Export a site from Tableau Server</td>
<td><code>tabadmin exportsite</code></td>
<td><code>tsm sites export</code></td>
</tr>
<tr>
<td>Initiate a repository failover</td>
<td><code>tabadmin fail</code></td>
<td><code>tsm topology failover-</code></td>
</tr>
<tr>
<td>Feature</td>
<td>Command 1</td>
<td>Command 2</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>Get a configuration option</td>
<td>tabadmin get</td>
<td>tsm configuration get</td>
</tr>
<tr>
<td>Get the OpenID redirect URL</td>
<td>tabadmin get_openid_redirect_url</td>
<td>tsm authentication openid get-redirect-url</td>
</tr>
<tr>
<td>Import site .csv files into Tableau Server</td>
<td>tabadmin importsite</td>
<td>tsm sites import</td>
</tr>
<tr>
<td>Import a site into Tableau Server using .csv files</td>
<td>tabadmin importsite_verified</td>
<td>tsm sites import-verified</td>
</tr>
<tr>
<td>Display license information for Tableau Server</td>
<td>tabadmin licenses</td>
<td>tsm licenses list</td>
</tr>
<tr>
<td>Note: For more information about the output of this command, see View Server Licenses.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Move a file store from read-only mode to an active read/write state</td>
<td>tabadmin recommission</td>
<td>tsm topology filestore recommission</td>
</tr>
<tr>
<td>Regenerate internal security tokens</td>
<td>tabadmin regenerate_internal_tokens</td>
<td>tsm security regenerate-internal-tokens</td>
</tr>
<tr>
<td>Register Tableau Server</td>
<td>tabadmin register</td>
<td>tsm register</td>
</tr>
<tr>
<td>Task</td>
<td>Command</td>
<td>TSM Command</td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
<td>------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Rebuild the search index for Tableau Server</td>
<td><code>tabadmin reindex</code></td>
<td><code>tsm maintenance reindex-search</code></td>
</tr>
<tr>
<td>Reset the Tableau Server administrator account</td>
<td><code>tabadmin reset</code></td>
<td><code>tsm reset</code></td>
</tr>
<tr>
<td><strong>Note:</strong> Added in version 2018.1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stop and restart all Tableau Server processes</td>
<td><code>tabadmin restart</code></td>
<td><code>tsm restart</code></td>
</tr>
<tr>
<td>Restore from a Tableau Server backup file</td>
<td><code>tabadmin restore</code></td>
<td><code>tsm maintenance restore</code></td>
</tr>
<tr>
<td><strong>The restore command does not restore any server configuration data. This is true whether you are using a backup created with TSM or a backup created with tabadmin.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set a configuration option</td>
<td><code>tabadmin set</code></td>
<td><code>tsm configuration set</code></td>
</tr>
<tr>
<td>Activate or suspend a site</td>
<td><code>tabadmin sitestate</code></td>
<td><code>tsm sites unlock</code></td>
</tr>
<tr>
<td>Start all Tableau Server processes</td>
<td><code>tabadmin start</code></td>
<td><code>tsm start</code></td>
</tr>
<tr>
<td>Get the status of Tableau</td>
<td><code>tabadmin status</code></td>
<td><code>tsm status</code></td>
</tr>
</tbody>
</table>
### Server and server processes

<table>
<thead>
<tr>
<th>Command</th>
<th>Tabadmin Command</th>
<th>TSM CLI Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop all Tableau Server processes</td>
<td><code>tabadmin stop</code></td>
<td><code>tsm stop</code></td>
</tr>
<tr>
<td>Create an archive (.zip) file with Tableau Server log files</td>
<td><code>tabadmin ziplogs</code></td>
<td><code>tsm maintenance ziplogs</code></td>
</tr>
</tbody>
</table>

---

### Tabadmin commands with no corresponding TSM CLI command

The following table lists the `tabadmin` commands for which a comparable TSM CLI command is not available.

<table>
<thead>
<tr>
<th>Command Description</th>
<th>Tabadmin Command</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add or remove a user from the system administrator group</td>
<td><code>tabadmin administrator</code></td>
<td>You can use the Tableau Server REST API <a href="https://software.tableau.com/docs/current/api/server/administration.html#AddUserToGroup">Add User to Group</a> and <a href="https://software.tableau.com/docs/current/api/server/administration.html#RemoveUserFromGroup">Remove User from Group</a> methods to add or remove a user from the system administrator group.</td>
</tr>
<tr>
<td>Create a new key to encrypt sensitive information stored in the repository</td>
<td><code>tabadmin assetkeys</code></td>
<td>Use the <code>tsm security regenerate-internal-tokens</code> command to create or regenerate secrets and master keys.</td>
</tr>
<tr>
<td>Specify whether Tableau Server starts at system</td>
<td><code>tabadmin autostart</code></td>
<td>Tableau Server returns to the state it was in prior to a system restart. If it was running, it will...</td>
</tr>
<tr>
<td>start-up time</td>
<td>restart. If it was stopped it will be stopped after the system starts.</td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Identify a second server node for backup</td>
<td><img src="https://example.com" alt="" />tabadmin fail-overprimary</td>
<td>TSM does not have primary nodes, so a TSM equivalent to this command is not needed.</td>
</tr>
<tr>
<td>Manage credentials for delegated data access on Tableau Server</td>
<td>tabadmin manage_global_credentials</td>
<td>We recommend that you use Kerberos delegation to Apache Impala for global credential management. To learn more, see Kerberos and Enable Kerberos Delegation for Hive/Impala in the Tableau Community.</td>
</tr>
<tr>
<td>Reset the password for a Tableau Server account</td>
<td>tabadmin passwd</td>
<td>If your server uses local authentication, you can use the Tableau Server REST API Update User method to reset the password for a user account.</td>
</tr>
<tr>
<td>Reset binding between Tableau Server user ID and Open ID Connect identity provider</td>
<td>tabadmin reset_openid_sub</td>
<td></td>
</tr>
<tr>
<td>Determine whether your environment meets the minimum requirements to run Tableau Server</td>
<td>tabadmin validate</td>
<td></td>
</tr>
</tbody>
</table>
Verify that a backup of the Tableau Server repository will restore successfully

```
  tabadmin verify_database
```

The `tsm maintenance backup command` automatically verifies that a backup will restore correctly unless you use the `--skip-verification` parameter.

Prepare VizQL processes for fast load times after a Tableau Server restart

```
  tabadmin warmup
```

The `tabadmin warmup command` is no longer necessary, as Tableau Server is now optimized to automatically provide fast load times after a server restart.

---

**Uninstall Tableau Server**

Do not uninstall Tableau before upgrading. For details on upgrading, see Upgrade Tableau Server on Linux.

You can have multiple versions of Tableau Server installed at the same time. This allows you to run most of an upgrade while an existing version is running, and reduces downtime and impact to users. Once you have upgraded, you can uninstall your previous version. Doing this frees up disk space. You do not have to uninstall the previous version.

This article explains how to uninstall previous versions, after you've upgraded to a newer version.

**Uninstalling and completely removing Tableau Server**

There are two primary "uninstall" scenarios that Tableau Server on Linux supports:
• **Uninstall Tableau Server:** *After you upgrade* to a new version of Tableau Server you can uninstall your previous version to free up disk space. Continue reading for information about uninstalling Tableau.

• **Remove Tableau Server:** If you want to complete remove Tableau Server from a computer, you can use a script provided by Tableau to remove Tableau Server and all related files. *This removes all data as well as server components, so should only be done if you know you want to reset the computer to a pre-Tableau state.* You might need to do this if Technical Support recommends this step when troubleshooting an installation problem. We recommend you create a backup of your data before removing Tableau. Save the backup file to a safe location on a computer that is not part of your Tableau installation. Completely remove Tableau Server without uninstalling any version first. The script will uninstall all existing versions found on the computer. If you have already uninstalled your existing version and now want to completely remove Tableau, you can find the script to do so in a temporary location. For more details, see Remove Tableau Server from Your Computer.

### Uninstall a Tableau Server package

Use this procedure to free up disk space by uninstalling packages for previous Tableau Server versions after you have upgraded to a newer version of Tableau Server.

1. Look at the environment.bash file to confirm which version of Tableau Server is currently in use. At a command prompt, type:

   ```bash
grep TABLEAU_SERVER_DATA_DIR_VERSION /etc/-opt/tableau/tableau_server/environment.bash
   ```

2. Determine which versions of the Tableau Server package are installed on your computer.

   • On RHEL-like distributions, including CentOS, run the following command:

   ```bash
yum list installed tableau-server"*"
   ```
On Ubuntu, run the following command:

```bash
apt list --installed tableau-server"*"
```

3. Remove the Tableau Server package with your package manager.

- On RHEL-like distributions, including CentOS, run the following command:
  ```bash
  sudo yum remove tableau-server-<version>.x86_64
  ```
- On Ubuntu, run the following commands:
  ```bash
  sudo apt-get purge tableau-server-<version>_amd64
  ```

**Reinstall a Tableau Server package that was accidentally uninstalled**

Do *not* uninstall the package for your currently running version of Tableau Server. Doing so will make the server unusable. To completely remove Tableau Server and all its files, see Remove Tableau Server from Your Computer.

When you uninstall the Tableau Server package for the current instance of Tableau Server the following operations run:

- All files under `/opt/tableau/tableau_server` are removed. These files are the unmodified installation files.
- Tableau Server services are stopped and disabled
- Service files for all Tableau Server services are persisted
- Data files are left in place

If you accidentally uninstall the package for your currently running version of Tableau Server, follow this procedure to correct the situation.

To reinstall after uninstalled the running instance of Tableau Server:

1. Reinstall the package for the version you accidentally uninstalled.
2. Run `initialize-tsm`.
Remove Tableau Server from Your Computer

**Warning:** The steps below completely remove Tableau Server on Linux, and delete users and groups created by initialize-tsm, all related data, configuration information, and logs. This includes any files in /tmp or /var/tmp that are owned by users configured in /etc/opt/tableau/tableau_server/environment.bash as privileged and unprivileged users (by default, tsmagent and tableau). Tableau Server licenses are also deactivated, unless you omit the -l option when running the command shown below.

If you want to uninstall a particular Tableau Server package to free up disk space (after upgrading, for example), see Uninstall Tableau Server.

As part of the regular installation of Tableau Server, a script is installed that provides you a way to completely remove Tableau and all associated files from your computer. This is something you would only do if you did not care about your Tableau data, configuration, or log files, or if you are working with Tableau Technical Support and need to reinstall Tableau Server after an installation or upgrade attempt fails. The obliterate script will not remove any drivers you installed separately, even those you installed to use with Tableau Server.

The `tableau-server-obliterate` script is intended for when you want to completely remove Tableau Server from your computer. You might want to do this for a couple of different reasons:

- You no longer want Tableau Server installed on the computer. Use the `tableau-server-obliterate` script to remove Tableau Server completely. If this is the case, you can include a -l option to deactivate the Tableau Server license.

- Troubleshooting Tableau Server installation problems—If you run into issues installing Tableau, you may need to use the `tableau-server-obliterate` script to completely remove Tableau Server from your computer before reinstalling. Doing this will clean up any older settings or states (such as the
The intent of the `tableau-server-oblitrate` script is to completely remove Tableau Server from your computer. This includes files, system settings and configurations, and, if you specify, licensing information.

Note: An older version of `tableau-server-oblitrate` may miss files from new versions of Tableau Server. As a best practice you should always run the obliterate script from the most recent version of Tableau you installed.

When you run `tableau-server-oblitrate`, the following steps are taken:

- Uninstall is run for all installed versions of Tableau Server (yum erase or apt-get remove).
- All contents of the data directory is removed (by default `/var/-opt/tableau/tableau_server`).
- All semaphores and shared memory segments are deleted.
- All temp files owned by the “tableau” user are deleted from `/tmp` and `/var/tmp`.
- All users and groups created during install are deleted.
- `/etc/opt/tableau` is deleted.
Trusted certificates are removed from /etc/pki/ca-trust/source/anchors/TableauServer and /usr/share/ca-certificates/tableau

Configuration files are removed from:
- /etc/sysctl.d/99-tableau-server.conf
- /etc/profile.d/tableau_server*
- /etc/security/limits.d/99-tableau_server*
- /usr/share/systemd/logind.conf.d/tableau_server*
- /usr/share/bash-completion/completions/tsm
- /etc/bash_completion.d/tsm
- /usr/share/bash-completion/completions/tabcmd
- /etc/bash_completion.d/tabcmd
- /run/tableau
- /usr/lib/tmpfiles.d/tableau-server.conf

All server licenses (except trial licenses) are deactivated if you use the -l option.

Running the tableau-server-oblitrate script

You can completely remove Tableau Server from a computer, either preserving the licensing information, or removing the licensing information along with all other aspects of Tableau Server. You might want to preserve licensing if you are going to reinstall Tableau Server on the computer.

To completely remove Tableau Server without removing server licensing:

1. On the initial node, open a terminal session.

2. Run the tableau-server-obliterate script:

   ```
   sudo /opt/tableau/tableau_server-
packages/scripts.<version_code>/tableau-server-obliterate
   -y -y -y
   ```

   **Note:** If you have already uninstalled Tableau Server and now you want to remove it, run the copy of the tableau-server-obliterate script located...
in the /var/tmp directory. If the script is not in that directory, reinstall the Tableau Server package and then run the tableau-server-obliterate script.

If you have a multi-node (distributed) installation of Tableau Server, run the tableau-server-obliterate script on each node in the cluster.

3. Restart each computer you ran the tableau-server-obliterate script on.

To completely remove Tableau Server and licensing:

1. On the initial node, open a terminal session.

2. Deactivate any active product keys.

   tsm licenses deactivate -k <product_key>

3. Run the tableau-server-obliterate script:

   sudo /opt/tableau/tableau_server/packages/scripts.<version_code>/tableau-server-obliterate -y -y -y -l

   The -l option removes all licensing files from the computer. The script first attempts to deactivate any active licenses, but it will remove all licensing information whether or not deactivation was successful. This is why we recommend you run the tsm licenses deactivate command before running the obliterate script.

   **Note:** If you have already uninstalled Tableau Server and now you want to remove it, run the copy of the tableau-server-obliterate script located in the /var/tmp directory. If the script is not in that directory, reinstall the Tableau Server package and then run the tableau-server-obliterate script.
If you have a multi-node (distributed) installation of Tableau Server, run the `tableau-server-obliterate` script on each node in the cluster. You do not need to deactivate licenses on any additional nodes.

4. Restart each computer you ran the `tableau-server-obliterate` script on.

Upgrade Tableau Server Overview

The articles in this section help you upgrade an existing installation of Tableau Server. They describe the recommended steps of planning and testing before actually performing the upgrade. There's information about best practices, and when you're ready to actually perform your upgrade, steps for upgrading a single node server and a multi-node installation. Where possible, we call out possible pitfalls and help you to avoid these.


**Important:** Your upgrade steps depend on which version you are upgrading from. When you are ready to actually upgrade, be sure you follow the procedure that applies to your installation:

- Upgrading from Tableau Server on Linux version 10.5 (10.5.0 or later) requires special steps. If you are upgrading from version 10.5, use the Upgrade Tableau Server on Linux from 10.5 procedure.

- Upgrading from Tableau Server on Linux version 2018.1 or later is more straightforward. If you are upgrading from version 2018.1.0 or later, follow the steps in Upgrade Tableau Server on Linux.

For instructions on how to determine your version of Tableau Server, see View Server Version.
Upgrade Tableau Server on Linux

The articles in this section help you upgrade and existing installation of Tableau Server. They describe the recommended steps of planning and testing before actually performing the upgrade. There’s information about best practices, and when you’re ready to actually perform your upgrade, steps for upgrading a single node server and a multi-node installation. Where possible, we call out possible pitfalls and help you to avoid these.

Important: Your upgrade steps depend on which version you are upgrading from. When you are ready to actually upgrade, be sure you follow the procedure that applies to your installation:

- Upgrading from Tableau Server on Linux version 10.5 (10.5.0 or later) requires special steps. If you are upgrading from version 10.5, use the Upgrade Tableau Server on Linux from 10.5 procedure.

- Upgrading from Tableau Server on Linux version 2018.1 or later is more straightforward. If you are upgrading from version 2018.1.0 or later, follow the steps in Upgrade Tableau Server on Linux.

For instructions on how to determine your version of Tableau Server, see View Server Version.


Research the Upgrade

Before you upgrade Tableau Server, we recommend that you plan the upgrade.
• Learn about the new version of Tableau Server, including what's new and what's changed.
  • Search for "What's New" in the Tableau Server on Linux Help.

• Make sure the computers you are going to upgrade (both for the test environment and the production environment) meet the minimum hardware requirements. Minimum requirements and recommendations can change from version to version.
  • Minimum Hardware Requirements and Recommendations for Tableau Server

You may need to allocate additional disk space depending on the various factors like whether or not you will be using extracts. For more information, see Disk Space Requirements.

**Important:** As a best practice, you should never install a beta version of Tableau Server in your production environment. You should also never restore a production Tableau Server installation using a backup of a beta version.

• Confirm licensing requirements

The computers you are going to upgrade (both for the test environment and the production environment) must meet these licensing requirements:

• Trial licenses—When upgrading from one major version to another (version 10.x to version 2018.x for example), you must have a valid license. You cannot directly upgrade to a new major version if your server is running a trial license. If you have a trial license and want to upgrade to a new major version, follow these steps:
  1. Backup of your existing Tableau Server. For details, see Back up Tableau Server data.
  2. Install the new Tableau Server version on a separate computer and
activate a trial license.

3. Restore your backup to the new version. For more information, see Restore from a backup.

- Expired maintenance—You should not upgrade your server if your maintenance is expired. If you attempt to upgrade a server with expired maintenance the upgrade may fail, or, if it succeeds, may result in an unlicensed server. You can refresh your maintenance before upgrading:

  - If you are upgrading Tableau Server on Windows version 2018.1 or earlier, use the Manage Product Keys application. For more details, see Refresh Maintenance Date for the Product Key.

  - If you are upgrading Tableau Server on Windows version 2018.2 or later, or Tableau Server on Linux, run this tsm command:

    `tsm licenses refresh`

    If refreshing the product key does not update maintenance with a valid date, check in the Tableau Customer Portal to confirm you have a Tableau Server product key with up-to-date maintenance.

- Understand how version compatibility might impact your installation of Tableau Server.

  - Desktop and Server Compatibility in the Tableau Help.

- Add-on licenses—Data Management Add-on license is required if you want to use Tableau Prep Conductor. Tableau Prep Conductor enables publishing, running and scheduling flows on Tableau Server. For more information, see Licensing Tableau Prep Conductor.
What's New in Tableau Server

This article lists what's new in Tableau Server, beginning with version 10.5. Version 10.5 was the first version of Tableau Server for Linux. If you are looking for a historical list of new features in Tableau Server for Windows versions prior to 10.5, see What's New in Tableau Server for Windows 10.5.

What's new in version 2019.1

Help Design

Updates have been made to help you navigate our content, including a new right-hand menu to quickly scan and select different topics on a page. We've also created content within tabs, to easily show how to complete tasks for web or command line interface.

User

- New features and enhancements related to web authoring and interacting with views on the web are listed in What's New in Tableau for Users and Web Authoring and Tableau Desktop Feature Comparison. For topics related to web authoring and interacting with views, see Using Tableau on the Web.
- Web authoring auto recovery

Server or site administrator

- Option to install to non-default location on RHEL-distros
- Microservice Container Processes
- Pluggable Authentication Modules (PAM)
- TSM client authentication
- Ask Data and Elastic Server Processes
- Tableau Prep Conductor Server Process
- Node roles for Backgrounder Process
- Tableau Data Management Add-On
- SSL connection to Rserve external service
Web authoring auto recovery

With Tableau Server 2019.1, editing and authoring content on the server will auto-recover in the event of a process failure. As you make changes to content, Tableau Server will intermittently (and silently) save changes. In previous versions, a process failure results in lost changes if you did not save them prior to the failure. In Tableau Server 2019.1, changes you make prior to a failure will be persisted when you reconnect to the content.

By default, Tableau Server will save content after you make five changes to it. Your server admin can adjust this interval with the `vizqlserver.NumberOfWorkbookChangesBetweenAutoSaves` option using `tsm configuration set Options`. File size limit (`vizqlserver.WorkbookTooLargeToCheckpointSizeKiB`) and recovery attempts per session (`vizqlserver.RecoveryAttemptLimitPerSession`) can also be configured.

Option to install to non-default location on RHEL-distros

Starting with version 2019.1, if you are installing Tableau Server on a RHEL-like distribution of Linux, you can choose to install to a non-default location. The default location is `/opt`. If you want or need to install Tableau to another location, you can now do so, even when upgrading. Installing to a non-default location is not supported on Ubutu because of limitations of the `deb` package. For more information about installing Tableau Server, see Install and Initialize TSM. For more information about upgrading, see Upgrade Tableau Server on Linux.

Microservice Container Processes

The 2019.1 release adds some new processes to Tableau Server. Two container processes, Interactive Microservice Container and Non-Interactive Microservice Container now appear on the TSM Status page and in the output of the TSM command `tsm status -v`. These processes contain microservices and cannot be configured independently by administrators. For more information, see Tableau Server Microservice Containers.
Pluggable Authentication Modules (PAM)

In the 2019.1 release, TSM authentication process uses PAM directly and then falls back to an authentication scheme using substitute user (su) if PAM fails or is not configured with a directory service. This improvement provides a more integration with LDAP directory services. See TSM Authentication.

TSM client authentication

In the 2019.1 release, certificate trust and management for TSM clients (Web UI and CLI) have been updated to make encrypted connections to Tableau Server easier to manage. See Connecting TSM clients.

Ask Data and Elastic Server Processes

With Tableau Server 2019.1, Ask Data and Elastic Server processes have been added to Tableau Server to support the new Ask Data feature. For more information, see Tableau Server Processes.

The Ask Data process is installed and configured automatically. It cannot be configured manually. Logs are stored in the nlp directory. For more information, see Server Log File Locations.

The Elastic Server process is installed and configured automatically. The Elastic Server heap size can be configured by using the elasticserver.vmopts TSM configuration option. For more information, see tsm configuration set Options. Only one Elastic Server process can be running and it can optionally be moved to any node in the cluster.

Tableau Prep Conductor Server Process

Tableau Prep Conductor is a new server process that has been added to Tableau Server to support automation of running and managing flows. Tableau Prep Conductor leverages the scheduling and tracking functionality of Tableau Server so you can automate running flows.
to update the flow output instead of logging into Tableau Prep to manually run individual flows as your data changes. For more details, see Tableau Prep Conductor.

Tableau Prep Conductor is licensed through Tableau Data Management Add-on. For more information, see Licensing Tableau Prep Conductor.

Tableau Data Management Add-On

The Data Management Add-on is a new license that includes Tableau Prep Conductor. For more information, see Licensing Tableau Prep Conductor.

Node roles for Backgrounder Process

A new `tsm topology` command that gives you the ability to specify the type of tasks that backgrounder can perform has been added. In 2019.1, using the new command, you can isolate certain nodes to run only flow tasks or run all tasks other than flows. This is useful if you are planning to use Tableau Prep Conductor to publish, run and schedule flows. For more information, see Node Roles in Tableau Server and Tableau Prep Conductor.

SSL connection to Rserve external service

In previous versions, SSL connections to Rserve were not supported. In Tableau Server 2019.1, you can configure SSL connections. In addition, configuring external services is now done with native tsm commands under tsm security.

Added in previous versions

What's new in version 2018.3

Changes to Tableau Help

Search results within the product help have been expanded to include results for all Tableau products and help articles. Help layout and navigation, such as table of contents placement
and breadcrumbs, have been updated to create a more consistent cross-product help experience.

**User**

- New features and enhancements related to web authoring and interacting with views on the web are listed in *What's New in Tableau for Users* and *Web Authoring and Tableau Desktop Feature Comparison*. For topics related to web authoring and interacting with views, see *Using Tableau on the Web*.
- Secure extract data at the row level

**Server or site administrator**

- Materialize calculations in extracts already published to Tableau Server
- Improved content browsing (in-release beta)
- Support for Content Security Policy
- Improved support for LDAP
- SSL connection to Rserve external service
- SAML now supports PKCS#8 key files
- Improved key and secrets refresh process
- Backup without compression (added in version 2018.3.2)

**Materialize calculations in extracts already published to Tableau Server**

If you need to retroactively materialize calculations in extracts that have already been published to Tableau Server, you can use tabcmd to refresh the published extract with the `--addcalculations` option. For more information about materializing calculations in extracts, see *Materialize Calculations in Your Extracts* in the Tableau User Help. For more information about the tabcmd command option, see *refreshextracts workbook-name or datasource-name*.

**Secure extract data at the row level**

Secure your extract data at the row level using existing approaches for implementing row-level security in Tableau. For more information, see *Restrict Access at the Data Row Level* in the Tableau User Help.
Improved content browsing (in-release beta)

With Tableau Online and Tableau Server 2018.3, you and your web users can get a sneak preview of our reorganized content browsing experience. The new experience lets you see multiple content types—views, workbooks, data sources, flows, projects—in one grid or list. For example, you can now see all content inside a particular project and its sub-projects.

This new experience intends to make content discovery more intuitive, and it’s the first in a set of planned changes that are aimed at improving self-service and governance of your Tableau content.

To try the new browsing experience, enable the site-level setting we’ve provided for it. For more information, see Preview the Updated Content Browsing Experience.

After you enable the new experience, encourage your users to sign in to our Early Feedback site, share their thoughts with us, and see our regular development updates.

Support for Content Security Policy

Tableau Server supports the Content Security Policy (CSP) standard. CSP is intended to be an additional layer of security against cross-site scripting and other malicious web-based attacks. CSP is implemented as a HTTP response header that allows you to specify where external resources, such as scripts and images, can be safely loaded from.

See Content Security Policy.

Improved support for LDAP

Tableau Server 2018.3 includes improved support for LDAP, such as connection pooling, more flexible root configuration, and commas in object class names. See the new topic, LDAP Configuration Reference.

Connections to external services support SSL

In previous versions, SSL connections to Rserve and TabPy were not supported. In Tableau Server 2018.3, you can configure SSL connections. In addition, connecting to external ser-
vices is now enabling, disabling, and configuring is now done with native tsm commands under tsm security.

SAML now supports PKCS#8 key files

You can now use password-protected key files with SAML. See Configure Server-Wide SAML. The passphrase is encrypted at rest along with other server secrets. See Manage Server Secrets.

Improved key and secrets refresh process

In previous versions of Tableau Server, refreshing server secrets, keys, and tokens required that admins manually copied the keystore to each node in distributed deployments.

In Tableau Server 2018.3, the keystore is distributed to all nodes when you run the tsm security regenerate-internal-tokens command.

Backup without compression (added in version 2018.3.2)

Tableau Server version 2018.3.2 introduced a new option for the tsm maintenance backup command that allows you to disable compression when doing the backup. This can be beneficial for customers who have backups that take a long time. Using the option speeds up the time for the backup, but results in a larger backup file. If using this command option in a multi-node installation, we strongly recommend you have a File Store instance configured on your initial node to reduce the need to backup across nodes. To learn more about TSM backup, see tsm maintenance backup.

What's new in version 2018.2

User

- Include colleagues on data conversations with @mentions

New features and enhancements related to web authoring and interacting with views on the web are listed in What's New in Tableau for Users and Web Authoring and Tableau
Desktop Feature Comparison. For topics related to web authoring and interacting with views, see Using Tableau on the Web.

Server or site administrator

- Create a support case from the TSM UI or CLI
- Manage Dashboard Extensions in Tableau Server
- Automated daemon port configuration
- Amazon Linux 2 now supported

Include colleagues on data conversations with @mentions

To engage people in a conversation about compelling data you find in a view, @mention them in comments. As you begin to type a name, matching people with Tableau accounts at your organization appear in a list you can choose from. For more information, see Comment on Views in Tableau User Help.

Site administrators can disable @mentions in the General section of site settings.

Create a support case from the TSM UI or CLI

You can take a log file snapshot and send it to Tableau Support directly from the Tableau Services Manager UI or CLI. To learn how, see Log File Snapshots (Archive Logs)
Manage Dashboard Extensions in Tableau Server

Dashboard extensions are web applications that provide users new ways to interact with data from other applications directly in Tableau. You can control the dashboard extensions that you allow to run in Tableau. You can manage an extension’s access to data and can block extensions to prevent them from running. To learn more about controlling extensions, see Manage Dashboard Extensions in Tableau Server.

Automated daemon port configuration

In previous versions of Tableau Server on Linux, configuring the licensing daemon port was a required, manual step for multinode deployments. In the 2018.2 version, this process happens automatically. Tableau Server on Linux will automatically detect and configure the appropriate ports for the licensing daemon.

Amazon Linux 2 now supported

Beginning with version 2018.2, Amazon Linux 2 (AL2) is now a supported distro for Tableau Server on Linux.

What’s new in version 2018.1

User

- Resize headers on the web
- Streamline discussion threads by deleting comments

New features and enhancements related to web authoring and interacting with views on the web are listed in What’s New in Tableau for Users and Web Authoring and Tableau Desktop Feature Comparison. For topics related to web authoring and interacting with views, see Using Tableau on the Web.

Server or site administrator
New user-based term licenses are now available
New and renamed site roles are now available
Improved support for managing web data connectors

Resize headers on the web

When editing a view on the web, you can resize the width of row headers and the height of column headers.

Streamline discussion threads by deleting comments

If a comment on a view is unnecessary or inaccurate, users can quickly delete it by clicking the X in the upper-right corner. For more information, see Comment on Views in Tableau User Help.

To disable the ability to delete comments, change the tsm configuration set option, viz-portal.commenting.delete_enabled, to false.

New user-based term licenses are now available

Tableau offers multiple types of user-based term licenses that grant a range of web authoring and other capabilities at various price points, providing the flexibility for organizations to pay for the data analysis and data visualization capabilities that each type of user in their organization needs. To learn more, see User-based licenses.
New and renamed site roles are now available

Starting in the version 2018.1 release, new and updated site roles are now available. To learn about these site roles, see Set Users’ Site Roles. To learn about changes in the REST API to accommodate new site roles, see What’s New in the REST API.

Improved support for managing web data connectors

Tableau Server now provides improved support for web data connectors (WDCs):

- A new set of tsm data-access commands are now available to help you manage WDCs.
- You can also manage WDCs using the new web-data-connector-settings Entity.

What’s new in version 10.5

User

- Extracts use the new .hyper format
- Changes to the way values are computed
- Filtered search hidden by default

New features and enhancements related to web authoring and interacting with views on the web are listed in What’s New in Tableau for Users and Web Authoring and Tableau Desktop Feature Comparison. For topics related to web authoring and interacting with views, see Using Tableau on the Web.

Server or site administrator

- Optimized server performance for data alerts
- Nested projects
- Tableau Data Engine with Hyper
Tableau Server on Linux Administrator Guide

- Tableau Services Manager
- Hot topology support
- Lightweight Directory Access Protocol (LDAP) support

Optimized server performance for data alerts

To improve overall performance, Tableau Server now rechecks failing data alerts only when it next checks data conditions for all alerts. You can revert to the previous setting, which checked failing alerts every 5 minutes, by changing the tsm configuration set option, dataAlerts.retryFailedAlertsAfterCheckInterval, to false.

Nested projects

You can now create project hierarchies when you want to create content segments within a larger area. For example, create a project for each department, say Operations. In each of those top-level projects, separate content based on how the audience uses it, say connecting to certified data versus in-progress collaboration. For more information, see the following articles:

- Use Projects to Manage Content Access
- **Navigate projects** in the article Navigate Tableau on the Web

Filtered search hidden by default

Filtered search options are now located on the right side of pages, and are hidden by default. The toggle is a dark icon (§) when the Filters pane is open and a light icon (§§) when the Filters pane is closed. For details on searching, see Search Content.

To use filtered search, click §.
Tableau Data Engine with Hyper

Hyper is Tableau’s new in-memory Data Engine technology optimized to bring faster extract and query performance, and increased scalability. You can now analyze large data sets faster and faster extract creation. For more information, see Tableau Server Data Engine.

Extracts use the new .hyper format

Beginning with version 10.5, new extracts use the new .hyper format. Extracts in the new format take advantage of the improved data engine, which supports the same analytical and query performance as the data engine before it, but for even larger extracts. Similarly, when an extract task is performed on a .tde extract using version 10.5, the extract is upgraded to a .hyper extract. For more information, see Extract Upgrade to .hyper Format.

Changes to the way values are computed

To improve data source efficiency and scalability, and produce results that are consistent with commercial databases, values in your data source can be computed differently in
version 10.5. In some cases, these changes can cause differences with the values and marks in your view between version 10.4 (and earlier) and version 10.5 (and later). This applies to extract data sources, and can apply to multi-connection data sources, data sources that use live connections to file-based data, data sources that connect to Google Sheets data, cloud-based data sources, extract-only data sources, and WDC data sources. For more information, see Changes to values and marks in the view in the Tableau User Help.

Tableau Services Manager

Tableau Server version 10.5 features our new web-based server configuration and management application, Tableau Services Manager (TSM). To learn more about TSM, see Tableau Services Manager Overview.

Hot topology support

Tableau Server includes support for hot topology changes. This allows you to change the number of Backgrounder and VizQL processes running on nodes that already have these processes - without the need to restart Tableau Server. To learn more about these and other Tableau Server processes, see Tableau Server Processes.

Lightweight Directory Access Protocol (LDAP) support

Tableau Server now supports Lightweight Directory Access Protocol (LDAP). To learn more about LDAP support in Tableau Server, see Identity Store
What's Changed - Things to Know Before You Upgrade

This article lists important changes in Tableau Server, beginning with version 10.5. Version 10.5 was the first version of Tableau Server for Linux. This list is cumulative. If you are upgrading from an early version (for example, 9.3), read the list of changes for every version between your current version and the version you are upgrading to. If you are upgrading from Tableau Server on Windows to Tableau Server on Linux, read both versions of "What's Changed."

Looking for Tableau Server on Windows? See What's Changed - Things to Know Before You Upgrade.

What Changed in Version 2019.1

Version 2019.1 includes changes you should know about before upgrading.


Install to non-default locations (RHEL-like distributions only)

Beginning with version 2019.1, on RHEL-like distributions, you can install Tableau Server to a location other than the default /opt. This is not supported on Ubuntu due to limitations of the deb package. For details, see install instructions in Install and Initialize TSM or upgrade instructions in Upgrade Tableau Server on Linux.
High-resolution thumbnails

In version 2019.1 and later, workbooks and views use higher resolution thumbnails. When you upgrade to Tableau Server version 2019.1 or later, the Backgrounder runs the Enqueue Thumbnails Upgrade job and the Upgrade Thumbnails job, which refreshes thumbnails for any views that have not been edited or published since Tableau version 2018.2 and converts them from low resolution thumbnail images (192 x 192 pixels) to high resolution thumbnail images (300 x 300 pixels), as shown in the figure below.

When the Upgrade Thumbnails job refreshes the thumbnail images, the modified date of the view is changed to match the thumbnail update date. The Upgrade Thumbnails job does not change the modified date of workbooks when it updates the contained view’s thumbnails.

Thumbnails may appear blurry until the Upgrade Thumbnails job is complete. Depending on the number of workbooks you have, this could take a few minutes to a few hours. You may also notice that thumbnail images may appear in low resolution for up to a week after upgrading to Tableau Server 2019.1. For more information, see Upgrade Thumbnails Job.

Project card images

In version 2019.1 and later, project card images will not appear on the project card unless they are added as the last item in the project description and encapsulated with ! (exclamation marks). For more information, see Add a Project Image.

What Changed in Version 2018.3
Version 2018.3 includes some changes you should know about before upgrading.


**Floating worksheet captions become transparent**

To make a floating caption visible again, content authors will need to change the caption background to a color.

**Changes to some Data Engine tsm configuration set options**

Two new configuration tsm set configuration options have been added: hyper.hard_concurrent_query_thread_limit and hyper.soft_concurrent_query_thread_limit

The new options replace the hyper.num_job_worker_threads and hyper.num_task_worker_threads options available in Tableau Server versions 2018.3 and earlier. The hyper.num_job_worker_threads and hyper.num_task_worker_threads have been deprecated and will no longer work in 2019.1 and later.

**SSL Off-loading and SAML**

Beginning with version 2018.3, Tableau Server validates SAML response message returned from the IdP. If your organization terminates SSL connections from the IdP at a proxy server before sending the authentication request to Tableau Server, then users may be unable to login with SAML after you upgrade from 2018.2.

In this scenario, SSL is "off-loaded" at the proxy server, which means the https request is terminated at the proxy server and then forwarded to Tableau Server over http. Since SSL is off-loaded at the proxy, Tableau Server will validate with the protocol that it receives (http), but the IdP response is formatted with https, so validation will fail unless your proxy server includes the X-Forwarded-Proto header set to https. See Configuring Proxies for Tableau Server.
What Changed in Version 2018.2

Version 2018.2 includes some significant changes you should know about before upgrading.


The following sections summarize the significant changes to Tableau Server 2018.2 and provide links for additional information.

- Updates to Tableau Server Apache Logs
- The Read Only site role is now deprecated
- The tabcmd initialuser command prompts for password
- New ports added

Moving the repository in a two-node cluster not supported

Updates to Tableau Server Apache Logs

Apache log files stored in /logs/httpd now contain records with several formatting improvements, including the following:

- Server names are shown according to the UseCanonicalName setting, which makes it easier to distinguish between nodes in a multi-node server deployment.
- Date and time are now tracked in a single date-and-time string that can be readily recognized as a single value by a variety of data analysis tools, including Tableau Desktop.
- Time zones are now easier to parse
  - On Linux, the numerical offset from UTC is provided.
  - On Windows, the name of the timezone is enclosed in quotes
Date, time and time zone formatting changes are illustrated by an example log entry from Tableau Server version 2018.1 and earlier releases:

```
::1 - - 2018-05-09 08:51:48.872 GMT Daylight Time 80 "POST /vizql/w/Re-
gional/v/Obesity/sessions/A971A92AF77A4F4A9813065BDCEB24D6-0:0/-commands/tabsrv/render-tooltip-server HTTP/1.1" "-" 200 445 "593" 135021 WvKolPH4UcM5KrzUbLi8EwAAA@E
```

For purposes of comparison, here is a log entry from Tableau Server version 2018.2:

```
10.210.24.3 127.0.0.1 - 2018-05-09T16:07:58.120 "GMT Daylight Time" 80 "POST /vizql/w/Su-
per-store/v/Overview/bootstrapSession/sessions/185CCDC854A44765BB0298E93B403879-0:3 HTTP/1.1" "-" 200 136026 "784" 2370951 WvMOzgKIhfzh9kFWO@ow2gAAA1Y
```

The Read Only site role is now deprecated

The Read Only site role that was introduced in Tableau Server version 2018.1 is now deprecated. Any users assigned to the Read Only site role in version 2018.1 are reassigned to the Viewer site role after an upgrade to version 2018.2. To learn more about site roles, see Set Users’ Site Roles.

The `tabcmd initialuser` command prompts for password

In previous versions, the `tabcmd initialuser` command required a `--password` parameter to set the initial administrator password. In the `tabcmd` included with this version of Tableau Server, you can leave the `--password` parameter out of the command to be prompted in the shell instead. See `initialuser`. 
New ports added

We've added new service ports in 2018.2.

Automatic port assignment

For installations where automatic port assignment is enabled (this is recommended and the default) there should be no impact to upgrading. The new ports will be automatically selected on upgrade.

Manual port assignment

If you have disabled automatic port assignment, you will need to manually specify the new ports in your configuration before upgrading. For more information about manually assigning ports, see Manual port assignment.

Ports added in 2018.2

<table>
<thead>
<tr>
<th>Port names</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>You must define each of these for every node if you disable dynamic port mapping.</td>
<td></td>
</tr>
<tr>
<td>hyper.port</td>
<td>Data engine primary port.</td>
</tr>
<tr>
<td>hyper.connection.port</td>
<td>Data engine connection port.</td>
</tr>
<tr>
<td>licenseservice.vendor_dae-mon.port</td>
<td>License service vendor daemon port.</td>
</tr>
<tr>
<td>samlservice.port</td>
<td>SAML service port.</td>
</tr>
<tr>
<td>tabadminagent.columbo.port</td>
<td>Administration Agent service discovery port</td>
</tr>
<tr>
<td>tabadminagent.filetransfer.port</td>
<td>TSM Agent file transfer port.</td>
</tr>
<tr>
<td>vizportal_0.microservice.extensions.port</td>
<td>Application server extensions port.</td>
</tr>
<tr>
<td>vizportal_0.monolith_grpc.port</td>
<td>Application server GRPC port.</td>
</tr>
</tbody>
</table>
What Changed in Version 2018.1

Version 2018.1 includes some changes you should know about before upgrading.


The following sections summarize the significant changes to Tableau Server 2018.1 and provide links for additional information.

- Removed tabadmin command options
- Updated tsm commands
- Updated upgrade-tsm script

Removed tabadmin command options

The previously deprecated `--license` and `--administrator` options are no longer available when using the `tabcmd createsiteusers`, `tabcmd createusers` and `tabcmd syncgroup` commands. These are breaking changes for any scripts that still use the `--license` or `--administrator` options. To update your scripts, use the `--role` option with these commands to specify the license levels or site roles. For details, see `tabcmd` Commands.

Updated tsm commands

As of version 2018.1 we have added or expanded the following tsm commands:

- `tsm maintenance cleanup`—The tsm maintenance cleanup command was added in version 10.5.1. For version 2018.1 it has been enhanced with additional options to give you more flexibility. For details, see tsm maintenance cleanup.
tsm reset — Added in version 2018.1, this command allows you to reset the initial administrative user. For details, see tsm reset.

Updated upgrade-tsm script

As of version 2018.1 the upgrade-tsm script you run when you upgrade from a previous version now requires you to include the name of a TSM administrator when you run it. For example:

```
sudo /opt/tableau/tableau_server/packages/scripts.<version_code>/upgrade-tsm -u <tsm_system_admin> -p <tsm_system_admin_password> --accepteula
```

where tsm_system_admin is a user with administrative permissions on the initial node computer.

What Changed in Version 10.5

Version 10.5 includes some changes you should know about before upgrading.


The following sections summarize the significant changes to Tableau Server 10.5 and provide links for additional information.

- Tableau Server configuration changes
- Changes to extracts
- Version compatibility
- Viewer (can publish) and Unlicensed (can publish) site roles removed
- Nested projects and content navigation
Nested projects and tabcmd

Filtered search hidden by default

Tableau Server configuration changes

Hyper powers the new Data Engine in Tableau Server 10.5 and introduces the changes described below. For more information, see Tableau Server Data Engine.

Beginning with version 10.5, Tableau Installer automatically installs Data Engine when you install file store, Vizportal, VizQLServer, data server, or backgrounder and cannot be installed separately. Every node that has an instance of one of these processes will also have a single instance of the data engine process. You can no longer configure more than one instance of data engine on a node. To learn more about Tableau Server Processes see Tableau Server Processes.

Previously, in versions 10.4 and earlier, for distributed installations, the backgrounder process launched temporary instances of data engine (tdeserver64.exe) process during extract creation or refreshes. In Tableau Server 10.5, a single instance of data engine is installed automatically when you install backgrounder. The backgrounder process uses this single instance of data engine that is installed on the same node. For more information on configuration recommendations, see Distributed Installation Recommendations.

Upgrade may affect your current configuration for a multi-node cluster, especially if you have certain processes isolated on a separate node. For more information, see Tableau Server Data Engine.

Changes to extracts

Beginning with version 10.5, new extracts use the new .hyper format. The improved data engine can read both the .tde and .hyper file formats, so the latest version of Tableau Server can continue to view and read workbooks that are using .tde extracts.

Existing extracts will not automatically be upgraded to the new .hyper format during the Tableau Server or Tableau Desktop upgrade process. Only when certain extract tasks are
performed on the .tde extract, the extract is upgraded to the .hyper format. For example, an automatic or scheduled refresh will upgrade a .tde extract to a .hyper extract.

- For more information on extract upgrades, see Extract Upgrade to .hyper Format.
- For recommendation on how to handle automated or schedule refresh tasks before you upgrade, see Prepare for the Upgrade.

**NOTE:** Use the Extract API 2.0 to create (.hyper) extracts, which requires Tableau 10.5 and later. If you are using Tableau 10.4 and earlier, continue to use the Tableau SDK to create .tde extracts. The Tableau SDK is no longer being maintained. For more information, see Extract API 2.0.

**Version compatibility**

Upgraded extracts are not backward compatible. After extracts are upgraded from .tde to .hyper format, they cannot be opened or refreshed in Tableau Desktop 10.4 and earlier. Tableau recommends that Tableau Server and all Tableau Desktops in your organization be on the same version and be upgraded to 10.5 on the same schedule. For more information on specific extract compatibility scenarios, see Impact of extract upgrade.

**Viewer (can publish) and Unlicensed (can publish) site roles removed**

The site roles **Viewer (can publish)** and **Unlicensed (can publish)** have been deprecated and are no longer available. Users who have either of these site roles on Tableau Server 10.4 or earlier will be reassigned in Tableau Server 10.5.

<table>
<thead>
<tr>
<th>Deprecated site role</th>
<th>In 10.5 is reassigned to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewer (can publish)</td>
<td>Viewer</td>
</tr>
<tr>
<td>Unlicensed (can publish)</td>
<td>Unlicensed</td>
</tr>
</tbody>
</table>

**Nested projects and content navigation**

You can now create project hierarchies when you want to segment content into sub-sections within a larger area. For example, you might create a project for each department. In each of
those top-level projects, you can separate content based on how the audience uses it, such as connecting to certified data versus in-progress collaboration. For more information, see the following articles:

- Use Projects to Manage Content Access
- **Navigate projects** in the article Navigate Tableau on the Web

Nested projects and tabcmd

Using tabcmd, you can specify only a top-level project in a project hierarchy. To automate tasks you want to perform on a sub-project or content in a sub-project, you must use the equivalent Tableau REST API call.

Not all actions are available through the REST API. If you use Server on Windows and want to run an unscheduled extract refresh or append a file to an extract, a possible alternative is to use the Tableau Data Extract Command Line Utility.

Filtered search hidden by default

Filtered search options are now located on the right side of pages, and are hidden by default. The toggle is a dark icon (_private) when the Filters pane is open and a light icon (private) when the Filters pane is closed. For details on searching, see Search Content.

To use filtered search, click [Private].
Minimum Hardware Requirements and Recommendations for Tableau Server

The following minimum hardware requirements and recommendations apply to all computers running Tableau Server, including physical hardware and virtual machines (VMs):

- **Minimum requirements for testing and prototyping** are the minimum hardware your computer must have in order to install Tableau Server. If your computer does not meet these requirements, the Setup program will not install Tableau Server. These requirements are appropriate for testing and prototyping, but are not appropriate for most production environments.

- **Minimum recommendations for production** go beyond minimum requirements, and represent the minimum hardware configuration you should use for a production installation of Tableau Server. If your computer meets the minimum requirements but does not meet these recommendations, the Setup program will warn you, but you can continue the installation.
In addition, Tableau Server should not be installed on a physical computer or on a VM instance that is also running resource-intensive applications such as databases or application servers.

**Note:** If you install Tableau Server on a computer that meets the minimum requirements but does not have at least 8 cores and 16 GB of system memory, the default number of all processes installed is reduced to one of each process by design. For more information about processes, see Server Process Limits.


Minimum Hardware Requirements for Testing and Prototyping

The computer on which you are installing or upgrading Tableau Server must meet the minimum hardware requirements. If the Setup program determines that your computer does not meet the following requirements, you will not be able to install Tableau Server.

These minimum requirements are appropriate for a computer that you use for prototyping and testing of Tableau Server. They apply to single-node installations and to each computer in a distributed installation.

<table>
<thead>
<tr>
<th>Processor CPU</th>
<th>RAM Free</th>
<th>Disk Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>64-bit</td>
<td>8</td>
<td>15</td>
</tr>
<tr>
<td>2-core</td>
<td>GB</td>
<td>GB</td>
</tr>
</tbody>
</table>

**Minimum Hardware Requirements**

**Note:** These minimum requirements are not recommended for use in production environments. For production minimum recommendations, see Minimum Hardware Recommendations for Production.
For the requirements:

- Free disk space is calculated after the Tableau Server Setup program is unzipped. The Setup program uses about 1 GB of space. You may need to allocate additional disk space depending on various factors like whether you will be using extracts. For more information, see Disk Space Requirements.

The core Tableau Server bits must be installed in a directory with at least 15 GB of free disk space. If you attempt to install Tableau Server on a computer that does not have enough space, the Tableau Server package will install, but you will be unable to continue with setup. By default the install location is the /opt directory. You can change the installation path for Tableau Server on RHEL distros. For more information, see Option to install to non-default location on RHEL-distros.

If you plan to make heavy use of extracts then you may need to allocate additional disk space. You can specify a different directory for data (extract) storage during installation. See Install and Initialize TSM.

- Core count is based on "physical" cores. Physical cores can represent actual server hardware or cores on a virtual machine (VM). Hyper-threading is ignored for the purposes of counting cores.

Minimum Hardware Recommendations for Production

For production use, the computer on which you install or upgrade Tableau Server should meet or exceed the minimum hardware recommendations. These recommendations are general. Actual system needs for Tableau Server installations can vary based on many factors, including number of users and the number and size of extracts. If the Setup program determines that your computer does not meet the following recommendations, you will get a warning, but you can continue with the setup process. The minimum recommendations listed here are intended as general guidance. However the recommendations for your environment may vary. For more information, see the Hardware recommendations section of the Recommended Baseline Configurations topic.
<table>
<thead>
<tr>
<th>Install Type</th>
<th>Processor</th>
<th>CPU</th>
<th>RAM</th>
<th>Free Disk Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single node</td>
<td>64-bit</td>
<td>8-core, 2.0 GHz</td>
<td>32 GB</td>
<td>50 GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>or higher</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If you are adding Tableau Prep Conductor to your Tableau Server installation, it is recommended to add a second node and dedicate this to running Tableau Server Prep Conductor. This node should have a minimum or 4 cores (8 vCPUs), and 16 GB of RAM.

Multi-node and enterprise deployments

Contact Tableau for technical guidance.

Nodes must meet or exceed the minimum hardware recommendations, except:

- Nodes running backgrounder, where 4 cores may be acceptable.
- Dedicated node for Tableau Prep Conductor: Minimum of 4 cores (8 vCPUs), and 16 GB of RAM.

For the recommendations:

- Free disk space is calculated after the Tableau Server Setup program is unzipped. The Setup program uses about 1 GB of space. You may need to allocate additional disk space depending on various factors like whether you will be using extracts. For more information, see Disk Space Requirements.

The core Tableau Server bits must be installed in a directory with at least 15 GB of free disk space. If you attempt to install Tableau Server on a computer that does not have enough space, the Tableau Server package will install, but you will be unable to continue with setup. By default the install location is the `/opt` directory. You can change the installation path for Tableau Server on RHEL distros. For more information, see Option to install to non-default location on RHEL-distros.
If you plan to make heavy use of extracts then you may need to allocate additional disk space. You can specify a different directory for data (extract) storage during installation. See Install and Initialize TSM.

- Core count is based on "physical" cores. Physical cores can represent actual server hardware or cores on a virtual machine (VM). Hyper-threading is ignored for the purposes of counting cores.

- RAM shown is the minimum recommended for a single-node installation. Your installation may function better with more RAM, depending on activity, number of users, and background jobs, for example. For hardware specifications Tableau uses internally for testing scalability, see Hardware Recommendations.

For hardware recommendations for Tableau Server in the cloud, see the following:

- Selecting an AWS Instance Type and Size in the Tableau Server on Linux in the AWS Cloud Administrator Guide
- Selecting a Google Compute Engine Virtual Machine Type and Size in the Tableau Server on Linux in the Google Cloud Platform Administrator Guide
- Selecting a Microsoft Azure Virtual Machine Type and Size in the Tableau Server on Linux in Microsoft Azure Administrator Guide

Prepare for the Upgrade

To properly prepare for a Tableau Server upgrade, gather the following information about your existing installation, key files related to your installation and the upgrade, and complete the pre-upgrade tasks.

Gather custom configuration information

If you are upgrading on the existing hardware your configuration will be preserved, but it’s a good practice to collect this configuration information about your existing installation for several reasons: you need this information when you configure a test environment, you need this information if you are migrating to new hardware migration as part of the upgrade, and
you can use the information to confirm that the upgraded Tableau Server is configured as expected if you notice something unexpected after upgrading.

Collect this information and any associated files and save them to a location that is not on any of the Tableau Server computers.

The following list includes examples of the type of information you should gather:

- **TSM Controller certificate** Verify the certificate for the TSM Controller is still valid.

  To verify your TSM Controller SSL certificate's expiration date:

  1. Open a terminal session.

  2. Type the following commands to display the dates when the certificate is valid:

     ```
     openssl s_client -connect <tsm_servername>:8850
     echo | openssl s_client -connect <tsm_servername>:8850 2>/dev/null | openssl x509 -noout -dates
     ```

  3. If the certificate is expired, open a case with our Support team, and they will be happy to help with the upgrade.

- **Customizations** This includes non-default ports, timeout values, custom logo images, and fonts.

- **SMTP configuration.**

  For more information, see Configure SMTP Setup.

- **SSL configuration and certificates.**

  For more information, see Configure SSL for External HTTP Traffic to and from Tableau Server.

- **SAML configuration, certificates and any IdP metadata files.**
For more information, see SAML.

- **Kerberos** configuration.
  
  For more information, see Configure Kerberos.

- **OpenID** configuration.
  
  For more information, see Configure Tableau Server for OpenID Connect.

- **Additional node** configurations. Collect the configurations of any additional Tableau Server nodes, including any certificates or other supporting files that you copied to these nodes.

- **Other** values. Note the number of projects, groups, workbooks, views, data sources, and users you have in your production environment. Having this information makes it easy to do a quick check after the upgrade to make sure everything was restored as expected.

**Gather the environment configuration**

The steps you need to take during the upgrade process depend on whether you’re installing the upgrade on the same hardware or you’re migrating to new hardware. Upgrading on the same hardware is straightforward and requires a minimum of manual steps (the steps you need to take depend on what version you are upgrading from, what version you are migrating to, and whether or not your existing installation is in the default location). Migrating to new hardware requires you to manually restore your Tableau Server data and reconfigure your settings after you install the new version.

**Copy the setup files to a local file share**

You will need the following setup files before you upgrade Tableau Server:
The installer for your existing version of Tableau Server.

You might not need the installer. However, we recommend that you have it available in case there's a problem during the upgrade. That way you can use the setup program and your server backup to restore your installation to its pre-upgrade state.

**Note:** If you do not have the installer for your existing version, you can download it from the Alternate Downloads Site. Save the installer in a safe location that is not part of your production or test version of Tableau Server. You will need the Setup program if you need to go back to your existing version after upgrading.

The setup program for the new version of Tableau Server.

**Update tabcmd**

A new version of tabcmd is released with every release of Tableau Server. If you install tabcmd on computers that are not part of your Tableau Server installation, you need to update tabcmd on those computers. For more information, see tabcmd.

**Back up Tableau Server data**

We recommend that you make a backup of your installation of Tableau Server before beginning the upgrade process. This provides data that you'll need to set up a test version of the upgraded environment. It also lets you recover if the upgrade process fails.

**Notes:**

- Backups from versions of Tableau Server older than version 9.x cannot be used with version 2018.2.x or later. If you are running an older version of Server, you may need to do an intermediate upgrade to version 9.x through 10.x before upgrading to version 2018.2 or later.

- We recommend you disable subscriptions and scheduling in your production
environment immediately before taking the backup, and reenable them after the backup is complete. Doing this will help avoid having your users receive duplicate subscriptions and email messages when you restore your backup in your test environment.

- The full backup can take a while if you have a large installation or a lot of extracts.

- Any changes made between the time you took the backup and the time you do the upgrade are lost because they aren't included in the backup.

For more information, see Remove Unneeded Files and Back up Tableau Server data.

Generate asset keys file before uninstalling Tableau Server for Windows 2018.1.x or earlier

If you are upgrading from Tableau Server on Windows version 2018.1.x or earlier, and you generated a custom asset key, save a copy of the asset_keys.yml file before you uninstall your earlier version. Store this file in a safe place that is not part of your Tableau Server installation (a network share for example).

In most cases you will not need this file. The upgrade process updates asset keys automatically when an upgrade is successful. You only need this file if the upgrade fails and you need to install a new version of Tableau Server and manually restore your backup file. In this case, you also need to specify the asset keys file when doing the restore.

Locating an existing asset keys file

If you generated a custom asset key file, you will have an asset_keys.yml file in the data directory. By default this is:

\ProgramData\Tableau\Tableau Server\data\tabsvc\config

If you do not see an asset_keys.yml file, you can skip this.

Restoring a pre-2018.2 Tableau Server for Windows backup along with asset keys

To manually restore a backup from Tableau Servers for Windows 2018.1.x or earlier, and include asset keys, use tsm, for example:
For more information, see tsm maintenance restore.

Check your product maintenance status

If you attempt to upgrade a Tableau Server installation that has a product key with expired maintenance, your upgraded Tableau Server will be unlicensed and the upgrade may fail. Before upgrading, make sure that the server’s maintenance hasn't expired.

If your maintenance has expired, select the product key and then click Refresh. If this does not update the maintenance date, check the Tableau Customer Portal for a replacement Tableau Server product key with a later maintenance date. For any questions or concerns, please contact Tableau Technical Support. Reactivating the product key will be part of the upgrade process.

For more information, see Activate and Register Tableau Server. If your server doesn’t have internet access, see Activate Tableau Server Offline - Adding a License.

Disable your extract refreshes

Beginning in 10.5, extracts use .hyper format instead of .tde. Once the file format has been upgraded to .hyper, it cannot be reverted back to .tde format and cannot be opened in Tableau Desktop version earlier than 10.5. For more information, see Extract Upgrade to .hyper Format.

The following tasks on Tableau Server will upgrade a .tde extract to a .hyper extract:

- Manual refresh
- A scheduled full or incremental extract refresh
- Automated refresh tasks that are performed through tabcmd, Extract API 2.0, or through Extract Command Line Utility
Automated append data to an extract using tabcmd or using the Extract Command Line Utility

**Note:** We recommend that you disable any automated tasks and schedules that result in an extract upgrade. If you have desktop versions that have not yet been upgraded to 10.5, your desktop users will not be able to open the upgraded .hyper extracts. You may also want to first test a few extracts manually after doing the server upgrade, and then reenable any schedules or automated refresh tasks.

For more information about extract refresh scheduling, see Enable Extract Refresh Scheduling and Failure Notification.

Ensure that your license has enough user capacity

When upgrading from a Tableau 2018.1 or earlier license with legacy site roles, all users are automatically mapped to their current equivalent site role. Before upgrading, it’s important to make sure that your new license supports the number of users you have. Otherwise, some users may become unlicensed after the upgrade.

The following table shows the mapping of the legacy site roles to the current site roles.

<table>
<thead>
<tr>
<th>2018.1 legacy site role</th>
<th>2018.1 user-based site role</th>
<th>2018.2 and later site role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Administrator</td>
<td>Server Administrator</td>
<td>Server Administrator</td>
</tr>
<tr>
<td>Site Administrator</td>
<td>Site Administrator Explorer</td>
<td>Site Administrator Explorer</td>
</tr>
<tr>
<td>Publisher</td>
<td>Explorer (can publish)</td>
<td>Explorer (can publish)</td>
</tr>
<tr>
<td>Interactor</td>
<td>Explorer</td>
<td>Explorer</td>
</tr>
<tr>
<td>Viewer</td>
<td>Read Only</td>
<td>Viewer</td>
</tr>
</tbody>
</table>

Users always use the highest level role they have on any site, which is called the Maximum Site Role. You can view the Maximum Site Role is for users before you convert your license. For more information, see Content Permissions and Ownership.
If you have more users than licenses for your current roles, you should reallocate or balance users to the available roles by changing their role, unlicensing users, or moving users. You can use the following steps to synchronize groups of new users after upgrading to 2018.2 or later:

1. Unlicense all users.

2. Create five Active Directory (AD) groups (one for each site role).

3. Import users into the correct AD group for the appropriate site role, and then sync those groups with Tableau Server. For more information, see Create Groups via Active Directory.

4. Restart Tableau Server. Users are automatically migrated into their new site roles. Content permissions are not affected.

Plan your strategy if you use virtual machines (VMs)

If you run Tableau Server on VMs, either locally, or in the cloud, be aware of the potential for complications related to licensing. If you are simply upgrading Tableau Server on the VM, you do not need to take any extra action related to licensing. If you plan to clone the VM to create either a new production or test environment to upgrade, you need to deactivate any Tableau Server licenses before cloning. If you do not do this, the new VM environment can end up with an untrusted license, and any attempts to upgrade will fail. You may also end up hitting the maximum number of activations for the licenses.

To avoid issues with licensing on VMs, deactivate all Tableau licenses before cloning a VM or allowing it to be permanently shut down.

Test the Upgrade

The best way to learn what impact a Tableau Server upgrade will have to your current environment is to test it. Knowing how an upgrade will affect your users and your server helps you plan and communicate before the actual upgrade, ensuring that your users will not be caught by surprise.

If you have a Tableau Server test environment this is a great place to test out the upgrade.
We recommend the following sequence for testing a Tableau Server upgrade:

1. **Prepare a test environment**
2. **Upgrade the test environment**
3. **Confirm that existing functionality works**
4. **Performance and user acceptance testing**
5. **Test new features**
6. **Communicate about the upgrade**

**Prepare a test environment**

To start, create a test environment that mirrors your production environment as closely as possible. The closer your test environment is to the actual environment you will be upgrading, the more accurate a representation you will have of how the upgrade will impact you. This includes identical or similar hardware and operating systems, as well as the same authentication options and network access.

When you've got a test computer or virtual machine ready, follow these steps for creating a test environment.

1. **On the existing production environment, create a backup of Tableau Server using the `tsm maintenance backup` command.**
   
   For more information, see [Create a pre-upgrade backup](#).
2. **On your test environment, install a copy of the same version of Tableau Server as you have in your production environment.**

**Note:** You can download the setup program for your current version from the [Alternate Downloads Site](#).
3. Restore your existing database data using the `tsm maintenance restore` command.

   For more information, see Restore from a backup.

4. Manually replicate your existing Tableau Server configuration.

   You need to manually configure certain aspects of your environment because when you restore the Tableau database it doesn’t include configuration details and customizations.

Upgrade the test environment

Follow the appropriate steps for upgrading the test environment, based on your environment:

- Upgrade Tableau Server on Linux
- Upgrade Tableau Server on Linux from 10.5

Confirm that everything works as expected

After you have the new version of Tableau Server installed and configured in your test environment, you are ready to test. You should test basic functionality, along with any special aspects of server that your organization relies on. For example, if there are key subscriptions that your organization relies on, make sure that you test those.

These are some areas of testing to consider:

- **Server processes.** Sign in to Tableau Server as a server administrator, and then open the Server Status page to confirm that all services and processes are running as expected (including on all additional nodes if this is a distributed installation).

- **User access.** Confirm that Tableau Server users can sign in. Test your normal user sign in process. Have some of your users participate in the testing to make sure they are able to sign in as expected, and that they can get to the same content that they
have access to in your production environment.

- **Publishing workbooks and data sources.** Have users publish workbooks and data sources from Tableau Desktop to make sure this goes as you expect.

- **Viewing published workbooks.** Have users who are familiar with the content try to view published workbooks to make sure they appear as expected. Test views embedded in web pages (for example, in SharePoint pages).

- **Subscriptions and extract refreshes.** Manually run some extract refreshes to confirm that they complete successfully. Run some key scheduled extract refreshes to confirm that they complete as expected.

- **Permissions.** Confirm that permissions are still set as expected for users and content.

- **Command-line utilities and APIs.** If applicable, test the command line utilities (tsm and tabcmd) and programmatic access via APIs.

Performance and user acceptance testing

Use tools like Tabjolt, Replayer, and Scout to do performance and user acceptance testing on your test environment. For more information about these and other performance testing tools, see Performance Monitoring Tools. If you have workbooks that have calculations and use extracts as the data source, we recommend that you test the performance of these workbooks before you upgrade. For more information, see Test Workbook Performance.

Test new features

Take a look at the new features that come with the version you are upgrading to, and at any features that were added between the version you currently have and the new version. Think about how to help your users understand the benefits of the features that apply to your environment.

For more information on new features, see What's New in the Tableau Server Help.
Communicate about the upgrade

The best way to make an upgrade go smoothly is by letting your organization know ahead of time about the upgrade and how it might impact them. If you’ve had users help test, take advantage of their experience by having them help communicate the changes they saw while testing. You can also provide user access to the test environment if there are key people who should see the upgraded version before the actual upgrade.

Test Workbook Performance

In most cases, you can expect to see similar or better performance after upgrading your Tableau Server from versions 10.4 or earlier to 10.5 or later. However, for workbooks that use complex calculations, you may see performance issues after you upgrade. This article describes how to test performance and troubleshoot these performance issues before you upgrade your production Tableau Server from versions 10.4 and earlier to 10.5 or later.

If you have already upgraded your production Tableau Server to 10.5 or later, and you are seeing performance issues for workbooks that have calculations and use extracts as the data source, see Troubleshoot Performance of Workbooks with Calculations.

Since Linux was first released in 10.5, this only applies when you are migrating from Tableau Server versions 10.4 or earlier on Windows to Linux 10.5 or later.

To make sure your workbook performance is same or better after your upgrade to Tableau 10.5 or later, we strongly recommend that you set up a test environment and do performance testing before you upgrade your production Tableau Server.

Use the following sequence of steps for testing workbook performance:

1. Set up your test environment
2. Capture performance metrics and analyze
3. Troubleshoot performance issues
4. Capture the conclusions and results
Set up your test environment

1. Create a test environment that mirrors your production environment as closely as possible.

   Follow the steps described in Migrate Tableau Server from Windows to Linux.

2. Disable any automated or scheduled extract refresh schedules.

Capture performance metrics and analyze

1. Run Tabjolt or any other tool of your choice to capture performance metrics on your current version of Tableau Server to set a baseline. Use workbooks that have calculations and use extracts as the data source for testing. For more information about how install and use Tabjolt, see the Tabjolt Installation Guide.

2. Perform a full backup to capture the metrics from the first step.

3. Upgrade your test environment to 10.5.3 or later. We are recommending 10.5.3 as the minimum version since the settings you need to enable in order to resolve performance issues later on are only available in 10.5.3 or later versions of Tableau.

4. **Checkpoint:** Run Tabjolt to compare workbook performance before and after upgrade.

   If you see performance degradation after upgrade at this step, it may be due to other Tableau Server issues and might require further investigations. For more information, see Record and Analyze Workbook Performance.

   If you see no difference in performance before and after upgrade, continue to the next step.

5. Select a subset of workbooks and run a full refresh of the extracts. Doing a full refresh will upgrade the extracts from .tde to .hyper.

6. **Checkpoint:** Run the tool again to compare the performance of your workbooks between step 4 and step 6 which is essentially before and after doing extract
refreshes. Specifically, check for workbooks with slower response times or failure to load.

Troubleshoot performance issues

If you find that you are unable to test due to performance issues, or you find that VizQL server is consuming all or most of the available memory on the machine while viewing them, follow **steps 1 through 3**.

For workbooks that load successfully, but have slower response after upgrade, follow **steps 4 and 5**.

1. Enable the following setting that checks the number of query nodes required for Tableau to generate the workbook and displays an error when the set limit is exceeded. This helps prevent VizQL process from consuming the memory resources on the machine that might result in critical Server issues:

   Use TSM CLI to run the following commands:

   ```
   tsm configuration set -k native_api.node_limit_checker_pre_rewrite_disable -v false
   tsm pending-changes apply
   ```

   **Note:** This setting is only available in Tableau Server 10.5.3 or later. While enabling this setting improves the reliability and stability of Tableau Server, you may see errors on a very small percentage of workbooks with when you enable this setting. For example, the Tableau team saw errors on 0.01% of the workbooks with this setting enabled on Tableau Online.

2. Test the workbooks by viewing or interacting with them. You should see an error message informing you about exceeding the node limits on workbooks that have performance issues - The error message might say something like: *Logical Query tree*
Tableau Server on Linux Administrator Guide

has 2348182 nodes, maximum number allowed is 1000000...."

3. Use Tableau Desktop to troubleshoot your workbook performance. Run this command to enable the node limit check in your Tableau Desktop:

    tableau.exe -DNodeLimitCheckerPreRewriteDisable=false

**Note:** This setting is only available in Tableau Desktop 10.5.3 or later.

In Tableau Desktop, download and open the workbooks that displayed the error message about high node limits in step 2. Try optimizing the performance of workbooks using methods described in the Best Practices for Creating Calculations in Tableau topic. If successful, then publish them to Tableau Server. If you are still experiencing performance issues, continue to the next step.

4. For workbooks that load successfully, but the overall response times is slower after upgrade, materialize calculations for your extract:

    Using Tabcmd:

    tabcmd refreshextracts --workbook "My Workbook" --addcalculations

    For more information, Compute Calculations Now option.

5. If you have a large number of workbooks that fall under the above category (overall response times is slower after upgrade), consider enabling the server wide setting to retain materialized calculations for all extracts when they are upgraded from .tde to .hyper:

    Using TSM CLI:

    tsm configuration set -k native_api.preserve_calculations_on_hyper_refresh_conversion -v true
    tsm pending-changes apply
Considerations for turning on this setting:

Turn this setting on only if majority of your workbooks require calculations to be materialized. There are resource and time costs associated with this setting, as described below:

- When this setting is set to true, the extract file size will increase, affecting the overall disk space.

- Extracts with materialized calculations take a longer time to refresh than extracts without materialized calculations.

This setting only affects extracts that are not yet upgraded to .hyper. Extracts already upgraded to .hyper before turning on this setting will not have the calculations materialized. This setting will also not affect workbooks and extracts published from Tableau Desktop, or any new extract refreshes published to Tableau Server that do not use the **Compute Calculations Now** option.

**Note:** This setting is only available in Tableau Server 10.5.3 or later.

6. Enable the extract refresh schedules and monitor the performance of your workbooks to make sure that your workbooks are performing as expected.

Capture the conclusions and results from your testing

Make a note of the settings and steps that helped resolve the performance issues to use them to prevent performance degradation when you upgrade your Production Tableau Server.

For example, if during your testing, you found that you needed to set the `native_api.preserve_calculations_on_hyper_refresh_conversion` setting to true, remember to disable your extract refreshes just before you upgrade your production Tableau Server.
After upgrade, set the `native_api.preserve_calculations_on_hyper_refresh_conversion` setting to true, and then re-enable your extract refreshes after you have confirmed that you are not experiencing slow response times after upgrade.

**Perform the Upgrade**

After you’ve completed the tasks in Prepare for the Upgrade, you're ready to upgrade your existing Tableau Server installation to version 2019.1

As a best practice, you should always make a backup of your Tableau Server data before upgrading, and save this backup in a safe place that is not part of your Tableau installation. This backup preserves your Tableau data if something unexpected happens during the upgrade, or if you need to go back to your previous version of Tableau Server. For more information, see Back up Tableau Server data.

Upgrade Tableau Server on Linux

To upgrade Tableau Server you install the new version while your existing version is running, then run an upgrade script to switch over to the new version. This reduces the amount of downtime for users because the server continues to run while you install the new version. You only stop the server to run the upgrade script.

**Important:** Upgrading Tableau Server on Linux from version 10.5.x (10.5.0 or later) requires special steps that are documented separately. For instructions for how to upgrade from 10.5.x, see Upgrade Tableau Server on Linux from 10.5.

General notes about upgrading:

All upgrades:

- **Backup**—Create a backup. You are responsible for creating a backup of your existing Tableau Server data before upgrading. We strongly recommend creating a backup before upgrading as this provides you with an up-to-date version of your data you can...
use if you need to go back to your earlier version of Tableau Server. For more information on properly preparing for an upgrade, see Prepare for the Upgrade.

- **Licenses**—
  
  - **Trial product keys**—You cannot directly upgrade a server that is running a trial product key from one major version to another (for example, from version 10.5.x to version 2018.x). To upgrade from one major version to another with a trial product key, install the new version of Tableau Server on a separate machine, activate a trial key there, and restore a backup from your existing version. For more information, see Confirm licensing requirements.

  - **Expired maintenance**—You cannot upgrade a server with a product key whose maintenance has expired or expires on a date earlier than the release date of the version you are upgrading to. If you attempt to upgrade a server in this state, your server will be unlicensed and the upgrade may fail. If your maintenance has expired or is too old, refresh your product key before you run the upgrade script to upgrade to your new version. If refreshing the key does not update maintenance to a valid date, check in the Tableau Customer Portal for a Tableau Server key with current maintenance. For details on refreshing the product key, see Refresh Expiration Date for the Product Key.

- **Ports**—Before upgrading, read and understand the requirements for ports: Tableau Services Manager Ports.

- **Install while running**—When you upgrade Tableau Server, you install the new version before uninstalling the old version. The upgrade process will leave the old version in place. You can uninstall the old version after the upgrade is complete to free up disk space, though this is not required.

- **Upgrade script**—To complete the upgrade and switch to the new version, after installing the new version on all nodes in your cluster, run the upgrade script `upgradetsm` on the initial node. The script is installed in the
\scripts.<version_code> directory. Run the script from the new version you just installed.

- **Multiple directories**—After an upgrade, you will see multiple versions of Tableau Server directories in the /packages directory. When the upgrade is completed successfully, you can delete the directories related to the older version you upgraded from. You can identify these by the version code in the directory name. For example, \scripts.<version_code>. For more information about version codes, see View Server Version.

Multi-node upgrades:

- **Node installation**—Run the installer on all nodes in a cluster.

The steps below describe the general process for an upgrade of Tableau Server on Linux. Upgrades from beta versions of Tableau Server on Linux are not supported. If you are a Tableau Server on Windows user and want to switch to Tableau Server on Linux, see Migrate Tableau Server from Windows to Linux.


As a best practice you should always make a full backup before upgrading any version of Tableau Server. Save this backup file to a location that is not part of your server installation. Creating and saving a backup preserves your pre-upgrade data and configuration and gives you a rollback option in the event of issues during the upgrade. For more information, see Back up Tableau Server data.

When upgrading Tableau Server on Linux, you do not need to uninstall the previous version. After upgrading you can uninstall the package for the previous version if you choose to do so. One reason to do this is to free up disk space used by the older version. To understand the difference between removing and uninstalling Tableau Server on Linux, see Uninstall Tableau Server.
Upgrading Tableau Server requires a stop and start the server as part of the upgrade process. During this stop/restart Tableau Server is unavailable.

Upgrading will also apply any pending changes. If you have pending changes you do not want applied, you can discard those changes using the `tsm pending-changes discard` command. To see what changes might be pending, use the `tsm pending-changes list` command.

Upgrading Tableau Server on Linux

Follow these steps on each node in your cluster to upgrade Tableau Server.

1. On each node in your cluster:
   a. Copy the new Tableau Server .rpm or .deb package to a location accessible from the computer you are upgrading.
      
      If you are upgrading a distributed deployment of Tableau Server, then copy the .rpm or .deb package to each node in the cluster or to a location accessible from each node.
   b. Log on as a user with sudo access to the computer you are upgrading.
   c. Navigate to the directory where you copied the .rpm or .deb Tableau Server package.
   d. Use the package manager to install the Tableau Server package.
      
      Do not install to a location using a symbolic link or to a directory on a Network File System (NFS) volume.
      
      • On RHEL-like distributions, including CentOS, you have the option to install Tableau to a non-default location. If you choose to do so, you need to take extra steps.
Tableau Server on Linux Administrator Guide

- **Default location**—To install to the default location (/opt/tableau/tableau_server), run the following commands:

  sudo yum update

  sudo yum install tableau-server-<version>.x86_64.rpm

- **Non-default location**—To install to a non-default location, you must use `rpm -i`. You will also need to install all dependent packages. See the note below.

  Run the following command:

  sudo rpm -i --prefix /preferred/install/path tableau-server.rpm

  **Note:** When you use `yum` to install Tableau Server, all dependent packages are automatically downloaded and installed. This is the preferred method for installing Tableau. If you want to install to a non-default location, or your organization does not allow you to use `yum` and you must install using `rpm -i`, you must also install all dependent packages separately. For information about installing dependent packages, see Installing Tableau Server on an Air-Gapped Computer Running Linux.

- On Ubuntu, run the following commands:

  sudo apt-get update
  sudo apt-get upgrade
  sudo apt-get -y install gdebi-core
  sudo gdebi -n tableau-server-<version>_amd64.deb

  2. After you have installed the new package on every node in your cluster, stop Tableau
3. With Tableau Server stopped, run the following command on the initial node. Do not run this command on any additional nodes.

```bash
sudo /opt/tableau/tableau_server/packages/scripts.<version_code>/upgrade-tsm -u <system_admin> --accepteula
```

where `<version_code>` is the long form of new version you are upgrading to, for example `scripts.20183.18.1128.2033`, and `<system_admin>` is a user with administrative permissions on the computer where the initial node is installed. You will be prompted for the password for the administrative user.

The `-u` option was added as of 2018.1. For more information, see Updated `upgrade-tsm` script. To see all the options available for the `upgrade-tsm` script, use the `-h` option. For example:

```bash
upgrade-tsm -h
```

4. After the upgrade is completed, exit the terminal session on the initial node and log in again. This ensures that your session will be using the updated TSM version.

5. Start Tableau Server:

```bash
tsm start
```

If you are planning to enable Tableau Prep Conductor on your Tableau Server, you can do so once you have completed upgrading your Tableau Server to 2019.1. Tableau Prep Conductor allows you to publish, run, and schedule flows on your Tableau Server and is available for Tableau Server 2019.1 and later. For more information, see the following topics:

- Licensing Tableau Prep Conductor
- Tableau Prep Conductor
Upgrade Tableau Server on Linux from 10.5

When you upgrade Tableau Server on Linux from version 10.5, you need to take several unique steps to complete the upgrade. These are necessary because of a change made after version 10.5.0 released, related to sudo privileges. For more information, see System User, sudo Privileges, and systemd. You only need to do these extra steps once, during the upgrade to 2018.1. This topic describes how to upgrade from version 10.5.0 or 10.5.x (10.5.1 or later) to version 2018.x (2018.1 or later).

If you attempt to upgrade from 10.5.0 or 10.5.x without following these instructions, warnings are displayed and the upgrade is canceled. You will not break your existing Tableau Server installation, but you cannot continue the upgrade.

To identify the version of your installation, see View Server Version.

Follow these steps to upgrade from 10.5.0:

1. Upgrade to 10.5.x—If you are running version 10.5.0, you must first upgrade to 10.5.x (10.5.1 or higher) by installing 10.5.x and running the upgrade-tsm script in the 10.5.x scripts directory on your initial node.

2. Install 2018.x—With 10.5.x installed and running as expected, install 2018.x but do not upgrade to this version yet.

3. Run TSM commands—Use TSM to stop the server and run three additional commands.

4. Migrate 10.5.x to single user—Run the migration script in the 2018.x scripts directory.
   Do this on every node in your cluster.
5. Upgrade to 2018.x— Upgrade Tableau Server by running the upgrade-tsm script from the 2018.x scripts directory on your initial node.

Upgrade to 10.5.x

If you are running version 10.5.0 of Tableau Server on Linux, the first step you need to take is to upgrade to a later version of 10.5. Beginning with version 10.5.1 changes were made that are needed in order to upgrade to 2018.1 or later. (If you are already on a version of 10.5 that is higher than 10.5.0, you can skip to the Install 2018.x step.)

To upgrade from 10.5.0 to a later version of 10.5:

1. On each node in your cluster:
   a. Copy the Tableau Server version 10.5.x .rpm or .deb package to location accessible from the computer you are upgrading.

   If you are upgrading a distributed deployment of Tableau Server, copy the .rpm or .deb package to each node in the cluster or to a location accessible from each node.

   b. Log on as a user with sudo access to the computer you are upgrading.

   c. Navigate to the directory where you copied the .rpm or .deb Tableau Server package.

   d. Use the package manager to install the Tableau Server package.

      • On RHEL-like distributions, including CentOS, run the following command:

        ```bash
        sudo yum install tableau-server-<version>.x86_64.rpm
        ```
On Ubuntu, run the following commands:

```
sudo gdebi -n tableau-server-<version>_amd64.deb
```

2. Stop Tableau Server. If you are upgrading a cluster, do this after you have installed the new package on every node in your cluster.

```
tsm stop
```

3. With Tableau Server stopped, run the following command on your initial node. Do not run this command on any additional nodes:

```
sudo /opt/tableau/tableau_server/packages/scripts.<version_code>/upgrade-tsm --accepteula
```

where `<version>` is the 10.5.x version you are upgrading to.

To see all the options available for the `upgrade-tsm` script, use the `-h` option. For example:

```
upgrade-tsm -h
```

4. After the upgrade is completed, ensure your session is using the updated TSM version by doing one of the following:

   - Use the source command:

     ```
     source /etc/profile.d/tableau_server.sh
     ```

   - Exit the terminal session on the initial node and log in again.

5. Start Tableau Server:

```
tsm start
```

Install 2018.x

Install the Tableau Server 2018.x package but do not upgrade to this version yet. Before you do so, you need to run several commands and a migration script. You can install the 2018.x
package without stopping the server. When you install the new package you are copying the software to your computer but not changing anything about the currently running version.

To install the 2018.x package, on each node in your cluster:

1. Copy the Tableau Server 2018.x .rpm or .deb package to location accessible from the computer you are upgrading.

   If you are upgrading a distributed deployment of Tableau Server, then copy the .rpm or .deb package to each node in the cluster or to a location accessible from each node.

2. Log on as a user with sudo access to the computer you are upgrading.

3. Navigate to the directory where you copied the .rpm or .deb Tableau Server package.

4. Use the package manager to install the Tableau Server package.

   • On RHEL-like distributions, including CentOS, run the following command:

     
     ```
     sudo yum install tableau-server-<version>.x86_64.rpm
     ```

   • On Ubuntu, run the following commands:

     
     ```
     sudo gdebi -n tableau-server-<version>_amd64.deb
     ```

Run TSM commands

Using version 10.5.x of Tableau Server that is installed and running:

1. Stop the server:

   ```
   tsm stop
   ```

2. Run these three commands:
Migrate 10.5.x to single user

Run this script from the 2018.x scripts directory:

```bash
sudo /opt/tableau/tableau_server/packages/scripts.<version_code>/migrate-to-single-user
```

where `<version>` is your 2018.x version number.

**Important:** If you have a multi-node installation, you must run this script on every node in your cluster.

At this point Tableau Server is running 10.5.x but configured to work with a single user. This is an interim stage. You should complete the upgrade to version 2018.x before using Tableau.

Upgrade to 2018.x

After completing the above steps:

1. Run the upgrade-tsm script for 2018.x on the initial node:

```bash
sudo /opt/tableau/tableau_server/packages/scripts.<version_code>/upgrade-tsm -u <tsm_system_admin> --accepteula
```
where `<version_code>` is the long version of the 2018.x version you are upgrading to, and `<system_admin>` is a user with administrative permissions on the computer where the initial node is installed. You will be prompted for the password for the administrative user.

The `-u` option was added as of 2018.1. For more information, see Updated `upgradetsm` script. To see all the options available for the `upgradetsm` script, use the `-h` option. For example:

```
upgrade-tsm -h
```

**Note:** If Tableau Server is not stopped the script will not run.

2. After the upgrade is completed, ensure your session is using the updated TSM version by doing one of the following:

   - Use the source command:
     
     ```
     source /etc/profile.d/tableau_server.sh
     ```

   - Exit the terminal session on the initial node and log in again.

3. Start Tableau Server:

   ```
   tsm start
   ```

   When desired, you can remove Tableau Server on Linux version 10.5 from your server. Unlike most other programs that run on Linux, previous Tableau Server versions are not automatically removed as part of a successful upgrade. To learn more, see Remove Tableau Server from Your Computer.

Related topics

   - Common Tableau Server Upgrade Issues
Troubleshoot Tableau Server Install and Upgrade

Follow the suggestions in this topic to resolve common issues with Tableau Server. For additional troubleshooting steps based on process status viewed on the Status page, see Troubleshoot Server Processes.

General Troubleshooting Steps

Many Tableau Server issues can be addressed with some basic steps:

1. Make sure there is enough disk space on each computer running Tableau Server. Limited disk space can cause a failure to install, a failure to upgrade, or problems running Tableau Server.

2. Restart Tableau Server. Issues related to indexing and processes not fully started can be resolved by restarting Tableau Server in a controlled way. To restart Tableau Server, use the `tsm restart` command. This will stop all the processes associated with Tableau Server and then restart them.

3. Reindex Tableau Server. Issues related to indexing can be resolved by reindexing Tableau Server. To reindex Tableau Server, use the `tsm maintenance reindex-search` command. For more information, see Reindexing Tableau Server Search & Browse below.

4. Restart the computer on which Tableau Server is running. Some issues, such as those related to data source connectivity, can be resolved by restarting the server computer.

Common Tableau Server Install Issues

Installation logs location

The install log, `app-install.log`, is located in `/var/opt/tableau/tableau_server/logs`. 

---

Tableau Software Version: 2019.1
The upgrade log, app-upgrade.log, is located in /var/opt/tableau/tableau_server/logs.

Unable to log into TSM or Tableau Server (sign in screen redisplays after entering credentials)

Using Internet Explorer or Edge, if you enter your credentials into the TSM or Tableau Server sign-in screen and the page redisplays without signing you in, verify that the hostname or domain in your URL does not include an underscore (_). If the hostname or domain of the Tableau Server computer includes an underscore (_) Internet Explorer or Edge browsers will not set a cookie, so the page will redisplay without signing you in. To work around this, use "localhost" or the IP address of the computer in the URL. For example: https://localhost:8850.

For more information, see the Tableau Knowledge Base.

Multiple install attempts fail

If you attempt to install Tableau Server and the install fails, any subsequent installation attempts are likely to fail unless you run the tableau-server-obliterate script to clean Tableau off the computer.

A failed install attempt can leave the computer in a state that causes subsequent attempts to also fail with errors that don't seem directly related to a previous install attempt. One possible error is:

Enabling and starting all services
+ services=(appzookeeper* tabadmincontroller* tabsvc* licenseservice* fnplicenseselect* tabadminagent* clientfileservice*)
+ systemctl_user enable appzookeeper_0.service
  'tabadmincontroller*' 'tabsvc*' 'licenseservice*' fnplicenseservice_0.service 'tabadminagent*' 'clientfileservice*' ++ id -ru a_tabadminpoc
+ local unprivileged_uid=222954
+ su -l a_tabadminpoc -c 'XDG_RUNTIME_DIR=/run/user/222954'
systemctl --user enable appzookeeper_0.service tabadmincontroller* tabsvc* licenseservice* fnpliceseservice_0.service tabadminagent* clientfileservice

Failed to execute operation: No such file or directory

To fix this problem, run the tableau-server-obliterate script to clean up any leftover remnants of the previous install attempt and then restart the computer. For more information, see Running the tableau-server-obliterate script.

**Important:** If you created a backup of Tableau (<file>.tsbak) you want to keep (for example, to restore to your new installation), copy that file to a safe location on another computer to guarantee it is not removed when you clean up your Tableau computer.

Install fails due to hardware requirements

Tableau Server cannot install if the computer you are installing on does not meet the minimum hardware requirements. The requirements apply to all computers on which you are installing Tableau Server. For details on minimum hardware requirements, see Minimum Hardware Requirements and Recommendations for Tableau Server.

Common Tableau Server Upgrade Issues

Upgrade logs location
The upgrade log, app-upgrade.log, is located in /var/opt/tableau/tableau_server/logs.

Upgrade multi-node, initializing additional node fails with "Enter your credentials again" error

If you attempt to initialize an additional node when upgrading Tableau Server and see this error:

Enter your credentials again. The credentials you enter must provide administrative access to the computer where you generated the configuration file.
this is an indication that the node is unable to connect to or communicate with the initial
node. This can happen for multiple reasons:

- The credentials you entered are not valid or you mistyped them. The credentials must
  be for a user who has administrative permissions on the computer where Tableau
  Server was first installed. You do not need to use the credentials of the user who cre-
  ated the bootstrap file but doing so will ensure you are using valid credentials.

- The local firewall of the computer you are trying to add is not allowing communication
to the initial node. For more information, see Local firewall configuration.

- The nodes are on different subnets. In distributed installations, all nodes should be
  installed on the same subnet. For more information, see Distributed Requirements.

Upgrading fails due to lack of disk space

If there is not enough disk space for the Tableau Server Setup program to run and do the
upgrade, the installation will fail. The amount of disk space required will depend on the size
of your repository database and the number and size of your extracts. As a part of upgrad-
ing to version 9.0, the Setup program migrates extracts to the new File Store and this takes
space.

To free up disk space:

1. Create a log archive snapshot using the $tsm maintenance ziplogs$ command.

   After you create the ziplogs file, save it to a safe location that is not part of your
   Tableau Server installation.

2. Clean up unnecessary files using the $tsm maintenance cleanup$ command.
   For more information, see Remove Unneeded Files.
Tableau Server on Linux Administrator Guide

Starting Tableau Server

Tableau Server cannot determine if it fully started

In some instances Tableau Server may report that it could not determine if all components started properly on startup. A message displays: "Unable to determine if all components of the service started properly."

If you see this message after starting, verify that Tableau Server is running as expected by using a `tsm status -v` command.

If the status shows as running ("Status: RUNNING"), then the server successfully started and you can ignore the message. If the status is DEGRADED or STOPPED, see "Tableau Server doesn't start" in the next section.

Tableau Server doesn't start

If Tableau Server does not start or is running in a degraded state, run the `tsm restart` command from a command prompt. This will shut down any processes that are running, and restart Tableau Server.

Reindexing Tableau Server Search & Browse

Problems that can be solved by rebuilding Search & Browse index

Symptoms of an index that needs to be rebuilt include:

- A blank list of sites when a user attempts to log in
- A blank list of projects when a user tries to select a project
- Missing content (workbooks, views, dashboards)
- Unexpected or inaccurate alerts (for example, an "refresh failed" alert on a workbook that does not include an extract)

If you see any of these behaviors, reset and rebuild the Search & Browse index using the `tsm maintenance reset-searchserver` command.
Activating Tableau Server

Tableau Server license activation fails

In some instances Tableau Server license activation may fail. Error messages can range from a very generic one:

- An error has occurred

To more specific messages:

- Function flxActCommonLicSpcPopulateFromTS returned error 50030, 71521,
- No license found for 'Tableau Server'

To resolve this issue, try these solutions in the order listed:

Confirm you can access the licensing server

The Tableau licensing service was moved to a new data center on October 6, 2018. This means any environments that required special configuration (static IP safe listing for example) to access licensing.tableau.com or licensing.tableausoftware.com will need to be updated before you can activate, refresh, or deactivate a Tableau product key.

Tableau Server needs to connection to the following internet locations for licensing purposes:

- licensing.tableau.com:443
- atr.licensing.tableau.com:443
- o.ss2.us
- ocsp.rootg2.amazontrust.com
- ocsp.rootca1.amazontrust.com
- ocsp.sca1b.amazontrust.com
Requests to the above domains may be on port 80 or 443.

Verify the date and time

Verify the date and time on the initial Tableau Server computer is correct. If the clock is set to a time and date earlier than the current date, Tableau Server cannot be activated.

Force the product key to be read again

1. On the initial Tableau Server computer, sign in as administrator and open a command prompt.

2. Change to the Tableau Server bin directory. By default this is:

   /opt/tableau/tableau_server/packages/bin.<version_code>/
3. Type the following commands:

   tsm stop

   ./lmreread

   tsm start

Send the contents of trusted storage to Tableau Support

If FlexNet Licensing Services is installed and running but you’re still seeing an error, there might be a problem with the Tableau product key information. To resolve this issue, complete the following steps to create a file of the key information located in trusted storage.

1. On the initial Tableau Server computer, sign in as administrator and open a command prompt.

2. Type the following command:

   serveractutil -view > <machine_name>-LicResults.txt

   This creates the <machine_name>-LicResults.txt file in your current directory. If you don’t have write permissions for that location and see an error, change to a location where you do have permission to create a file and run the command again.

3. Contact Tableau Support (http://www.tableau.com/support/request) and include the <machine_name>-LicResults.txt file that you created.
Manage Sites

What is a site ........................................................................................................... 409
Planning a Site ....................................................................................................... 412
Manage Users and Groups .................................................................................... 415
Dashboard-based Custom Portals ........................................................................ 470
Data Connection Authentication ............................................................................. 474
Manage Content Access .......................................................................................... 494

What is a site

You might be used to using the term site to mean “a collection of connected computers,” or perhaps as the short form of “website.” In Tableau-speak, we use site to mean a collection of users, groups, and content (workbooks, data sources) that’s walled off from any other groups and content on the same instance of Tableau Server. Another way to say this is that Tableau Server supports multi-tenancy by allowing server administrators to create sites on the server for multiple sets of users and content.

All server content is published, accessed, and managed on a per-site basis. Each site has its own URL and its own set of users (although each server user can be added to multiple sites). Each site’s content (projects, workbooks, and data sources) is completely segregated from content on other sites.

If you are a server administrator on your Tableau Server deployment, you can learn more about sites, when to use them (vs. projects), and more in Sites Overview, in the Manage Server section.
Site administrator tasks

Where the Server Administrator site role gives a user unrestricted access to the entire Tableau Server deployment, the Site Administrator site roles give a user unrestricted or minimally restricted access at the site level. The differences between Site Administrator Creator and Site Administrator Explorer are in the level of data connection and publishing access. Both site roles allow administering the site itself and managing site users. For more information, see Set Users’ Site Roles.

Although a server administrator can work at both the server and site levels, we make a distinction between the two levels of task. The site administrator is typically in charge of creating and maintaining the framework that enables Tableau users in the organization to publish, share, manage, and connect to data sources and workbooks. In this vein, site administrator tasks include any of the following (and both site roles allow this level of access):

- Creating project hierarchies to organize the site’s data sources and workbooks.
  This can include delegating project-level management to project leaders.

- Creating groups and assigning permissions that allow users to access only the content they need.

- Adding and removing users, assigning their site roles.
  This is allowed by default on a site; however, a server administrator can restrict this access to the server level only.

- Managing the site’s extract and subscription schedules.

- Monitoring site activity.
For more information about the distinction between server administrator and site administrator, see Administrator-level access to sites, in the Manage Server section.

Steps for setting up your site

The table below shows a loose sequence of steps for setting up a site, along with links to topics where you can get more information. You can complete the steps in any order that makes sense for you.

However, before you perform the steps to configure the site, we recommend spending some time with the articles in this section, learning about site authentication, site roles, projects, and permissions. Ideally you would document a plan for your projects, groups, and overall permissions strategy. Then set up a few projects and add a preliminary set of users, to test the plan and resolve issues before you add the remaining users. You can change many site settings after your users are working with the site, but try to go in with the intention of minimizing post-production changes.

<table>
<thead>
<tr>
<th>Plan</th>
<th>To supplement the recommendations above this table, get an overview of how the site components work together in Planning a Site.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure access</td>
<td>Work with the server administrator to determine how users sign in to the site, and configure the site appropriately. For example, if the server is configured for single sign-on using SAML, you might configure SAML authentication at the site level as well.</td>
</tr>
<tr>
<td>Create projects and the permissions structure</td>
<td>Projects help you organize content, delegate project-level content management, and manage permissions effectively. To get started, see Use Projects to Manage Content Access.</td>
</tr>
<tr>
<td>Add users</td>
<td>Determine the users who can sign in to the site. See Add Users to a Site.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Get your data to Tableau Server</td>
<td>After you create your projects and permissions structure, designate approved users for publishing and managing vetted data sources to the appropriate projects on the site. In some organizations, people serve in multiple Tableau roles. Site administrators commonly also are data stewards. By that, we mean they create, publish, and manage the Tableau data connections. If this is you, make sure you are assigned the Site Administrator Creator site role. After content is published to the site, you can maintain connection information (credentials, access tokens) and refresh schedules. For more information, see Refresh Data on a Schedule.</td>
</tr>
<tr>
<td>Analyze site usage and performance</td>
<td>Monitor usage, performance, and other metrics. See Administrative Views.</td>
</tr>
</tbody>
</table>

### Planning a Site

Before you add users and content to a site, we recommend that you plan the following aspects of the site.

- **Projects**
- **Users and groups**
The subsequent sections go over these site components, assuming that you are familiar with

**Note:** This article and section apply only to self-managed Tableau Server deployments on-premises or in the cloud. If you use Tableau Online, see Manage Content Access.

### Projects

You can create projects on a site, which act as containers in which you can organize related content assets (such as data sources and workbooks). For example, you might set up a project to contain all of the certified data sources and workbooks your organization uses for mission-critical decisions. Or you might set up projects by department.

Projects are also useful for managing permissions. Once you know how your users need to access content, it’s usually easier to create projects based on those the type of content, and maintain permissions at the project level.

Every site has a default project named **Default**. When you create projects, the new projects get their initial set of permissions from the default project. In effect, the default project is a template for new projects. As we explain in related articles, for most environments, we recommend that you use the Default project only as a permissions template, and not as a container for published content.

For more information, see Use Projects to Manage Content Access.

### Users and groups

Any user who will publish content or access published content on a site must be able to sign in to the site. If the user already has an account on the server, you’ll need to add that user to the appropriate site. You can add a user to more than one site as well. If the user doesn’t
already exist, you need to create a user account. Either way, make a list of the users who will need to be able to sign in to each site.

**Note:** The server license might restrict how many users you can have, or what level of access they can have. Check with the server administrator to make sure that you’ll be able to have an account for all your users.

In general, we recommend that you create groups on the server and then add users to the groups. This helps to make permissions much easier to manage. You can assign permissions on groups, to give those permissions to all users in the group. (See the next section.)

A typical strategy is to create groups for users who use content in similar ways. For example, you might create a group named SalesWBPublishers for all the users in the Sales department who publish workbooks, and a separate group named SalesDSPublishers for people in Sales who publish data sources. Each of these sets of users needs its own set of capabilities, so it makes sense to have a group for each for these needs.

**Site roles and permissions**

Each user has a *site role* that determines the maximum permissions that they can have on the site. As part of your site planning, you need to decide each user’s site role. A user with a site role that’s too restrictive might not be able to do the work they need. By the same token, a security best practice is to limit users’ capabilities to only those that they need to do their work. This is referred to as following the principle of *least privilege*.

You or a site administrator you delegate this task to must also determine the permissions a user needs to work with content. Each content asset (workbook, data source, project) supports a set of *capabilities*. For example, you can View or Add Comments to a workbook. Before a user can perform tasks on a workbook, their permissions must allow those capabilities. A recommended practice is to sketch out a mapping of permissions to users outside of Tableau before you try to set this up on the server.
Permissions determine what a user can do within the context of the site role. A user whose site role is **Viewer** can never publish to the site, regardless of the permissions you grant them. A user whose site role is **Creator** can publish a workbook to the site, but only if that user has permission to save and view workbooks.

**Extract refresh schedules**

If users publish data sources or workbooks that include extracts, you usually want to make sure that the extracts are refreshed, so that they contain the latest data. Users can manually refresh an extract, but this isn’t always a good idea if the extract is large, and the refresh takes a long time. Instead, you can set up schedules for when an extract should be refreshed. Another planning task for a site administrator, therefore, is to think about when extracts should be refreshed and to work out schedules.

**Manage Users and Groups**

**Add Users to a Site**

Everyone who needs to access Tableau Server—whether to browse, publish, edit content or administer the site—must be added as a user. Administrators have the following options for adding users:

- Add a local user account or a user account from Active Directory, described later in this article.

You can also add users by importing an Active Directory group. See Create Groups via Active Directory.

For Tableau Server on Linux, all external directory communication is configured and managed with a LDAP identity store. In the context of user and group synchronization, Tableau Server configured with LDAP identity store is equivalent to Active Directory. Active Directory synchronization features in Tableau Server function seamlessly with...
properly configured LDAP directory solutions.

- Import Users via a CSV file that you create using the CSV Import File Guidelines.

Site administrator access to user management

By default site administrators can add and remove users on a site. On the site’s Settings page, server administrators can revoke that capability, so that only server administrators can manage the site’s users.

A site administrator can edit an existing local user account only if the administrator has access to all of the sites the user is a member of. For example, if User1 is a member of sites A and B, an administrator of only site B cannot edit User1’s full name or reset the password.

Add local users to a site

1. Sign in to Tableau Server as an administrator, and if applicable select the site.

2. At the top, select Users. On the Users page, click Add Users, and then click New User.

   ![Add Users to this Site](image)

3. Enter a user name. With local authentication, using an email address for the user name is the best way to avoid user name collisions (for example,
User names are not case sensitive. Characters not allowed in user names include the semi-colon (;) and colon (:).

Also enter information in the following fields:

- **Display Name**—Type a display name for the user (e.g., Laura Rodriguez).
- **Password**—Type a password for the user.
- **Confirm password**—Retype the password.
- **Email**—This is optional and can be added at a later time in the user profile settings.

4. Select a site role.

For site role definitions, see Set Users' Site Roles.
5. Click **Add User**.

Add Active Directory users to a site

Before adding users to a site, be sure to review User Management in Active Directory Deployments to understand how multiple domains, domain naming, NetBIOS, and Active Directory user name format influence Tableau user management.

1. In a site, click **Users**, and then click **Add Users**, and then click **Active Directory User**.

2. Enter one or more user names (separated by semicolons).

   For example, *tdavis; jjohnson; hwilson*

   If you are adding a user that is from the same Active Directory domain that the server is running on, you can type the AD user name without the domain. The server’s domain will be assumed.

   **Note:** Do not enter the user’s full name in this field; it can cause errors during the importing process.

3. Select a site role.
Set Users’ Site Roles

When you add users to a site on Tableau Server or Tableau Online, independent of their license type, you must apply a site role to them. The site role signifies the maximum level of access a user can have on the site. Along with content permissions, the site role determines who can publish, interact with, or only view published content, or who can manage the site’s users and administer the site itself.

How user licenses, site roles, and content permissions work together

The intersection of a user’s license type, site role, and content permissions determines the level of access a user has on the Tableau site.

1. The license type is associated with the user. The site role you want to assign to the user determines the license type they will require.

   In a multi-site environment on Tableau Server, a user’s license applies to all sites the user is a member of.

2. The site role is also set at the user level. In a multi-site environment, you assign site roles on each site. For example, the same user can have the Site Administrator Creator site role on one site, and Viewer site role on another site.

   The site role defines the maximum capabilities the user has to work with content on the site, or manage users or the site itself.

3. Whether the site role’s maximum capabilities are available to the user depends on the permissions set on the content resources (projects, data sources, workbooks).

   For example, let's say that User A has the following access on a site:

   - Creator license (due to their access on another site)
   - Explorer site role (on this site)
   - Publisher permissions on a project (on this site)

   In this scenario, even though the license allows connecting to and creating new data sources in the web editing environment or Tableau Desktop, and the content resources allow publishing, the site role denies publishing new content on that site.
Similarly, if User A’s site role and license are both Creator, the user can connect to and save (publish) new data sources only in projects on which permissions settings grant those capabilities.

For more information, see Content Permissions and Ownership.

Change a user’s site role

1. Sign in to the site as a server or site administrator, and go to the Users area.

   If you are a site administrator and do not see the Users area, check with your server administrator on whether they have denied user management capabilities to site administrators.

2. Select the users, and then select Actions > Site Role.

3. Select the new site role, and then click Change Site Role.
You can hover the pointer over the information icon to display a matrix that shows the maximum level of general capabilities each site role allows. For more information, continue to General capabilities allowed with each site role.

General capabilities allowed with each site role

The following table lists the license types as of version 2018.1, the highest level of site role allowed with each, how each site role maps to its pre-2018.1 equivalent; and summarizes the maximum capabilities each site role allows.

What this article covers and where to find what’s not covered here

- This information focuses on site roles and is more generalized. For a list of common specific tasks available per license role, see the matrix on the For Teams & Organizations tab on the Tableau pricing page.

- This information describes site roles as of version 2018.1. To learn more about how core-based licensing relates to user-based licensing, how licenses transfer, or other specific licensing transition scenarios, start with the following topics:

  Migrate from Core-Based to User-Based Licensing

  Troubleshoot Licensing
Tableau site roles as of version 2018.1

<table>
<thead>
<tr>
<th>Site role name as of version 2018.1</th>
<th>Previous site role name</th>
<th>Maximum capabilities this site role allows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site roles that use a Creator license</td>
<td></td>
<td></td>
</tr>
<tr>
<td>—Users with these site roles have access to Tableau clients such as Tableau Prep, Tableau Desktop, Tableau Bridge, and Tableau Mobile.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server Administrator</td>
<td>Server Administrator</td>
<td>Available on Tableau Server only; not applicable to Tableau Online.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This site role always occupies the highest license activated on the server between Creator and Explorer. It allows unrestricted access to the configuration settings for the Tableau Server browser environment, all sites on the server, users and groups, and all content assets, such as flows, projects, data sources (including connection information), and workbooks.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connect to Tableau published data sources or external data, from the browser, Tableau Desktop, or Tableau Prep; create and publish new data sources; author and publish workbooks.</td>
</tr>
<tr>
<td>Site Administrator Creator</td>
<td>--</td>
<td>This is the highest level of access for Tableau Online.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unrestricted access to content as described above, but at the site level. Connect to Tableau or external data in the browser, Tableau Desktop, or Tableau Prep; create new data sources; build and</td>
</tr>
<tr>
<td>Site role name as of version 2018.1</td>
<td>Previous site role name</td>
<td>Maximum capabilities this site role allows</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>publish content.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On Tableau Server, server administrators can determine whether or not to allow site administrators to manage users and assign site roles and site membership. By default, on Tableau Server, and always on Tableau Online, site administrators are allowed these capabilities.</td>
</tr>
<tr>
<td>Creator</td>
<td>--</td>
<td>This is similar to the former Publisher site role, but allows new features. This site role offers non-administrators the maximum level of <em>content</em> access.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connect to Tableau or external data in the browser, build and publish flows, data sources and workbooks, have access to Dashboard Starters, and use interaction features on published views. Can also connect to data from Tableau Prep or Tableau Desktop, publish (upload/save) and download flows, workbooks and data sources.</td>
</tr>
</tbody>
</table>

**Site roles that use an Explorer license**

—Users with these site roles can access the server from the browser or Tableau Mobile.

<table>
<thead>
<tr>
<th>Server Administrator</th>
<th>N/A</th>
<th>Tableau Server only; not applicable to Tableau Online.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>If Explorer is the highest license type activated on the server when a new server administrator user is created, the user’s site role is Server Administrator;</td>
</tr>
<tr>
<td>Site role name as of version 2018.1</td>
<td>Previous site role name</td>
<td>Maximum capabilities this site role allows</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Site Administrator Explorer</td>
<td>Site Administrator</td>
<td>however, the user will not have the connecting and publishing capabilities that come only with the Creator license. With the Explorer license a Server Administrator has unrestricted access to the configuration settings for the Tableau Server browser environment, all sites on the server, users and groups, and all content assets, such as projects, flows, data sources (including connection information), and workbooks. However, with the Explorer license, a Server Administrator cannot connect to Tableau published data sources or external data, from the browser, Tableau Desktop, or Tableau Prep; they cannot create and publish new data sources; and they cannot author or publish workbooks.</td>
</tr>
<tr>
<td>Explorer (Can Publish)</td>
<td>Publisher</td>
<td>Same access to site and user configuration as Site Administrator Creator, but cannot connect to external data from the web editing environment. Can connect to Tableau published data sources to create new workbooks, and edit and save existing workbooks. Can publish workbooks from the web using existing data sources, browse and interact with published views, use all interaction features, and can save new standalone data sources from data connections</td>
</tr>
<tr>
<td>Site role name as of version 2018.1</td>
<td>Previous site role name</td>
<td>Maximum capabilities this site role allows</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>Explorer</td>
<td>Interactor</td>
<td>Can browse and interact with published views. Can subscribe to content, create data driven alerts, connect to Tableau published data sources and open workbooks in the web authoring environment for ad-hoc queries, but they cannot save their work.</td>
</tr>
<tr>
<td>Read Only</td>
<td>Viewer</td>
<td>This site role is available only in version 2018.1, for transitioning users to the user-based Viewer (or other) license and site role. Any users in the Read Only site role prior to upgrading to version 2018.2 or later are reassigned to the Viewer site role. In 2018.1 versions, Read Only users can see and subscribe to published views others have created. Cannot use other interaction features or save custom views.</td>
</tr>
</tbody>
</table>

### Site roles that use a Viewer license

| Viewer | N/A | Can see published and custom views others have created; can use most interaction features, such as subscribing to views, downloading as images, and downloading summary data. Cannot connect to |

**Tableau Server on Linux Administrator Guide**
### Site role name as of version 2018.1

<table>
<thead>
<tr>
<th>Site role name as of version 2018.1</th>
<th>Previous site role name</th>
<th>Maximum capabilities this site role allows</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>data; create, edit, or publish content; or set data alerts. For a list of specific capabilities, see the Viewer column in the matrix on the Tableau pricing page. <strong>Note:</strong> Although the Viewer site role existed in previous versions, the new Viewer site role has additional capabilities.</td>
</tr>
</tbody>
</table>

### Other site roles

<table>
<thead>
<tr>
<th>Unlicensed</th>
<th>Unlicensed</th>
<th>Unlicensed users cannot sign in to Tableau Server or Tableau Online. Users are assigned the Unlicensed role in the following circumstances:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>- You import users from a CSV file and their license level is set to unlicensed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The number of available licenses is reached at the time you add or import users.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- You remove a user who owns content on the site. The user will still own the content but not be able to do anything with it.</td>
</tr>
</tbody>
</table>

### Who can publish content

The following site roles allow the specified level of publishing access.
Server Administrator (Tableau Server only); Site Administrator Creator; and Creator allow full connecting and publishing access.

This includes connecting to data and publishing new flows, new workbooks, and new data sources from Tableau Desktop and the web editing environment. The site roles also allow editing and saving existing published workbooks, or publishing updates to existing data sources.

- Explorer (Can Publish) and Site Administrator Explorer have limited publishing capabilities, as described in General capabilities allowed with each site role.

- Explorer, Viewer, Read Only, and Unlicensed do not allow publishing.

Site roles and Active Directory import and synchronization

When you import Active Directory users to a site, you can specify the site role. If a user is not yet a member of any site on the server, the user is added to the site with the assigned role.

When you synchronize Active Directory groups, the site role is applied through the Minimum Site Role setting on the Groups - Details page.

**Note:** If you run Tableau Server on Linux, all external directory communication is configured and managed with a LDAP identity store. In the context of user and group synchronization, Tableau Server configured with LDAP identity store is equivalent to Active Directory. Active Directory synchronization features in Tableau Server function seamlessly with properly configured LDAP directory solutions.

If a user already exists in a Tableau Server site, the site role assigned during the import or sync process will be applied if it gives the user more access in a site. Importing or synchronizing AD users and groups can promote a user’s site role, but does not demote a user’s site role.

If a user already has the ability to publish, that ability is maintained.

The matrix below shows the rules applied for site roles on import.
Note: The **Import Site Role** row abbreviated headers indicate the site role specified for import. The **Current Site Role** column headers represent the current user site role. The table values represent the abbreviated resulting site role.

- Site Administrator: SA
- Site Administrator Creator: SC
- Site Administrator Explorer: SE
- Creator: C
- Explorer: E
- Explorer (Can Publish): EP
- Viewer: V
- Unlicensed: U

<table>
<thead>
<tr>
<th>Import Site Role</th>
<th>Current Site Role</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SC</td>
</tr>
<tr>
<td>Site Administrator Creator (SC)</td>
<td>SC</td>
</tr>
<tr>
<td>Site Administrator Explorer (SE)</td>
<td>SE</td>
</tr>
<tr>
<td>Creator (C)</td>
<td>SC</td>
</tr>
<tr>
<td>Explorer</td>
<td>SE</td>
</tr>
</tbody>
</table>
View, Manage, or Remove Users

Administrators can manage a site’s users such as adding and removing users, setting the groups they’re members of, setting their site roles, and so on. On Tableau Server, server administrators can manage users on multiple sites at a time on the All Sites page.

View and manage users on a site

Sign in to a site as an administrator, and then select Users. On this page you can do any of the following to manage users:

- Set group membership, set site role, or remove the user from the site. If you’ve configured the site for SAML single sign-on, you can set the selected users’ authentication type.
• Select a user name to see details about them, such as content they own, views they subscribe to, and their account settings.

The user **Settings** page is available when the following conditions are true:

• The user is a member only of sites that the site administrator controls

• Site administrators can manage users. This is always the case for Tableau Online and is the default for Tableau Server; Tableau Server administrators can change this access for site admins.
If the server is configured to use the internal user management system (Local Authentication), you can edit the Display Name, Email, and Password for users after they have been added. If you are making many changes, you may find it easier to import the changes from a CSV file. For details, see Import Users and CSV Import File Guidelines.

**View and edit server users**

Sign in to Tableau Server as a server administrator. On the site menu, select **Manage All Sites**, and then select **Users**.
Manage users’ site membership

By default, server and site administrators can manage users at the individual site level. Server administrators can also manage users and their site roles on multiple sites. You do this at the All Sites level (at the server level).

1. In the site menu, select Manage All Sites, and then select Users.

2. On the Server Users page, select the check boxes next to the users, and then select Actions > Site Membership.

3. Select one or more sites, and a site role for each site, and then click Save.

Search for users

To search for a specific user
Use the filter toggle in the upper right to display the search box and site role filter. Then use the search box or filters to find the users you want.

The search operation checks the display name and user name attributes.

You can use the asterisk (*) character as a search wildcard. For example, searching for John* will return all user names that start with John.

Remove users from a site

You can remove a user only if the user does not own any content (projects, workbooks, views, or data sources). If you attempt to remove a user who owns content, the user site role will be set to Unlicensed, but the user will not removed.

**Note:** On Tableau Server, when an administrator removes a user from a site (and the user belongs only to that one site), the user is also deleted from the server.

1. Sign in to a site as an administrator, and go to the **Users** area. Select one or more users to remove, and then select **Actions** > **Remove**.
2. Click **Remove** in the confirmation dialog.

**Remove users from the server**

You can remove a user only if the user does not own any content (projects, workbooks, views, or data sources). If you attempt to remove a user who owns content, the user site role will be set to Unlicensed, but the user will not removed.

If a user is a member of multiple sites, and they own content on any of those sites, they are removed from the sites on which they don’t own content. The user remains a member on sites where they own content, but demoted to the Unlicensed site role.

1. In the site menu, click **Manage All Sites**, and then click **Users**. In a single-site environment, click **Users**.

   Select one or more users to delete, and then click **Actions > Delete**.
2. Click **Delete** in the confirmation dialog box.

**Change passwords for users of a single site**

To change the password for a user with membership to a single site, sign in to Tableau Server as a site administrator or a server administrator.

1. Ensure that the correct site is selected in the menu.

2. Click **Users**.

3. Click the display name of a user.

4. Click **Settings**.

5. Click the **Change Password** link, edit the password, and then click **Save**
Change passwords for users of multiple sites

To change the password of a user with membership to multiple sites, sign in to Tableau Server as a server administrator.

1. In the site menu, click **Manage All Sites**.
2. Click **Users**.
3. Click the display name of a user.
4. Click the Change Password link, edit the password, and then click Save Password.

Set the User Authentication Type for SAML

On a site that has been configured for site-specific SAML, administrators can specify users’ authentication type. For example, if Tableau Server was configured for site-specific SAML and server-wide SAML, administrators can specify which users authenticate with site-specific SAML and which users authenticate with server-wide SAML.

You can assign authentication type at the time you add users to Tableau Server, as well as any time afterward.

1. When you’re signed in to the Tableau Server site, select Users.

2. On the Site Users page, select the check boxes next to the users you want to assign an authentication type.

3. On the Actions menu, select Authentication.
4. In the Authentication dialog box, select **Site SAML** or **Server Default**.

**Notes**

- Users that authenticate with site-specific SAML can only belong to one site. If a user needs to belong to multiple sites, set their authentication type to the server default. Depending on how site-specific SAML was configured by the server administrator, the server default is either local authentication or server-wide SAML.

- If you change users’ authentication to site-specific SAML, the next time they sign in, they will be directed to your identity provider's site to provide their credentials.

**Import Users**

To automate the process of adding users to a site, you can create a CSV file that contains user information, and then import the file.

Site administrators can import users to a particular site; server administrators (Tableau Server only) can import users at the server level, to later add them to multiple sites.

**Note:** This topic contains the steps for importing, assuming that you have already created the CSV file. If you have not created the file yet, see CSV Import File Guidelines for a list of file format requirements and import options.
Add users from a CSV file

The following steps describe how to add users to a site or to the server. The images reflect adding users at the site level.

1. Do one of the following:

   - To add users at the site level, select Users, and then Add Users.

   ![Add Users to this Site](image)

   - To add users at the server level on a single-site server, select Users, and then Add Users.

   - To add users at the server level on a multi-site server, open the list of sites, and select Manage All Sites. Select Users, and then Add Users.

2. Click Import From File, click Browse and navigate to the file, and then click Import Users.
3. Click **Done**.

**How users’ site roles are assigned or maintained**

When you import at the site level or on a single-site server using `tabcmd`, you can specify the site role for all users in the CSV file. If a user already exists in the Tableau Server site, the site role assigned during the import process will be applied, even if it is more restrictive than users’ existing site role. The exception is that you cannot affect a server administrator’s site role.

For a multi-site server, when you import users in the Server Users page, you create server users with no site affiliation. Because these users do not belong to a site, they cannot have a
site role. The only site role a user can have at the server level is **Unlicensed** or **Server Administrator**.

You can also specify the user’s site role when you assign site membership to a user. For information, see Manage users’ site membership.

**Importing at the server level in multi-site environments**

If the server is running multiple sites and you are a server administrator, you can import a CSV file from two locations. Where existing user accounts are concerned, each location has different capabilities.

- The **Server Users** page appears in a multi-site environment. Only server administrators can access this page.

You can import the CSV file from here if you want to update existing user accounts in addition to adding new ones. For example, if you import a file that has a new password for each existing user, their passwords will be reset.

- The **Site Users** page.
Server administrators can add new user accounts with CSV imports. If the CSV file includes existing users, the **Password** and **Display Name** fields must either match the existing or be left blank. If new passwords or full names are used, the import will fail.

**Importing to a single-site environment**

Server and site administrators on a single-site server perform CSV user imports from the **Users** page in a site.

**Multi-site versus single-site import**

Users can belong to more than one site on the same server, but they must use the same credentials for each site. This becomes important when you’re adding users to a site and those users might already be members of a different site. If you try to import a user who already
exists, and if the user’s credentials in the CSV file don’t match the existing credentials, the import fails for that user.

If you’re importing users to a site and think the users might already exist on the server, you can try leaving the **Password** field in the CSV file blank (while including the delimiters for the field). If a user who is defined in the CSV already exists in another site, the user is added to the site where you’re importing. However, if the user *doesn’t* already exist on the server, the user is created, and the CSV import window alerts you that the new user doesn’t have a password. You can then use the server administrator pages to assign a password to any user who doesn’t have one.

**Note:** If the server is configured to use Active Directory for authentication, user passwords are managed by Active Directory, and you can leave the password field in the CSV file blank.

### CSV Import File Guidelines

You can automate adding users by creating a comma-separated values (CSV) file with user information and then importing the file. You can include attributes in the CSV file, such as license level and the publishing access, to apply to the users at the same time you import them.

To import users, you can use the server or site administration pages or the `tabcmd` utility. Using `tabcmd` provides an option for assigning a site role to all users in the CSV file. For information, see Import Users or `createsiteusers filename.csv`.

You can import users at the site or server level. If you import users to the server (not to a specific site), the users aren’t assigned to a site and are imported as Unlicensed.

### CSV file format requirements

When you create the CSV file for importing users, make sure that the file meets the following formatting requirements:
The file does not include column headings. Tableau Server assumes that every line in the file represents a user.

The file is in UTF-8 format, and includes the byte-order mark (BOM).

Character encodings such as BIG-5 have been converted to UTF-8. You can do this by opening the file in a text editor and using the **Save As** command.

If a user name includes an @ character that represents anything other than a domain separator, you need to refer to the symbol using the hexadecimal format: \0x40

For example, `user@fremont@mycompany.com` should be `user-\0x40fremont@mycompany.com`

### Required columns in the CSV file

The following values are required for each user:

- **User name**
  
- **Password**: If Tableau Server is configured to use Active Directory authentication, there must be a password column, but the column itself should be empty. If the server is using local authentication, you must provide passwords for new users.

### Additional import file options

The CSV file can contain the following fields, in the order shown here:

- **User name**. The user name. If the server is configured to use Active Directory, this value must match a user defined in Active Directory. If the user name is not unique across domains, you must include the domain as part of the user name (for example, `example\Adam` or `adam@example`). This is the only required field.

- **Password**. A password for the user. If the server is configured to use Active Directory, this value is not used.

- **Display name**. The display name is part of the information used to identify a user on
the server. If the user’s display name is already in use, Tableau Server updates the existing user information with the settings in the CSV file. If the server is configured using Active Directory, this value is not used.

- License level. This can be Creator, Explorer, Viewer, or Unlicensed.

- Administrator level (System, Site, or None). This setting determines whether the user is imported as an administrator.

  If you are using the web UI to import users, you can set the administrator site role to System only if you import the file at the server (All Sites) level. If you are signed in to a specific site, and if the administrator column for a user in the CSV file is set to System, Tableau Server imports the user as a site administrator.

- Publishing capability (yes/true/1 or no/false/0). If you are using the web UI, the publisher setting is used only if you import while signed in to a specific site. If you import users at the server (All Sites) level, this value isn't used.

- Email address. The email address is part of the information used to identify a user on the server. If the email address is already in use, Tableau Server updates the existing user information with the settings in the CSV file.

The order of the columns is significant. The first column is treated as the user name, the second as the password, the third as display name, and so on, regardless of the content in the columns. If you omit values for a field, you must still include the field’s comma delimiter.

Improve performance for large CSV files passed through tabcmd

A server administrator can enable server settings that help to improve performance for importing large CSV files through tabcmd commands. You can do this using the tsm configuraiton set command with the following options:

- vizportal.csv_user_mgmt.index_site_users

- vizportal.csv_user_mgmt.bulk_index_users
Tableau Server on Linux Administrator Guide

- `searchserver.index.bulk_query_user_groups`

Essentially, these options index users after the CSV file is processed, instead of one-by-one as they are added to the server’s database. This reduces the number of calls to the database and the memory required to process the file. These `tsm configuration set options` apply to the `tabcmd createsiteusers, deletesiteusers, addusers, and removeusers commands.`

For descriptions for these settings, see `tsm configuration set Options`.

Notes

- If you are not signed in to a specific site and are importing users at the server level, you can assign only the Server Administrator and Unlicensed site roles.

- If you have a user-based server installation, and if adding users would exceed the number of users allowed by your license, the users are added as unlicensed users.

- If you use `tabcmd` and specify the license, but importing users would exceed your license limits, users are imported as Unlicensed.

CSV settings and site roles

The license level, administrator, and publishing settings for a user determine how the user’s site role is set during the import process. The following table shows how the settings are converted to site roles.

<table>
<thead>
<tr>
<th>CSV settings</th>
<th>Site role</th>
</tr>
</thead>
<tbody>
<tr>
<td>License level=(any)</td>
<td>Server Administrator. This setting applies to Tableau Server only, and it is valid only if you are importing users while managing the server (that is, not signed in to a specific site). The Server Administrator site role always takes a Creator license if one is available. If no Creator...</td>
</tr>
<tr>
<td>Administrator=System</td>
<td></td>
</tr>
<tr>
<td>Publisher=true</td>
<td></td>
</tr>
<tr>
<td>CSV settings</td>
<td>Site role</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>license is available, see Troubleshoot Licensing to learn about the way Tableau Server handles this.</td>
</tr>
<tr>
<td>License level=Creator or Explorer Administrator=Site Publisher=true</td>
<td>Site Administrator Creator or Site Administrator Explorer. This setting is valid only if you are importing users while signed in to a specific site.</td>
</tr>
<tr>
<td>License level=Creator Administrator=None Publisher=true</td>
<td>Creator</td>
</tr>
<tr>
<td>License level=Explorer Administrator=None Publisher=true</td>
<td>Explorer (Can Publish)</td>
</tr>
<tr>
<td>License level=Explorer Administrator=None Publisher=false</td>
<td>Explorer</td>
</tr>
<tr>
<td>License level=Viewer Administrator=None Publisher=false</td>
<td>Viewer</td>
</tr>
<tr>
<td>License level=Unlicensed Administrator=None</td>
<td>Unlicensed</td>
</tr>
</tbody>
</table>
### CSV settings | Site role
---|---
Publisher=false |  

#### CSV import example for Tableau Server

The following example shows a CSV file that contains information for several users.

```
henryw,henrypassword,Henry Wilson,Creator,None,yes,henryw@example.com
freds,fredpassword,Fred Suzuki,Viewer,None,no,freds@example.com
alanw,alanpassword,Alan Wang,Explorer,Site,yes,alanw@example.com
michellek,michellepassword,Michelle Kim,Creator,System,yes,michellek@example.com
```

If you import this file while managing a site, four users are added to that site. The Administrator setting for user Michelle is System. However, because you are importing the users into a site, Tableau Server give Michelle the Site Administrator Creator site role. Three of the users are allowed to publish.

If you import this file while managing the server, four users are added to the server, but they are not added to any site. Only one user is imported as a server administrator; the rest are set to Unlicensed.

### Guest User

Core-based licenses of Tableau Server include a Guest user option, which you can use to let people access Tableau views without an account on the server.

Guest user access is enabled by default when Tableau Server is installed with a core-based license. It is not available with user-based licensing. If you do not intend to use Guest user access, you should disable it.
Guest access allows users only to see and interact with Tableau views. The Guest user cannot browse the Tableau Server interface or see server interface elements in the view, such as user name, account settings, comments, and so on. For more information about licenses, see Manage Licenses.

**Tip:** To share views with Guest users, either provide URL links or embed views into web pages. For more information, see Tableau User Help.

**Guest user permissions**

A Guest user can have the following maximum capabilities:

- **Workbooks and views:** View, Export Image, Summary Data, View Comments, Filter, Full Data, Web Edit, Download (to save a local copy)

- **Data sources:** View and Download

If you add the Guest user to a group that has a higher level of access to a content resource, the Guest user’s access does not exceed the capabilities listed above. However, the Guest user account will comply with more restrictive permissions settings.

**Enable or disable Guest access**

You must be a server administrator to change Guest account settings at either the server or the site level.

**Note:** Enabling the Guest user for a site can increase the number of potential simultaneous viewers beyond the user list you might be expecting. The administrative view **Status > Traffic to Views** can help you gauge the activity.

1. In the site menu, click **Manage All Sites** and then click **Settings > General**.

2. For **Guest Access**, select or clear **Enable Guest account** to toggle Guest user
Click **Save**.

This enables the Guest user on all sites. You can then go to the same setting for a specific site. To disallow Guest access for a site:

1. In the site menu, select a site.
2. Click **Settings**, and on the Settings page, clear the **Enable Guest account** check box.

If the Guest account is enabled on some or all sites, and you turn off Guest access at the server level, it is turned off for all sites as well.

**Note**: You can turn off Guest user access at the server or site level; however, you aren’t able to remove the user. So, although no one can access data or views without signing in to the server, the Guest user still appears in the Site Users list and group lists for groups you’ve added the Guest user to.

**Additional Guest account characteristics**

The Guest user is unique in the following additional ways:

- As a single user account, it represents all unauthenticated users accessing Tableau views.
- When enabled, it is a member of the All Users group.
- You can add it as a member of other groups on a site.
- You cannot edit it or select it as the owner of a content resource.
- If the Guest user needs to access a workbook with an extract connection, the Guest must also have the **View** capability on the published data source. (The Guest user is
not allowed to connect to published data sources.)

- The account is not allowed to save custom views.

- Guest cannot be used in a user filter.

- You cannot delete the account; however, you can turn off access to it by clearing the check box described in the steps above.

Groups

Add Users to a Group

You can organize Tableau Server users into groups to make it easier to manage multiple users. You can create groups on the server or import groups from Active Directory.

**Note:** If you run Tableau Server on Linux, all external directory communication is configured and managed with a LDAP identity store. In the context of user and group synchronization, Tableau Server configured with LDAP identity store is equivalent to Active Directory. Active Directory synchronization features in Tableau Server function seamlessly with properly configured LDAP directory solutions.

To keep Active Directory group membership up-to-date:

- Site administrators can synchronize selected groups on demand in a site. For more information, see Synchronize Active Directory Groups on a Site.

- Server administrators can synchronize all Active Directory groups on the server based on a schedule or on-demand. For more information, see Synchronize All Active Directory Groups on the Server.

To add a user to a group, the group must already exist.
Add users to a group (Users page)

1. In a site, click Users.

2. Select the users you want to add to a group, and then click Actions > Group Membership.

3. Select the groups and then click Save.

Add users to a group (Groups page)

1. In a site, click Groups, and then click the name of the group.

2. In the group's page, click Add Users.
3. Select the users to be added, and then click **Add Users**.

Create a Local Group

Local groups are created using the Tableau Server internal user management system. After you create a group you can add and remove users.
1. In a site, click **Groups**, and then click **New Group**.

2. Type a name for the group and click **Create**.

**Create Groups via Active Directory**

You can import Active Directory groups to create matching groups on Tableau Server, as well as a user for each member of an Active Directory group that is not already on the server.

**Note:** If you run Tableau Server on Linux, all external directory communication is configured and managed with a LDAP identity store. In the context of user and group synchronization, Tableau Server configured with LDAP identity store is equivalent to Active Directory. Active Directory synchronization features in Tableau Server function seamlessly with properly configured LDAP directory solutions.

Each user is assigned a site role as part of the import process. If any of the users to be imported exist in Tableau Server, the site role assigned during the import process is applied only if it gives the user more access to the server. Importing users does not demote site roles.
Before importing groups, review User Management in Active Directory Deployments to understand how multiple domains, domain naming, NetBIOS, and Active Directory user name format influence Tableau user management.

1. In a site, click **Groups**, and then click **Add Groups**

2. Type the name of the Active Directory group you want to import, and then select the group name in the resulting list.

3. Select the site role for the users.
4. Click **Import**.

**Note**: You cannot change the name of groups imported from Active Directory. The group name can only be changed in Active Directory.

**Synchronize Active Directory Groups in a Site**

At any time, you can synchronize an Active Directory group with Tableau Server to ensure new users in Active Directory are also added in Tableau Server. You can synchronize individual groups or multiple groups at once.

**Note**: If you run Tableau Server on Linux, all external directory communication is configured and managed with a LDAP identity store. In the context of user and group
synchronization, Tableau Server configured with LDAP identity store is equivalent to Active Directory. Active Directory synchronization features in Tableau Server function seamlessly with properly configured LDAP directory solutions.

1. In a site, click **Groups**.

On the Groups page, select one or more groups.

2. Click **Actions > Synchronize**.

![Tableau Server Groups page with Synchronize option highlighted](image)

Set the minimum site role for users in an Active Directory group

In the **Groups - Details** page, administrators can set the minimum site role for group users to apply during synchronization.

This setting does not run synchronization; it sets the minimum site role to applied to the group every time synchronization runs. When you synchronize Active Directory groups, new users are added to the site with the minimum site role. If a user already exists, the minimum site role will be applied if it gives the user more access in a site. If you don’t set a minimum site role, new users are added as **Unlicensed** by default.
**Note:** A user’s site role can be promoted but never demoted based on the minimum site role setting. If a user already has the ability to publish, that ability will always be maintained. For more information on minimum site role, see Site roles and Active Directory import and synchronization.

1. In a site, click **Groups**.

2. On the Groups page, select a group, and then select **Actions > Minimum Site Role**.

3. Select the minimum site role, and then click **Change Site Role**.

![Minimum Site Role](image)

What happens when users are removed in the source Active Directory?

Users cannot be automatically removed from the Tableau Server through an Active Directory sync operation. Users that are disabled, deleted, or removed from groups in Active Directory remain on Tableau Server so that administrators can audit and reassign the user’s content before removing the user’s account completely. For more information, see Sync behavior when removing users from Active Directory.
What happens when a user name changes in the source Active Directory

By default, Tableau Server will not synchronize changes to the user display name or email address after the initial synchronization when the corresponding account is created in Tableau Server. For example, if the user name jsmith is used for the display name John Smith, changing the display name in Active Directory to Joe Smith will not synchronize to the corresponding jsmith user in Tableau Server. Similarly, if the user’s email changes in Active Directory, Tableau Server will not synchronize changes.

You can configure Tableau Server to update the name and email properties when they change in the source Active Directory by setting `vizportal.adsync.update_system_user` to `true`.

To change this behavior run the following tsm commands:

```
tsm configuration set -k vizportal.adsync.update_system_user -v true

 tsm pending-changes apply
```

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

What happens when an Active Directory group is removed from Tableau Server?

Many Tableau administrators use Active Directory groups to import and create users. After the users are imported into Tableau Server, administrators will then delete the group in Tableau Server. Deleting a group does not delete the users in it.

Synchronize All Active Directory Groups on the Server

As a server administrator, you can synchronize all Active Directory groups (that have been configured on Tableau Server) on a regular schedule or on-demand on the General tab of the Settings page for the server.
Note: If you run Tableau Server on Linux, all external directory communication is configured and managed with a LDAP identity store. In the context of user and group synchronization, Tableau Server configured with LDAP identity store is equivalent to Active Directory. Active Directory synchronization features in Tableau Server function seamlessly with properly configured LDAP directory solutions.

Before you begin

Before synchronizing groups as described in this topic, you must first import the Active Directory group into Tableau Server. See Create Groups via Active Directory.

Synchronize Active Directory groups on a schedule

1. **Single-site**: Click **Settings** > **General**.

   **Multisite**: In the site menu, click **Manage All Sites** and then click **Settings** > **General**.

2. Scroll down the page to **Active Directory Synchronization**, and then select **Synchronize Active Directory groups on a regular schedule**.
3. Select the frequency and time of synchronization.

4. Click Save.

Synchronize all Active Directory groups on demand

At any time, you can synchronize Active Directory groups with Tableau Server to ensure that new users and changes in Active Directory are reflected in all Active Directory groups on Tableau Server.

1. **Single-site**: Click **Settings > General**.

   **Multisite**: In the site menu, click **Manage All Sites**, and then click **Settings > General**.
2. Under **Active Directory Synchronization**, click **Synchronize All Groups**.

View synchronization activity

You can view the results of synchronization jobs in the **Background Tasks for Non Extracts** administrative view. **Queue Active Directory Groups Sync** is the task that queues and indicates the number of **Sync Active Directory Group** tasks to be run.

1. **Single-site**: Click **Status**.

   **Multisite**: In the site menu, click **Manage All Sites** and then click **Status**.

2. Click the **Background Tasks for Non Extracts** link.

3. Set the **Task** filter to include **Queue Active Directory Groups Sync** and **Sync Active Directory Group**.

You can quickly navigate to this administrative view by clicking the **View synchronization activity** link in the **Settings** page for the server.

Set the minimum site role for users in an Active Directory group

In the **Groups - Details** page, you can set the minimum site role for group users to be applied during Active Directory synchronization.
This setting does not run synchronization; instead, it sets the minimum site role to applied to the group every time synchronization runs. The result is that when you synchronize Active Directory groups, new users are added to the site with the minimum site role. If a user already exists, the minimum site role is applied if it gives the user more access in a site. If you don’t set a minimum site role, new users are added as Unlicensed by default.

**Note:** A user’s site role can be promoted but never demoted based on the minimum site role setting. If a user already has the ability to publish, that ability will always be maintained. For more information on minimum site role, see Site roles and Active Directory import and synchronization.

1. In a site, click **Groups**.

2. On the Groups page, select a group.

   Click **Actions > Minimum Site Role**.

3. Select the minimum site role, and then click **Change Site Role**.

![Screenshot of minimum site role settings in Tableau Server on Linux Administrator Guide](attachment:image.png)
What happens when users are removed in the source Active Directory?

Users cannot be automatically removed from the Tableau Server through an Active Directory sync operation. Users that are disabled, deleted, or removed from groups in Active Directory remain on Tableau Server so that administrators can audit and reassign the user’s content before removing the user’s account completely. For more information, see Sync behavior when removing users from Active Directory.

Improving group synchronization performance

Active Directory synchronization is performed by the backgrounder process. The Backgrounder process is the same process that is used for managing and creating extracts, and is also used to generate subscription content. In large organizations with dynamic group membership and heavy extract usage, the Active Directory group synchronization process may be disruptive. We recommend running group synchronization during non-business hours.

By default, the Backgrounder process performs synchronization in a serial operation. This means that each group is synchronized, one after the other, in a single Backgrounder process. If you are running multiple instances of Backgrounder processes either on a single Tableau Server or across a distributed deployment, consider enabling parallel processing for Active Directory synchronization. When parallel Backgrounder processing is enabled, the group synchronization is distributed across multiple Backgrounder processes for better performance.

To enable parallel backgrounder processing for group synchronization, open TSM CLI and enter the following commands:

```bash
tsm configuration set -k backgrounder.enable_parallel_adsync -v true
tsm pending-changes apply
```

Quick Start: Synchronize All Active Directory Groups on a Schedule

After you import Active Directory groups in Tableau Server, you can make sure they stay synchronized in Tableau Server by setting up a schedule. You can also synchronize all Active
Directory groups on the server on-demand, at any time. The minimum site role setting for the group is applied when users are synchronized.

**Note:** If you run Tableau Server on Linux, all external directory communication is configured and managed with a LDAP identity store. In the context of user and group synchronization, Tableau Server configured with LDAP identity store is equivalent to Active Directory. Active Directory synchronization features in Tableau Server function seamlessly with properly configured LDAP directory solutions.

1 Set a minimum site role for synchronization

In a site, click **Groups**. Select a group, and then click **Actions** > **Minimum Site Role**. Select the minimum site role, and then click **Change Site Role**. Server and site administrators can set the minimum site role for group users to be applied during Active Directory synchronization. If you don't set a minimum site role, new users are added as **Unlicensed**.

Synchronizing can promote a user’s site role, but will never demote a user’s site role.
Set the schedule

Server administrators can enable synchronization for all Active Directory groups on the **General** tab of the **Settings** page for the server. Enable synchronization, select the frequency settings, and then click **Save**.

All Active Directory groups on the server are synchronized according to the same schedule.

3 Run synchronization on-demand (optional)

On the **General** tab of the **Settings** page, click **Synchronize All Groups** to synchronize all Active Directory groups on Tableau Server immediately. Click this button at any time to ensure new users and changes are reflected in all Active Directory groups on the server.
Click **Synchronize All Groups** to synchronize all Active Directory groups on the server outside of a schedule.

4 View the status of synchronization tasks

Server and site administrators can view the results of Active Directory synchronization jobs in the **Background Tasks for Non Extracts** administrative view. On the server or in a site, click **Status**. Under **Analysis**, click **Background Tasks for Non Extracts** and filter on the **Queue Active Directory Groups Sync** and **Sync Active Directory Group** tasks.
Queue Active Directory Groups Sync queues the Sync Active Directory Group tasks to be run.

Delete Groups

You can delete any group from the server (with the exception of the All Users group). When you delete a group, the users are removed from the group but they are not deleted from the server.

1. In a site, click **Groups**.

2. On the Groups page, select one or more groups to delete.
3. Select **Actions > Delete**.

![Dashboard-based Custom Portals](image)

**Dashboard-based Custom Portals**

*Note:* This overview was inspired by the work of Tableau Zen Master Mark Jackson. For more details about the process, check out Mark's blog.

The standard Tableau Online or Tableau Server interface works great for many organizations, but if you want to create a company-branded experience and don't have API developer skills, consider creating a custom portal based on a Tableau dashboard. A custom portal lets you organize content around specific departments or job roles, and you can even incorporate training that helps people interact with data more fully. As the volume of Tableau content grows, a custom portal guides your users directly to the data they need, while providing ready access to related views and Tableau Server search so they can easily explore further.
Sketch out a portal design

Begin outside of Tableau, on paper or in a wireframing application. Consider the structure of your organization and the number of Tableau views that apply to each group of users. Do you simply need one level of navigation that points immediately to content? Or might you need to start with a main page that provides navigational links for separate groups of users or report types, followed by a second level with related dashboards and views?

<table>
<thead>
<tr>
<th>Medical Staff</th>
<th>Illness trend report</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Patient demographics</td>
</tr>
<tr>
<td>Facilities</td>
<td>Hospital occupancy</td>
</tr>
<tr>
<td></td>
<td>Real estate transactions</td>
</tr>
</tbody>
</table>

After you get buy-in on your design from key stakeholders and data consumers, you’re ready to move on to the next phase.

Gather images for logos and navigation elements

Start thinking about images while refining your initial mockup, and then gather them from libraries of clip-art or approved brand graphics, or create them from scratch in an application like Photoshop or SnagIt. PowerPoint can also be a good source if you plan to create navigation thumbnails of common chart types.
Lay out text, images, and selected sheets on a dashboard

Create a workbook with a dashboard for the portal, using a tiled layout for more predictable positioning and scaling of elements on different devices. Then start adding Text and Image objects, as well as any sheets for data views you want to highlight right up front in your portal. To refine spacing between these dashboard elements, insert Blank objects and adjust their size. For more information, see Create a Dashboard.

Tip: For dynamic elements that show popular or recently created content, include sheets based on custom administrative views.

Link dashboard elements to content

If you have a second level of navigation in your portal, use filter actions to point to a secondary dashboard from the main one. To create links that directly open data views, right-click Image objects and choose Set URL. (In our example below, each colored arrow and accompanying text is an image that links to a view URL.) You can even point to empty views with preloaded data sources, encouraging users to create new Tableau content in the web-authoring workspace.

Tip: To add hyperlinks to text objects, include the full URL (for example, http://www.tableau.com).
Publish, test, and refine your portal

Publish the workbook to your server and distribute the dashboard URL to your users. Portal design, like data analysis itself, is a cyclical process. Now that your portal is out in the wild, start gathering user feedback so you can continuously improve the experience.
Tip: As a finishing touch, hide the Tableau toolbar to give your portal a custom feel. After the question mark at the end of the dashboard URL, add `embed-d=y&amp;toolbar=n`.

Data Connection Authentication

More information

- [Setting an Oracle Connection to Use TNSNames.ora or LDAP.ora](https://support.tableau.com/articles/Setting-an-Oracle-Connection-to-Use-TNSNames-ora-or-LDAP-ora) (Tableau Support)

Enable Kerberos Delegation

Kerberos delegation enables Tableau Server to use the Kerberos credentials of the viewer of a workbook or view to execute a query on behalf of the viewer. This is useful in the following situations:

- You need to know who is accessing the data (the viewer’s name will appear in the access logs for the data source).
- Your data source has row-level security, where different users have access to different rows.

Supported data sources

Tableau supports Kerberos delegation with the following data sources:

- Cloudera: Hive/Impala
- Denodo
- PostgreSQL
Tableau Server on Linux Administrator Guide

- SQL Server
- Teradata

Requirements

Kerberos delegation requires Active Directory.

- The Tableau Server information store must be configured to use LDAP - Active Directory.
- The computer where Tableau Server is installed must be joined to Active Directory domain.
- MIT KDC is not supported.

Configuration process

This section provides an example of the process to enable Kerberos delegation. The scenario also includes example names to help describe the relationships between the configuration elements.

1. Tableau Server will need a Kerberos service ticket to delegate on behalf of the user that is initiating the call to the database. You must create a domain account that will be used to delegate to the given database. This account is referred to as the Run As service account. In this topic, the example user configured as the delegation/Run As account is tabsrv@example.com.

   The account must be configured with Active Directory User and Computers on a Windows Server that is connected to the user domain:

   - Open the Properties page for the Run As service account, click the Delegation tab and select Trust this user for delegation to specified services only and Use any authentication protocol.

2. Create a keytab file for the Run As service account.

   For example, the following commands create a keytab (tabsrv-runas.keytab) using the ktutil tool:

   `sudo ktutil`
ktutil: addent -password -p tabsrv@EXAMPLE.COM -k 2 -e <encryption scheme>

Encryption schemes for this command include RC4-HMAC, aes128-cts-hmac-shal-96, and aes256-cts-hmac-shal-96. Consult your IT team for the correct encryption scheme for your environment and data source.

ktutil: wkt tabsrv-runas.keytab

Tableau Server will use the Run As service account and the associated keytab to authenticate and make a direct connection to the database.

3. Copy the keytab into the Tableau Server data directory and set proper ownership and permissions.

mkdir /var/opt/keytab
sudo cp -p tabsrv-runas.keytab /var/opt/keytab

sudo chown $USER /var/opt/keytab/tabsrv-runas.keytab
chgrp tableau /var/opt/keytab/tabsrv-runas.keytab
chmod g+r /var/opt/keytab/tabsrv-runas.keytab

4. Run the following TSM commands to enable Kerberos delegation, set the delegation service account, and associate the keytab file with the service account:

tsm configuration set -k wgserver.delegation.enabled -v true
tsm configuration set -k native_api.datasource_imper-
sonation_runas_principal -v tabsrv@EXAMPLE.COM
tsm configuration set -k native_api.datasource_imper-
sonation_runas_keytab_path -v /var/opt/keytab/tabsrv-
Tableau Server on Linux Administrator Guide

runas.keytab

tsm configuration set -k native_api.protocol_transition_a_d_short_domain -v false

tsm configuration set -k native_api.protocol_transition_uppercase_realm -v true

In some cases, TSM may return an error mentioning --force-keys. If you get this error, run the command again with the --force-keys parameter appended to the argument.

5. Run the following TSM command apply the changes to Tableau Server:

```bash
tsm pending-changes apply
```

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the --ignore-prompt option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

6. Enable delegation for data connections:

- **SQL Server**—See Enabling Kerberos Delegation for SQL Server in the Tableau Community.

- **PostgreSQL**—See Enabling Kerberos Delegation for PostgreSQL in the Tableau Community.

- **Teradata**—See Enabling Kerberos Delegation for Teradata in the Tableau Community.

- **Denodo**—See Enabling Kerberos Delegation for Denodo on Linux in the Tableau Community.
- **Cloudera**—See Enable Kerberos Delegation for Hive/Impala in the Tableau Community.

See also

Troubleshoot Kerberos

**OAuth Connections**

For Google BigQuery, Google Analytics, Salesforce, OneDrive, Dropbox, and QuickBooks Online, an alternative to storing your sensitive database credentials with Tableau Server is to create connections using the **OAuth 2.0** standard.

From Tableau, when you sign in to data with a provider that uses OAuth, you are redirected to the provider’s sign-in page. After you provide your credentials and authorize Tableau to access your data, the data provider sends Tableau an **access token** that uniquely identifies requests from Tableau. For more information, see Overview of the OAuth process below.

Using OAuth connections provides the following benefits:

- **Security**: Your database credentials are never known to or stored in Tableau Server, and the access token can be used only by Tableau.

- **Convenience**: Instead of having to embed your data source ID and password in multiple places, you can use the token provided for a particular data provider for all published workbooks and data sources that access that data provider.

In addition, for live connections to Google BigQuery data, each workbook viewer can have a unique access token that identifies the user, rather than sharing a single user name and password credential.

**Overview of the OAuth process**

The following steps describe a workflow in the Tableau environment that calls the OAuth process.
Tableau Server on Linux Administrator Guide

1. You take an action that requires access to a cloud data source.

   For example, you open a workbook that’s published to Tableau Server.

2. Tableau directs you to the cloud data provider’s sign-in page. The information that is sent to the data provider identifies Tableau as the requesting site.

3. When you sign in to the data, the provider prompts you to confirm your authorization for Tableau Server to access the data.

4. Upon your confirmation, the data provider sends an access token back to Tableau Server.

5. Tableau Server presents your workbook and data to you.

The following workflows can use the OAuth process:

- Creating a workbook and connecting to the data source from Tableau Desktop or from Tableau Server.

- Publishing a data source from Tableau Desktop.
Signing in to Tableau Server from an approved client, such as Tableau Mobile or Tableau Desktop.

Access tokens for data connections

You can embed credentials based on access tokens with data connections, to enable direct access after the initial authentication process. An access token is valid until a Tableau Server user deletes it, or the data provider revokes it.

It is possible to exceed the number of access tokens your data source provider allows. If that's the case, when a user creates a new token, the data provider uses length of time since last access to decide which token to invalidate to make room for the new one.

Access tokens for authentication from approved clients

By default, Tableau Server sites allow users to access their sites directly from approved Tableau clients, after users provide their credentials the first time they sign in. This type of authentication also uses OAuth access tokens to store the users' credentials securely.

For more information, see Disable Automatic Client Authentication

Configure the Server for OAuth Support

Instead of individual usernames and passwords, OAuth works through limited-purpose access tokens. Before you can obtain access tokens needed to create an OAuth connection in Tableau, you need to configure your server so that the data provider sending the token can recognize Tableau Server as a trusted destination. The following section describes how to prepare for setting up OAuth regardless of your data provider. The topics listed below it contain the steps for configuring your server for specific data providers.

Preparing for Configuring OAuth Support

Before you begin the configuration steps specific to your data provider, complete the following prerequisites:
Obtain the fully qualified domain name of each Tableau Server node that will host views that connect to this data source. For example:

https://sales.your_domain.com

If you use Salesforce.com, you will need to provide an https address.

Make sure at least one of your data-provider accounts is enabled for API access.

For Google data types, you need access to the developers console on the Google Cloud Platform.

For Salesforce.com, you need access to the Force.com platform.

For QuickBooks Online, you need access to the Intuit platform.

Configure Settings for Your Data Provider

When you complete the OAuth-preparation steps, you can configure the appropriate settings with your data provider.

- Set up OAuth for Google
- Set up OAuth for Salesforce.com
- Set up OAuth for QuickBooks Online

Set up OAuth for Google

This topic describes how to set up your Google BigQuery, Google Sheets, and Google Analytics data sources for OAuth.

Complete these steps for each Tableau Server instance.

**Note** Before you complete these steps, make sure you have completed the pre-requisites described in Preparing for Configuring OAuth Support.

Set up OAuth by following these three procedures:
Enable API access and create access token from Google.
Configure OAuth on Tableau Server.
Create and edit Google data source.

Obtain a Client ID and Enable Google APIs

**Note** These steps reflect the settings in the Google Cloud Platform console at the time of this writing. For more information, see Using OAuth 2.0 for Web Server Applications in the Google Developers Console Help.

1. Sign in to Google Cloud Platform, and then click **Go to my console**.
2. On the drop-down menu next to the Google Cloud Platform title, select **Create project**.
3. In the new project form that appears, complete the following:
   - Give the project a meaningful name that reflects the Tableau Server instance for which you'll use this project.
   - Determine whether you want to change the project ID.

   **Note** After you create the project, you will not be able to change the project ID. For information, click the question mark icons.
4. Open the new project, and navigate to APIs Manager > Credentials.

**Note:** You must generate credentials with the Google API Manager for Tableau Server. Do not attempt to use a Service Account, which generates a key, and is not supported.

5. Click the OAuth consent screen tab and then enter a meaningful name for Product name shown to users.

6. Click the Credentials tab, then click the Create credentials drop-down list, and then select OAuth client ID. Complete the following:

   - Select Web Application.
   - For Authorized JavaScript Origins, enter the local computer name of your Tableau Server.
   - For Authorized Redirect URI, replace the existing text with the Internet address for your server, and add the following text to the end of it: auth/add_oauth_token. For example:

     https://your_server_url.com/auth/add_oauth_token

7. Copy the Authorized Redirect URI, and paste it in a location that you can access from your Tableau Server computer.

8. Click Create.

9. Copy the following values that Google returns, and paste them in a location that you can access from your Tableau Server computer:

   - Client ID
   - Client secret
10. In **APIs Manager > Dashboards**, verify that **BigQuery API**, **Google Drive API** (to enable Google Sheets) or **Analytics API** is enabled. To enable APIs, click **ENABLE API** at the top of the page.

**Configure Tableau Server for Google OAuth**

Using the information you obtained by completing the steps in Obtain a Client ID and Enable Google APIs, configure your Tableau Server:

- On the Tableau Server computer, open the shell and run the following commands to specify the access token and URI:

  ```bash
  tsm configuration set -k oauth.google.client_id -v <your_client_ID>
  tsm configuration set -k oauth.google.client_secret -v <your_client_secret>
  tsm configuration set -k oauth.google.redirect_uri -v <your_authorized_redirect_URI>
  tsm pending-changes apply
  ```

  The **pending-changes apply** command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the **--ignore-promt** option, but this does not change the restart behavior. For more information, see tsm pending-changes apply.

**Create and edit Google data source**

Next, you must publish the Google data sources to the server. See the Tableau Desktop topic, **Google BigQuery**.

After you’ve published the data sources, the final step is to edit the data source connection to use the embedded access token that you configured earlier. See Edit Connections on Tableau Server.
Managing access tokens

After you configure the server for OAuth, you can allow users to manage their own access tokens in their profile settings, or you can manage the tokens centrally. For more information, see Allow Saved Access Tokens.

Set up OAuth for Salesforce.com

This topic describes how to set up your Salesforce.com data sources for OAuth. Complete these steps for each Tableau Server instance.

**Note**: Before you complete these steps, make sure you have completed the prerequisites described in Preparing for Configuring OAuth Support.

Set up OAuth by following these two procedures:

- Create a Connected App in Salesforce
- Use the information you obtained to configure your server.

Create a Connected Salesforce App

1. Sign in to your Salesforce.com developer account, click your user name in the upper-right, and then select **Setup**.

2. In the left navigation column, under App Setup, select **Create > Apps**.
3. In the Connected Apps section, click **New**.

4. Complete the **Basic Information**, and in the API section, select **Enable OAuth Settings**.

5. In the new OAuth settings that appear, for **Callback URL**, type the fully qualified domain name of your server, using the https protocol, and append the following text to the URL: **auth/add_oauth_token**.

For example:

https://www.your_server.com/auth/add_oauth_token

6. Move the following items from Available OAuth Scopes to Selected OAuth Scopes:

   - Access and manage your data (api)
   - Access your basic information (id)
   - Perform requests on your behalf at any time (refresh_token)
7. Click **Save**.

After you save the app, Salesforce populates the API section with the following IDs that you will use to configure Tableau Server:

- Consumer Key
- Consumer Secret
- Callback URL

Configure Tableau Server for Salesforce.com OAuth

1. On the Tableau Server computer, run the following commands:

   ```
   tsm configuration set -k oauth.salesforce.client_id -v <your_client_ID>
   tsm configuration set -k oauth.salesforce.client_secret -v <your_client_secret>
   tsm configuration set -k oauth.salesforce.redirect_uri -v <your_authorized_redirect_URI>
   ```

2. (Optional) To change the default login server, type the following command:

   ```
   tsm configuration set -k oauth.salesforce.server_base_url -v <URL>
   ```

3. Enter the following command to apply changes:
The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

Managing access tokens

After you configure the server for OAuth, you can allow users to manage their own access tokens in their profile settings, or you can manage the tokens centrally. For more information, see Allow Saved Access Tokens.

Set up OAuth for QuickBooks Online

This topic describes how to set up your QuickBooks Online data sources for OAuth authentication. Complete these steps for each Tableau Server instance.

**Note:** Before you complete these steps, make sure you have completed the prerequisites described in Preparing for Configuring OAuth Support.

Setting up OAuth for QuickBooks Online consists of two tasks:

- Create a Connected App on the Intuit developer platform.
- Use the information you get as part of the Connected App to configure your server.

Create a Connected Intuit App

1. Sign in to your Intuit developer account, and then click My Apps.
2. In the Just start coding section, click Select APIs.
3. Select Accounting and click Create App.
4. In the Get your app ready for submission section, click the link to get your
production keys.

**Important:** You must use production keys rather than development keys.

5. Copy the app token, OAuth consumer key, and OAuth consumer secret.

Configure Tableau Server for QuickBooks Online

- On the Tableau Server computer, open the bash shell and run the following commands:

  ```
  tsm configuration set -k oauth.quickbooks.oauth_callback_uri -v http://YOUR-SERVER/auth/add_oauth_token
  
  tsm configuration set -k oauth.quickbooks.consumer_key -v <your_consumer_key>
  
  tsm configuration set -k oauth.quickbooks.consumer_secret -v <your_consumer_secret>
  
  tsm pending-changes apply
  ```

  The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

Managing access tokens

If you run an extract refresh job for your QuickBooks Online data source, Tableau Server attempts to renew access tokens for you. To help ensure that your access tokens do not expire, run your extract refresh jobs more than once a month. Otherwise, the access tokens from QuickBooks Online expire and your extract refresh jobs fail. If your access tokens do expire, you can edit your saved credentials from the **Settings** page.
The saved credentials can be managed centrally or by your users. For more information, see Allow Saved Access Tokens.

**Allow Saved Access Tokens**

After you configure Tableau Server for OAuth, you can decide to allow users to manage their own OAuth credentials, or you want to manage them centrally. If you want users to manage their own, you need to enable user profile settings from the server.

**Note:** If you have not yet configured your server to enable OAuth data connections, see the related topics listed below.

1. Sign in to Tableau Server as a server administrator.

2. **Single-site:** Click **Settings > General**.

   **Multisite:** In the site menu, click **Manage All Sites** and then click **Settings > General**.

3. In the **Saved Credentials** section, select the following:

   - **Allow users to save passwords for data sources** (allows users to save their individual credentials with data sources).
• Allow users to save OAuth access tokens for data sources

4. Click **Save**.

After you select these check boxes, users will see a **Manage Credentials** section in their profile settings, where they can add access tokens for OAuth data connections.

Managing credentials centrally

Server administrators alternatively can manage OAuth credentials centrally. This can work well, for example, if multiple users work from the same data, and you have a dedicated user account for your data provider.

To manage credentials centrally, you do the following:

• Clear the check boxes described in the preceding procedure.

• Edit connection information as data sources are published.
When you edit the connection, you embed credentials that use an OAuth access token instead of an individual’s user name and password.

When the settings for saving passwords and access tokens are not enabled, the Manage Credentials section is excluded from users’ profile settings.

See also

Set up OAuth for Google

Set up OAuth for Salesforce.com

Set up OAuth for QuickBooks Online

Configure SAP HANA SSO

You can configure Tableau Server to use SAML delegation to provide a single sign-on (SSO) experience for SAP HANA. This scenario is not dependent on SAML authentication to Tableau Server. You do not need to use SAML sign on with Tableau Server in order to use HANA SAML delegation. You can sign in to Tableau Server using whatever method you choose.

With SAML delegation for SAP HANA, Tableau Server functions as an identity provider (IdP).

Before you begin

Configuring SAML delegation with SAP HANA requires configuration on both Tableau Server and on SAP HANA. This topic provides configuration information about configuring Tableau Server. Before you configure Tableau Server, you must complete the following:

- Acquire a SAML certificate and key file for Tableau Server. The certificate file must be a PEM-encoded x509 certificate with the file extension .crt or .cert. This file is used by Tableau Server, and must also be installed on HANA. The private key must be a DER-encoded private key file that is not password protected, and that has the file extension .der. This file is only used by Tableau Server.
- Install the certificate in HANA.
Install the latest version of SAP HANA driver (minimum version is 1.00.9) on Tableau Server.
- Configure network encryption from Tableau Server to SAP HANA (recommended).

For more information about generating the certificate/key pair, encrypting the SAML connection, and configuring SAP HANA, see How to Configure SAP HANA for SAML SSO with Tableau Server in the Tableau Community.

Configure Tableau Server SAML for SAP HANA

The following procedure describes how to configure SAML for SAP HANA on Tableau Server using tsm data-access. You can also configure SAML for SAP HANA using the sapHanaSettings Entity.

If you are running Tableau Server in a distributed deployment, run the following procedure on the initial node.

1. Place certificate files in a folder named saml. For example:

   /var/opt/saml

2. Run the following commands to specify the location of the certificate and key files:

   tsm data-access set-saml-delegation configure --cert-key <cert-key> --cert-file <cert-file>

Where <cert-key> and <cert-file> are file paths to the private key and certificate file, respectively.

For example,

   tsm data-access set-saml-delegation configure --cert-key /var/opt/saml/hana_pkey_pkcs8.der --cert-file /var/-opt/saml/hana_cert.pem

You can specify other options. For example, you can specify user name format and how credentials are normalized. See tsm data-access.
3. Run the following commands to enable delegation:

   `tsm data-access set-saml-delegation enable`

   `tsm configuration set -k wgserver.sap_hana_sso.enabled -v true`

   `tsm configuration set -k wgserver.delegation.enabled -v true`

4. When you have finished, run `tsm pending-changes apply`.

   The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

Manage Content Access

Set a Site’s Web Authoring Access

Tableau Server administrators can specify at the site level whether to allow users to edit published views in the web environment.

By default web authoring functionality is enabled for all sites. Users with the Web Edit capability to edit workbooks directly on the server. Turn off web authoring if you want users to be able to view and interact with published workbooks but not make any changes to the core information.

The steps below describe how to set web authoring for an entire site. For more granular control over which users can use web editing, you can use projects, groups, and permissions. See Set Web Edit, Save, and Download Access on Content.
Turn web authoring on or off for a site

1. In a web browser, sign in to the server as an administrator and go to the site in which you want web authoring to be enabled. In that site, click **Settings**.

   ![Settings](image)

2. Select **Allow users to use web authoring** to enable the functionality.

   Clear the check box to turn off web authoring for that site.

   ![Web Authoring](image)

3. If your site is already in production, and you want the change to take effect immediately, restart the server.

   Otherwise, the change takes effect after server session caching expires or the next time users sign in after signing out.

**Notes**

- When you enable web authoring, make sure that, on the appropriate workbooks or views, the permission rule for a user or group allows the **Web Edit** capability.

- If you turn off web authoring on a production site and do not complete the last step to restart the server, users might continue to have authoring access until their session caches expire or they sign out.

**See which sites allow web authoring**

To confirm which sites allow web authoring, on the site-selection menu at the top, select **Manage All Sites**, and then go to the **Sites** page.
Set Web Edit, Save, and Download Access on Content

If you’re enabling web authoring functionality on your site, you can configure more precisely which users on the site have access to this functionality. Using site roles and permissions rules at the content level, you can grant or deny Web edit, Save, or Download capabilities on projects, workbooks, and data sources.

Note: This document strives to use the phrase Web edit only to specify the name of the capability in permissions rules, and web authoring to refer to the general functionality of creating and modifying workbooks on the server. However, you might otherwise see these two phrases used interchangeably.

Why allow users to work on the server directly

As an administrator, your initial thought about allowing people to populate a site with content, seemingly indiscriminately, might be one of skepticism. However, with a few controls, you can limit where this is done, while providing important benefits that centralized content management offers both you and your users.

Web authoring pros and cons

For publishers and business users, some benefits of web authoring include the following:
It provides analyst teams who work collaboratively with a central location in which to provide input.

It enables people who do not have Tableau Desktop to connect to data sources and create workbooks.

It enables people to access content when they are away from their Tableau Desktop computer or VPN, whether on a computer or a hand-held device.

It can provide a framework for enabling consistency across Tableau reports.

By making template workbooks available on the server, analysts can download or create new workbooks with data connections, branding, and formatting already in place.

For administrators, benefits can include the following:

- Fewer Tableau Desktop deployments to manage and support.
- Fewer computers that need to have database drivers installed.
- Capacity to govern content.
- More accurate monitoring of what people are doing with Tableau.

Some disadvantages to web editing include the following:

- For analysts, web editing functionality is not as extensive as in Tableau Desktop (although it continues to evolve toward that parity).
- For administrators, more people working on the server might mean upgrading systems.
- Without publishing guidelines, content proliferation on the server is expected.

This can confuse the people who rely on published Tableau dashboards and data sources, degrade server performance and data quality, and potentially affect data security.
Managing permissions to help users avoid content proliferation

To help users to avoid content proliferation on the server, many Tableau administrators use projects to allow varying levels of access to content. For example, one project can allow all users to edit and save workbooks; another can allow only approved publishers to save new content.

To get a better idea how this works, see the following resources:

- Configure Projects, Groups, and Permissions for Managed Self-Service
- Projects and Content Permissions in Everybody’s Install Guide
- Governed Self-Service at Scale, a Tableau whitepaper by Rupali Jain.

To view the PDF, you might need to provide your Tableau website credentials. These are the same ones you use for the community forums or to submit support cases.

Coordinate edit and save capabilities with site roles for the appropriate level of access

To edit, save, and download workbooks, users must have a site role that allows those actions, along with the capabilities—defined in permissions rules—that grant or deny editing-related access.

Site role access

- When the appropriate permissions are set at the content level, the Creator or Explorer (Can Publish) site role allows both Save (overwrite) and Save As/Download.

Users with these site roles can save (overwrite) only workbooks that they own. If they edit a workbook owned by another user, only the Save As command is available, and they can save the workbook with a new name.

- The Explorer site role allows downloading but not saving (neither overwriting existing nor saving changes to a new workbook).
Capabilities set on content

These capabilities coordinate with the site role to allow levels of editing and saving.

- **Web Edit** determines whether users can edit workbooks directly on the server.

- **Download Workbook/Save As** determines whether users have access to the **Save As** option while they are editing a workbook, or can download a workbook as a Tableau packaged workbook (.twbx).

**Save As** allows users to save changes they’ve made to an existing workbook as a new workbook on the server. It also determines whether they can open a workbook on the server from Tableau Desktop.

Tableau treats saving like publishing, so to save new workbooks, users must have a site role of **Creator** or **Explorer (Can Publish)**.

- **Save** determines whether users can save changes to an existing workbook on the server (overwrite a workbook).

  To overwrite a workbook with changes made on the server, a user must have a site role of **Creator** or **Explorer (Can Publish)**.

Configure site roles and permissions

Use the tables in the following sections to coordinate the site role with saving and editing capabilities.

Set these capabilities at the project level, using permissions rules.

Allow users who can publish to edit, save changes to, and download existing and new workbooks

Apply these capabilities to users who have the **Creator** or **Explorer (Can Publish)** site role.

<table>
<thead>
<tr>
<th>Capability</th>
<th>For the project</th>
<th>For specified workbooks in the project</th>
</tr>
</thead>
</table>

Tableau Server on Linux Administrator Guide

Tableau Software Version: 2019.1

499
<table>
<thead>
<tr>
<th>Capability</th>
<th>For the project</th>
<th>For specific workbooks in the project</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Edit</td>
<td>-</td>
<td>Allowed</td>
</tr>
<tr>
<td>Download Workbook/Save As</td>
<td>-</td>
<td>Allowed</td>
</tr>
<tr>
<td>Save</td>
<td>Allowed</td>
<td>Denied</td>
</tr>
</tbody>
</table>

Allow users who can publish to edit, save changes to, and download new workbooks, but not overwrite existing workbooks.

Apply these capabilities to users who have the **Creator** or **Explorer (Can Publish)** site role.

**Important:** In the “save but not overwrite” case above, allowing Save access at the project level is required for publishers to be able to publish workbooks from Tableau Desktop. To deny overwriting existing workbooks, you must deny the Save capability explicitly on each relevant workbook, and not lock permissions to the project. If project permissions are locked, permissions set on the project apply to all workbooks in it.

Allow explorers to download workbooks.

Apply these capabilities to users who have the **Explorer** site role.
### Web Edit

- Allowed

### Download Workbook/Save As

- Allowed

### Save

- -

The **Save** and **Save As** capabilities will be denied by the Explorer.

See also

- Set Permissions on Individual Content Resources
- Set Users’ Site Roles
- Permissions Reference

## Configure Projects, Groups, and Permissions for Managed Self-Service

Tableau Online and Tableau Server each provide an environment for easy open publishing and collaborative analysis of visualizations created in Tableau Desktop or web authoring. With that flexibility comes the challenge of making sure the right content is easy to find for the people who rely on it for their work. Likewise, making sure the access you allow doesn’t create performance or management nightmares on the site.

To address these challenges, many administrators set up their Tableau sites for what we’ll refer to as **managed self-service**. This is just a way of saying that the site allows areas of open collaboration and web editing, alongside areas in which access to data and reports is more controlled. As the site administrator, you put guidelines in place to help users figure out where to go for the type of work they need to do.

To get started with a managed self-service approach, the following sections discuss how you as the site administrator can meet the following objectives:
Create projects on the Tableau Server or Tableau Online site to match the ways people need to work with content.

For example, some projects are open to all for collaboration; others are visible only to authorized publishers.

- Create user groups based on the type of access users need to the content.

- Create a clear and scalable permissions strategy.

**Note:** The information provided here is adapted and simplified from practices of existing Tableau Zen Masters and customers who have shared their experiences. Links to their talks are available at the bottom of this page.

### Create a project team and adopt a permissions strategy

Although changing the project structure on your site after your users are publishing to it is not impossible, it’s difficult and can be daunting. So before you make any lasting decisions or take definitive actions on your Tableau site, we recommend that you recruit users from various segments of your Tableau population, to create a project team of people who have differing uses for Tableau content.

Your permissions strategy will help your environment scale as you add new Tableau users. Make sure it incorporates two important practices: manage permissions only for groups, and set permissions only at the project level. Setting permissions at the individual user level and on individual content resources becomes unmanageable quickly. If you need to deviate from this practice, make sure you document and communicate your strategy to other administrators and project leaders.

### Steps to coordinate projects and groups

To get projects and permissions (content) to work together with groups (people) in a managed self-service environment, you generally take the following steps:
1. Plan your permissions: Find common themes in the type of access users need. This helps determine projects and groups.

2. Remove permissions that will cause ambiguities

3. Create groups

4. Assign permissions to the groups

5. Create projects and adjust permissions

6. Lock permissions in each project

If you decide to follow the guidelines described here, you might want to Automate working with groups and projects.

1. Plan your permissions

Before you create groups and start assigning permissions, create a list of people who need access to content, and arrange them in groups according to what they’ll want to do.

For example, someone who publishes or moves a data source to a certified content project would need different level of access than someone who only consumes published reports. (We use the term “certified” to mean “trusted” — these are the data sources or reports that your Tableau community can trust to be a source of truth for your organization.)

Keep in mind also that you can set permissions differently for each project. So someone who is a data steward for the Ops department might not get the equivalent access to the Marketing content.

This exercise, done outside of the Tableau environment, can be the most challenging part of setting up a site.
Use a closed permissions model for managed content

General models for setting permissions are open or closed. In an open model, users get a high level of access, and you explicitly deny capabilities. This model can work when your organization is very small, and everyone has a similar level of responsibility.

In a closed model, users get only the access they need to do their jobs. This is the model security professionals advocate, and the examples in this article will attempt to show.

2. Remove permissions that will cause ambiguities

Every site has a Default project and an All Users group. Any user added to the site becomes a member of the All Users group automatically. The Default project works as a template for new projects in the site and cannot be deleted, but you can change the permissions. Creating groups and setting baseline permissions here helps you to know and manage exactly who gets what level of access for each new project.

In the managed self-service context, setting baseline permissions means removing the permissions from the All Users group, so that the permissions are enabled only on groups you create and have control over.

1. Select the Content tab to open the top-level projects on the site.

2. On the Default project’s Actions (…) menu, select Permissions.
3. Next to the **All Users** group name, select …, and then select **Edit**.

4. In the drop-down lists under **Project**, **Workbooks**, and **Data Sources**, select **None**.

5. Select **Delete** to apply the changes.
3. Create groups

You create groups to match what people need to do with a set of content. In this case “a set of content” refers to the workbooks and data sources in a project.

When you create your groups, use descriptive names that make sense for your organization. For example, one possible set of groups might be as follows:

- **Project leaders.** You might also think of these as project-level administrators. Users who can perform all available capabilities on data sources, with the possible exception of setting permissions on them. People in this group can be site administrators, or users whose job it is to approve or certify data models or reports.

  To grant administrator capabilities at the project level, you can assign the **Project Leader** permissions role to users with the appropriate site roles. To learn more, see Project-level administration.

- **Analysts/Publishers.** This group is for users who can publish workbooks to production and other open projects, use web editing on some projects, and connect to data sources certified by the data stewards. This group is not allowed to set permissions on content or move it between projects.

- **Business Users.** This group is the most likely to include people who do not use Tableau Desktop, but use data to answer questions and make business decisions. They can view and interact with workbooks only in specific projects, and they can’t publish, edit, save, or delete anything.

- **Administrators.** Depending on the size of your deployment, managing site or server administrators as a group helps you keep track of who has that level of access.

  **Note:** Users with the Server Administrator or Site Administrator Creator site role have access to everything on the site, regardless of the groups you add them to.
If you have multiple Tableau roles per department, creating corresponding groups manually can be labor intensive. For alternatives, see Automate working with groups and projects later in this article.

**Learn more:** Add Users to a Group

4. Assign permissions to the groups

After you create groups, you can assign permissions in one of the following ways:

- In the Default project, apply a core set of permissions on each group that will stay more or less the same for all projects. You can then make minor adjustments in specific projects.

  Or

- Keep the Default project clean, and apply permissions only on projects you create.

For the example we’re using, it makes more sense to set permissions templates in the Default project. You will want to explicitly deny some capabilities across the board, and then allow them on only a few projects where you want to allow more open access.

Set permissions templates

1. While you have the Default project open, on the **Actions** menu (...), select **Permissions**.

   The **Permissions** pane shows only the All Users group that has no permissions.

2. Create a permission rule for each group as follows:

   a. Select **Add a user or group rule**, and then select one of your groups.

      This adds the group to the **User/Group** column, open for editing.

   b. Select a permission role in the **Project, Workbook, and Data Source**
columns.

Permission roles are predefined sets of capabilities that make setup easier.

c. Refine permissions in any of the columns by selecting the expand icon (>>) to display individual capabilities and set them explicitly.

3. **Lock permissions to the project.**

Example

For the groups defined in 3. Create groups, here is one way you might set default permissions.

**Project leader roles**

- Project: **Project Leader**
- Workbooks: **Editor**
- Data Sources: **Editor**

This gives site administrators and data stewards full access to a project and its content. If you’re an IT admin, this enables you to delegate Tableau content administration to people who are closer to that content.

**Analyst Publisher roles**

- Project: **Publisher**
- Workbooks: **Editor**
- Data Sources: **Connector**

**Business Users roles**

- Project: **Viewer**
- Workbooks: **Interactor**
- Data Sources: **Denied**

**Default project settings for individual capabilities**
Under Workbooks, set Web Edit and Download Full Data to Deny.

This assumes you want to allow web editing and downloading data only on select projects. When you create those projects, you can refine the permissions.

If you want to put more than a couple of users in the Project administrators group for each project, consider denying the Set Permissions capability for that group. An alternative for delegating the task of setting permissions is to set individual users’ site roles to Site Administrator.

Leave capabilities in the Edit category set to None.

If you want to allow other capabilities only as an exception, set those to Deny here as well.

5. Create projects and adjust permissions

After the Default project is set with your custom permissions template, you can create projects that allow the content use cases you identified. For each project, you can adjust the default permissions as appropriate.

Example project structure

One way to structure projects could be to reflect the following use cases:

Workbooks shared for open collaboration on the server
Anyone in the department can publish to the open-collaboration project while their content is in development. Colleagues can collaborate using web editing on the server. Some people call this a sandbox, some call it staging, and so on. On this project you can allow web editing, saving, downloading, and so on.

Here you want not only to enable collaboration, but also to enable people who don’t have Tableau Desktop to contribute and provide feedback.

**Shared reports that cannot be edited**

This could be a project that people who create workbooks and data sources (Analysts and Data Stewards) could publish to when they want to make content available to business users for viewing, with confidence that their work cannot be “borrowed” or modified.

For this type of project, you would deny all capabilities that allow editing or getting the data off of the server for reuse. You would allow viewing and interacting capabilities.

**Vetted data sources for Analysts to connect to**

This would be where Data Stewards publish the data sources that are meet all of your data requirements and become the “source of truth” for your organization. Project leaders on this project can certify these data sources, so that they rank higher in search results and are included in recommended data sources.

You would allow authorized Analysts (that is, the Publishers group described earlier) to connect their workbooks to data sources in this project, but not download or edit them. You would deny capabilities to the Business Users group, so those users would not even see this project.

**Inactive content**

Another possibility is to segregate workbooks and data sources that the site’s administrative views show haven’t been used for a period of time. You could give content owners a time limit before their content is removed from the server.
Tableau Server on Linux Administrator Guide

Whether you do this or delete directly from the working projects is up to your organization. In an active environment, don’t be afraid to be intentional about removing content that is not being used.

**Source for workbook templates**

This is a project that people can download from but not publish or save to, where authorized publishers or project leaders make template workbooks available. Templates that have your organization’s approved fonts, colors, images, and even data connections built in can save authors a lot of time and keep your reports looking consistent.

Help project leaders manage content and users find it

- Devise a scalable project-naming scheme that makes sense in your organization.

  For example, basic structure might be `<Department> - <ContentUse>`; such as **Ops - Production**.

- Use the project’s **Description** field.

  The description you enter when you create a project appears when you hover the pointer over the project thumbnail, as well as on the **Project details** page.
6. Lock permissions in each project

After you refine the capabilities for each group in a project, you can lock the project’s permissions. Do this on the Default project, too.

1. With a project’s Permissions page open, select the button next to Permissions for workbooks and data sources are

2. In the dialog box that appears, select Locked to the project.

Locking permissions prevents publishers from setting permissions explicitly as part of the publishing process in Tableau Desktop. Instead, content inherits permissions set on the project it’s published to, and only administrators and project leaders can set permissions.

Automate working with groups and projects

Creating multiple groups and projects and setting permissions manually can get a little tedious. To automate these processes, as well as make them repeatable for future updates, you can perform these tasks using REST API commands.

You can use tabcmd commands for tasks such as adding or deleting a single project or group and adding users, but not for setting permissions.
Next steps

Besides projects, groups, and permissions, other data governance themes include:

**User education**

Help *all* of your Tableau users become good data stewards. The most successful Tableau organizations create Tableau user groups, have regular training sessions, and so on.

For a common approach to orienting users to the site, see Dashboard-based Custom Portals.

For publishing and data certification tips, see the following topics:

- Use Certification to Help Users Find Trusted Data
- Prepare for Publishing a Workbook (links to Tableau Help)
- Best Practices for Published Data Sources (links to Tableau Help)

**Optimize extract refresh and subscription activity**

If you use Tableau Server, create policies for extract refresh and subscription schedules, to avoid them dominating the site’s resources. The TC customer presentations by Wells Fargo and Sprint address this subject in detail. In addition, see the topics under Tuning & Operations.

If you use Tableau Online, see the following topics to become familiar with the ways people can refresh extracts:

- Keep Data Fresh
- Use Tableau Bridge to Expand Data Freshness Options

**Monitoring**

Use administrative views to keep an eye on the site’s performance and content use.

**Administrative Views**
Learn how Tableau and some of our customers address governance and self-service

The following list contains links to data governance and Center of Excellence (COE) presentations given at the Tableau Conference over recent years. Even if Tableau versions have evolved, the principles remain the same. You can explore the playlists for other videos related to COE, managing Tableau at scale.

Creating a Centre of Excellence in Tableau (TC Europe 2018)

Server Admins: Don’t Fear Web Authoring (Sprint, TC16)

The Past, Present, & Future at Charles Schwab (TC 17)

Content Strategies in Tableau (TC 17)

Use Projects to Manage Content Access

When Tableau Desktop users publish a workbook or data source to a site on Tableau Server, they can select a project to publish it to. If they don’t specify a project, their content is published to the Default project.

As an administrator, you can create projects to hold and organize related content resources, or to delegate content management. Content resources on Tableau Server are workbooks, views, and data sources, and the projects that hold them.

The following image shows content within the top-level Operations project in the web authoring environment. The Operations project contains a few child projects (highlighted) and published workbooks. A project can also contain other content types, such as data sources and flows.
Why use projects

Projects help you to create a scalable process for managing access to the content published to Tableau Server. Advantages they have include:

- They enable administrators to delegate content management to project leaders who work with the content more closely, without having to give them administrator access to site or server settings.

  Project leaders can create nested projects under their top-level project, enabling them to maintain their team’s content within a single hierarchy.

  **Note:** Project owners can delete top-level projects they own.

- They can make the site easier to navigate for self-service users.
They segment the Tableau Server site into areas that give users access based on how they use the data published to those areas, or on the Tableau user group they work with.

You can hide projects from groups who don’t need to use them, create a distinguishable project-naming scheme, and take advantage of project descriptions to clarify how to use the project.

- They enable you to track permissions effectively.

You can create groups based on the level of content access users in the group need, and set default permissions on projects. This enables you to know exactly which capabilities new users get by default, and likewise which capabilities all users get when a new project is created.

When to create project hierarchies (example)

Many organizations have several or more distinct groups of Tableau users, each with its own priorities and leaders. These groups might share some organization-wide content (or even draw from an org-wide pool of data sources), but primarily they use data and reports that are specific to their team. In this or similar scenario, an example for using project hierarchies might look as follows:

1. You, as a site or server administrator, can create top-level projects for each of your distinct Tableau teams.

2. On each top-level project, you assign the Project Leader role to team leads, and change project ownership.

   Project leaders effectively are the content administrators, so it’s important that they understand how permissions work in Tableau, along with Tableau content management best practices.

3. Each project leader takes over their project, creating the structure within the project that works for their team.
That is, they can create child projects they need, based on how their team members collaborate and share data and reports.

The benefit to you as the site administrator is that you can focus on system health. The benefit to your Tableau users is that people who know the best practices for working with Tableau and data can manage these things for their teams, without having to submit IT requests to change permissions or add projects.

Why not use sites?

If you manage your own Tableau Server deployment, you can create as many sites as you want. However, for managing data and reports across your company, projects allow the flexibility you need to administer shared data and reports, and users who might belong to multiple groups. Many Tableau administrators configure projects as described in the previous section, to expose only what’s necessary to users who need to work with it. Projects work better than sites for evolving content from development to staging to production.

Sites work well when content can remain completely separate during all phases, and there is little to no user overlap. A good (and common) example for using multiple sites is to create a site for each of multiple external clients, whose published content you manage as a consultant or vendor. Our own Tableau Online is an example of this on a large scale. Another example might be to use a separate site for sensitive content that you want only specific Human Resources or medical staff to use.

Project-level administration

As a server or site administrator, you can delegate administration of projects and their content, without exposing access to your site or server settings. You can do this by changing the ownership of a project or granting a group or user the Project Leader permissions role on a project.

The **project owner** is always one individual user. By default, the user who creates a project is its owner. The project owner has administrative access to the project and content in it—including making someone else the owner and assigning Project Leader permissions.
The **Project Leader** permissions role provides a way to allow multiple users administrative access to a project, its child projects, and all workbooks and data sources in those projects.

A project leader does not have to be a project owner or administrator. In addition to server and site administrators, the full scope of Project Leader permissions is available to users with a **Creator** or **Explorer (Can Publish)** site role.

**Project ownership and project leader access in project hierarchies**

In a multi-level project hierarchy, a user or group that is given the Project Leader permissions role to a project, at any level within the hierarchy, is implicitly given Project Leader access to all of that project’s child projects and their content items.

To remove the Project Leader access, you must do so at the parent level in the hierarchy on which the ownership or role was explicitly assigned.

Similarly, the owner of a project at any level has project leader access to all content in that project, as well as to any of its child projects, even if they do not own the child projects.

Only a project owner or administrator can change ownership of a content resource, and this can be done regardless of whether the project permissions are locked at the top level.

**Actions project-level administrators can take on projects**

Project leaders and owners can perform the tasks in the following list, as can server or site administrators.

- Create and delete projects as follows:
  
  Server or site administrators can create or delete top-level or nested projects anywhere on the site.

  Project owners and project leaders can create and delete child (nested) projects in projects they own, or on which they have Project Leader permissions.

  Project owners can change ownership of their projects. Both project owners and
project leaders can assign the Project Leader permissions to groups or users.

As a project leader or owner, if you assign the Project Leader permissions role to someone else, remember that full access to this role’s capabilities depends on the user’s site role, as specified earlier in this section.

- Set permissions for a project, as well as the child projects, workbooks, and data sources in it.

- Lock permissions to apply the top-level project’s default settings to all workbooks, data sources, and child projects and their content. Permissions can be modified only from the project on which they’re locked.

In a locked project hierarchy, only the owner or project leader of the top-level project in the hierarchy can change permissions.

- Move workbooks and data sources to another project to which they have Project Leader or owner access.

Moving the project can affect permissions. For information, see Add Projects and Move Content Into Them.

- Run, add, or remove extract refresh schedules.

See also Permissions in Project Hierarchies

How the Default project acts as a permissions template

Tableau creates a **Default** project with every site.

The Default project serves as a template for new top-level projects you create on the site. When you create a new top-level project, settings and permissions from the Default template are applied to the new project, including permissions set on content within the project.
**Note:** Nested projects (projects you create within other projects) take the permissions set at their parent project, not the Default project.

Before you create other top-level projects, you can take steps to set up the Default project, to help you to know exactly:

- Which type of user gets what level of access for each new project.
- How you might need to modify permissions for each new project.

For more information, see Steps to coordinate projects and groups in the topic Configure Projects, Groups, and Permissions for Managed Self-Service.

**Prevent publishers from changing permissions on content they own**

Administrators and project leaders can prevent users from changing the permissions for workbooks and data sources in a project hierarchy. For example, you can disable the option to set permissions during the publishing process, and prevent publishers and content owners from changing them after publishing. To do this, you lock content permissions to the project. For more information, see the links below.

**Next steps**

- Add Projects and Move Content Into Them
- Permissions in Project Hierarchies
- Set Project Default Permissions and Lock the Project

**Add Projects and Move Content Into Them**

A content resource (workbooks and data sources) can live in only one project. Server and site administrators can add or remove top-level projects on a site, and move published content from one project to another. Project leaders with appropriate site roles can add or remove
child projects and move content between projects on which they have Project Leader access.

This article contains the steps for creating and moving projects. We recommend becoming familiar with the following related content as well:

- To learn about projects and when or why to use them, see Use Projects to Manage Content Access.
- Before you create project hierarchies, become familiar with Permissions in Project Hierarchies.
- To see the specific site roles that allow full Project Leader access, see Project-level administration.

Add a top-level or child (nested) project

1. While you’re signed in to Tableau Server as an administrator or project leader, select the Content tab, and then do one of the following:
   - Select Create > Project to create a new top-level project (only administrators can do this).
   - Navigate to and open the project in which you want to create a sub-project, and then select Create > Project.

   If you’re not sure where to find a child project, display filters, and select Show all projects.

2. Enter a name and description for the project, and then click Create.
You can include formatting and hyperlinks in the project description. Select **Show formatting hints** for syntax.

**Note:** To edit a project description later, select it to open it, select the information icon next to its name, and then click **Edit**.

Move a content resource to another project

1. On the **Content** tab, find the content resource you want to move.
   
   If you’re not sure where to find a child project, display filters, and select **Show all projects**.
   
   For other content types, you can navigate through its project hierarchy, or by selecting the content type on the **Explore** menu.

2. On the workbook’s **Actions(...)** menu, select **Move**.

3. Select the new project for the workbook, and then click **Move Content**.
Moving a project includes moving everything in it, including child projects and their content.

How moving projects affects Project Leader permissions

When you move a project, Project Leader permissions adapt to the new project environment.

- When the target project hierarchy is **locked**, previous Project Leader permissions are removed, and new Project Leader permissions are granted according to those set at the top-level of the target hierarchy.

- When the target project hierarchy is **unlocked** (managed by owner), previous implicitly granted Project Leader permissions are removed, explicitly set Project Leader permissions are retained, and new Project Leader permissions are granted according to those set at the top-level of the target hierarchy.
Delete a project

When you delete a project, all of the workbooks and data sources in the project are also deleted from the site. If you want to delete a project but not its content, move the content to another project, and then delete the project.

Important

- You cannot undo deleting a project.
- Deleting a project deletes all content in it, including child projects and their content.
- You cannot delete the Default project.

To delete a project:

1. On the Content tab, find the project you want to remove.
   
   If you’re not sure where to find a child project, display filters, and select Show all projects.

2. On the project’s Actions (…) menu, select Delete.

3. Confirm that you want to delete the project.

Required access level for moving content

Moving content is effectively like removing it from one project and publishing it to another. For non-administrators, the permissions needed on the source project are different than those needed on the destination project.

Note: The term permissions role refers to the collection of related capabilities you can assign as a set.
Required site role

To move content, users must have one of the following site roles:

- Server Administrator (Tableau Server only)
- Site Administrator Creator or Site Administrator Explorer
- Creator or Explorer (Can Publish)

Users with a Server Administrator or Site Administrator site role do not need any additional capabilities.

Required permissions for the project that users move content to

Non-administrators must have the Publisher or higher permissions role set on the project that is the move destination.

Required permissions for the project that users move content from

Non-administrator users must have these additional capabilities on the project:

- Ownership of the project or the Project Leader or Publisher permissions role.
  
  OR

- In a project hierarchy, project owner of, or Project Leader permissions role on the project or a parent project higher in the hierarchy.
If they have the Publisher permissions role on the project, and they are not the project owner (or owner or leader of a parent project), they must have the following capabilities:

**Data sources:** Data source owner

**Workbooks:** Workbook owner or Move capability set explicitly on the workbook.

You can grant the Move capability individually, or along with related capabilities allowed through the Editor permissions role.

**Set Project Default Permissions and Lock the Project**

As an administrator or project leader, you can organize related content into projects. You can then set a project’s permissions—including the default permissions that will be set on child projects you create under that project, and on other content published in that project hierarchy. You can further lock the top-level project, at which point only administrators and project leaders can change permissions, and then only at the top-level project.

Administrators and users with an appropriate site role plus the **Project Leader** permissions role can lock permissions to a project. For more information, see Permissions in Project Hierarchies.

**Prerequisites**

The remaining sections in this article assume the following:

- You have already created your user groups.
  
  For a best practice recommendation for creating groups, see Steps to coordinate projects and groups in the topic Configure Projects for Managed Self-Service.

- You understand which site roles allow access to all Project Leader capabilities. For information, see Project-level administration.

**Set the default permissions for a project or multiple projects**

These steps focus on our recommended practice of assigning permissions to groups; however, you can assign permissions to individual users the same way.
Tableau Server on Linux Administrator Guide

Before you can complete these steps, you must create your groups, as mentioned in Pre-requisites.

1. While you’re signed in to Tableau Server as an administrator or project leader, go to the Content page, and locate the project you want to work with.

   If you’re not sure where to find a child project, display filters, and select Show all projects.

2. Select the check box next to each project for which you want to set default permissions, and select Actions > Permissions.

3. Click Add a user or group rule, select Group, and then select the group or name from the list.
For an existing group, open the actions menu, and then select **Edit**.

4. Select a permissions role for **Project**, **Workbooks**, or **Data Sources**, and then click **Save**.
To create a custom set of capabilities, select the **Project**, **Workbooks**, or **Data Sources** labels to expand the permissions view. Click capabilities to set them to **Allowed**, **Denied**, or **Unspecified**. Click **Save**.

The following image shows how to set project permissions. The same general steps apply for workbooks and data sources.

**Note:** To change the settings after saving, open the group’s or user’s actions menu (….), and then select **Edit**.

5. View the effective permissions:

   Select a group name or user name in the permission rules to see the resulting user permissions.
Expand the Project, Workbooks, or Data Sources permissions views to see individual capabilities.
Hover over a capability box to see a tooltip with details on whether a capability is allowed or denied.

6. Follow the same steps to configure additional permission rules for more groups.

Lock or unlock permissions on a top-level project

1. Sign in to your Tableau Server site as an administrator or project leader, and go to the Content page to see the top-level projects.

2. On a project’s Actions (...) menu, select Permissions.

3. Click Edit Content Permissions.

4. In the Content Permissions in Project dialog box, select Locked to the project, and then click Save.
5. To unlock content permissions for the projects, click **Edit Content Permissions** again, and select **Managed by owner**.
The default permissions are re-applied to content in the project, and permissions for each item are now editable.

Permissions roles you can set at the project level

Permissions roles are built-in templates that assign a common set of capabilities on content. You can assign them only at the project level, for the project itself, and the workbook and data sources in it.

<table>
<thead>
<tr>
<th>Template</th>
<th>General description</th>
</tr>
</thead>
</table>
| Project Leader | Combined with the appropriate site role, allows the user or group full access to the project, its child projects, and content published into that project hierarchy.  
To learn more, see Project-level administration. |
| Editor      | Allows the user or group to connect to, edit, download, delete, and set permissions for data sources or workbooks in the project. |
They can also publish data sources, and as long as they are the owner of a data source they publish, can update connection information and extract refresh schedules. This permission is relevant for views when the view they access connects to a data source.

<table>
<thead>
<tr>
<th>Capability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publisher</td>
<td>Allows the user or group to publish content to the project.</td>
</tr>
<tr>
<td>Connector</td>
<td>Allows the user or group to connect to data sources in the project.</td>
</tr>
<tr>
<td>Viewer</td>
<td>Allows the user or group to view, download, and add comments to workbooks and views in the project.</td>
</tr>
<tr>
<td>None</td>
<td>Sets all capabilities for the permission rule to <strong>Unspecified</strong>.</td>
</tr>
<tr>
<td>Denied</td>
<td>Sets all capabilities for the permission rule to <strong>Denied</strong>.</td>
</tr>
</tbody>
</table>

Capabilities you can set for a project

The three capabilities you can set specifically for a project are: **View**, **Save**, and **Project Leader**.

<table>
<thead>
<tr>
<th>Capability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td>Allows the user or group to view the workbooks and views in the project. The View capability must also be allowed for the individual workbooks and views in the project.</td>
</tr>
<tr>
<td>Save</td>
<td>Allows the user or group to publish workbooks and data sources to the server and overwrite content on the server. The Save capability must also be allowed for the individual workbooks and data sources in the project. When allowed, the user with a site role that supports publishing</td>
</tr>
</tbody>
</table>
can re-publish a workbook or data source from Tableau Desktop, thereby becoming the owner and gaining all permissions.

Subsequently, the original owner’s access to the workbook is determined by that user’s group permissions and any further permissions the new owner might set.

This permission also determines the user’s or group’s ability to overwrite a workbook after editing it on the server. For related information, see Set Web Edit, Save, and Download Access on Content.

| Project Leader | Combined with the appropriate site role, allows the user or group to set permissions for all items in the project, lock project permissions, and edit default permissions.

To learn more, see Project-level administration.

See also

Content Permissions and Ownership

Use Projects to Manage Content Access

Configure Projects, Groups, and Permissions for Managed Self-Service

Permissions in Project Hierarchies

As an administrator or project leader, you can decide how permissions are set in a project hierarchy you manage. On the top-level project in a hierarchy, you can set the project to one of two available states: locked and managed by owner. Locking permissions can help you maintain a predictable permissions model within a project hierarchy. For example, it denies publishers the option to set explicit permissions on workbooks and data sources they own.
Project permissions states: locked and managed by owner

You can lock permissions in project hierarchies at the top level of the hierarchy. When you lock permissions, the top-level project’s permissions settings are applied to all workbooks, views, and data sources in the hierarchy.

In a locked project hierarchy, only administrators and project leaders with an appropriate site role can modify permissions, and they can do so only on the top level. Publishers cannot set permissions on their content during or after publishing from Tableau Desktop.

When permissions are managed by the owner (“unlocked”), they become editable by content owners and other users with the appropriate access level. During publishing, users have the option to set permissions explicitly on the workbook or data source they are publishing, unless you explicitly deny this capability on groups they are members of or individual users.

To clarify, owners always get full read, write, and other access to the content they publish, but in a locked state, they cannot change permissions on it.

**Note:** If a workbook, data source, or project with editable permissions is moved to a locked project, the permissions set on the locked project are applied to that content. The moved content’s permissions are then locked.

When to use each state

In general permissions are easier to manage when you lock projects. You need to go only to one place to see how they’re set for all content in that project’s hierarchy.

However, this requires that all child projects have the same permissions as set at the top level. The following common scenarios are possible only when you keep the project hierarchy unlocked:
You want to create projects for different types of access your team needs for content in child projects. This strategy is described in Configure Projects, Groups, and Permissions for Managed Self-Service, and it requires setting unique permissions on each child project.

If you keep permissions unlocked, you can still set permissions at a parent project level that you want all new child projects to take by default. You can use groups to set capabilities explicitly, including denying the Set Permissions capability, so that users cannot set permissions on content they don’t own. Users will always be able to set permissions on content they own within unlocked project hierarchies.

In web editing, you want to allow publishers to save changes to workbooks but not overwrite them.

For more information, see Allow users who can publish to edit, save changes to, and download new workbooks, but not overwrite existing workbooks.

How permissions are evaluated in project hierarchies

The following diagram shows how ownership and Project Leader permissions are applied in a hierarchy.

- PL = Project Leader
- O = Owner
- Dotted line indicates implicit permissions “inherited” at a parent level.
- * = Owner was assigned explicitly by the owner of the parent project.
How permissions are applied in locked project hierarchies

You can lock permission only at the top-level in a project hierarchy, and the following behavior applies:

- All child projects you create within a top-level project use the default permissions set at that top-level project (not the Default project), and you cannot modify permissions at the child-project level.

- Workbooks, views, and data sources also use the default permissions set on the top-level project.

- Users, including content owners, cannot edit permissions for individual workbooks, views, or data sources.

When users publish workbooks and data sources from Tableau Desktop, they cannot set permissions in the Publish dialog box, and their content gets the default permissions for the project they publish it to.

- Users or groups that have an appropriate site role and are assigned the Project
Leader permissions role at the top-level project get project leader access to all child projects and their workbooks and data sources.

- Administrators and content owners can change ownership at any level in the hierarchy.

- Administrators and project leaders can edit permissions at the top-level project, and those changes propagate to all child projects.

How permissions are applied in unlocked project hierarchies

If the top-level project’s permissions are not locked, you can set permissions on its child projects in the same way you can on top-level projects, with the exception of locking the child project.

When you create a child project, it takes default permissions from the parent project. Users implicitly get the same permissions they have on the parent project.

If you set permissions at the child level, those settings take precedence over permissions set at the parent level.

See also

For a couple of best-practice steps for how to implement permissions, see the following:

- Configure Projects, Groups, and Permissions for Managed Self-Service

- Structure Content Projects, Groups, and Permissions (links to Everybody’s Admin Guide)

Add a Project Image

To help distinguish projects you manage on Tableau Server (and help your users find them), you can add an image that appears in the thumbnail.
Set a project image

Before you begin, verify that image you will be referencing meets the following requirements:

- The image must be accessible using the HTTP or HTTPS protocols. Shared network directory and related protocols (UNC, SMB, AFP, NFS, etc) are not supported.
- All users who access the project must have, at a minimum, “read-only” permission on the target image.
- The image must be common internet format: .jpg, png, or gif.

1. Sign in to a site on Tableau Server. In the list of **Top-level Projects** you have access to, select or navigate to the project you want to update.

   If you’re not sure where to find a child project, use the *Explore* drop-down list and select **All Projects**.

2. Click the **Details** icon (i), to open the **Project details** dialog box, and then click **Edit**.
3. In the **About** field, at the end of the project description, add the URL for your image using the following syntax:

```
!http://www.example.com/image.png!
```
Select **Show formatting hints** to see how you can format description text.

**Note:** Images embedded in project descriptions cannot be resized or positioned. Recommended size is (300 x 184 pixels). Images that are not 300 x 184 pixels may be stretched, shrunk, or cropped to fit the width of the thumbnail. In addition, they must be added at the end of the project description and be enclosed in ! (exclamation marks), otherwise they will not be displayed as the thumbnail.

4. **Click Save.**
Content Permissions and Ownership

In Tableau Server, you set content permissions to specify who is allowed to work with which content resources on a particular site.

For example, you can tightly restrict who has access to your company’s financial information, but widely share organizational development content.

Content resources on which you assign permissions include the following:

- Projects
- Workbooks
- Data sources
- Flows

Views in a workbook inherit permissions from the workbook, although you might have an edge case for which you want to set permissions for a single view.
What makes up a user's permissions

When Tableau determines which tasks (or capabilities) a user is allowed to perform on a content asset, it takes the following pieces into account:

**Site role:** At the time that you add users to a site, you must apply a site role to them. The site role and license role are the only attributes that you apply to users (as opposed to content) to affect permissions. The site role determines the license role that the user occupies, and together they determine whether the user can publish, interact with, or only view published content on that site. See Set Users’ Site Roles.

**Permissions rules and templates:** You authorize content access through permissions rules. These rules describe the capabilities that you want a user or group to be able to perform on a set of content assets. Examples of capabilities include editing a view or connecting to a data source. Tableau provides a set of templates for common permissions roles, such as Editor, Project Leader, and so on.

**Content ownership:** By default, the person who publishes a flow, data source, or workbook to the server is the owner of that content asset. Content owners can set permissions on the content assets they own. A project owner, an administrator, or a project leader can change ownership or set defaults at the project level.

**Effective permissions:** are the capabilities that define what a user is allowed to do with a content resource after Tableau Server evaluates permissions rules and settings.

Who can set permissions

Among the actions that users can be allowed to do with content is the Set Permissions capability. By default, the following users can set permissions in the specified contexts:

- Administrators, for all content on the site.
- Project leaders, for all content in the project and its child projects.
Tableau Server on Linux Administrator Guide

- Content owners, generally those who create projects or publish flows, data sources, or workbooks.

Quick Start: Permissions

You can use permission rules to control access to content on a site. A permission rule is a set of capabilities that defines the level of access a group or user has on a content item. Content items are projects you create, and the workbooks and data sources published to them.

The most efficient way to manage permissions is to remove permissions from the All Users group before you create new groups for your environment. Then assign the permissions to groups at the project level.

1 Add users to groups

Create groups for users based on who should have the same permissions, and then add users to those groups. Within a site, select Groups. Select a group name, and then select Add Users.
2 Open a project's permissions settings

The site’s **Content** page shows the top-level projects. Navigate to the project you want to update, select its **Actions (…)** menu, and then select **Permissions**.
If you’re not sure where to find a child project, display filters, and select **Show all projects**.

3 Create a permissions rule

Click **Add a user or group rule**, select **Group**, and then find and select the group.

Select a permissions role template to apply an initial set of capabilities for the group. Click a capability to set it to **Allowed** or **Denied**, or leave it **Unspecified**. Click **Save** when you are done.
Whether a user can set permissions is based on their site role and how their *Set Permissions* capability is set.

4 View a user's effective permissions

After you save the permissions rule for the group, you can view the effective permissions for that content.

Click a group name to see the group's users and their permissions. Hover over a capability box to see a tooltip with details on whether a capability is allowed or denied.
**Custom** indicates a user’s capabilities have been changed from the initial settings for their site role or content role.

Site roles

A user’s site role determines the maximum permissions allowed for that user.

- Server and site administrators can access all site content and take actions on it.
- Owners always get full access to the content they’ve published. When the parent project permissions are not locked, owners can change permissions for their published content.

For more information, see Set Users’ Site Roles and Use Projects to Manage Content Access.

Permissions evaluation

- **Denied** takes precedence over **Allowed**.
- **Unspecified** results in **Denied** if no other permissions are specified.
Specific user permissions on content take precedence over group permissions on content. In other words, user permissions trump group permissions.

For a couple of best-practice steps for how to implement permissions, see the following:

- Configure Projects, Groups, and Permissions for Managed Self-Service
- Structure Content Projects, Groups, and Permissions (links to Everybody’s Admin Guide)
Manage Content Ownership

When you publish a data source or workbook on Tableau Server or when you create a project, you become its owner. A content owner, a project leader with an appropriate site role, or an administrator can change ownership of a content asset. After ownership is reassigned, the original owner has no special connection to the content item, and their ability to access it is determined by their permissions on the project or that specific item.

Who can change or be given ownership, by content type

Whether you can change or be given ownership depends on your permissions and your relationship to the content asset, as described in the following table.

Note: Full project leader access is available only with some site roles. For information, see Project-level administration.

<table>
<thead>
<tr>
<th>Content asset type</th>
<th>Who can change ownership</th>
<th>Who can be given ownership</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top-level projects</td>
<td>Server administrator¹</td>
<td>Server administrator</td>
</tr>
<tr>
<td></td>
<td>Site administrator</td>
<td>Site administrator (Creator and Explorer)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Creator</td>
</tr>
<tr>
<td>Child (nested) projects</td>
<td>Server administrator</td>
<td>Any administrator or user of the site, excluding users with a Read Only site role.</td>
</tr>
<tr>
<td></td>
<td>Site administrator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Project leader or owner</td>
<td></td>
</tr>
<tr>
<td>Workbooks and data sources</td>
<td>Server administrator</td>
<td>Any administrator or user of the site, excluding users with a Read Only site role.</td>
</tr>
<tr>
<td></td>
<td>Site administrator</td>
<td></td>
</tr>
</tbody>
</table>
Workbook or data source owner

Project leader or owner of the project that contains the item

<table>
<thead>
<tr>
<th>Flows</th>
<th>Server administrator</th>
<th>Site administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Flow owner</td>
<td>Project leader or owner of the project that contains the item</td>
</tr>
</tbody>
</table>

Any administrator or user of the site, excluding users with a Read Only site role.

1 The Server Administrator site role applies to Tableau Server only; not Tableau Online.

Considerations for changing content ownership

- Before you remove a user from Tableau Server, make sure they do not own any content assets.

  If the user does own content, you must first reassign ownership of those assets before you can delete the user. Otherwise, their site role is set to **Unlicensed**, but they are not deleted, and only an administrator can take certain actions on that content.

- If you change the ownership of a flow, workbook or data source that includes embedded credentials, to connect to underlying data, the embedded credentials will be deleted.

  You can update the embedded credentials by editing the connection information on Tableau Server. For more information, see **Edit Connections**. Alternatively, the new
owner can download the flow, workbook or data source, and open the item in Tableau Desktop to update the embedded credentials, and then re-publish the workbook or data source.

- If you do not lock permissions to projects, make sure users you give content ownership to know your permissions guidelines, or you account for permissions as you change ownership. In unlocked projects, by default, content owners can set permissions on their content. For more information, see Permissions in Project Hierarchies.

Change the owner of a content resource

1. Sign in to the Tableau Server web environment and select the Content tab.

2. Navigate to the content you want to assign to someone else.

   - If you want to re-assign multiple of the same type of content, for example, multiple workbooks, open the Explore menu, and select the content type.

   - If you want to re-assign multiple items within the same project, navigate to the project.

     If you’re not sure where to find a child project, display filters, and select Show all projects.

3. Select the items you want to reassign, and then select Actions > Change Owner.

   The other menu commands you see will depend on the content type.
4. Type the name of a user or select a user from the list.

5. Click **Change Owner**.

View or Edit Permissions

When you specify permissions for a project, workbook, view, flow, or data source, you use a permissions rule to express who is allowed to work with that resource. Permissions rules
are the explicit capabilities that can be set for an individual user—or for a group—for each resource.

You work with these rules in the Permissions window, described in the steps below. You define permissions rules in the upper section. The User Permissions section below it shows the effective, or resulting, permissions after Tableau evaluates your rule.

View or edit a permissions rule for a selected content resource

1. Sign in to your Tableau site, go to the Content page, and navigate to the item on which you want to set permissions.

   If you’re not sure where to find a child project, display filters, and select Show all projects.

2. On the item’s Actions (…) menu, select Permissions.
This opens the current permissions rules.

3. To edit a rule, do the following:
   a. Select the Actions menu (…) next to the rule name, and then select **Edit**.
   
   b. Select a permissions role to assign a set of capabilities and leave the rest unspecified.
      See How the permissions rules settings work together below for more information.
      
   c. Select an individual capability to cycle through **Allowed** or **Denied**, or **Unspecified** settings.
      
   d. Click **Save**.

4. To see the resulting permissions for the selected group or user, do the following:
   a. In the permissions rules area, select the group or user name.
      
   b. In the **User Permissions** area, hover over a capability box to show a tooltip that indicates the capability name, its resulting setting, and how the result was determined.
      
      The following image shows permissions on a selected workbook for Andrew Allen in the Finance group. The tooltip indicates that a rule assigned to a group he is a member of denies the web edit capability.
How the permissions rules settings work together

In the Permissions window, the settings that appear depend on the type of content you select, and some are not available until you edit the rule, as described earlier in this article.

The following settings apply to permissions on projects. Data sources and workbooks show similar sections:

- **User / Group**: Lists users or groups that a rule applies to. If the permissions are not locked to the top-level project, you can select **Add a user or group rule** to configure permissions on the selected project, which then become default settings for this project’s child projects.

- **Project**: Lists available permissions-role **templates** for projects. Each template contains a predefined set of capabilities for the rule.

- **Workbooks / Data Sources**: Similar to Project, lists the permissions-role templates for assigning predefined sets of capabilities for workbooks or data sources.

- **View / Interact / Edit**: These are categories of capabilities that you can set to **Allowed**, **Denied**, or **Unspecified**. Setting **Unspecified** evaluates to **Denied** if no other permissions are specified for a user or group on the content.
Although some of the permissions-role names are the same as or similar to site role names, the permissions roles are separate, and they indicate groups of capabilities that are typically configured as a set.

What determines users’ effective permissions

Effective user permissions for a content resource are determined by the following:

- The maximum capabilities allowed for a user’s site role. The site role acts as the “ceiling” for what permissions are allowed. For more information, see Set Users’ Site Roles.

- Whether the user is a project leader for a project hierarchy or is shown as the owner of a content asset.

- The evaluation of each permissions rule that applies to that user, or a group the user is a member of, for the selected content type or content item.

For example, if a user is granted the Editor permissions role for workbooks in a project (which allows all available workbook capabilities), but has the site role of Viewer and does not own any workbooks, the user will be allowed only the capabilities of View, Download Image, Download Summary Data, View Comments, and Add Comments.

In the following example, a permissions rule has been created for the Finance group. Initially, the administrator applied the Editor permissions role to the group. This granted all capabilities. Then the admin set the Save capability to Denied. This changed the name of the permissions role to Custom. The User Permissions (effective permissions) section for the Finance group reflects these actions. You can also see that one user has fewer capabilities, because that user has a site role of Viewer.
Tip: The All Users group permissions rule in this example has been set to None, which leaves all of the permissions as Unspecified for the All Users group. This approach requires the administrator to assign permissions only to the groups or users that should have access to content assets, which makes for more predictable effective permissions. For more information, see 2. Remove permissions that will cause ambiguities in the topic Configure Projects, Groups, and Permissions for Managed Self-Service.

Set Permissions on Individual Content Resources

As an administrator, or as a user granted the Set Permissions capability on a specific resource, you can change permissions on that resource (data source or workbook).

Generally we recommend setting permissions at the project level for all content in the project. A reason you might want to deviate from this practice, for example, is to explicitly deny the some capabilities on a data source or workbook that has a data source or user filter that enables a form of row-level security.
Capabilities you can set on data sources

Use permission rules to set the following capabilities for a data source:

<table>
<thead>
<tr>
<th>Capability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td>View the data source on the server.</td>
</tr>
<tr>
<td>Connect</td>
<td>Connect to the data source. The <strong>Connect</strong> permission allows a user to connect to a data source from an editor (in Tableau Desktop or Tableau Server web editing). <strong>Note:</strong> If a workbook author embeds credentials in a workbook or view, users who also have the <strong>Web Edit</strong> permission will be able to access the workbook’s data source regardless of their <strong>Connect</strong> permissions.</td>
</tr>
<tr>
<td>Save</td>
<td>Publish data sources to the server and overwrite data sources on the server.</td>
</tr>
<tr>
<td>Download Data Source</td>
<td>Download the data source from the server.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Cube data sources, like those for Microsoft Analysis Services or Oracle Essbase connections, must be used locally. To download the published data source to Tableau Desktop, the user must have the <strong>Download</strong> capability. You must explicitly grant the <strong>Download</strong> permissions regardless of the permissions role you apply. For more information, see Cube Data Sources.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete the data source.</td>
</tr>
</tbody>
</table>
Set Permissions

Grant or deny permissions for the data source.

Permission role templates for data sources

<table>
<thead>
<tr>
<th>Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connector</td>
<td>Allows the user or group to connect to the data source on the server.</td>
</tr>
<tr>
<td>Editor</td>
<td>Allows the user or group to connect to, download, delete, and set permissions on data sources on the server. They can also publish data sources, and as long as they are the owner of a data source they publish, they can update connection information and extract refresh schedules. (The latter two capabilities are no longer available if an administrator or project leader changes data source ownership.)</td>
</tr>
<tr>
<td>None</td>
<td>Sets all capabilities for the permission rule to Unspecified.</td>
</tr>
<tr>
<td>Denied</td>
<td>Sets all capabilities for the permission rule to Denied.</td>
</tr>
</tbody>
</table>

Capabilities you can set on workbooks and views

The list of capabilities and the available permission role templates vary depending on whether you are setting permissions for a workbook or a view. For information about capability definitions, see Permissions Reference.

Editing view-level permissions

When a Tableau Desktop author publishes a workbook with the Show Sheets as Tabs enabled, these tabbed views take on the workbook permissions rules. Changes you make to
the workbook permissions affect all of its tabbed views.

To edit an individual view’s permissions, save the workbook again without tabs (or hide sheets). The default permissions are applied to the workbook, and you can then edit view permissions.

We recommend that you set view-level permissions sparingly, as an exception. Try to manage permissions at the project level as much as possible. When permissions are locked to a project, views in a workbook use the workbook permissions.

Permission role templates for workbooks and views

<table>
<thead>
<tr>
<th>Template</th>
<th>Applies to...</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewer</td>
<td>workbooks and views</td>
<td>Allows the user or group to view the workbook or view on the server.</td>
</tr>
<tr>
<td>Interactor</td>
<td>workbooks and views</td>
<td>Allows the user or group to view the workbook or view on the server, edit workbook views, apply filters, view underlying data, export images, and export data. All other permissions are inherited from the user’s or group’s project permissions.</td>
</tr>
<tr>
<td>Editor</td>
<td>workbooks and views</td>
<td>Sets all capabilities for the rule to <strong>Allowed</strong>.</td>
</tr>
<tr>
<td>None</td>
<td>workbooks and views</td>
<td>Sets all capabilities for the rule to <strong>Unspecified</strong>.</td>
</tr>
<tr>
<td>Denied</td>
<td>workbooks and views</td>
<td>Sets all capabilities for the rule to <strong>Denied</strong>.</td>
</tr>
</tbody>
</table>

Capabilities you can set on flows

Use permission rules to set the following capabilities for a flow:
## Tableau Server on Linux Administrator Guide

### Capability | Description
--- | ---
View | View the flow on the server.
Run | Run the flow on the server
Save | Publish flows to the server and overwrite flows on the server.
Download flow | Download the flow from the server.
Delete | Delete the flow.
Set Permissions | Grant or deny permissions for the data source.

### Set permissions on a content resource

1. Sign in to your Tableau site, go to the **Content** page, and find the project that contains the items on which you want to set permissions.

   If you’re not sure where to find a child project, display filters, and select **Show all projects**.

2. Select the check boxes for each item, and then select **Actions > Permissions**.
Note: If you select multiple items, and the Permissions menu is not available, make sure you have been granted the Set Permissions capability on all of the selected items.

3. Click Add a user or group rule, select Group or User, and then select the group or user name from the list.

4. Select a permission role template to apply an initial set of capabilities for the group or user, and then click Save.

5. To further customize the rule, click the actions menu (…) next to the rule name, and
then click **Edit**. Click a capability in the rule to set it to **Allowed** or **Denied**, or leave it unspecified. Click **Save** when you are done.

![Permissions](image)

6. Configure any additional rules you want for other users or groups.

7. View the resulting permissions.

   Click a group name or user name in the permission rules to see the resulting permissions. Hover over a capability box to see a tooltip that shows whether a capability is allowed or denied, and what determined that result.
See also

How data access is evaluated for workbooks that connect to Tableau data sources

Manage a Flow

How Permissions are Evaluated

Permissions in Tableau Server are assigned to content assets—projects, workbooks, data sources, and occasionally to individual views. You use permissions rules to specify who can work with a content asset.

Each user’s level of access to content published to a site is determined by the following:

- **Site role.** A user’s site role determines whether a user can publish, interact with, or only view content assets. For more information, see Set Users’ Site Roles.

- **Content permissions.** Every project, workbook, data source, flow, or view theoretically can have a unique set of permissions rules.
A permissions rule includes the user or group, and the set of capabilities you want to grant users for an asset or set of assets. An example of a capability is Download Data Source.

Each permissions role template (such as Editor, Interactor, Viewer) specifies a pre-defined set of capabilities.

Available capabilities vary depending on the content type. Capabilities can be set to Allowed, Denied, or Unspecified. Denied always takes precedence over Allowed; Unspecified results in Denied if no other permissions rules allow a capability for a user.

- **Ownership**. Content owners always get full access to the content they've published, including setting permissions on it. In locked project hierarchies, you can prevent content owners from modifying permissions on their workbooks and data sources. For information, see Set Project Default Permissions and Lock the Project.

A user's effective permissions for a given content asset are determined by the following:

- The maximum capabilities allowed through the site role.

- Whether the user owns the content item.

- The result after Tableau evaluates permissions rules applied to that user and all groups the user is a member of.

You can set permissions rules for an individual user or group for each content asset. This diagram illustrates how permission rules are evaluated in Tableau Server.
Notes on permissions

- You cannot set permissions at the site level; permissions are assigned to only to content.

- Individual user permissions take precedence over group permissions.

- Workbook permissions serve as templates for view permissions. In a locked project, when a workbook uses tabbed views, views inherit workbook permissions. In an unlocked project, when a workbook is saved without tabs, the workbook and view permissions can be edited independently.

- For each content item, every site user is automatically included in the All Users group. As a result, when you create additional group permissions rules for a content item, the All Users permissions rules affect how permissions are evaluated. For more information, see 2. Remove permissions that will cause ambiguities in the topic “Configure Projects, Groups, and Permissions for Managed Self-Service.”

The order of precedence in which Tableau evaluates permissions

Tableau steps through the following rules, continuing to the next rule if the current one evaluates to “denied.” If any rule evaluates to “allowed,” the capability is allowed, and Tableau stops evaluating.

1. **Administrator site roles**: People with a site role of Server Administrator (Tableau Server only) or Site Administrator Creator can access all site content with full permissions, regardless of the permissions set on projects or individual content assets.

2. **License denies capabilities**: If a user’s license type explicitly denies the capability, the user is denied. For example, a user with a Viewer license cannot connect to data sources.

3. **Project Owner**: If the user owns a project that contains a content asset, the capability is allowed.

4. **Project Leader**: If the user has, or is in a group that has, the Project Leader
permissions role on a project, the user has administrative access to content in that pro-
ject.

5. **User is content owner**: If a user is the owner of a content asset, they are allowed all
access. However, in locked projects, administrators or project leaders can deny cap-
abilities at the project level, such as setting permissions on content the user owns. In
locked project hierarchies, content assets inherit permissions set on the top-level pro-
ject.

6. **User - capability denied**: If the user has been explicitly denied the capability on a
content asset, they are denied.

7. **User - capability allowed**: If the user has been explicitly allowed the capability for the
content, they are allowed.

8. **Group - capability denied**: If the user belongs to a group that has been explicitly
denied the capability for the content, they are denied.

9. **Group - Capability Allowed**: If the user belongs to a group that has been explicitly
allowed the capability for the content, they are allowed.

10. The user is denied access to the content.

Permissions Reference

This article lists the user and content settings that make up a given user’s ability to access
published data sources and workbook on a given site on Tableau Server.

Site and permissions roles that allow full content access

The following list describes roughly who gets full access to content and the scope of that
access:

- Server administrators (Tableau Server only) are allowed all capabilities on all content
  published to the server.

- Site administrators are allowed all capabilities on content published to the site they
Users with the Site Administrator Creator site role can also publish or save new content from any Tableau client that supports publishing functionality. For example, Tableau Desktop, Tableau Prep Builder, and the web authoring environment.

- In groups to which you apply the Project Leader role, users with the appropriate site roles are allowed all capabilities on content in the project.

To learn more about Project Leader permissions, see Project-level administration.

- Publishers become the owners of content they publish, and, by default, they are allowed all capabilities on that content. If they publish to a locked project hierarchy, they cannot set permissions on their content after publishing, unless they also are the top-level project owner or leader.

**Note:** For more information on permissions related to managing flows, see Managing Flows.

Capabilities available for each content type

The following table shows how permissions apply to content and describes each capability.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Applies to…</th>
<th>When allowed, users can…</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td>workbooks, data sources, views, projects, flows</td>
<td>Open the item on Tableau Server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> When a workbook is configured to show sheets as tabs, all views use the workbook permissions, even if different permissions are specified on an individual view.</td>
</tr>
<tr>
<td>Web Edit</td>
<td>workbooks</td>
<td>Edit views in workbooks. For information, see Set</td>
</tr>
<tr>
<td>Permission</td>
<td>Applies to...</td>
<td>When allowed, users can...</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>[ ]</td>
<td>views</td>
<td>Web Edit, Save, and Download Access on Content.</td>
</tr>
<tr>
<td>Save</td>
<td>workbooks</td>
<td>Overwrite the content asset on the server.</td>
</tr>
<tr>
<td></td>
<td>data sources</td>
<td>When allowed, the user can re-publish a workbook or data source from Tableau Desktop or save it in web authoring, thereby becoming the owner and gaining access to all permissions. Subsequently, the original owner’s access to the workbook is determined by that user’s group permissions, and by any further permissions the new owner might set. This capability also determines the user’s or group’s ability to overwrite a workbook after editing it on the server. The <strong>All Users</strong> group has special treatment: When a user publishes to a project on which the <strong>All Users</strong> group has permissions, the <strong>Save</strong> capability for the <strong>All Users</strong> group is changed from <strong>Allowed</strong> to <strong>Unspecified</strong>. This is to help protect an owner’s content from being overwritten by another user. You can manually modify this capability if you want to allow users to overwrite other users’ published content.</td>
</tr>
<tr>
<td>Download Workbook/Save As</td>
<td>workbooks</td>
<td>Download a Tableau packaged workbook (.twbx) from the server. Save an edited workbook as a new workbook on the server.</td>
</tr>
<tr>
<td>Permission</td>
<td>Applies to...</td>
<td>When allowed, users can...</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Download Data Source</td>
<td>data sources</td>
<td>Download the data source from the server.</td>
</tr>
<tr>
<td>Download Flows/Save As</td>
<td>flows</td>
<td>Download the flow from the server.</td>
</tr>
<tr>
<td>Delete</td>
<td>workbooks</td>
<td>Delete the content resource.</td>
</tr>
<tr>
<td></td>
<td>data sources</td>
<td></td>
</tr>
<tr>
<td></td>
<td>views</td>
<td></td>
</tr>
<tr>
<td></td>
<td>flows</td>
<td></td>
</tr>
<tr>
<td>Filter</td>
<td>workbooks</td>
<td>Modify filters in the view, keep only filters, and exclude data.</td>
</tr>
<tr>
<td></td>
<td>views</td>
<td></td>
</tr>
<tr>
<td>Add Comments</td>
<td>workbooks</td>
<td>Add comments to views in a workbook.</td>
</tr>
<tr>
<td></td>
<td>views</td>
<td></td>
</tr>
<tr>
<td>View Comments</td>
<td>workbooks</td>
<td>View the comments associated with the views in a workbook.</td>
</tr>
<tr>
<td></td>
<td>views</td>
<td></td>
</tr>
<tr>
<td>Download Summary Data</td>
<td>workbooks</td>
<td>View the aggregated data in a view, or in the user’s selection within the view, and download that data as</td>
</tr>
<tr>
<td>Permission</td>
<td>Applies to…</td>
<td>When allowed, users can…</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td><img src="image1.png" alt="Icon" /></td>
<td>views</td>
<td>a text file in .csv format.</td>
</tr>
<tr>
<td><img src="image2.png" alt="Icon" /></td>
<td>workbooks</td>
<td>View the underlying data behind each row in a view, as restricted by any marks the user has selected, and download the data as a text file in .csv format.</td>
</tr>
<tr>
<td><img src="image3.png" alt="Icon" /></td>
<td>workbooks</td>
<td>Download each view as to PNG or PDF format.</td>
</tr>
<tr>
<td><img src="image4.png" alt="Icon" /></td>
<td>workbooks</td>
<td>Users can save customizations they’ve made to a view using the interaction features (such as filters). They can then share their custom view for others to see. Customization in this way does not change the view’s default state or its underlying data.</td>
</tr>
<tr>
<td><img src="image5.png" alt="Icon" /></td>
<td>workbooks</td>
<td>Move flows or workbooks between projects. For more information, see Required access level for moving content.</td>
</tr>
<tr>
<td><img src="image6.png" alt="Icon" /></td>
<td>workbooks</td>
<td>Specify permissions for the content asset. Views in a workbook take permissions set at the workbook level.</td>
</tr>
<tr>
<td><img src="image7.png" alt="Icon" /></td>
<td>data sources</td>
<td>Connect to a published data source from Tableau</td>
</tr>
<tr>
<td>Permission</td>
<td>Applies to...</td>
<td>When allowed, users can...</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td><img src="image" alt="Commit" /></td>
<td>Desktop or the web editing environment.</td>
<td>See also: How data access is evaluated for workbooks that connect to Tableau data sources</td>
</tr>
<tr>
<td>Run Flow flows</td>
<td>Run a flow manually.</td>
<td></td>
</tr>
<tr>
<td><img src="image" alt="Commit" /></td>
<td>Set permissions for all content assets in a project, individual assets, or the project itself. Can lock project permissions, change content owner, move content, and run refresh schedules.</td>
<td>Full project leader capabilities are available only with some site roles. For more information, see Project-level administration.</td>
</tr>
</tbody>
</table>

How data access is evaluated for workbooks that connect to Tableau data sources

When a Tableau Desktop user publishes a workbook that connects to a data source published to the server (a Tableau data source), the user can set the data authentication type to **Embed password** or **Prompt users**. In this specific publishing case, data authentication refers to the workbook’s connection to the Tableau data source. This is independent of the authentication set in the published data source’s connections to the underlying data.

When a user subsequently opens the workbook on the server, the workbook-specific data authentication is evaluated along with the **Connect** capability, set in permissions rules. Whether the user can see the data in the workbook is determined as follows:

- When the workbook publisher selects the **Embedded password** option, they effectively embed their own **Connect** permissions, allowing anyone who can view the
workbook to see the data it connects to. How the viewer’s Connect capability is set on the data source does not affect this outcome.

- When the publisher selects the Prompt users option, viewers who are allowed the Connect capability are on the data source are prompted for their credentials. Users who are denied the Connect capability are denied access the data.

The following table summarizes the two bullet points above.

<table>
<thead>
<tr>
<th>Workbook</th>
<th>Data source authentication</th>
<th>Connect capability</th>
<th>Resulting access to data in the workbook</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded password</td>
<td>Embedded password or Prompt user</td>
<td>Allowed or Denied</td>
<td>Allowed through the workbook publisher’s Connect capability set on the data source</td>
</tr>
<tr>
<td>Prompt user</td>
<td>Embedded password</td>
<td>Allowed</td>
<td>Allowed through the viewer’s Connect capability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Denied</td>
<td>Denied</td>
</tr>
<tr>
<td>Prompt user</td>
<td>Allowed</td>
<td></td>
<td>Viewer is prompted for database credentials</td>
</tr>
<tr>
<td></td>
<td>Denied</td>
<td></td>
<td>Denied</td>
</tr>
</tbody>
</table>

See also

Permissions in Project Hierarchies—describes how permissions are applied in project hierarchies.

Manage Data
Tableau Server Data Sources

When your Tableau users want to share data connections they’ve defined, they can publish data sources to Tableau Server. When a data source is published to the server, other users can connect to it from their own workbooks, as they do other types of data. When the data in the Tableau data source is updated, all workbooks that connect to it pick up the changes.

Looking for Tableau Server on Windows? See Tableau Server Data Sources.

A Tableau Server data source consists of metadata that describes the following:

- **The connection information**: Defines whether the data is in a live database or an extract, and which of that data to bring in to Tableau.

- **Customization and cleanup**: Includes information that facilitates efficient use of the data. For example, calculations, sets, groups, bins, parameters, custom field formatting, and so on.

- **Data access and refresh instructions**: Includes the location of the underlying database server (whether on-premises or in the cloud), network paths for file-based data, security information such as credentials or access tokens, and related information.

In addition to helping your users create data consistency and reliability, using Tableau data sources offers advantages to you as the administrator. Because multiple workbooks can connect to one data source, you can minimize data source proliferation and save on storage space and processing time. When someone downloads a workbook that connects to a Tableau data source that in turn has an extract connection, the extract stays on the server, reducing network traffic. Finally, if a connection requires a database driver, you need to install and maintain the driver only on the server, instead of on each user’s computer. If you use Tableau Online, all supported drivers are available to data sources published to your site.
Managing data sources

You can perform some or all management tasks on a data source if you have one of the following levels of access:

- Site or server administrator
- Project leader or owner of the project the data source is published to
  
  Full project leader access is available only with some site roles. For information, see Project-level administration.
- Data source owner

Unless you’re a site or server administrator, you might not have access to all management tasks. For example, if the Permissions menu is not available, chances are that the project permissions are locked, which denies setting permissions on individual workbooks and data sources.

Tip: A best practice is to designate a person or team to manage all data sources published to a project or to the whole site, so that all data sources can be maintained under the same set of guidelines.

To perform the management tasks that you have access to, do the following:

1. Sign in to the site, and on the Content tab, select Explore > Data sources.

2. On a data source, select the Actions (…) menu.
- **New workbook or Download**: Create a new workbook in the browser environment that connects to this data source. Or download the data source to use locally.

- **Tag**: Add or remove keyword tags. Tags can contain a single word or multiple words, delimited by a comma.

- **Move**: Move a data source from one project to another. This requires specific settings on each project. For information, see Required access level for moving content.

- **Permissions**: View or update permissions that specify which users or groups can connect to, modify, or download the data source. As mentioned at the beginning of this section, if this action is not available, the project permissions might be locked, and only the project leader or administrator can change permissions.

- **Change owner**: Making someone an owner gives them complete access to it.

- **Refresh extracts**: If a data source includes an extract, you can assign the extract to a refresh schedule.

For information, see Refresh Data on a Schedule.
• **View the data source’s revision history**

• **Delete:** Deleting a data source affects workbooks that connect to the data source. Before you delete a data source, ensure that there are no workbooks that connect to the data source or edit the workbooks to use another data source.

In addition, for data sources that are proxy connections, administrators can stay aware of how users authenticate to the database, and whether the appropriate drivers are installed. For information, see Database Drivers and Data Security.

**Extract Upgrade to .hyper Format**

Beginning in version 10.5, new extracts use the .hyper format instead of the .tde format. Extracts in the .hyper format take advantage of an improved data engine, which supports the same fast analytical and query performance as the data engine before it, but for even larger extracts.

This article covers what you and your users should be aware of as a result of the extract format change in version 2019.1 and how the change impacts your users.

**Changes to extracts in version 10.5**

With the introduction of Tableau’s improved data engine technology, Hyper, comes a change to the extract format. As mentioned above, extracts created in version 2019.1 use the .hyper format. Though Tableau version 2019.1 can continue to read .tde extracts, it cannot create new .tde extracts. The impact of this format change means that when certain extract tasks are performed either by a user or by Tableau Server, such as an extract refresh or append data, the .tde extract is automatically upgraded and converted to a .hyper extract.

After an extract is upgraded to a .hyper extract, your users can interact with the .hyper extract as they would a .tde extract. However, your users should be aware of the following backward limitations:
The upgrade can't be reversed. An upgraded extract can't be converted back to a .tde extract.

The upgraded extract can't be opened in Tableau Desktop 10.4 and earlier.

Workbooks that contain upgraded extracts can't be published as an older version from Tableau Desktop to Tableau Server.

Workbooks that contain upgraded extracts can't be downgraded as an older version in Tableau Desktop.

Workbooks that contain an upgraded extract, which are downloaded from Tableau Server using the Download Tableau Workbook option, cannot be opened in Tableau Desktop 10.4 and earlier.

Tasks that cause extract upgrade

There are three distinct ways a .tde extract can get upgraded to a .hyper extract: 1.) during an extract refresh (full or incremental), 2.) when appending data to an extract, and 3.) when an extract is upgraded manually using Tableau Desktop 2019.1. After an extract has been upgraded, the original .tde extract is automatically removed from Tableau Server if it's not being reference by other workbooks.

The followings tasks on Tableau Server automatically upgrades and converts a .tde extract to a .hyper extract:

- Manual extract refresh
- Scheduled extract refresh
- Automated refresh task that's performed through tabcmd
- Automated refresh task that's performed through the Extract Command-Line Utility
- Automated append data to an extract using tabcmd
- Automated append data to an extract using the Extract Command-Line Utility
Impact of extract upgrade

Tableau recommends that the Tableau Desktop version in your environment be upgraded to match Tableau Server 2019.1. If they don't match, extract compatibility can be an issue depending on the task your users want to perform.

To get a better understanding of when extract upgrades can occur and potential compatibility issues your users might experience, review a detailed explanation of the extract compatibility scenarios on the Tableau Support page or a summary explanation below.

**Note:** In the tables below, "10.4" represents Tableau 10.4 and earlier and "10.5" represents Tableau 10.5 and later.

Performing tasks on Tableau Server 10.5

When working with extracts created in Tableau Desktop 10.4 and earlier, your users should be aware of the following extract-related compatibility scenarios around common tasks performed on Tableau Server 10.5.

<table>
<thead>
<tr>
<th>Task</th>
<th>10.4 workbook</th>
<th>10.5 workbook</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>.tde extract</td>
<td>.tde extract</td>
</tr>
<tr>
<td>Publish from Tableau Desktop 10.4</td>
<td>✓</td>
<td>Not possible</td>
</tr>
<tr>
<td>Publish from Tableau Desktop 10.5</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Refresh, scheduled refresh, or append</td>
<td>Workbook version remains unchanged, but extract upgrades to .hyper format</td>
<td>Workbook version remains unchanged, but extract upgrades to .hyper format</td>
</tr>
<tr>
<td>Edit/save in</td>
<td>Workbook version</td>
<td>✓</td>
</tr>
</tbody>
</table>
### Task 10.4 workbook 10.5 workbook

<table>
<thead>
<tr>
<th>Task</th>
<th>.tde extract</th>
<th>.tde extract</th>
<th>.hyper extract</th>
</tr>
</thead>
<tbody>
<tr>
<td>web authoring</td>
<td>changes to 10.5, extract remains in .tde format</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit/save in web authoring then refresh or append</td>
<td>Workbook version changes to 10.5, and extract upgrades to .hyper format</td>
<td>Workbook version remains unchanged, but extract upgrades to .hyper format</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Downloading from Tableau Server 10.5**

When working with extracts created in Tableau Desktop 10.4 and earlier, your users should be aware of the following extract-related compatibility scenarios when downloading from Tableau Server 10.5.

<table>
<thead>
<tr>
<th>Task</th>
<th>10.4 workbook</th>
<th>10.5 workbook</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download and open in Tableau Desktop 10.4</td>
<td>✓</td>
<td>Can't open workbook; you see a &quot;this workbook uses a .hyper extract and is not compatible with this version; open the workbook in version 10.5 or later&quot; error message, and then Can't open workbook; you see a &quot;this file was created by a newer version; upgrade Tableau&quot; error message</td>
</tr>
</tbody>
</table>
### Automating refresh and append tasks

When working with extracts created in Tableau Desktop 10.4 and earlier, your users should be aware of the following extract-related compatibility scenarios around automating refresh and append tasks using tabcmd or the Tableau Command-Line Utility.

<table>
<thead>
<tr>
<th>Task</th>
<th>10.4 workbook</th>
<th>10.5 workbook</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh or append</td>
<td>.tde extract</td>
<td>.tde extract</td>
</tr>
<tr>
<td>using 10.4 tabcmd</td>
<td>Workbook version remains unchanged, but extract upgrades to .hyper format</td>
<td>Workbook version remains unchanged, but extract upgrades to .hyper format</td>
</tr>
<tr>
<td>using 10.5 tabcmd</td>
<td>Workbook version remains unchanged, but</td>
<td>Workbook version remains unchanged, but</td>
</tr>
<tr>
<td></td>
<td>.tde extract</td>
<td>.hyper extract</td>
</tr>
<tr>
<td>Export As Version</td>
<td>.tde extract</td>
<td>.hyper extract</td>
</tr>
<tr>
<td>Task</td>
<td>10.4 workbook</td>
<td>10.5 workbook</td>
</tr>
<tr>
<td>------</td>
<td>---------------</td>
<td>---------------</td>
</tr>
<tr>
<td></td>
<td>.tde extract</td>
<td>.tde extract</td>
</tr>
<tr>
<td></td>
<td>extract upgrades to .hyper format</td>
<td>extract upgrades to .hyper format</td>
</tr>
<tr>
<td>Publish</td>
<td>using 10.4 tabcmd</td>
<td>√</td>
</tr>
<tr>
<td></td>
<td>using 10.5 tabcmd</td>
<td>Not possible</td>
</tr>
<tr>
<td>Refresh or append</td>
<td>using 10.4 Tableau Command-Line Utility</td>
<td>√</td>
</tr>
<tr>
<td></td>
<td>using 10.5 Tableau Command-Line Utility</td>
<td>Workbook version remains unchanged, but extract upgrades to .hyper format</td>
</tr>
</tbody>
</table>

**Why keep an extract in .tde format?**

If the version of Tableau Desktop cannot be upgraded to match Tableau Server 2019.1, your users will need to keep their extracts in .tde format.

**How to keep an extract in .tde format**

To keep an extract in the .tde format, the extract should not be upgraded. To help your users keep their extracts from upgrading, advise them against performing any of the tasks listed above in the Extract Upgrade to .hyper Format section. Then, consider the following suggestions to maintain a .tde version of an extract:
Tableau Server on Linux Administrator Guide

- Disable existing extract refresh schedules on Tableau Server until you can identify which extracts should and shouldn't be upgraded.

  **Note:** To access an extract's refresh schedule, you must be a data source owner, or be a server administrator, site administrator, or Project Leader. For more information about which site roles allow full Project Leader capabilities, see Project-level administration.

- Continue to perform extract refresh and append data tasks using Tableau Server 2019.1, but maintain an earlier version of Tableau Desktop and the ability to connect to the original data in case you need to recreate the .tde extract.

- Use an earlier version of Tableau Desktop to perform extract tasks, such as extract refresh or append data.

**What to expect after extract upgrade**

After an extract upgrade has taken place, your users should expect some additional changes when working with extracts in version 2019.1. For more information, see After an extract upgrade section in Tableau Help.

**View Data Source Attributes**

In the **Content** area of the Tableau Server web authoring environment, you can filter the view to show only data sources or connections and their attributes.

**View data sources by name**

To filter by data source name, under **Explore**, select **Data sources**.
Attributes in the data source name list include the following:

- **Type**—The icon next to the data source name indicates whether the data source is published as a live connection (☐), an extract connection (), or is embedded in a workbook ().
  
  - Select the name of a published data source to open its data source page, with tabs for viewing connections and workbooks that connect to it.
  
  - Select the name of an embedded data source to open the workbook associated with it, as well as tabs for viewing other data it connects to.

- **Connects To**—Indicates the name of the database server or data file. This could be a database outside of Tableau Server, an extract, or a published data source.

- **Live or Last Extract**—This column tells you whether the connection to the data is live, or, if it is a connection to an extract, when the extract was last updated.

**View a list of connections**

To filter by connection type, in the **View** list, select **Connections**.
Connection attributes include:

- **Connects to**—Indicates the name of the database server or data file. This could be a database outside of Tableau Server, an extract, or a published data source.

- **Connection type**—Shows the type of data. Tableau Server indicates that the connection is to a data source published on the site. Tableau Data Engine means the data source has an extract stored on the Tableau data server.

### Use Certification to Help Users Find Trusted Data

In a self-service environment with multiple publishers, it’s common for a project on Tableau Server to contain a variety of data sources that are named similarly, or are based on the same or similar underlying data, or are published without any descriptive information about them. When this is the case, analysts who create views in Tableau Desktop or web authoring can’t be confident knowing which data source is the right one to connect to.

To help your users find the data that’s trusted and recommended for their type of analysis, you can certify the data sources that comply with your organization’s data standards.

Certification complements the Recommendations Trainer feature, by offering a way to promote data sources through curation.

### How certification helps users find trusted data

When you certify a data source, its icon in the list view, or thumbnail in the grid view shows a green check mark. This appears anywhere the data source is shown, including when connecting to data in web authoring or from Tableau Desktop.
Certified data sources rank higher in search results and are added to recommended data sources.

In addition, you can provide notes about the certification status, which appear in a tooltip when users hover over the data source icon or card. The tooltip in list view also shows who certified the data source and the data source’s connection type.
For more information, see the Certify a data source steps below.

Create guidelines for selecting data sources to certify

As with most Tableau functionality, certification is flexible. You can define for your organization the criteria you use to determine when to certify a data source. As you do this, you might want to document and share your guidelines. As new data sources are published, the guidelines can help you and other administrators or project leaders to be consistent with your certification choices. They can also help users understand what certification means.

Whether you use the same certification criteria across all projects, or define unique criteria for each project, the important thing is to be clear about what certification means in your environment.

Who can certify data sources

To access data source certification, a user must have either of the following permissions levels on Tableau Server:

- Site Administrator site role.
- Creator site role with the Project Leader permissions role on the project that contains the data sources.
Certify a data source

1. Sign in to Tableau Server and under **Explore**, select **Data Sources**.

2. On the **Data Sources** page, select the data source to expose its information, and then select the **Details** tab.

3. Next to **Certification**, select **Edit Certification Status**, and then do the following:
   
   a. Select the **This data is certified** check box.
   
   b. Add a note that gives users context for the certification status, intended use for the data, or other helpful information.

   ![Certification Configuration](image)

   Information you add to the **Note** section appears in the certification badge tooltip, mentioned earlier in How certification helps users find trusted data.

Keep Data Fresh

Manage Refresh Tasks

Administrators can change the priority of scheduled extract refreshes relative to other server tasks, manually refresh extracts, or delete their schedules.

1. Sign in to the site that has the schedules you want to manage, and then click **Tasks**.

2. Select one or more scheduled extract refreshes.

3. From the **Actions** menu, do any of the following:
Select **Change Schedule**, and choose a new schedule from the list.

Select **Run Now** to refresh manually.

**Note:** If an extract does not have a scheduled refresh, you can refresh it on demand from the Data Connections page.

Select **Change Priority**, and enter a number between 1 and 100 to move the extract up or down in the priority list.

Select **Delete** to completely remove the schedule for the selected data sources.

See also

Enable Extract Refresh Scheduling and Failure Notification

**Refresh Data on a Schedule**

You can schedule refresh tasks for published extract data sources and published workbooks that connect to extracts.

**Note:** When a refresh is performed on extracts created in Tableau 10.4 and earlier (that is, a .tde extract), the extract is upgraded to .hyper extract automatically. While there are many benefits of upgrading to a .hyper extract, your users won't be able open the extract with earlier versions of Tableau Desktop. For more information, see Extract Upgrade to .hyper Format.

For information on how to refresh flow outputs, see Schedule a Flow Task.
1. When you're signed in to Tableau Server, go to Content > Data Sources or Content > Workbooks, depending on the type of content you want to refresh.

2. Select the check box for the data source or workbook you want to refresh, and then select Actions > Extract Refresh.

3. In the Refresh Extracts dialog, select Schedule a Refresh, and complete the following steps:

   - Select the schedule you want.

   - If available, specify whether you want a full or incremental refresh.

   By default, and if this option is not shown, a full refresh is performed. Incremental refresh is available only if you configured it in Tableau Desktop before publishing the extract. For information, see Refreshing Extracts in the Tableau Help.
Click the **Schedule Refresh** button.

**Note:** If you want to add a new schedule, you can do so on the **Schedules** page.

**Quick Start: Refresh Extracts on a Schedule**

For published workbooks that connect to data extracts, you can set up the server to refresh the extracts on a recurring schedule, so all workbooks connected to them always show the most up-to-date data.

To schedule refreshes you need to have administrator or data owner permissions.

**Note:** This topic applies to extracts published to Tableau Server. For Tableau Online, how you refresh extracts depends on the underlying data they connect to. For more information, see **Keep Data Fresh**.
1 Set up a schedule on the server

Sign in to the server, go to the Schedules page, and click New Schedule.

Tableau provides a few refresh schedules. You create additional schedules you need.

2 Enable scheduled extract refreshes and failure emails

As a server or site administrator, you can enable schedules, as well as email notification when extract refreshes fail.

Select Settings, and then go to the General page.

- Under Email Notification, select **Send email to data source and workbook owners when scheduled refreshes fail**.

- Under **Embedded Credentials**, select both check boxes to allow publishers to
3 Publish a workbook with an extract

In Tableau Desktop, select Server > Publish Workbook. Sign in to the server if you’re not already. In the Publish Workbook to Tableau Server dialog box, click Schedules & Authentication. Under Extract Schedule, select the schedule from the list.
If the original data requires authentication, you will also need to select how you want people to access it.

4 Monitor refresh performance

You can monitor scheduled tasks by viewing **Background Tasks for Extracts** on the **Status** page.
Automate Refresh Tasks

You can associate extract refresh tasks with schedules in Tableau Server to automate refreshing extracts. You can also automate extract refreshes using tabcmd, a command line utility that you can download for use with Tableau Server. In particular, you can use the `refreshextracts` command in combination with other commands in your own script. For example:

```
  tabcmd login -u http://mytabserver -u jsmith -p P@ssw0rd!
  refreshextracts --datasource salesq4
```

**Note:** When an extract refresh is performed on extracts created in Tableau 10.4 and earlier (that is, a .tde extract), the extract is upgraded to .hyper extract automatically. While there are many benefits of upgrading to a .hyper extract, your users won’t be able open the extract with earlier versions of Tableau Desktop. For more information, see Extract Upgrade to .hyper Format.

For information about downloading the tabcmd utility, see tabcmd.

Handle Extract Refresh Alerts

When Tableau Server cannot complete a scheduled refresh, an alert appears to indicate that the refresh has failed. If a scheduled refresh fails five consecutive times, Tableau Server suspends the refresh. When a refresh is suspended, Tableau Server does not try to run it again until someone takes an action that attempts to correct the cause of the failure.

**Note:** The number of consecutive failures for a refresh is set to five by default, but can be changed by a Tableau Server administrator, using the `backgrounder.failure_threshold_for_run_prevention` option. For more information, see tsm configuration set Options.
You will see the Alerts menu only if an extract refresh failed and you are:

- A system or site administrator
- The author of the workbook or data source that couldn't be refreshed
- The author of a workbook that connects to a data source that couldn't be refreshed

When you open the Alerts menu you can see more information about the refresh failure(s):

When a **Data source** is listed as **Embedded** it means that the data source definition (which includes things like the data source credentials or the database name) is embedded, or resides, within the workbook itself, originally created in Tableau Desktop.

When a data source name or workbook name is listed as the **Data source** (for example, **Data source: sales_data**), it means that the data source is a Tableau Server data source. The data source definition resides on Tableau Server.

In the Data pane on Tableau Desktop, you can determine whether the data source is on Tableau Server or is local. If the data source is on the server, a Tableau icon is displayed next to the data source name instead of a database icon:
Resolving Extract Refresh Problems

To resolve refresh issues, you can take any of these actions, based on the cause indicated in the alert:

- **Errors related to access token validation or user credentials**

  You can resolve some extract refresh problems by clicking the **Connection Details** in the alert. Select the check box next to the problematic data source, click **Actions > Edit Connection**, and then enter the missing information. Click **Save** when you're done. After you update the connection information, Tableau Server restarts the refresh schedule.

  If you originally embedded the credentials or other data connection information when you published the workbook or data source from Tableau Desktop, you can also republish the workbook or data source. As part of the publishing process, you can choose to set a new refresh schedule. If you don't choose a new schedule, Tableau Server restarts the existing schedule.

- **Errors that indicate the database was unreachable**

  Confirm that the database is online and that you can sign in to access the data. You can use the **Try again** link in the alert to restart the refresh schedule.

- **Errors when using user filters or impersonation**

  See the **Tableau Knowledge Base**.

  If the problem cannot be corrected by editing the data connection, you will need to resolve it in Tableau Desktop and republish the workbook.
Tip: Administrators can edit data connections at any time on the Data Connections page, accessible from each site by clicking the Content tab and Data Connections.

Edit Connections on Tableau Server

Administrators and data source owners can manage the information that describes how a published data source connects to the underlying data. This information includes the database server name or address, the server port, the database user name, and whether or not the password is embedded in the connection.

Note: Ability to edit connections is determined primarily by your site role, rather than by your permissions on the data source. To edit connections, your site role must be Server Administrator, Site Administrator, or Creator. If your site role is Creator, you also must be the data source owner.

1. Sign in to the site that has the data sources you want to modify, and on the Content tab, select Explore > Data sources.

2. Select the name of the data source with the connection you want to update.

   Display filters to search for the data source or narrow the scope of the data source list. The values you type into the Server name and Database username fields are treated as regular expressions.

3. In the Connections view, select the Actions (...) menu for the data source, and then select Edit Connection.
4. Update the connection information.

For **Server name**, if you want to use an IP address, make sure the database or its driver supports that type of connection. If it doesn’t, enter the database server name.

See also Authentication types for Google, Salesforce, and WDC data later in this topic.
5. Click **Save**.

6. Refresh the browser page for your changes to take effect.

**Authentication types for Google, Salesforce, and WDC data**

Google BigQuery, Google Analytics, Salesforce.com, and many web data connector (WDC) connections use the OAuth authentication standard, which uses secure access tokens instead of “raw” user name and password credentials. With OAuth, database credentials do not need to be stored in Tableau, and all users connect through this access token, including Tableau Desktop users who want to create or edit workbooks that connect to the data source.

The following sections describe Google and Salesforce connection options. Web data connector options vary, but all involve signing in through the provider’s web-based sign-in form to establish the access token.
Google authentication options

When you edit Google BigQuery or Google Analytics connections, select either of the following options in the Edit Connection dialog box:

- Select **Embed Google BigQuery (or Google Analytics) credentials in the connection** to authenticate through a designated account, and then select an existing account from the list or select **authenticate account now...** to add a new one.

  When you add a new account, the Google sign-in page appears. After you provide your database credentials, Google prompts you to confirm Tableau access to the data. When you click **Accept**, Google returns an access token to use for connecting to the data.

  **Note**: If you create extracts of your Google data source, select this first option, so that you can schedule refresh tasks.

- Select **Prompt user for Google BigQuery/Analytics credentials** to require users to connect through their own individual access tokens or sign in each time they connect.

Salesforce.com authentication options

When you edit Salesforce.com connections, you can select any of the following options in the Edit Connection dialog box:

- Select **Embed a Salesforce username and password** to use a traditional authentication method.

- Select **Embed Salesforce credentials in the connection** to use an OAuth connection and schedule refresh tasks, and then select an existing account from the list or click **Add a Salesforce Account** to add a new one.
When you add a new account, the Salesforce.com sign-in page appears. After you provide your database credentials, Salesforce.com prompts you to confirm Tableau access to the data. When you allow Tableau access, Salesforce.com creates an access token through which it connects to the data.

- Select **No Salesforce authentication** to require users to sign in to Salesforce.com each time they connect. (This option does not allow scheduled extract refreshes.)

**Monitor progress**

When you save your changes in the **Edit Connection** dialog box, the dialog displays the progress. If you close the dialog box, the modifications continue to run in the background until completed. Tableau Server will make as many changes as possible. Any failures will be skipped, but they will not impede other changes. For example, if you try to change the server name and add a password to several connections, the server names will be
changed, and the passwords on workbooks will be changed. However, because you cannot
add a password to a data source, the passwords for the data sources will not be changed.

For information about checking the progress of these tasks, see Background Tasks for
Extracts.

Cube Data Sources

Cube (multidimensional) data sources have certain characteristics that make them unique in
Tableau.

Cube data sources do not support pass-through connections. This means that when a cube
data source is published, you cannot make a connection from Tableau Server using the data
source. It also means you cannot create a workbook using the data source in Tableau
Server.

Publishing a cube data source to Tableau Server gives you the ability to store the data
source on the server. However, to use the data source, you must download the data source
to Tableau Desktop and use it locally. To download a published data source you need:

- The **Download/Web Save As** permission for the data source. For more information,
  see Set Permissions on Individual Content Resources.
- Correct drivers installed and ports opened on computer running Tableau Desktop.

Web Data Connectors in Tableau Server

Web data connectors (WDCs) are web pages that provide a data connection that is access-
able over HTTP for data sources that don’t already have a connector in Tableau. WDCs allow
users to connect to almost any data that is accessible over the web and to create extracts for
their workbooks. Data sources for a WDC can include internal web services, JSON data,
REST APIs, and other sources that are available over HTTP or HTTPS. Users can create
their own WDC or use connectors that were created by others.
For information about how to use a WDC in Tableau Desktop, see Web Data Connector in the Tableau Desktop documentation.

For information about how to create a WDC, see the Web Data Connector documentation on Github.

**Before you run connectors on Tableau Server**

As a security measure, Tableau Server won't run WDCs unless you approve the connector, as explained in this topic.

>Note: You must be a server administrator to approve WDCs for use on Tableau Server.

WDCs require your approval because they contain executable code and typically make requests to third-party websites. Before a user can use a WDC with Tableau Server, you must either add the domain and port used by the connector to a safe list (whitelist) and also include the domains that a connector can send requests to and receive requests from on a secondary safe list (secondary whitelist). Before you do this, we recommend that you vet and test the connector so that you know what the connector does and what sites it connects to. For more information, see Testing and Vetting Web Data Connectors.

When you add a connector to the safe lists (whitelists), you configure Tableau Server to allow connections to a particular URL where the connector is hosted and from a URL which the connector can query. This is the only way to allow Tableau Server to run WDCs. The connectors can then be hosted on a server inside your organization’s firewall or on an external domain. Importing WDCs is not supported for Tableau Server.

**Manage connectors in a safe list**

To add a WDC to the safe list, use the `tsm data-access web-data-connectors add` command. This command and the related commands described below let you perform the following tasks:
Tableau Server on Linux Administrator Guide

- Add WDCs to the safe list and secondary safe list.
- Allow or disallow all WDCs, or WDC refreshes.
- Remove one or more connectors from the safe list.
- List all WDCs on the safe list and secondary safe list.

Updating WDC safe lists requires a server restart

After running any commands that make changes to WDCs, you need to apply your pending changes using the `tsm pending-changes apply` command.

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

Add connectors to the safe list and secondary safe list

To add a connector to the safe list and secondary safe list, use the `tsm data-access web-data-connectors add` command, providing the name, safe list URL, and secondary safe list URLs. You can also manage WDCs using the `web-data-connector-settings` Entity. After running this command, you need to apply your pending changes using the `tsm pending-changes apply` command.

```
```

**Notes on formatting:**

- Be sure to use straight quotes (" and "), not curly or "smart" quotes, around the name of the WDC.
For many WDCs, the port specified for the --url option is 443 or 80, but you can check the value for your connector by looking at the data source details on Tableau Server.

If a WDCs send requests to and receive data from multiple domains, use a comma-delimited list of URL for the --secondary option.

To add an entire domain to the secondary safe list, end the domain URL with a wildcard expression. Use (.* ) as the wildcard to indicate the entire domain. Be sure to include the parentheses () as part of the expression.

Allow or disallow WDCs or WDC extract refreshes

To allow or disallow WDCs, or WDC extract refreshes, use the following command before running tsm pending-changes apply:

```bash
tsm data-access web-data-connectors allow
```

Remove one or more WDCs from the safe list

To remove one or more WDCs from the safe list, use the following command before running tsm pending-changes apply:

```bash
tsm data-access web-data-connectors delete
```

List all WDCs on the safe list

To list all WDCs on the safe list, use the following command:

```bash
tsm data-access web-data-connectors list
```

Refresh the extract for a connector

When a user creates a workbook that uses a WDC, Tableau Server creates an extract from the data returned by the connector. If the user then publishes the workbook, the publish process sends the workbook and the data extract to the server.

Tableau can refresh an extract that was created by a WDC, the same as it can refresh any extract. If the connector requires credentials to sign in to the web-based data source, you need to ensure that the credentials are embedded with the data source, and that the WDC
Tableau Server on Linux Administrator Guide

is on the safe list for the server. Tableau Server cannot refresh the extract if the connector requires credentials and they are not embedded with the data source. This is because the refresh can occur on a schedule or in some other background context, and the server cannot prompt for credentials.

Currently, there is no way to re-authenticate a data source from Tableau Server directly. If the data source has credentials that expire, or was published without embedding the credentials, the workbook and data extract need to be published again with the new embedded credentials.

If the background process that performs the refresh operation fails, it creates an alert and a log entry that indicates this issue. Users will be able to see that the timestamp on the extract does not change.

To disable refresh for all WDCs, use the `tsm data-access web-data-connectors allow -r false` command.

Troubleshooting

If the server experiences problems with adding connectors to the safe list, you can examine the log files. Be sure to check the log files on both the initial server node and on the other nodes that are running the gateway process. For more information about log files, Server Log File Locations.

If the issue is that Tableau Server will not refresh an extract that was created by a WDC, make sure that the `webdataconnector.refresh.enabled` configuration setting has been set to `true`. If it is set to `false`, run the following command to allow extract refreshes for all WDCs on the server:

`tsm data-access web-data-connectors allow -r true`

**Note:** The safe list is the only way of allowing Tableau Server to run web data connectors. Importing web data connectors was deprecated starting with version 10.5.
Testing and Vetting Web Data Connectors

Web Data Connectors (WDCs) contain JavaScript that typically connects to data on another site. Because of this, you should test and vet web data connectors before users use them as data sources for a workbook, and before you use them with Tableau Server.

This topic includes some suggestions for testing and vetting web data connectors.

Examine the source

The code in a web data connector is in JavaScript, so you can open the file (and any external files that the connector uses) and examine the source code.

Many connectors reference external JavaScript libraries, such as the jQuery library or API libraries for third parties. Validate that the URL for external libraries points to a trusted location for the library. For example, if the connector references the jQuery library, make sure that the library is on a site that is considered standard and safe. If it is practical for you to change the source code of the connector, use HTTPS protocol (https://) to reference external libraries (if the source site supports HTTPS) to help verify the site’s authenticity.

To the extent possible, make sure you understand what the code is doing. In particular, try to understand how the code is constructing requests to external sites, and what information is being sent in the request.

Note: Experienced JavaScript programmers often compress (minify) their code to reduce the size of the code for download. Dense blocks of code that use cryptic function and variable names are not uncommon. While this can make it more difficult to examine the code, it is not a sign that the code was written to be deliberately difficult to understand.

Test the web data connector in an isolated environment

If possible, test the web data connector in an environment that is isolated from your production environment and from user computers. For example, add a web data connector to a
safe list on a test computer or virtual machine that's running a version of Tableau Server that is not used for production.

Monitor the traffic created by the web data connector

When you test a web data connector, use a tool like Fiddler, Charles HTTP proxy, or Wireshark to examine the requests and responses that the connector makes. Make sure that you understand what sites the connector makes requests to and what content the connector is requesting. Similarly, examine the responses and their content to be sure that the connector is not reading data or code that is not directly related to the connector’s purpose.

Test the performance and resource usage of the web data connector

When you test a web data connector, use tools to monitor its CPU and memory usage. Remember that the web data connector will run on Tableau Server, which is an environment in which many processes are already running. You want to make sure that when the connector fetches data, the connector does not have an undue impact on server performance.

Check whether the connector writes to disk. If it does, check how much disk space it occupies, and examine the output to make sure you understand what it's writing and why.

Creators: Connect to data on the web

Before you can create a new workbook and build a view on the web to analyze your data on the web, you need to connect to your data. Tableau supports connecting to data sources on the web published through Tableau Desktop, or, connecting to data directly through Tableau Online or Tableau Server.

**Note:** Data connections created in Tableau Online or Tableau Server are **live connections** only. If you need to use an extract for web authoring, you can publish your data source through Tableau Desktop. To publish through Tableau Desktop, see Publish Data Sources and Workbooks.

To create a new workbook, sign into Tableau Online or Tableau Server.
In the Content tab, do either of the following:

- Go to the Projects section, select a project, and select New Workbook.
- Go to the Workbooks section and select New Workbook.

A Connect to Data window opens, which contains several tabs: Files, Connectors, On this Site, and, if you’re connected to Tableau Online, Dashboard Starters.

As a Creator, you can create a new workbook or add a new data source to an existing workbook in several ways:

- Upload Excel or text-based data from the Files tab
- Connect to server or cloud data with Connectors
- Connect to published data sources with On This Site
- On Tableau Online, quickly author and analyze data from Oracle Eloqua, Salesforce, ServiceNow ITSM, and QuickBooks Online from the Dashboard Starters tab
Connect to Files

Tableau supports uploading Excel or text-based data sources (.xlsx, .csv, .tsv) directly in your browser. In the Files tab of the Connect to Data window, connect to an Excel or text file by dragging and dropping it into the field or clicking "Upload from computer."

When Tableau successfully connects to your data, the Data Source page opens so that you can prepare the data for analysis and begin building your view. To learn more, see Creators: Prepare Data on the Web.

Use connectors

From the Connectors tab, you can connect to data housed in a cloud database or on a server in your enterprise. You need to supply connection information for each data connection that you make. For example, for most data connections, you need to supply a server name and your sign-in information. Supported connectors for Tableau Online and Tableau Server are:

**Tableau Online connectors:**

- Amazon Aurora
- Amazon RedShift
- Box
- Denodo
- Dropbox
- Exasol
- Google BigQuery
- Google Cloud SQL
- Google Drive
- MemSQL
- Microsoft Azure SQL Data Warehouse
- Microsoft SQL Server

**Tableau Server connectors:**

- OneDrive
- Oracle
- PostgreSQL
- Snowflake
- Tableau Data Server (single connections)
- Vertica
| Supported Connectors has information on how to connect Tableau to each of these connector types to set up your data source. If the connector you need doesn’t appear in the Connectors tab, you can connect to data through Tableau Desktop and publish your data source to Tableau Online or Tableau Server for web authoring. Learn more about how to Publish a Data Source in Tableau Desktop. When Tableau successfully connects to your data, the Data Source page opens so that you can prepare the data for analysis and begin building your view. To learn more, see Creators: Prepare Data on the Web. |
**Note:** If you’re unable to connect to your data from Tableau Online, check to see if the database is publicly accessible. Tableau Online can only connect to data that's accessible from the public internet. If your data is behind a private network, you can connect using Tableau Bridge. To learn more, see Publishers: Use Tableau Bridge to Keep Tableau Online Data Fresh.

**Connect to published data sources "On this Site"**

Tableau supports connecting to published data saved to your site with the **On this Site** tab. If you or another user has saved a data source or published to the web through Tableau Desktop, it will appear in Tableau Online or Tableau Server as a published data source.

When Tableau successfully connects to your data, the Data Source page opens so that you can prepare the data for analysis and begin building your view. To learn more, see Creators: Prepare Data on the Web.

**Dashboard Starters**

Dashboard Starters help you quickly author and analyze data from cloud-based systems like Salesforce, ServiceNow ITSM, Oracle Eloqua, and Marketo. Simply create a new workbook and choose from several beautiful, informative designs that are tailor-made for key business metrics. For more information, see Dashboard Starters for Cloud-based Data Sources.

**Keeping data fresh in web authoring**

**Update uploaded files in Tableau Online or Tableau Server:** If you manually upload a file (Excel or text) for web authoring, Tableau can’t refresh the file automatically. To update your data, select “Edit Connection” to upload a new version of the file.

**Update file-based published data sources in Tableau Online:** If you have a published data source in Tableau Online (published through Tableau Desktop) that uses file-based data, you can keep it fresh using Tableau Bridge. For more information, see Expand Data Freshness Options by Using Tableau Bridge.
Run Initial SQL

When connecting to some databases, you can specify an initial SQL command that will run when a connection is made to the database, for example, when you open the workbook, refresh an extract, sign in to Tableau Server, or publish to Tableau Server. Initial SQL is not run when your refresh your view. Note that this initial SQL is different than a custom SQL connection. A custom SQL connection defines a relation (or table) to issue queries against. For more information, see Connect to a Custom SQL Query.

You can use this command to:

- Set up temporary tables to use during the session.
- Set up a custom data environment.

You have the option to add an initial SQL command in the Server Connection dialog box or on the Data Source page.

**Note:** If your data source supports running an initial SQL statement, an **Initial SQL** link appears in the lower-left corner of the Server Connection dialog box. For information about your data source, see Supported Connectors.

To use initial SQL

1. In the Server Connection dialog box, click **Initial SQL**. Or, on the Data Source page, select **Data > Initial SQL** or **Data > Query Banding and Initial SQL** depending on the database you connect to.

2. Enter the SQL command into the Initial SQL dialog box. You can use the **Insert** drop-
down menu to pass parameters to your data source.

![Initial SQL dialog box]

**Note:** Tableau does not examine the statement for errors. This SQL statement is simply sent to the database when you connect.

Your software license may restrict you from using initial SQL with your connection. If you publish to Tableau Server, the server must be configured to allow Initial SQL statements. By default, the server software is configured to allow these statements to run when the workbook is loaded in a web browser.

Administrators can configure server to ignore initial SQL statements by using the `tsm configuration set` command:

```
 tsm configuration set -k vizqlserver.initialsql.disabled -v true
```

If the server doesn’t allow initial SQL statements, the workbook opens, but the initial SQL commands are not sent.

For more information about the `tsm configuration set` command, see the Tableau Server Help.
Parameters in an initial SQL statement

You can pass parameters to your data source in an initial SQL statement. There are several reasons why this is useful:

- You can configure impersonation using the `TableauServerUser` or `TableauServerUserFull` parameters.

- If your data source supports it, you can set up row-level security (for example, for Oracle VPD or SAP Sybase ASE) to make sure that users see only the data that they are authorized to see.

- You can provide more details in logging, for example, the Tableau version or the workbook name.

The following parameters are supported in an initial SQL statement:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example of returned value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TableauServerUser</td>
<td>The user name of the current server user. Use when setting up impersonation on the server. Returns an empty string if the user is not signed in to Tableau Server.</td>
<td>asmith</td>
</tr>
<tr>
<td>TableauServerUserFull</td>
<td>The user name and domain of the current server user. Use when setting up impersonation on the server. Returns an empty string if the user is not signed in to Tableau Server.</td>
<td>domain.lan\asmith</td>
</tr>
<tr>
<td>TableauApp</td>
<td>The name of the Tableau application.</td>
<td>Tableau Desktop Professional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tableau Server</td>
</tr>
<tr>
<td>TableauVersion</td>
<td>The version of the Tableau application.</td>
<td>9.3</td>
</tr>
</tbody>
</table>
WorkbookName | The name of the Tableau workbook. Use only in workbooks with an embedded data source. | Financial-Analysis

Examples

The following examples show different ways you can use parameters in an initial SQL statement.

- This example sets the security context on Microsoft SQL Server:

  ```sql
  EXECUTE AS USER = [TableauServerUser] WITH NO REVERT;
  ```

- This example shows how, on a DataStax data source, you can use parameters to add detail to logging or to set up a session variable to keep track of the data:

  ```sql
  SET TABLEAUVersions [TableauVersion];
  ```

- This example can be used to help set up row-level security for Oracle VPD:

  ```sql
  begin
  
  DBMS_SESSION.SET_IDENTIFIER([TableauServerUser]);
  
  end;
  ```

  **Note:** Oracle PL/SQL blocks require a trailing semicolon to terminate the block. Consult Oracle documentation for the proper syntax.

Defer execution to the server

You can defer an initial SQL statement so that it is executed only on the server. One reason to defer execution to the server is if you don’t have permission to execute the commands that set up impersonation. Use `<ServerOnly>` </ServerOnly> tags to enclose the commands to be executed only on the server.

Example:
CREATE TEMP TABLE TempTable(x varchar(25))
INSERT INTO TempTable VALUES (1);
<ServerOnly>INSERT INTO TempTable Values(2);</ServerOnly>

Security and impersonation

If you use the `TableauServerUser` or `TableauServerUserFull` parameter in an initial SQL statement, you will create a dedicated connection that can’t be shared with other users. This will also restrict cache sharing, which can enhance security, but may also slow performance.

Create, Interact with, and Embed Views on the Web

You can create and interact with views on Tableau Server. For more information, see the following topics in the Tableau Help for users.

Using Tableau on the Web

Tour your Tableau Site

Edit Views on the Web

Create a Dashboard

Create a Story

Embed Views and Dashboards in Web Pages

Make Workbooks Compatible Between Versions

Alerts and subscriptions

Troubleshoot Subscriptions

Send Data-Driven Alerts from Tableau Online or Tableau Server
Automatically Build Views with Ask Data

Ask Data introduces an entirely new way to interact with your data, letting you type a question and instantly get a response right in Tableau. Answers come in the form of automatic data visualizations, with no need to manually drag-and-drop fields or understand the nuances of your data’s structure.

Ask Data lets you ask sophisticated questions naturally, with support for key analytical concepts like time series and spatial analysis, and an understanding of conversational phrases like “last year”, “earliest”, and “most popular”.

Ask Data is available for all user roles with direct access to data sources: Creators, Explorers, and Interactors.

Note: Ask Data requires English analytical phrases but works great with non-English data. For example, you could ask “how many pedidos of manzanas” (how many orders of apples) if you have Spanish data with a field named “pedidos” and a value of “manzanas”.

Ask Data to quickly build a viz

1. In Tableau Server or Tableau Online, navigate to a data source, and then click Ask Data at left.
2. In the text box reading “Ask about fields in this data source”, enter terms from the data source fields at left.

Hover over each field to learn more about the data it contains. Unlike the data fields seen in standard Tableau views, these fields can't be dragged to the canvas.

3. As you type, Ask Data automatically completes your entry using likely combinations of data fields and analytical functions. To automatically create a viz, either press **Enter**, or choose from suggested entries below the text box.

Just like that, you've created a compelling visualization of your data!
Change the viz type

If the default viz doesn’t fully reveal your data, either click the menu at upper right, or specify a viz type at the end of your entry with phrasing like “as a bar chart”.

Here are all the supported viz types:

- Bar
- Gantt Bar
- Histogram
- Line
- Map
- Pie
- Scatter
- Text
- Treemap
Note: To automatically create certain viz types, Ask Data sometimes adds fields like “Number of Records” to your entries.

Customize fields and their data

Ask Data gives you several ways to fine-tune how field values are displayed.

- To switch the fields used for the vertical and horizontal axes, click the Swap Axes button above the text box.

- To change a field or its aggregation type (for example, from sum to average), click the field name in the text box.

- If a field is used as a filter, click the name to specify values or wildcard parameters.
To adjust a numeric range, click words like “high”, “between”, or “cheap” in the text box.

To delete a field, hover over it and click the X.
Save the viz in a new workbook

Save vizzes from Ask Data to combine them with other Tableau views and dashboards in a workbook. In a workbook, Ask Data is unavailable, but you gain access to Tableau’s full range of data analysis and visualization tools.

1. Above the viz, click the save icon, and choose Save as if you’re saving the viz for the first time, or Save to overwrite a previously saved version.

2. If you chose Save as, select Embed password for data source if people who lack access will be viewing the viz.

Tip: To quickly navigate to the workbook, click the save icon again, and choose Edit workbook.

Add synonyms for field names

People may not use the same terminology found in your data source, so Ask Data lets you add synonyms for specific data fields. Synonyms you enter are available throughout your organization, making data analysis quicker and easier for everyone. (Be careful about deleting synonyms that other people may be using.)

1. Hover over a data source field at left, click the down arrow, and choose Edit synonyms.

2. Enter synonyms for the field name, separated by commas.

Be aware that you can't use synonyms that reflect standard analytical terms like “by” or “max”. Likewise, you can't create synonyms for these special types of data: sets, bins, clusters, hierarchies, combined fields, table calculations, or latitude and longitude.
Tips for success

Use keywords

For example, instead of “I want to see all the countries that these airports are in”, try “by airport and country”.

Use exact wording for attributes and values when possible

For example, if your data source includes Airport Code, Airport Name, and Airport Region fields, specify those by name.

See a ranked list

Ask Data maps terms like “best” and “worst” to Top 1 and Bottom 1, respectively. If you want to see broader rankings, use “high” and “low” instead. For example, enter “houses with low sale prices”.

Surround unusually long values with quotation marks

If you want to analyze long field values that contain more than 50 characters or two separate words, or that include line returns or tabs, surround them with quotation marks. To improve performance, Ask Data doesn't index fields of that length.

Subscribe to Views

Subscriptions email you a snapshot of a view at regular intervals—without requiring you to sign in to Tableau Server or Tableau Online.

Note: In Tableau Server, administrators determine whether subscriptions are enabled for a site.

Subscribe yourself or others to a view

When you open a view in Tableau Server or Tableau Online, if you see a subscription icon ( constexpr ) in the toolbar, you can subscribe to that view or the entire workbook. If you own a
workbook, if you are a project leader with an appropriate site role, or if you are an administrator, you can also subscribe other users who have permission to view the content.

1. In a site, select All Workbooks or All Views, or open the project that contains the view you want to subscribe to.

![Explore](image)

2. Open a view either directly, or after opening the containing workbook.

3. In the toolbar above the view, click Subscribe.

4. Add the Tableau users or groups you want to receive the subscription. To receive a subscription, users must have the View and Download Image/PDF permissions. If they use Tableau Server, their accounts must also have email addresses.

**Note:** When you subscribe a group, each user is added individually at the time the subscription is created. If more users are added to the group later, you must
re-subscribe the group for those new users to receive the subscription. Likewise, users later removed from the group will not have their subscriptions removed automatically unless their permissions to the subscribed view are removed.

5. Choose whether subscription emails include the current view or the entire workbook.

6. Pick a schedule:

   • For Tableau Server, choose from subscription schedules established by your administrator.

   • For Tableau Online and Tableau Server with custom schedules enabled, click the drop-down arrow to the right of the current settings.

   5 days a week, at 08:00

Then specify a custom schedule that sends subscription emails whenever you wish. (The precise delivery time may vary if server load is high.)
To change the time zone, click the Time Zone link it to go to your account settings page.

7. To clarify subscription emails, customize the subject line, and add a message.

8. If the view contains data only when high-priority information exists, select **Don't send if view is empty**.

9. If you own the workbook, select **Subscribe me**.

10. Click **Subscribe**.

When you receive the email on the subscription schedule, click the image to open the view in Tableau Server or Tableau Online.

**Unsubscribe yourself from a view**

1. Access your Tableau Server or Tableau Online account settings by doing one of the following:
Click **Manage my subscriptions** at the bottom of a subscription email.

Sign in to Tableau Server or Tableau Online. At the top of the page, select your name, and then select **My Content**.

2. Click **Subscriptions**.
3. Select the check box next to the view you want to unsubscribe from, click Actions, and then click Unsubscribe.

Resume or delete suspended subscriptions

If a subscription fails more than five times, you'll receive a notification email that your subscription has been suspended. There are a few ways to resume a suspended subscription if you’re a subscription owner or administrator:

- From the My Content area of Tableau web pages, an icon appears in the Last update column to indicate that the subscription is suspended. Select ... > Resume Subscription to resume.

- From the Subscriptions tab of the affected workbook, an icon appears in the last update column to indicate that the subscription is suspended. Select ... > Resume Subscription to resume.

You'll receive an email notification when the subscription is working again.

See also

Change Subscription Settings in the Tableau Desktop and Web Authoring Help.

Project-level administration in the Tableau Online Help, to learn which site roles allow full Project Leader capabilities.

Use Dashboard Extensions

Extensions let you add unique features to dashboards or directly integrate them with applications outside Tableau. Adding extensions is easy; you incorporate them into dashboard layouts just like other dashboard objects.

Extensions expand dashboard functionality with the help of web applications created by third-party developers. If you're a developer and want to create your own extensions, see the Tableau Extensions API documentation on GitHub.
**Note:** Tableau administrators can turn off dashboard extensions for **Tableau Desktop**, **Tableau Server**, and **Tableau Online**.

The animation below shows an example extension. With other extensions, you'll see different options.

Click the image to replay the animation.

### Add an extension to a dashboard

To add an extension, you first need to download the related `.trex` file, which specifies the extension's properties, including the URL for the web-based application.

1. In a Tableau workbook, open a dashboard sheet.
2. From the **Objects** section, drag **Extension** to the dashboard.
3. In the “Choose an Extension” dialog box, do either of the following:

- Click My Extensions, and navigate to a .trex file you previously downloaded.

- Click Extension Gallery, and download a new extension. Then click My Extensions, and navigate to the downloaded .trex file.

4. If prompted, allow or deny the dashboard extension access to data in the workbook. For more information, see Data security and dashboard extensions.

   If you allow access, follow any on screen instructions for configuring the extension.

   **Note:** Extension objects will appear blank in prints, PDFs, and images of dashboards (including images in subscription emails).

Configure a dashboard extension

Some dashboard extensions provide configuration options that let you customize features.

1. Select the extension in the dashboard, and from the drop-down menu in the upper-right corner, choose Configure.
2. Follow the on-screen instructions to configure the extension.

Reload a dashboard extension

If a dashboard extension becomes unresponsive, you might need to reload it, which is similar to refreshing a web page in a browser.

1. Select the extension in the dashboard, and from the drop-down menu in the upper-right corner, choose **Reload**.

   The dashboard extension is refreshed and set to its original state.

2. If reloading the extension fails to return it to a useable state, try removing it from the dashboard and adding it again.

Ensure that extensions run on Tableau Online or Tableau Server

You can add extensions to workbooks you publish from Tableau Desktop or directly in the web-authoring mode of Tableau Online and Tableau Server. A Tableau administrator must allow extensions to run on a site and add extensions that access full underlying data to a safe list. Administrators should only allow extensions that you have tested and trust.

If you want to use a dashboard extension on Tableau Online or Tableau Server, direct your administrator to **Manage Dashboard Extensions in Tableau Online** or **Manage Dashboard Extensions in Tableau Server**.
Data security and dashboard extensions

Dashboard extensions are web applications, which can be running on web servers located outside of your local network. Before adding an extension or viewing a dashboard with one, be certain that you trust the website that hosts it. By default, dashboard extensions use the HTTPS protocol, which guarantees an encrypted channel for sending and receiving data, and ensures some privacy and security.

Allow or deny data access to an extension

Depending on how an extension is designed, it can access either visible data in a view, or full underlying data, table and field names from data sources, and information about data source connections. When you add an extension, or view a dashboard with one, you’re given an opportunity to allow or deny the extension to run and access this data.

If you’re viewing a dashboard with an extension that requires full data access, and that access has been denied, a message appears in place of the extension. If you trust the extension and want to use it, you can reset permissions and allow the extension to run.

1. Select the extension in the dashboard, and from the drop-down menu in the upper-right corner, choose Reset Permissions.
2. Click either Allow to let the extension run and access data, or Deny to prevent the extension from running.

Enable JavaScript

Dashboard extensions interact with data using the Tableau Extensions API library, a JavaScript library. If you want to use extensions, be sure that JavaScript is enabled in the dashboard security settings: Choose Help > Settings and Performance > Set Dashboard Web View Security > Enable JavaScript.

Get support for dashboard extensions

To get help for an extension, you'll need to contact the developer or company who created it.

1. Select the extension in the dashboard, and from the drop-down menu in the upper-right corner, choose About.

2. Click Get Support to go to the support page of the extension developer.

Tableau doesn't provide support for extensions or for other programs that interface with the Extensions API. However, you can submit questions and ask for help in the Tableau developer community.
Manage Server

Security ................................................................. 640
Preparing for Configuring OAuth Support .......................... 764
Configure Settings for Your Data Provider ....................... 764
Obtain a Client ID and Enable Google APIs ....................... 765
Configure Tableau Server for Google OAuth ....................... 767
Create and edit Google data source ............................... 768
Managing access tokens ........................................... 768
Create a Connected Salesforce App ................................. 769
Configure Tableau Server for Salesforce.com OAuth ............ 771
Managing access tokens ........................................... 771
Create a Connected Intuit App ..................................... 772
Configure Tableau Server for QuickBooks Online ................ 773
Managing access tokens ........................................... 773
Managing credentials centrally .................................... 775
See also ............................................................. 775
Manage Licenses .................................................... 852
Add Users to Tableau Server ...................................... 880
Sign in to the Tableau Server Admin Area ....................... 884
Sign in to Tableau Services Manager Web UI .................... 889
Security

Authentication

Authentication verifies a user’s identity. Everyone who needs to access Tableau Server—whether to manage the server, or to publish, browse, or administer content—must be represented as a user in the Tableau Server repository. The method of authentication may be performed by Tableau Server (“local authentication”), or authentication may be performed by an external process. In the latter case, you must configure Tableau Server for external authentication technologies such as Kerberos, SSPI, SAML, or OpenID. In all cases, whether authentication takes place locally or is external, each user identity must be represented in the Tableau Server repository. The repository manages authorization metadata for user identities.
Although all user identities are ultimately represented and stored in the Tableau Server repository, you must manage user accounts for Tableau Server in an identity store. There are two, mutually exclusive, identity store options: LDAP and local. Tableau Server supports arbitrary LDAP directories, but it’s been optimized for Active Directory LDAP implementation. Alternatively, if you are not running an LDAP directory, you can use the Tableau Server local identity store. For more information see Identity Store.

As shown in the following table, the type of identity store you implement, in part, will determine your authentication options.

<table>
<thead>
<tr>
<th>Identity Store</th>
<th>Authentication Mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Basic</td>
</tr>
<tr>
<td>Local</td>
<td>X</td>
</tr>
<tr>
<td>Active Directory</td>
<td>X</td>
</tr>
<tr>
<td>LDAP</td>
<td>X</td>
</tr>
</tbody>
</table>

Access and management permissions are implemented through site roles. Site roles define which users are administrators, and which users are content consumers and publishers on the server. For more information about administrators, site roles, groups, Guest User, and user-related administrative tasks, see Users and Site Roles for Users.
Note: In the context of authentication, it's important to understand that users are not authorized to access external data sources through Tableau Server by virtue of having an account on the server. In other words, in the default configuration, Tableau Server does not act as a proxy to external data sources. Such access requires additional configuration of the data source on Tableau Server or authentication at the data source when the user connects from Tableau Desktop.

Client authentication compatibility

<table>
<thead>
<tr>
<th>Clients</th>
<th>Authentication Mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Baseline</td>
</tr>
<tr>
<td>Tableau Desktop</td>
<td>X</td>
</tr>
<tr>
<td>Tableau Prep</td>
<td>X</td>
</tr>
<tr>
<td>Tableau Mobile</td>
<td>X</td>
</tr>
<tr>
<td>Tabcmd</td>
<td>X</td>
</tr>
<tr>
<td>Web Browser-</td>
<td>X</td>
</tr>
</tbody>
</table>
Local authentication

If the server is configured to use local authentication, then Tableau Server authenticates users. When users sign-in and enter their credentials, either through Tableau Desktop, tabcmd, API, or web client, Tableau Server verifies the credentials.

To enable this scenario, you must first create an identity for each user. To create an identity, you specify a username and a password. To access or interact with content on the server, users must also be assigned a site role. User identities can be added to Tableau Server in the server UI, using `tabcmd Commands`, or using the `REST API`.

You can also create groups in Tableau Server to help manage and assign roles to large sets of related user groups (e.g., “Marketing”).

When you configure Tableau Server for local authentication, you cannot set password policies or account lockout on failed password attempts. If you require these account safeguards, then you should use Active Directory or other supported authentication.

External authentication solutions

Tableau Server can be configured to work with a number of external authentication solutions.

NTLM and SSPI

If you configure Tableau Server to use Active Directory during installation, then NTLM will be the default user authentication method.

When a user logs onto Tableau Server from Tableau Desktop or a web client, the credentials are passed through to Active Directory, which then verifies them and sends an access token to Tableau Server. Tableau Server will then manage user access to Tableau resources based on the site roles stored in the repository.
If Tableau Server is installed on a Windows computer in Active Directory, they you may optionally enable automatic logon. In this scenario, Tableau Server will use Microsoft SSPI to automatically sign in your users based on their Windows username and password. This creates an experience similar to single sign-on (SSO). Do not enable SSPI if you plan to configure Tableau Server for SAML, trusted authentication, or for a proxy server. See tsm authentication sspi <commands>.

Kerberos

You can configure Tableau Server to use Kerberos for Active Directory. See Kerberos.

SAML

You can configure Tableau Server to use SAML (security assertion markup language) authentication. With SAML, an external identity provider (IdP) authenticates the user’s credentials, and then sends a security assertion to Tableau Server that provides information about the user’s identity.

For more information, see SAML.

OpenID Connect

OpenID Connect is a standard authentication protocol that lets users sign in to an identity provider (IdP) such as Google. After they’ve successfully signed in to their IdP, they are automatically signed in to Tableau Server. To use OpenID Connect (OIDC) on Tableau Server, the server must be configured to use the local identity store. Active Directory or LDAP identity stores are not supported with OIDC. For more information, see OpenID Connect.

Mutual SSL

Using mutual SSL, you can provide users of Tableau Desktop, Tableau Mobile, and other approved Tableau clients a secure, direct-access experience to Tableau Server. With mutual SSL, when a client with a valid SSL certificate connects to Tableau Server, Tableau Server confirms the existence of the client certificate and authenticates the user, based on the user name in the client certificate. If the client does not have a valid SSL certificate,
Tableau Server can refuse the connection. For more information, see Configure Mutual SSL Authentication.

Trusted authentication

Trusted authentication (also referred to as "Trusted tickets") lets you set up a trusted relationship between Tableau Server and one or more web servers. When Tableau Server receives requests from a trusted web server, it assumes that the web server has already handled whatever authentication is necessary. Tableau Server receives the request with a redeemable token or ticket and presents the user with a personalized view which takes into consideration the user’s role and permissions. For more information, see Trusted Authentication.

LDAP

You can also configure Tableau Server to use LDAP for user authentication. Users are authenticated by submitting their credentials to Tableau Server, which will then attempt to bind to the LDAP instance using the user credentials. If the bind works then the credentials are valid and Tableau Server grants the user a session.

“Binding” is the handshake/authentication step that happens when a client tries to access an LDAP server. Tableau Server does this for itself when it makes various non-authentication related queries (such as importing users and groups).

You can configure the type of bind you want Tableau Server to use when verifying user credentials. Tableau Server supports GSSAPI and simple bind. Simple bind passes credentials directly to the LDAP instance. We recommend that you configure SSL to encrypt the bind communication. Authentication in this scenario maybe be provided by the native LDAP solution, or with an external process, like SAML.

For more information about planning for and configuring LDAP, see Identity Store and LDAP Configuration Reference.
Other authentication scenarios

- REST API: Signing In and Out (Authentication)
- Mobile device authentication: Single sign-on for Tableau Mobile
- Certificate trust for TSM clients: Connecting TSM clients
- PAM integration for TSM administration: TSM Authentication

Data access and source authentication

You can configure Tableau Server to support a number of different authentication protocols to various different data sources. Data connection authentication may be independent of Tableau Server authentication.

For example, you may configure user authentication to Tableau Server with local authentication, while configuring Kerberos delegation, OAuth, or SAML authentication to specific data sources. See Data Connection Authentication.

SAML

SAML (Security Assertion Markup Language) is an XML standard that allows secure web domains to exchange user authentication and authorization data. You can configure Tableau Server to use an external identity provider (IdP) to authenticate users over SAML 2.0. No user credentials are stored with Tableau Server, and using SAML enables you to add Tableau to your organization’s single sign-on environment. Tableau Server supports all SAML 2.0 features including multi-factor authentication (MFA), forcing password change on first login, password complexity requirements, account lockout, and more.

You can use SAML server wide, or you can configure sites individually. Here’s an overview of those options:

- **Server-wide SAML authentication.** A single SAML IdP application handles authentication for all Tableau Server users. Use this option if your server has only the
Default site, as it is unnecessary to configure site specific SAML in this case. You may also use Server-wide SAML in multisite environments, but users are limited to a single IdP to across all sites.

- **Server-wide local authentication and site-specific SAML authentication.** In a multi-site environment, users who are not enabled for SAML authentication at the site level can sign in using local authentication.

- **Server-wide SAML authentication and site-specific SAML authentication.** In a multi-site environment, all users authenticate through a SAML IdP configured at the site level, and you specify a server-wide default SAML IdP for users that belong to multiple sites.

If you want to use site-specific SAML, you must configure server-wide SAML before you configure individual sites. Server-side SAML does not need to be enabled for site-specific SAML to function, but it must be configured.

User authentication through SAML does not apply to permissions and authorization for Tableau Server content, such as data sources and workbooks. It also does not control access to underlying data that workbooks and data sources connect to.

**Note:** Tableau Server supports both service provider initiated and IdP initiated SAML in browsers only. Connections from Tableau Desktop or the Tableau Mobile app require that the SAML request be service provider initiated.

The following image shows the steps to authenticate a user with single sign-on in a typical service provider initiated flow:
1. User navigates to the Tableau Server sign-in page or clicks a published workbook URL.

2. Tableau Server starts the authentication process by redirecting the client to the configured IdP.

3. The IdP requests the user’s username and password from the user. After the user submits valid credentials, the IdP authenticates the user.

4. The IdP returns the successful authentication in the form of a SAML Response to the client. The client passes the SAML Response to Tableau Server.

5. Tableau Server verifies that the username in the SAML Response matches a licensed user stored in the Tableau Server Repository. If a match is verified, then Tableau Server responds to the client with the requested content.

SAML Requirements

Before you configure SAML on Tableau Server, make sure your environment meets the requirements.
Certificate and identity provider (IdP) requirements

To configure Tableau Server for SAML, you need the following:

- **Certificate file.** A PEM-encoded x509 certificate file with a .crt extension. This file is used by Tableau Server, not the IdP. If you have an SSL certificate, it is possible in some circumstances to use the same certificate with SAML. For more information, see Using SSL certificate and key files for SAML later in this article.

Tableau Server requires a certificate-key pair to sign the request that is sent to the IdP. This reduces the threat of a man-in-the-middle attack given the difficulty of spoofing a signed request. Additionally, Tableau Server verifies that the AuthNResponse it receives from the trusted IdP. Tableau Server verifies the AuthNResponse by using the signature produced by the IdP. The IdP certificate metadata is provided to Tableau Server as part of the initial SAML configuration process.

Signed requests are not always necessary for all IdPs. By default, Tableau Server requires signed requests. We recommend this configuration to ensure a more secure communication transmission with the IdP. Work with your IdP team to understand if disabling signed requests is necessary. To disable signed requests see samlSettings Entity.

- **Certificate key file.** An RSA or DSA private key file that has the .key extension. RSA keys must be in PKCS#1 or PKCS#8 format. Password protection requirements are as follows:
  - The PKCS#1 RSA key file cannot be password protected.
  - To use a password-protected key file, you must configure SAML with a RSA PKCS#8 file. Note that a PKCS#8 file with a null password is not supported.

- **IdP account that supports SAML 2.0 or later.** You need an account with an external identity provider. Some examples are PingFederate, SiteMinder, and Open AM.

- **IdP provider that supports import and export of XML metadata.** Although a
manually created metadata file might work, Tableau Technical Support cannot assist with generating the file or troubleshooting it.

SSL Off-loading

If your organization terminates SSL connections from the IdP at a proxy server before sending the authentication request to Tableau Server, then you may need to make a proxy configuration. In this scenario, SSL is "off-loaded" at the proxy server, which means the https request is terminated at the proxy server and then forwarded to Tableau Server over http.

Tableau Server validates the SAML response message returned from the IdP. Since SSL is off-loaded at the proxy, Tableau Server will validate with the protocol that it receives (http), but the IdP response is formatted with https, so validation will fail unless your proxy server includes the X-Forwarded-Proto header set to https. See Configuring Proxies for Tableau Server.

Using SSL certificate and key files for SAML

If you are using a PEM-encoded x509 certificate file for SSL, you can use the same file for SAML. For SSL, the certificate file is used to encrypt traffic. For SAML, the certificate is used for authentication.

In addition to the requirements listed in Certificate and identity provider (IdP) requirements above, to use the same certificate for both SSL and SAML, the certificate must also meet the following condition to work for SAML:

- Confirm that the certificate includes only the certificate that applies to Tableau Server and not any other certificates or keys.

To do this, you can create a backup copy of the certificate file, and then open the copy in a text editor to review its contents.
User management requirements

When you enable SAML, user authentication is performed outside of Tableau, by the IdP. However, user management is performed by an identity store: either an external identity store (Active Directory or LDAP) or by Tableau Server in a local identity store. For more information about planning for user management with Tableau Server, see Identity Store.

When you configure the identity store during Setup, you must select the option that reflects how you want to use SAML. If you want to use site-specific SAML, you must configure server-wide SAML before you configure individual sites.

- **For site-specific SAML**: If you have multiple sites on Tableau Server and want to set up each site for a particular IdP or IdP application (or configure some sites not to use SAML), configure Tableau Server to manage user with a local identity store. For site-specific SAML, Tableau Server relies on the IdP for authentication and does not use passwords.

- **For server-wide SAML**: If you configure server-wide SAML with a single IdP, you can configure Tableau Server to use the local identity store or an external identity store.

- **Server-wide SAML authentication and site-specific SAML authentication**. In a multi-site environment, all users authenticate through a SAML IdP configured at the site level. In this scenario, you specify a server-wide default SAML IdP for users who belong to multiple sites. To configure this scenario, Tableau Server must be configured with a local identity store.

**Note:** The REST API and tabcmd do not support SAML single-sign (SSO). To sign in, you must specify the name and password of a user who has been created on the server. The user may be managed by the local identity store or an external identity store, depending on how you have configured Tableau Server. For Tableau Online, you can specify the TableauID credentials of the user. REST API or tabcmd calls will have the permissions of the user you sign in as.
SAML compatibility notes and requirements

- **Matching usernames**: The user name stored in Tableau Server must match the user name stored in the IdP. For example, if the user name for Jane Smith is stored in PingFederate as `jsmith`, it must also be stored in Tableau Server as `jsmith`.

If you are configuring SAML as part of the initial Tableau Server setup, make sure the account you plan to use exists in your IdP before you run setup. During Tableau Server setup you create the server administrator account.

If you use an Active Directory or LDAP external identity store and you are running in multiple domains (that is, users belong to multiple domains, or your Tableau Server installation includes multiple domains), the IdP must send both the username and domain for a user, and they must match exactly in Tableau Server. Although these can be sent as either `domain\username` or `username@domain.com`, we recommend using `domain\username`.

For more information, see User Management in Active Directory Deployments.

- **Default signature algorithm**: Tableau Server uses SHA1 signature algorithm. Many IdPs default to SHA256. A mismatch between the IdP and Tableau Server signature algorithms will cause SAML authentication failures. To change to SHA256, set the `SHA256Enabled` configuration entity to `true` during your initial configuration. See `samlSettings` Entity. You can also change to SHA256 by running the following TSM command:

  ```
tsm configuration set -k wgserver.saml.sha256 -v true
  ```

- **External authentication types**: Tableau Server supports using one external authentication type at a time.

- **Mutual SSL**: Tableau Server does not support mutual SSL (two-way SSL) and SAML together. If you want to use mutual SSL, you can configure it on the IdP.

- **Encryption and site-specific SAML assertions**: Although Tableau Server does
not support encrypted SAML assertions from the IdP, all SAML requests and responses are sent over HTTPS.

- **User identity in Tableau Server for tabcmd users:** As described in User management requirements section above, to use tabcmd, you must sign in as a user defined on the server. You cannot use SAML accounts with tabcmd.

- **Using SAML SSO with Tableau clients:** By default, both Tableau Desktop and the Tableau Mobile app allow SAML authentication.

  If your IdP does not support this functionality, you can disable SAML sign-in for Tableau clients using the following commands:

  tsm authentication saml configure --desktop-access disable
  tsm authentication saml configure --mobile-access disable

  **Note:** The `--mobile-access disable` option is ignored by devices running Tableau Mobile app version 19.225.1731 and higher. To disable SAML for devices running these versions you must disable SAML as a client login option on Tableau Server.

  For more information, see tsm authentication saml <commands>.

- **Distributed installations:** TSM versions of Tableau Server (2018.2 and newer) use the Client File Service to share files in a multi node cluster. After you have configured SAML on the initial node in your cluster, the Client File Service will distribute certificate and key files to the other nodes.

- **Login URL:** For users to be able to sign in, your IdP must be configured with SAML Login endpoint that sends a POST request to the following URL:


- **Logout URL:** To enable users to sign out after signing in with SAML (single logout,
SLO), your IdP must be configured with a SAML Logout endpoint that sends a POST request to the following URL:


SLO is only supported for server-wide SAML. SLO is not supported for site-specific SAML.

- **Post-logout redirect URL**: By default, when a user signs out of Tableau Server, the sign-in page is displayed.

To display a different page after sign-out, use the `tsm authentication saml configure` command with the `-su` or `--signout-url` option.

- To specify an absolute URL, use a fully-qualified URL starting with http:// or https://, as in this example:

  tsm authentication saml configure -su https://example.com

- To specify a URL relative to the Tableau Server host, use a page starting with a / (slash):

  tsm authentication saml configure -su /our-logoutpage.html

- **Active Directory Federation Service (AD FS)**: You must configure AD FS to return additional attributes for Tableau authentication with SAML. The `Name ID` and `username` attributes can be mapped to the same AD attribute: `SAM-Account-Name`.

Using SAML SSO with Tableau client applications

Tableau Server users with SAML credentials can sign in to the server from Tableau Desktop or the Tableau Mobile app. For full compatibility, we recommend that the Tableau client application version matches that of the server. To connect using site-specific SAML, users must run version 10.0 or later of the Tableau client application.
Connecting to Tableau Server from Tableau Desktop or Tableau Mobile uses a service provider (SP) initiated connection.

Redirecting authenticated users back to Tableau clients

When a user signs in to Tableau Server, Tableau Server sends a SAML request (AuthnRequest) to the IDP, which includes the Tableau application’s RelayState value. If the user has signed in to Tableau Server from a Tableau client such as Tableau Desktop or Tableau Mobile, it’s important that the RelayState value is returned within the IDP’s SAML response back to Tableau.

When the RelayState value is not returned properly in this scenario, the user is taken to their Tableau Server home page in the web browser, rather than being redirected back to the application they signed in from.

Work with your Identity Provider and internal IT team to confirm that this value will be included as part of the IDP’s SAML response, and then preserved by any network appliance (such as a proxy or load balancer) that resides between your IDP and Tableau Server.

XML data requirements

As part of SAML configuration, you exchange XML metadata between Tableau Server and the IDP. This XML metadata is used to verify a user’s authentication information when the user initiates the Tableau Server sign-in process.

Tableau Server and the IDP each generates its own metadata. Each set of metadata must contain the information described in the following list. If either set is missing information, errors can occur when you configure SAML or when users try to sign in.

- **HTTP POST**: Tableau Server accepts only HTTP POST requests for SAML communications. HTTP Redirect is not supported.
- With the Binding attribute set to HTTP-POST, the SAML metadata that Tableau Server and the IDP each export must contain the following elements.
- The element that specifies the URL that the IdP redirects to after successful authentication. This is required in the Service Provider metadata, not the Identity Provider metadata.


  For Site SAML, the Location endpoint is /samlservice/public/sp/metadata?alias=<site alias>.

- The logout endpoint element appears in Tableau Server metadata and specifies the URL that the IdP will use for Tableau Server's logout endpoint. If this element is not in the IdP metadata, Tableau Server cannot negotiate a logout endpoint with the IdP and the SAML Logout feature will not be available within the Tableau Server:


  SLO is only supported for server-wide SAML. SLO is not supported for site-specific SAML.

- Verify that the metadata XML from the IdP includes a `SingleSignOnService` element, in which the binding is set to `HTTP-POST`, as in the following example:


- This element should appear in IdP metadata and specifies the URL that
Tableau Server on Linux Administrator Guide

Tableau Server will use for the IdP's logout endpoint.

```xml
<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Location="https://SERVER-NAME:9031/idp/slo"/>
```

- **Attribute named `username`:** You must configure the IdP to return an assertion that includes the `username` attribute in the `saml:AttributeStatement` element. The assertion's attribute type must be `xs:string` (it should not be typed as `xs:any`).

The following example shows what this might look like.

```xml
<saml:Assertion assertion-element-attributes>
  <saml:Issuer>issuer-information</saml:Issuer>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    ...
  </Signature>
  <saml:Subject>
    ...
  </saml:Subject>
  <saml:Conditions condition-attributes >
    ...
  </saml:Conditions>
  <saml:AuthnStatement authn-statement-attributes >
    ...
  </saml:AuthnStatement>

  <saml:AttributeStatement>
    <saml:Attribute Name="username" NameFormat- t="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml:AttributeValue
```
By default, Tableau Server will read the `username` attribute in the AuthNResponse returned from the IdP. However, some IdPs may return a different attribute that is intended to identify the user. In this case, you may need to change the attribute that Tableau Server reads for the username. To authenticate successfully, the attribute’s value that is returned from the IdP must match an actual username value of a Tableau Server user.

To change the SAML attribute that passes the `username` value, run the following TSM command:

```
tsm authentication saml map-assertions --user-name <USER-NAME>.
```

See tsm authentication.

Configure Server-Wide SAML

Configure server-wide SAML when you want all single sign-on (SSO) users on Tableau Server to authenticate through a single SAML identity provider (IdP), or as the first step to configuring site-specific SAML in a multi-site environment.

If you have configured server-wide SAML and are ready to configure a site, see Configure Site-Specific SAML.

The SAML configuration steps we provide make the following assumptions:
You are familiar with the options for configuring SAML authentication on Tableau Server, as described in the SAML.

You have verified that your environment meets the SAML Requirements, and obtained the SAML certificate files described in those requirements.

Before you begin

Gather the certificate files and place them on the Tableau Server.

In the Tableau Server folder, create a new folder named SAML, and place copies of the SAML certificate files in that folder. For example:

/var/opt/tableau/tableau_server/data/saml

(Keep the certificate files in a safe location outside of the Tableau Server directory tree as well.)

**Note:** If you use the same certificate files for SSL, you could alternatively use the existing certificate location for configuring SAML, and add the IdP metadata file to that directory when you download it later in this procedure. For more information, see Using SSL certificate and key files for SAML in the SAML requirements.

If you are running Tableau Server in a cluster, then the SAML certificates, keys, and metadata file will be automatically distributed across the nodes when you enable SAML.

Use the TSM web interface

**Note:** Where indicated, you will also need to obtain metadata from your IdP. Information for how to do this will be in the IdP’s documentation.
1. Open TSM in a browser:

https://<tsm-computer-name>:8850. For more information, see Sign in to Tableau Services Manager Web UI.

2. On the **Configuration** tab, select **User Identity & Access**, and then select the **Authentication Method** tab.

3. For **Authentication Method**, select **SAML**.

4. In the SAML section that appears, complete Step 1, entering the following settings (do not yet select the check box to enable SAML for the server):

   **Tableau Server return URL**—The URL that Tableau Server users will access, such as https://tableau-server.

   Using https://localhost or a URL with a trailing slash (for example, http://tableau_server/) is not supported.

   **SAML entity ID**—The entity ID uniquely identifies your Tableau Server installation to the IdP.

   You can enter your Tableau Server URL again here. If you plan to enable site-specific SAML later, this URL also serves as the base for each site’s unique ID.
Tableau Server on Linux Administrator Guide

**SAML certificate and key files**— Enter the path you created in Configure Server-Wide SAML.

After you provide the information required in Step 1, the **Download XML Metadata File** button in Step 2 becomes available. If you are using a passphrase-protected key file, you will need to enter the passphrase with TSM CLI. See the final step in this procedure.

5. Now select the **Enable SAML authentication for the server** check box above Step 1.

6. Complete the remaining SAML settings.

   a. For Steps 2 and 3, exchange metadata between Tableau Server and the IdP. (Here’s where you might need to check in with the IdP’s documentation.)

      Select **Download XML Metadata File**, and specify the file location.

      For other IdPs, go to your IdP account to add Tableau Server to its applications (as a service provider), providing the Tableau metadata as appropriate.

      Follow the instructions in the IdP’s website or documentation to download the IdP’s metadata. Save the .xml file to the same location that holds your SAML certificate and key files. For example:

      ```
      /var/opt/tableau/tableau_server/data/saml/idp-metadata.xml
      ```

   b. Return to the TSM web UI. For Step 4, enter the path to the IdP metadata file, and then select **Upload**.
c. For Step 5: In some cases, you may need to change the assertion values in the Tableau Server configuration to match the assertion names that are passed by your IdP.

You can find assertion names in the IdP’s SAML configuration. If different assertion names are passed from your IdP, then you must update Tableau Server to use the same assertion value.

**Tip:** “Assertions” are a key SAML component, and the concept of mapping assertions can be tricky at first. It might help to put this in a tabular-data context, in which the assertion (attribute) name is equivalent to a column heading in the table. You enter that “heading” name, rather than an example of a value that might appear in that column.

d. For Step 6, select the Tableau applications in which you want to give users a single sign-on experience.

**Note:** The option to disable mobile access is ignored by devices running Tableau Mobile app version 19.225.1731 and higher. To disable SAML for devices running these versions you must disable SAML as a client login option on Tableau Server.

e. For the SAML sign-out redirect, if your IdP supports single logout (SLO), enter the page you want to redirect users to after they sign out, relative to the path you entered for the Tableau Server return URL.

f. (Optional) If you are using a PKCS#8 key that is protected with a passphrase,
open the TSM CLI and enter the passphrase as follows:

```
tsm configuration set -k wgserver.saml.key.passphrase -v <passphrase>
```

The passphrase will be encrypted and saved. See Manage Server Secrets.

7. Click **Save Pending Changes** after you've entered your configuration information.

8. Click **Pending Changes** at the top of the page:

9. Click **Apply Changes and Restart**.

Use the TSM CLI

**Before you begin**

- Go to your IdP’s website or application, and export the IdP’s metadata XML file.

Confirm that the metadata XML from the IdP includes a **SingleSignOnService** element, in which the binding is set to **HTTP-POST**, as in the following example:

```
<md:SingleSignOnService Binding=
```

**Configure return URL, SAML entity ID, and specify certificate and key files**

1. Open the command prompt shell and configure the SAML settings for the server (replacing placeholder values with your environment path and file names).
tsm authentication saml configure --idp-entity-id https://tableau-server --idp-metadata /var/-
  opt/tableau/tableau_server/data/saml/<metadata-file.xml> --idp-return-url https://tableau-server --cert-file /var/-
  opt/tableau/tableau_server/data/saml/<file.crt> --key-file /var/opt/tableau/tableau_server/data/saml/<file.key>

For more information, see tsm authentication saml configure.

2. If you are using a PKCS#8 key that is protected with a passphrase, enter the passphrase as follows:

   tsm configuration set -k wgserver.saml.key.passphrase -v <passphrase>

3. If SAML is not already enabled on Tableau Server; for example, you’re configuring it for the first time, or you have disabled it, enable it now:

   tsm authentication saml enable

4. Apply the changes:

   tsm pending-changes apply

   The pending-changes apply command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the --ignore-prompt option, but this does not change the restart behavior. For more information, see tsm pending-changes apply.

Generate Tableau Server metadata and configure the IdP

1. Run the following command to generate the required XML metadata file for Tableau server.

   tsm authentication saml export-metadata -f <file-name.xml>
You can specify a file name, or omit the `-f` parameter to create a default file named `samlmetadata.xml`.

2. On your IdP’s website or in its application:

- Add Tableau Server as a Service Provider.

  Refer to your IdP’s documentation for information about how to do this. As part of the process of configuring Tableau Server as a Service Provider, you will import the Tableau Server metadata file you generated from the `export-metadata` command.

- Confirm that your IdP uses `username` as the attribute to verify users.

**Match assertions**

In some cases, you may need to change the assertion values in the Tableau Server configuration to match the assertion names that are passed by your IdP.

You can find assertion names in the IdP’s SAML configuration. If different assertion names are passed from your IdP, then you must update Tableau Server to use the same assertion value.

**Tip:** "Assertions" are a key SAML component, and the concept of mapping assertions can be tricky at first. It might help to put this in a tabular-data context, in which the assertion (attribute) name is equivalent to a column heading in the table. You enter that “heading” name, rather than an example of a value that might appear in that column.

The following table shows the default assertion values and the configuration key that stores the value.

<table>
<thead>
<tr>
<th>Assertion</th>
<th>Default value</th>
<th>Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td><code>username</code></td>
<td><code>wgserver.saml.idpattribute.username</code></td>
</tr>
<tr>
<td>Display name</td>
<td><code>displayName</code></td>
<td><code>wgserver.saml.idpattribute.displayName</code></td>
</tr>
</tbody>
</table>
To change a given value, run the `tsm configuration set` command with the appropriate key:value pair.

For example, to change the `username` assertion to the value, `name`, run the following command:

```
$ tsm configuration set -k wgserver.saml.idpattribute.username -v name
```

After you have updated the assertions, you must run the following command to apply the changes:

```
$ tsm pending-changes apply
```

## Optional: Disable client types from using SAML

By default, both Tableau Desktop and the Tableau Mobile app allow SAML authentication.

If your IdP does not support this functionality, you can disable SAML sign-in for Tableau clients using the following commands:

```
$ tsm authentication saml configure --desktop-access disable
$ tsm authentication saml configure --mobile-access disable
```

**Note:** The `--mobile-access disable` option is ignored by devices running Tableau Mobile app version 19.225.1731 and higher. To disable SAML for devices running these versions you must disable SAML as a client login option on Tableau Server.
After you have updated the assertions, you must run the following command to apply the changes:

```bash
tsm pending-changes apply
```

Test the configuration

1. In your web browser, open a new page or tab, and enter the Tableau Server URL.

![Browser with Tableau Server URL](image)

The browser redirects you to the IdP’s sign-in form.

2. Enter your single sign-on user name and password.

![Sign-in form](image)

The IdP verifies your credentials and redirects you back to your Tableau Server start page.
Configure SAML with AD FS on Tableau Server

You can configure Active Directory Federation Services (AD FS) as a SAML identity provider, and add Tableau Server to your supported single sign-on applications. When you integrate AD FS with SAML and Tableau Server, your users can sign in to Tableau Server using their standard network credentials.

Prerequisites

Before you can configure Tableau Server and SAML with AD FS, your environment must have the following:

- A server running Microsoft Windows Server 2008 R2 (or later) with AD FS 2.0 (or later) and IIS installed.
- We recommend that you secure your AD FS server (for example, using a reverse proxy). When your AD FS server is accessible from outside your firewall, Tableau Server can redirect users to the sign in page hosted by AD FS.
- SSL certificate encrypted using SHA-2 (256 or 512 bit) encryption, and that meets the additional requirements listed in the following sections:
  - SSL certificate requirements
  - SAML Certificate and identity provider (IdP) requirements

Step 1: Verify SSL connection to AD FS

AD FS requires an SSL connection. If you haven’t done so yet, complete the steps in Configure SSL for External HTTP Traffic to and from Tableau Server, using a certificate that meets the requirements as specified above.

Alternatively, if Tableau Server is configured to work with a reverse proxy or load balancer where SSL is being terminated (commonly referred to as SSL off-loading), then you do not need to configure external SSL.
Step 2: Configure SAML on Tableau Server

Complete the steps in Configure Server-Wide SAML through downloading the Tableau Server metadata to an XML file. At that point, return here and continue to the next section.

Step 3: Configure AD FS to accept sign-in requests from Tableau Server

**Note:** These steps reflect a third-party application and are subject to change without our knowledge.

Configuring AD FS to accept Tableau Server sign-in requests is a multi-step process, starting with importing the Tableau Server XML metadata file to AD FS.

1. Do one of the following to open the Add Relying Party Trust Wizard:

   **Windows Server 2008 R2:**
   
   a. Select **Start menu> to Administrative Tools> AD FS 2.0**.
   
   b. In **AD FS 2.0**, under **Trust Relationships**, right-click the **Relying Party Trusts** folder, and then click **Add Relying Party Trust**.

   **Windows Server 2012 R2:**
   
   a. Open **Server Manager**, and then on the **Tools** menu, click **AD FS Management**.
   
   b. In **AD FS Management**, on the **Action** menu, click **Add Relying Party Trust**.

2. In the Add Relying Party Trust Wizard, click **Start**.

3. On the **Select Data Source** page, select **Import data about the relying party from a file**, and then click **Browse** to locate your Tableau Server XML metadata file. By default, this file is named **samls.metadata.xml**.

4. Click **Next**, and on the Specify Display Name page, type a name and description for
the relying party trust in the **Display name** and **Notes** boxes.

5. Click Next to skip the **Configure Multi-factor Authentication Now** page.

6. Click Next to skip the **Choose Issuance Authorization Rules** page.

7. Click Next to skip the **Ready to Add Trust** page.

8. On the **Finish** page, select the **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes** check box, and then click **Close**.

Next, you'll work in the **Edit Claim Rules** dialog, to add a rule that makes sure the assertions sent by AD FS match the assertions Tableau Server expects. At a minimum, Tableau Server needs an email address. However, including first and last names in addition to email will ensure the user names displayed in Tableau Server are the same as those in your AD account.

1. In the **Edit Claim Rules** dialog box, click **Add Rule**.

2. On the **Choose Rule Type** page, for **Claim rule template**, select **Send LDAP Attributes as Claims**, and then click **Next**.

3. On the **Configure Claim Rule** page, for **Claim rule name**, enter a name for the rule that makes sense to you.

4. For **Attribute store**, select **Active Directory**, complete the mapping as shown below, and then click **Finish**.

The mapping is case sensitive and requires exact spelling, so double-check your entries.

<table>
<thead>
<tr>
<th>LDAP Attribute</th>
<th>Outgoing Claim Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAM-Account-Name</td>
<td>Name ID</td>
</tr>
<tr>
<td>SAM-Account-Name</td>
<td>username</td>
</tr>
</tbody>
</table>
Tableau Server on Linux Administrator Guide

<table>
<thead>
<tr>
<th>Given-Name</th>
<th>firstName</th>
</tr>
</thead>
<tbody>
<tr>
<td>Surname</td>
<td>lastName</td>
</tr>
</tbody>
</table>

If you are running AD FS 2016 or later, then you must add a rule to pass through all claim values. If you are running an older version of AD FS, skip to the next procedure to export AD FS metadata.

1. Click **Add Rule**.
2. Under **Claim rule template**, choose **Pass Through or Filter an Incoming Claim**.
3. Under **Claim rule name**, enter Windows.
4. On the **Edit Rule - Windows** pop-up:
   - Under **Incoming claim type**, select **Windows account name**.
   - Select **Pass through all claim values**.
   - Click **OK**.

Now you will export AD FS metadata that you'll import to Tableau Server later. You will also make sure the metadata is configured and encoded properly for Tableau Server, and verify other AD FS requirements for your SAML configuration.

1. Export AD FS Federation metadata to an XML file, and then download the file from https://<adfs server name>/FederationMetadata/2007-06/FederationMetadata.xml.
2. Open the metadata file in a text editor like Sublime Text or Notepad++, and verify that it is correctly encoded as UTF-8 without BOM.

   If the file shows some other encoding type, save it from the text editor with the correct encoding.

3. Verify that AD FS uses forms-based authentication. Sign-ins are performed in a browser window, so you need AD FS to default to this type of authentication.

   Edit c:\inetpub\adfs\ls\web.config, search for the tag , and move the line so it appears first in the list. Save the file so that IIS can automatically reload it.
Note: If you don’t see the c:\inetpub\adfs\ls\lsweb.config file, IIS is not installed and configured on your AD FS server.

4. (Optional) This step is required only if AD FS is configured as an IDP for site-specific SAML. This step is not required if AD FS is configured as the IDP for server-wide SAML.

Configure an additional AD FS relying party identifier. This allows your system to work around any AD FS issues with SAML logout.

Do one of the following:

Windows Server 2008 R2:

a. In AD FS 2.0, right-click on the relying party you created for Tableau Server earlier, and click Properties.

b. On the Identifiers tab, in the Relying party identifier box, enter https://<tableauservername>/public/sp/metadata and then click Add.

Windows Server 2012 R2:

a. In AD FS Management, in the Relying Party Trusts list, right-click on the relying party you created for Tableau Server earlier, and click Properties.

b. On the Identifiers tab, in the Relying party identifier box, enter https://<tableauservername>/public/sp/metadata and then click Add.

Note: AD FS can be used with Tableau Server for a single relying party to the same instance. AD FS cannot be used for multiple relying parties to the same instance, for example, multiple site-SAML sites or server-wide and site SAML configurations.
Tableau Server on Linux Administrator Guide

5. Turn off AD FS assertion encryption for the relying party. Tableau Server does not currently support assertion encryption.

On the AD FS server, use Windows PowerShell to run the following command, replacing `<MyRelyingPartyName>` in the example command below to the name of the ADFS relying party *display name*:

```
Set-ADFSRelyingPartyTrust -TargetName <MyRelyingPartyName> -EncryptClaims 0
```

**Note:** If you receive the error `Set-ADFSRelyingPartyTrust Cmdlet cannot be found`, you must add the AD FS PowerShell snap-in. At the command prompt, type: `Add-PSSnapin Microsoft.Adfs.PowerShell`, and then repeat this step.

Step 4: Provide AD FS metadata to Tableau Server

1. Return to the TSM web UI, and navigate to **Configuration > User Identity & Access > Authentication Method** tab.

2. In Step 4 of the SAML configuration window, enter the location of the XML file you exported from AD FS, and select **Upload**.

3. Complete the remaining steps (matching assertions and specifying client type access) as specified in Configure Server-Wide SAML. Save and apply changes.

4. Stop Tableau Server, open TSM CLI, and run the following commands.
The first command assures that AD FS can properly redirect to Tableau Server after it accepts users’ SAML credentials. The second command configures Tableau Server with the same "Refresh Token Max Inactive Time" that is the default on AD FS and Azure AD FS. Setting the maximum inactive time to match AD FS avoids a common error state as described in Tableau Knowledge Base article, Intermittent Error "Unable to Sign In" with SAML SSO on Tableau Server.

```
tsm configuration set -k wgserver.saml.sha256 -v true
```

```
tsm authentication saml configure -a 7776000
```

5. Apply the changes:

```
tsm pending-changes apply
```

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

Use SAML SSO with Kerberos Database Delegation

In a Windows Active Directory (AD) environment, you can enable SAML single sign-on (SSO) to Tableau Server, along with Kerberos database delegation. This provides authorized users direct access to Tableau Server, as well as to the underlying data defined in their published workbooks and data sources.
Overview of the process

In a typical scenario:

1. One of your Tableau analysts publishes a dashboard to Tableau Server. That dashboard contains a connection to a Hadoop cluster, for example, that is configured to accept Kerberos credentials.

   Then the workbook publisher sends a link to colleagues for review.

2. When a colleague clicks the link, Tableau Server authenticates the user through the SAML SSO process. Then it looks at the user’s authorization scheme, and if allowed, uses the Tableau Server keytab to accesses the underlying database on behalf of the user. This populates the dashboard with the Hadoop data that the user is authorized to see.
Configure Tableau Server for SAML with Kerberos

Using SAML with Kerberos works inherently when you complete the processes to enable each separately:

1. Configure Tableau Server for SAML, as described in Configure Server-Wide SAML.
2. Configure Tableau Server and your underlying databases to accept Kerberos credentials, as described in Enable Kerberos Delegation and related articles.

Configure Site-Specific SAML

Use site-specific SAML in a multi-site environment when you want to enable single sign-on, and you also use multiple SAML identity providers (IdPs) or IdP applications. When you enable site SAML, you can specify the IdP or IdP application for each site, or configure some sites to use SAML and the others to use the default server-wide authentication method.

If you want all server users to use SAML and sign in through the same IdP application, see Configure Server-Wide SAML.

Prerequisites for enabling site-specific SAML

Before you can enable SAML single sign-on at the site level, complete the following requirements:

- The Tableau Server identity store must be configured for local identity store.
  
  You cannot configure site-specific SAML if Tableau Server is configured with an external identity store such as Active Directory or OpenLDAP.

- Make sure your environment and your IdP meet the general SAML Requirements.

  Some features are supported only in server-wide SAML deployments. For example, single logout (SLO) is only supported for server-wide SAML. SLO is not supported for site-specific SAML.

  You must configure server-wide SAML before you configure site-specific SAML. You
do not need to enable server-wide SAML, but site-specific SAML requires the server-wide configuration. See Configure Server-Wide SAML.

- Note the location of the SAML certificate files. You will provide this when you configure the server to support site-specific SAML.

For more information, see Put metadata and certificate files in place in the topic on configuring server-wide SAML.

- Add Tableau Server as a service provider to your IdP. You can find this information in the documentation the IdP provides.

- Confirm that the system clocks of the computer hosting the site-SAML IdP and the computer hosting Tableau Server are within 59 seconds of each other. Tableau Server does not have a configuration option to adjust the response skew (time difference) between the Tableau Server computer and the IdP.

Server-wide settings related to site-specific SAML

In the server’s workgroup.yml file, server-wide settings that are used in some way for site-specific SAML include:

- wgserver.saml.returnurl and wgserver.saml.entityid: In the settings for configuring site-specific SAML, Tableau provides a site-specific return URL and entity ID based on these settings. The site-specific return URL and entity ID cannot be modified.

- wgserver.saml.domain, wgserver.saml.port, and wgserver.saml.protocol are used for SAML requests at the site level.

Server-wide settings wgserver.saml.maxauthenticationage and wgserver.saml.responseskew do not apply to site-specific SAML.
Configure the server to support site-specific SAML

After you complete the prerequisites listed above, you can run the following commands to configure the server to support site-specific SAML.

1. **Configure Server-Wide SAML**. At a minimum, you must run the following TSM command (if you have already configured server-wide SAML, skip to Step 2):

   ```bash
   tsm authentication saml configure --idp-entity-id <tableau-server-entity-id> --idp-return-url <tableau-server-return-url> --cert-file <path-to-saml-certificate.crt> --key-file <path-to-saml-keyfile.key>
   ``

2. **Enable site SAML**. Run the following commands:

   ```bash
   tsm authentication sitesaml enable
   tsm pending-changes apply
   ``

### About the commands

The `sitesaml enable` command exposes the **Authentication** tab on each site’s **Settings** page in the Tableau Server web UI. After you configure the server to support site SAML, you can continue to Configure SAML for a site to work through the settings on the **Authentication** tab.

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

If you want to review the commands and settings that will be carried out when you run `pending-changes apply`, you can run the following command first:

```bash
 tsm pending-changes list --config-only
```
Configure SAML for a site

This section takes you through the configuration steps that appear on the Authentication page in the Tableau Server web UI. In a self-hosted Tableau Server installation, this page appears only when support for site-specific SAML is enabled at the server level. It is enabled by default in Tableau Online.

**Note:** To complete this process, you will also need the documentation your IdP provides. Look for topics that refer to configuring or defining a service provider for a SAML connection, or adding an application.

### Step 1: Export metadata from Tableau

To create the SAML connection between Tableau Server and your IdP, you need to exchange required metadata between the two services. To get metadata from Tableau Server, do either of the following steps. See the IdP’s SAML configuration documentation to confirm the correct option.

- Select **Export metadata** to download an XML file that contains the Tableau Server SAML entity ID, Assertion Consumer Service (ACS) URL, and X.509 certificate.

  The entity ID is site-specific, and based on the server-wide entity ID that you specified when you enabled site SAML on the server. For example, if you specified https://tableau_server, you might see the following entity ID for the site:

  https://tableau_server-/samlservice/public/sp/metadata?alias=48957410-9396-430a-967c-75bdb6e002a0

  You cannot modify the site-specific entity ID or ACS URL that Tableau generates.

- Select **Download signing and encryption certificate** if your IdP expects the
required information in a different way. For example, if it wants you to enter the Tableau Server entity ID, ACS URL, and X.509 certificate in separate locations.

The following image has been edited to show that these settings are the same in Tableau Online and Tableau Server.

Steps 2 and 3: External steps

For Step 2, to import the metadata you exported in step 1, sign in to your IdP account, and use the instructions provided by the IdP’s documentation to submit the Tableau Server metadata.

For Step 3, the IdP’s documentation will guide you also in how to provide metadata to a service provider. It will instruct you to download a metadata file, or it will display XML code. If it displays XML code, copy and paste the code into a new text file, and save the file with a .xml extension.

Step 4: Import IdP metadata to the Tableau site

On the Authentication page in Tableau Server, import the metadata file that you downloaded from the IdP or configured manually from XML it provided.

Step 5: Match attributes
Attributes contain authentication, authorization, and other information about a user. In the **Identity Provider (IdP) Assertion Name** column, provide the attributes that contain the information Tableau Server requires.

- **Username or Email**: (Required) Enter the name of the attribute that stores user names or email addresses.

- **Display name**: (Optional but recommended) Some IdPs use separate attributes for first and last names, and others store the full name in one attribute.

Select the button that corresponds to the way your IdP stores the names. For example, if the IdP combines first and last name in one attribute, select **Display name**, and then enter the attribute name.

![Match attributes screenshot](image)

**Step 6: Manage users**
Select existing Tableau Server users, or add new users you want to approve for single sign-on.

When you add or import users, you also specify their authentication type. On the Users page, you can change users’ authentication type any time after adding them.

For more information, see Add Users to a Site or Import Users and Set the User Authentication Type for SAML.

**Important:** Users that authenticate with site-specific SAML can belong only to one site. If a user needs to access multiple sites, set their authentication type to the server default. Depending on how site-specific SAML was configured by the server administrator, the server default is either local authentication or server-wide SAML.

## Default authentication type for embedded views

Part of enabling SAML on your site is to specify how users access views embedded in web pages.

- **Allow users to choose their authentication type**

  When you select this, two sign-in options appear where a view is embedded: a sign-in button that uses single sign-on authentication and a link to use TableauID as an alternative.

  **Tip:** With this option, users need to know which alternative to choose. As part of notification you send your users after you add them to the single sign-on site, let them know which type of authentication to use for a variety of sign-in scenarios. For example, embedded views, Tableau Desktop, Tableau Bridge, Tableau Mobile, and so on.
Tableau Server on Linux Administrator Guide

- **TableauID**

  This option requires users to sign in using a TableauID even if SAML is enabled on the site. Generally it’s reserved for administrators for troubleshooting issues with embedded views and SAML.

- **Single sign-on with SAML**

  If your IdP doesn’t support signing in from an iframe, select **Authenticate in a separate pop-up window**. When a user goes to the web page with the embedded view, the pop-up window appears when they select the sign-in button.

  If your IdP supports signing in from an iframe, select **Authenticate using an inline frame (less secure; not supported by all IdPs)**. Iframe embedding can provide a more seamless user experience. For example, if a user is already authenticated with your IdP, and iframe embedding is enabled, the user seamlessly authenticates with Tableau Server when browsing to pages that contain embedded Tableau views.

  **Caution**: Because iframes can be vulnerable to *clickjacking* attacks, not all IdPs support signing in through an iframe. With clickjacking, the attacker tries to lure users into clicking or entering content. They do this by displaying the page to attack in a transparent layer over an unrelated page. For Tableau Server, an attacker might try to capture user credentials or to get an authenticated user to change settings. For more information, see *Clickjacking* on the Open Web Application Security Project website.

Troubleshoot SAML

This topic provides information about resolving issues that can occur when you configure SAML authentication.
SAML and Enable Automatic Logon

If you are using SAML and if Tableau Server is also configured to use Active Directory, do not also select **Enable automatic logon.** **Enable automatic logon** and SAML cannot both be used on the same server installation.

HTTP Status 500 error when configuring SAML

Under some circumstances you might get an HTTP status 500 error and see the following error after enabling SAML and navigating to the Tableau Server URL in a browser:

```java
org.opensaml.saml2.metadata.provider.MetadataProviderException:
User specified binding is not supported by the Identity Provider using profile urn:oasis-is:names:tc:SAML:2.0:profiles:SSO:browser
```

To help resolve this error, make sure of the following:

- The IdP URL for the SSO profile specified in the SAML tab is correct.
- The IdP URL for the SSO profile provided while creating the service provider in the IdP is correct.
- The IdP is configured to use **HTTP-POST** requests. (Redirect and SOAP are not supported.)

If any of these settings were not correct, make appropriate updates and then perform the SAML configuration steps again, starting with generating and exporting the XML metadata document from Tableau Server.

If these settings are correct, but you still see the error, examine the metadata XML that is produced by Tableau Server and by the IdP, as described in SAML Requirements.

Signing In from the Command Line

SAML is not used for authentication when you sign in to Tableau Server using tabcmd or the Tableau Data Extract command line utility (provided with Tableau Desktop), even if
Tableau Server on Linux Administrator Guide

Tableau Server is configured to use SAML. These tools require the authentication configured when Tableau Server was originally installed (either local authentication or AD).

Login fails: failed to find the user

Login fails with the following message:

> Login failure: Identity Provider authentication successful for user <username from IdP>. Failed to find the user in Tableau Server.

This error typically means that there is a mismatch between the usernames stored in Tableau Server and provided by the IdP. To fix this, make sure that they match. For example, if Jane Smith's username is stored in the IdP as jsmith it must be stored in Tableau Server as jsmith.

Login fails: SSL offloading

Logon fails with the following message:

Unable to Sign In - Invalid username or password.

Additionally, the vizportal logs (set to debug mode) contain the following message:

DEBUG com.tableausoftware.core.util.RemoteIP - Found header null in X-FORWARDED-PROTO

For more information about setting log levels, see Change Logging Levels.

This combination of messages indicates a misconfiguration of an external proxy server that is offloading SSL for the connection to Tableau Server. To resolve this issue, see the KB article, "Unable to Sign In" and "Invalid username or password" Error With SAML After Upgrading.
SAML Error Log

SAML authentication takes place outside Tableau Server, so troubleshooting authentication issues can be difficult. However, login attempts are logged by Tableau Server. You can create a snapshot of log files and use them to troubleshoot problems. For more information, see Log File Snapshots (Archive Logs).

**Note:** To log SAML-related events, `vizportal.log.level` must be set to `debug`. For more information, see Change Logging Levels.

Check for SAML errors in the following files in the unzipped log file snapshot:
\vizportal\vizportal-<n>.log

In Tableau Server 9.0 and later, the application process (`vizportal.exe`) handles authentication, so SAML responses are logged by that process.

**Trailing Slash**

On the SAML tab, confirm that the **Tableau Server return URL** does not end with a trailing slash

Correct: `http://tableau_server`

Incorrect: `http://tableau_server/`

**Confirm Connectivity**

Confirm that the Tableau Server you are configuring has either a routeable IP address or a NAT at the firewall that allows two-way traffic directly to the server.

You can test your connectivity by running `telnet` on Tableau Server and attempting to connect with the SAML IdP. For example: `C:\telnet 12.360.325.10 80`

The above test should connect you to the HTTP port (80) on the IdP and you should receive an HTTP header.
Kerberos

Kerberos is a three-way authentication protocol that relies on the use of a trusted third-party network service called the Key Distribution Center (KDC) to verify the identity of computers and provide for secure connections between the computers through the exchange of tickets. These tickets provide mutual authentication between computers or services, verifying that one has permission to access the other.

Tableau Server supports Kerberos authentication in an Active Directory Kerberos environment, with authentication to Tableau Server being handled by Kerberos.

**Note:** The Kerberos support in Tableau Server is for user authentication. It does not handle internal permissions and authorization related to Tableau Server content, such as workbooks.

How Kerberos works

When you configure Tableau Server for Kerberos in an Active Directory (AD) environment, the AD domain controller also serves as the Kerberos Key Distribution Center (KDC) and issues Ticket Granting Tickets to the other nodes in the domain. Users authenticated by the KDC do not have to authenticate further when connecting to Tableau Server.

The following is a diagram of the authentication workflow.
User logs into their Active Directory domain.

The Kerberos KDC authenticates the user and sends a Ticket Granting Ticket (TGT) to the user's computer.

The user connects to Tableau Server in Tableau Desktop or in a web browser.

Tableau Server authenticates the user.

Kerberos Requirements

You can configure Kerberos authentication for Tableau Server running in Active Directory environments.

General requirements

- **External Load Balancer/Proxy Server:** If you are going to use Tableau Server with Kerberos in an environment that has external load balancers (ELBs) or proxy server, you need to set these up before you configure Kerberos in the Tableau Server Configuration utility. See Configuring Proxies for Tableau Server.

- **iOS Browser Support:** An iOS user can use Kerberos authentication with mobile...
Tableau Server supports constrained delegation for authentication to datasources. In this scenario, the Tableau data access account is specifically granted rights to the target database SPNs. Unconstrained delegation is not supported.

- The supported data sources (SQL Server, MSAS, PostgreSQL, Hive/Impala, and Teradata) must be configured for Kerberos authentication.
- A keytab file that is configured with the service provider name for the Tableau Server for user authentication. If you are using Kerberos authentication for datasources then those credentials should be included in the single keytab file that you will specify during Kerberos configuration on Tableau Server.

Active Directory requirements

You must meet the following requirements to run Tableau Server with Kerberos in an Active Directory environment:

- Tableau Server must use Active Directory (AD) for authentication.
- The domain must be an AD 2003 or later domain for Kerberos connections to Tableau Server.
- Smart Card Support: Smart cards are supported when users sign into their workstations with a smartcard and this results in a Kerberos TGT being granted to the user from Active Directory.
- Single-Sign On (SSO): Users must be granted a Kerberos Ticket Granting Ticket (TGT) from Active Directory when they sign into their computers. This is standard behavior for domain-joined Windows computers and standard for Mac computers that use AD as their network account server. For more information on using Mac...
computers and Active Directory, see Join your Mac to a network account server in the Apple Knowledge Base.

Kerberos delegation

For Kerberos delegation scenarios the following are required:

- If the domain is AD 2003 or later, single domain Kerberos delegation is supported. The users, Tableau Server, and backend database must be on the same domain.

- If the domain is AD 2008, there is limited cross domain support. Users from other domains can be delegated if the following conditions are met. Tableau Server and the backend database must be on the same domain, and a two way trust is required between the domain where Tableau Server resides and the user's domain.

- If the domain is 2012 or later, full cross-domain delegation is supported. AD 2012 R2 is preferred because it has a dialog for configuring constrained delegation, while 2012 non-R2 requires manual configuration.

Understanding Keytab Requirements

Kerberos authentication relies on credentials that are stored in specially formatted files called keytab files. You may need to generate keytab files for your Tableau Server deployment. This topic describes the keytab files that Tableau Server uses to access various services in a typical organization. You may need to generate keytabs for Tableau Server to integrate into the following services:

- User authentication (SSO) in Windows Active Directory
- Datasource delegation
- Operating system
- Directory service

If your organization includes IT professionals who handle identity, authentication, and/or security, then you should work with them to create a plan for generating appropriate keytabs for your Tableau Server deployment.
Tableau Server on Linux Administrator Guide

User authentication (SSO) in Windows Active Directory

If you will be using Active Directory as the identity store for Tableau Server, and you want users to authenticate with Kerberos SSO, then you will need to generate a keytab file for Tableau Server.

<table>
<thead>
<tr>
<th>Tableau is running on...</th>
<th>Need to manually generate a keytab?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows in Active Directory domain</td>
<td>Yes</td>
</tr>
<tr>
<td>Linux in Active Directory domain</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows or Linux in non-Active Directory environment</td>
<td>Kerberos SSO is not a supported scenario.</td>
</tr>
</tbody>
</table>

Follow these recommendations (for Windows and Linux versions of Tableau Server):

- Create a service account in your directory for Tableau Server.

- Create a keytab specifically for the Tableau Server service account. Do not reuse the keytab file that the computer account/OS uses to authenticate. You may use the same keytab for Kerberos SSO as you use for the directory authentication in the scenario above.

- You must create service principal names (SPN) in Active Directory for the Tableau Server service.

- Use the batch file in the next section to create the SPNs and the keytab file.

- After you have created the SPNs, upload the keytab file as described in Configure Kerberos.

Batch file: Set SPN and create keytab in Active Directory

You can use a batch file to set the service principal names (SPN) and create a keytab file. These operations are a part of the process to enable Kerberos SSO for Tableau Server (on
Windows or Linux) running in Active Directory.

In previous versions of Tableau Server (before 2018.2), the configuration script was generated from the Tableau Server Configuration utility.

To generate a configuration script, copy and paste the following batch file contents into a text file. The batch file creates service principal names (SPN) for Tableau Server and will create a keytab file for the user you specify in the file.

Follow the directions in the file contents. After you have finished customizing the file, save it as a .bat file.

This file must be run in an Active Directory domain by a Domain admin, who will be prompted for the service account password of the account you specify in the file.

The batch file uses the Windows `set`, `setspn`, and `ktpass` commands.

```
@echo off
setlocal EnableDelayedExpansion

REM *******
```

**Note:** The batch file below is self-documented. However, if you do not have experience with Kerberos and generating keytab files, we recommend that you read the Microsoft blog post, *All you need to know about Keytab files*, before proceeding. Environmental details in your organization may require additional configuration of the `ktpass` command. For example, you must determine what to set for the `/crypto` parameter. We recommend specifying a single `/crypto` value that is required by your KDC. See the Microsoft article, `ktpass` for the full list of supported values for the `/crypto` parameter.

### SPN and keytab batch file contents

```
@echo off
setlocal EnableDelayedExpansion

REM *******
```
Tableau Server on Linux Administrator Guide

REM This script generates the Service Principal Names (SPNs) and keytab files required for
REM Kerberos SSO with Apache.
REM This script executes set, setspn, and ktpass commands
included in any Windows Server
REM Operating System from 2003 on.
REM Before running this script you must enter configuration
information for the setspn and
REM ktpass commands.
REM Elements that require your configuration information are
enclosed in as such:
REM ! -- and --!
REM After you customize this file, save it as a .bat file, and
run on a domain-joined
REM computer.
REM This script must be run by a Domain admin.

REM **********

REM The following set command will prompt the domain admin for
credentials of the
REM Tableau Server service account.
REM This account must be a valid domain user account.
REM If the password contains a literal " (blackslash - double
quote), all backslashes
REM immediately before the double quote must be
REM duplicated when typed for the password to work, e.g. if pass-
word contains
REM " replace with ", if passwords contains \" replace with
\\"

set /p adpass= "Enter password for the Tableau Server service
account."
set adpass=!adpass:="\"
The following setspn commands create the SPN in the domain. More information on setspn can be found here:
Enter the canonical FQDN and the host names for Tableau Server followed by the Tableau Server service account name.
Use this syntax: HTTP/hostname domain\service_account_name.
The example below shows syntax for a computer named "tableau01" in the "example.lan" domain, with service account, "tab-serv-account":
setspn -s HTTP/tableau01 example\tab-serv-account
setspn -s HTTP/tableau01.example.lan example\tab-serv-account
DNS and AD are not case sensitive, but the keytab files are. Verify that host names match letter case as stored in DNS.
Use Windows Server's DNS Manager utility to verify host name case.

echo Creating SPNs...
setspn -s HTTP/!--replace with canonical host name and service account --!
setspn -s HTTP/!--replace with canonical FQDN and service account --!

REM The following commands create the keytab file in the same
directory where the REM bat file is run. More information on ktpass can be found here:
REM https://docs.microsoft.com/en-us/windows-server-
/administration/windows-commands/ktpass
REM Note: keytab files are case-sensitive.
REM The realm following the FQDN should be all uppercase.
REM Syntax is:
REM ktpass /princ HTTP/!--FQDN--!@!--Kerberos_Realm--! /pass !ad-
pass!
REM /pttype KRB5_NTPRINCIPAL /crypto !--cipher--! /out
keytabs\kerberos.keytab
REM Best practice: specify the /crypto value that is required by
your KDC.
REM Specifying /crypto All will result in passwords stored with
RC4 cipher, which is
REM no longer considered secure.
REM The following example shows the ktpass syntax with the
example.lan configuration from above:
REM ktpass /princ HTTP/tableau01.example.lan@EXAMPLE.LAN /pass
!adpass! /pttype KRB5_NT_PRINCIPAL /crypto AES256-SHA1 /out keyt-
abs\kerberos.keytab

REM *********

echo Creating Keytab files in %CD%\keytabs
mkdir keytabs
ktpass /princ HTTP/!--FQDN--!@!--Kerberos_Realm--! /pass !ad-
pass! /pttype KRB5_NT_PRINCIPAL /crypto AES256-SHA1 /out keyt-
abs\kerberos.keytab

Operating system

If your organization uses Kerberos for authentication, then the computer where Tableau
Server is running must be authenticated with the Kerberos realm in which it's running.
If you are running Tableau Server on Windows, and the computer is joined to the Active Directory, then you do not need to manage or generate a keytab file for the operating system.

If you are running Tableau Server on Linux in a Kerberos realm (MIT KDC or Active Directory), then you will need to generate a keytab file specifically for the computer operating system. The keytab you create for the computer should be specifically for OS authentication. Do not use the same keytab file for OS authentication that you will be using for the other services described later in this topic.

Directory service

If your organization uses a directory service, such as LDAP or Active Directory, to manage user identity, then Tableau Server requires read-only access to the directory.

Alternatively, you can configure Tableau Server to manage all accounts by installing with a local identity store. In this case, you do not need a keytab.

The following table summarizes keytab requirements:

<table>
<thead>
<tr>
<th>Tableau is running on...</th>
<th>Directory service</th>
<th>Need to manually generate a keytab?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows in AD domain</td>
<td>Active Directory</td>
<td>No</td>
</tr>
<tr>
<td>Windows</td>
<td>LDAP (GSSAPI bind)</td>
<td>Yes</td>
</tr>
<tr>
<td>Linux</td>
<td>Active Directory or LDAP</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Tableau Server on Linux Administrator Guide

<table>
<thead>
<tr>
<th>(GSSAPI bind)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows or Linux</td>
<td>Active Directory or LDAP (Simple bind)</td>
</tr>
<tr>
<td>Windows or Linux</td>
<td>Local identity store</td>
</tr>
</tbody>
</table>

If you need to manually generate a keytab for this scenario, then you will use it for GSSAPI bind to the directory. Follow these recommendations:

- Create a service account in your directory for Tableau Server.
- Create a keytab specifically for the Tableau Server service account. Do not reuse the keytab file that the computer account/OS uses to authenticate.
- Upload the keytab file as part of the json configuration of the Tableau Server identity store. See identityStore Entity.

Datasource delegation

You can also use Kerberos delegation to access data sources in an Active Directory. In this scenario, users can be authenticated to Tableau Server with any supported authentication mechanism (SAML, local authentication, Kerberos, etc), but can access datasources that are enabled by Kerberos.

<table>
<thead>
<tr>
<th>Tableau is running on...</th>
<th>Need to manually generate a keytab?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows in Active Directory domain</td>
<td>Yes</td>
</tr>
<tr>
<td>Linux in Active Directory domain</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows or Linux in non-Active Directory environment</td>
<td>Not a supported scenario.</td>
</tr>
</tbody>
</table>

Follow these recommendations:
The keytab file that you use for Kerberos delegation can be the same keytab that you use for Kerberos user authentication (SSO).

The keytab must be mapped to the service principal for Kerberos delegation in Active Directory.

You may use the same keytab for multiple data sources.

For more information, see the following configuration topics:

- Tableau Server on Linux: Enable Kerberos Delegation
- Tableau Server on Windows: Enabling Kerberos Delegation

Configure Kerberos

You can configure Tableau Server to use Kerberos. This allows you to provide a single sign-on (SSO) experience across all the applications in your organization. Before you configure Tableau Server for Kerberos make sure your environment meets the Kerberos Requirements.

**Note:** Kerberos constrained delegation for SSO to Tableau Server is not supported. (Constrained delegation for data sources is supported.) For more information, see Single-Sign On (SSO) in Kerberos Requirements.

To configure Kerberos, you must first enable Kerberos, and then specify a keytab file for user authentication. The keytab file you specify must be configured with the service provider name for the Tableau Server for user authentication. If you are using Kerberos authentication for data sources, those credentials should be included in the single keytab file that you will specify during Kerberos configuration on Tableau Server.

Use the TSM web interface
1. Open TSM in a browser:

https://<tsm-computer-name>:8850. For more information, see Sign in to Tableau Services Manager Web UI.

2. Click User **Identity & Access** on the **Configuration** tab and then click **Authentication Method**.

3. Under **Authentication Method**, select **Kerberos** in the drop-down menu.

4. Under Kerberos, select **Enable Kerberos for single sign-on (SSO)**.

5. To copy the keytab file to the server, click **Select File**, and then browse to the file on your computer.

6. Click **Save Pending Changes** after you've entered your configuration information.

7. Click **Pending Changes** at the top of the page:

8. Click **Apply Changes and Restart**.
Use the TSM CLI

1. Copy the keytab file to the computer running Tableau Server and run the following command to set permissions on the file:

   `chmod 644 "/path/keytab_file"`

   If you are running Tableau Server on in a distributed cluster deployment, then you will need to manually distribute the keytab file to each node and then set the permissions. Copy the keytab file to the same directory on each node in the cluster. After you have copied the keytab file to each node and set permissions on the file, then run the following TSM commands on one node. The configuration will propagate to each node.

2. Type the following command to specify the location and name of the keytab file:

   `tsm authentication kerberos configure --keytab-file <path-to-keytab_file>`

3. Type the following command to enable Kerberos:

   `tsm authentication kerberos enable`

4. Run `tsm pending-changes apply` to apply changes.

   The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

   Confirm your SSO configuration

   Once Tableau Server has restarted, test your Kerberos configuration from a web browser on a different computer by typing the Tableau Server name in the URL window:
You should be automatically authenticated to Tableau Server.

Tableau Client Support for Kerberos SSO

This article describes some requirements for and nuances with using Kerberos single sign-on (SSO) with Tableau Server, depending on the particular Tableau client and operating system. Tableau clients covered in this article include common web browsers, Tableau Desktop, and the Tableau Mobile app.

General browser client support

To use browser-based Kerberos Single Sign-on (SSO), the following must be true:

- Kerberos must be enabled on Tableau Server.
- The user must have a user name and password to sign in to Tableau Server.

  **Note:** If Kerberos SSO fails, users can fall back on their user name and passwords credentials.

- The user must be authenticated to Active Directory through Kerberos on the client computer or mobile device. Specifically, this means that they have a Kerberos Ticket Granting Ticket (TGT).

Tableau Desktop and browser clients

On Windows or the Mac, you can use Kerberos SSO to sign in to Tableau Server from the following versions of Tableau Desktop or browser. Where noted, additional configuration is required.
Windows

- Tableau Desktop 8.3 or later supported.
- Internet Explorer - supported, may require configuration - see Note 1.
- Chrome - supported, may require configuration - see Note 1.
- Firefox - requires configuration - see Note 2.
- Safari - not supported.

Mac OS X

- Tableau Desktop 8.3 or newer
- Safari - supported
- Chrome - see Note 3
- Firefox - see Note 2
- Internet Explorer - not supported

Tableau Mobile app clients

On a Mac iOS or Android device, you can use the following Tableau Mobile or mobile browser versions to use Kerberos authentication to Tableau Server:

Mac iOS

- Tableau App 8.3 or newer - see Note 4
- Safari - see Note 4
- Chrome - not supported

Android - see Note 5

- Tableau App 8.3 or newer
- Android Browser
- Chrome

OS- and browser-specific notes

The following notes describe configuration requirements or issues with specific operating system and client combinations.
Note 1: Internet Explorer or Chrome on Windows desktop

Kerberos SSO is supported in both Internet Explorer and Chrome, but it requires configuration in **Windows Internet Options**:

1. Enable **Integrated Windows Authentication**.
2. Verify that Tableau Server URL is in the local intranet zone.

   Internet Explorer can sometimes detect intranet zones and configure this setting. If it has not detected and configured the Tableau Server URL, you must manually add the URL to the local intranet zone.

To enable Integrated Windows Authentication:

1. In Windows Control Panel, open **Internet Options**.
2. On the **Advanced** tab scroll down to the **Security** section.
3. Select **Enable Integrated Windows Authentication**.
4. Click **Apply**.

To verify or add the Tableau Server URL to the local intranet zone:

1. In Windows Control Panel, open **Internet Options**.
2. On the **Security** tab, select **Local intranet**, and then click **Sites**.
3. On the **Local intranet** dialog box, click **Advanced**.

   In the **Websites** field, look for the internal Tableau Server URL.

   In some organizations, IT administrators will use a wildcard (*) to specify internal URLs. For example, the following URL includes all servers in the internal **example.lan** namespace in the local intranet zone:

   `https://*.example.lan`
The following image shows a specific URL of https://tableau.example.lan.

![Image showing a specific URL](image_url)

4. If the Tableau Server URL or a wildcard URL is not specified in the Websites field, enter the Tableau Server URL in the **Add the website to the zone** field, click **Add**, and then click **OK**.

   If the Tableau Server URL is already listed in **Websites**, you can simply close the dialog.

**Note 2: Firefox on Windows or Mac OS X desktop**

You can use Firefox with Kerberos SSO on either Windows or Mac to sign in to Tableau Server. To do this, you must complete the following steps to configure Firefox to support Kerberos:

1. In Firefox, enter `about:config` in the address bar.

2. Click **I'll be careful, I promise** when warned about changing advanced settings.

3. Enter `negotiate` in the **Search** box.
4. Double-click `network.negotiate-auth.allow-non-fqdn`, and then set the value to `true`.

5. Double-click `network.negotiate-auth.trusted-uris` and enter the Tableau Server fully qualified domain name (FQDN). For example, `tableau.example.com`.

**Note 3: Chrome on Mac OS X desktop**

According to Chrome documentation, Kerberos SSO works on a Mac when you launch Chrome from a terminal window with the following command:

```
open -a "Google Chrome.app" --args --auth-server-whitelist="tableauserver.example.com"
```

where `tableauserver.example.com` is the URL for Tableau Server in your environment.

However, we have found inconsistent results in our testing. Therefore, if you want to use Kerberos SSO on a Mac, we recommend that you use Safari or Firefox. For more information, see the *Integrated Authentication* section at [HTTP authentication](http://projects.chromium.org) on The Chromium Projects site.
Note: Users can still use Chrome on Mac OS X to sign in to Tableau Server, but they might be prompted to enter their user name and password (single sign-on may not work).

Note 4: Mobile Safari or Tableau Mobile on Mac iOS

Kerberos SSO is supported if iOS is configured for Kerberos. The iOS device must have a Kerberos authentication configuration profile installed. This is usually done by an enterprise IT group. Tableau Support cannot assist with configuring iOS devices for Kerberos.

Note 5: Android platform

Kerberos SSO is not supported on the Android operating system because there is no platform-level support for Kerberos. You can still use your Android device and the Tableau Mobile app or a supported mobile browser to connect to and sign in to Tableau Server.

Troubleshoot Kerberos

The troubleshooting suggestions in this topic are divided into issues related to single sign-on (SSO) on the server and issues with the delegated data sources.

Single sign-on to Tableau Server

In a Kerberos SSO environment, a user signing in to Tableau Server from a web browser or Tableau Desktop might see a message indicating that Tableau Server can’t sign them in automatically (using single sign-on). It suggests that they provide a Tableau Server user name and password instead.
Troubleshooting sign-in errors on the client computer

- **Enter the user name and password**—To check the user's general access to Tableau Server, sign in by entering the user’s name and password.

  If these credentials fail, the user might not be a user on Tableau Server. For Kerberos SSO to work, the user must be able to access Tableau Server, and they must be granted a Ticket Granting Ticket (TGT) by Active Directory (as described in the TGT item later in this list).

- **Check other users' SSO credentials**—Try to connect with SSO to Tableau Server using other user accounts. If all users are affected, the problem might be in the Kerberos configuration.

- **Use a computer other than the server computer**—Kerberos SSO does not work when you sign in to Tableau Server on localhost. Clients must connect from a computer other than the Tableau Server computer.

- **Use a server name, not IP address**—Kerberos SSO does not work if you enter an
IP address as the Tableau Server name. In addition, the server name you use to access Tableau Server must match the name used in the Kerberos configuration (see Key table entry, below).

- **Confirm that the client has TGT**—The client computer must have a TGT (Ticket Granting Ticket) from the Active Directory domain. Constrained delegation, with the proxy granting a ticket, is not supported.

To confirm the client computer has a TGT, do the following:

- On Windows, open a command prompt and type the following: `klist tgt`
- On the Mac, open a terminal window and type the following: `klist`

The output should show a TGT for the user/domain trying to authenticate to Tableau Server.

The client computer might not have a TGT in the following circumstances:

- The client computer is using a VPN connection.
- The client computer is not joined to the domain (for example, it is a non-work computer being used at work).
- The user signed in to the computer with a local (non-domain) account.
- The computer is a Mac that is not using Active Directory as a network account server.

- **Confirm browser version and settings**—For web browser sign-in, make sure the browser is supported for Kerberos and, if necessary, is configured correctly.

  - Internet Explorer (IE) and Chrome work “out of the box” on Windows.
  - Safari works “out of the box” on the Mac.
  - Firefox requires additional configuration.
Troubleshooting sign-in errors on the server

If you cannot solve the problem from the client computer, your next steps are to troubleshoot on the computer running Tableau Server. The administrator can use the request ID to locate the sign-in attempt in the Apache logs on Tableau Server.

- **Log files**—Check the Apache error.log for an error with the exact time/date of the failed sign-in attempt.

- **Key table entry**—If the error.log entry includes the message, “No key table entry matching HTTP/<servername>.<domain>.<org>@”, for example:

  [Fri Oct 24 10:58:46.087683 2014] [:error] [pid 2104:tid 4776] [client 10.10.1.62:56789] gss_acquire_cred() failed: Unspecified GSS failure. Minor code may provide more information (, No key table entry found matching HTTP/server-name.domain.com@)

  This error is a result of a mismatch of any of the following:

  - **Tableau Server URL** - The URL used by the client computer to access the server.

    This is the name that you type into Tableau Desktop or a browser address bar. It could be a shortname (http://servername) or a fully-qualified domain name (http://servername.domain.com)
**DNS reverse lookup** for the server IP address.

This looks up a DNS name using an IP address.

At a command prompt type:

```bash
ping servername
```

with the IP address returned by pinging the server, do a reverse DNS lookup type:

```bash
nslookup <ip address>
```

The nslookup command will return network information for the IP address. In the *Non-authoritative answer* portion of the response, verify that the fully qualified domain name (FQDN) matches the following configured values:

- The Kerberos .keytab file
- Service Principal Name (SPN) for the server

For more information about configuring these values, see Understanding Keytab Requirements.

**Verify Kerberos configuration script**

You may need to modify the ktpass command that you used to generate the keytab file for environmental variables. Review the troubleshooting steps in the Knowledge Base article, *Unable to Generate Kerberos Script Configuration for Tableau Server*.

**Data source SSO**

**Delegated data source access failures**

Check the vizqlserver log files for "workgroup-auth-mode."

Look for "workgroup-auth-mode" in the log files. It should say "kerberos-impersonate" not "as-is".
Kerberos delegation multi-domain configuration

Tableau Server can delegate users from other Active Directory domains. If your database uses MIT Kerberos, you may need to adjust your Kerberos principal to database user mapping. Specifically, you will need to update krb5.conf with rules for each Kerberos realm that users will connect from. Use the `auth_to_local` tag in the `[realms]` section to map principal names to local user names.

For example, consider a user, EXAMPLE\jsmith, whose Kerberos Principal is jsmith@EXAMPLE.LAN. In this case, Tableau Server will specify a delegated user, jsmith@EXAMPLE. Tableau Server will use the Active Directory legacy domain alias as the Kerberos Realm.

The target database may already have a rule such as the following to map the user, jsmith@EXAMPLE.LAN to the database user, jsmith.

```plaintext
EXAMPLE.LAN = {
  RULE:[1:$1@$0](.*@EXAMPLE.LAN)s/@.*//
  DEFAULT
}
```

To support delegation, you must add another rule to map jsmith@EXAMPLE to a database user:

```plaintext
EXAMPLE.LAN = {
  RULE:[1:$1@$0](.*@EXAMPLE.LAN)s/@.*//
  RULE:[1:$1@$0](.*@EXAMPLE)s/@.*//
  DEFAULT
}
```

See the MIT Kerberos Documentation topic, `krb5.conf`, for more information.
Cross-domain constrained delegation

In some cross-domain scenarios where the KDC is running on a Windows Server prior to Windows 2012, delegation may fail. Errors you may see include:

- SQL Server Network Interfaces: The system cannot contact a domain controller to service the authentication request. Please try again later.
- SQL Server Native Client: Cannot generate SSPI context
- The Domain Controller returns: KRB-ERR-POLICY error with a status STATUS_CROSSREALM_DELEGATION_FAILURE (0xc000040b).

Cross-domain refers to a scenario where Tableau Server is running in a different domain than the data source with different service accounts. For example:

- Tableau Server runs on DomainA with DomainA service account.
- SQL Server runs on DomainB with DomainB service account.

Traditional constrained delegation only works if both servers are in the same domain. The user can come from other domains.

If you are seeing the errors noted above, then to enable this scenario, your Active Directory administrator should remove any traditional constrained delegation which is configured on the delegating account. Removing delegation can be achieved with Active Directory management tools or by removing the values associated with the Active Directory property, msDS-AllowedToDelegateTo.

If you want to preserve an existing single domain delegation alongside cross-domain delegation, you must configure both using resource-based constrained delegation.

The article, How Windows Server 2012 Eases the Pain of Kerberos Constrained Delegation, Part 2, provides a detailed description of how Microsoft KDC and Active Directory handle delegated scenarios. To configure these scenarios, refer to the Microsoft Kerberos documentation.
Configure Mutual SSL Authentication

Using mutual SSL, you can provide users of Tableau Desktop and other approved Tableau clients a secure, direct-access experience to Tableau Server. With mutual SSL, when a client with a valid SSL certificate connects to Tableau Server, Tableau Server confirms the existence of the client certificate and authenticates the user, based on the user name in the client certificate. If the client does not have a valid SSL certificate, Tableau Server can refuse the connection. You can also configure Tableau Server to fall back to username/password authentication if mutual SSL fails.

Mutual SSL authentication is not supported on Tableau Mobile.

Use the TSM web interface

1. Configure SSL for External HTTP Traffic to and from Tableau Server.

2. Open TSM in a browser:

   https://<tsm-computer-name>:8850. For more information, see Sign in to Tableau Services Manager Web UI.


4. Under Authentication Method, select Mutual SSL in the drop-down menu.

5. Under Mutual SSL, select Use mutual SSL and automatic sign in with client certificates.

6. Click Select File and upload your certificate authority (CA) issued certificate to the server.

   This certificate must be a valid PEM-encoded x509 certificate with the extension .crt.

7. Enter remaining SSL configuration information for your organization.
Username format: When Tableau Server is configured for mutual SSL, the server gets the user name from the client certificate, so it can establish a direct sign-in for the client user. The name that Tableau Server uses depends on how Tableau Server is configured for user authentication:

- Local Authentication—Tableau Server uses the UPN (User Principal Name) from the certificate.
- Active Directory (AD)—Tableau Server uses LDAP (Lightweight Directory Access Protocol) to get the user name.

Alternatively, you can set Tableau Server to use the CN (Common Name) from the client certificate.

8. Click **Save Pending Changes** after you've entered your configuration information.

9. Click **Pending Changes** at the top of the page:

10. Click **Apply Changes and Restart**.
Use the TSM CLI

Step 1: Require SSL for external server communication

To configure Tableau Server to use SSL for external communication between Tableau Server and web clients, run the `external-ssl enable` command as follows, providing the names for the server certificate’s .crt and .key files:

```
tsm security external-ssl enable --cert-file <file.crt> --key-file <file.key>
```

- For `--cert-file` and `--key-file`, specify the location and file name where you saved the server’s CA-issued SSL certificate (.crt) and key (.key) files.
- The above command assumes the you are signed in as a user that has the **Server Administrator** site role on Tableau Server. You can instead use the `-u` and `-p` parameters to specify an administrator user and password.
- If the certificate key file requires a passphrase, include the `--passphrase` parameter and value.

Step 2: Use mutual SSL

Add mutual authentication between the server and each client, and allow for Tableau client users to be authenticated directly after the first time they provide their credentials.

1. Run the following command:

   ```
tsm authentication mutual-ssl configure --cert-file <file.crt>
   ```

   For `--cert-file`, specify the location and file name of the server’s CA certificate (.crt) file, as in the previous step for external SSL.

   See the remaining sections in this article for any additional options you might want to include with the `mutual-ssl configure` command.

2. Run the following commands to enable mutual SSL and apply the changes:
The pending-changes apply command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the --ignore-prompt option, but this does not change the restart behavior. For more information, see tsm pending-changes apply.

Additional options for mutual SSL

You can use tsm authentication mutual-ssl configure to configure Tableau Server to support the following options.

For more information, see tsm authentication mutual-ssl <commands>.

Fallback authentication

When Tableau Server is configured for mutual SSL, authentication is automatic and clients must have a valid certificate. You can configure Tableau Server to allow a fallback option, to accept user name and password authentication.

tsm authentication mutual-ssl configure -fb true

Tableau Server accepts username and password authentication from REST API clients, even if the above option is set to false.

User name mapping

When Tableau Server is configured for mutual SSL, the server authenticates the user directly by getting the user name from their client certificate. The name that Tableau Server uses depends on how the server is configured for user authentication:

- **Local Authentication**—uses the UPN (User Principal Name) from the certificate.

- **Active Directory (AD)**—uses LDAP (Lightweight Directory Access Protocol) to get
Tableau Server on Linux Administrator Guide

the user name.

You can override either of these defaults to set Tableau Server to use the common name.

```
tsm authentication mutual-ssl configure -m cn
```

For more information, see Mapping a Client Certificate to a User During Mutual Authentication

Certificate Revocation List (CRL)

You might need to specify a CRL if you suspect that a private key has been compromised, or if a certificate authority (CA) did not issue a certificate properly.

```
tsm authentication mutual-ssl configure -rf <revoke-file.pem>
```

Mapping a Client Certificate to a User During Mutual Authentication

When you use mutual (two-way) SSL authentication, the client presents its certificate to Tableau Server as part of the authentication process. Tableau Server then maps user information in the client certificate to a known user identity. The strategy that Tableau Server uses to perform client mapping depends on the content of your organization’s client certificates.

This topic discusses the ways information in a client certificate can map to a user identity and how to change the way Tableau Server performs that mapping. To understand how the mapping happens and whether you need to change it, you must know how client certificates are structured in your organization.

- User-name mapping options
- Change the certificate mapping
- Address user-name ambiguity in multi-domain organizations

User-name mapping options

Tableau Server uses one of the following approaches to map a client certificate to a user identity:
- **Active Directory.** If Tableau Server is configured to use Active Directory for user authentication, when Tableau Server receives a client certificate, it passes the certificate to Active Directory, which maps the certificate to an Active Directory identity. Any explicit user name information in the certificate is ignored.

  **Note:** This approach requires client certificates to be published for the user accounts in Active Directory.

- **User principal name (UPN).** A client certificate can be configured to store the user name in the user principal name field. Tableau Server reads the UPN value and maps it to a user in Active Directory or to a local user.

- **Common name (CN).** A client certificate can be configured to store the user name in the common name field of the certificate. Tableau Server reads the CN value and maps it to a user in Active Directory or to a local user.

  If you configure the server for Active Directory authentication and UPN or CN user-name mapping, put the user name in one of the following formats:

  `username`, `domain/username`, or `username@domain`.

  **For example:** `asmith`, `example.org/asmith`, or `asmith@example.org`.

  If the server uses local authentication, the format of the name in the UPN or CN fields is not predetermined, but the name in the field must match a user name on the server.

  Change the certificate mapping

  You use the `tsm authentication mutual-ssl <commands>` commands to map a client certificate to a user identity in Tableau Server:

  `tsm authentication mutual-ssl configure -m <value>`

  Possible values are `ldap` for Active Directory mapping, `upn` for UPN mapping, or `cn` for CN mapping.
When you first install and configure Tableau Server, the server sets the default user-name mapping to match the server’s authentication type:

- If the server is configured to use Active Directory, it also uses Active Directory for mapping the certificate to the user identity.

- If the server is configured to use local authentication, the server gets the user-name value from the UPN field in the certificate.

If the default behavior for how Tableau Server maps a user name to an identity is not correct for your server configuration, run the following set of commands to change the mapping to use the CN value:

```bash
tsm authentication mutual-ssl configure -m cn
tsm pending-changes apply
```

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

Address user-name mapping ambiguity in multi-domain organizations

Under some circumstances, the user name in a certificate’s UPN or CN field can be ambiguous. This ambiguity can lead to unexpected results when the user name is mapped to a user identity on the server.

For example, if Tableau Server is presented with a user name that does not include a domain, the server maps the user name to an identity using the default domain. This can cause an incorrect user-name mapping, potentially assigning a user a different user’s identity and permissions.

This can occur particularly in environments where the following conditions apply:
• Your organization supports multiple Active Directory domains.

• The server is configured to use Active Directory authentication.

• The server is configured to use UPN or CN mapping.

• Some users have the same user name but different domains. For example, asmith@example.org and asmith@example.com.

• The user name in the certificate’s UPN or CN fields does not include the domain as part of the user name—for example, it shows asmith.

To avoid incorrect user-name mapping, make sure the client certificates include fully qualified user names with the domain, using the format asmith@example.org or example.org/asmith.

OpenID Connect

You can configure Tableau Server to support OpenID Connect for single sign-in (SSO). OpenID Connect is a standard authentication protocol that lets users sign in to an identity provider (IdP) such as Google. After they’ve successfully signed in to their IdP, they are automatically signed in to Tableau Server.

Configuring OpenID Connect involves several steps. The topics in this section provide general information about using Tableau Server with OpenID Connect, and provide a sequence for configuring the IdP and Tableau Server.

Authentication overview

This section describes the OpenID Connect authentication process with Tableau Server.
Step 1: A user attempts to log in to Tableau Server from a client computer.

Step 2: Tableau Server redirects the request for authentication to the IdP gateway.

Step 3: The user is prompted for credentials and successfully authenticates to the IdP. The IdP responds with a redirect URL back to Tableau Server. The redirect URL includes an authorization code for the user.

Step 4: The client is redirected to Tableau Server and presents the authorization code.

Step 5: Tableau Server presents the client's authorization code to the IdP along with its own client credentials. Tableau Server is also client of the IdP. This step is intended to prevent spoofing or man-in-the-middle attacks.

Step 6: The IdP returns an access token and an ID token to Tableau Server.
- **JSON Web Token (JWT) validation:** By default Tableau Server performs a validation of the IdP JWT. During discovery, Tableau Server retrieves the public keys specified by the `jwks_uri` in the IdP configuration discovery document. Tableau Server validates the ID token for expiry and then verifies the JSON web signature (JWS), the issuer (IdP), and the client ID. You can learn more about the JWT process in the OpenID documentation, 10. Signatures and Encryption, and the IETF proposed standard, JSON Web Token. We recommend leaving JWT validation enabled, unless your Idp does not support it.

- **The ID token is a set of attribute key-pairs for the user.** The key-pairs are called *claims*. Here is an example IdP claim for a user:

```json
"sub" : "7gYhRR3HiRRCaRcgvY50ubrtjGQBMMJW4rXbpPFpg2cptHP62m2sqowM7G1LwjN5"
"email" : "alice@tableau.com",
"email_verified" : true,
"name" : "Alice Adams",
"given_name" : "Alice",
"family_name" : "Adams",
"phone_number" : "+359 (99) 100200305",
"profile" : "https://t-
ableau.com/users/alice"
```

**Step 7: Tableau Server identifies the user from the IdP claims and completes the authentication request from Step 1.** Tableau Server searches for the user's account record stored in the repository by matching the "sub" (subject identifier) to identify the correct user account. If no user account is stored with the sub claim value, then Tableau Server searches for a username in the repository that matches the "email" claim from the IdP. When a username match succeeds, Tableau Server will store the corresponding sub claim to the user's record in the repository. Tableau Server can be configured to use different claims for this process. See Requirements for Using OpenID Connect.

**Step 8: Tableau Server authorizes the user.**
How Tableau Server Works with OpenID Connect

OpenID Connect is a flexible protocol that supports many options for the information that's exchanged between a service provider (here, Tableau Server) and an IdP. The following list provides details about the Tableau Server implementation of OpenID Connect. These details can help you understand what types of information Tableau Server sends and expects, and how to configure an IdP.

- Tableau Server supports only the OpenID Authorization Code Flow as described in the OpenID Connect final specification.

- Tableau Server relies on using discovery or a provider URL to retrieve the OpenID Provider metadata. Alternatively, you can host a static discovery document on Tableau Server. For more information see Configure Tableau Server for OpenID Connect.

- Tableau Server supports only the `client_secret_jwt` Client Authentication method specified in the OpenID Connect specification. In addition, Tableau Server supports only RSA Asymmetric Encryption for handling the JWT. However, you can turn off JWT validation. See tsm authentication openid <commands>.

- Tableau Server expects a `kid` value in the `id_token` attribute's JOSE Header. This value is matched with one of the keys found in the JWK Set document, whose URI is specified by the `jwks_uri` value in the OpenID discovery document. A `kid` value must be present even if there is only one key in the JWK Set document.

- Tableau Server does include OpenID support for the JWK `x5c` parameter or for using X.509 certificates.

Requirements for Using OpenID Connect

This topic describes the requirements to use OpenID Connect with Tableau Server.

IdP account

You must have access to an identity provider (IdP) that supports the OpenID Connect (OIDC) protocol. You must also have an account with the IdP. OpenID Connect is supported
by many identity providers. The OIDC protocol is an open and flexible standard, and as such, not all implementations of the standard are identical. As you configure Tableau Server for OIDC, work with your IdP.

The Google IdP implementation has been extensively tested with Tableau Server and is the model IdP for the configuration documented in these topics.

Local authentication

To use OpenID Connect on Tableau Server, the server must be configured to use local authentication—that is, the server must be configured so that you explicitly create users on the Tableau Server, rather than importing them from Active Directory. Active Directory authentication is not supported with OpenID.

IdP claims: mapping users

To sign in successfully to Tableau Server, a given user must be provisioned in OpenID and then mapped to a user account on Tableau Server. OpenID uses a method that relies on claims to share user account attributes with other applications. Claims include user account attributes such as email, phone number, given name, etc. To understand how Tableau Server maps IdP claims to user accounts, see Authentication overview.

Tableau Server relies on the IdP claims to map user accounts from the IdP to those hosted on Tableau Server. By default, Tableau Server expects the IdP to pass the email claim. Depending on your IdP, you may need to configure Tableau Server to use a different IdP claim.

If you are using Google as an IdP, then use the default, email claim to map IdP identities to Tableau Server user accounts. If you are not using Google as an IdP, then work with your IdP to determine the claim for which you should configure Tableau Server.

**Default: using email claim to map users**

By default, the user’s user name in Tableau Server must match the email claim in the IdP ID token. Therefore, in the default configuration, you must use email addresses (also referred to as UPN) as the username in Tableau Server. If you use Google as the IdP, the
user name in Tableau Server must be the user's Gmail address (alice@gmail.com). Using a complete email address helps to guarantee the uniqueness of the user name in Tableau Server, even when two users have the same email but are on different email hosts.

**Note:** When you create a user identity in Tableau Server, you specify a user name, password, and optionally an email address. For using OpenID Connect in the default configuration, the user name (expressed as an email address) is the value that must match the user's name in the IdP. The optional email address in the Tableau Server user identity is not used for OpenID authentication.

**Ignoring the domain name**

You can configure Tableau to ignore the domain portion of an email address when matching the IdP email claim to a user account on Tableau Server. In this scenario, the email claim in the IdP might be alice@example.com, but this will match a user named alice in Tableau Server. Ignoring the domain name might be useful if you already have users defined in Tableau Server that match the user names portion of the email claim, but not the domain portions.

**Important:** We do not recommend ignoring the user domain name without taking precautions. Specifically, verify that user names are unique across the configured domains that you’ve created in your IdP.

Setting Tableau Server to ignore the user domain name has the potential to result in unintended user log on. Consider the case where your IdP has been configured for multiple domains (example.com and tableau.com). If two users with the same first name, but different user accounts (alice@tableau.com and alice@example.com) are in your organization, then the first one to complete the OpenID provisioning sequence will claim the sub mapping in the IdP. If the wrong user is mapped, then the other user will be unable to log on until the associated sub value is reset.
To configure Tableau Server to ignore domain names in user names from the IdP, set `tsm authentication openid configure --ignore-domain` to `true`. For more information, see `tsm authentication openid <commands>`.

When you change the `tsm authentication openid configure --ignore-domain` option to ignore the domain in user names, all user names in Tableau Server must have a domain name.

**Using custom claims to map users**

As referenced in Authentication overview, the `sub` claim is often included in IdP claims. Typically, the `sub` claim is a unique string that identifies a given user account. The benefit of using a `sub` claim is that it will not change, even if you or another admin updates other user attributes or IdP claims (email, phone number, etc) associated with that account. By default, Tableau Server identifies and verifies OpenID users according to the `sub` claim in the IdP ID token.

The OpenID `sub` claim value must be mapped to the corresponding user in Tableau Server. Since the `sub` claim is an arbitrary string, a different claim is used to associate accounts during the first sign-in session. The first time a user signs in to Tableau Server with OpenID, Tableau will match the OpenID user account to a corresponding user account on Tableau. By default, Tableau will use the IdP claim, `email`, to identify the Tableau user. Tableau will then update that user’s record with the `sub` claim from OpenID. Since the ID token always includes the `sub` claim along with other claims, on subsequent sessions, Tableau will identify that user with the `sub` claim only.

For some organizations, mapping user names with the email address is not reliable or not supported by the IdP. Beginning with Tableau Server 10.2, you can map user accounts from any arbitrary IdP claim to the Tableau Server username.

The IdP claim you are using must map exactly to a corresponding Tableau Server username. In the example below, the username is `kwilliams`. 
To change the IdP claim that is used to map identity on Tableau Server, use the `tsm authentication openid map-claims --user-name` command. For more information, see `tsm authentication openid <commands>`.

**Changing the `sub` Claim**

As described above, the `sub` claim is the identifier that Tableau Server uses to identify users after the initial mapping session. The `sub` claim is written to the corresponding user account in Tableau Server. If your IdP does not provide a `sub` claim, then you can specify an arbitrary claim to use instead. Like `sub`, the claim value you specify must be unique and should not change when other user claims are updated.
To specify a different IdP claim for default sub claim, use the use the `tsm authentication openid map-claims --id` command. For more information, see `tsm authentication openid <commands>`.

Where `arbitraryClaim` is the name of the IdP claim that you want to use as the replacement for the sub claim.

Configure the Identity Provider for OpenID Connect

This topic provides information about configuring an identity provider (IdP) to use OpenID Connect with Tableau Server. This is one step in a multi-step process. The following topics provide information about configuring and using OpenID Connect with Tableau Server.

- OpenID Connect
- Configure the Identity Provider for OpenID Connect (you are here)
- Configure Tableau Server for OpenID Connect
- Signing In to Tableau Server Using OpenID Connect

Configure the IdP

Before you can use OpenID Connect with Tableau Server, you must have an account with an identity provider (IdP) and a project or application with the IdP. When you configure Tableau Server, you will need to be able to provide the following information:

- Provider client ID. This is the identifier that the IdP assigned to your application.
- Provider client secret. This is a token that is used by Tableau to verify the authenticity of the response from the IdP. This value is a secret and should be kept securely.
- Provider configuration URL. This is the URL at the provider’s site that Tableau Server should send authentication requests to.
Redirect URL

Some IdPs will require a redirect URL for your Tableau Server. You can manually construct your URL for the IdP using the following syntax:

<protocol>://<host>/vizportal/api/web/v1/auth/openIdLogin

For example, https://tableau.example.com/vizportal/api/web/v1/auth/openIdLogin.

Example IdP process

The following procedure provides an outline of the steps that you follow with the provider. As an example, the procedure discusses using Google as a provider. However, each provider has a somewhat different flow, so the specifics of the steps (and their order) might vary depending on your provider.

1. Register at the provider’s developer site and sign in. For example, for Google, you can go to the Developers Console at this URL: https://console.developers.google.com

2. Create a new project, application, or relying party account.

3. In the developer dashboard, follow the steps for getting an OAuth 2.0 client ID and client secret. Record these values for later.

   **Note:** Keep the client secret in a secure place.

4. On the developer site, find the URL of the endpoint that the IdP uses for OpenID Connect discovery. For example, Google uses the URL https://accounts.google.com/.well-known/openid-configuration. Record this URL for later.

   Alternatively, if your IdP has provided you with a static discovery document, copy that file to a local directory on the Tableau Server for later.
Configure Tableau Server for OpenID Connect

This topic describes how to configure Tableau Server to use OpenID Connect for single-sign on (SSO). This is one step in a multi-step process. The following topics provide information about configuring and using OpenID Connect with Tableau Server.

- OpenID Connect
- Configure the Identity Provider for OpenID Connect
- Configure Tableau Server for OpenID Connect (you are here)
- Signing In to Tableau Server Using OpenID Connect

**Note**: Before you perform the steps described here, you must configure the OpenID identity provider (IdP) as described in Configure the Identity Provider for OpenID Connect.

Use the TSM web interface

1. Open TSM in a browser:

   https://<tsm-computer-name>:8850. For more information, see Sign in to Tableau Services Manager Web UI.

2. Click User **Identity & Access** on the **Configuration** tab and then click **Authentication Method**.


4. Under OpenID Connect, select **Enable OpenID authentication for the server**.

5. Enter the OpenID configuration information for your organization:
Note: If your provider relies on a configuration file hosted on the local computer (rather than a file hosted at a public URL), you can specify the file with the tsm authentication openid <commands>. Use the --metadata-file <file_path> option to specify a local IdP configuration file.

6. Click Save Pending Changes after you’ve entered your configuration information.

7. Click Pending Changes at the top of the page:

8. Click Apply Changes and Restart.

Use the TSM CLI

The procedure in this section describes how to use TSM command line interface to configure OpenID Connect. You can also use a configuration file for the initial configuration of OpenID
1. Use the `configure` command of `tsm authentication openid <commands>` to set the following required options:

   `--client-id <id>`: Specifies the provider client ID that your IdP has assigned to your application. For example, “laakjwdlnaioiloadjkwha”.

   `--client-secret <secret>`: Specifies the provider client secret. This is a token that is used by Tableau to verify the authenticity of the response from the IdP. This value is a secret and should be kept securely. For example, “fwah-fkjaw72123=".

   `--config-url <url> or --metadata-file <file_path>`: Specifies location of provider configuration json file. If the provider hosts a public json discovery file, then use `--config-url`. Otherwise, specify a path on the local computer and file name for `--metadata-file` instead.

   `--return-url <url>`: The URL of your server. This is typically is the public name of your server, such as "http://example.tableau.com".

   For example, run the command:

   
   ```
   tsm authentication openid configure --client-id "laakjwdlnaioiloadjkwha" --client-secret "fwah-fkjaw72123="
   --config-url "https://example.com/openid-configuration"
   return-url "http://tableau.example.com"
   ```

   There are additional, optional configurations that you can set for Open ID Connect using either `openIDSettings Entity` or `tsm authentication openid <commands>`. In addition, if you need to configure IdP claim mapping, see Options for `openid map-claims`.

2. Type the following command to enable Open ID Connect:

   ```
   tsm authentication openid enable
   ```
3. Run `tsm pending-changes apply` to apply changes.

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

Signing In to Tableau Server Using OpenID Connect

This topic provides information about signing in to Tableau Server using OpenID Connect. The following topics provide information about configuring and using OpenID Connect with Tableau Server.

- OpenID Connect
- Configure the Identity Provider for OpenID Connect
- Configure Tableau Server for OpenID Connect
- Signing In to Tableau Server Using OpenID Connect (you are here)

Signing in using OpenID Connect

After Tableau Server has been configured to use OpenID Connect, users who access the server and aren't already signed in are redirected to the IdP site, where they are prompted to sign in. Users enter the credentials that they have with the IdP. In many cases, the user is also asked to authorize the IdP to share information with Tableau Server, as in the following example:
When a user signs in using OpenID Connect, the IdP sends a unique user identifier (known in OpenID as the sub value) as part of the information that's redirected to Tableau Server. This sub value is associated with the user's Tableau user identity.

Restricting sign-in to server administrators for command-line tools

Command-line tools for working with Tableau Server (tabcmd, TSM, and tableau.com) do not support sign-in using OpenID Connect. When OpenID Connect is enabled for the server, these tools still require sign-in using a Tableau Server username and password.

Even if users normally authenticate using OpenID Connect, each user has a Tableau Server username and password. This means that users could use command-line tools like tabcmd. As a security measure, you can make sure that only server administrators can use command-line tools. To do this, use `tsm configuration set to set wgserv- er.authentication.restricted to true`. When this setting is true, only server administrators can sign in to Tableau Server using a username and password; all other users must sign in to the server using a single sign-on (SSO) option like OpenID Connect.
The effect is that users who are not administrators also cannot then use command-line tools. To make this change, run the following sequence of TSM commands:

```
tsm configuration set -k wgserver.authentication.restricted -v true
tsm pending-changes apply
```

OpenID Connect Authentication Request Parameters

The OpenID authentication request sent from Tableau Server passes information using a limited set of parameters, as listed in this topic. If your OpenID IdP requires parameters that are not in the following list, it is not compatible for use with Tableau Server.

- **scope.** This value specifies a profile that tells the IdP what user information claims to return. This value can be configured by a Tableau Server administrator. The default value is "openid email profile". For more information, see Configure the scope value later in this document.

- **response_type.** OpenID Connect supports multiple flows. This value tells the IdP which flow Tableau Server expects. Tableau supports only the authorization code flow, and the value is always set to "code".

- **client_id.** This value specifies the server’s ID (Provider client ID in the Tableau Server Configuration dialog box), which lets the IdP knows where the request came from. It is provided by the IdP when the service is registered. The value is configurable by a Tableau Server administrator.

- **redirect_uri.** This value specifies the URL that the IdP redirects to after the user has authenticated using OpenID Connect. The URL must include the host and protocol (for example, http://example.tableau.com), but Tableau provides the URL endpoint.

- **nonce.** Tableau Server generates a nonce value to verify that the client that it redirected to matches the entity that comes back from the IdP.
Configure the scope value

The `scope` value indicates to the IdP the information that Tableau Server requests about the user. By default, Tableau Server sends the value "openid profile email". This indicates that Tableau uses OpenID to authenticate (this part of the `scope` attribute value must always be included) and that Tableau Server is requesting the user profile and email information during the exchange of the user authorization code.

If this default scope is not appropriate for your scenario, you can have Tableau Server request custom information about the user. To do so, you configure the IdP with a custom profile (for example, something like "tableau-scope"). You can then configure Tableau Server to send the scope request using the name of the custom profile.

To change the scope value that Tableau Server requests, use the following TSM CLI command:

```
tsm authentication openid configure --custom-scope-name custom-scope-name
```

**Note**: Tableau Server always includes "openid" as part of the scope value (even if you don't include it in the `custom_scope` setting).

Troubleshoot OpenID Connect

Use the following topics to troubleshoot OpenID Connect (OIDC) issues in Tableau Server.

OpenID Connect protocol is supported by many identity providers. The OIDC protocol is an open and flexible standard, and as such, not all implementations of the standard are identical. Most issues that administrators encounter when configuring Tableau Server for OIDC are the result of how different identity providers implement OIDC. If you encounter errors as you set up OIDC with Tableau Server, we recommend that you work with your IdP to resolve them.
Signing In from the Command Line

Even if Tableau Server is configured to use OpenID, it is not used if you sign in to Tableau Server using tabcmd, the REST API, or the Tableau Data Extract command line utility (provided with Tableau Desktop).

Login Failed

Login can fail with the following message:

Login failure: Identity Provider authentication successful for user <username from IdP>. Failed to find the user in Tableau Server.

This error typically means that there is a mismatch between a username stored in Tableau Server and the username provided by the IdP. To fix this, make sure that they match. For example, if Jane Smith’s username is stored in the IdP as jsmith it must be stored in Tableau Server as jsmith as well.

Error 69: "Unable to Sign In"

An error 69 may be returned when you attempt to sign in to Tableau Server with a web browser and receive an error, "Unable to Sign In. Sign in failed. Contact your Tableau Server administrator." The URL that returns this message is https://example.-com/#!/error/signin/69?redirectPath=%2.

If you receive this error, check with your IDP provider to verify if the IdP is expecting client_secret_post instead of client_secret_basic (the Tableau default).

If the IdP is expecting client_secret_post, then you must set the vizportal.openid.client_authentication parameter to client_secret_post.

For example: If you receive this error and you have configured OIDC for the Salesforce IdP, then you must set the vizportal.openid.client_authentication parameter.

See tsm configuration set Options for more information.
OpenID Error Log

OpenID authentication takes place outside Tableau Server, so troubleshooting authentication issues can be difficult. However, sign-in attempts are logged by Tableau Server. You can create a snapshot of log files and use them to troubleshoot problems. For more information, see Server Log File Locations.

**Note:** To log OpenID-related events, `vizportal.log.level` must be set to `debug` with `tsm configuration set Options`.

Check for OpenID errors in the following files in the unzipped log file snapshot:

`\vizportal\vizportal-<n>.log`

**Trusted Authentication**

When you embed Tableau Server views into webpages, everyone who visits the page must be a licensed user on Tableau Server. When users visit the page they are prompted to sign in to Tableau Server before they can see the view. If you already have a way of authenticating users on the webpage or within your web application, you can avoid this prompt and save your users from having to sign in twice by setting up trusted authentication.

Trusted authentication simply means that you have set up a trusted relationship between Tableau Server and one or more web servers. When Tableau Server receives requests from these trusted web servers it assumes that your web server has handled whatever authentication is necessary.

If your web server uses SSPI (Security Support Provider Interface), you do not need to set up trusted authentication. You can embed views and your users will have secure access to them as long as they are licensed Tableau Server users and members of your Active Directory.
**Note:** Client browsers must be configured to allow third-party cookies if you want to use trusted authentication with embedded views.

How Trusted Authentication Works

The diagram below describes how trusted authentication works between the client's web browser, your web server(s) and Tableau Server.

1. **User visits the webpage:** When a user visits the webpage with the embedded Tableau Server view, the webpage sends a GET request to your web server for the HTML for that page.

2. **Web server POSTS to Tableau Server:** The web server sends a POST request to the trusted Tableau Server (for example, `https://tabaserver/trusted`, not `https://tabserver`). That POST request must have a username parameter. The
username value must be the username for a licensed Tableau Server user. If Tableau Server is hosting multiple sites and the view is on a site other than the Default site, then the POST request must also include a target_site parameter.

3 **Tableau Server creates a ticket:** Tableau Server checks the IP address or host name of the web server (192.168.1.XXX in the above diagram) that sent the POST request. If the web server is listed as a trusted host then Tableau Server creates a ticket in the form of a unique string. Tickets must be redeemed within three minutes after they are issued. Tableau Server responds to the POST request with that ticket. Or if there is an error and the ticket cannot be created, then Tableau Server responds with a value of -1.

4 **Web server passes the URL to the browser:** The web server constructs the URL for the view and inserts it into the HTML for the page. The ticket is included (for example, https://tabserver/trusted/<ticket>/views/requested_view_name). The web server passes the HTML back to the client’s web browser.

5 **Browser requests view from Tableau Server:** The client web browser sends a GET request to Tableau Server that includes the URL with the ticket.

6 **Tableau Server redeems the ticket:** Tableau Server redeems the ticket, creates a session, logs the user in, removes the ticket from the URL, and then sends the final URL for the embedded view to the client.

The session allows the user to access any of the views that the user would have if they logged onto the server. In the default configuration, users authenticated with trusted tickets have restricted access such that only views are available. They cannot access workbooks, project pages, or other content hosted on the server.

To change this behavior, see the `wgserver.unrestricted_ticket` option at `tsm configuration set Options`. 
How is a trusted ticket stored?

Tableau Server stores trusted tickets in the Tableau Server repository using the following process:

1. Tableau Server generates a two-part ticket: the first part is a Base64-encoded unique ID (UUID) and the second part is a 24-character random secret string.
2. Tableau Server hashes the secret string and stores it with the unique ID in the repository. Hashing takes the secret string as input, and uses an algorithm to compute a unique string. This unique string protects the security of the secret string from unauthorized users.
3. Tableau Server sends the Base64 UUID and the original 24-character random string to the client.
4. The client returns the Base64 UUID and the original 24-character secret string to Tableau Server as part of the request for a view.
5. Tableau Server locates the string pair with the Base64 UUID, and then hashes the secret string to verify that it matches the hash stored in the repository.

This process ensures that any trusted ticket content stored on Tableau Server cannot be used to impersonate users or access content protected by authentication. However, because the full trusted ticket is sent over HTTP between Tableau Server and the client, the process relies on secure and encrypted transmission of HTTP data. Therefore, we recommend that you only deploy trusted tickets over SSL/TLS or another layer of network encryption.

Add Trusted IP Addresses or Host Names to Tableau Server

The first step in setting up trusted authentication is to configure Tableau Server to recognize and trust requests from one or more web servers:

Use the TSM web interface

1. Open TSM in a browser:
   https://<tsm-computer-name>:8850. For more information, see Sign in to Tableau Services Manager Web UI.
2. Click User **Identity & Access** on the **Configuration** tab and then click **Trusted**
3. Under **Trusted Authentication**, for each trusted host, enter the name or IP address and then click **Add**:

![Trusted Authentication]

**Notes:**
The values you specify completely overwrite any previous setting. Therefore, you must include the full list of hosts if you want to amend an existing list.

Static IP addresses are required: The web servers you specify must use static IP addresses, even if you use host names.

If you have one or more proxy servers between the computer that is requesting the trusted ticket (one of those configured in Step 2 as shown at Trusted Authentication) and Tableau Server, you also need to add them as trusted gateways using the `tsm configuration set gateway.trusted` option. See Configuring Proxies for Tableau Server for steps.

4. Enter a value in **Token Length** (Optional).
The token length determines the number of characters in each trusted ticket. The default setting of 24 characters provides 144 bits of randomness. The value can be set to any integer between 9 and 255, inclusive.

5. Click **Save Pending Changes** after you've entered your configuration information.

6. Click **Pending Changes** at the top of the page:

7. Click **Apply Changes and Restart**.

Use the TSM CLI

1. Enter the following command:

   ```
   tsm authentication trusted configure -th <trusted IP address or host name>
   ```

   In the command above, `<trusted IP address>` should be a comma-separated list of the IPv4 addresses or host names of your web server(s), with each host name or IP address in quotes.

   **Note**: The values you specify completely overwrite any previous setting. Therefore, you must include the full list of hosts in the `tsm authentication trusted configure -th` command. (You cannot amend the list of hosts by running the `tsm authentication trusted configure -th` command repeatedly.)

   For example:

   ```
   tsm authentication trusted configure -th "192.168.1.101", "192.168.1.102", "192.168.1.103"
   ```
or

tsm authentication trusted configure -th "webserv1", "web-serv2", "webserv3"

**Notes:**

Each host name or IP address in the list must be in double-quotes, followed by a comma and one space after each comma.

The web servers you specify must use static IP addresses, even if you use host names.

2. If you have one or more proxy servers between the computer that is requesting the trusted ticket (one of those configured in Step 2 as shown at Trusted Authentication) and Tableau Server, you also need to add them as trusted gateways using the tsm configuration set gateway.trusted option. See Configuring Proxies for Tableau Server for steps.

3. Type the following command to save the changes to all the server configuration files:

    tsm pending-changes apply

    The pending-changes apply command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the --ignore-prompt option, but this does not change the restart behavior. For more information, see tsm pending-changes apply.

    There are other optional trusted authentication configurations (legacy support, logging, and timeout settings) that you can make by passing a json file to Tableau Server. See trustedAuthenticationSettings Entity.

Next, you need to configure your web server to receive tickets from Tableau Server.
Get a Ticket from Tableau Server

After you’ve added trusted IP addresses to Tableau Server, you’re ready to configure your web server to get tickets from Tableau Server via POST requests (step 3 in the diagram). The POST request must be sent to http://<server name>/trusted, not http://tabserv. For example http://tabserv/trusted.

Note: If SSL is enabled you must use https instead of http. For example: https://tabserver/trusted.

Here’s the data you can use in a POST request to Tableau Server:

- **username=<username>** (required): The username for a licensed Tableau Server user. If you are using Local Authentication the username can be a simple string (for example, username=jsmith). If you are using Active Directory with multiple domains you must include the domain name with the user name (for example, username=MyCo\jsmith).

- **target_site=<site id>** (required if view not on Default site): Specifies the site containing the view if Tableau Server is running multiple sites and the view is on a site other than the Default site (for example, target_site=Sales). The value you use for <site id> should be the Site ID that was provided when the site was created. This value is case sensitive. If the Site ID is SAles, then the target_site=SAles.

- **client_ip=<IP address>** (optional): Used to specify the IP address of the computer whose web browser is accessing the view (for example, client_ip=123.45.67.891). It is not the IP address of the web server making the POST request of Tableau Server. If you decide to use this parameter, see Optional: Configure Client IP Matching for more information.

Tableau Server’s response to the POST request will be a unique string (the ticket). If Tableau Server isn’t able to process the request, the return will be -1. See Ticket Value of -1 Returned from Tableau Server for tips on how to correct this. Also, in order for users to
successfully authenticate when they click an embedded view, their browsers must be configured to allow third-party cookies.

The ticket format changed in Tableau Server 10.2. The ticket format is now a string composed of two parts. Each part is a 128 bit string that is encoded before it is returned to the client. The first part is a universally unique ID (UUID v4) that is Base64-encoded. The second part is a 24-character secure random string. The concatenation of these parts can be expressed as Base64(UUIDv4):SecureRandomString. An example of a ticket might look like this: 9D1ObyqDQmSIOyQpKdy4Sw==:dg62gCsSE0QRArXNTOp6mlJ5.

Next, you need to add code that allows the web server to construct an URL for the view that includes the view’s location and the ticket.

Display the View with the Ticket

After you create the POST request, you need to write code that provides the web server with the view’s location and the ticket from Tableau Server. It will use this information to display the view. How you specify it depends on whether the view is embedded, and if Tableau Server is running multiple sites.

Tableau Server View Examples

Here’s an example of how to specify a view that users only access via Tableau Server (the view is not embedded):

http://tabserver/trusted/<ticket>/views/<workbook>/<view>

If Tableau Server is running multiple sites and the view is on a site other than the Default site, you need to add t/<site ID> to the path. For example:

http://t-abserver/trusted/<ticket>/t/Sales/views/<workbook>/<view>

Use the same capitalization that you see in the Tableau Server URL.
Embedded View Examples

Here are some examples of how to specify embedded views. Because there are two approaches you can take with embed code, both ways are provided below. Regardless of which you use, there is some information unique to trusted authentication that you must provide. For more information, search for "Writing Embed Code" in the Tableau Server Help.

**Note:** The examples below use embed code parameters. For more information, see [Embed Code Parameters](#) in the Tableau Help.

**Script Tag Examples**

This example uses the **ticket** object parameter:

```html
<script type="text/javascript" src="http://myserver/javascripts/api/viz_v1.js"></script>
<object class="tableauViz" width="800" height="600" style="display:none;">
    <param name="name" value="MyCoSales/SalesScoreCard" />
    <param name="ticket" value="9D1ObyqDQmSI0yQpKdy4Sw==:dg62gCsSE0QRArXNTOp6mlJ5" />
</object>
```

Here's what the above example looks like for a multi-site Tableau Server, where the view is published on the **Sales** site:

```html
<script type="text/javascript" src="http://myserver/javascripts/api/viz_v1.js"></script>
<object class="tableauViz" width="800" height="600" style="display:none;">
    <param name="site_root" value="/t/Sales" />
    <param name="name" value="MyCoSales/SalesScoreCard" />
    <param name="ticket" value="
```
Instead of using ticket, you can use the path parameter to state the full path of the view explicitly. When path is used, you do not also need the name parameter, which is usually a required parameter in Tableau JavaScript embed code:

```html
<script type="text/javascript" src="http://myserver/javascripts/api/viz_v1.js"></script>
<object class="tableauViz" width="900" height="700" style="display:none;">
  <param name="path" value="trusted/9D1ObyqDQmSI0yQpKdy4Sw==:dg62gCsSE0QRArXNT0p6m1J5"/>
</object>
```

Here's the same example, but for a multi-site server. Note that /t/<site ID> is used here:

```html
<script type="text/javascript" src="http://myserver/javascripts/api/viz_v1.js"></script>
<object class="tableauViz" width="900" height="700" style="display:none;">
  <param name="path" value="trusted/9D1ObyqDQmSI0yQpKdy4Sw==:dg62gCsSE0QRArXNT0p6m1J5/t/Sales/views/MyCoSales/SalesScoreCard"/>
</object>
```

**Iframe Tag Example**

```html
<iframe src="http://tabserver/trusted/9D1ObyqDQmSI0yQpKdy4Sw==:dg62gCsSE0QRArXNT0p6m1J5/views/workbookQ4/SalesQ4?:embed=yes" width="800" height="600"></iframe>
```
Optional: Configure Client IP Matching

By default, Tableau Server does not consider the client web browser IP address when it creates or redeems tickets. To change this, you need to do two things: specify an IP address using the `client_ip` parameter in the POST request that obtains the ticket, and follow the steps below to configure Tableau Server to enforce client IP address matching.

1. Open TSM CLI and type the following command:

   ```bash
tsm configuration set -k wgserver.extended_trusted_ip_checking -v true
   ```

2. Then type the following command:

   ```bash
tsm pending-changes apply
   ```

   The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

Test Trusted Authentication

The steps below provide a method you can use to test retrieving a trusted ticket from your web server. This simple test can help evaluate connectivity between the web server and Tableau Server, and whether or not trusted authentication has been configured correctly.

Alternatively, run a trusted ticket generator to test your configuration. The following URL references a trusted ticket generator that is not supported by Tableau. However the generator has been used by many customers to test their trusted ticket configuration: https://github.com/mkannan-tsi/Trusted-Ticket-Generator.

Step 1: Add a test user

Create a user on the Tableau Server that you can use to test trusted ticket functionality. See Add Users to Tableau Server. Add that user to a site on the server, and set the user’s site
role to Explorer.

Step 2: Create a test HTML page

Paste the following code into a new .html file that you save on the web server you specified in Step 1. You can change the labels and style attributes as you prefer.

```html
<html>
<head>
<title>Trusted Ticket Requester</title>
<script type="text/javascript">
function submitForm(){
    document.getElementById('form1').action =
    document.getElementById('server').value + "/trusted";
}
</script>
<style type="text/css">
.style1 {width: 100%;}
.style2 {width: 429px;}
#server {width: 254px;}
</style>
</head>
<body>
<h3>Trusted Ticketer</h3>
<form method="POST" id="form1" onSubmit="submitForm()">
<table class="style1">
    <tr>
        <td class="style2">Username</td>
        <td><input type="text" name="username" value="" /></td>
    </tr>
    <tr>
        <td class="style2">Server</td>
        <td><input type="text" id="server" name="server" value="" /></td>
    </tr>
</table>
</form>
</body>
</html>
```
Step 3: Retrieve a trusted ticket from Tableau Server

The following procedure will return a trusted ticket from Tableau Server.
1. Open the web page that you created in the previous step.

![Trusted Ticketer](image)

This operation requires JavaScript, so the web browser might prompt you to allow scripts to run.

2. In the text boxes, enter the following:
   - **Username**: The test user that was created in Step 1.
   - **Server**: the address of your Tableau Server, e.g., `https://server_name`.
   - **Client IP (optional)**: The IP address of the user's computer, if it's configured for client trusted IP matching.
   - **Site**: The name of the Tableau Server site that the test user is a member of.

3. Click **Get Ticket**. One of the following will be returned:
   - **A unique ticket**: A trusted ticket is a string composed of a base64-encoded UUID and a 24-character random string, for example, `9D1OlxmDQmSIOyQpKdy4Sw==:dg62gCsSE0QRArXNTOp6mlJ5`.
   - **-1**: If the value, -1 is returned, the configuration contains an error. See Ticket Value of -1 Returned from Tableau Server.

**Step 4: Test access with trusted ticket**

Now that you have a ticket, you can use it to access content on Tableau Server.

Construct a URL with the unique ticket that you generated in the previous step to verify access with the trusted ticket. The URL syntax is different if you are accessing a Tableau Server with a single site vs a server that hosts multiple sites.

**Single (Default) site server url**
Tableau Server on Linux Administrator Guide

https://<server-name>/trusted/<unique-ticket>/views/<workbook-name>/<view-name>

**Non-default site server url**

https://<server-name>/trusted/<unique-ticket>/t/<site-name>/views/<workbook-name>/<view-name>

Variables in the URLs are indicated by angle brackets (< and >). All other syntax is literal.

Troubleshoot Trusted Authentication

This section includes some common issues and errors you might encounter when you’re configuring trusted authentication.

Trusted authentication information is written to /var/opt/tableau/tableau_server-/data/tabsvc/logs/vizqlserver/vizql-*.*.log.

To increase the logging level from info to debug, use the tsm configuration set Options setting vizqlserver.trustedticket.log_level.

To test your trusted authentication deployment, see Test Trusted Authentication.

Ticket Value of -1 Returned from Tableau Server

Tableau Server returns -1 for the ticket value if it cannot issue the ticket as part of the trusted authentication process. Before troubleshooting this scenario, be sure to set the log level for trusted authentication to debug as specified in Troubleshoot Trusted Authentication.

The exact reason for this message is written to the vizqlserver_node*-*.*.log.* files in the following folder:

/var/opt/tableau/tableau_server/data/tabsvc/logs/vizqlserver

Here are some things to confirm:
• **All web server host names or IP addresses are added to trusted hosts**

The log error, "Invalid request host: <IP address>" may indicate that the IP address or host name for the computer sending the POST request is not in the list of trusted hosts on Tableau Server. See Add Trusted IP Addresses or Host Names to Tableau Server to learn how to add IP addresses or host names to this list.

• **IP addresses are IPv4**

If you are using IP addresses to specify trusted hosts, they must be in Internet Protocol version 4 (IPv4) format. An IPv4 address looks like this: 123.456.7.890. IPv6 addresses (for example, fe12::3c4a:5eab:6789:01c%34) are not supported as a way of inputting trusted hosts.

• **Username in POST request is a valid Tableau Server user**

The username you send in the POST request must be a licensed Tableau Server user. You can see a list of users by signing in to Tableau Server as an administrator.

The following log errors indicate a user POST issue:

• "Missing username and/or client_ip"

• "Invalid user: <username>"

• "Unlicensed user is not allowed: <username>"

**Username in POST request includes domain**

If Tableau Server is configured to use Local Authentication, the username that you send in the POST can be a simple string. However, if the server is configured for Active Directory you must include the domain name with the username (domain\username). For example, the username parameter might be: `username=dev\jsmith`. A common error log for this scenario is "Invalid user: <username>.

• **Content-Type is specified**
If you are designing an ASP.NET or C# application, you need to declare the content type in your HTTP request. For example:

```javascript
http.setRequestHeader("Content-Type","application/x-www-form-urlencoded; charset=UTF-8")
```

If you do not specify content type and Tableau Server returns a -1, the log files contain the error: "missing username and/or client_ip".

**HTTP 401 - Not Authorized**

If you receive a 401- Not Authorized error, you may have configured Tableau Server to use Active Directory with SSPI. If your web server uses SSPI, you do not need to set up trusted authentication. You can embed views and your users will have access to them as long as they are licensed Tableau server users and members of your Active Directory.

See tsm authentication sspi <commands>.

If you see a 401 error (or a 302 - Redirect error) after you have deployed Tableau Server 2019.1, then it's likely the trusted ticket code you have written to construct the URL for the client has not been updated to account for the two-part ticket URL format.

See Get a Ticket from Tableau Server.

**HTTP 404 - File Not Found**

You may receive this error if your program code references a Tableau Server URL that does not exist. For example, your web server may construct an invalid URL that cannot be found when the webpage tries to retrieve it.

Another cause for this error is if you did not enter the trusted web servers as specified in Add Trusted IP Addresses or Host Names to Tableau Server. If you have already entered the trusted web servers, verify that the IP addresses or host names are correct.

**Invalid User (SharePoint or C#)**

You may encounter this error if you’ve configured Tableau Server for trusted authentication.
The example code for the SharePoint .dll references the following GET request:

```c
```n
The above request will return the display name of the current Windows Active Directory user. If you want to use the login ID, then you will need to change the code to:

```c
```n
After you make the change, recompile the SharePoint .dll.

Attempting to Retrieve the Ticket from the Wrong IP Address

You may encounter this error if you've configured Tableau Server for trusted authentication.

The client web browser IP address is not considered by default when redeeming the ticket. If Tableau Server is configured to enforce client IP address matching, make sure that the client's web browser IP address that is sent in the POST to Tableau Server is the same as when the browser tries to retrieve the embedded view. For example, in the Trusted Authentication diagram, if the POST request in step 3 sends the parameter client_ip=74.125.19.147, then the GET request in step 5 must come from that same IP address.

See Optional: Configure Client IP Matching to learn how to configure Tableau Server to enforce client IP address matching.

Cookie Restriction Error

When a user signs in to Tableau Server, a session cookie is stored in their local browser. The stored cookie is how Tableau Server maintains that the signed in user has been authenticated and can access the server. Because the cookie is set with the same domain or subdomain as the browser’s address bar, it is considered a first-party cookie. If a user's browser is configured to block first-party cookies, they will be unable to sign in to Tableau Server.

When a user signs in to Tableau Server via an embedded view, or in an environment where trusted authentication has been configured, the same thing happens: a cookie is stored. In this case, however, the browser treats the cookie as a third-party cookie. This is because
the cookie is set with a domain that's different from the one shown in the browser's address bar. If a user's web browser is set to block third-party cookies, authentication to Tableau Server will fail. To prevent this from occurring, web browsers must be configured to allow third-party cookies.

An error occurred communicating with the server (403)

If Tableau Server is configured for trusted authentication, you may receive this error after opening a new view in a browser and attempting to navigate back to views you’d opened earlier. Tableau Server provides protection against unauthorized reuse of VizQL sessions through the tsm configuration set Optionsvizqlserver.protect_sessions, which is set to true by default. Because Tableau Server is configured for trusted authentication, you may not also need to enable vizqlserver.protect_sessions. To disable it, use tsm configuration set Options to change it to false.

Data Connection Authentication

More information

- Tableau Server on Linux - Connecting to a Windows Shared Directory (Tableau Community)

- Setting an Oracle Connection to Use TNSNames.ora or LDAP.ora (Tableau Support)

Enable Kerberos Delegation

Kerberos delegation enables Tableau Server to use the Kerberos credentials of the viewer of a workbook or view to execute a query on behalf of the viewer. This is useful in the following situations:

- You need to know who is accessing the data (the viewer's name will appear in the access logs for the data source).

- Your data source has row-level security, where different users have access to different rows.
Supported data sources

Tableau supports Kerberos delegation with the following data sources

- Cloudera: Hive/Impala
- Denodo
- PostgreSQL
- SQL Server
- Teradata

Requirements

Kerberos delegation requires Active Directory.

- The Tableau Server information store must be configured to use LDAP - Active Directory.
- The computer where Tableau Server is installed must be joined to Active Directory domain.
- MIT KDC is not supported.

Configuration process

This section provides an example of the process to enable Kerberos delegation. The scenario also includes example names to help describe the relationships between the configuration elements.

1. Tableau Server will need a Kerberos service ticket to delegate on behalf of the user that is initiating the call to the database. You must create a domain account that will be used to delegate to the given database. This account is referred to as the Run As service account. In this topic, the example user configured as the delegation/Run As account is tabsrv@example.com.

   The account must be configured with Active Directory User and Computers on a Windows Server that is connected to the user domain:

   - Open the Properties page for the Run As service account, click the Delegation tab and select Trust this user for delegation to specified services only and Use any authentication protocol.

2. Create a keytab file for the Run As service account.
For example, the following commands create a keytab (tabsrv-runas.keytab) using the ktutil tool:

```
sudo ktutil
```

```
ktutil: addent -p tabsrv@EXAMPLE.COM -k 2 -e <encryption scheme>
```

**Encryption schemes for this command include** RC4-HMAC, aes128-cts-hmac-shal-96, and aes256-cts-hmac-shal-96. **Consult your IT team for the correct encryption scheme for your environment and data source.**

```
ktutil: wkt tabsrv-runas.keytab
```

Tableau Server will use the Run As service account and the associated keytab to authenticate and make a direct connection to the database.

3. Copy the keytab into the Tableau Server data directory and set proper ownership and permissions.

```
mkdir /var/opt/keytab
sudo cp -p tabsrv-runas.keytab /var/opt/keytab
```

```
sudo chown $USER /var/opt/keytab/tabsrv-runas.keytab
```

```
chgrp tableau /var/opt/keytab/tabsrv-runas.keytab
```

```
chmod g+r /var/opt/keytab/tabsrv-runas.keytab
```

4. Run the following TSM commands to enable Kerberos delegation, set the delegation service account, and associate the keytab file with the service account:

```
tsm configuration set -k wgserver.delegation.enabled -v true
```
tsm configuration set -k native_api.datasource_imper-sonation_runas_principal -v tabsrv@EXAMPLE.COM

```
$ tsm configuration set -k native_api.datasource_imper-
sonation_runas_keytab_path -v /var/opt/keytab/tabsrv-
runas.keytab
```

```bash
tsm configuration set -k native_api.protocol_transition_a-
d_short_domain -v false
```

```bash
tsm configuration set -k native_api.protocol_transition_
uppercase_realm -v true
```

In some cases, TSM may return an error mentioning `--force-keys`. If you get this error, run the command again with the `--force-keys` parameter appended to the argument.

5. Run the following TSM command apply the changes to Tableau Server:

```
tsm pending-changes apply
```

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior.

For more information, see `tsm pending-changes apply`.

6. Enable delegation for data connections:

- **SQL Server**—See Enabling Kerberos Delegation for SQL Server in the Tableau Community.

- **PostgreSQL**—See Enabling Kerberos Delegation for PostgreSQL in the Tableau Community.

- **Teradata**—See Enabling Kerberos Delegation for Teradata in the Tableau Community.
Tableau Server on Linux Administrator Guide

- **Denodo**—See [Enabling Kerberos Delegation for Denodo on Linux](#) in the Tableau Community.

- **Cloudera**—See [Enable Kerberos Delegation for Hive/Impala](#) in the Tableau Community.

See also

Troubleshoot Kerberos

OAuth Connections

For Google BigQuery, Google Analytics, Salesforce, OneDrive, Dropbox, and QuickBooks Online, an alternative to storing your sensitive database credentials with Tableau Server is to create connections using the **OAuth 2.0** standard.

From Tableau, when you sign in to data with a provider that uses OAuth, you are redirected to the provider’s sign-in page. After you provide your credentials and authorize Tableau to access your data, the data provider sends Tableau an **access token** that uniquely identifies requests from Tableau. For more information, see Overview of the OAuth process below.

Using OAuth connections provides the following benefits:

- **Security**: Your database credentials are never known to or stored in Tableau Server, and the access token can be used only by Tableau.

- **Convenience**: Instead of having to embed your data source ID and password in multiple places, you can use the token provided for a particular data provider for all published workbooks and data sources that access that data provider.

In addition, for live connections to Google BigQuery data, each workbook viewer can have a unique access token that identifies the user, rather than sharing a single user name and password credential.
Overview of the OAuth process

The following steps describe a workflow in the Tableau environment that calls the OAuth process.

1. You take an action that requires access to a cloud data source.

   For example, you open a workbook that’s published to Tableau Server.

2. Tableau directs you to the cloud data provider’s sign-in page. The information that is sent to the data provider identifies Tableau as the requesting site.

3. When you sign in to the data, the provider prompts you to confirm your authorization for Tableau Server to access the data.

4. Upon your confirmation, the data provider sends an access token back to Tableau Server.

5. Tableau Server presents your workbook and data to you.

The following workflows can use the OAuth process:
Tableau Server on Linux Administrator Guide

- Creating a workbook and connecting to the data source from Tableau Desktop or from Tableau Server.

- Publishing a data source from Tableau Desktop.

- Signing in to Tableau Server from an approved client, such as Tableau Mobile or Tableau Desktop.

Access tokens for data connections

You can embed credentials based on access tokens with data connections, to enable direct access after the initial authentication process. An access token is valid until a Tableau Server user deletes it, or the data provider revokes it.

It is possible to exceed the number of access tokens your data source provider allows. If that's the case, when a user creates a new token, the data provider uses length of time since last access to decide which token to invalidate to make room for the new one.

Access tokens for authentication from approved clients

By default, Tableau Server sites allow users to access their sites directly from approved Tableau clients, after users provide their credentials the first time they sign in. This type of authentication also uses OAuth access tokens to store the users' credentials securely.

For more information, see Disable Automatic Client Authentication

Configure the Server for OAuth Support

Instead of individual usernames and passwords, OAuth works through limited-purpose access tokens. Before you can obtain access tokens needed to create an OAuth connection in Tableau, you need to configure your server so that the data provider sending the token can recognize Tableau Server as a trusted destination. The following section describes how to prepare for setting up OAuth regardless of your data provider. The topics listed below contain the steps for configuring your server for specific data providers.
Preparing for Configuring OAuth Support

Before you begin the configuration steps specific to your data provider, complete the following prerequisites:

- Obtain the fully qualified domain name of each Tableau Server node that will host views that connect to this data source. For example:

  https://sales.your_domain.com

  If you use Salesforce.com, you will need to provide an https address.

- Make sure at least one of your data-provider accounts is enabled for API access.

  For Google data types, you need access to the developers console on the Google Cloud Platform.

  For Salesforce.com, you need access to the Force.com platform.

  For QuickBooks Online, you need access to the Intuit platform.

Configure Settings for Your Data Provider

When you complete the OAuth-preparation steps, you can configure the appropriate settings with your data provider.

- Set up OAuth for Google
- Set up OAuth for Salesforce.com
- Set up OAuth for QuickBooks Online

Set up OAuth for Google

This topic describes how to set up your Google BigQuery, Google Sheets, and Google Analytics data sources for OAuth.

Complete these steps for each Tableau Server instance.
Before you complete these steps, make sure you have completed the pre-requisites described in Preparing for Configuring OAuth Support.

Set up OAuth by following these three procedures:

- Enable API access and create access token from Google.
- Configure OAuth on Tableau Server.
- Create and edit Google data source.

Obtain a Client ID and Enable Google APIs

These steps reflect the settings in the Google Cloud Platform console at the time of this writing. For more information, see Using OAuth 2.0 for Web Server Applications in the Google Developers Console Help.

1. Sign in to Google Cloud Platform, and then click Go to my console.

2. On the drop-down menu next to the Google Cloud Platform title, select Create project.

3. In the new project form that appears, complete the following:

   - Give the project a meaningful name that reflects the Tableau Server instance for which you’ll use this project.
   - Determine whether you want to change the project ID.

   After you create the project, you will not be able to change the project ID.
4. Open the new project, and navigate to **APIs Manager > Credentials**.

**Note:** You must generate credentials with the Google API Manager for Tableau Server. Do not attempt to use a Service Account, which generates a key, and is not supported.

5. Click the **OAuth consent screen** tab and then enter a meaningful name for **Product name** shown to users.

6. Click the **Credentials** tab, then click the **Create credentials** drop-down list, and then select **OAuth client ID**. Complete the following:

   - Select **Web Application**.

   - For **Authorized JavaScript Origins**, enter the local computer name of your Tableau Server.

   - For **Authorized Redirect URI**, replace the existing text with the Internet address for your server, and add the following text to the end of it: `auth/add_`
oauth_token. For example:

https://your_server_url.com/auth/add_oauth_token

7. Copy the Authorized Redirect URI, and paste it in a location that you can access from your Tableau Server computer.

8. Click Create.

9. Copy the following values that Google returns, and paste them in a location that you can access from your Tableau Server computer:
   - Client ID
   - Client secret

10. In APIs Manager > Dashboards, verify that BigQuery API, Google Drive API (to enable Google Sheets) or Analytics API is enabled. To enable APIs, click ENABLE API at the top of the page.

Configure Tableau Server for Google OAuth

Using the information you obtained by completing the steps in Obtain a Client ID and Enable Google APIs, configure your Tableau Server:

• On the Tableau Server computer, open the shell and run the following commands to specify the access token and URI:

  tsm configuration set -k oauth.google.client_id -v <your_client_ID>

  tsm configuration set -k oauth.google.client_secret -v <your_client_secret>

  tsm configuration set -k oauth.google.redirect_uri -v <your_authorized_redirect_URI>
tsm pending-changes apply

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

Create and edit Google data source

Next, you must publish the Google data sources to the server. See the Tableau Desktop topic, Google BigQuery.

After you've published the data sources, the final step is to edit the data source connection to use the embedded access token that you configured earlier. See Edit Connections on Tableau Server.

Managing access tokens

After you configure the server for OAuth, you can allow users to manage their own access tokens in their profile settings, or you can manage the tokens centrally. For more information, see Allow Saved Access Tokens.

Set up OAuth for Salesforce.com

This topic describes how to set up your Salesforce.com data sources for OAuth. Complete these steps for each Tableau Server instance.

**Note:** Before you complete these steps, make sure you have completed the prerequisites described in Preparing for Configuring OAuth Support.

Set up OAuth by following these two procedures:
Create a Connected Salesforce App

1. Sign in to your Salesforce.com developer account, click your user name in the upper-right, and then select **Setup**.

2. In the left navigation column, under App Setup, select **Create > Apps**.

3. In the Connected Apps section, click **New**.

4. Complete the **Basic Information**, and in the API section, select **Enable OAuth Settings**.

5. In the new OAuth settings that appear, for **Callback URL**, type the fully qualified
domain name of your server, using the https protocol, and append the following text to the URL: `auth/add_oauth_token`.

For example:

`https://www.your_server.com/auth/add_oauth_token`

6. Move the following items from Available OAuth Scopes to Selected OAuth Scopes:

   - Access and manage your data (api)
   - Access your basic information (id)
   - Perform requests on your behalf at any time (refresh_token)

7. Click **Save**.

After you save the app, Salesforce populates the API section with the following IDs that you will use to configure Tableau Server:

- Consumer Key
- Consumer Secret
- Callback URL
Configure Tableau Server for Salesforce.com OAuth

1. On the Tableau Server computer, run the following commands:

   tsm configuration set -k oauth.salesforce.client_id -v <your_client_ID>

   tsm configuration set -k oauth.salesforce.client_secret -v <your_client_secret>

   tsm configuration set -k oauth.salesforce.redirect_uri -v <your_authorized_redirect_URI>

2. (Optional) To change the default login server, type the following command:

   tsm configuration set -k oauth.salesforce.server_base_url -v <URL>

3. Enter the following command to apply changes:

   tsm pending-changes apply

   The pending-changes apply command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the --ignore-prompt option, but this does not change the restart behavior. For more information, see tsm pending-changes apply.

Managing access tokens

After you configure the server for OAuth, you can allow users to manage their own access tokens in their profile settings, or you can manage the tokens centrally. For more information, see Allow Saved Access Tokens.
Set up OAuth for QuickBooks Online

This topic describes how to set up your QuickBooks Online data sources for OAuth authentication. Complete these steps for each Tableau Server instance.

Note: Before you complete these steps, make sure you have completed the prerequisites described in Preparing for Configuring OAuth Support.

Setting up OAuth for QuickBooks Online consists of two tasks:

- Create a Connected App on the Intuit developer platform.
- Use the information you get as part of the Connected App to configure your server.

Create a Connected Intuit App

1. Sign in to your Intuit developer account, and then click My Apps.

2. In the Just start coding section, click Select APIs.

3. Select Accounting and click Create App.

4. In the Get your app ready for submission section, click the link to get your production keys.

   Important: You must use production keys rather than development keys.

5. Copy the app token, OAuth consumer key, and OAuth consumer secret.
Configure Tableau Server for QuickBooks Online

- On the Tableau Server computer, open the bash shell and run the following commands:

```bash
tsm configuration set -k oauth.quickbooks.oauth_callback_uri -v http://YOUR-SERVER/auth/add_oauth_token

tsm configuration set -k oauth.quickbooks.consumer_key -v <your_consumer_key>

tsm configuration set -k oauth.quickbooks.consumer_secret -v <your_consumer_secret>

tsm pending-changes apply
```

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

Managing access tokens

If you run an extract refresh job for your QuickBooks Online data source, Tableau Server attempts to renew access tokens for you. To help ensure that your access tokens do not expire, run your extract refresh jobs more than once a month. Otherwise, the access tokens from QuickBooks Online expire and your extract refresh jobs fail. If your access tokens do expire, you can edit your saved credentials from the Settings page.

The saved credentials can be managed centrally or by your users. For more information, see Allow Saved Access Tokens.
Allow Saved Access Tokens

After you configure Tableau Server for OAuth, you can decide to allow users to manage their own OAuth credentials, or you want to manage them centrally. If you want users to manage their own, you need to enable user profile settings from the server.

**Note:** If you have not yet configured your server to enable OAuth data connections, see the related topics listed below.

1. Sign in to Tableau Server as a server administrator.

2. **Single-site:** Click **Settings** > **General**.

   **Multisite:** In the site menu, click **Manage All Sites** and then click **Settings** > **General**.

3. In the **Saved Credentials** section, select the following:
   
   - **Allow users to save passwords for data sources** (allows users to save their individual credentials with data sources).
   - **Allow users to save OAuth access tokens for data sources**

4. Click **Save**.
After you select these check boxes, users will see a **Manage Credentials** section in their profile settings, where they can add access tokens for OAuth data connections.

### Managing credentials centrally

Server administrators alternatively can manage OAuth credentials centrally. This can work well, for example, if multiple users work from the same data, and you have a dedicated user account for your data provider.

To manage credentials centrally, you do the following:

- Clear the check boxes described in the preceding procedure.
- Edit connection information as data sources are published.

  When you edit the connection, you embed credentials that use an OAuth access token instead of an individual’s user name and password.

When the settings for saving passwords and access tokens are not enabled, the Manage Credentials section is excluded from users’ profile settings.

### See also

- Set up OAuth for Google
- Set up OAuth for Salesforce.com
- Set up OAuth for QuickBooks Online
Configure SAP HANA SSO

You can configure Tableau Server to use SAML delegation to provide a single sign-on (SSO) experience for SAP HANA. This scenario is not dependent on SAML authentication to Tableau Server. You do not need to use SAML sign on with Tableau Server in order to use HANA SAML delegation. You can sign in to Tableau Server using whatever method you choose.

With SAML delegation for SAP HANA, Tableau Server functions as an identity provider (IdP).

Before you begin

Configuring SAML delegation with SAP HANA requires configuration on both Tableau Server and on SAP HANA. This topic provides configuration information about configuring Tableau Server. Before you configure Tableau Server, you must complete the following:

- Acquire a SAML certificate and key file for Tableau Server. The certificate file must be a PEM-encoded x509 certificate with the file extension .crt or .cert. This file is used by Tableau Server, and must also be installed on HANA. The private key must be a DER-encoded private key file that is not password protected, and that has the file extension .der. This file is only used by Tableau Server.
- Install the certificate in HANA.
- Install the latest version of SAP HANA driver (minimum version is 1.00.9) on Tableau Server.
- Configure network encryption from Tableau Server to SAP HANA (recommended).

For more information about generating the certificate/key pair, encrypting the SAML connection, and configuring SAP HANA, see How to Configure SAP HANA for SAML SSO with Tableau Server in the Tableau Community.

Configure Tableau Server SAML for SAP HANA

The following procedure describes how to configure SAML for SAP HANA on Tableau Server using tsm data-access. You can also configure SAML for SAP HANA using the sapHanaSettings Entity.
If you are running Tableau Server in a distributed deployment, run the following procedure on the initial node.

1. Place certificate files in a folder named `saml`. For example:

   /var/opt/saml

2. Run the following commands to specify the location of the certificate and key files:

   ```
   tsm data-access set-saml-delegation configure --cert-key <cert-key> --cert-file <cert-file>
   ```

   Where `<cert-key>` and `<cert-file>` are file paths to the private key and certificate file, respectively.

   For example,

   ```
   tsm data-access set-saml-delegation configure --cert-key /var/opt/saml/hana_pkey_pkcs8.der --cert-file /var/opt/saml/hana_cert.pem
   ```

   You can specify other options. For example, you can specify user name format and how credentials are normalized. See `tsm data-access`.

3. Run the following commands to enable delegation:

   ```
   tsm data-access set-saml-delegation enable
   tsm configuration set -k wgserver.sap_hana_sso.enabled -v true
   tsm configuration set -k wgserver.delegation.enabled -v true
   ```

4. **When you have finished,** run `tsm pending-changes apply`. 
The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

Enable Kerberos Service Account Access

You can configure Tableau Server to use a Kerberos service account to access a database. In this scenario, Tableau Server connects to databases with a service account, also referred to as a "RunAs account".

To use RunAs authentication on Tableau Server you must first create a workbook or data-source that uses integrated authentication. When users publish to Tableau Server they will get the option for RunAs authentication. If you create a datasource with Tableau Server web authoring that uses integrated authentication, the datasource will use RunAs authentication by default.

**Note:** *Integrated authentication* is also referred to as *Windows Authentication* on some connectors. In both cases, Tableau Server uses Kerberos authentication.

Data Access with the RunAs Service Account

To use RunAs authentication, the RunAs account requires read and query permissions to external databases. As designed, Tableau Server users with the *Creator* role or the *Explorer (Can Publish)* role have full access to the RunAs account for queries to external databases.

For example, a user with the Creator role can view all databases that have been granted access to the RunAs service account. They can also list tables and run Custom SQL.

If the Creator-user specifies the database host name and selects Integrated Authentication when creating a new data source with web authoring, then databases that have been granted RunAs access will be displayed to the user.
View access to database assets are not restricted to users who connect to Tableau Server with web authoring. Sophisticated users, who have the same roles noted above and who have knowledge of database server names, could create workbooks with Tableau Desktop that display databases that have been granted RunAs access.

**Recommendations**

Whether user access to databases in these scenarios is acceptable must be assessed by your organization. Generally, reducing the usage and scope of the RunAs service account will reduce the likelihood of inadvertent user access to database content. However, reducing the usage and scope of the RunAs service account may also impose more credential management to you and your users.

Evaluate the following recommendations in context of your business needs and data access policies.

- Firstly, be sure that you trust all users who have Creator roles or Explorer (Can Publish) roles. You will rely on these users to perform actions in Tableau with integrity.
- If you cannot trust all of your users who have publishing rights on data sources that are accessed by the RunAs service account, then you should consider embedding credentials for those data sources.
- If a data source is not set up for automated extract refreshes, that is, the data source is primarily accessed as a live connection, then you may be able to use Kerberos Delegation. For requirements, see Enable Kerberos Delegation.

**Requirements**

- MIT Kerberos is not supported.
- The RunAs service account must have read access to the target database.

**Configuration process**

This section provides an example of the process to enable Kerberos service account access.

1. Create a domain user account to act as the RunAs service account. This account must have read access to the target database.
In the example here, the RunAs service account is User principal named `tab-srv@example.com`.

2. Create a keytab file for the RunAs service account.

   For example, the following commands create a keytab (`tabsrv-runas.keytab`) using the `ktutil` tool:

   ```
   ktutil
   ktutil:  addent -password -p tabsrv@EXAMPLE.COM -k 2 -e <encryption scheme>
   
   Encryption schemes for this command include RC4-HMAC, aes128-cts-hmac-shal-96, and aes256-cts-hmac-shal-96. Consult your IT team for the correct encryption scheme for your environment and data source.
   
   ktutil:  wkt tabsrv-runas.keytab
   ```

   Tableau Server will use the RunAs service account and the associated keytab to authenticate and make a direct connection to the database.

3. Copy the keytab into the Tableau Server data directory and set proper ownership and permissions. The keytab should be readable by the unprivileged user. The default unprivileged user created by Tableau Setup is `tableau`.

   If you are running a multi-node deployment, then you must run the following commands on each node in the cluster:

   ```
   mkdir /var/opt/tableau/tableau_server/keytab
   
   sudo cp -p tabsrv-runas.keytab /var/opt/tableau/tableau_server/keytab
   sudo chown $USER /var/opt/tableau/tableau_server/keytab/tabsrv-runas.keytab
   chgrp tableau /var/opt/tableau/tableau_server/keytab
   ```
server/keytab/tabsrv-runas.keytab
chmod g+r /var/opt/tableau/tableau_server/keytab/tabsrv-runas.keytab

4. Run the following TSM commands to enable RunAs access, set the RunAs service account, and associate the keytab file with the service account.

   tsm configuration set -k features.RunAsAuthLinux -v true --force-keys
   tsm configuration set -k native_api.datasource_runas_principal -v tabsrv@EXAMPLE.COM --force-keys
   tsm configuration set -k native_api.datasource_runas_keytab_path -v /var/opt/tableau/tableau_server-/keytab/tabsrv-runas.keytab --force-keys

5. Run the following TSM command apply the changes to Tableau Server deployment:

   tsm pending-changes apply

   The pending-changes apply command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the --ignore-prompt option, but this does not change the restart behavior. For more information, see tsm pending-changes apply.

SQL Server Impersonation

Impersonation in the context of Tableau Server means allowing one user account to act on behalf of another user account. You can configure Tableau and Microsoft SQL Server to perform database user impersonation, so that the SQL Server database account used by Tableau Server queries on behalf of SQL Server database users, who are also Tableau users.

The main benefit of this feature is it allows administrators to implement and control their data security policy in one place: their databases. When Tableau users access a view with a live connection to a SQL Server database, the view only displays what the users' database
permissions authorize them to see. An additional benefit is that the users don’t have to respond to a database sign-in prompt when they open the view. Also, workbook publishers don’t have to rely on user-specific filters to restrict what’s seen in views.

Impersonation Requirements

Here’s what you need to use feature:

- **Live connections to SQL Server only**: Impersonation can only be used for views that have a live connection to a SQL Server database, version 2005 or newer.

- **Individual database accounts**: Each person who’ll be accessing the view must have an explicit, individual account in the SQL Server database to which the view connects. Members of an Active Directory (AD) group cannot be impersonated. For example, if Jane Smith is a member of the AD group Sales, and her database administrator adds the Sales AD group to the SQL Server database, Jane cannot be impersonated.

- **Matching credentials and authentication type**: The credentials of each Tableau user’s account and their Tableau user authentication type must match their credentials and authentication type in the SQL Server database. For example, if Jane Smith’s Tableau Server user account is `MyCo\jsmith`, the username on the SQL Server database must also be `MyCo\jsmith`. SQL Server must be using Windows Integrated Authentication.

- **SQL Server prerequisites**: In SQL Server you should have a data security table, a view that enforces data security, and you should require that your database users use the view.

- **SQL IMPERSONATE account**: You need a SQL Server database account that has IMPERSONATE permission for the above database users. This is either an account with the sysadmin role or one that has been granted IMPERSONATE permission for each individual user account (see the MSDN article on EXECUTE AS). The SQL Server account must be one of the following:
Tableau Server on Linux Administrator Guide

- The Tableau Server Run As service account. See Enable Kerberos Service Account Access.
- The workbook publisher’s account. See Impersonate with Embedded SQL Credentials.

How Impersonation Works

Here’s an illustration of how database user impersonation works:

In the above illustration, Jane Smith (MyCo\jsmith) is a West Coast sales representative and Henry Wilson (MyCo\hwilson) covers the East. In the SQL Server database, the account permissions for Jane's account, MyCo\jsmith, only give her access to West Coast data. Henry's account, MyCo\hwilson, can only access data for the East Coast.

A view has been created that displays data for the entire country. It has a live connection to a SQL Server database. Both users sign in to Tableau Server and click the view. Tableau Server connects to SQL Server using a database account with IMPERSONATE permission for each user's database account. This account acts on behalf of each user's database account.
When the view displays, it is restricted by each user's individual database permissions: Jane sees only the West Coast sales data, Henry sees only the East Coast data.

Impersonate with a Run As Service Account

Impersonating via a Run As service account is the recommended way to perform impersonation. The Run As service account is an Active Directory user account the Tableau Server service can run under on the machine hosting Tableau Server. This same account must have IMPersonate permission for the database user accounts in SQL Server. From a data security standpoint, using the Tableau Server Run As service account for impersonation gives the administrator the most control.

To set up impersonation with a Run As User account:

1. Enable Kerberos Service Account Access.

2. Create a workbook in Tableau Desktop. When you create the data connection, select **Use Windows NT Integrated security** for the workbook's live connection to a SQL Server database:

3. In Tableau Desktop, publish the workbook to Tableau Server (**Server > Publish Workbook**).

4. In the Publish dialog box, click Authentication, then in the Authentication dialog box, select **Impersonate via server Run As account** from the drop-down list:
5. Click **OK**.

6. Test the connection by signing into Tableau Server as a user. When you click a view, you should not be prompted for database credentials and you should only see the data the user is authorized to see.

**Impersonate with Embedded SQL Credentials**

You can also perform impersonation by having the person who publishes a view embed their SQL Server account credentials in the view. Tableau Server can be running under any type of account, but it will use these credentials, supplied by the publisher, to connect to the database.
This may be the right choice for your site if the account that handles the impersonation cannot be an Active Directory (AD) account and if you’re comfortable giving workbook publishers an account with a potentially high permission level on SQL Server.

**Note:**

To use this approach, Embedded Credentials must be enabled on the server Settings page in Tableau Server:

To impersonate with the workbook publisher’s SQL account:

1. In Tableau Desktop, create a workbook. When you create the data connection, select Use a specific username and password for the workbook’s live connection to a SQL Server database:

2. Publish the workbook to Tableau Server (*Server > Publish Workbook*).

3. In the Publish dialog box, click Authentication, then in the Authentication dialog box,
select **Impersonate via embedded password** from the drop-down list:

4. Click **OK**.

5. Test the connection by signing in to Tableau Server as a user. When you click a view, you should not be prompted for database credentials and you should only see the data the user is authorized to see.

**Authorization**

*Authorization* refers to how and what users can access on Tableau Server after authentication has been verified. Authorization includes:

- What users are allowed to do with content hosted on Tableau Server, including projects, sites, workbooks, and views.
What users are allowed to do with the data sources that are managed by Tableau Server.

What tasks users are allowed to perform to administer Tableau Server, such as configuring server settings, running command line tools, creating sites, and other tasks.

Authorization for these actions is managed by Tableau Server and determined by a combination of the user’s site role and permissions associated with specific entities such as workbooks and data sources.

Site roles

Site roles define who is an administrator. Administrators can be assigned at the site or server level. For nonadmins, site roles indicate the maximum level of access a user can have on a given site, subject to permissions set on content assets. For example, if one user is assigned the Viewer site role, and another the Creator site role.

For more information about site roles, see Set Users’ Site Roles.

Permissions

Permissions determine whether a given user is allowed or denied to perform a specific action on a specific content asset.

As an administrator setting up Tableau Server, it’s important that you understand how permissions are evaluated. Understanding the Tableau permissions process will enable you to set up and configure permissions on sites, projects, and other assets so that you can control how content and data is shared, published, viewed, extracted, and imported.

Four important concepts to understand about permissions in Tableau are:

- **Permissions are asset-based.** Permissions are assigned to individual content assets (projects, data sources, workbooks) and are granted to users or groups.

- **Permissions are implicitly denied, and non-admin users must explicitly be allowed to access content.** The process by which Tableau Server determines the “allow” or “deny” permission is explained in detail in the topic, How Permissions are Evaluated.
Permissions inheritance exists only in locked projects and in workbooks with tabbed views. When content permissions are locked to the top-level project, workbooks, views, and data sources in the entire project hierarchy will use the default permissions set at the top-level project. In workbooks saved with the option Show sheets as tabs, views inside those workbooks use the workbook permissions. For more information, see Content Permissions and Ownership.

In a project that is not locked, initial permissions are a one-time copy of the container item’s permissions. A data source or workbook starts with the default permissions, but authorized users can subsequently edit permissions on those assets. For more information on default permissions and projects, see Set Project Default Permissions and Lock the Project.

Tableau Server provides a flexible permissions infrastructure that allows you to manage access to all content for countless scenarios. For more detailed information, see Content Permissions and Ownership.

Data access and external authorization

There are scenarios where Tableau Server and Desktop rely on external authorization to enable access to data. For example:

- Users connecting to external data sources might require authorization that is outside the scope of Tableau Server’s authority. If users publish an external data source, Tableau Server will manage access and capabilities of that data source. But if users embed an external data source in a workbook, it’s up to the user who publishes the workbook to determine how other users who open the workbook will authenticate with the underlying data that the workbook connects to.

- Running Tableau Server in an organization with Active Directory, where Tableau has been configured with a Run As user account, results in a dependency on Active Directory and NTFS for authorization. For example, if you configure Tableau Server to use the Run As account to impersonate users connecting to SQL, then object-level authorization is reliant on NTFS and Active Directory.

- How users authenticate and are authorized by specific database solutions can differ. As noted, Tableau Server can be configured to provide access authorization when a data source is configured, but some databases will authorize access according to their own authentication scheme.
Data Security

Tableau provides several ways for you to control which users can see which data. For data sources that connect to live databases, you can also control whether users are prompted to provide database credentials when they click a published view. The following three options work together to achieve different results:

- **Database login account**: When you create a data source that connects to a live database, you choose between authenticating to the database through Windows NT or through the database’s built-in security mechanism.

- **Authentication mode**: When you publish a data source or a workbook with a live database connection, you can choose an Authentication mode. Which modes are available depends on what you choose above.

- **User filters**: You can set filters in a workbook or data source that control which data a person sees in a published view, based on their Tableau Server login account.

The table below outlines some dependencies with the above options:

<table>
<thead>
<tr>
<th><strong>Database Connection Options</strong></th>
<th><strong>Data Security Questions</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Database login account uses...</td>
<td>Authentication mode</td>
</tr>
<tr>
<td>Active Directory credentials (Windows Authentication)</td>
<td>Kerberos service account</td>
</tr>
<tr>
<td></td>
<td>Impersonate via server Kerberos service account</td>
</tr>
</tbody>
</table>
### Database Connection Options vs Data Security Questions

<table>
<thead>
<tr>
<th>Database login account uses...</th>
<th>Authentication mode</th>
<th>Is database security possible per Tableau Server user?</th>
<th>Are user filters the only way to restrict which data each user sees?</th>
<th>Are web caches shared among users?</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name and password</td>
<td>Viewer enters their credentials</td>
<td>Yes</td>
<td>No*</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Prompt user: Viewers are prompted for their database credentials when they click a view. Credentials can be saved.</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Embedded credentials: The workbook or data source publisher can embed their database credentials.</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Impersonate via embedded password: Database credentials with impersonate permission are embedded.</td>
<td>Yes</td>
<td>No*</td>
<td>No</td>
</tr>
</tbody>
</table>
Because it can create unexpected results, Tableau recommends that you not use this authentication mode with user filters.

User filters, the embedded credentials option and the impersonation modes have similar effects—when users click a view, they are not prompted for database credentials and they see only the data that pertains to them. However, user filters are applied in the workbook by authors, and the impersonation authentication modes rely on security policies defined by administrators in the database itself.

Manage Server Secrets

Tableau Server needs to store a number of secrets it uses to perform various functions, typically securing internal communication, communicating with other applications or the operating system, or providing secure communication with clients. In this context, the term secret may refer to a password, a token, or other string that is used to authenticate one entity to another.

There are two categories of secrets that are required to run Tableau Server. They differ according to how the secrets are generated:

- **Secrets that are generated by administrators.** These include credentials and associated secrets for the Run As User account and the SMTP credentials used by Tableau Server.
- **Secrets that are automatically generated by various processes in the system.** For example, a secret is required to protect communication between the Cluster Controller and ZooKeeper processes. And a number of different passwords are required for each service and programmatic user that communicates with Postgres.

Most secrets are encrypted while at rest. When a secret is needed, it is decrypted at run time.

This topic describes how secrets storage works and what you need to do to properly manage storage of secrets on Tableau Server.
Understanding how secrets storage works

During installation Tableau Server generates and stores a master key in a Java keystore. The master key is used to encrypt a configuration encryption key that is used across the system.

Whenever a new secret is created or updated, the secret is encrypted with the configuration encryption key. The encrypted value is then stored with its corresponding configuration parameter in a YAML file on the server. Parameters that hold an encrypted value use the format, ENC(<encrypted string>), where <encrypted string> is a Base64-encoded encrypted string.

At run time, when a given secret needs to be accessed, the encrypted values are read into memory and decrypted with the configuration encryption key.

Tableau Server encrypts secrets using 256-bit AES in GCM mode. The keys used for secure storage are different than the asset keys that are used to encrypt embedded database credentials before they are stored in the repository.

Who has access to the master key?

In a default installation, the Java keystore for Tableau Server will be replicated into the /tabsvc/keystores folder for each service on that node under /var/-opt/tableau/tableau_server/data/tabsvc/config.

For example,

/var/opt/tableau/tableau_server-
data/tabsvc/config/tabadminagent_<version_number>/tabsvc/keystores/tableauserver.jks.

If you use a custom install directory, then the keystore files will be found under

<install directory>/tableau_server/data/tabsvc/config/<service name_#.version_number>/tabsvc/keystores

By default, the following users and groups have access to this directory:
Import and export configuration information

Tableau Services Manager introduces the capability to import and export configuration information using tsm configuration.

**Note:** This version of Tableau Server does not support restoring configuration information from a backup. Instead, we recommend using the export and import configuration commands to backup and restore configuration information.

While configuration secrets are encrypted when stored on disk internally, when the configuration is exported to a file, secrets are written into the file in plain text. It is up to the administrator to take measures to protect this file. There are a variety of options available:

- Write the file to an encrypted file system.
- Write the file to a directory that is restricted to specific users or groups by file system permissions.
- Encrypt the output file.

Securing secrets for import and export operations

This section describes how to PGP encrypt the backup output. With this method, you will create a named pipe and provide it as the file argument, then use that as input to gpg encrypt it. The advantage is the secrets are never written to disk in plain text. gpg must be available and a private key available. An example of this method is shown in the following section.

The example in this section describes one way of handing secrets to store them on a separate computer.

See the following external references for more information:
File encryption on the command line

Example: encrypt and export

The following is an example of how to secure the file when exporting the configuration.

```
mkfifo -m 600 /tmp/secure1 && (gpg --symmetric --batch --yes --passphrase-file ~/.secrets/pgppassphrase.txt --cipher-algo AES256 --output encrypted.enc < /tmp/secure1 &) && tsm settings export -f /tmp/secure1 && rm /tmp/secure1
```

The details of this operation are:

- Create a named pipe with access limited by file permissions to rw for current user.

  ```
  mkfifo -m 600 /tmp/secure1
  ```

- Call gpg to encrypt the data sent to the named pipe, backgrounding it to a separate process. It will block waiting for data. The result will be a file containing the encrypted data.

  ```
  gpg --symmetric --batch --yes --passphrase-file ~/.secrets/pgppassphrase.txt --cipher-algo AES256 --output encrypted.enc < /tmp/secure1 &
  ```

- Call tsm to export the configuration, providing the named pipe as the file argument.

  ```
  tsm settings export -f /tmp/secure1
  ```

- Delete the named pipe.

  ```
  rm /tmp/secure1
  ```

The encrypted data is in the file "encrypted.enc."

Example: decrypt and import
The following is an example of how to decrypt and import the configuration.

```
mkfifo -m 600 /tmp/secret2 && (gpg --decrypt --batch --yes --passphrase-file ~/.secrets/pgppassphrase.txt encrypted.enc > /tmp/secret2 &) && tsm settings import -f /tmp/secret2 && rm /tmp/secret2
```

The details of this operation are:

- Create a named pipe with access limited by file permissions to \(\text{rw}\) for current user.

  ```
mkfifo -m 600 /tmp/secure2
  ```

- Decrypt the configuration and send it to the named pipe. Background this to a separate process, it will block waiting to be read.

  ```
gpg --decrypt --batch --yes --passphrase-file ~/.secrets/pgppassphrase.txt encrypted.enc > /tmp/secret2 &
gpg --decrypt --batch --yes --passphrase-file ~/.secrets/pgppassphrase.txt encrypted.enc > /tmp/secret2 &
  ```

- Execute the tsm configuration import command, logging in as needed.

  ```
  tsm settings import -f /tmp/secret2
  ```

- Delete the named pipe.

  ```
  rm /tmp/secure1
  ```

The pending configuration contains the imported configuration.

Run `tsm pending-changes apply` to commit changes. The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`. 
When adding a new node to your Tableau Server cluster, you will first need to generate the node configuration file (tsm topology). The node configuration file contains a copy of the master keystore file used for encrypting the configuration secrets.

**Important:** We strongly recommend that you take additional measures to secure the node configuration file when exporting a configuration file with secrets.

When installing and configuring Tableau Server on the new node, you will need to provide the node configuration file to the `initialize-tsm` command. You can use a similar technique as described above to decrypt the contents of the file that was previously encrypted and send it via a named pipe to the `initialize-tsm` command.

Secrets storage event logging

The following events related to secrets storage are logged:

- Generating new encryption keys
- Encryption key is rolled or changed
- Encrypting a new value in the configuration file

For more information about log files and where they are stored, see Work with Log Files.

Managing secrets

As a Tableau Server administrator the most important task related to secrets storage is to periodically update secrets. In some cases (server troubleshooting or auditing), you may need to retrieve a password.

For other operations, such as upgrading versions, backing up and restoring, or adding new nodes to a cluster—as noted above—Tableau Server manages secrets storage and related processes automatically.

Updating secrets

You should update secrets periodically, according to your company’s security policy.
To update the master key and automatically generated secrets, run `tsm security regenerate-internal-tokens`.

Retrieving passwords

In some cases, you may need to retrieve a password for troubleshooting or other operations. For example, you may need the Postgres readonly user credentials that are generated and encrypted by Tableau Server. In these cases, you can run a `tsm` command that will retrieve and decrypt the password for you.

To retrieve a password, open Command Prompt and issue a `tsm configuration get` command for one of the parameters listed in the table below.

For example, to retrieve a password for the readonly Postgres user, type the following command:

```
tsm configuration get -k pgsql.readonly_password
```

The command will return the password in clear text:

```
$ tsm configuration get pgsql.readonly_password

password
```

<table>
<thead>
<tr>
<th>Configuration Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clustercontroller.zookeeper.password</code></td>
<td>Password for cluster controller to connect to zookeeper.</td>
</tr>
<tr>
<td><code>filestore.zookeeper.password</code></td>
<td>Password for filestore to connect to zookeeper.</td>
</tr>
<tr>
<td><code>jdbc.password</code></td>
<td>Password for the rails Postgres user.</td>
</tr>
<tr>
<td><code>oauth.google.client_secret</code></td>
<td>Client secret of the Google Cloud Platform account.</td>
</tr>
<tr>
<td><code>oauth.quickbooks.consumer_secret</code></td>
<td>Consumer secret of the Intuit developer account.</td>
</tr>
<tr>
<td>Environment Variable</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>oauth.salesforce.client_secret</td>
<td>Client secret of the Salesforce developer account.</td>
</tr>
<tr>
<td>pgsq1.adminpassword</td>
<td>Password for the tblwgadmin Postgres user.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Although the configuration parameter is encrypted in Tableau's configuration files (tabsvc.yml, workgroup.yml), this password is stored in plain text in other files used by SAML and the Postgres recovery process.</td>
</tr>
<tr>
<td>pgsq1.readonly_password</td>
<td>Password for the readonly Postgres user.</td>
</tr>
<tr>
<td>pgsq1.remote_password</td>
<td>Password for the tableau Postgres user.</td>
</tr>
<tr>
<td>redis.password</td>
<td></td>
</tr>
<tr>
<td>servercrashupload.proxy_server_password</td>
<td>Password for custom proxy server used to upload crash reports.</td>
</tr>
<tr>
<td>service.runas.password</td>
<td>Password of the Run As users. Stored temporarily.</td>
</tr>
<tr>
<td>ssl.key.passphrase</td>
<td>Optional passphrase used to protect the Apache SSL key.</td>
</tr>
<tr>
<td>svcmonitor.notification.smtp.password</td>
<td>SMTP Server password supplied by the administrator through TabConfig.exe.</td>
</tr>
<tr>
<td>tabadminservice.password</td>
<td>Password for the service that allows server admins to download log files through the web interface.</td>
</tr>
</tbody>
</table>
Extension Security - Best Practices for Deployment

The following information is for IT officers and administrators, Tableau server and site administrators, and anyone who is interested in managing dashboard extensions and the security of their data and business. The suggestions for deployment are intended for companies that have a mix of users who are on Tableau Desktop and Tableau Server or Tableau Online.

Security for extensions in Tableau

Extensions are web applications that could be hosted inside your network, or outside on a third-party server. Extensions can interact with other components in the dashboard and potentially have access to the visible and underlying data in the workbook (through a well-defined API). Tableau supports extensions in Tableau Desktop, Tableau Server, and Tableau Online. Tableau Server and Tableau Online provide the most control over the extensions your users can run.
Potential security risks

Because extensions are web applications there is the potential that the extension could be vulnerable to certain types of malicious attacks, which in turn could present a risk to your computer or data. The Open Web Application Security Project (OWASP) annually identifies the most critical web application security risks. These risks include the following:

- SQL injection
- Cross-site scripting (XSS)
- Sensitive data exposure

These risks could compromise the extension if the developers of the extension do not properly validate and handle user inputs, or if they generate dynamic queries to access sensitive databases. As you evaluate the extensions that you want to allow in Tableau, be sure to consider how they manage authentication, data access, or user input, and how they mitigate security risks.

Mitigating the security threats

Understanding what an extension does is a first step to identifying the risks for your enterprise. In many cases, a dashboard extension does not access underlying data in the workbook and all the JavaScript code runs in the context of the browser running on the user’s computer. In these cases, no data leaves the computer even though the extension might be hosted on a third-party site outside of your domain. Some extensions allow you to connect Tableau with other applications you have already deployed in your domain.

Tableau provides security measures and security requirements for extensions. These are enabled for Tableau Desktop, Tableau Server, and Tableau Online.

- All extensions must use the HTTP Secure (HTTPS) protocol.
- By default, anyone using a dashboard with an extension will be prompted and asked to allow or deny the extension permission to run. The extension must request permission if it will access underlying data.
- Starting in 2019.1, to run on Tableau Server or Tableau Online, the URL of the extension must be added to a safe list. The site administrator manages this list.
- On Tableau Server and Tableau Online, the site administrator can control whether the prompt appears for each extension.
For more information, see Manage Dashboard Extensions in Tableau Server.

Manage extensions using Tableau

Extensions provide a way to add unique features to dashboards. You can use extensions to directly integrate the dashboard with applications outside of Tableau. While extensions open up a world of possibilities, there are instances where you need or want to maintain control of how extensions are deployed in your company or enterprise. In this respect, extensions are no different from any other software that you intend to use. Before you deploy software applications in your company you should thoroughly test and verify that the software works as expected and is secure. The same is true for extensions.

After you determine what level of access your users should have, and identify the extensions you want to use (or conversely, the extensions you don’t want used), you can use the controls and features within Tableau to restrict and curate the dashboard extensions users have access to.

- Do you need to restrict who can add or use extensions in Tableau Desktop? See Recommendations for Tableau Desktop
- Do you need to restrict or control the extensions your users have access to? See Recommendations for Tableau Server and Tableau Online.

Recommendations for Tableau Desktop

You have a range of options for deploying Tableau Desktop in your company. You can allow unrestricted access to third-party extensions, or you can put limits and restrictions on who has access to extensions and under what circumstances.

- **All users** - All Tableau Desktop users are empowered to use extensions. If you want to enable your Tableau Desktop users to choose which extensions they should run, you can use the default installation settings. Starting in Tableau 2018.2, extensions are enabled by default. Tableau Desktop users will have unrestricted access to third-party extensions.

- **Select users** - Only some Tableau Desktop users are empowered to use extensions. Others can use web authoring to access extensions, as determined by server and site administrators. If you want to limit who in your organization who has access to extensions, and only let those Tableau Desktop users choose which extensions they
should run, you can use the custom installation settings and use that to turn off extensions by default for most users. You can selectively enable extensions for the Tableau Desktop users.

- **Web authoring only** - Only allow users to add extensions on Tableau Server and Tableau Online. To provide you with the most control over which extensions users have access to, you can turn off extensions for all Tableau Desktop users and then allow users to add extensions to dashboards on Tableau Server or Tableau Online using web authoring. In this scenario, the server and site administrators can determine which extensions to allow users access to.

Selectively enable extensions on Tableau Desktop

By default, Tableau Desktop supports extensions and Tableau Desktop users have unrestricted access to extensions. You can use options during installation to change the default setting and turn off support for extensions. You can also turn off extensions after installation using registry settings and scripts.

- **During installation** You can turn support for extensions off during Tableau Desktop installation, using the **DISABLEEXTENSIONS** property (**DISABLEEXTENSIONS=1**). See Install Tableau Desktop from the Command Line.
- **After installation** You can also turn off support for extensions after installation by editing the Registry (Windows) or running a script (Mac) on each Desktop. See Turn off dashboard extensions.
Recommendations for Tableau Server and Tableau Online

If your users have access to Tableau Server or Tableau Online, you can use the built-in security controls to put limits and restrictions on the extensions that can be used and under what circumstances. If you have turned off extensions on Tableau Desktop, you can still allow users to add extensions in web authoring, but you can limit the number of extensions that can be used to just ones you approve of.

Trust extensions on the safe list

Starting with Tableau Server 2019.1, no extensions are allowed to run unless they have been added to the safe list. Users can only use extensions to dashboards that are explicitly listed on the settings page for the site (Settings > Extensions > Enable specific Extensions).

Note To make the safe list the default behavior in Tableau 2018.2 and Tableau 2018.3, you need to change the settings for the site. On the Extensions settings page, under Default behavior for Extensions, clear the Enable unknown extensions... option.
Checklist for the safe list:

- Does the extension come from a source that you know and trust?
- Check the URL of the extension. Does the URL look suspicious or contain dubious domain names?
- Does the extension require access to full (underlying data) or summary data? See Understand data access.
- Test the extensions before allowing broad use. See Test extensions for security.

Add extensions to the safe list:

- See Add extensions to the safe list and configure user prompts.

Block specific extensions from running on Tableau Server

On Tableau Server, you can block specific extensions by adding their URL to the block list. This is useful if you have multiple sites that are configured differently for extensions. For example, if you have a test site where you want to be able to test internal or third-party extensions, you might have enabled the default behavior for extensions, where unlisted extensions are allowed to run provided they do not access the underlying data in the workbook. Adding an extension to the block list will prevent it from inadvertently being used on the test site.

- Add the URL of the extensions that you do not want to allow to the blocked list. This option is only available on Tableau Server. See Block specific extensions.

Turn off extensions for a site

By default, extensions are enabled on Tableau Server and Tableau Online. On both Tableau Server and Tableau Online, the site administrator can turn off extensions for the site. The server administrator can turn off extensions for Tableau Server, this overrides the site settings. You should not have to change this setting. Only the extensions you add to the safe list are allowed. If you don’t add the URL of the extension to the safe list, the extension will not run.

- To disable extensions on a site (Tableau Server, Tableau Online), change the site settings that enables users to run extensions on the site. See Control dashboard.
extensions and access to data.

Show or hide user prompts to run extensions

When you add an extension to the safe list, you can configure whether users see prompts by default when they are adding an extension to a dashboard, or when they are interacting with a view that has an extension. The prompt tells users details about the extension and whether the extension has access to full data. The prompt gives users the ability to allow or deny the extension from running. You can hide this prompt from users, allowing the extension to run immediately.

Turn off the default behavior for extensions

Tableau Server and Tableau Online have another option for allowing extensions to run. Administrators can control whether to enable the default behavior (or policy) for extensions. That is, if enabled, the default behavior is that extensions that are not already on the safe list are allowed, provided that they do not request full data. Users will see prompts asking for permission to run those extensions.

In Tableau 2018.2 and 2018.3, this default behavior was enabled. Unless you clear this option, extensions that are not on a safe list are allowed to run, provided that they do not access full data.

Under some circumstances you might want to enable the default behavior for a site. For example, if you have a site that you reserve for testing, you might want the flexibility of being able to use extensions without having to first add them to the safe list. There are some extensions that do not access data directly, but control setting or clearing filters and parameters. Enabling the default behavior makes it easier to use those extensions. However, it does open the door for other extensions, so use this option cautiously.

Network Security

There are three main network interfaces in Tableau Server:
**Client to Tableau Server**: The client can be a web browser, Tableau Mobile, Tableau Desktop, or the tabcmd utility.

**Tableau Server to your database(s)**: To refresh data extracts or handle live database connections, Tableau Server needs to communicate with your database(s).

**Server component communication**: This applies to distributed deployments only.

### Client to Tableau Server

A Tableau Server client can be a web browser, a device running Tableau Mobile, Tableau Desktop, or tabcmd commands. Communications between Tableau Server and its clients use standard HTTP requests and responses. We recommend configuring Tableau Server for HTTPS for all communications. When Tableau Server is configured for SSL, all content and communications between clients are encrypted using SSL, and the HTTPS protocol is used for requests and responses.

By default, passwords are communicated from browsers and tabcmd to Tableau Server using 1024-bit public/private key encryption. This level of encryption is not considered robust enough for secure communications. Additionally, this method, where a public key is sent to the recipient in the clear and without network layer authentication is susceptible to man-in-the-middle attacks.

To adequately secure network traffic from clients to Tableau Server, you must configure SSL with a certificate from a trusted certificate authority.

See Configure SSL for External HTTP Traffic to and from Tableau Server.

### Client access from the Internet

We recommend a gateway proxy server to enable secure client access from the internet to your Tableau Server. We do not recommend running Tableau Server in a DMZ or otherwise outside your protected, internal network.

Configure a reverse proxy server, with SSL enabled, to handle all inbound traffic from the internet. In this scenario, the reverse proxy is the only external IP address (or range of
addresses if multiple reverse proxies are load-balancing inbound requests) that Tableau Server will communicate with. Reverse proxies are transparent to requesting clients, thereby obfuscating Tableau Server network information and simplifying client configuration.

For configuration information, see Configuring Proxies for Tableau Server.

Clickjack Protection

By default, Tableau Server has clickjack protection enabled. This helps prevent certain types of attacks in which the attacker overlays a transparent version of a page on top of an innocuous-looking page in order to lure a user into clicking links or entering information. With clickjack protection enabled, Tableau Server imposes certain restrictions on embedding views. For more information, see Clickjack Protection.

Tableau Server to your database

Tableau Server makes dynamic connections to databases to process result sets and refresh extracts. It uses native drivers to connect to databases whenever possible and relies on a generic ODBC adapter when native drivers are unavailable. All communications to the database are routed through these drivers. As such, configuring the driver to communicate on non-standard ports or provide transport encryption is part of the native driver installation. This type of configuration is transparent to Tableau.

When a user stores credentials for external data sources on Tableau Server, they are stored encrypted in Tableau Server’s internal database. When a process uses those credentials to query the external data source, the process retrieves the encrypted credentials from the internal database and decrypts them in process.

Tableau Server to the Internet

In some cases, where users connect to external data sources, such as the Tableau map servers, then Tableau Server will need to connect to the internet. We recommend that you run all components of Tableau inside your protected network. Therefore, connections to the internet may require that you configure Tableau Server to use a forward proxy.
Communication with the repository

You can configure Tableau Server to use Secure Sockets Layer (SSL) for encrypted communications on all traffic that is exchange with the Postgres repository to and from other server components. By default, SSL is disabled for communications between server components and the repository.

For more information, see tsm security repository-ssl enable

Server component communication in a cluster

There are two aspects to communication between Tableau Server components in a distributed server installation: trust and transmission. Each server in a Tableau cluster uses a stringent trust model to ensure that it is receiving valid requests from other servers in the cluster. Computers in the cluster running a gateway process accept requests from third parties (clients), unless they are fronted by a load balancer, in which case the load balancer receives the requests. Servers not running a gateway process only accept requests from other trusted members of the cluster. Trust is established by a whitelist of IP address, port, and protocol. If any of these are invalid, the request is ignored. All members of the cluster can communicate with each other.

When a user stores credentials for external data sources on Tableau Server, they are stored encrypted in Tableau Server's internal database. When a process uses those credentials to query the external data source, the process retrieves the encrypted credentials from the internal database and decrypts them in process.

Clickjack Protection

Tableau Server includes protection against clickjack attacks. Clickjacking is a type of attack against web pages in which the attacker tries to lure users into clicking or entering content by displaying the page to attack in a transparent layer over an unrelated page. In the context of Tableau Server, an attacker might try to use a clickjack attack to capture user credentials or to get an authenticated user to change settings on your server. For more information about clickjack attacks, see Clickjacking on the Open Web Application Security Project website.
Note: Clickjack protection was available in previous versions of Tableau Server, but was disabled by default. New installations of Tableau Server 9.1 and later will always have clickjack protection on unless you explicitly disable it.

Effects of clickjack protection

When clickjack protection is enabled on Tableau Server, the behavior of pages loaded from Tableau Server changes in the following ways:

- **Tableau Server adds the X-Frame-Options: SAMEORIGIN header to certain responses from the server.** In the current versions of most browsers, this header prevents the content from being loaded into an `<iframe>` element, which helps prevent clickjacking attacks.

- **The top-level page from Tableau Server cannot be loaded in `<iframe>` elements.** This includes the sign-in page. One consequence is that you cannot host Tableau Server pages in an application that you create.

- **Only views can be embedded.**

- **If an embedded view requires data source credentials, a message is displayed in the `<iframe>` element with a link to open the view in a secure window where the user can safely enter credentials.** Users should always verify the address of the opened window before entering credentials.

- **Views can be loaded only if they include the `:embed=y` parameter in the query string,** as in this example:

  
  http://<server>/views/Sales/CommissionModel?:embed=y

  
  Note: When clickjack protection is enabled, embedded views that use the URL copied from the browser address bar might not load. These view URLs usually
contain the hash symbol (#) after the server name (for example, http://myserver/#/views/Sales/CommissionModel?:embed=y) are blocked when clickjack protection is enabled on Tableau Server.

Disabling clickjack protection

You should leave clickjack protection enabled unless it is affecting how your users work with Tableau Server. If you want to disable clickjack protection, use the following tsm commands:

1. tsm configuration set -k wgserver.clickjack_defense.enabled -v false
2. tsm pending-changes apply

The pending-changes apply command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the --ignore-prompt option, but this does not change the restart behavior. For more information, see tsm pending-changes apply.

Content Security Policy

Tableau Server supports the Content Security Policy (CSP) standard. CSP is intended to be an additional layer of security against cross-site scripting and other malicious web-based attacks. CSP is implemented as a HTTP response header that allows you to specify where external resources, such as scripts and images, can be safely loaded from.

See the Mozilla website for more information about CSP.

Note: If your Tableau Server is configured to use SAML for user authentication, then do not enable CSP. Running CSP on Tableau Server with SAML is not supported.
Configure and enable CSP

CSP is configured and enabled using the tsm configuration set Options command. If you are running Tableau Server in a distributed deployment, run these commands on the initial node in the cluster. The configuration will be applied across the cluster after you run tsm pending-changes apply.

Step 1: Set default directives

Tableau Server includes the set of default directives in the table below.

To set a directive, use the following tsm syntax:

```
tsm configuration set -k content_security_policy.-directive.<directive_name> -v "<value>"
```

For example, to set the `connect_src` directive, run the following command:

```
tsm configuration set -k content_security_policy.-directive.connect_src -v "* unsafe-inline"
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>content_security_policy.-directive.default_src</code></td>
<td>‘none’</td>
<td>Serves as a fallback for the other fetch directives.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Valid values for <code>default_src</code>.</strong></td>
</tr>
<tr>
<td><code>content_security_policy.-directive.connect_src</code></td>
<td>*</td>
<td>Restricts the URLs which can be loaded using script interfaces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Valid values for <code>connect_src</code>.</strong></td>
</tr>
<tr>
<td><code>content_security_policy.-directive.script_src</code></td>
<td>*</td>
<td>Specifies valid sources for</td>
</tr>
<tr>
<td>Content Security Policy Directive</td>
<td>Valid Values</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><code>script-src</code></td>
<td><code>*</code> ‘unsafe-inline’</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specifies valid sources for stylesheets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Valid values for script-src.</code></td>
<td></td>
</tr>
<tr>
<td><code>style-src</code></td>
<td><code>*</code> data:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specifies valid sources of images and favicons.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Valid values for style-src.</code></td>
<td></td>
</tr>
<tr>
<td><code>img-src</code></td>
<td><code>*</code> data:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specifies valid sources of images and favicons.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Valid values for img-src.</code></td>
<td></td>
</tr>
<tr>
<td><code>font-src</code></td>
<td><code>*</code> data:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specifies valid sources for fonts loaded using @font-face.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Valid values for font-src.</code></td>
<td></td>
</tr>
<tr>
<td><code>frame-src</code></td>
<td><code>*</code> data:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specifies valid sources for nested browsing contexts loading using elements</td>
<td></td>
</tr>
<tr>
<td></td>
<td>such as <code>&lt;frame&gt;</code> and <code>&lt;iframe&gt;</code>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Valid values for frame-src.</code></td>
<td></td>
</tr>
<tr>
<td><code>object-src</code></td>
<td><code>data:</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specifies valid sources for the <code>&lt;object&gt;</code>, <code>&lt;embed&gt;</code>, and <code>&lt;applet&gt;</code> elements.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Valid values for object-src.</code></td>
<td></td>
</tr>
</tbody>
</table>
Valid values for `object-src`.

| `content_security_policy.directive.report_uri` | `/vizql/csp-report` | Instructs the user agent to report attempts to violate the CSP. These violation reports consist of JSON documents sent via an HTTP POST request to the specified URI. 
Valid values for `report_uri`. |

**Step 2: Add additional directives (optional)**

The default directives included with Tableau Server are a subset of directives that are supported by CSP.


You can add directives to the existing default set, by using adding the new directive in the `content_security_policy.directive` namespace. You must include the `--force-keys` parameter when adding new directives. The syntax is as follows:

```bash
tsm configuration set -k content_security_policy.directive.<new_directive_name> -v "<value>" --force-keys
```

For example, to add the `worker-src` directive, run the following command:

```bash
tsm configuration set -k content_security_policy.directive.worker-src -v "none" --force-keys
```
Step 3: Specify report-only directives (optional)

You can configure CPS to report some directives and to enforce others. When you set content_security_policy.enforce_enabled to true, then all directives are enforced (even if content_security_policy.report_only_enable is also set to true).

To specify directives as "report-only" and not enforced, add the directives to the report_only_directive namespace. You must include the --force-keys parameter when adding new directives. The syntax is as follows:

```
 tsm configuration set -k content_security_policy.report_only_directive.<directive_name> -v "<value>" --force-keys
```

For example, to report only on the script_src directive, run the following command:

```
 tsm configuration set -k content_security_policy.report_only_directive.script_src -v " http://*.example.com" --force-keys
```

Step 4: Enable CSP on Tableau Server

After you have configured directives, enable CSP on Tableau Server.

The following options are used to enable enforcement or report only mode for the directives you have set.

<table>
<thead>
<tr>
<th>Option</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>content_security_policy.enforce_enabled</td>
<td>false</td>
<td>Adds a CSP header to all requests so that any violation will be enforced by the browser.</td>
</tr>
<tr>
<td>content_security_policy.report_only_enabled</td>
<td>true</td>
<td>Adds a CSP header to all requests so that any violation will be recorded in our vizql-client logs, but will not be enforced by the browser.</td>
</tr>
</tbody>
</table>
To enable enforcement of the CSP directives that you’ve specified, run the following command:

```bash
tsm configuration set -k content_security_policy.enforce_enabled -v true
```

**Step 5: Run tsm pending-changes apply**

When you are finished configuring CSP, run `tsm pending-changes apply`.

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

**View CSP report**

To view CSP violations for a given viz, load the viz in a browser that includes developer tools. This example uses the Chrome browser.

1. Load a test viz with violations that is hosted on the Tableau Server deployment where you configured CSP.

2. Enter `CTRL+Shift+I` to open the developer tools in Chrome.

3. Click the `Network` tab.

4. In the `Filter` field, enter `csp-report`, and then click `Find All`.

   - If there are no violations then the search will not return any CSP reports.
   - If there are violations, click the Headers tab in the results pane and scroll to the bottom to view `Request Payload`. 
SSLSecure Sockets Layer) is a standard security technology that establishes an encrypted link between a web server and clients. To use SSL, you need to install an SSL certificate on Tableau Server.

You can configure Tableau Server to use SSL in the following ways:

- Use SSL for external HTTP traffic.
- Use mutual (two-way) SSL between clients (Tableau Desktop, web browsers, and tabcmd.exe) and Tableau Server.
- Use SSL for all HTTP traffic between internal server components and the repository.

If you are using mutual SSL, each client also needs a certificate.

**Note:** Tableau Server uses SSL for user authentication. SSL is not used to handle permissions and authorization to content (data sources and workbooks) hosted on Tableau Server.

Configure SSL for External HTTP Traffic to and from Tableau Server

You can configure Tableau Server to use Secure Sockets Layer (SSL) encrypted communications on all external HTTP traffic. Setting up SSL ensures that access to Tableau Server is secure and that sensitive information passed between the server and Tableau clients—such as Tableau Desktop, the REST API, and so on—is protected. Steps on how to configure the server for SSL are described this topic; however, you must first acquire a certificate from a trusted authority, and then import the certificate files into Tableau Server.

For a basic primer about SSL and Tableau Server, see Using SSL to encrypt Tableau Server communication in the Everybody's Install Guide.

Mutual SSL authentication is not supported on Tableau Mobile.
SSL certificate requirements

Acquire an Apache SSL certificate from a trusted authority (for example, Verisign, Thawte, Comodo, GoDaddy). You can also use an internal certificate issued by your company. Wildcard certificates, which allow you to use SSL with many host names within the same domain, are also supported.

When you acquire an SSL certificate for external communication to and from Tableau Server, follow these guidelines and requirements:

- All certificate files must be valid PEM-encoded X509 certificates with the extension .crt.
- Use a SHA-2 (256 or 512 bit) SSL certificate. Most browsers no longer connect to a server that presents an SHA-1 certificate.
- In addition to the certificate file, you must also acquire a corresponding SSL certificate key file. The key file must be a valid RSA or DSA private key file (with the extension .key by convention).

You can choose to passphrase-protect the key file. The passphrase you enter during configuration will be encrypted while at rest. However, if you want to use the same certificate for SSL and SAML, you must use a key file that is not passphrase protected.

- SSL certificate chain file: A certificate chain file is required for Tableau Desktop on the Mac and for Tableau Prep Builder on the Mac and Tableau Prep Builder on Windows. The chain file is also required for the Tableau Mobile app if the certificate chain for Tableau Server is not trusted by the iOS or Android operating system on the mobile device. The chain file is a concatenation of all of the certificates that form the certificate chain for the server certificate. All certificates in the file must be x509 PEM-encoded and the file must have a .crt extension (not .pem).
- For multiple sub-domains, Tableau Server supports wildcard certificates.
Tableau Server supports certificates that list multiple domains, IP addresses, or host names in the Subject Alternative Names (SAN) field.

**Note:** If you plan to configure Tableau Server for single-sign on using SAML, see Using SSL certificate and key files for SAML in the SAML requirements to help determine whether to use the same certificate files for both SSL and SAML.

## Configuring SSL for a Cluster

You can configure a Tableau Server cluster to use SSL. If the initial node is the only one running the gateway process (which it does by default), you need to configure SSL only on that node, using the steps described in this topic.

### SSL with multiple gateways

A highly available Tableau Server cluster can include multiple gateways, fronted by a load balancer. If you are configuring this type of cluster for SSL, you have the following choices:

- **Configure the load balancer for SSL:** Traffic is encrypted from the client web browsers to the load balancer. Traffic from the load balancer to the Tableau Server gateway processes is not encrypted. No SSL configuration in Tableau Server is required by you. It's all handled by the load balancer.

- **Configure Tableau Server for SSL:** Traffic is encrypted from the client web browsers to the load balancer, and from the load balancer to the Tableau Server gateway processes. For more information, continue to the following section.

## Additional configuration information for Tableau Server cluster environments

When you want to use SSL on all Tableau Server nodes that run a gateway process, you complete the following steps.
1. Configure the external load balancer for SSL passthrough.

Or if you want to use a port other than 443, you can configure the external load balancer to terminate the non-standard port from the client. In this scenario, you would then configure the load balancer to connect to Tableau Server over port 443. For assistance, refer to the documentation provided for the load balancer.

2. Make sure the SSL certificate is issued for the load balancer’s host name.

3. Configure the initial Tableau Server node for SSL.

4. If you are using mutual SSL, upload the SSL CA certificate file. See `tsm authentication mutual-ssl <commands>`. SSL certificate and key files will be distributed to each node as part of the configuration process.

Prepare the environment

When you get the certificate files from the CA, save them to a location accessible by Tableau Server, and note the names of the certificate .crt and .key files and the location where you save them. You’ll need to provide this information to Tableau Server when you enable SSL.

A common practice is to place a copy of the certificate files in a location that’s within the Tableau Server directory tree. For example:

```
/var/opt/tableau/tableau_server/data/ssl
```

Name the directory whatever is appropriate depending on whether you’ll use the certificate files only for SSL or also for configuring SAML authentication.

**Note:** If you think you might want to use the same certificate for SSL and SAML, see the Certificate and identity provider (IdP) requirements in the SAML Requirements topic.
Configure SSL on Tableau Server

Use the method you’re most comfortable with.

Use the TSM web interface

1. Open TSM in a browser:

   https://<tsm-computer-name>:8850. For more information, see Sign in to Tableau Services Manager Web UI.

2. On the **Configuration** tab, select **Security > External SSL**.

   **Note**: If you are updating or changing an existing configuration, click **Reset** to clear the existing settings before proceeding.

3. Under **External web server SSL**, select **Enable SSL for server communication**.

4. Upload the certificate and key files, and if required for your environment, upload the chain file and enter the passphrase key:

   If you are running Tableau Server in a distributed deployment, then these files will be automatically distributed to each appropriate node in the cluster.

5. Click **Save Pending Changes**.
6. Click **Pending Changes** at the top of the page:

![Screenshot of Tableau Server interface with Pending Changes button highlighted]

7. Click **Apply Changes and Restart**.

Use the TSM CLI

After you have copied the certificate files to the local computer, run the following commands:

```
tsm security external-ssl enable --cert-file <path-to-file.crt> --key-file <path-to-file.key>
tsm pending-changes apply
```

See the command reference at `tsm security external-ssl enable` to determine whether you want to include additional options for `external-ssl enable`. Tableau has specific recommendations for the `--protocols` option.

The `external-ssl enable` command imports the information from the .crt and .key files. If you run this command on a node in a Tableau Server cluster, it also distributes the information to any other gateway node.

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

Port redirection and logging

After the server has been configured for SSL, it accepts requests to the non-SSL port (default is port 80) and automatically redirects to the SSL port 443.
Tableau Server on Linux Administrator Guide

**Note:** Tableau Server supports only port 443 as the secure port. It cannot run on a computer where another application is using port 443.

SSL errors are logged in the at the following location. Use this log to troubleshoot validation and encryption issues:

/var/opt/tableau/tableau_server/data/tabsvc/logs/httpd/error.log

**Add SSL port to the local firewall**

If you are running a local firewall, you must add the SSL port to the firewall on Tableau Server. The example below describes how to configure the firewall running on RHEL/CentOS distributions. The example uses Firewalld, which is the default firewall on CentOS.

1. Start firewalld:

   ```bash
   sudo systemctl start firewalld
   ```

2. Add port 443 for SSL:

   ```bash
   sudo firewall-cmd --permanent --add-port=443/tcp
   ```

3. Reload the firewall and verify the settings:

   ```bash
   sudo firewall-cmd --reload
   
   sudo firewall-cmd --list-all
   ```

**Change or update SSL certificate**

After you have configured SSL, you may need to periodically update the certificate. In some cases, you may need change the certificate for operational changes in your IT environment. In either case, you must use TSM to replace the SSL certificate that has already been configured for external SSL.
Do not copy a new certificate to the file directory on the operating system. Rather, when you add the certificate with either the TSM web UI or the `tsm security external-ssl enable` command, the certificate file is copied to the appropriate certificate store. In a distributed deployment, the certificate is also copied across the nodes in the cluster.

To change or update the SSL certificate (and the corresponding key file if required), follow the steps in the previous section of this topic, Configure SSL on Tableau Server.

**Example: SSL Certificate - Generate a Key and CSR**

**Important:** This example is intended to provide general guidance to IT professionals who are experienced with SSL requirements and configuration. The procedure described in this article is just one of many available methods you can use to generate the required files. The process described here should be treated as an example and not as a recommendation.

When you configure Tableau Server to use Secure Sockets Layer (SSL) encryption, this helps ensure that access to the server is secure and that data sent between Tableau Server and Tableau Desktop is protected.

Looking for Tableau Server on Windows? See Example: SSL Certificate - Generate a Key and CSR.

Tableau Server uses Apache, which includes OpenSSL. You can use the OpenSSL toolkit to generate a key file and Certificate Signing Request (CSR) which can then be used to obtain a signed SSL certificate.

**Steps to generate a key and CSR**

To configure Tableau Server to use SSL, you must have an SSL certificate. To obtain the SSL certificate, complete the steps:

1. Generate a key file.
2. Create a Certificate Signing Request (CSR).
3. Send the CSR to a certificate authority (CA) to obtain an SSL certificate.
4. Use the key and certificate to configure Tableau Server to use SSL.
You can find additional information on the SSL FAQ page on the Apache Software Foundation website.

Configure a certificate for multiple domain names

Tableau Server allows SSL for multiple domains. To set up this environment, you need to modify the OpenSSL configuration file, openssl.conf, and configure a Subject Alternative Name (SAN) certificate on Tableau Server. See For SAN certificates: modify the OpenSSL configuration file below.

Generate a key

Generate a key file that you will use to generate a certificate signing request.

1. Change to the Apache directory for Tableau Server:

   /opt/tableau/tableau_server/packages/apache.<version>

2. Run the following command to create the key file:

   openssl genrsa -out <yourcertname>.key 4096

   **Note:** This command uses a 4096-bit length for the key. You should choose a bit length that is at least 2048 bits because communication encrypted with a shorter bit length is less secure. If a value is not provided, 512 bits is used.

Create a certificate signing request to send to a certificate authority

Use the key file you created in the procedure above to generate the certificate signing request (CSR). You send the CSR to a certificate authority (CA) to obtain a signed certificate.
Important: If you want to configure a SAN certificate to use SSL for multiple domains, first complete the steps in For SAN certificates: modify the OpenSSL configuration file below, and then return to here to generate a CSR.

1. Run the following command to create a certificate signing request (CSR) file:

   ```bash
   openssl req -new -key yourcertname.key -out yourcertname.csr -config ../conf/openssl.cnf
   ```

2. When prompted, enter the required information.

   **Note:** For **Common Name**, type the Tableau Server name. The Tableau Server name is the URL that will be used to reach the Tableau Server. For example, if you reach Tableau Server by typing `tableau.example.com` in the address bar of your browser, then `tableau.example.com` is the common name. If the common name does not resolve to the server name, errors will occur when a browser or Tableau Desktop tries to connect to Tableau Server.

Send the CSR to a certificate authority to obtain an SSL certificate

Send the CSR to a commercial certificate authority (CA) to request the digital certificate. For information, see the Wikipedia article Certificate authority and any related articles that help you decide which CA to use.

Use the key and certificate to configure Tableau Server

When you have both the key and the certificate from the CA, you can configure Tableau Server to use SSL. For the steps, see Configure External SSL.
For SAN certificates: modify the OpenSSL configuration file

In a standard installation of OpenSSL, some features are not enabled by default. To use SSL with multiple domain names, before you generate the CSR, complete these steps to modify the openssl.cnf file.

1. Navigate to the Apache conf folder for Tableau Server.

For example: /opt/tableau/tableau_server-
packages/apache.<version_code>/conf

2. Open openssl.cnf in a text editor, and find the following line: req_extensions = v3_req

This line might be commented out with a hash sign (#) at the beginning of the line.

UTF8Strings
  # so use this option with caution!
  string_mask = nombstr

  # req_extensions = v3_req # The extensions to add to a certificate request
  [ req_distinguished_name ]
  countryName = Country Name (2 letter code)

If the line is commented out, uncomment it by removing the # and space characters from the beginning of the line.

3. Move to the [ v3_req ] section of the file. The first few lines contain the following text:

    # Extensions to add to a certificate request
    basicConstraints = CA:FALSE
    keyUsage = nonRepudiation, digitalSignature, keyEncipherment

After the keyUsage line, insert the following line:
subjectAltName = @alt_names

If you're creating a self-signed SAN certificate, do the following to give the certificate permission to sign the certificate:

a. Add the cRLSign and keyCertSign to the keyUsage line so it looks like the following: keyUsage = nonRepudiation, digitalSignature, 
keyEncipherment, cRLSign, keyCertSign

b. After the keyUsage line, add the following line: subjectAltName = 
@alt_names

4. In the [alt_names] section, provide the domain names you want to use with SSL.

DNS.1 = [domain1] 
DNS.2 = [domain2] 
DNS.3 = [etc]

The following image shows the results highlighted, with placeholder text that you would replace with your domain names.

[ v3_req ]

# Extensions to add to a certificate request

basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names

[alt_names]
DNS.1 = domain1
DNS.2 = domain2
DNS.3 = etc

5. Save and close the file.

6. Complete the steps in Create a certificate signing request to send to a certificate
Configure SSL for Internal Postgres Communication

You can configure Tableau Server to use SSL (TLS) for encrypted communication between the Postgres repository and other server components. By default, communication that is internal to Tableau Server components is not encrypted.

While you enable support for internal SSL, you can also configure support for direct connections to the repository from Tableau clients, such as Tableau Desktop, Tableau Mobile, REST API, web browsers.

Use the TSM web interface

1. As a server administrator, open TSM in a browser:
   
   https://<tsm-computer-name>:8850
   
   For more information, see Sign in to Tableau Services Manager Web UI.

2. On the Configuration tab, select Security > Repository SSL.

3. Select one of the options for using repository SSL.
• **Required for all connections**—uses SSL for internal Tableau Server communication, and requires SSL for Tableau clients that connect directly to the repository, including those using the `tableau` or `readonly` user.

    **Important:** If you select this option, you must also complete the steps in Configure Postgres SSL to Allow Direct Connections from Clients, to place the certificate files in the correct location on the client computers.

• **Optional for user connections**—uses SSL for internal Tableau Server communication, and supports but does not require SSL for direct connections to the server from Tableau clients.

• **Off for all connections (default)**—Internal server communication is not encrypted, and SSL is not required for direct connections from clients.

4. Click **OK**.

   The first two options generate the server’s certificate files, `server.crt` and `server.key`, and place them in the following location.

   `/var/opt/tableau/tableau_server/data/tabsvc/config/pgsql_\<version>/security`

   Use this `.crt` file if you need to configure clients for direct connections.

   Use the TSM CLI

   To enable SSL for internal traffic among the server components, run the following commands:

   ```
   tsm security repository-ssl enable
   tsm pending-changes apply
   ```
What the command does

repository-ssl enable generates the server’s certificate files, which it places in the following location:

/var/opt/tableau/tableau_server/data/tabsvc/config/pgsql_<version>/security

By default, this command sets Tableau Server to require SSL for traffic between the repository and other server components, as well as for direct connections from Tableau clients (including for connections through the tableau or readonly users).

To complete the configuration, you must also do the steps described in Configure Postgres SSL to Allow Direct Connections from Clients, to place the certificate files in the correct location on the client computers.

The pending-changes apply command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the --ignore-prompt option, but this does not change the restart behavior. For more information, see tsm pending-changes apply.

Option for repository-ssl enable

If you want to require SSL only for internal Tableau Server communication, and not for direct connections from client apps, use the following option with the repository-ssl enable command:

--internal-only

Cluster environments

If you run repository-ssl enable on a node in a cluster, it copies the required certificate file to the same location on each other node.
For more information about downloading the public certificate for direct connections, see Configure Postgres SSL to Allow Direct Connections from Clients.

Configure Postgres SSL to Allow Direct Connections from Clients

When Tableau Server is configured to use SSL for internal communication with the Postgres repository, you can also require SSL for Tableau clients that connect directly to the repository. Direct connections include those using the **tableau** user or the **readonly** user. Examples of Tableau clients include Tableau Desktop, Tableau Mobile, REST API, web browsers.

1. Run the following commands:

   ```bash
   tsm security repository-ssl enable
   tsm pending-changes apply
   ```

   This enables internal SSL support, generates new server certificate and key files, and requires all Tableau clients to use SSL to connect to the repository. For additional repository-ssl commands and options, see tsm security.

   The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see tsm pending-changes apply.

2. (Optional) If you have configured your client computer to validate Postgres SSL connections, then you must import the certificate that is generated by Tableau Server onto the computers running Tableau Desktop. For each client computer that will connect directly to the repository, do the following:

   - Copy the **server.crt** file to the client computer. You can find this file in the following directory:
Note: Do not copy `server.key` to the client computer. This file should reside only on the server.

- Import the certificate into the computer’s certificate store.

  For information, use the documentation from the operating system manufacturer.

Configure Mutual SSL Authentication

Using mutual SSL, you can provide users of Tableau Desktop and other approved Tableau clients a secure, direct-access experience to Tableau Server. With mutual SSL, when a client with a valid SSL certificate connects to Tableau Server, Tableau Server confirms the existence of the client certificate and authenticates the user, based on the user name in the client certificate. If the client does not have a valid SSL certificate, Tableau Server can refuse the connection. You can also configure Tableau Server to fall back to username/password authentication if mutual SSL fails.

Mutual SSL authentication is not supported on Tableau Mobile.

Use the TSM web interface

1. Configure SSL for External HTTP Traffic to and from Tableau Server.

2. Open TSM in a browser:

   https://<tsm-computer-name>:8850. For more information, see Sign in to Tableau Services Manager Web UI.


4. Under Authentication Method, select Mutual SSL in the drop-down menu.
5. Under Mutual SSL, select **Use mutual SSL and automatic sign in with client certificates**.

6. Click **Select File** and upload your certificate authority (CA) issued certificate to the server.

   This certificate must be a valid PEM-encoded x509 certificate with the extension .crt.

7. Enter remaining SSL configuration information for your organization.

   **Username format**: When Tableau Server is configured for mutual SSL, the server gets the user name from the client certificate, so it can establish a direct sign-in for the client user. The name that Tableau Server uses depends on how Tableau Server is configured for user authentication:

   - **Local Authentication**—Tableau Server uses the UPN (User Principal Name) from the certificate.
   - **Active Directory (AD)**—Tableau Server uses LDAP (Lightweight Directory Access Protocol) to get the user name.

   Alternatively, you can set Tableau Server to use the CN (Common Name) from the client certificate.

8. Click **Save Pending Changes** after you’ve entered your configuration information.
9. Click **Pending Changes** at the top of the page:

10. Click **Apply Changes** and **Restart**.

Use the TSM CLI

**Step 1: Require SSL for external server communication**

To configure Tableau Server to use SSL for external communication between Tableau Server and web clients, run the `external-ssl enable` command as follows, providing the names for the server certificate’s .crt and .key files:

```
tsm security external-ssl enable --cert-file <file.crt> --key-file <file.key>
```

- For `--cert-file` and `--key-file`, specify the location and file name where you saved the server’s CA-issued SSL certificate (.crt) and key (.key) files.

- The above command assumes the you are signed in as a user that has the **Server Administrator** site role on Tableau Server. You can instead use the `-u` and `-p` parameters to specify an administrator user and password.

- If the certificate key file requires a passphrase, include the `--passphrase` parameter and value.

**Step 2: Use mutual SSL**

Add mutual authentication between the server and each client, and allow for Tableau client users to be authenticated directly after the first time they provide their credentials.
1. Run the following command:

   tsm authentication mutual-ssl configure -cert-file
   <file.crt>

   For --cert-file, specify the location and file name of the server’s CA certificate (.crt) file, as in the previous step for external SSL.

   See the remaining sections in this article for any additional options you might want to include with the mutual-ssl configure command.

2. Run the following commands to enable mutual SSL and apply the changes:

   tsm authentication mutual-ssl enable
   tsm pending-changes apply

   The pending-changes apply command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the --ignore-prompt option, but this does not change the restart behavior. For more information, see tsm pending-changes apply.

---

**Additional options for mutual SSL**

You can use mutual-ssl configure to configure Tableau Server to support the following options.

For more information, see tsm authentication mutual-ssl <commands>.

**Fallback authentication**

When Tableau Server is configured for mutual SSL, authentication is automatic and clients must have a valid certificate. You can configure Tableau Server to allow a fallback option, to accept user name and password authentication.

   tsm authentication mutual-ssl configure -fb true
Tableau Server accepts username and password authentication from REST API clients, even if the above option is set to false.

User name mapping

When Tableau Server is configured for mutual SSL, the server authenticates the user directly by getting the user name from their client certificate. The name that Tableau Server uses depends on how the server is configured for user authentication:

- **Local Authentication**—uses the UPN (User Principal Name) from the certificate.
- **Active Directory (AD)**—uses LDAP (Lightweight Directory Access Protocol) to get the user name.

You can override either of these defaults to set Tableau Server to use the common name.

```bash
tsm authentication mutual-ssl configure -m cn
```

For more information, see Mapping a Client Certificate to a User During Mutual Authentication

**Certificate Revocation List (CRL)**

You might need to specify a CRL if you suspect that a private key has been compromised, or if a certificate authority (CA) did not issue a certificate properly.

```bash
tsm authentication mutual-ssl configure -rf <revoke-file.pem>
```

Mapping a Client Certificate to a User During Mutual Authentication

When you use mutual (two-way) SSL authentication, the client presents its certificate to Tableau Server as part of the authentication process. Tableau Server then maps user information in the client certificate to a known user identity. The strategy that Tableau Server uses to perform client mapping depends on the content of your organization’s client certificates.

This topic discusses the ways information in a client certificate can map to a user identity and how to change the way Tableau Server performs that mapping. To understand how the
mapping happens and whether you need to change it, you must know how client certificates are structured in your organization.

- **User-name mapping options**
- **Change the certificate mapping**
- **Address user-name ambiguity in multi-domain organizations**

**User-name mapping options**

Tableau Server uses one of the following approaches to map a client certificate to a user identity:

- **Active Directory.** If Tableau Server is configured to use Active Directory for user authentication, when Tableau Server receives a client certificate, it passes the certificate to Active Directory, which maps the certificate to an Active Directory identity. Any explicit user name information in the certificate is ignored.

  **Note:** This approach requires client certificates to be published for the user accounts in Active Directory.

- **User principal name (UPN).** A client certificate can be configured to store the user name in the user principal name field. Tableau Server reads the UPN value and maps it to a user in Active Directory or to a local user.

- **Common name (CN).** A client certificate can be configured to store the user name in the common name field of the certificate. Tableau Server reads the CN value and maps it to a user in Active Directory or to a local user.

If you configure the server for Active Directory authentication and UPN or CN user-name mapping, put the user name in one of the following formats:

`username`, `domain/username`, or `username@domain`.

**For example:** `asmith`, `example.org/asmith`, or `asmith@example.org`. 

---

Tableau Server on Linux Administrator Guide

Tableau Software
If the server uses local authentication, the format of the name in the UPN or CN fields is not predetermined, but the name in the field must match a user name on the server.

Change the certificate mapping

You use the tsm authentication mutual-ssl <commands> commands to map a client certificate to a user identity in Tableau Server:

```bash
tsm authentication mutual-ssl configure -m <value>
```

Possible values are `ldap` for Active Directory mapping, `upn` for UPN mapping, or `cn` for CN mapping.

When you first install and configure Tableau Server, the server sets the default user-name mapping to match the server's authentication type:

- If the server is configured to use Active Directory, it also uses Active Directory for mapping the certificate to the user identity.
- If the server is configured to use local authentication, the server gets the user-name value from the UPN field in the certificate.

If the default behavior for how Tableau Server maps a user name to an identity is not correct for your server configuration, run the following set of commands to change the mapping to use the CN value:

```bash
tsm authentication mutual-ssl configure -m cn

tsm pending-changes apply
```

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see tsm pending-changes apply.
Address user-name mapping ambiguity in multi-domain organizations

Under some circumstances, the user name in a certificate’s UPN or CN field can be ambiguous. This ambiguity can lead to unexpected results when the user name is mapped to a user identity on the server.

For example, if Tableau Server is presented with a user name that does not include a domain, the server maps the user name to an identity using the default domain. This can cause an incorrect user-name mapping, potentially assigning a user a different user’s identity and permissions.

This can occur particularly in environments where the following conditions apply:

- Your organization supports multiple Active Directory domains.
- The server is configured to use Active Directory authentication.
- The server is configured to use UPN or CN mapping.
- Some users have the same user name but different domains. For example, asmith@example.org and asmith@example.com.
- The user name in the certificate’s UPN or CN fields does not include the domain as part of the user name—for example, it shows asmith.

To avoid incorrect user-name mapping, make sure the client certificates include fully qualified user names with the domain, using the format asmith@example.org or example.org/asmith.

How Mutual SSL Authentication Works

Mutual (or two-way) SSL authentication provides a combination of an encrypted data stream, mutual authentication of both server and client, and direct access convenience. To use mutual SSL with Tableau Server, you need the following:

- A trusted CA-issued SSL certificate for Tableau Server.
- A certificate on each client that will connect to Tableau Server.
A Tableau Server configured to use mutual SSL.

Tableau Server and the client verify that each other has a valid certificate, and Tableau Server authenticates the user, based on the user name in the client certificate.

The following image shows a little more detail about the sequence of events that occurs with mutual SSL.

1. The user navigates to Tableau Server.
2. Tableau Server sends its SSL certificate to the client computer.
3. The client computer verifies the Tableau Server certificate.
4. The client computer sends its certificate to Tableau Server.
5. Tableau Server verifies the client certificate.
6. Tableau Server references the user name in the client certificate to authenticate the user.

**System User, sudo Privileges, and systemd**

This topic describes system user, systemd user service, and sudo privilege in the context of Tableau Server.
Privilege separation

Following standard security best practices, Tableau Server for Linux runs processes with the least privilege possible. During installation, the unprivileged user, `tableau`, is created in a server authorized group (`tableau`).

An example user entry in the `/etc/passwd` file is as follows:

- `tableau:x:993:991:Tableau Server:/var/opt/tableau/tableau_server:/bin/bash`

All processes run as the unprivileged `tableau` user. This means that if one of the Tableau Server processes (such as a process displaying vizzes to users) were compromised in some fashion, it would only be able to impact Tableau Server, not the rest of the Linux system. For this reason, you should not add the `tableau` unprivileged user to the `tsadmin` group. The `tsadmin` group should only contain accounts that require authorization to access OS-related Tableau configurations.

The `tableau` user and `tsadmin` group are created by the Tableau Server initialization process. You can specify a different unprivileged user or TSM authorization group during installation. For more information about system users and groups, in the context of installation and LDAP configuration, see Identity Store.

**sudo privileges**

The first version (10.5) of Tableau Server on Linux relied on sudo privileges by updating the sudoers file. Updating the sudoers file conflicts with some system management configuration best practices and security policies. Therefore, the 2018.1 version (and later) of Tableau Server no longer creates or uses a privileged user (`tsmagent`). Nor does the current version of Tableau Server update or include a Tableau-specific sudoers file.

All privileged operations now occur during package and software installation.
**systemd user service**

In the 10.5 version of Tableau Server on Linux, sudo privileges were required to modify or restart the TSM services, which required systemctl commands. All TSM services were run from the normal system-wide systemd process (process ID 1, which runs all processes on the operating system). In this scheme, systemd process runs as root. Therefore, the 10.5 version of Tableau Server required sudo privileges.

With the current 2018.1 (and later) releases, we have removed the need for sudo privileges by making use of the systemd capability to run as a user service. The systemd user service runs as a normal user, so it does not need any special privileges once it has been enabled.

In normal use cases, you will not need to issue commands to systemd because TSM takes care of that. However, for troubleshooting scenarios, you may need to interact with the TSM services. As with the previous versions, you will issue the same systemctl commands for these scenarios. However, commands should be run as the tableau user, and not as root. If you specified a different unprivileged system user during Tableau Server setup, then run the commands as that user.

**Running systemctl commands**

Use the following syntax example to issue request to systemd with the systemctl commands.

Start a session as the unprivileged user. The `-l` flag is critical to set environment variables properly.

```
sudo su -l tableau
```

Then issue commands. For example:

```
systemctl --user status tabadmincontroller_0
```

```
systemctl --user restart tabadmincontroller_0
```
Security Hardening Checklist

The following list provides recommendations for improving the security ("hardening") of your Tableau Server installation.

1. Update to the current version

We recommend that you always run the latest version of Tableau Server. Additionally, Tableau periodically publishes maintenance releases of Tableau Server that include fixes for known security vulnerabilities. (Information regarding known security vulnerabilities can be found on the Security Bulletins page.) We recommend that you review maintenance release notifications to determine whether you should install them.

To get the latest version or maintenance release of Tableau Server, visit the Customer Portal page.

2. Configure SSL/TLS with a valid, trusted certificate

Secure Sockets Layer (SSL/TLS) is essential for helping to protect the security of communications with Tableau Server. Configure Tableau Server with a valid, trusted certificate (not a self-signed certificate) so that Tableau Desktop, mobile devices, and web clients can connect to the server over a secured connection. For more information, see SSL.

3. Disable older versions of TLS

Tableau Server uses TLS to authenticate and encrypt many connections between components and with external clients. External clients, such as browsers, Tableau Desktop, Tableau Mobile connect to Tableau using TLS over HTTPS. Transport layer security (TLS) is an improved version of SSL. In fact, older versions of SSL (SSL v2 and SSL v3) are no longer considered to be adequately secure communication standards. As a result, Tableau Server does not allow external clients to use SSL v2 or SSL v3 protocols to connect. We recommend that you only allow external clients to connect to Tableau Server with TLS v1.2.

Specifically, we recommend that you disable TLS v1 and TLS v1.1 on Tableau Server. However, before you disable a specific version of TLS, verify that the browsers that your
users connect to Tableau Server with support TLS v1.2. In some cases, you may need to preserve support for TLSv1.1.

The following tsm command enables TLS v1.2 (using the "all" parameter) and disables SSL v2, SSL v3, TLS v1, and TLS v1.1 (by prepending the minus [-] character to a given protocol).

```
tsm configuration set -k ssl.protocols -v 'all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1'
```

```
tsm pending-changes apply
```

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see tsm pending-changes apply.

4. Disable Triple-DES cipher suite

The Triple-DES cipher suite is no longer considered adequate to encrypt sessions on the internet. Specifically, running Triple-DES ciphers leaves the Tableau Server vulnerable to information disclosure and denial of service attacks. You can learn more at the National Vulnerability Database webpage for CVE-2016-2183.

Triple-DES is enabled by default on the version of OpenSSL that is running on Tableau Server. However, other deprecated cipher suites (MD5 and RC4) are disabled. To add Triple-DES to the list of disabled ciphers, run the following commands. (The `!aNULL` parameter forces clients to use a legitimate cipher.)

```
tsm configuration set -k ssl.ciphersuite -v
'HIGH:MEDIUM:!aNULL:!MD5:!RC4:!3DES'
```

```
tsm pending-changes apply
```
5. Configure SSL encryption for internal traffic

Configure Tableau Server to use SSL to encrypt all traffic between the Postgres repository and other server components. By default, SSL is disabled for communications between server components and the repository. We recommend enabling internal SSL for all instances of Tableau Server, even single-server installations. Enabling internal SSL is especially important for multi-node deployments. See Configure SSL for Internal Postgres Communication.

6. Enable firewall protection

Tableau Server was designed to operate inside a protected internal network.

**Important:** Do not run Tableau Server, or any components of Tableau Server on the internet or in a DMZ. Tableau Server must be run within the corporate network protected by an internet firewall. We recommend configuring a reverse proxy solution for internet clients that need to connect to Tableau Server. See Configuring Proxies for Tableau Server.

A local firewall should be enabled on the operating system to protect Tableau Server in single and multi-node deployments. In a distributed (multi-node) installation of Tableau Server, communication between nodes does not use secure communication. Therefore, you should enable firewalls on the computers that host Tableau Server. See Configure Local Firewall.

To prevent a passive attacker from observing communications between nodes, configure a segregated virtual LAN or other network layer security solution.

See Tableau Services Manager Ports to understand which ports and services Tableau Server requires.
7. Restrict access to the server computer and to important directories

Tableau Server configuration files and log files can contain information that is valuable to an attacker. Therefore, restrict physical access to the machine that is running Tableau Server. In addition, make sure that only authorized and trusted users have access to the Tableau Server files in the /var/opt/tableau/tableau_server/ directory.

8. Generate fresh secrets and tokens

Any Tableau Server service that communicates with repository or the cache server must first authenticate with a secret token. The secret token is generated during Tableau Server setup. The encryption key that internal SSL uses to encrypt traffic to Postgres repository is also generated at during setup.

We recommend that after you install Tableau Server, you generate new encryption keys for your deployment.

These security assets can be regenerated with the tsm security regenerate-internal-tokens command.

Run the following commands:

    tsm security regenerate-internal-tokens
    tsm pending-changes apply

9. Disable services that you're not using

To minimize the attack surface of the Tableau Server, disable any connection points that are not needed.

REST API

The REST API interface is enabled by default. If no applications will make REST API calls to your installation of Tableau Server 9.3 (or later), disable it by using the following commands:

    tsm configuration set -k api.server.enabled -v false
Important: Tableau Prep uses REST API to access Tableau Server. If your organization uses Tableau Prep, do not disable REST API.

JMX Service

JMX is disabled by default. If it’s enabled but you’re not using it, you should disable it by using the following:

```
tsm configuration set -k service.jmx_enabled -v false
```

tsm pending-changes apply

10. Verify session lifetime configuration

By default, Tableau Server does not have an absolute session timeout. This means that client sessions can remain open indefinitely if the Tableau Server inactivity timeout is not exceeded. (The default inactivity timeout is 240 minutes.)

If your security policy requires it, you can set an absolute session timeout. Be sure to set your absolute session timeout in a range that allows the longest-running extract or publishing operations in your organization. Setting the session timeout too low may result in extract and publishing failures for long-running operations.

To set the session timeout run the following commands:

```
tsm configuration set -k wgserver.session.apply_lifetime_limit -v true
```

tsm configuration set -k wgserver.session.lifetime_limit -v value, where value is the number of minutes. The default is 1440, which is 24 hours.

```
tsm configuration set -k wgserver.session.idle_limit -v value, where value is the number of minutes. The default is 240.
```
11. Configure a server safelist for file-based data sources

By default, Tableau Server allows authorized Tableau Server users to build workbooks that use files on the server as file-based data sources (such as spreadsheets). In this scenario, files are accessed by the `tableau` system account.

To prevent unwanted access to files, we recommend that you configure safelist (sometimes referred to as "whitelist") functionality. This lets you limit `tableau` account access to just the directory paths where you host data files.

1. On the computer running Tableau Server, identify the directories where you will host data source files.

   **Important** Make sure the file paths you specify in this procedure exist on the server. If the paths do not exist when the computer starts, Tableau Server will not start.

2. Run the following commands:

   ```bash
   tsm configuration set -k native_api.allowed_paths -v "path"
   , where path is the directory to add to the safelist. All subdirectories of the specified path will be added to the safelist. If you want to specify multiple paths, separate them with a semicolon, as in this example:
   
   tsm configuration set -k native_api.allowed_paths -v "/data-sources;/HR/data"
   
   tsm pending-changes apply
   ```
12. Enable HTTP Strict Transport Security for web browser clients

HTTP Strict Transport Security (HSTS) is a policy configured on web application services, such as Tableau Server. When a conforming browser encounters a web application running HSTS, then all communications with the service must be over a secured (HTTPS) connection. HSTS is supported by major browsers.

For more information about how HSTS works and the browsers that support it, see The Open Web Application Security Project web page, HTTP Strict Transport Security Cheat Sheet.

To enable HSTS, run the following commands on Tableau Server:

```
tsm configuration set -k gateway.http.hsts -v true
```

By default, HSTS policy is set for one year (31536000 seconds). This time period specifies the amount of time in which the browser will access the server over HTTPS. You should consider setting a short max-age during initial roll-out of HSTS. To change this time period, run `tsm configuration set -k gateway.http.hsts_options -v max-age=<seconds>`.

For example, to set HSTS policy time period to 30 days, enter `tsm configuration set -k gateway.http.hsts_options -v max-age=2592000`.

```
tsm pending-changes apply
```

13. Disable Guest access

Core-based licenses of Tableau Server include a Guest user option, which allows any user in your organization to see and interact with Tableau views embedded in web pages.

Guest user access is enabled by default on Tableau Servers deployed with core-based licensing.
Tableau Server on Linux Administrator Guide

Guest access allows users to see embedded views. The Guest user cannot browse the Tableau Server interface or see server interface elements in the view, such as user name, account settings, comments, and so on.

If your organization has deployed Tableau Server with core licensing and Guest access is not required, then disable Guest access.

You can disable Guest access at the server or site level.

You must be a server administrator to disable the Guest account at either the server or the site level.

**To disable Guest access at the server level:**

1. In the site menu, click **Manage All Sites** and then click **Settings > General**.
2. For **Guest Access**, clear the **Enable Guest account** check box.
3. Click **Save**.

**To disable Guest access for a site:**

1. In the site menu, select a site.
2. Click **Settings**, and on the Settings page, clear the **Enable Guest account** check box.

For more information, see Guest User.

**Change List**

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 2017</td>
<td>Ported and updated for Tableau Services Manager and Linux platform.</td>
</tr>
<tr>
<td>May 2018</td>
<td>Added clarification: Do not disable REST API in organizations that are running Tableau Prep.</td>
</tr>
</tbody>
</table>
Manage Licenses

Licensing Overview

Tableau Server term licenses are available with two different license metrics: User-Based and Core-Based. Term licenses, also known as subscription licenses, allow you to use and update Tableau Server for a specified period of time.

Tableau offers multiple types of User-Based term licenses that grant a range of capabilities at various price points, providing the flexibility for organizations to pay for the data analysis and data visualization capabilities that each type of user in their organization needs. To learn more, see User-based licenses.

License metric: User-Based or Core-Based

Your license is defined by the metric that permits use of Tableau Server.

- A User-Based license metric allows you to deploy Tableau Server on a single computer or on multiple computers in a cluster. Each user that accesses Tableau Server must be licensed. Administrators add users and license them.

- A Core-Based license metric imposes no constraints on the number of user accounts in Tableau Server. Instead, the license specifies the maximum number of computer cores on which you can run Tableau Server. You can install Tableau Server on a single computer or across multiple computers as a multi-node cluster, as long as the total number of cores in all the computers does not exceed the total number that the license allows.

**Note:** Not all processes installed with Tableau Server impact the calculation of total number of cores used. A subset of processes are considered "licensed processes." Core licensing is calculated only on computers running licensed
processes. If a computer has one or more licensed processes installed on it, the cores on that computer count toward the total cores used. For more information about licensed processes, see Licensed processes.

The topics in this section provide guidance about how to view and refresh Tableau licensing, as well as a topic that describes how to add user capacity on Tableau Server.

**Note:** As a Tableau Server administrator, you may also be tasked with managing Tableau Desktop deployment and tracking license usage on client computers. If your organization will be using Desktop License reporting, you need to configure Tableau Server to support this. For details, see Configure Desktop License Reporting. For additional information on licensing and management tasks related to Tableau Desktop, see the Tableau Desktop Deployment Guide.

**User-Based licenses**

Tableau offers User-Based term licenses that grant a range of capabilities at various price points. Multiple types of User-Based term licenses are available: Viewer, Explorer and Creator. The following capabilities are available to users with these licenses:

- **Viewer licenses** let users view and interact with workbooks in Tableau Server or Tableau Online. Viewer licenses also let users access Tableau Mobile, add comments to workbooks, download .png and .pdf versions of workbooks, download workbook summary data, create subscriptions for themselves, and receive data-driven alerts.
- **Explorer licenses** are equivalent to the User-Based term licenses available in previous Tableau Server and Tableau Online releases, and include the capabilities provided with Viewer licenses. Depending on a user’s site role, a user with this license will have access to workbook authoring capabilities using a web browser, as well as a full set of collaboration features.
- **Creator licenses** grant a wide range of capabilities when using Tableau Server and Tableau Online, and also grant use of Tableau Desktop and Tableau Prep. Depending on a user’s site role, a user with a Creator license might have all of the capabilities
available under the Explorer license, as well as the following capabilities when using Tableau Server and Tableau Online:

- Create and publish new workbooks from a new data source.
- Edit embedded data sources in the Data pane.
- Create and publish new data connections.
- Create new workbooks using Dashboard Starters (Tableau Online only).

**Note:** Tableau Server administrators will always use a Creator license, if available; additionally, activating a Creator license on Tableau Server causes all Tableau Server administrator accounts to require Creator licenses.

Product keys provide administrators with a set of each type of license, which they can activate by assigning associated site roles to users. The first Creator or Explorer license that you add to Tableau Server activates Tableau Server, and will be used by a Server Administrator. Administrators can activate additional Creator, Explorer and Viewer licenses in Tableau Server or Tableau Online to increase licensed user capacity.

**Data Management Add-On**

The Data Management Add-on Product Key includes Tableau Prep Conductor for a single Tableau Server Deployment, which may be User-Based or Core-Based. A Deployment includes a licensed production Tableau Server installation and licensed non-production Tableau Server installations that support the production installation.

- For more information on Deployment, see the EULA Documentation.
- For more information on Tableau Prep Conductor licensing, see Licensing Tableau Server.

**Tableau Server licenses and site roles after an upgrade**

When upgraded to 2018.2, Tableau Server will display the new licensing information and site roles. Any users in the **Read Only** site role prior to the upgrade are reassigned to the **Viewer** site role.
To learn more about the site roles available with each type of User-Based license, see Set Users’ Site Roles. To learn about pricing for each type of User-Based license, see Tableau Pricing. To learn about troubleshooting issues with licensing, see Troubleshoot Licensing.

Tableau Server product key activation

You can activate the same Tableau Server product key up to three times. This allows you to test Tableau Server (in a sandbox or QA environments, for example), as well as use Tableau in production. To maximize your activations, you should deactivate your product key when you remove Tableau Server from a computer, unless you will be reinstalling Tableau on the same computer. Doing this gives you the opportunity to use the activation on a different computer. For example, if you move Tableau Server from one computer to another, deactivate the product key, then remove Tableau from the original computer. When you install Tableau on the new computer, you can activate the key there without any conflict. If you are removing Tableau Server to reinstall it on the same computer, you don't need to deactivate the key. Tableau will use the key when reinstalled. For example, if you are moving Tableau from one drive on a computer to a different drive on the same computer. For information on how to deactivate a product key, see tsm licenses deactivate.

Tableau Server licensing and virtual machines (VMs)

If you run Tableau Server on VMs, either locally, or in the cloud, be aware of the potential for complications related to licensing. If you are simply upgrading Tableau Server on the VM, you do not need to take any extra action related to licensing. If you plan to clone the VM to create either a new production or test environment to upgrade, you need to deactivate any Tableau Server licenses before cloning. If you do not do this, the new VM environment can end up with an untrusted license, and any attempts to upgrade will fail. You may also end up hitting the maximum number of activations for the licenses.

To avoid issues with licensing on VMs, deactivate all Tableau licenses before cloning a VM or allowing it to be permanently shut down.

View Server Licenses

Server administrators can view the license and product key information for Tableau Server.
Viewing licenses from the Tableau Server web UI

How you navigate to the Licenses page in Tableau Server depends on whether you have a single site, or multiple sites.

- On a server with a single site, click **Settings** and **Licenses**:

- On a multi-site server, click **Manage All Sites** on the site menu, **Settings**, and **Licenses**:

  ![Desktop.png](Desktop.png)

  ![Desktop.png](Desktop.png)

  **Note:** The **Manage All Sites** option only displays when you are signed in as a server administrator.

This page displays information for any licenses that have been activated on your server, including any user-based (term) or core-based licenses.

Use the TSM web interface

1. Open TSM in a browser:

   http://<tsm-computer-name>:8850

2. Click **Configuration**, and then click **Licensing**:

   The table displays the product key, expiration date, and expiration of maintenance.
Note: The TSM Web UI provides a limited amount of licensing information. Use the TSM CLI or the Tableau Server Web UI to see additional licensing information, including the number of each type of user-based license (Creator, Explorer and Viewer).

Use the TSM CLI

1. Open a command prompt as administrator on the initial node (the node where TSM is installed).

2. Run the following command:

   tsm licenses list

The command lists licenses that are activated on the Tableau Server deployment.

For example, a server with five Creator licenses, five Explorer licenses, 100 Viewer licenses, and a Data Management Add-on would provide command output similar to the following:

<table>
<thead>
<tr>
<th>KEY</th>
<th>TYPE</th>
<th>CREATOR</th>
<th>EXPLORER</th>
<th>VIEWER</th>
<th>DATA MANAGEMENT ADD-ON</th>
<th>GUEST ACCESS LIC EXP</th>
<th>LIC EXP</th>
<th>MAINT EXP</th>
<th>VALID</th>
</tr>
</thead>
<tbody>
<tr>
<td>TS53-0002 6558-3558-0055</td>
<td>Term</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>false</td>
<td>false</td>
<td>12/31/19</td>
<td>N/A</td>
<td>true</td>
</tr>
<tr>
<td>TS53-0002 6558-3558-0055</td>
<td>Term</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>false</td>
<td>false</td>
<td>12/31/19</td>
<td>N/A</td>
<td>true</td>
</tr>
<tr>
<td>TS53-0002 6558-3558-0055</td>
<td>Term</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>false</td>
<td>false</td>
<td>12/31/19</td>
<td>N/A</td>
<td>true</td>
</tr>
<tr>
<td>TS53-0002 6558-3558-0055</td>
<td>Term</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>true</td>
<td>true</td>
<td>12/31/19</td>
<td>N/A</td>
<td>true</td>
</tr>
</tbody>
</table>

The following fields are returned:

- **KEY**: A globally unique 16-character string that identifies the license.
- **TYPE**: Describes the type of license
  - Term: Term licenses map to a subscription schedule and must be renewed. The expiration date is listed under the LIC EXP field.
  - Perpetual: Perpetual licenses are purchased once and do not need to be renewed but must be refreshed to update the MAINT EXP or maintenance expiration date.
  - Cores: Core licenses are licenses that map to the number of cores on the computers running specific Tableau Server services. Core licensing allows for a
guest user access to views on the server or embedded on other web servers.
Core licenses also allow for unlimited Explorer and Viewer users.

- **CREATOR**: The number of Creator licenses issued to the Tableau Server deployment.
- **EXPLORER**: The number of Explorer licenses issued to the Tableau Server deployment.
- **VIEWER**: The number of Viewer licenses issued to the Tableau Server deployment.
- **DATA MANAGEMENT ADD-ON**: Tableau Server is licensed for the Data Management Add-on (True/False). See Data Management Add-On.
- **GUEST ACCESS**: Tableau Server is licensed for a Guest User. See Guest User. The ability to leverage a Guest User requires Core licensing. See TYPE field.
- **LIC EXP**: The date that the license expires and Tableau Server will stop working. Term licenses expire. See TYPE field. Visit the Tableau [Customer Portal](#) to refresh licenses.
- **MAINT EXP**: Applies only to legacy perpetual licenses (TYPE = Perpetual). For Term licenses, this field will output, N/A. MAINT EXP displays the date that the maintenance contract for the Tableau Server deployment expires. To update the license maintenance key see Refresh Expiration Date for the Product Key. Visit the Tableau [Customer Portal](#) to view maintenance purchase history and to purchase additional maintenance.
- **VALID**: Specifies if the license is valid (True/False). Invalid licenses will cause server failure.

**Note**: The license terms for Creator, Explorer and Viewer users are set according to the terms of the user-based license (term license), if present. So, a server with only a core-based license will have unlimited Explorer and Viewer users and guest access, but no Creator users. To learn more, see Use user-based licenses on a server with core-based licensing.

**Refresh Expiration Date for the Product Key**

When you purchase a new subscription, you must refresh your product key(s). Refreshing the product key(s) updates the product key with the new date that reflects the new
expiration dates. If a subscription (term) product key is not refreshed and has expired, Tableau will stop working and you will have to activate a new product key. On the other hand, if the product key is perpetual (legacy) and its maintenance has expired, Tableau will continue to operate but you will not have access to upgrades until the maintenance is renewed. After renewing the maintenance, refresh the existing key to update its maintenance expiration date. For more information about different product key types and associated licenses, see tsm licenses list.

**Note:** This topic describes how to refresh the expiration date for Tableau Server. For information about refreshing the maintenance date on Tableau Desktop see [Refreshing Tableau Desktop Product Key](#) in the Tableau Knowledge Base.

**Before you begin**

Verify the expiration date of your license(s). You can view the expiration date by following the TSM web interface procedure below, or by running tsm licenses list in the CLI.

- Compare the date with the date displayed in the Tableau Customer Portal.
- If the portal does not display the date that you expect, contact Customer Success.
- To renew your license, visit the Tableau renewal web page.

If the TSM date matches the portal date and the following refresh operation fails, contact Tableau Support.

**Use the TSM web interface**

1. Open TSM in a browser:

   http://<tsm-computer-name>:8850
2. Click **Configuration** and **Licensing** and click **Refresh All**:

![Configuration and Licensing](image)

**Use the TSM CLI**

1. Open a command prompt as administrator on the initial node (the node where TSM is installed).

2. Run the following command:

   ```
   tsm licenses refresh
   ```

**Add Capacity to Tableau Server**

You may need to add capacity to your Tableau Server installation to allow you to increase the number of users (if you have a user-based license) or the number of cores (if you have a core-based license).

Tableau will provide you with a new product key that adds capacity to your existing Tableau Server installation. You need to activate this key and use it together with your existing product key(s) to get the combined capacity you are licensed for. Each feature (e.g., "Data management add-on") and license type (e.g., "Explorer") requires a key. For more information about the relationship between keys and licenses, see tsm licenses list.

Follow the steps below to add a product key to Tableau Server.
Note: This process requires a restart of Tableau Server.

Use the TSM web interface

1. Open TSM in a browser:

   https://<tsm-computer-name>:8850

2. Click Licensing on the Configuration tab and click Activate License:

   ![TSM Configuration UI]

   Access Tableau Server product keys in the Customer Portal. View Desktop License Usage for more information about

3. Enter or paste your new product key and click Activate:
4. On the Register page, enter your information into the fields and click **Register**.
### Register with Tableau

Register with Tableau. All fields are required.

#### Contact Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>Last Name</td>
</tr>
<tr>
<td>Phone Number</td>
<td>Email</td>
</tr>
</tbody>
</table>

#### Company Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>Industry</td>
</tr>
<tr>
<td>Department</td>
<td>Job Role</td>
</tr>
</tbody>
</table>

#### Region Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>City</td>
<td>Postal Code</td>
</tr>
<tr>
<td>Country/Region</td>
<td>State/Province</td>
</tr>
</tbody>
</table>

[Register button]
5. Restart Tableau Server after registration is complete.

Use the TSM CLI

1. Copy the product key to your computer.

2. Run the following command:

   \texttt{tsm licenses activate --license-key \langle license key\rangle}

3. After activation, you need to register Tableau Server. To do this, create a registration file and then pass it as an option with the \texttt{tsm register} command.

   a. Generate a template that you can edit by running the following command:

   \texttt{tsm register --template > /path/to/<registration_file>.json}

   b. Edit the template file to create your completed registration file.

Here is an example of a registration file in the required format:

\{
   "zip" : "97403",
   "country" : "USA",
   "city" : "Springfield",
   "last_name" : "Simpson",
   "industry" : "Energy",
   "eula" : "yes",
   "title" : "Safety Inspection Engineer",
   "phone" : "5558675309",
   "company" : "Example",
   "state" : "OR",
   "department" : "Engineering",
   "first_name" : "Homer",
\}
c. After saving changes to the file, pass it with the \texttt{--file} option to register Tableau Server:

\texttt{tsm register --file /path/to/<registration_file>.json}

For example:

\texttt{tsm register --file /usr/share/tableau-reg-file.json}

4. Restart the server:

\texttt{tsm restart}

\textbf{Activate Tableau Server Offline - Adding a License}

When you install Tableau Server, you have to activate at least one product key. Doing this activates the server, and specifies the number of license levels you can assign to users. There are also times you may need to activate licenses after Tableau Server is installed, for example, if you add capacity to your server, or get a new product key. If you don't have your product key, you can get it from the Tableau Customer Account Center.

In most cases, you can activate your key directly from Tableau, either during installation, or later, using the Tableau Services Manager (TSM) Licenses page, but there are some circumstances that don't allow you to do this. If your computer is not connected to the internet for example, or has a firewall that restricts access outside your intranet. In these cases you need to do an offline activation.

- Offline activation during install—To complete an offline activation when you are installing Tableau Server, see Offline Activation When Installing Tableau Server.
- Offline activation of licenses after install—To complete an offline activation after your server is installed and running, follow the steps below.
Offline activation overview and prerequisites

Offline activation of Tableau Server involves several steps. If you have never activated a product key before on your computer, you need to run through the steps twice, once to initialize licensing on the computer, and a second time to activate the key. If you have had a license on the computer in the past, you run through the steps only once.

Offline activation steps:

1. Generate an offline activation request file (`offline.tlg`).
2. Upload the offline activation request to Tableau and download the resulting activation file (`activation.tlf`).
3. Upload the activation file to Tableau Server.

If this is the first time a Tableau product key has been activated on the computer, you repeat these three steps a second time.

Use the TSM web interface

If you attempt to activate your product key from the TSM licenses page and see a dialog that says online activation is unavailable, you can activate the key offline. Click **Activate License Offline**.
1. Create Offline File

Your first step is to create an offline file (offline.tlq).

Create an offline file you will upload to Tableau. If your license key is not pre-filled in the form, enter your key and click **Create Offline File** to generate an offline file (offline.tlq) on the local computer.
Copy the `offline.tlq` file to a computer with internet access. You need to upload this file to Tableau to generate an activation file.

2. Upload and Submit Offline File

Next, on the computer where you copied the `offline.tlq` file, go to [http://www.tableau.com/support/activation](http://www.tableau.com/support/activation) to upload your file and submit it. Doing this automatically generates an activation file (`activation.tlf`) that you can download and copy back to the Tableau Server computer.

   a. On the Offline Activation page, click **Choose File** to select the `offline.tlq` file.

   b. Click **Upload Activation File** to submit the file to Tableau.

   c. Click the [here](http://www.tableau.com/support/activation) link to download the resulting `activation.tlf` file to your computer.
d. Copy the downloaded activation.tlf file to the computer where Tableau Server is installed.

3. Click **Next Step** to move to the next dialog.

4. **Upload Activation File**

On the Tableau Server computer, click **Upload Activation File** to upload the activation.tlf file to Tableau Server.
5. Create, Upload, and Submit a Second Offline File
   a. Click Create Offline File to generate a second offline.tlf file.
   b. Copy that file to the computer that has internet access.
   c. Open a browser session to http://www.tableau.com/support/activation and upload your new offline file.
   d. Download the resulting activation.tlf file.
   e. Copy the file to the Tableau Server computer.

6. Click Next Step and then click Upload Activation File to upload the second activation.tlf file to Tableau Server.
Click **Activate License** to complete the offline activation. You will need to restart Tableau Server for the changes to take effect.

**Use the TSM CLI**

Log in to Tableau Services Manager

Before you can proceed you must log in to Tableau Services Manager (TSM).

To log in to TSM, run the following command:

```
tsm login -u <username>
```

**What if I can't log in?**

The account that you use to configure the rest of the installation must be a member of the tsmadmin group that was created during initialization. To view the user accounts in the tsmadmin group, run the following command:

```
grep tsmadmin /etc/group
```

If the user account is not in the group, run the following command to add the user to the tsmadmin group:

```
sudo usermod -G tsmadmin -a <username>
```

After you have added the user to the tsmadmin group, run the tsm login command.

**Step 1 - Generate an offline activation request file**

1. On the initial node, open a terminal session.

2. Type this command to get your offline activation file:

   ```
   tsm licenses get-offline-activation-file -k <product-key> -o <target-directory>
   ```
You can get your product key from the Tableau Customer Portal. The target directory must already exist.

3. Copy the offline activation file (offline.tlq) from the target directory to a computer that has internet access.

Step 2 - Upload the offline activation request to Tableau

1. On the computer that has internet access, go to the Tableau Product Activations page.

2. Complete the instructions to upload your offline.tlq file.
   
   This creates an activation file, activation.tlf.

3. Download the resulting activation file from Tableau.

Step 3 - Initialize or activate your license

1. Copy the activation file (activation.tlf) to a location accessible from your Tableau Server computer.

2. Run the following command:

   tsm licenses activate -f <path-and-activation-file>

3. Restart the server for licensing changes to take effect:

   tsm restart

First time license activation

If this is the first Tableau license activated on the computer, you will see this message:

Your license has been initialized. To complete the activation, we need one more exchange. Generate and send to Tableau a second activation request file.
Repeat steps 1 through 3 above to activate your license. You need to generate a second offline.tlg file, upload it to Tableau, and download the resulting activation.tlf file, then use that file to activate your license.

If you are not sure whether you need to repeat the steps, you can run this command:

```bash
tsm licenses list
```

If you see a message like this one you need to repeat the steps above:

*No licenses are currently activated.*

Subsequent license activation

If this is not the first Tableau license activated on the computer, or if you have completed the steps above two times, you should see a success message:

*Activation successful.*

Tableau Server is activated. If you need additional assistance, contact [Tableau Technical Support](https://www.tableau.com/support).

### Automate Licensing Tasks

You can use `tsm licenses` to perform licensing tasks such as activating or deactivating a Tableau Server product key on- or off-line, and getting associated files for offline activation or deactivation. However, Tableau Server must already be deployed and configured. You can automate these licensing tasks using the [Tableau Services Manager API](https://www.tableau.com/support/services-manager).

```bash
C:\ProgramData\Tableau\Tableau Server\data\tabsvc\logs\*
```

### Troubleshoot Licensing

This topic includes instructions for troubleshooting issues related to Tableau Server licensing.
Handle an unlicensed server

Tableau offers two licensing models: user-based and core-based. To learn more about user-based and core-based licensing, see Licensing Overview.

User-based licensing requires each active user account to be covered by a license. User-based licenses have a defined capacity, or number of users that they allow. Each user is assigned a unique user name on the server and is required to identify themselves when connecting to the server.

Core-based licensing has no constraints on the number of user accounts in the system, but it does restrict the maximum number of processor cores that Tableau Server can use. You can install Tableau Server on one or more machines to create a cluster, with the restriction that the total number of cores in all the machines does not exceed the number of cores you have licensed and that all of the cores on a particular machine are covered by the license.

Unlicensed User-Based Server

The most common reason for a server that has user-based licensing to be unlicensed is an expired product key or an expired maintenance contract.

Unlicensed Core-Based Server

A core-based server can become unlicensed for a variety of reasons, such as when Tableau Server nodes running licensed processes cannot contact the Tableau Server node running the License Manager service. To learn more about licensed processes, see Tableau Server Processes.

When the server is unlicensed you may not be able to start or administer the server. You can, however, manage your licenses using the tsm licenses command.

Troubleshoot user-based licensing

This section provides information about resolving issues that can occur when adding the user-based Viewer, Explorer and Creator licenses to Tableau Server or Tableau Online, or when these licenses expire. The highest available license type is Creator, followed by
Explorer, and finally Viewer. To learn more about user-based licensing, see Licensing Overview.

A user or administrator is unlicensed due to license expiration

To avoid having users unexpectedly become unlicensed or move to another site role, you should always do one of the following before the license that they are currently using expires:

- Renew and activate a replacement license. If a user occupies a Creator, Explorer or viewer license and their license expires, they will use another license of the same type, if available.
- Change the site role of those users to allow the use of a license that is not due to expire.

To learn how site roles can be changed to require a different license, see Set Users’ Site Roles.

The reassignment of users to new licenses is governed by the following logic:

- When a Server Administrator user occupies a Creator license and their license expires (with no replacement licenses available), they are reassigned to an Explorer license if any Explorer licenses are available. This license reassignment occurs in order of most recent login. Server Administrators displace other users who might be currently using an Explorer license. If no Creator or Explorer licenses are available a Server Administrator becomes unlicensed.
- When a non-Server Administrator user occupies a Creator license and their license expires (with no replacement licenses available), they become unlicensed. To avoid having these users become unlicensed, change their site role prior to license expiration. This is especially important for users in the Site Administrator Creator site role, who must move to the Site Administrator Explorer site role before their Creator license expires to avoid losing Site Administrator capabilities.
- When a non-Server Administrator user occupies an Explorer or Viewer license and their license expires (with no replacement licenses available), they are upgraded to a higher license type, if licenses of that type are available. Specifically, the following occurs when a license expires:
  - Users who occupy an Explorer license will move to a Creator license, if available (with no change to site role).
Users who occupy a Viewer license will move to an Explorer license, if available. If no Explorer licenses are available, these users will move to a Creator license, if available (with no change to site role).

If no licenses are available at the higher license types, those users are moved to Unlicensed.

Users are reassigned to a new license as described above in order of most recent login, with lower license types reassigned first (first Viewer, then Explorer, and then Creator).

For example: Two users with a Viewer license, a user with the Creator license, and two Server Administrators with a Creator license all have their licenses expire. Four unexpired Explorer licenses are available for these users. In this situation, the following occurs in the order shown below:

1. The user with a Viewer license who logged in most recently is reassigned to an Explorer license.
2. The second user with a Viewer license is reassigned to an Explorer license.
3. The Server Administrator user with a Creator license who logged in most recently is reassigned to an Explorer license, and then the second Server Administrator with a Creator license is reassigned to the remaining Explorer license.
4. The user with the Creator license becomes unlicensed.

Server Administrator site role is unchanged when using a Creator license

Server Administrators gain Creator capabilities if Creator licenses are available in Tableau Server, with no change to their site role name. All other Tableau Server and Tableau Online users gain Creator licenses only if assigned to a site role that includes Creator in its name.

Licenses are not immediately available

When you add a role-based license to Tableau Server, those licenses become available to all users when you restart Tableau Server. If you don’t restart Tableau Server, role-based licenses become available to all users within 24 hours.
A user with a Viewer license cannot open Tableau Server or Tableau Online workbooks from Tableau Desktop.

A user with a Viewer license who also has a separate Tableau Desktop license will be unable to open workbooks on Tableau Server or Tableau Online using Tableau Desktop. To open workbooks such using Tableau Desktop, that user will need an Explorer or Creator license on Tableau Server or Tableau Online.

**Migrate from Core-Based to User-Based Licensing**

This guide tells you how to migrate Tableau Server from a core-based license metric (which counts the processor cores on which you have Tableau Server installed) to a user-based license metric (which counts named users). To learn more about licensing metrics, see Licensing Overview.

**Note:** As an alternative to migrating to user-based licensing, you can also continue using a core-based license and add user-based Viewer, Explorer and Creator licenses as-needed to provide users with the capabilities granted by these licenses. To learn more, see [Use user-based licenses on a server with core-based licensing](#).

**Prepare for migration to user-based licensing**

Core-based licenses allow an unlimited number of users, including view-only guest accounts. Every user has a site role when they are added to Tableau Server, and these users and site roles persist when licensing is changed. Because user-based licenses limit the number of users, you should ensure that your new user-based licenses accommodate the number of users who are currently connecting to Tableau Server, including the users currently using guest accounts. If your new user-based licenses don’t accommodate the full number of users, some users will move to the Unlicensed site role. To learn more about site roles, see [Set Users’ Site Roles](#).
To count the number of users in your Tableau Server installation, export a list of users to count them with a tool such as Microsoft Excel. To learn how to export a list of users, see Export a User List.

Migrate to user-based licensing

To migrate to user-based licensing you must stop Tableau Server, deactivate the core-based product key, activate the user-based product key(s), and then start Tableau Server. Because this process will result in a restart of Tableau Server and cause downtime for Tableau Server users, you should migrate licensing during a period of low usage.

1. Stop Tableau Server:

   Use the `tsm stop` command. To learn more, see: `tsm stop`.

2. Deactivate the core-based product key:

   Use the `tsm licenses deactivate` command with the core-based product key.

3. Activate the user-based product key:

   Use the `tsm licenses activate` command with the user-based product key.

4. Start Tableau Server:

   Use the `tsm start` command.

Use user-based licenses on a server with core-based licensing

The 2018.1 release of Tableau Server now lets you to add user-based licenses to Tableau Server installations with core-based licensing. If you upgrade a Tableau Server installation to 2018.1 without activating user-based licenses, Tableau Server will continue to operate as it did previously, with no changes to Tableau Server UI or permissions except that the legacy Viewer site role is renamed to Read Only.

The first Creator or Explorer license that you add to Tableau Server will be used by Server Administrator users. Administrators can activate additional Creator, Explorer and Viewer licenses in Tableau Server to increase licensed user capacity. Activating these user-based licenses gives you a combination of the capabilities granted by user-based Creator,
Explorer and Viewer licenses and the capabilities granted by your core-based license. To learn more about the different types of user-based licenses, see User-based licenses.

Note: The unlimited number of users who have full access to Tableau Server under core-based licensing have equivalent capabilities to users with an Explorer license under user-based licensing.

For example, if a Tableau Server installation has a 16 core license that includes guest access, and you added 10 Creator licenses, that server would have the following capabilities:

- A limit of 16 processor cores on hardware that runs Tableau Server
- Guest access
- Unlimited Explorer licenses (from the unlimited user licenses that come with a core license)
- 10 Creator licenses

Example of completing a migration from core-based licensing

To extend the example above: If the core-based license was then deactivated, the following capabilities would be available:

- No limits on server hardware
- No guest access
- 10 Creator licenses

If you then added 50 Explorer licenses and 200 Viewer licenses, the following capabilities would be available:

- No limits on server hardware
- No guest access
- 10 Creator licenses
- 50 Explorer licenses
- 200 Viewer licenses
Add Users to Tableau Server

You can add users to Tableau Server one at a time or in batches. You can add them to the server as unlicensed users, and then add them to sites and assign site roles as you onboard them to Tableau Server. Or you can add users to sites and specify their site roles at the same time, at which point they are ready to sign in.

Before you begin

- If your Tableau Server is configured with an Active Directory external identity store, review User Management in Active Directory Deployments to understand how multiple domains, domain naming, NetBIOS, and Active Directory user name format influence Tableau user management.

**Note:** If you run Tableau Server on Linux, all external directory communication is configured and managed with a LDAP identity store. In the context of user and group synchronization, Tableau Server configured with LDAP identity store is equivalent to Active Directory. Active Directory synchronization features in Tableau Server function seamlessly with properly configured LDAP directory solutions.

- Verify that you have enough user licenses and role licenses for your user base. If you attempt to add a user for a site role that you do not have a license for, then you will receive an error.
- To add user licenses to your Tableau Server deployment, visit the Tableau Customer Portal to purchase licenses and the corresponding product key(s). After you have purchased licenses, see Add Capacity to Tableau Server to update the server with the new key(s).
- The steps in this topic describe how to add an individual user and assign their site role. To add users in batches, see Import Users.

Adding users at the server level vs. the site level

In a single-site environment, server administrators can add users on the Users page.
After you add a site to Tableau Server, it becomes a multi-site server with a **Server Users** page (all server users from every site appear here) and a **Site Users** page. Only server administrators can access the **Server Users** page, and both site administrators and server administrators can access the **Site Users** page.

The **Server Users** page is the only place where you can assign users to multiple sites, delete users from the server, and if the server is using local authentication, reset user passwords.
Add a user to the server

1. In the site menu, select **Manage All Sites > Users**, and then click **Add Users**.

To add a user to a site, you select the site and go to the **Users** page.

2. Do one of the following:

   - If the server is configured for **local authentication**, click **New User**, and enter a user name. With local authentication, the best way to avoid user name collisions is to provide an email address for the user name. For example, `jsmith@example.com` instead of `jsmith`. 
User names are not case sensitive. Characters not allowed in user names include the semi-colon (;) and colon (,).

- If the server is configured for **Active Directory authentication**, click **Active Directory User**. If you are adding a user from the same Active Directory domain that Tableau Server runs on, the server domain will be assumed, and you can type the AD user name without the domain.

**Note:** Do not enter the user’s full name; this can cause errors during the importing process.

3. If the server is using local authentication, provide the following:

- **Display Name**—Type a display name for the user (e.g., *John Smith*).
- **Password**—Type a password for the user.
- **Confirm password**—Retype the password.
- **Email**—This is optional and can be added at a later time in the user profile settings.
- **Selected users are Server Administrators**: Specify whether the user should be a server administrator.
- **Name (Site Membership) / Site Role**: If the user is not a server administrator, you can assign a user to zero or more sites, along with a site role for each site. You do not have to choose site membership and site role at this time. If you don’t specify site membership and site role for a new server user, the user will be added as a server user only, with a site role of Unlicensed. For details, see Set Users’ Site Roles.

4. Click **Create**.
Sign in to the Tableau Server Admin Area

As a server administrator on Tableau Server, you can access admin settings to configure sites, users, projects, and to do other content-related tasks.

If you want to change server settings such as processor, caching, authentication, distributed deployment, and other related configurations, see Sign in to Tableau Services Manager Web UI.

If you are running Tableau Desktop and want to sign in to Tableau Server to publish or access content and data sources, see Sign in to Tableau Server in Tableau Desktop.

Here's how to sign in to the Tableau Server admin pages:
1. Open your browser and enter the server URL. Here are some examples of what the URL might look like:

http://localhost/ (if you’re working directly on the server computer)

http://MarketingServer/ (if you know the server’s name)

http://10.0.0.2/ (if you know the server’s IP address)

If the server is *not* using port 80, you need to include the port number in the URL, as in these examples:

http://localhost:8000/

http://MarketingServer:8080/

http://10.0.0.2:8888/

...where 8000 or 8080 or 8888 is the port that you configured.

Tableau Server displays a page where you can enter a user name and password:
2. Enter the credentials for the server administrator that you created when you finished installing Tableau Server.

You're then taken to the main page of the Default site, and you're ready to create users, sites, and manage content.

Navigate the Admin Areas of the Tableau Web Environment

As an administrator on Tableau Server or Tableau Online, you can access admin settings that aren’t available to other users to configure sites, users, projects, and to do other content-related tasks.

The settings in this article refer to the Tableau web environment. Tableau Server administrators with appropriate credentials can also change server settings such as processor, caching, authentication, distributed deployment, and related configurations using the TSM web environment. For information, see Sign in to Tableau Services Manager Web UI.

Access based on site role and number of sites

The menus you get when you sign in to Tableau Server or Tableau Online depend on the following conditions:

- Whether you’re a site or server administrator.
  
  Site administrator access is available on Tableau Online and Tableau Server. Server administrator access is only on Tableau Server.

- Whether you have access to only one site or to multiple sites.

Server administrator

In a multi-site environment, menus at the top enable you to modify a specific site or all sites, and to configure users, groups, schedules, tasks, and server settings.

On a single-site server, the site selector does not appear, and all other menus are the same.
To access server administrator settings that affect all sites, open the site menu, and then select **Manage All Sites**.

The **Content** and **Group** tabs go away, and the site menu text changes to **All Sites** to let you know you are managing server-wide settings.

To return to the site administration menus, select **All Sites**, and then select the site you want to manage.

Site administrator

If you are a site administrator for Tableau Online or Tableau Server, and you have access to multiple sites, you’ll get menus for selecting which site to manage, and for managing that site’s content, users, groups, schedules, and tasks, and for monitoring its status.
The site selector displays the name of the current site. To go to another site, select the site menu, and then select the site name.

If you have access to only one site, the site selector does not appear, but all other menus are the same.

**Server administrator tasks**

Server administrators (available with Tableau Server Enterprise only) can do the following:

- Monitor server status and activity.
- Generate log files.
- Add sites and edit site settings. Only server administrators can add sites to the server.
- Add users to the server, and assign users to sites.
- Add and manage site groups.

To manage settings only for a specific site, you must first navigate to the site. Within each site, you can do the following:

- Administer content: Create projects, move content from one project to another, assign permissions, change ownership of a content resource, and so on.
- Manage schedules for extract refreshes and subscriptions.
- Monitor site activity and record workbook performance metrics.
- Manage storage space limits for content published by users.
- Allow web authoring.
- Enable revision history.
- Allow site administrators to add and remove users.
- Allow users to subscribe to workbooks and views, and allow content owners to
subscribe others to workbooks and views.

- Enable offline snapshots for favorites (iOS only).

Site administrator tasks

A site administrator on Tableau Online or Tableau Server can do the following tasks:

- Administer content: Create projects, move content from one project to another, assign permissions, change ownership of a content resource, and so on.

- View, manage, and manually run schedules for extract refreshes and subscriptions.

- Add and manage site users (if allowed by the server administrator; see Add or Update Sites).

- Add and manage site groups.

- Monitor site activity.

Sign in to Tableau Services Manager Web UI

This topic explains how to sign in to the Tableau Services Manager (TSM) web UI. The TSM web pages are used to configure Tableau Server settings such as user authentication, server processes, caching, and other server-related settings. You can also configure TSM from a command line shell. See tsm Command Line Reference.

The TSM web UI is not the same as the Tableau Server admin pages. Log on to the Tableau Server admin pages to create and edit sites, users, projects and other content-related tasks. See Sign in to the Tableau Server Admin Area.

If you are running Tableau Desktop and want to sign in to Tableau Server to publish or access content and data sources, see Sign in to Tableau Server in Desktop.
Requirements

- The account that you use to sign in to TSM must have administrative access to the local computer where Tableau Server is installed.

Specifically, the account that you use to sign in to TSM must be a member of the tsmadmin group that was created during initialization. To view the user accounts in the tsmadmin group, run the following command in the Bash shell:

```
grep tsmadmin /etc/group
```

If the user account is not in the group, run the following command to add the user to the tsmadmin group:

```
sudo usermod -G tsmadmin -a <username>
```

Tableau Server on Linux relies on PAM for core authentication scenarios. For more information about PAM integration for TSM administration, see TSM Authentication.

- If you are running a distributed deployment of Tableau Server, then enter the host name, or IP address of the computer running the initial node. The credentials you enter must have administrative access to the computer running the initial node, as specified above.

- Specify an HTTPS protocol in the server URL. Tableau Server installs a self-signed certificate as part of the installation process. Therefore, the protocol must be specified as https. For more information about the self-signed certificate and certificate trust for TSM connections, see Connecting TSM clients.

- Specify the default port for TSM web UI (8850) in the URL.

- If you are running a local firewall, open port 8850. See Configure Local Firewall.

- You must specify the hostname or IP address of the computer running TSM. If you have set up a load balancing or proxy solution in front of Tableau Sever, do not specify the load balancer or proxy address.
Sign in to the TSM web UI

1. Open a browser and enter the Tableau Server URL, and append the dedicated TSM web UI port.

   Here are some examples of what the URL might look like:

   https://localhost:8850/ (if you're working directly on the server computer)
   https://MarketingServer:8850/ (if you know the server's name)
   https://10.0.0.2:8850/ (if you know the server's IP address)

2. In the sign-in page that appears, enter your administrator user name and password.

   **Note:** Tableau Server creates and configures a self-signed certificate during the installation process. This certificate is used to encrypt traffic to the TSM Web UI. Because it's a self-signed certificate, your browser will not trust it by default. Therefore, your browser will display a warning about the trustworthiness of the certificate.
Customize Your Server

You can customize the Tableau Server web pages to personalize it for your company or group. You can perform these customizations:

- Change the server name that appears in the browser tab, tooltips, and messages.
- Change the logos that appear in the web environment.

For more information, see tsm customize.

- Set the language used for the web environment and the locale used for views. See
Language and Locale for Tableau Server

- Install custom fonts on Tableau Server and client computers that connect to Tableau Server. See Use Custom Fonts in Tableau Server.

Administrators and project leaders can also add images for projects in thumbnail view.

Language and Locale for Tableau Server

Tableau Server is localized into several languages. Server language and locale settings impact how this affects users. The **Language** setting controls user interface (UI) items such as menus and messages. The **Locale** setting controls items in views such as number formatting and currency.

Administrators can configure language and locale on a server-wide basis and individual users can configure their own settings (search for "Your Account Settings" in the Tableau Server Help). If a user configures their own language and locale, their settings override the server settings.

Supported Languages

Tableau Server is localized into several languages. See the "Internationalization" section of the Tableau Server Technical Specification page for more information.

Default Settings

The default language for Tableau Server is determined during Setup. If the host computer is configured for a language Tableau Server supports, Tableau Server installs with that language as its default. If computer is configured for a language that is not supported, Tableau Server installs with English as its default language.

How Language and Locale are Determined

Another influence on which language and locale display when a user clicks a view is the user's web browser. If a server user has not specified a **Language** setting on their User Account page, and their web browser is set to a language that Tableau Server supports, the
browser’s language will be used—even if Tableau Server itself is set to a different language.

Here’s an example: Assume that Tableau Server has a system-wide setting of English as the **Language** for all users. Server user Claude does not have a language specified on his Tableau Server User Account page. Claude’s browser uses German (Germany) for its language/locale.

When Claude signs in to Tableau Server, the server UI displays in German and when he clicks a view, the view uses the Germany locale for numbers and currency. If Claude had set his user account **Language** and **Locale** to French (France), the UI and view would have been displayed in French. His user account setting supersedes those of his web browser, and both of those have precedence over the Tableau Server system-wide setting.

Another setting to be aware of is the **Locale** setting in Tableau Desktop (**File > Workbook Locale**). This setting determines the locale of the data in the view, such as which currency is listed or how numbers are formatted. By default, **Locale** in Tableau Desktop is set to **Automatic**. However, an author can override that by selecting a specific locale. Using the above example, if the author of View A set **Locale** to **Greek (Greece)**, certain aspects of the data in View A would display using the Greek (Greece) locale.

Tableau Server uses these settings, in this order of precedence, to determine language and locale:

1. Workbook locale (set in Tableau Desktop)
2. Tableau Server User Account language/locale settings
3. Web browser language/locale
4. Tableau Server Maintenance page language/locale settings
5. Host computer’s language/locale settings
Use Custom Fonts in Tableau Server

You can use custom fonts with Tableau Server. When you do this the safest way to guarantee that users have the experience you intend is to keep the following in mind:

- The fonts need to be installed on the computer where Tableau Server is running.

- The fonts need to be installed on any client computers that will connect to Tableau Server. You need to have the fonts installed locally in order for your browser to properly display them.

- As a best practice, use "web safe" fonts that are installed by default on all major browsers. This increases the likelihood that the fonts will display properly on client machines.

- Different browsers render the same fonts differently, so even when a client browser has the custom font installed, it may look different when viewed in different browsers. This can be especially noticeable with comments or titles where specific spacing is used for an intentional effect.

**Note:** For more information about installing fonts on Linux, refer to your Linux distribution's documentation and support.

Manage Sites

Sites Overview

The topics in this section describe the Tableau Server concept of a site and aspects of working with multiple sites. Topics include authentication type each site uses, and what to know about user licenses and administrator-level access to sites.
What is a site

You might be used to using the term *site* to mean “a collection of connected computers,” or perhaps as the short form of “website.” In Tableau-speak, we use site to mean a collection of users, groups, and content (workbooks, data sources) that’s walled off from any other groups and content on the same instance of Tableau Server. Another way to say this is that Tableau Server supports multi-tenancy by allowing server administrators to create sites on the server for multiple sets of users and content.

All server content is published, accessed, and managed on a per-site basis. Each site has its own URL and its own set of users (although each server user can be added to multiple sites). Each site’s content (projects, workbooks, and data sources) is completely segregated from content on other sites.

For site administrator recommendations for how to set up users on a site, how to structure a site for publishers and other content users, how to give users permissions to share and manage their content, and so on, see the Manage Sites section.

For information about how users can get their content to Tableau Server, see Publish Data Sources and Workbooks in the Tableau user help.

Authentication and sign-in credentials

By default, all sites on a server use the same identity store type. You configure these settings when you install Tableau Server. For information, Configure Initial Node Settings.

Users who have access to more than one site on the same Tableau Server instance use the same credentials for each site. For example, if Jane Smith has a user name of *jsmith* and a password of *MyPassword* on Site A, she uses those same credentials on Site B. When she signs in to Tableau Server, she’ll be able to choose which site she wants to access.

The Default site

Tableau Server installs with a site named Default. If you maintain a single-site environment on Tableau Server, this becomes the site you work with, and on which your users share
their Tableau analysis. If you add sites, Default becomes one of the sites you can select when you sign in to Tableau Server. Default differs from sites that you add to the system in the following ways:

- It can never be deleted but, just like sites that you add, it can be renamed.
- It stores the samples and data connections that ship with Tableau Server.
- The URL used for Default does not specify a site. For example, the URL for a view named Profits on a site named Sales is http://localhost/#/site/sales/views/profits. The URL for this same view on the Default site would be http://localhost/#/views/profits.

Why or why not add sites

On Tableau Server, users, projects, groups, data sources, and workbooks are managed per site. You can add users to multiple sites.

Each environment and its needs is unique. However, as a baseline, Tableau Zen Masters and Product Managers tend to recommend using sites for true multi-tenancy needs. In other words, create a new site only when you need to manage a unique set of users and their content completely separately from all other Tableau users and content.

For site administrator recommendations for how to set up users on a site, how to structure a site for publishers and other content users, how to give users permissions to share and manage their content, and so on, see the Manage Sites section.

Examples for which it makes sense to use sites

- You are a consultant who manages Tableau analysis for multiple clients, and you want to create a site for each client, to ensure that data from one client is not exposed to another.

- You want to allow Guest user access to a small and contained area of the server.

Examples for which projects can work better than sites
A content-development process in which data sources and reports evolve from sandbox to production phases.

Migrating users and content from one site to another is a laborious process. Although you might have good reasons to use sites for this and similar processes, by creating sites, you as the site administrator compound your ongoing maintenance burden. For each configuration update you make to one site (for example creating new projects and setting permissions), you usually would need to duplicate the same work on each additional site.

You want to separate areas of the server by functional area.

Among a group of Tableau users, it’s common that some users need to access content in multiple areas. Using sites would encourage publishing the same data sources and reports to multiple sites. This leads to data source proliferation and can negatively impact server performance. Using projects is a simpler way to work with this scenario.

For additional ideas, see the following resources:

- Why use projects in the topic User Projects to Manage Content Access.
- Discussions about sites on the Tableau Community forums. Here’s a link to get you started.

Administrator-level access to sites

Tableau Server includes three administrator-level site roles: Server Administrator, Site Administrator Creator, and Site Administrator Explorer.

The **Server Administrator** site role always takes the highest license available, and it allows full access to Tableau Server, including all content access. You can find more information about this role in Server Administrator Overview. Server administrators also create sites as needed. (Site administrators don’t have permissions to do this.)
A server administrator can assign one of the Site Administrator site roles to users to delegate creating and maintaining a specific site’s user and content framework. The content framework enables Tableau users to share, manage, and connect to data sources and workbooks.

- Assign Site Administrator Creator to administrators who also connect to data, and create and publish data sources or workbooks. This site role takes a Creator license.

- Assign Site Administrator Explorer if the user manages the content framework but doesn’t need to edit the content itself. This site role takes an Explorer license, and it allows viewing and interacting access.

By default, the Site Administrator site roles allow creating and managing the site’s users and groups, creating projects to organize content on the site, assigning permissions to allow users (groups) to access the content they need, scheduling extract refreshes, and a few other tasks.

A server administrator can deny site administrators’ user management tasks. For example, you might do this if you use the Site Administrator Creator role for the data experts. In other words, you want to allow these users to manage connections to underlying data, create and publish “single source of truth” data sources, create top-level projects, and organize content across projects without restriction; but not necessarily add and remove site users.

For each site the server administrator can also limit site administrator access, so that site administrators can manage groups and content, but not add or remove users or set users’ site roles.

In some organizations, the same person might be both a server administrator and site administrator for one or more sites. Even so, the tasks performed by a site administrator and a server administrator are distinct.

Licensing and user limits

You can add server users to multiple sites, and set their site roles and permissions on each site. A user who belongs to several sites does not need a license for each site. Each server
user needs only one license.

Server administrators can use the **Limit number of users** setting (select **Site <name> > Settings**) to specify a user limit for the site. Only licensed users are counted. For example, if a site has 90 licensed users (including administrators), 20 unlicensed users, the user count is 90.

**Add or Update Sites**

Tableau Server comes with one site named Default. Server administrators can add sites to the server and modify any site’s settings.

**Add a site**

1. Do one of the following:

   - If you’re adding a site to the server for the first time, select **Settings > Add a Site**, and then click **Add a Site**.

   ![Add a Site](image)

   - If you’ve added sites before, in the site menu, click **Manage All Sites**, and then click **New Site**.
• If you’re editing an existing site, select it on the Sites page, and then select **Edit Settings**. Or, in a single-site deployment, click **Settings**, and then click the **General** tab.

2. Enter a **Site name** and **Site ID** for the site. (If you are editing the Default site, you cannot change the **Site ID**.)
**Note** The “#/site” portion of the URL (for example, http://localhost/#/site/sales) cannot be changed. In multi-site server environments, these segments appear in the URL for sites other than the Default site.

3. For **Storage**, select either **Server Limit** or **GB**, and enter the number of GB you want as a limit for storage space for published workbooks, extracts, and other data sources.

If you set a server limit and the site exceeds it, publishers will be prevented from uploading new content until the site is under the limit again. Server administrators can track where the site is relative to its limit using the **Max Storage** and **Storage Used** columns on the Sites page.
4. Select whether only server administrators can add and remove users and change their site roles, or whether you want to allow site administrators to manage users on this site.

If you are allowing site administrators to manage users, specify how many users they can add to the site by selecting one of the following:

- **Server limit**: For a server with user-based licensing, the limit is the number of available server seat licenses. For a server with core-based licensing, there is no limit. For more information, see View Server Licenses and Troubleshoot Licensing.

- **<number of> users**: Allows a site administrator to add users up to a limit you specify. See Work with Sites for information on licensing and user limits.

5. Select **Allow users to use web authoring** if you want to enable browser-based authoring for site content.

When web authoring is disabled, users cannot edit published workbooks from the server web environment. To update a workbook published to the server, a Tableau Desktop user must re-publish it. For more information, see Set a Site's Web Authoring Access.

6. Enable comments so users can share a conversation about data views, including
snapshot images to highlight discoveries. For more information, see Comment on Views in Tableau user Help.

7. Enable data-driven alerts to let users automatically receive emails when data reaches key thresholds. For more information, see Send Data-Driven Alerts in Tableau user Help.

8. Select **Allow users to subscribe to workbooks and views** to let site users subscribe to views and receive regular emails of them. Select **Allow content owners to subscribe other users to workbooks and views** to let administrators, project leaders, and content owners set up subscriptions for other users. These options are visible only if you have configured subscription settings.

9. Under **Email Settings**, you can enter a custom **From Address** for alerts and subscriptions. While the email address you enter should use valid syntax (such as bizdev@myco.com or noreply@sales), Tableau Server does not require it to correspond to a real email account. (Some SMTP servers may require an actual address, however).

If you want a standard email footer to appear, select **Custom footer**, and enter the text you want to display above Tableau Server links in email messages.

The email footer will look similar to the following:
10. Enable offline favorites for Tableau Mobile to let mobile users access cached snapshots of views.

11. Select **Record workbook performance metrics** to permit your site users to collect metrics on how workbooks perform, such as how quickly they load.

   To initiate recording, users must add a parameter to the workbook's URL. For more information, see **Create a Performance Recording**.

12. Click **Create** or **Save**.

   **Note:** After you add your first site to Tableau Server, the site menu becomes available. When you select **All Sites** and click **Users**, the **Server Users** page appears, showing all users. When you select a specific site and click **Users**, the **Site Users** page appears. To add users to the server or specific sites, see **Manage Users and Groups**.

---

**Export or Import a Site**

You can provision a new Tableau Server site by importing (migrating) information from another site. You do this by exporting the existing site’s (the **source** site) information to a file. Then you complete steps to verify and import that information to the **target** site.

**Site migration options**

You can migrate a site in any of these ways:
To another site on the same Tableau Server instance.

To a site on a separate Tableau Server instance.

From Tableau Online to your Tableau Server deployment.

Many of the tips listed in Prepare the source and target sites apply to the Tableau Online-to-Tableau Server migration. However, become familiar with what information is or isn’t preserved in a site export.

**Note:** After you prepare your Tableau Online site for export, contact your Tableau representative. Tableau will complete the export steps, and your representative will send you the export files, which you can then import to your site on Tableau Server.

- From Tableau Server on Windows to Tableau Server on Linux or vice-versa (or cross-platform Tableau Online-to-Tableau Server site migration).

**What information is or isn’t preserved in a site export**

The export file you create preserves workbooks, projects, data sources, and users. This includes permissions set on content, user favorites lists, site quota, and other site settings.

Users’ custom views are preserved; however, depending on the type of site migration, custom view URLs might change in a way that breaks users’ bookmarks to their views. For example, migrating from Tableau Online to a self-managed Tableau Server will change the host name and invalidate bookmarks.

In addition:

- When you export a site on Tableau Server to import to another Tableau Server site, subscription and extract refreshes schedules are preserved.

- When you export a Tableau Online site to import to Tableau Server, only the default
schedules are preserved.

On Tableau Online, users can create their own custom subscription schedules. These schedules currently are only supported on Tableau Server version 2018.2 if the administrator has followed the steps provided in Enable Custom Schedules for Subscriptions.

Usage data, which appears in the site’s administrative views, is not preserved. For example, view and data source counts, user actions, and performance data.

Backgrounder jobs that are in-progress while a site is being exported, will not be exported and will not show up on the new site once the import is complete.

In addition, OAuth access tokens embedded in data connections are reset. For those data sources, you will need to edit the connections and re-authenticate to the underlying data.

Prepare the source and target sites

Before you export a site, complete the following checklist to prepare both environments. Some of these instructions depend on whether both sites are on the same server instance or on separate ones.

• **Verify version compatibility**
To import a site successfully, the source and target sites must be in the same product version family. For example, 2019.1 through 2019.1.x. You cannot import a site that is outside the target site’s version family. For example, 2018.3 to 2019.1. For version information, see the Tableau Release Notes.

• **Identify node**
The `tsm sites` commands will use your local file store to hold the export and import data. If you are running a multinode Tableau cluster, then you must run the `tsm sites` commands on a Tableau Server that is running the Data Engine process. For information about the Data Engine process and the processes that require it, see Tableau Server Processes.
• **Delete stale content items**
  Make sure the source site contains only what you want to import to the new site. Delete unused workbooks, data sources, or projects.

• **Remove obsolete users**
  Confirm that all server users are licensed, and remove accounts that are no longer in use. You can’t remove users during the import process, so if the two sites are on the same server instance, all users you export from the source site are imported to the target site.

• **Create or identify the target site**
  You must import a site file to a site that already exists on the target Tableau Server instance. Because the import process removes anything from the target site that is not included in the import file, we recommend that you import to an empty site. For more information, see Add or Edit Sites.

**Notes**

- If the target site is not empty, workbooks and data sources with names that are identical on both target and source sites are replaced. This can be verified by the time stamp.

- If your source site has workbooks that use published data sources, the data connections in these workbooks continue to refer to the source site name. To maintain those connections without having to republish the workbooks, make sure the target and source site names match.

• **Locate site IDs**
  The tsm command you use to export or import a site requires a parameter that takes the site ID. You can get the site ID from the URL when you’re signed in to the site from a web browser.

  If only one site exists on the server, that site is named **Default**. When you’re signed in to the Default site, the browser URL looks something like this:

  **https://server-name/#/projects**
Tableau Server on Linux Administrator Guide

In the URL, the absence of the /site parameter indicates that it's the Default site. The site ID for the Default site is "Default" without the quotation marks.

On a multi-site Tableau Server deployment, the browser URL includes #/site/ followed by the site ID. The following URL would appear if you navigate to the Views page on a site whose site ID is finance:

https://localhost/#/site/finance/views

• **Check the identity store**
  You can export from and import to sites that do not use the same user identity store type, but you will need to modify the mapping files used for the import. This step is built into the import process and described in 3. Verify that site settings are mapped correctly.

• **Create users on the target server if necessary**
  The site import process assigns users to the target site. If the source site is on Tableau Online or on a Tableau Server instance other than the target site, you must create users on the target server before you can perform the import. If the two sites are on the same Tableau Server instance, the target site has access to the existing users, and you can skip this step.

  User names are stored differently in Tableau Online, so when you export a Tableau Online site, you must edit the user-specific mapping file as part of the verification steps.

• **Configure the target server to deliver subscriptions**
  Subscriptions are imported, but you must configure the server to deliver them.

  For more information, see Set Up a Site for Subscriptions.

• **Check schedules**
  The Schedules page lists the existing schedules for extract refreshes and subscriptions.
For migrations from one Tableau Server site to another, refreshes and subscriptions assigned to default schedules on the source site are mapped to the same schedules on the target site.

If the source site has schedules that do not exist on the target site, and the target site is on another Tableau Server instance, you must create the schedules on the target site that you want the source schedules to map to. You can edit the mapping files to make sure this is done as you expect.

For migrations from Tableau Online to Tableau Server, custom subscription schedules that users create are not mapped. Before you contact Tableau to request your site export, remove these custom schedules.

To remove them, go to Tasks > Subscriptions, and select the check boxes for the custom subscriptions. Then, on the Actions menu, select Unsubscribe.
Tips for importing to a target with fewer users or schedules than the source site

When a target site has fewer users or schedules than the source site, many-to-one importing is not supported. How you can address this depends on whether the source and target sites are on the same Tableau Server instance.

**Note:** Subscription schedule information in this section does not apply to Tableau Online-to-Tableau Server site migration.

You can take any of the following approaches that apply to your situation:

- Remove extra users or schedules from the source site before you export.
  
  This is the preferred option if the two sites are on the same server instance.

- Add missing users or schedules to the target site before beginning the import.
  
  This is required if the target site is on another server instance.

- Add the missing users or schedules to the target site in the middle of the import process and manually update the mapping files.
  
  This is an option only if the sites are on the same instance.
Manually map the users or schedules to different users and schedules in the target site during the import process.

This is required if a user name differs between servers—for example, the exported user named adavis@company.com is defined on the target site as davisa.

1. Export a site

On the Tableau Server machine, type the following command:

```
tsm sites export --site-id <source-siteID> --file <filename>.
```

Tableau Server must be running when you use the `export` command. During the export process, Tableau Server locks the site you’re exporting.

For example, to export a site with site ID `weather-data` to the file `export-file.zip`, type the following:

```
tsm sites export --site-id weather-data --file export-file
```

By default, Tableau Server saves `<export-file>.zip` to `/var/opt/tableau/tableau_server/data/tabsvc/files/siteexports`. For more information, see `tsm File Paths`.

2. Generate the import mapping files

To generate import files for the target site, you need the .zip file you created when you completed the steps in 1. Export a site.

1. On the Tableau Server machine, copy the exported .zip file to the directory Tableau Server expects to find the files for importing. For example:

```
/var/opt/tableau/tableau_server-
data/tabsvc/files/siteimports
```

2. Verify that the target site already exists on Tableau Server. The import process will
not create a site. See the previous section, Prepare the source and target sites.

3. Run the following command (Tableau Server must be running):

```
tsm sites import --site-id <target-siteID> --file <export-file.zip>
```

This command generates a set of .csv files that show how source site settings will map to the target site. In the steps described in the next section of this article, you confirm these mappings and adjust them where needed.

By default these .csv files are generated to a mappings directory created under siteimports. For example:

```
/var/opt/tableau/tableau_server-/data/tabsvc/files/siteimports/working/import_<id>_<date-time>/mappings
```

For more information, see tsm File Paths.

3. Verify that site settings are mapped correctly

The .csv files you generated in the previous section describe how the source site’s resources will be assigned to the target site when the import is complete. Items in the files that Tableau Server was unable to map, and that you need to edit, are indicated by a series of question marks (???). Before you can complete the import process, you must replace the question marks with valid assignments on the target site.

**Important:** Some requirements apply to mapping users, schedules, and published content resources, particularly when the source and target sites are on separate Tableau Server instances. For more information, see Prepare the source and target sites earlier in this article.
To verify mapping files

1. Navigate to the directory that contains the .csv map files generated by the `tsm sites import` command. By default:

```bash
/var/opt/tableau/tableau_server-/data/tabsvc/files/siteimports/working/import_<id>_<date-time>/mappings
```

2. Use your preferred text editor to open one of the .csv files in the `mappings` directory, and do the following.
   a. Confirm that the mappings are correct.
   b. If an entry shows a series of question marks (???), replace them with a valid value.
      
      For descriptions of the settings in each of these files, use the tables in Mapping file content reference later in this article.
   c. Save the changes and preserve the CSV file formatting.

Repeat this process for the remaining .csv files.

4. Import the correctly mapped files to the target site

After you verify the site mappings in the .csv files, you can import the settings to the new site to complete the migration process.

1. Run the following command:

```bash
tsm sites import-verified --import-job-dir <import-id-dir-directory> --site-id <target-siteID>
```

For example:

```bash
tsm sites import-verified --import-job-dir /var/-opt/tableau/tableau_
```
server/data/tabsvc/files/siteimports/working/import_ff00_20180102022014457
--site-id new-site

2. When the success message appears, sign in to the new site and confirm that everything was imported as you expected.

**Note:** The `tsm sites import` and `tsm sites export` commands can leave a site in a locked state if an error occurs. To unlock a site, use the `tsm sites unlock` command.

## Mapping file content reference

The following tables list the columns in each of the mapping files created when you run the `tsm site import` command.

CSV file name: `mappingsDomainMapperForGroups`

<table>
<thead>
<tr>
<th>Column title</th>
<th>Can it be edited?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source_name</td>
<td>No</td>
<td>A user group name on the source site.</td>
</tr>
<tr>
<td>source_domain_name</td>
<td>No</td>
<td>The identity store type on the source site: either <strong>local</strong> (for local identity store) or a domain name (for Active Directory or LDAP external identity store).</td>
</tr>
<tr>
<td>target_domain_name</td>
<td>Yes*</td>
<td>The identity store type on the target site: either <strong>local</strong> for local identity store, or a domain name (such as example.com or example.lan) for Active Directory or LDAP external identity store.</td>
</tr>
</tbody>
</table>

**Tableau Server on Linux Administrator Guide**
*For the **All Users** group, keep the **target_domain_name** value set to **local**, even if your target server is configured for Active Directory identity store. The **All Users** group is a special default user group that must exist on every Tableau Server.

**CSV file name:** mappingsScheduleMapper

<table>
<thead>
<tr>
<th>Column title</th>
<th>Can it be edited?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source_name</td>
<td>No</td>
<td>The names of custom and default extract or subscription schedules on the source site.</td>
</tr>
<tr>
<td>source_scheduled_action_type</td>
<td>No</td>
<td>The type of schedule, either <strong>Refresh Extract</strong>, for extract refreshes, or <strong>Subscriptions</strong>, for subscription deliveries on the source site.</td>
</tr>
<tr>
<td>target_name</td>
<td>Yes</td>
<td>The names of custom schedules on the target site. You can edit this value. For example, if the schedule is named <strong>Friday Update</strong> on the source site you can rename it <strong>Friday Refresh</strong> on the target site.</td>
</tr>
<tr>
<td>target_scheduled_action_type</td>
<td>No*</td>
<td>The type of schedule, either <strong>Refresh Extract</strong>, for extract refreshes, or <strong>Subscriptions</strong>, for subscription deliveries on the target site.</td>
</tr>
</tbody>
</table>

*In the rare case that you see question marks (???) in this column, replace them
with either Refresh Extract or Subscriptions, to match the entry you see under source_scheduled_action_type.

CSV file name: mappingsSiteMapper

<table>
<thead>
<tr>
<th>Column title</th>
<th>Can it be edited?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source_url_namespace</td>
<td>No</td>
<td>The site ID of the source site.</td>
</tr>
<tr>
<td>target_url_namespace</td>
<td>No</td>
<td>The site ID of the target site.</td>
</tr>
</tbody>
</table>

CSV file name: mappingsSystemUserNameMapper

<table>
<thead>
<tr>
<th>Column title</th>
<th>Can it be edited?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source_name</td>
<td>No</td>
<td>The user name attribute of a user on the source site.</td>
</tr>
<tr>
<td>source_domain_name</td>
<td>No</td>
<td>The identity store type on the source site: either local (for local identity store) or a domain name (for Active Directory or LDAP identity store), or external (for a Tableau Online site).</td>
</tr>
<tr>
<td>target_name</td>
<td>Yes</td>
<td>The user name attribute for users who will be assigned to the target site upon import. Confirm that all the user names in the list exist on the target server, and replace question marks (???) with user names that exist on the target server.</td>
</tr>
</tbody>
</table>
You cannot create user names by adding rows to the CSV file. Similarly, you cannot remove user names by deleting rows.

You can edit a user name in the **target_name** column to be different from its source user name, as long as the user already exists on the target server with that name.

For example, a user can have a **source_name** value of **agarcia@company.com** and a **target_name** value of **ashleygarcia@company.com**.

You can map a user on the source site to only one user name on the target site.

| target_domain_name | Yes | The identity store type on the target site: either **local** (for local identity store) or a domain name (for Active Directory or LDAP external identity store). |

CSV file name: **MappingsScheduleRecurrenceMapperWithAutoCreation**

This file does not require updates.

**Delete Sites**

Server administrators can delete sites that have been added to Tableau Server. Deleting a site also removes workbooks and data sources that were published to the site, as well as users. If a user belongs to additional sites, they will not be removed. To permanently delete a user, go to the Server Users page.
Note: The Default site cannot be deleted.

1. On the site menu, click Manage All Sites, and then click Sites.

2. Select the site you want to remove, and click Delete.

3. Click Delete in the confirmation dialog box that appears.

Site Availability

A site can become suspended or locked due to a site import failure, or because a server administrator chooses to suspend the site for a period of time.

When a site is suspended, only the server administrator can activate the site to make it available again.

Note: If a site becomes locked and you cannot access the Sites page through the Server interface, use the tsm sites unlock command to change the state to active.
To activate or suspend a site

1. In the site menu, click **Manage All Sites**, and then click **Sites**.

2. Select the site, and then select **Actions > Activate** or **Suspend**.

Allow Users to Save Revision History

Revision history enables your users to see how workbooks and data sources (content resources) have changed over time. Each time someone saves (publishes) a content resource, Tableau Server creates a new version, which becomes the current version. It makes the previous version the most recent revision in the revision history list. Revision history gives users confidence to experiment with their content, knowing that their older versions are available.
Notes

- This information applies to Tableau Server, and is for server administrators who want to allow publishers to work with revisions.

- On Tableau Online, workbook revision history (and not data source revision history) is enabled on all sites. Users can save up to 10 revisions.

- For information about working with the content revisions themselves, including potential issues, see Work with Content Revisions in the User/Analyst section of the Tableau help.

Permissions users need to work with revision history

To access revision history, a user must have a site role of Creator or Explorer (Can Publish), plus the following permissions, depending on the content type:

- Project: View and Save
- Workbooks in the project: View, Save, and Download Workbook/Save As
- Data sources in the project: View, Save, and Download Data Source

Enable revision history and set the number of revisions allowed

Revision history is set at the site level, and is enabled by default, with a limit of 25 revisions for each content resource.

1. Sign in to a site as a Server Administrator, and click Settings.

2. Under Revision History, select Save a history of revisions, and enter the maximum number of revisions you want to allow for each content resource.

3. Click Save.

When you lower the number of revisions, the most recent revisions are saved. For example, if you set the limit to 15, the 15 most recent versions of the workbook or data source are saved.
Clear all revisions

Server administrators can delete all previous revisions of published workbooks and data sources from a site. The most recent version of each published workbook and data source is always retained.

1. Sign in to a site as a Server Administrator, and click **Settings**.
2. Under **Revision History**, click **Clear Revision History**.
3. Click **Save**.

Security for previewing and restoring workbooks

When users select **Restore** or **Preview** for workbook revisions, user passwords are exchanged between the user’s browser and the server. Tableau Server encrypts these passwords using public/private key encryption. To ensure these public keys are provided by Tableau Server, you must configure the server to use SSL (HTTPS). For more information, see SSL.

See also

*Potential revision history issues* in the User/Analyst section of the Tableau help.

Extract Refresh Schedules

Tableau Desktop authors and data stewards can create and publish *extracts*. Extracts are copies or subsets of the original data. Because extracts are imported into the data engine, workbooks that connect to extracts generally perform faster than those that connect to live data. Extracts can also increase functionality.
Before refreshing extracts

When an extract refresh is performed on extracts created in Tableau 10.4 and earlier (that is, a .tde extract), the extract is upgraded to .hyper extract automatically. While there are many benefits of upgrading to a .hyper extract, you will be unable to open the extract with previous versions of Tableau Desktop. For more information, see Extract Upgrade to .hyper Format.

Setting up refresh schedules

As a server administrator, you can enable scheduling for extract refresh tasks, and then create, change, and reassign schedules. General scheduling options you change on the server are available as part of the publishing process when a Tableau Desktop user publishes an extract.

Schedules that you create have the following options:

**Priority**

The priority determines the order in which refresh tasks are run, where 0 is the highest priority and 100 is the lowest priority. The priority is set to 50 by default.

**Execution mode**

The execution mode indicates to the Tableau Server backgrounder processes whether to run refreshes in parallel or serially. Schedules that run in parallel use all available backgrounder processes and serial schedules run on only one backgrounder process. However, a schedule can contain one or more refresh tasks, and each task will only use one backgrounder process, whether in parallel or serial mode. This means that a schedule in parallel execution mode will use all **available** backgrounder processes to run the tasks under it in parallel, but each task will only use one backgrounder process. A serial schedule uses only one backgrounder process to run one task at a time.

By default, the execution mode is set to parallel, so that refresh tasks finish as quickly as possible. You might want to set the execution mode to serial (and set a lower priority) if you have a very large schedule that prevents other schedules from running.
Frequency

You can set the frequency to hourly, daily, weekly, or monthly.

For information, see Create or Modify a Schedule.

Refreshing extracts manually

In the Tableau Server web environment, both server and site administrators can run extract refreshes on-demand on the Schedules page:

- Select the schedule and click Actions > Run Now.

You can also refresh extracts from the command line using the `tabcmd refreshextracts` command. For more information, see `tabcmd Commands`.

Refreshing extracts from Tableau Desktop

Tableau Desktop users can refresh extracts they publish and own. They can do this the following ways:

- **At publish time**: When an author publishes a workbook or data source that uses an extract, that author can add it to server refresh schedule. The refresh can be a full or an incremental refresh.

  Incremental refreshes reference a column in the extract that has a data type of date, date/time, or integer; such as a timestamp. Tableau uses this column to identify new rows that need to be added to the extract. For more information, see Refreshing Extracts and Schedule Extract Refreshes as You Publish a Workbook in the Tableau Help.

  - **User interface**: In Tableau Desktop, you can use the Refresh from Source, Add Data From File, and Add Data From Data Source commands to upload an addition to or refresh an extract on Tableau Server. A user might want to do this if Tableau Server doesn’t have sufficient credentials to access the underlying data. For
Enable Extract Refresh Scheduling and Failure Notification

Your publishers can schedule extract refreshes when two conditions are met:

- **Tableau Server** is configured to send email messages when extract refreshes fail. This is configured by a Tableau Server Manager (TSM) administrator and is on by default. For details, see Configure Server Event Notification.
- The site or sites in which you want to allow publishers to schedule extract refreshes is configured to send email when the refresh fails. This is configured by a server administrator in Tableau Server and is on by default. The instructions below explain how to do this if it is not enabled.

While you’re enabling scheduling, you can decide whether also to enable sending email to owners of data sources or workbooks that are refreshed when those extract refreshes do not complete successfully. You can read more about these emails below. When you enable refresh failure notification, the owners of the content that has scheduled refreshes can opt out individually by changing their account settings.

1. Sign in to Tableau Server as a server administrator.

2. Go to the General tab of the Settings page for the site you want to configure for subscriptions:
   - If you have a single site, at the top the browser window, click **Settings and General**.
   - If you have multiple sites, select the site you want to configure and click **Settings and General**.

3. On the **General** page, do the following:
• Under **Refresh Failure Notifications**, select *Send email to data source and workbook owners when scheduled refreshes fail.*

To clarify, if a scheduled refresh for a particular data source fails, the email goes only to the owner of that data source, not to owners of workbooks that connect to that data source.

• Under **Embedded Credentials**, select both options to let publishers embed credentials and schedule extract refreshes. (Automatic refresh schedules require embedded credentials so Tableau Server can directly access data.)

**Note:** On a multi-site server, failure notifications are a site setting, and embedded credentials are a server setting. To configure embedded credentials on a multi-site server, select **Manage All Sites** and then **Settings**.

### Managing schedules from the server

In your organization it might be more appropriate to manage embedded credentials and refresh schedules centrally from the server. If you do that, you might clear the check boxes in the **Embedded Credentials** section described in the steps above, so that Tableau Desktop publishers do not see schedule options during publishing.

Managing schedules centrally enables you to distribute extract refresh and subscription tasks, so you can run them when most people are offline. It also enables you to oversee which credentials are embedded in connections.

For more guidelines for managing schedules and refreshes on the server, see **Provide access to data sources** and **Keep data fresh** in *Everybody’s Install Guide*.

### How refresh failure emails work

The email notification for a failed extract refresh lists the extract name and location on the server, gives the time of last successful refresh, the number of consecutive times the refresh
Tableau Server on Linux Administrator Guide

has failed, and suggests the reason for the failure and possible solution.

After five consecutive failures, the refresh schedule is suspended until you or the data owner takes an action to address the cause of the failure, such as updating database credentials or a path to the original data file.

How the last successful refresh date is determined

The last successful refresh date and time are shown when that last refresh occurred within a number of days. By default it is 14 days, and this value is set in \texttt{wgserv-er.alerts.observed\_days}. If the number of days since the last successful refresh exceeds the number specified in this setting, the message in the email shows “not in the last \textit{N} days.”

Create or Modify a Schedule

The Schedules page shows a list of schedules, including their name, type, what they’re for (scope), number of tasks, behavior (concurrent or serial processing), and when they are scheduled to run.

\textbf{Note}: If you enable custom schedules for subscriptions on one or more sites, users will control schedules for their subscriptions on those sites. To learn more, see Enable Custom Schedules for Subscriptions.

To create a new schedule

1. In a site, click \textbf{Schedules}.
2. Click **New Schedule**.

3. Specify a descriptive **Name** for the schedule. For example, End of week.

4. Select a **Task type** the schedule will handle—refreshing extracts, running flows, or delivering subscriptions.

5. Optionally you can define a **Default priority** from 1 to 100, where 1 is the highest priority. This is the priority that will be assigned to the tasks by default. If two tasks are pending in the queue, the one with the higher priority runs first.

6. **Execution**: choose whether a schedule will run in parallel or serially. Schedules that run in parallel run on all available backgrounder processes so that they can complete faster.

   **Note**: Schedules for the same workbook will always run serially, even if you set this option to parallel.

7. Finish defining the schedule. You can define an hourly, daily, weekly, or monthly schedule.
8. Click **Create**.

To modify an existing schedule

1. Navigate to the Schedules page.

2. Select an existing schedule, click the Actions drop-down arrow, and then select **Edit Settings**.
3. Finish editing the schedule, and click **Save**.

**See also**

Manage Refresh Tasks

Extract Refresh Schedules

**Schedule a flow task**

**Enable Custom Schedules for Subscriptions**

Custom schedules for subscriptions allow users to receive email messages on a schedule that they define, rather than using a fixed schedule defined by a server administrator. Custom schedules for subscriptions have been available to users of Tableau Online since March 2017, and these schedules can now be enabled on a per-site basis in Tableau Server version 2018.2. Enabling custom schedules for subscriptions is a permanent change on any sites where you make this change. Any sites where you don’t enable custom schedules remain on fixed schedules defined by a server administrator.

**Enable custom schedules**

Before you can enable custom schedules on one or more sites, you must first enable custom schedules on Tableau Server, and then enable custom schedules on one or more sites.
Step 1: Enable custom schedules on Tableau Server

From a command prompt with Tableau administrator permissions, run the following commands:

```
tsm configuration set -k features.SelfServiceSchedules -v true
tsm pending-changes apply
```

This operation will restart Tableau Server.

Step 2: Enable custom schedules on a site

1. Log in to Tableau Server as a server administrator using a web browser:

   https://<hostname>/#/login

2. Browse to the Site Settings page for a site, and then enable custom schedules:
   1. Click All Sites, and then choose one of the sites from the drop-down list.
   2. Click Settings.
   3. On the General tab, under Subscriptions, select the following checkbox: Permanently convert from fixed schedules created by administrators to custom schedules created by users. (You can't undo this).
   4. Click Save.

When custom schedules are enabled on a site, all fixed schedules with a subscription are converted to an equivalent custom schedule.

How Scheduled Server Jobs are Prioritized

Jobs and Tasks

In Tableau Server, users can schedule extract refreshes, subscriptions, or flows to run periodically. These scheduled items are referred to as tasks. The Backgrunder process initiates unique instances of these tasks to run them at the scheduled time. The unique
instances of the tasks that are initiated as a result are referred to as jobs. Jobs are also created for runs that are initiated manually, by clicking the Run now option.

For example, an extract refresh task is created to run daily at 9 AM. This is an extract refresh task, and every day at 9 AM, a job will be created for the Backgrounder to run.

You can assign a priority number to Tasks and Schedules using values from 1 to 100. Lower the number, higher the priority, 1 is the highest priority, and 100 is the lowest.

Priority Rules for Jobs

When processing scheduled extract refreshes, subscriptions, and flow runs, Tableau Server prioritizes background jobs in this order:

1. Any job already in process is completed first.

2. Any task or schedule that you initiate manually using Run now starts when the next backgrounder process becomes available. Exception to this are the flow tasks and schedules. Flow runs use the assigned task priority to determine the order in when they should run. If there is no task priority assigned it defaults to 0 which is the highest priority.

3. Jobs with the highest priority (the lowest number) start next, independent of how long they have been in the queue.

For extract refreshes and flows, this is the task priority. The task priority is inherited from the schedule priority when the task is first created. The task priority can be subsequently changed.

For subscriptions, this is the schedule priority. If you have enabled custom schedules for subscriptions, then the priority of those jobs is set to 50.

For example, a job with a priority of 20 will run before a job with a priority of 50, even if the second job has been waiting longer. To change task priority, see Create or Modify a Schedule.

4. Job with the same priority are executed in the order they were added to the queue.
The first job added to the queue starts first; then the second job starts.

5. When multiple jobs with the same priority are scheduled to run at the same time, they start in the order they were created or enabled. Jobs scheduled for the same time are executed by task type with the fastest category of jobs starting first: flows, followed by data driven alerts, followed by system jobs, followed by subscriptions, followed by incremental extract refreshes, and then full extract refreshes.

The following limitations also impact when the jobs are run:

- The number of concurrent jobs is limited to the number of backgrounder processes you have configured for Tableau Server.
- Separate refreshes for the same extract or data source cannot run at the same time.
- Jobs associated with a schedule that is set to run serially run one at a time.

**Configure Workbook Performance after a Scheduled Refresh**

To improve the load times for workbooks, Tableau Server caches the results of queries included in workbooks. For most workbooks, query results are computed and cached when they are first viewed by a user on Tableau Server. However, for workbooks that connect to data extracts, Tableau Server can recompute query results when the corresponding extract refresh tasks run. This reduces the load time for these workbooks when they are first viewed, so this option is turned on by default for workbooks that have been viewed recently.

**Determine the performance impact**

Although this option reduces the initial load time for workbooks, recomputing query results also increases the load on Tableau Server. If your Tableau Server installation is already performance-constrained, you might want to turn this option off or lower the threshold for workbook caching.
Here are some possible reasons why you might want to turn this option off or lower the threshold:

- The Background Tasks for Non Extracts administrative view displays many long-running jobs in the **Warming up external query cache on data change** category.

- The Background Task Delay administrative view displays long delays.

- CPU and memory consumption for the backgrunder processes is consistently high.

However, note that this is only one of the options that impacts the performance of background tasks. For more information about performance, see Performance.

**Turn off workbook caching for the server**

To decrease the load on Tableau Server, you can turn off workbook caching after a scheduled refresh at the server-level. If you turn this option off, Tableau Server caches query results for workbooks the first time the workbooks are viewed.

Use the following tsm configuration set option to turn off workbook caching after a scheduled refresh:

```
backgrunder.externalquerycachewarmup.enabled
```

For more information on how to use and apply tsm set options, see tsm configuration set Options.

**Turn off workbook caching for a site**

You can also turn off workbook caching after a scheduled refresh for an individual site. For example, you might do this if there is one site in particular that contains many slow workbooks which increase load on the server.

1. Select the site for which you want to turn off workbook caching in the sites drop-down.

2. Click **Settings**.
3. In the **Workbook Performance after a Scheduled Refresh** section, clear the check box.

**Note:** Although this option is available in the settings for an individual site, you must have server administrator permissions to view it.

**Configure the workbook caching threshold**

Tableau Server only recomputes query results for workbooks that both have scheduled refresh tasks and have been viewed recently.

You can increase or decrease the number of workbooks that are cached after a scheduled refresh with the following tsm configuration set option:

`backgrounder.externalquerycachewarmup.view_threshold`

By default, the threshold is set to 2.0. The threshold is equal to the number of views that a workbook has received in the past seven days divided by the number of refreshes scheduled in the next seven days. (If a workbook has not been viewed in the past seven days, it is unlikely that it will be viewed soon, so Tableau Server does not spend resources recomputing queries for the workbook.)

**Ensure Access to Subscriptions and Data-Driven Alerts**

To ensure that users see the Subscribe and Alert buttons in the Tableau Server toolbar and can receive related emails, do the following:

- **Configure SMTP and event notifications on Tableau Server:** See Set Up a Site for Subscriptions.

- **Ensure that users have an email address in Tableau Server:** Users can update their email address on their account settings page.

- **Embed database credentials or don't require them:** To email data in a view,
Tableau Server needs to access the data without user involvement. This can be accomplished by using a workbook with embedded database credentials, a Tableau Server data source, or data that doesn’t require credentials (such as a file that’s included with the workbook at publish time).

- **Ensure that users can access needed workbooks and views:** Access to content on the server is controlled by the View permission. To receive images of content in email messages, users also need the Download Image/PDF permission. For more information, see View or Edit Permissions.

- **Avoid trusted authentication for embedded views:** If you use restricted tickets (the default) to render an embedded view, the Subscribe and Alert buttons don’t appear.

**Set Up a Site for Subscriptions**

When users subscribe to a workbook or view, a snapshot of the view is email to them on scheduled basis, so they can see the latest updates without having to sign into Tableau Server. Administrators, project leaders with appropriate site roles, and content owners have the option to subscribe other users to workbooks and views. For more information, see Subscribe to Views.

**Note:** To create and receive subscriptions, users need access to related databases and views. See this list of requirements for details.


**Prerequisite: Configure the server to send subscription emails**

Before you can enable subscriptions for a site, you need to complete the steps to enable subscriptions on the server. Follow the steps in these topics to configure subscriptions on the server.
1. Configure SMTP Setup
2. Configure Server Event Notification

Enable subscriptions

After you have configured SMTP and server event notifications, you can enable subscriptions.

To enable subscriptions:

1. Sign into Tableau Server as a server administrator.

2. Go to the General tab of the Settings page for the site you want to configure for subscriptions:
   - If you have a single site, on the side navigation, click Settings and General.
   - If you have multiple sites, select the site you want to configure and click Settings and General.

3. On the General tab, scroll down to Subscriptions and select the subscription options for your users.

   **Note:** This section is only visible when the server-wide configuration option Allow users to receive email for views that they have subscribed to is enabled. For details, see Configure Server Event Notification.

   a. Select **Allow users to subscribe to workbooks and views**

   b. (Optional) To allow content owners to subscribe other users to their content, select **Allow content owners to subscribe other users to workbooks and sheets**.

4. (Optional) Scroll down to Email Settings.
Tableau Server on Linux Administrator Guide

a. Enter an **Email From Address** that will show as the "From" address in email messages.

b. Enter an **Email Footer** for email messages.

A site's "From" address and message footer are also used in emails for data-driven alerts.

5. Click **Save**.

To specify the subscription schedules available to users, see Create or Modify a Schedule.

**Test subscriptions in a site**

1. **Subscribe to a view.**

2. At the top the browser window, click **Schedules**.

3. Select the schedule you chose for the subscription, and then click **Actions > Run Now**.

A snapshot of the view should be emailed to you within 10 minutes. If you experience an issue, see Troubleshoot Subscriptions.
Manage all user subscriptions

1. At the top the browser window, click **Tasks**, and then click **Subscriptions**.

   All user subscriptions for the current site appear, including information like subscriber name, view name, and delivery schedule.

2. Select any subscription you want to update. From the **Actions** menu, select **Change Schedule**, **Change Subject**, **Change Empty View Mode**, or **Unsubscribe**.

   (The empty-view option sends subscription emails only when data exists in a view. It’s a good choice for high-priority alerts.)

Suspended Subscriptions

By default, a subscription is suspended after 5 consecutive subscription failures and result in the subscription emails not sent. To change the threshold number of subscription failures that can occur before they are suspended, use the tsm configuration set option, `back grounder.subscription_failure_threshold_for_run_prevention`. This sets the threshold for the number of consecutive failed subscriptions necessary before suspending the subscription.

This is a server-wide setting.

Only Server administrators can configure the threshold number of subscription failures before a subscription is suspended.

Server administrators can opt in to receive email notifications when a subscription is suspended. You can do this by navigating to **My account settings -> Subscription Notifications**. This setting is at a site-level so has to be configured for site separately.

Resume suspended subscriptions

If a subscription fails more than five times, you'll receive a notification email that your subscription has been suspended. There are a few ways to resume a suspended subscription if you’re a subscription owner or administrator:
• From the My Content area of Tableau web pages, an icon appears in the Last update column to indicate that the subscription is suspended. Select ... > Resume Subscription to resume.

• From the Subscriptions tab of the affected workbook, an icon appears in the last update column to indicate that the subscription is suspended. Select ... > Resume Subscription to resume.

• From the Subscriptions tab under Tasks, an icon appears in the last update column to indicate that the subscription is suspended. Select ... > Resume Subscription to resume (Server administrators only).

When a subscription is resumed, the alert failing count goes back to zero. The next evaluation of the subscription will occur at the next scheduled evaluation time.

See also

Subscribe to Views in the Tableau Desktop and web authoring Help.

Project-level administration to learn which site roles allow full Project Leader capabilities.

Set Up for Data-Driven Alerts

When data reaches important thresholds for your business, data-driven alerts automatically send email notifications to key people users specify. As a Tableau Server administrator, you set up data-driven alerts much like you do subscriptions. For information about how users create and manage these alerts, see Send Data-Driven Alerts in Tableau User Help.

**Note:** To create and receive data-driven alerts, users need access to related databases and views. See this list of requirements for details. If alerts are enabled for a site, any user on that site can create them.
Configure email for data-driven alerts

1. Complete the steps in Configure SMTP Setup so the server can send email.

2. While viewing a site, click **Settings** at the top of the browser window.

3. Under Email Settings, enter a site-specific "From" address or message footer.

   A site's "From" address and message footer are also used in emails for subscriptions.

4. Click **Save**.

Manage all data-driven alerts in a site

1. At the top the browser window, click **Tasks**, and then click **Alerts**.

2. Select any alerts you want to update.

3. From the **Actions** menu, do any of the following:
   - Add or remove yourself as a recipient.
   - Edit alerts to change data thresholds, delivery schedules, and the full list of recipients.
   - Change alert ownership to different users, or delete alerts.

Disable data-driven alerts for a site

Data-driven alerts are supported for all sites by default, but administrators can disable them for specific ones.

1. While viewing a site, click **Settings** at the top of the browser window.

2. Under Data-Driven Alerts, uncheck **Let users create alerts and receive alert emails**.

3. Click **Save**.
Control how often the server checks data-driven alerts

By default, Tableau Server checks every 60 minutes to confirm whether data conditions for alerts are true. If you notice performance impacts, you can customize this time interval with the `tsm configuration set option, dataAlerts.checkIntervalInMinutes`.

Regardless of the `dataAlerts.checkIntervalInMinute` setting, the server also checks alerts whenever extracts in the related workbook are refreshed. To check an alert more frequently than the setting specifies, change the extract-refresh schedule.

Track the server’s alert-checking process

In the Background Tasks for Non Extracts view, you can track the server’s alert-checking process by looking for these tasks:

- Find Data Alerts to Check
- Check If Data Alert Condition Is True

The "Find" task limits "Check" tasks to alerts that can currently send related emails. For example, if a user has chosen an email frequency of "Daily at most", after the alert condition becomes true, the server waits 24 hours before checking the alert again.

Each "Check" task uses one server backgrounder process, loading the related view to evaluate the alert condition. If all users see the same version of a view, it loads only once. But if users have applied filters to a view, or the data they see is limited by user-level security, the view loads once for each recipient.

Identify and fix failing alerts

As an administrator, you can proactively identify failing alerts that users may be unaware of.

To check:

1. Select Status in your site menu
2. Select Background tasks for non-extracts
3. From the Task drop-down menu, select Check if Data Alert is True

4. In the far right, click on Error to see a list of failing alerts

5. Hover over the red failure icon to display a tooltip with alert details

To determine the alert owner, look for the alert ID number in the data_alerts table of the Tableau Server Repository. (In the alert management area of a site, you can also look for the alert name following the number, but be aware that multiple different alerts may use the same name.)

**Note:** Starting in Tableau Server 2018.3, alert owners will be automatically notified when an alert fails ten times. Administrators can customize when alert owners receive notifications. Administrators can configure Users will not be notified for alerts that failed prior to upgrading to Tableau Server 2018.1.

![Check data alert](image)

Failing alerts are often caused by content changes on Tableau Server. Encourage users to recreate alerts if changes like the following occur:
• A workbook, view, or data field is removed or renamed.

• Database credentials embedded in workbooks expire. (Alerts require workbooks to use either embedded credentials, or none at all.)

• A data source becomes inaccessible.

**Tip:** To automatically get emailed when alerts fail, follow the steps in Collect Data with the Tableau Server Repository, and connect to the "background_jobs" table. From that table, create a custom view that includes the "Check If Data Alert Condition Is True" job name and its finish code. Then set up a data-driven alert to email you whenever a finish code equals 1 (failure).

### Administrative Views

The Status page contains an embedded Tableau workbook with various administrative views. These views help you to monitor different types of server or site activity.

**Note:** You must install PostgreSQL drivers before you can see Administrative views. For more information, see Database Drivers.

### Navigating to administrative views

To see administrative views, click **Status**. Site administrators can see administrative views for their site. Administrators of multiple sites can see views for the current site.

On a multi-site server, server administrators can see views for the entire server. Click the site menu, and then click **Manage All Sites** to access the server menus.
To see views for individual sites on a multi-site server, click the site menu, select the site name, and then click **Status**.

Pre-built Administrative Views

Administrative views are powerful monitoring tools that can help you optimize Tableau Server and better understand how your users are interacting with Tableau content. The administrative views listed to the right are included with Tableau Server. Click on the link for a view to learn more about how to interpret and act on the information the view provides.

To create your own administrative view, see Create Custom Administrative Views.

Performance of Views

**Note:** This view is only available to server administrators. For information about how to navigate to administrative views, see Administrative Views.

The Performance of Views administrative view displays how long it takes for views to load and how many sessions are running at a time on the server.
You can compare spikes in the number of sessions with spikes in slow load times to identify the times of day when high user traffic is slowing down the server. You can also look at the individual views by load time to understand which views take the longest to load.

Some views might take a long time to load regardless of when they are viewed. You can identify which workbooks need to be optimized with the Stats for Load Times administrative view. Some simple ways to optimize workbooks includes the following:

- Display less information in each view.
- Break up views.
- Reduce the number of filters.
- Use data extracts.
Performance of Flow Runs

Use this view to see the performance history for all the flows on a site. You can filter by Flow Name, the Output Step Name, Flow Owner, Run Type (Scheduled or Ad Hoc), and the time the flow runs were started.

Here are some questions you can answer using this view:

- **What flow tasks are currently scheduled?** – To do this, use the Start Time filter and select the time frame you want to look at. For example, to see flow tasks that are scheduled in the next 3 hours, select **Hours -> Next ->** and enter 3.

- **What is the duration of flow tasks?** - To answer this, click on a mark in the view and you should see details including the task duration.

**How many flows were run ad hoc, and how many were scheduled runs?** - To answer this, use the **Run Type** filter and select **Ad hoc or Scheduled**.

**Note:** This is not functional in this release and will not actually filter the data.

In addition to the questions described above, here are some examples of insights you might be able to gather:

- The flows that are running most frequently will have the most marks.

- To see how many flows are running at the same time currently, hover over a mark that
shows “In Progress” or “Pending and select “Keep Only” to filter all flow runs that are currently running.

- To see how many flows are running at the same time during a specific time range, select a range for the Start Time filter. For example, you can choose “Next three hours” to see which flows will be running in the next three hours.

Traffic to Views

The Traffic to Views view gives you the ability to see how much of your user traffic goes to views.

You can filter what information is displayed and the time frame it comes from by selecting the view, the workbook, and the time range. Server administrators can specify the site.

Two time lines at the top of the view show you how views are being used over a time range you specify (the default is the last 7 days):
What is the Total View Count by Day

This shows total view count by day, based on the filters you set. Hover your mouse pointer over a point on the line to see the count of views. Select the point to update the other sections of the view based on your selection.

What is the Total View Count by Time

This shows the view count by time of day. The filters and any selection impact this graph.

Two bar graphs at the bottom of the view show results that are filtered by the Min View Count filter at the top of the view. These show you the views that are most often accessed, and the users who most frequently access views. Only those views and users with counts greater than or equal to the minimum view count value are displayed:

What Views are Seen the Most

This is a list of the most visited views. Like the other sections of the view, the information is limited by filters and any selection you make.

Who Accesses Views Most Often

This shows the users who most often access the views and is limited by filters and any selection you make.

Traffic to Data Sources

The Traffic to Data Sources view gives you the ability to see usage of data sources on your Tableau Server installation. This can help you determine which data sources are most heavily used and those that are less often used. You can filter the information you see by selecting the data source, the action taken on that data source, and the time range. Server administrators can specify the site.
A time line at the top of the view shows you how data sources are being used over a time range you specify (the default is the last 7 days):

- **What is the Total Data Source Usage by Day**—This shows total data source usage by day, based on the filters you set. Hover your mouse pointer over a point on the line to see the count. Select the point to update the other sections of the view based on your selection.

Two bar graphs at the bottom of the view show results that are filtered by the Min Interactions filter at the top of the view. These show you which data sources are most used, and who uses data sources most often. Only those data sources and users with interaction counts greater than or equal to the minimum interactions value are displayed:

- **What Data Sources are Used Most**—This is a list of the most used data sources. Like the other sections of the view, the information is limited by filters and any selection you make.
- **Who Uses Data Sources Most Often**—This shows the users who most often use the data sources. This is impacted by filters and any selection you make.

**Actions by All Users**

The Actions by All Users view gives you insight into how your Tableau Server installation is being used. You can filter the view by actions and by time range. Server administrators can filter by site. The Total Users count shows the number of users who have performed an
action. This value is not affected by any filtering. The Active user count shows the number of active users who have performed one of the selected actions.

Up to three separate groups of time lines show you how users are using Tableau Server over a time range you specify (the default is the last 7 days). If no actions are selected for a particular group, that group does not display. Possible groups are:

- **Access & Interactions**—This shows you sign in (log on) activity, view access and data source use.
- **Publish & Download**—This shows publishing and downloading of flows, workbooks and data sources.
- **Subscriptions**—This shows counts of subscription email sent for workbooks and views. It also shows the counts of flow runs.

Use the legend at the bottom to view a subset of the displayed actions. Click a single action to highlight the line for the action, or **Ctrl + Click** on multiple actions to highlight more than one. To clear the selection and display all the selected actions, click on any action in the legend.
Actions by Specific User

The Actions by Specific User view gives you insight into how individual users are working in your Tableau Server installation. You can filter the view by user name, actions, and time range. Server administrators on multi-site installations can filter by site.

Up to three separate groups of time lines show you how a selected user is using Tableau Server over a time range you specify (the default is the last 7 days). If no actions are selected for a particular group, or if no actions were taken, that group does not display. Possible groups are:

- **Access & Interactions**—This shows you sign in (log on) activity, view access and data source use. This means any interaction with a Data Source by the selected user, including extract refreshes scheduled by that user, or the user accessing a workbook that is associated with that data source.
- **Publish & Download**—This shows publishing and downloading of flows, workbooks and data sources.
Subscriptions

- **Subscriptions**—This shows counts of subscription email sent for workbooks and views. It also shows the counts of flow runs.

A bar graph at the bottom of the view shows which items the selected user is using.

Use the legend at the bottom to view a subset of the displayed actions. Click a single action to highlight the line for the action, or **Ctrl + Click** on multiple actions to highlight more than one. To clear the selection and display all the selected actions, click on any action in the legend.

**Actions by Recent Users**

The Actions by Recent Users view shows you which signed-in users have been active on Tableau Server over the past 24 hours. This can be useful if you need to perform some maintenance activity and want to know how many and which users this will affect, and what they are doing on Tableau Server.

The view **Active**, **Recently Active**, and **Idle** users that are currently signed in to Tableau Server. For this view, an active user is one who took an action in the last 5 minutes, a recently active user is one who last took an action within 30 minutes, and an idle user is one who last took an action more than 30 minutes ago. The actions are displayed in the lower section of the view.
Select a user to see only the actions that user performed recently. Hover over an action to see details of the action.

Background Tasks for Extracts

The Background Tasks for Extracts view displays extract-specific tasks that run on the server.
Understand this view

To better understand this pre-built administrative view, make note of the following:

- The table, "What Extracts Ran on this Server," lists the extracts that ran in the time period specified in **Timeline**.
- You can click **Success** or **Error** to filter the table based on status.
- You can also click a specific task to update the "How Much Time did Extracts Take" graph for the selected task.
- The table, "How Many Extracts Succeeded or Failed," updates for the status (success or failure) of the task, but the count of extracts that succeeded or failed does not change.

Status

Tasks can have a status of success or error.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✗</td>
<td><strong>Error</strong>—Server was unable to complete the task.</td>
</tr>
</tbody>
</table>
### Success—Server completed the task.

See details about a task

For details on about the task, use your mouse to hover over the success or error icon.

---

**Background Tasks for Non Extracts**

The Background Tasks for Non Extracts view displays tasks that the server runs that are not related to refreshing extracts. For example, edited OAuth connections, subscription notifications, and so on.
A table lists the tasks that ran in the time range specified. Click **Success** or **Error** to filter the table based on status. Select a specific task in the **How Many Tasks Succeeded or Failed on this Site** table to update the **What Background Tasks Ran on this Site** graph for the selected task.

Tasks can have a status of success or error. For details about the task, use your mouse to hover over the success or error icon.

**Icon**  
**Error**—Server was unable to complete the task.  
**Success**—Server completed the task.

Upgrade Thumbnails Job

In Tableau Server version 2019.1 and later, workbooks and views use higher resolution thumbnails. When you upgrade to Tableau Server version 2019.1 or later, the Backgrounder
runs the Enqueue Thumbnails Upgrade job and the Upgrade Thumbnails job, which refreshes thumbnails for any views that have not been edited or published since Tableau version 2018.2 and converts them from low resolution thumbnail images (192 x 192 pixels) to high resolution thumbnail images (300 x 300 pixels), as shown in the figure below.

![Health Indicators](image1)

When the Upgrade Thumbnails job refreshes the thumbnail images, the modified date of the view is changed to match the thumbnail update date. The Upgrade Thumbnails job does not change the modified date of workbooks when it updates the contained view’s thumbnails.

Depending on the number of workbooks you have, the Upgrade Thumbnails job can run for a few minutes to a few hours. You may notice that CPU usage on Backgrounder nodes is higher than normal during the time that the Upgrade Thumbnails job is running. You may also notice that thumbnail images may appear in low resolution for up to a week after upgrading to Tableau Server 2019.1 or later, while the Upgrade Thumbnails job processes all of the thumbnail images used in your workbooks. We recommend that you wait for the Upgrade Thumbnails job to complete before you back up Tableau Server.

After the first run of the Upgrade Thumbnails job, it runs on a predefined weekly schedule. The Upgrade Thumbnails job runs at lowest priority and creates one task per workbook in the background_jobs table to upgrade any low resolution thumbnails. Low resolution thumbnails published to Tableau Server by Tableau Desktop version 2018.3 and earlier are automatically cleaned up each week when the Upgrade Thumbnails job runs.
Troubleshooting

You can check the status of the Upgrade Thumbnails job using the Background Tasks for Non Extracts administrative view. The Upgrade Thumbnails job can display either the success or error status.

**Upgrade Thumbnails job failed, or it completed but some thumbnails are still low-resolution.**

The Upgrade Thumbnails job might show error status if your credentials are wrong. In that case, the workbook thumbnails will still appear in fuzzy, low-resolution (192 x192 pixels). Update your credentials, and the Upgrade Thumbnails job will update the workbook thumbnails the next time it runs.

**Background Task Delay**

**Note:** This view is only available to server administrators. For information about how to navigate to administrative views, see Administrative Views.

The Background Task Delay view displays the delay for flow tasks, extract refresh tasks and for subscription tasks—that is, the amount of time between when they are scheduled to run and when they actually run. You can use the view to help you identify places you can improve server performance by distributing your task schedules and by optimizing tasks.
Here are possible reasons for the delays, and ways that you might reduce the delays:

- Many tasks are scheduled for the same time. In the example view, tasks that show long delays are clustered at the same time every day, which creates spikes in the wait time. Note that you can set the **Timeline** filter to a single day to view task delays by hour and identify the hours of the day which have many tasks scheduled at the same time. A solution to this issue can be to distribute the tasks to off-peak hours to reduce load on the server.

- Specific tasks take a long time to run and are preventing other tasks from running. For example, there might be an extract refresh job that is connecting to a slow data source or that is processing a large amount of data. Use the **Background Tasks for Extracts** administrative view to identify which extract refresh tasks are running slowly. You can then optimize the extract refresh task by filtering the data, aggregating the data, or creating multiple data sources for individual tables in a data source.
Other server processes are running at the same time and are consuming server resources and slowing down performance. Monitor the CPU and memory usage of server processes to see which processes are consuming the most resources and then adjust the configuration of processes on your server.

Stats for Load Times

The Stats for Load Times view shows you which views are the most expensive in terms of server performance. You can filter by view and time range. Server administrators can filter by site. You can also limit the view based on load time in seconds, using the sliding Load Time filter. Load times are for the server. Depending on your client browser and networking, actual load time may vary slightly.

The **Average Load Times** graph shows average load times for views based on the filters you set. Hover over a point to see details. Select a point on the line to update the rest of the view for the selection:
The **Exact Load Times** view shows exact time to load the listed views. A vertical line shows the average load time for each view. Select a mark to see details of a specific instance of the view loading:

Stats for Space Usage

The Stats for Space Usage view can help you identify which workbooks and data sources are taking up the most disk space on the server. Disk space usage is displayed by user, project, and by the size of the flow output, workbook or data source and is rounded down to the nearest number:
Use the **Min Size** filter to control which data sources and workbooks are displayed, based on the amount of space they take up.

Three bar graphs give you information about space usage on your Tableau Server:

- **What Users Use the Most Space**—This shows the users who own data sources and workbooks that are taking up the most space. Click a user name to filter the next two graphs for that user. Click the data source bar or the workbook bar for a user to filter the next two graphs for that type of object for that user. Click the selected user or bar to clear the selection.

- **What Projects Use the Most Space**—This shows the projects with the data sources and workbooks that are using the most space. If a user or object type is selected in the What Users Use the Most Space graph, this displays information specific to the selection.

- **What Workbooks, Flows, and Data Sources Use the Most Space**—This shows
the workbooks and data sources that are taking the most space. The bars are color-coded based on the length of time since the last refresh.

Move your cursor over any bar to display usage details:

Click on a bar to select it and update the other areas of the view based on that selection.

**Server Disk Space**

**Note:** This view is only available to server administrators. For information about how to navigate to administrative views, see Administrative Views.

Use the Server Disk Space view to see how much disk space is in use on the computer or computers that run Tableau Server, where disk space refers only to the partition where Tableau Server is installed. You can also use this view to identify sudden changes in disk space usage.

For a distributed installation, the view displays information about each computer in the cluster.
The Server Disk Space view includes two graphs:

- **What is the most recent disk space usage?**—This graph shows disk space usage for the last 30 days both in gigabytes and as a percentage. Disk space refers only to the partition where Tableau Server is installed.

- **How has free disk space trended in the last month?**—This graph shows changes to disk space usage over the last month. Rest your pointer on a line to view the exact amount of free disk space for a point in time.

When Tableau Server is low on disk space, you can remove files to free space.

**Tip:** You can have Tableau Server notification you when free disk space falls below a threshold that you specify. For more information, see Configure Server Event Notification.
Desktop License Usage

**Note:** This view is only available to server administrators. For information about how to navigate to administrative views, see Administrative Views.

The Desktop License Usage view lets server administrators see usage data for Tableau Desktop licenses in your organization. This can help you manage licenses efficiently and determine if you need more or fewer licenses. This view can help you answer the following questions:

- Who is using a Tableau Desktop license in my enterprise?
- Have any licenses been shared or transferred?
- Is any license being used on a computer where it should not be?
- Does a specific user use their license?
- What types of licenses are being used in my enterprise?
- Do I need to convert any trial licenses?

**Note:** To get data about licenses, each copy of Tableau Desktop version 10.0 or later needs to be configured to send data to Tableau Server. This configuration can be done at installation time, using scripting or third-party software to install and configure Tableau, or after installation, by modifying the registry or property list file. For more information, see Configure Desktop License Reporting.

In order to view license data, Desktop License Reporting must be enabled on Tableau Server. See Enable and configure Desktop license reporting.

Filters

- **Product Keys.** Type a string to filter the dashboard to only those licenses that
include the string anywhere in the product key. For example, to see only licenses that begin with TDTD, type TDTD and press Return to filter the view. Click the X after the string to reset the filter.

- **Action.** Use this filter to control what the dashboard displays, based on the action taken. Actions are **Activate, Use**, and **Return** (deactivate). If the **Use** action is not selected, nothing is displayed in the top bar graph.

- **Department.** Use this filter to control what departments the dashboard displays licenses for. The filter is populated based on the **Department** values specified when Tableau Desktop is registered.

- **Select time duration in days.** Use this slider to specify the time length in days that the dashboard displays information for. The default value is 183 days.

When you hover over the filter card in the first three filters, a drop-down icon appears. Click the icon to specify whether the view should include data that matches the filter (the default) or exclude data that matches the filter:

![Filter options](image)

**Who has used Tableau in the last <nn> days?**

This area of the dashboard shows a bar graph of three types of Tableau Desktop licenses (Perpetual, Trial, and Term) and the number of users who have used each license type during the specified time period. Hover over a license type segment to see an explanation of the license type. Click a segment to filter the rest of the dashboard for only that license type. This action filters both the tables that show licenses that have been used and those that have not been. For example, to see a list of term licenses that have been used during the time period, click the Term bar. The "used" and "not been used" lists are filtered to just show term licenses.
A table of detailed information shows under the bar graph. For each row in the table, action icons display on the right, above a timeline that shows you when the action last took place.

To see a list of the underlying data in a format that allows you to select and copy values like email or product key, click a row in the list of licenses and click the View Data icon:

The data displays in summary form. Click Full data to see all the data. From this view you can select and copy individual values, or download the data as a text file.

**What licenses have not been used in the last <nn> days**

This area of the dashboard shows a list of licenses that have not been used during the specified time period. A timeline shows the last use date. Hovering over a last use mark gives you information including the registered user of the copy of Tableau.

**Desktop License Expiration**

**Note:** This view is only available to server administrators. For information about how to navigate to administrative views, see Administrative Views.

The Desktop License Expiration view gives server administrators information about which Tableau Desktop licenses in your organization have expired or need maintenance renewal. This can help you manage licenses efficiently. This view can help you answer the following questions:

- What trial or term licenses have expired?
- What perpetual licenses have expired maintenance?
- What perpetual licenses have maintenance renewals coming up?
To renew a license or get additional renewal information, see How to renew your Tableau licenses.

**Note:** In order to get data about licenses, each copy of Tableau Desktop version 10.0 or later needs to be configured to send data to Tableau Server. This configuration can be done at installation time, using scripting or third-party software to install and configure Tableau. For more information, see Configure Desktop License Reporting.

In order to view license data, Desktop License Reporting must be enabled on Tableau Server. See Enable and configure Desktop license reporting.

**Filters:**

- **Product Keys**—Type a string to filter the dashboard to only those licenses that include the string. For example, to only see licenses that begin with TDTD, type TDTD and press return to filter the view. Click the "x" after the string to reset the filter.

- **Department**—Use this filter to control what department(s) the dashboard displays licenses for. The filter is populated based on the Department values used when registering copies of Tableau Desktop.

- **Time Duration**—Use this filter to control the length of time for which the dashboard displays information.

The view includes the following tables, which are affected by the filters you set at the top of the view:

- **What keys have expired maintenance**—This table shows the product keys for which maintenance has expired, with a vertical line indicating the point at which the six month window for renewing maintenance closes. If maintenance for a key is expired for more than six months you need to purchase a new key in order to qualify for
support or upgrades.

- **What trial and term licenses have expired**—This shows the trial or term product keys that have expired.
- **What is the maintenance schedule for my keys**—This shows the keys and their maintenance status.

Create Custom Administrative Views

In addition to the pre-built administrative views available on the Maintenance page on the Server, you can use Tableau Desktop to query and build your own analyses of server activity. To do this, you can connect to and query views in the Tableau Server repository using one of two built-in users: the "tableau" or "readonly" user.

To connect to the Tableau Server repository, see Collect Data with the Tableau Server Repository.

- The **tableau** user—The tableau user has access to special views and a subset of tables in repository database. These views and tables are provided so that administrators can create custom administrative views. Tableau makes an effort to limit changes to these tables and views so that custom views built with them do not break.

- The **readonly** user—The readonly user has access to a large number of the repository tables, providing more data about server usage. Administrators can use these to create custom administrative views too, but many of the tables are intended primarily to support the functioning of Tableau Server and may be changed or removed without warning. This means that views created from these tables can break when the database structure is changed.

For examples of custom administrative views, see the Tableau Community.

Before you can connect using one of the built-in users, you must enable access to the Tableau Server database. After doing this you can use Tableau Desktop to connect to and query the database as the tableau user or the readonly user.

The tsm configuration set option auditing.enabled controls whether Tableau
Tableau Server collects historical user activity and other information in the repository. It is enabled by default. Be aware that collecting historical events impacts the size of Tableau Server's backup file (.tsbak).

- **All hist_tables are controlled by the** `tsm configuration set option wgserv-er.audit_history_expiration_days`, which controls how many days of event history are kept in the repository and has default value of 183 days.

- **The _http_requests table** is cleaned of all data older than 7 days when you run tsm maintenance cleanup. For more information, see Remove Unneeded Files.

- **The _background_tasks table** is cleaned automatically and keeps data for the last 30 days.

- **All other tables with names that begin with a ")_" prefix contain current data.**

**Performance**

**Tableau Server Performance Overview**

When you take the time to understand the performance of Tableau Server, you make it easier to serve your users by improving the efficiency of Tableau Server. Although every server environment is unique, and there are many variables that can impact performance, the general steps that you take to understand and act on performance data in Tableau Server are the same.

- **Notifications**. Configure email notifications for important server events. For example, you can receive notifications when server processes become unavailable and when the server is running out of disk space.

- **Monitoring**. Collect and analyze data about Tableau Server to understand how well the server is performing.

- **Tuning**. Make adjustments to tasks, process configurations, and more to improve the
performance of Tableau Server.

- **Troubleshooting.** Identify bottlenecks in resources, workbooks, and more to improve the performance of Tableau Server.

### General Performance Guidelines

#### Hardware and Software

**Add more cores and memory:** Regardless of whether you’re running Tableau Server on one computer or several, the general rule is that more CPU cores and more RAM will give you better performance. Make sure you meet the Tableau Server recommended hardware and software requirements.

If you are running Tableau Server in a virtual environment, use your VM host’s best practices for vCPU allocation in relation to the number of physical CPU cores on the VM host.

#### Configuration

**Schedule refreshes for off-peak hours:** Backup tasks tend to stall other background tasks until the backup is completed. Use the Background Tasks for Extracts administrative view to see your refresh and backup task schedules. Your refresh tasks should be scheduled for off-peak hours that don’t overlap with your backup window.

**Look at caching:** Caching helps Tableau Server respond to client requests quickly, especially for views that connect to live databases. Use the tsm data-access caching list command to confirm the caching frequency is set to low (this is the default).

**Consider changing two session memory settings:**

- **VizQL session timeout limit:** The default VizQL session timeout limit is 30 minutes. Even if a VizQL session is idle, it is still consuming memory and CPU cycles. If you can make do with a lower limit, use tsm configuration set Options to change the 
  vizqlserver.session.expiry.timeout setting.

- **VizQL clear session:** By default, VizQL sessions are kept in memory even when a
user navigates away from a view. This reduces the need to rebuild views but consumes more session memory. To free up memory, you can end sessions when users leave views by changing the value of the `vizqlserver.clear_session_on_unload` setting to `true`. (Regardless of this setting, sessions for the Tableau Mobile app are always kept in memory, improving mobile performance.)

Assess your process configuration: Tableau Server is divided into six different components called server processes. While their default configuration is designed to work for a broad range of scenarios, you can also reconfigure them to achieve different performance goals. Specifically, you can control on which computers the processes run and how many are run. See Performance Tuning Examples for general guidelines for one-, two-, and three-node deployments.

Server Resource Manager (SRM)

The Server Resource Manager (SRM) monitors the system resources each Tableau process is using as well as tracking the total usage of Tableau Server on the system. If either a specific process or the product as a whole takes up too much system resources, SRM can notify the processes to free the resources or restart those processes.

The thresholds that determine when SRM will notify or restart a process are set in the SRM configuration options. The Tableau development team has set the default settings based on internal testing and don’t recommend you change these settings directly.

If you are seeing excessive system resource usage, we recommend that you contact Tableau Support to help determine if these configuration options need to be modified to solve the problem or issue that you are seeing.

Performance Monitoring Overview

When you monitor a server, you collect and analyze data that signals whether the server is performing badly or running into problems. For example, if you notice that your server is using 100% of its processing capacity for long periods of time, you know that there's a problem.
The data that you need to collect and analyze can be broken down into the following broad categories:

- **Resource usage data**—how Tableau Server uses hardware resources like disk space, memory, and processors.
- **Session and load time data**—how users interact with Tableau Server, including how long it takes for views to load and how many concurrent users there are.
- **Background task data**—how Tableau Server runs tasks that are not directly tied to a user action. For example, background tasks include extract refresh tasks, subscription tasks, and more.

Some of this data, including load time data and extract refresh data, is already accessible from the administrative views that are built into Tableau Server. However, to collect resource usage data you need to use a external performance monitoring tools. To collect additional load time data and background task data, you can connect to the Tableau Server repository.

For more information on the built-in administrative views, see Administrative Views.

**Note:** To use the sample workbook and to publish views to Tableau Server, you must have Tableau Desktop.

### Collect Data with the Tableau Server Repository

The Tableau Server repository is a PostgreSQL database that stores data about all user interactions, extract refreshes, and more. You can enable access to the repository and use the data in it to help analyze and understand Tableau Server performance.

Looking for Tableau Server on Windows? See [Collect Data with the Tableau Server Repository](#).
Tableau Server on Linux Administrator Guide

After you enable access to the Tableau Server repository, you can create views with data from the repository. The views that you create with this data are sometimes called custom administrative views. In addition to being used for performance monitoring, custom admin views can be used for tracking user activity, workbook activity, and more. For more information on the type of data that you can use for these views, see Create Custom Administrative Views. Alternatively, if you are only interested in performance data, you can use the preselected database tables in the sample performance workbook.

Enable access to the Tableau Server repository

You can use Tableau Desktop to connect to and query the Tableau Server repository using two built-in users. The user named tableau has access to several database views you can use as part of building your own analyses of Tableau Server activity. The user named readonly has access to additional database tables that you can use to create views for even more in-depth analysis and this is the user we recommend you use.

Before you can connect to the repository, you need to enable access for the readonly user to the database. Use the tsm data-access repository-access enable command to enable repository access. When you enable repository access, you also create a password for the readonly user. You will use this password to access to the repository. You may also need to have port 8060 opened on the repository node so you can connect to the database.

1. Verify that port 8060 is opened on the computer where the repository is installed. This is a requirement if you are connecting remotely.

2. Enable repository access and create a readonly user password:

   tsm data-access repository-access enable --repository-user-name readonly --repository-password <PASSWORD>

   If your password includes special characters, you may need to escape the characters or enclose the password in quotes. Refer to the documentation for the Linux distro that you are running for information about passing special characters in bash shell.
This command will restart Tableau Server.

**Note:** If you later decide that you want to disable remote access to the Tableau Server repository, use the `tsm data-access repository-access disable` command. The command disables external access to the repository. This will not disable access from localhost. For more information, see `tsm data-access repository-access disable`.

Connect to the Tableau Server repository

This section describes how to connect to a custom set of tables from Tableau Server repository.

1. In Tableau Desktop select **Data > Connect to Data**, and then select **PostgreSQL** as the database to connect to.

   **Note:** You might need to install the PostgreSQL database drivers. You can download drivers from [www.tableau.com/support/drivers](http://www.tableau.com/support/drivers).

2. In the PostgreSQL connection dialog box, enter the name or URL for Tableau Server in the **Server** box. If you have a distributed server installation, enter the name or IP address of the node where the repository is hosted.

   Connect using the port you have set up for the `pgsql.port`, which is 8060 by default.

3. Specify **workgroup** as the database to connect to.

4. Connect using the user and the password you specified.

5. Click the **Require SSL** option if you have configured Tableau Server to use SSL for connecting to the repository. For more information, see Configure Postgres SSL to Allow Direct Connections from Clients.
6. Click **Connect**.

7. Select one or more tables to connect to.

The **tableau** user has access to all of the tables that start with an underscore or with **hist_**. For example, you can connect to **_background_tasks** and **_data-sources**. The **hist_** tables include information about server users that isn't currently presented in the Actions by Specific User view. The **readonly** user has access to additional tables that can be used to query other information about server usage.
Performance Tuning

This section describes how to use the performance data that you collect to identify ways to improve the performance of Tableau Server. Because no two server environments are identical, we can’t provide hard and fast rules for tuning server performance. However, you can draw conclusions about performance from patterns in the data that you collected.

For example, are there recurring spikes? Do any of the patterns that you notice in the administrative views correspond to similar patterns in a monitoring tool? Observing patterns like this can guide you in testing and incremental tuning.

Most performance tuning for Tableau Server boils down to these general approaches:

- **Optimize for User Traffic**: This tunes the server to respond to user requests and to display views quickly.

- **Optimize for Extracts**: This tunes the server to refresh extracts for published data sources. You might want to optimize for extract refreshes if your organization has a lot of data and the data needs to be as up to date as possible.

- **Optimize for Query Heavy Environments**: This is a specialized server configuration to optimize for query performance of workbooks that use extracts as their data source.

Rendering views and refreshing extracts generate the most load on the server, so you should optimize for the task that your organization is most interested in.

**Topics in this section:**

Optimize for User Traffic

You can optimize for traffic if you have many active Tableau Server users and few published data sources that need extract refreshes.
When to optimize for user traffic

Ways to optimize for user traffic

When to optimize for user traffic

Slow load times for views

Use the **Requests and Sessions** dashboard of the sample performance workbook to analyze how long views take to load.

![Requests and Sessions]

If multiple views take longer than 10 seconds to load, and if the slow load times correspond to a large number of sessions, that can indicate that user traffic is slowing down the server.

However, if a particular view takes a long time to load regardless of when it is viewed, it's a sign that the workbook for the view needs to be optimized. You can identify which workbooks need to be optimized with the Stats for Load Times administrative view. Some simple ways of optimizing workbooks includes displaying less information in each view or breaking up views, reducing the number of filters, and using data extracts.
High resource usage corresponding to user traffic

If your server displays high CPU and memory usage during peak traffic hours, you should optimize for user traffic. To determine peak traffic hours and analyze how many concurrent users are on your server, use the Users and Actions dashboard. In addition, you can use the Traffic to Views administrative view to see how much user traffic involves accessing views (as opposed to performing administrative functions, publishing, or other tasks).

If you click a point in the Number of Users view, the dashboard displays the users that were active at the time and the number of user actions that those users performed. By default, the only user actions displayed are user views, but you can use the Action Types filter to display additional user actions.

Make a note of the times of day when there are many concurrent users and views so that you can compare this to resource usage. As a rule of thumb, the number of users should correspond to a high number of user actions. However, the view in this example displays an artificially high number of actions for a single user as part of a load generation test. As an example, you can compare the high number of views at 12 AM on June 28th with the resource usage in the dashboard illustrated later.
Use the **CPU Usage** dashboard to display the percent of total CPU usage and the percent of CPU usage for each process. In the following example, note the large spike in total CPU usage and in the VizQL server process at 12 AM on June 28th. Because the VizQL server process loads and render views, the VizQL server process is often the first process to show strain under high user traffic.

**Note:** The percent of CPU usage for individual processes may add up to more than 100 percent. This is because processor utilization for individual processes is measured for a given processor core. By contrast, the total CPU usage is measured for all processor cores.

Use the **Memory Usage** dashboard to display the percent of total memory usage and the average memory usage in gigabytes. As a general rule, memory usage increases steadily with user traffic. Here again the VizQL server process is the first to show strain under high traffic.
Ways to optimize for user traffic

When high user traffic corresponds to high resource usage as it does in the example shown previously, you should optimize for user traffic.

Adjust the number of VizQL server processes

The most effective way of optimizing for user traffic is to adjust the number of VizQL server processes. Add one VizQL server process at a time and measure the effect with more performance monitoring. Because VizQL server processes can consume a lot of CPU and memory, adding too many processes can slow down the server instead. If you see consistently high memory usage, try to reduce the number of VizQL server processes to reduce the amount of memory reserved.

For more information about configuring processes, see Configure Nodes.

Adjust the number of other processes

Although the most effective way of improving performance for user traffic is to adjust the number of VizQL server processes, you can also tune other processes that support the VizQL server process or that prevent the VizQL server process from accessing resources.
For example, the VizQL server process makes frequent requests to the cache server process, so you might also want to increase the number of cache server processes. On the other hand, the Backgrounder processes might contend for CPU resources with the VizQL server process. As a result, if you do not need to run frequent extract refreshes, you might reduce the number of processes for the backgrounder. If you do need additional instances of the backgrounder, and if you’re running Tableau Server on a cluster, you can move the Backgrounder process to a dedicated node.

Adjust the VizQL session timeout limit

In the example shown previously, the amount of memory used by the VizQL server process increases with user traffic, and it remains reserved by Tableau Server for some time after the traffic finished. This is because the VizQL server process reserves memory for each session for a specified amount of time. If the VizQL server process uses a high percentage of the available memory, try reducing the timeout for each session to make memory available more quickly.

To do this, use the `tsm configuration set` command to reduce the `vizqlserver.session.expiry.timeout` setting. The default is 30 minutes.

Refresh the cache less often

If your users do not always need the most up-to-date data, you can optimize for user traffic by configuring Tableau Server to cache and reuse data as much as possible.

To do this, use the `tsm data-access caching list` command to confirm the refresh frequency. The default is Low. Use the `tsm data-access caching set` command to change the refresh frequency.

Assess view responsiveness

When a user opens a view, the components of the view are first retrieved and interpreted, then displayed in the user’s web browser. For most views, the display rendering phase occurs in the user’s web browser and in most cases, this yields the fastest results and highest level of interactive responsiveness. Handling most interactions in the client web browser reduces bandwidth and eliminates round-trip request latencies. If a view is very
complex, Tableau Server handles the rendering phase on the server instead of in the client web browser, because that generally results in the best performance. If you find that views aren’t as responsive as you’d like, you can test and change the threshold that causes views to be rendered by the server instead of in the client web browser. For more information, see About Client-Side Rendering.

About Client-Side Rendering

When you navigate to a view in Tableau Server, the processing required to display the view (the rendering) can either be performed by your client web browser or by Tableau Server depending on the complexity of the view. The complexity of the view is determined by the number of marks, rows, columns, and more. If a view is less complex, then it is faster for your web browser to render the view than it is to send a request to Tableau Server. If a view is more complex, then it is faster to send a request to Tableau Server and take advantage of the server’s computing power.

As a server administrator, you can configure when client-side rendering happens both for web browsers on your computer and web browsers on mobile devices by adjusting the complexity threshold.

Requirements

- **Supported browsers**: Client-side rendering is supported in Internet Explorer version 9.0 or higher, Firefox, Chrome, and Safari. All of these web browsers include the HTML 5 `<canvas>` element, which is used by client-side rendering.

- **Polygons and the page history feature**: If a view uses the polygon mark type or the page history feature, server-side rendering is performed, even if client-side rendering is otherwise enabled.

Configure the complexity threshold for computers and mobile devices

Because computers have more processing power than mobile devices, Tableau Server performs more client-side rendering in your computer’s web browser than in your mobile device’s web browser. You can adjust how much client-side rendering happens for computers and mobile devices with the complexity thresholds. You might want to adjust the
complexity thresholds if you notice that views display slowly on mobile devices. Alternatively, you might want to increase the thresholds to reduce the number of requests to Tableau Server.

By default, the complexity threshold for computer web browsers is 100. To adjust the complexity threshold for computer web browsers, use the following command:

```bash
tsm configuration set -k vizqlserver.browser.render_threshold -v [new value]
```

By default, the complexity threshold for web browsers on mobile devices is 60. To adjust the complexity threshold for web browsers on mobile devices, use the following command:

```bash
tsm configuration set -k vizqlserver.browser.render_threshold_mobile -v [new value]
```

For example, to change the mobile threshold to 40, you might enter the following command:

```bash
tsm configuration set -k vizqlserver.browser.render_threshold_mobile -v 40
```

For more information on how to use tsm option set, see tsm configuration set Options.

Disable client-side rendering

Client-side rendering is enabled by default and is recommended to improve the performance of views. However, you might want to disable client-side rendering temporarily for testing or if your server is being accessed primarily by computers or mobile devices with very little processing power.

Use the following command to disable client-side rendering:

```bash
tsm configuration set -k vizqlserver.browser.render -v false
```

For more information on how to use tsm option set, see tsm configuration set Options.
Testing with the URL Parameter

To test server-side rendering on a session basis, type ?:render=false at the end of the view's URL. For example:

http://localhost/views/Supplies/MyView?:render=false

If client-side rendering is disabled on Tableau Server, enter ?:render=true to enable it for the session:

http://localhost/views/Supplies/MyView?:render=true

You can also test particular complexity thresholds on individual views to see if it’s appropriate to adjust the server-wide threshold for your server and network conditions. For example, you may find that lower complexity (such as 80) or higher complexity (such as 120) tipping points result in more responsiveness to user interactions. To test a threshold, you can keep the server’s default configuration (client-side-rendering enabled) and enter the test threshold number at the end of the view's URL. For example:

http://localhost/views/Supplies/MyView?:render=80

Optimize for Extracts

Try to optimize for extracts if the extract schedules correspond to high resource usage or if extracts take a long time to finish.

When to optimize for extracts

High CPU usage corresponds to extract schedules

Use the Background Jobs dashboard of the sample performance workbook to view the number of background jobs run by Tableau Server, including extract refresh jobs. The dashboard also displays how long background jobs are delayed—that is, the amount of time between when a background job is scheduled and when it actually runs. If you see long delays at particular times of the day or if many jobs are running at the same time, try distributing the job schedules across different times of the day to reduce the load on the server.
Also compare the times when there are many background jobs or long delays with the CPU usage of the server. Use the **CPU Usage** dashboard to display the percent of total CPU usage and the percent of CPU usage for each process. Because the backgrounder process runs background jobs, it is the first process to show strain when there are many extract refresh jobs or when there are slow extract refresh jobs. Note that the CPU usage of the backgrounder process periodically but briefly reaches 100 percent. This indicates that there are intensive refresh jobs on a recurring schedule.

**Note:** The percent of CPU usage for individual processes may add up to more than 100 percent because processor utilization for individual processes is measured for a given processor core. By contrast, the total CPU usage is measured for all processor cores.
Extracts fail or run slowly

Use the Background Tasks for Extracts administrative view to determine how many extracts fail and how long extracts take to complete. Frequent failures can indicate a problem with a particular data source.
Ways to optimize for extracts

When high CPU usage corresponds to extract refresh schedules like it does in the example shown previously, you should optimize for extracts.

Adjust the extract refresh schedule

Use the **Background Jobs** dashboard of the sample performance workbook to identify optimal times for running extracts. In addition to running extracts in off-peak hours, you can distribute extract refreshes to minimize concurrent server load. If extract refreshes continue to cause problems, reduce the frequency of extract refreshes as much as possible in these ways:

- Schedule extracts for times when the server isn’t busy.
- Reduce the frequency of refreshes.
Speed up specific extracts

Use the Background Tasks for Extracts administrative view to identify failing extracts and long-running extracts.

- Reduce the size of extracts. You can help improve server performance by keeping the extract’s data set short, through filtering or aggregating, and narrow, by hiding unused fields. To make these changes, use the Tableau Desktop options **Hide All Unused Fields** and **Aggregate data for visible dimensions**. For more information, see Creating an Extract in the Tableau Help.

For general tips on building well-performing workbooks, search for “performance” in the Tableau Help. To see how workbooks perform after they’ve been published to Tableau Server, you can create a performance recording. For more information, see Create a Performance Recording.

- Use incremental refresh jobs. Incremental refresh jobs append new rows to an existing extract instead of creating the extract from scratch. This type of extract refresh runs quickly because it processes only the data that has been added since the last time the extract refresh job ran. However, it does not account for data that has been updated rather than appended to a data source. As a result, if you run incremental refresh jobs, you should still occasionally run full refresh jobs. For example, you might run a full refresh job once or twice a week for a data source instead of every day.

Configure the execution mode for extract refreshes

When you create extract refresh schedules, ensure that they run in parallel execution mode. When you run a schedule in parallel, it runs on all available backgrounder processes, even if the schedule contains only one refresh task. When you run a schedule serially, it only runs on one backgrounder process. By default, the execution mode is set to parallel so that refresh tasks finish as quickly as possible.

However, in some circumstances, it can make sense to set the execution mode to serial. For example, you might set the execution mode to serial if a very large job is preventing other schedules from running because it uses all available backgrounder processes.
Increase the number of backgrounder processes

A single background process can consume 100 percent of a single CPU core for certain tasks. As a result, the total number of instances you should run depends on the computer’s available cores. If you have Tableau Server installed in a cluster and you run backgrounder processes on a separate node, a good rule of thumb is to set the number of backgrounder process to between half the number of cores and the full number of cores of the computer running the backgrounder processes.

For more information about configuring processes, see Configure Nodes.

Isolate processes

If you have Tableau Server installed in a cluster, you see the largest benefit from moving the backgrounder processes to a separate node to avoid resource contention. This is because the backgrounder process is very CPU-intensive and running it on the same node where other CPU-intensive processes are running can slow down the server. For example, both the VizQL server process and the data engine process can be CPU-intensive. Read the two-node configuration in the Recommended Baseline Configurations topic for more details.

Optimize for Query Heavy Environments

This configuration has been tested by the Tableau team using Tableau Server Data Engine powered by Hyper technology and is recommended for Tableau Server versions 10.5 and later.

When to use this configuration

There are several factors that affect query performance, including, but not limited to: large extract size, complex calculations, or multiple views in a dashboard. Use this configuration to improve workbook performance if one of the two following conditions apply to your environment:

- Your workbooks use extracts and you are seeing long-running queries. In this context long-running queries means that the query execution time on extracts is taking more than 5 seconds.
You are seeing resource contention between Data Engine and VizQL Server when File Store is present on the box.

**Note:** Use performance recording to determine query execution times. To determine resource usage of Tableau use **Performance monitor** for Windows installations, and **sysstat** or **vmstat** tools for Linux installations.

**Important:** Network bandwidth is an important consideration for this configuration. Once a query result is generated, it is sent from the node with the File Store to the node with VizQL Server. Or when publishing an extract, the extract must be sent over the network to the File Store node. Both of these may take additional time depending on the size of data and network bandwidth available.

When not to use this configuration

If you are not seeing a large number of slow running queries (queries taking more than 5 seconds to complete), are unsure of your workload type, or do not see resource contention between Data Engine and VizQL Server when File Store is present, then this configuration may not be optimal for you. Before implementing this configuration, it is highly recommended to evaluate your CPU usage for VizQL Server and Data Engine installed with the File Store.

Furthermore, you should also consider the overall mix of workbooks in your environment. Tableau team tested this configuration using workbooks that have slow running queries (taking more than 5 seconds to complete) and workbooks with queries that take less than 5 seconds to complete. During that testing, Tableau team found that queries that take less than 5 seconds may get slightly slower. Depending on your workload mix of slow and fast running queries, you should evaluate whether this configuration will result in overall better performance for your environment.
The guiding principle for this configuration is to separate the node with File Store from the node that has VizQL Server installed. This is because of the following reasons:

- On Tableau Server, the Data Engine co-located with File Store is used for querying extracts.

- VizQL Server consumes noticeable resources when loading views and interactive use from a web browser. If both File Store and VizQL Server are on the same node, there can be contention for resources between VizQL Server and Data Engine, especially if you are running heavy queries (for example, workbooks with complex calculations) on extracts to load the views.

Thus, by separating VizQL Server and File Store processes, the load between querying extracts and loading or interacting with views can be balanced and better managed. This configuration is targeted at making slow queries faster. By slow queries, we mean queries that take more than 5 seconds to complete.

Here is a visual representation of how to configure your Tableau Server installation to optimize the performance of workbooks that use extracts and have long query execution times:
In this example, all computers are assumed to be at least 64-bit, 16 core, 16+GB systems.

General configuration notes

These configuration guidelines apply to all configurations for Tableau Server installations.

- To calculate the minimum number of Backgrounder processes to run, divide the computer’s total number of physical cores by 4. To calculate the maximum number, divide the computer’s total physical cores by 2.

- Run two VizQL Server processes, two Cache Server processes, and two Data Server processes on the nodes that are not running File Store processes.

Special configuration notes

These configuration recommendations are specific to this configuration.

- For this configuration, typically 16 cores are recommended for each node, with 16 GB of RAM per core. Adding more cores to the node where File Store is running will improve performance since Data Engine is designed to maximize and leverage available cores on the machine. In tests performed by the Tableau team indicates that the File Store/Data Engine dedicated nodes benefited from adding more cores. Pursuing this configuration will allow for more flexibility when scaling your deployment as you are now able to scale the File Store node independently of other processes.

- Run one process of File Store on a separate node that is not running VizQL or Backgrounder processes. Tableau also strongly recommends that you compare the CPU usage for Data Engine to the CPU usage for VizQL Server, and distribute the cores for each of the processes accordingly. The exact ratio can vary depending on your workload type, but a starting point would be to have one File Store/Data Engine node for every 2 VizQL Server nodes.

- The default of this configuration is 4 nodes for high availability considerations.
Performance Benefits

Here are the general benefits you can expect to see from this configuration and the trade-offs you should consider when adopting this configuration:

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Trade-offs</th>
</tr>
</thead>
<tbody>
<tr>
<td>More consistent performance in user experience when loading extract-dependent workbooks*</td>
<td>Fast-running queries may potentially get slightly slower</td>
</tr>
<tr>
<td>Better response times on workbooks with long-running queries*</td>
<td>You may have fewer VizQL Server processes moving to this topology without growing your deployment</td>
</tr>
<tr>
<td>More scalability options to grow your deployment</td>
<td></td>
</tr>
<tr>
<td>Reduction in resource consumption on nodes with VizQL Server</td>
<td></td>
</tr>
<tr>
<td>Reduction in CPU spikes above 95%</td>
<td></td>
</tr>
</tbody>
</table>

*While under moderate (<80%) CPU usage

Additional Benefits

- In the tests done by the Tableau team, we found that for the same number of users, the more the number of query intensive workbooks (which use extracts) in an environment, the faster the time it took to reach the saturation point. If you want to make these workbooks more performant, or service more users using these workbooks, this configuration will help you achieve these objectives.

- This configuration also opens a new scalability option for your installation. You now have the option to scale horizontally or vertically with respect to querying on extracts. Unlike other Tableau processes, the Data Engine leverages as many cores as available on the machine. Given this, you have the flexibility to add more resources to the
standalone File Store nodes to reduce query response time and variability on expensive extract queries or add more File Store nodes to get more extract query throughput in your Server.

When to Add Nodes and Reconfigure

Tableau Server can scale up and out as your needs and requirements evolve. Here are some guidelines to help you figure out whether it’s time to add more nodes to your system, reconfigure the server, or both:

- **More than 100 concurrent users**: If your deployment is user-intensive (>100 simultaneous viewers), it’s important to have enough VizQL processes—but not so many that they exceed your hardware’s capacity to handle them. Also, enabling the Tableau Server Guest User account can increase the number of potential simultaneous viewers beyond the user list you may think you have. The administrative view can help you gauge this. For more information, see Actions by Specific User.

- **Heavy use of extracts and frequent extract refreshes**: Extracts can consume a lot of memory and CPU resources. There’s no one measurement that qualifies a site as extract-intensive. Having just a few, extremely large extracts could put your site in this category, as would having very many small extracts. Sites where extracts are frequently refreshed (for example, several times a day) are often helped by more emphasis on the background process, which handles refresh tasks. Use the Background Tasks for Extracts administrative view to see your current refresh rate. Extract heavy sites benefit from isolating the Backgrounder process on its own machine. For more information, see the two-node configuration in the Recommended Baseline Configurations topic.

- **Query heavy environments**: If you are experiencing slow query performance for Workbooks that use extracts, isolating nodes that handle queries on extracts from VizQL processes can improve and stabilize performance. For more information, see Optimize for Query Heavy Environments.

- **Downtime potential**: If your server system is considered mission critical and
requires a high level of availability, you can configure it so there’s redundancy for the server processes that handle extracts, the repository, and the gateway.

Performance Tuning Examples

Performance tuning examples have been expanded and moved to separate topics. For more information, see Performance Tuning.

For recommended baseline configurations that serve as starting point for installations with one, two, and three nodes, see Recommended Baseline Configurations.

Performance Recording

This section describes how to create performance recordings and use the results to improve workbook performance. With performance recordings, you can view how long workbook events take. For example, you can see how long it takes to connect to a data source, run a query, render data, and more.

Create a Performance Recording

The Performance Recording feature in Tableau records performance information about key events as you interact with a workbook. You can then view performance metrics in a workbook that Tableau creates to analyze and troubleshoot different events that are known to affect performance:

- Query execution
- Geocoding
- Connections to data sources
- Layout computations
- Extract generation
Blending data

Server blending (Tableau Server only)

Tableau support may ask that you create a performance workbook as they work with you to diagnose performance issues.

Looking for Tableau Server on Windows? See Create a Performance Recording.

Enable Performance Recording for a Site

By default, performance recording is not enabled for a site. A server administrator can enable performance recording site by site.

1. Navigate to the site for which you want to enable performance recording.

2. Click Settings:


4. Click Save.

Start a Performance Recording for a View

1. Open the view for which you want to record performance.

When you open a view, Tableau Server appends ":iid=<n>" after the URL. This is a session ID. For example:
Tableau Server on Linux Administrator Guide

http://10.32.139.22/#/views/Coffee_Sales2013/USSalesMarginsByAreaCode?iid=1

2. Type `:record_performance=yes&` at the end of the view URL, immediately before the session ID. For example:

http://10.32.139.22/#/views/Coffee_Sales2013/USSalesMarginsByAreaCode?:record_performance=yes&:iid=1

3. Click the **Refresh** button in the toolbar.

4. Load the view.

   A visual confirmation that performance recording has started is the **Performance** option in the view toolbar:

View a Performance Recording

1. Click **Performance** to open a performance workbook. This is an up-to-the-minute snapshot of performance data. You can continue taking additional snapshots as you continue working with the view; the performance data is cumulative.

2. Move to a different page or remove `:record_performance=yes` from the URL to stop recording.

Interpret a Performance Recording

A performance recording workbook is a Tableau dashboard that contains three views: **Timeline**, **Events**, and **Query**.
For information on how to create a performance recording in Tableau Server, see Create a Performance Recording.

Timeline

The uppermost view in a performance recording dashboard shows the events that occurred during recording, arranged chronologically from left to right. The bottom axis shows elapsed time since Tableau started, in seconds.

In the Timeline view, the **Workbook**, **Dashboard**, and **Worksheet** columns identify the context for events. The **Event** column identifies the nature of the event, and the final column shows each event’s duration and how it compares chronologically to other recorded events:

![Timeline view](image)

Events

The middle view in a performance recording workbook shows the events, sorted by duration (greatest to least). Events with longer durations can help you identify where to look first if you want to speed up your workbook.

![Events view](image)
Different colors indicate different types of events. The range of events that can be recorded is:

- Computing layouts

  If layouts are taking too long, consider simplifying your workbook.

- Connecting to data source

  Slow connections could be due to network issues or issues with the database server.

- Executing query

  - For live connections, if queries are taking too long, it could be because the underlying data structure isn’t optimized for Tableau. Consult your database server’s documentation. As an alternative, consider using an extract to speed performance.

  - For extracts, if queries are taking too long, review your use of filters. If you have a lot of filters, would a context filter make more sense? If you have a dashboard that uses filters, consider using action filters, which can help with performance.

- Generating extract

  To speed up extract generation, consider only importing some data from the original data source. For example, you can filter on specific data fields, or create a sample based on a specified number of rows or percentage of the data.

- Geocoding

  To speed up geocoding performance, try using less data or filtering out data.

- Blending data

  To speed up data blending, try using less data or filtering out data.

- Server rendering
You can speed up server rendering by running additional VizQL Server processes on additional machines.

Query

If you click on an **Executing Query** event in either the **Timeline** or **Events** section of a performance recording dashboard, the text for that query is displayed in the Query section.

If you are connected to a published data source, the query text is displayed in XML. If you are connected to the data source directly, the query is displayed in SQL like shown below:

```
SELECT "State"."ID" AS "ID",
    "StateSynonyms"."Name" AS "State_Name",
    "State"."ParentID" AS "State_ParentID"
FROM "StateSynonyms"
INNER JOIN "State" ON (("State"."ID" = "StateSynonyms"."ParentID") AND ("State"."MapCode" = "StateSynonyms"."MapCode"
```

If it makes sense, you can use the query text to work with your database team on optimizing at the database level. Sometimes the query is truncated and you'll need to look in the Tableau log to find the full query. Most database servers can give you advice about how to optimize a query by adding indexes or other techniques. See your database server documentation for details.

Sometimes for efficiency, Tableau combines multiple queries into a single query against the data. In this case, you may see an **Executing Query** event for the Null worksheet and zero queries being executed for your named worksheets.

**Performance Monitoring Tools**

This topic describes external resources that you can use to monitor and tune performance.

**Disclaimer**: This topic includes information about third-party and community supported products. Please note that while we make every effort to keep references to third-party and community content accurate, the information we provide here might
change without notice. For the most up-to-date information, please consult the documentation for products referenced here. To learn more about community supported tools, see Support levels for IT and developer tools.

- **TabJolt.** A load and performance testing tool that you can use to understand how Tableau Server scales with your workloads, in your environment, and to inform your scalability and capacity needs. Here are some key use cases for when you would use TabJolt:
  
  - To establish a baseline for server performance and test deployments before pushing them to production environments.
  
  - In a new Tableau Server, to help understand how the new server scales in your environment, specifically to your hardware and workload?
  
  - Before upgrading to understand the new version will scale in your environment.
  
  - To find the best server deployment configuration, given your hardware, workbooks and environments.
  
- **Replayer.** A tool that can replay log-based real user traffic from a Tableau Server against any other server or configuration. It replays Tableau Server single- or multi-user sessions. Here are some ways that Replay can be used:
  
  - Playback specific Tableau Server sessions, and filter the session based upon start time or RequestID.
  
  - Use it to simulate load conditions so that you can test how to scale and balance your Tableau Server installations.
  
  - Perform regression testing by running and comparing end-to-end user scenarios for Tableau Server upgrades.
- Capture and report HTTP exceptions that occur in a single-user session.
- Replay a defect, so that you can troubleshoot and verify that it is fixed.

**Scout.** An exploratory tool that captures performance metrics across any workbooks on both Tableau Desktop and Tableau Server Here are some ways that Scout can be used:

- Find slow workbooks on Server.
- Validate performance improvements or regressions after making server configuration or topology changes.
- Validate that workbooks and dashboards are loading properly after upgrading to new Tableau Server.
- Validate that workbooks are still working properly after data source changes.

**Sitescope.** An agentless application monitoring tool.

**Zabbix.** An open-source, real-time monitoring tool.

**Splunk.** A tool for monitoring and analyzing machine data, including logs.

**Graylog.** An open-source log management tool.

### About Client-Side Rendering

When you navigate to a view in Tableau Server, the processing required to display the view (the rendering) can either be performed by your client web browser or by Tableau Server depending on the complexity of the view. The complexity of the view is determined by the number of marks, rows, columns, and more. If a view is less complex, then it is faster for your web browser to render the view than it is to send a request to Tableau Server. If a view is more complex, then it is faster to send a request to Tableau Server and take advantage of the server’s computing power.
As a server administrator, you can configure when client-side rendering happens both for web browsers on your computer and web browsers on mobile devices by adjusting the complexity threshold.

Requirements

- **Supported browsers**: Client-side rendering is supported in Internet Explorer version 9.0 or higher, Firefox, Chrome, and Safari. All of these web browsers include the HTML 5 `<canvas>` element, which is used by client-side rendering.

- **Polygons and the page history feature**: If a view uses the polygon mark type or the page history feature, server-side rendering is performed, even if client-side rendering is otherwise enabled.

Configure the complexity threshold for computers and mobile devices

Because computers have more processing power than mobile devices, Tableau Server performs more client-side rendering in your computer’s web browser than in your mobile device’s web browser. You can adjust how much client-side rendering happens for computers and mobile devices with the complexity thresholds. You might want to adjust the complexity thresholds if you notice that views display slowly on mobile devices. Alternatively, you might want to increase the thresholds to reduce the number of requests to Tableau Server.

By default, the complexity threshold for computer web browsers is 100. To adjust the complexity threshold for computer web browsers, use the following command:

```
  tsm configuration set -k vizqlserver.browser.render_threshold -v [new value]
```

By default, the complexity threshold for web browsers on mobile devices is 60. To adjust the complexity threshold for web browsers on mobile devices, use the following command:

```
  tsm configuration set -k vizqlserver.browser.render_threshold_mobile -v [new value]
```

For example, to change the mobile threshold to 40, you might enter the following command:
tsm configuration set -k vizqlserver.browser.render_threshold_mobile -v 40

For more information on how to use tsm option set, see tsm configuration set Options.

Disable client-side rendering

Client-side rendering is enabled by default and is recommended to improve the performance of views. However, you might want to disable client-side rendering temporarily for testing or if your server is being accessed primarily by computers or mobile devices with very little processing power.

Use the following command to disable client-side rendering:

`tsm configuration set -k vizqlserver.browser.render -v false`

For more information on how to use tsm option set, see tsm configuration set Options.

Testing with the URL Parameter

To test server-side rendering on a session basis, type `?:render=false` at the end of the view’s URL. For example:

`http://localhost/views/Supplies/MyView?:render=false`

If client-side rendering is disabled on Tableau Server, enter `?:render=true` to enable it for the session:

`http://localhost/views/Supplies/MyView?:render=true`

You can also test particular complexity thresholds on individual views to see if it’s appropriate to adjust the server-wide threshold for your server and network conditions. For example, you may find that lower complexity (such as 80) or higher complexity (such as 120) tipping points result in more responsiveness to user interactions. To test a threshold, you can keep the server’s default configuration (client-side-rendering enabled) and enter the test threshold number at the end of the view’s URL. For example:

`http://localhost/views/Supplies/MyView?:render=80`
Monitoring Tableau Server

Configure SMTP Setup

Tableau Server can email server administrators about system failures, and email server users about subscribed views and data-driven alerts. First, however, you need to configure the SMTP server that Tableau Server uses to send email. After configuring SMTP, complete the steps to configure notifications (Configure Server Event Notification), then when you start or restart the server, it will trigger an email notification, which confirms that you have set up notifications correctly.

Encrypted SMTP connections are not supported for notifications or subscriptions.

Configuring SMTP requires that you restart Tableau Server services.

Use the TSM web interface

1. Open TSM in a browser:

   https://<tsm-computer-name>:8850. For more information, see Sign in to Tableau Services Manager Web UI.

2. Click **Notifications** on the **Configuration** tab and click **Email Server**.

3. Enter the SMTP configuration information for your organization:
4. Click **Save Pending Changes** after you've entered your configuration information.

5. Click **Pending Changes** at the top of the page:

6. Click **Apply Changes and Restart**.

Use the TSM CLI

For the initial configuration of SMTP, we recommend that you use the configuration file template below to create a json file. You can also set any single configuration key listed below with the syntax described in tsm configuration set.

1. Copy the following json template to a file. Fill in the key values with your SMTP configuration. See the reference section that follows for more information about SMTP key options.

```json
{
}
```
"configKeys": {
    "svcmonitor.notification.smtp.server": "SMTP server url",
    "svcmonitor.notification.smtp.send_account": "SMTP user name",
    "svcmonitor.notification.smtp.port": 25,
    "svcmonitor.notification.smtp.password": "SMTP server password",
    "svcmonitor.notification.smtp.ssl_enabled": false,
    "svcmonitor.notification.smtp.from_address": "From email address",
    "svcmonitor.notification.smtp.target_addresses": "To email address1,address2",
    "svcmonitor.notification.smtp.canonical_url": "Tableau Server URL"
}

2. Run the `tsm settings import -f file.json` to pass the json file with the appropriate values to Tableau Services Manager to configure Tableau Server for SMTP. Tableau Services Manager will validate the entity values.

3. Run the `tsm pending-changes apply` command to apply the changes. See `tsm pending-changes apply`.

Configuration file reference

This table lists all of the options that can be used to configure SMTP.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>svc-</code></td>
<td>Address of SMTP server.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>mon-itor.notification.smtp.server</code></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>&quot;svc- mon-itor.notification.smtp.server&quot;: &quot;mail.example.com&quot;</td>
</tr>
<tr>
<td><code>svc- mon-itor.notification.smtp.send_account</code></td>
<td>User name for SMTP account.</td>
</tr>
<tr>
<td><code>svc- mon-itor.notification.smtp.port</code></td>
<td>Port number for SMTP server. The default is 25.</td>
</tr>
<tr>
<td><code>svc- mon-itor.notification.smtp.password</code></td>
<td>Password for SMTP server account.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>&quot;svc- mon-itor.notification.smtp.password&quot;: &quot;password&quot;</td>
</tr>
<tr>
<td><code>svc- mon-itor.notification.smtp.ssl_enabled</code></td>
<td>Specifies whether the connection to the SMTP server is encrypted. The default is false.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This should be left as <code>false</code>. Encrypted SMTP connections are not supported for notifications or subscriptons.</td>
</tr>
</tbody>
</table>
| `svc- mon-itor.notification.smtp.from`      | Email address that will send an notification if there's a system failure. The email address must have valid syntax (for example, ITalerts@bigco.-
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **address** | com or noreply@mycompany), but it does not have to be an actual email account on Tableau Server. (Some SMTP servers may require an actual email account, however.)  

**Note:** You can override the system-wide email address on a per-site basis. For more information, see What is a site. |
| **svc-monitor.notification.smtp.target_addresses** | Email address to receive notifications. If email notifications are enabled, you need to include at least one address. Separate multiple addresses with commas.  

**Example:**  
"svc-monitor.notification.smtp.target_addresses": "iluvdata@example.com" |
| **svc-monitor.notification.smtp.canonical_url** | URL of the Tableau Server. Enter http:// or https://, followed by the name or IP address of the Tableau server. Used in the footer of subscription email. |
Configure Server Event Notification

A Tableau Services Manager (TSM) administrator can configure Tableau Server to allow notifications for the following events:

- Content updates
  - Extract failures (enabled by default)
  - Subscription views for users (disabled by default)
- Server health monitoring
  - Server status changes (disabled by default)
  - License reporting (disabled by default)
- Drive space
  - Email alerts when space crosses or remains below pre-configured thresholds (disabled by default)
  - Recording usage history (enabled by default)

**Note:** You need to configure SMTP before you can configure subscriptions or notifications. For more information, see Configure SMTP Setup.

Use the TSM web interface

1. Open TSM in a browser:

   https://<tsm-computer-name>:8850.
For more information, see Sign in to Tableau Services Manager Web UI.

2. Click **Notifications** on the **Configuration** tab and click **Events**.

3. Configure notification settings for your organization:
   - Content updates
     - **Send emails for extract refresh failures**
       When this option is enabled (the default), a server administrator can configure email notifications to be sent when extract refreshes fail. These messages are configured at the site level, so even if this option is enabled, messages are not sent unless the **Send email to data source and workbook owners when scheduled refreshes fail** option is enabled for a site (this is enabled by default). For details, see Enable Extract Refresh Scheduling and Failure Notification.
     - **Allow users to receive email for views that they have subscribed to**
       When this option is enabled (by default is it disabled), a server administrator can configure a site to send subscription email. These email messages are configured at the site level and can only be configured when this option is enabled. For details, see Set Up a Site for Subscriptions.
       When users subscribe to a workbook or view, a snapshot of the view is emailed to them on a scheduled basis, so they can see the latest updates without having to sign into Tableau Server.
     - **Server health monitoring**
       - **Send emails for Tableau Server process events (up, down, and failover)**
Tableau Server sends an email message when the data engine, repository, or gateway server processes stop or restart, or when the initial Tableau Server node stops or restarts.

If you are running a single-server installation (all processes on the same computer), health alerts are only sent when Tableau Server is up. No "down" alerts are sent. If you are running a distributed installation that's configured for failover, a DOWN alert means that the active repository or a data engine instance has failed and the subsequent UP alert means that the passive instance (repository) or second instance (data engine) of that process has taken over.

- **Send emails for Tableau Server license reporting**

  License reporting is generated at Tableau Desktop and sent to Tableau Server.

- **Drive space**

  Enable notifications for remaining drive space on your Tableau Server.

  - **Send emails when unused drive space drops below thresholds**

    You can configure Tableau Server to send email alerts when disk space usage on any node crosses a threshold, or remains below the threshold. And you can configure how often threshold alerts are sent.

    There are two thresholds you must set, **Warning threshold** and **Critical threshold**. Thresholds are expressed in percentage of disk space remaining. The critical threshold must be less than the warning threshold.
You also specify the **Send threshold alert every** option. This determines how often, in minutes, warning and critical alerts should be sent. The default value is 60 minutes.

- **Record disk space usage information and threshold violations for use in custom administrative views**

When you configure Tableau Server to record disk space usage, information about free disk space is saved in the repository and you can view the usage history using the Administrative Views.

4. Click **Save Pending Changes** after you've entered your configuration information.

5. Click **Pending Changes** at the top of the page:

6. Click **Apply Changes and Restart**.

**Use the TSM CLI**

The various notification values described above can be set individually with the `tsm configuration set` command. Alternatively, you can construct a json file and pass all configuration values in one operation. Both methods are described in this section.

**Set notification values individually**

The following table shows the key/value pairs that map to the notification events described earlier in this topic. Use the `tsm configuration set` command with the following syntax to set a single key/value pair:

```
tsm configuration set -k <config.key> -v <config_value>
```

For example, to enable job failure notifications, run the following command:
**tsm configuration set -k backgrounder.notifications_enabled -v true**

<table>
<thead>
<tr>
<th>Notification option</th>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extract failures or Flow run failures</td>
<td>backgrounder.notifications_enabled</td>
<td>true</td>
</tr>
<tr>
<td>Enable subscription views for user</td>
<td>subscriptions.enabled</td>
<td>true</td>
</tr>
<tr>
<td>Server status changes</td>
<td>svcmonitor.notification.smtp.enabled</td>
<td>true</td>
</tr>
<tr>
<td>License reporting</td>
<td>features.DesktopReporting</td>
<td>true</td>
</tr>
<tr>
<td>Remaining space thresholds: enable email notifications</td>
<td>storage.monitoring.email_enabled</td>
<td>true</td>
</tr>
<tr>
<td>Remaining space thresholds: warning percentage</td>
<td>storage.monitoring.warning_percent</td>
<td>integer value, for example, 20</td>
</tr>
<tr>
<td>Remaining space thresholds: critical percentage</td>
<td>storage.monitoring.critical_percent</td>
<td>integer value, for example, 15</td>
</tr>
<tr>
<td>Set email interval</td>
<td>storage.monitoring.email_interval_</td>
<td>integer value, in...</td>
</tr>
</tbody>
</table>
After you are done setting values, you must run the following command:

```bash
tsm pending-changes apply
```

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

Set all notification values with a single json file

To make all notifications settings with a single configuration, you can pass a json file.

Copy and edit the following template to create a file for your configuration.

```json
{
    "configKeys": {
        "backgrounder.notifications_enabled": true,
        "subscriptions.enabled": true,
        "svc-monitor.notification.smtp.enabled": true,
        "features.DesktopReporting": true,
        "storage.monitoring.email_enabled": true,
        "storage.monitoring.warning_percent": 20,
        "storage.monitoring.critical_percent": 15,
        "storage.monitoring.email_interval_min": 25,
        "storage.monitoring.record_history_enabled": true
    }
}
```

After you have saved the file, pass it with the following command:

```bash
tsm settings import -f <path-to-file.json>
```

To apply changes, run the following command:

```bash
tsm pending-changes apply
```
The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

**Maintenance**

**Backup and Restore**

A Tableau Server administrator should perform regular database maintenance, monitor disk usage on the server, clean up unnecessary files to free up space on the server, and back up Tableau Server and its data. Taking these steps can help ensure that Tableau Server runs with maximum efficiency.

You can use the Tableau Services Manager (TSM) command line tool to back up and restore your Tableau data. Tableau data includes data extract files, as well as Tableau Server's own PostgreSQL database, which stores workbook and user metadata, and server configuration data. Tableau Server log files capture activity and can help you diagnose problems. Logs are written to folders on the server and you can archive and remove them to save disk space.

**Note:** You can use the `tsm maintenance restore` command to restore Tableau Server backups created using `tabadmin backup` and `tsm maintenance backup`. Database backups made in other ways, and virtual machine snapshots are not valid sources for restoring Tableau Server.
Platform compatibility

You can use a backup created with Tableau Server on Linux to restore Tableau Server on Windows version 2018.2 and later.

You cannot use a backup created with Tableau Server on Linux to restore earlier versions of Tableau Server on Windows (version 2018.1 and earlier).

You can use a backup created with Tableau Server on Windows (version 2018.2 and earlier) to restore Tableau Server on Linux. For more information about restoring a Windows backup on Tableau Server on Linux, see Migrate Tableau Server from Windows to Linux.

Backup Disk Space Usage

You must have adequate disk space for database backup and restore processes to run successfully. In addition to the amount of space needed for the backup file, you need temporary disk space roughly 10 times the size of the backup file (so if your backup is 4 GB, you should have about 40 GB of temporary disk space available). Similarly you will need adequate temporary disk space for restoring from a backup.

When calculating disk space, be aware that background tasks for cleaning up old extracts are temporarily paused. This means that, for the duration of the backup, extract refreshes will leave extra files in place, adding to disk space usage. If your backup takes a long time, or if your organization uses many extracts that are regularly updated, this can result in a significant amount of temporary disk space usage. These old files will be removed after the backup is complete.

Best Practices for Backing Up Tableau Server

There are several ways you can maximize backup efficiency. Your environment can impact how effective each of these is, so test with your data to see what works best.

- Locating the repository (pgsql) and the File Store on the same node as the Administration Controller can reduce the length of time it takes to back up Tableau Server.
The Administration Controller is usually on the initial node, unless you have had an initial node failure and had to move the controller to another node. When the repository is co-located with the controller it eliminates or greatly reduces the need to compress and transfer data between nodes during the backup process. This is also true with the File Store, especially if your organization uses extracts heavily.

- Use the `--skip-compression` option when backing up Tableau Server. This creates the backup without using compression, and results in a larger backup file but can reduce the amount of time it takes for the backup to complete. For more information, see tsm maintenance backup.

Perform a Full Backup and Restore of Tableau Server

You can use the following steps to back up your Tableau Server deployment. Specifically, these steps describe how to recover a clone of a server from a collection of backup data and assets.

**Note:** The backup process can take a long time to run. Since no other jobs can be run while backup is running, we recommend that you run backup during non-business hours.

Backup data types

There are two types of backup data that Tableau Server can generate. We recommend performing regular backups of each type in case you must restore a server in a recovery scenario:

- Repository data: Tableau Server data consists of the Tableau PostgreSQL database or repository, which contains workbook and user metadata, data extract files, and site configuration data. When you use TSM to create a backup, all of this data is saved in a single file with a .tsbak extension. This data is backed up with the tsm maintenance backup command.

- Configuration and Topology data: includes most of the server configuration
information required to fully recover a server. SMTP, alerting, authentication, are all examples of configuration data that are exportable for backup. Topology data defines how your Tableau Server processes are configured in both single-server and multiple node deployments. Configuration and topology data is backed up with the `tsm settings export` command.

**Note:** You can change the file path used by the `tsm maintenance backup` command from the default value. For more information, see tsm File Paths.

Backup assets that require a manual process

Some configuration data is not included in the `tsm settings export` command and must therefore be documented and restored manually. The following configuration data is excluded from the `tsm settings export` operation. Your backup maintenance process should include documenting the following Tableau Server configuration data:

- **System user accounts.** Tableau Server setup creates an unprivileged user account, `tableau`. This account is used to access Tableau Server resources. This account can be changed during setup. If you have not changed this account, then you do not need to document it.

- **TSM group membership.** There are two groups created by Tableau Server: `tableau` and `tsmadmin`. If you configured alternative groups when you installed Tableau Server, then you’ll need to document the group names.

  In all cases you should document the user accounts that are in these groups. To view membership in a group, run the following command `grep <group_name> /etc/group`.

- **Coordination Service deployment configuration.** If you are running a multinode cluster, document which nodes are running the Coordination Services process. To view process configuration on your nodes, run `tsm topology list-nodes -v`.

- **Customization settings.** If your organization uses custom header or sign-in logos for
Tableau Server on Linux Administrator Guide

Tableau Server web pages, you should include a copy of those assets with your back up portfolio. See tsm customize.

- Authentication assets. Most certificate files, key files, keytab files or other authentication-related assets are not backed up by TSM. The exception are the public certificate and private key for the PostgreSQL database and certificate and key for the gateway process.

  However, all other authentication-related assets are not backed up. For example, if you have enabled access to the PostgreSQL database with the tsm data-access repository-access enable command, be sure to document the name/password pairs for each account you’ve configured. These credentials are not backed up.

- LDAP assets. Keytab files, configuration files, and or other LDAP-related assets are not backed up by TSM.

Internal server secrets and repository passwords are crypto-related configurations that are not exported. However, you do not need to document configuration values. New secrets will be created as part of the restoration process when you initialize the new instance.

Back up Tableau Server for recovery

Tableau Server includes commands that you run to generate backup data for Tableau Server.

> **Note:** When backing up Tableau Server on Linux, the unprivileged user must have write access to the network share where the backup files are written. Otherwise, backup will fail.

To back up server topology and configuration data, use the tsm settings command.

1. Topology and configuration data are included when you run the `tsm settings export` command. The data is exported as a json file. Specify the name and location
of the json file by running the following command:

```
tsm settings export -f <filename>.json
```

**Note:** Because the backup contains secrets, we recommend that you encrypt the backup and store it in a secure place. For more information about Tableau Server secrets, see Manage Server Secrets.

2. Back up repository data. Repository data is backed up with the `tsm maintenance backup` command. Specify the name and location of the backup file by running the following command:

```
tsm maintenance backup -f <filename>.tsbak -d
```

By default, the back up file is written here:

```
/var/opt/tableau/tableau_server-/data/tabsvc/files/backups/<filename>.tsbak
```

For more information about where back up files are written, see `tsm File Paths`. For more information about backing up the repository data, see Back up Tableau Server data for more information.

**Restoring core Tableau Server functionality**

The procedure below uses the assets from the previous two sections to rebuild a Tableau Server in a recovery scenario.

**Note:** If you need to restore only the repository on an otherwise functional Tableau Server, see Restore from a backup. If you are running a distributed deployment, and your initial node has failed, see Recover from an Initial Node Failure.
Topology and configuration backup data must be from Tableau Server on Linux. You cannot restore configuration data from a backup file that was generated on Tableau Server on Windows. To restore a backup made from Tableau Server on Windows to Tableau Server on Linux, see Migrate Tableau Server from Windows to Linux.

You must have the following assets ready:

- Topology and configuration data: This is the json file that is generated by the `tsm settings export` command.

- Repository backup file: This is the file with a `.tsbak` extension that is generated by the `tsm maintenance backup` command.

- Backup assets: These assets include the list of documented configurations as noted in the previous section.

To restore a standalone Tableau Server

1. On the computer where you want to restore Tableau Server, Install and Initialize TSM. If your organization used non-default system user accounts, as described in an early section of this topic, then you must specify the users during this step.

2. Activate and Register Tableau Server.

3. (Optional). On the initial node, Configure Local Firewall.

4. Import topology and configuration data. Copy the topology and configuration json backup file to the computer. Import the json file by running the following command:

   ```bash
   tsm settings import -f <filename>.json
   ```

5. Restore repository data. See Restore from a backup.

6. (Optional). Repopulate TSM group membership. Add users to groups with this
To restore a Tableau Server cluster

1. On the initial node, Install and Initialize TSM. If your organization used non-default system user accounts, as described in an early section of this topic, then you must specify the users during this step.

2. On the initial node, Activate and Register Tableau Server.

3. (Optional). On the initial node, Configure Local Firewall.

4. On the initial node, restore repository data. See Restore from a backup.

5. On the initial node, run `tsm topology nodes get-bootstrap-file --file <path\file>.json`.

6. Copy the bootstrap.json file to all additional nodes in the cluster.

7. On each additional node in the cluster:
   a. Install the Tableau Server package.
   b. Navigate to the scripts directory.
   c. Initiate communication between initial node and the additional node:

      ```
      sudo ./initialize-tsm -b <path-to-bootstrap>.json -u <admin-user-on-first-node> --accepteula
      ```

8. On the initial node, run `tsm topology list-nodes -v` and ensure that the node names have not changed from exported topology settings. If they have, topology
settings should be manually updated with new names, or the processes should be manually configured.

9. **On the initial node**, run `tsm settings import -f <filename>.json --topology-only` to import topology settings if not configuring manually.

10. **On the initial node**, Deploy a Coordination Service Ensemble. The ensemble configuration must match your previous configuration.

11. (Optional). **On the initial node**, finalize setup, verify LDAP (optional), and initialize Tableau Server. See Configure Initial Node Settings.

12. (Optional). **On the initial node**, run `tsm pending-changes apply`

13. **On the initial node**, run `tsm restart`

14. **On the initial node**, repopulate TSM group membership. Add users to groups with this command:

   ```bash
   sudo usermod -G <group_name> -a <username>
   ```

**Restore other functionality**

If the previous server was configured with the following features, then you will need to re-enable and reconfigure them on the restored server:

- **Authentication solutions**: OpenID, external SSL, and trusted authentication. See Authentication.

- **Site customizations**: See `tsm customize`.

- **Enable access to PostgreSQL repository**: See `tsm data-access repository-access enable`.

**Back up Tableau Server data**

Regularly backing up Tableau Server is an important step in proper administration and maintenance of your server. You can use the `tsm maintenance restore` command to
Tableau Server backups created using `tabadmin backup` and `tsm maintenance backup`. Database backups made in other ways, and virtual machine snapshots are not valid sources for restoring Tableau Server, so it is critical that you have an up-to-date backup.


Tableau Server data includes data extract files, as well as the Tableau PostgreSQL database, which contains workbook and user metadata, and configuration data. When you use TSM to create a backup, all of this data is saved in a single file with a .tsbak extension. If you are running a distributed installation of Tableau Server data from all the nodes is backed up.

The frequency of your backups depends on your environment, including how much use your server gets and how much and frequently the content and users change. Any changes or updates that happen after your backup will be lost if there is a system failure and you need to restore Tableau Server. The more activity there is, the more often you need to back the server up.

In addition to regular backups, you should always create a backup before upgrading to a new version of Tableau Server.

To help protect against data loss, after you create the backup, you should store the .tsbak file on a computer that is not a part of your Tableau Server installation.

Backup and Disk Space Usage

You must have adequate disk space for database backup and restore processes to run successfully. In addition to the amount of space needed for the backup file, you need temporary disk space roughly 10 times the size of the backup file (so if your backup is 4 GB, you should have about 40 GB of temporary disk space available). Similarly you will need adequate temporary disk space for restoring from a backup.
When calculating disk space, be aware that background tasks for cleaning up old extracts are temporarily paused. This means that, for the duration of the backup, extract refreshes will leave extra files in place, adding to disk space usage. If your backup takes a long time, or if your organization uses many extracts that are regularly updated, this can result in a significant amount of temporary disk space usage. These old files will be removed after the backup is complete.

Create a backup using the TSM command line interface (CLI)

Use the `tsm maintenance backup` command to create a backup of the data managed by Tableau Server. This data includes data extract files and the Tableau PostgreSQL database, which contains workbook and user metadata.

**Note:** When backing up Tableau Server on Linux, the unprivileged user must have write access to the network share where the backup files are written. Otherwise, backup will fail.

To back up server configuration data, use the `tsm settings` command. When you use the `tsm maintenance backup` command, the current date is appended to the backup file:

```
tsm maintenance backup -f <backup_file> -d
```

For more information, see `tsm maintenance backup`.

Create a pre-upgrade backup

You should always create a backup before upgrading Tableau Server. You can create a backup while Tableau Server is running and minimize the amount of time the server is unavailable during upgrade. The process for creating a pre-upgrade backup is the same as for creating regular backups, with one additional consideration for distributed installations.
**Note:** Uninstall Tableau Server from any nodes that you are not including in your new installation to avoid conflicts between the older nodes and the new installation.

Script the backup process

If you back up often, you might want to create a script that performs the backup and related tasks for you. These tasks include:

- Clean up files and folders before running the backup.
- Running the backup itself.
- Copying the backup file to a separate computer for safekeeping.

This section discusses `tsm` commands you can use together to perform a backup and related tasks.

For additional information about scripting TSM commands, see the Tableau Community Forums.

Remove log files and clear temporary folders

You can clean old Tableau Server log file and temporary files to reduce the time it takes to create a backup, and to ensure the backup file is as small as possible.

To clean log files older than a few days, run the following command:

```
tsm maintenance cleanup
```

Run the backup

**Note:** When backing up Tableau Server on Linux, the unprivileged user must have write access to the network share where the backup files are written. Otherwise, backup will fail.
To create the backup, use the `tsm maintenance backup` command:

```
tsm maintenance backup --file <backup_file> --append-date
```

Note the following about the command:

- Add `--append-date` to the command to include the date in the backup file name.
- By default the backup file is created in `/var/opt/tableau/tableau_server-<data>/tabsvc/files/backups/`. For more information, see `tsm maintenance backup`.

Copy the backup file to another computer

As a best practice, after the backup is created, copy the backup file to another location that is separate from Tableau Server.

**Restore from a backup**

Use the `tsm maintenance restore` command to restore your Tableau Server data. You might do this if you had a system failure and need to restore your data, if you need to switch back to a previous version of Tableau Server (for example, if there is a problem with an upgrade), or if you are moving Tableau Server to new hardware. You can use the `tsm maintenance restore` command to restore Tableau Server backups created using `tabadmin backup` and `tsm maintenance backup`. If you are restoring a backup created using `tabadmin backup`, *and* you used a custom asset key, you must save a copy of your `asset_keys.yml` file so you can include the file when doing your restore. For more information, see Save your asset keys file before uninstalling Tableau Server for Windows 2018.1.x or earlier.

Database backups made in other ways, and virtual machine snapshots are not valid sources for restoring Tableau Server.

When you use `tsm maintenance restore` to restore your Tableau data, data extract files and the contents of the PostgreSQL database are overwritten with the content in the
backup file (.tsbak). If you are running a distributed installation of Tableau Server, perform the restore on the initial node or wherever the TSM Controller is running.

You can only restore from a backup that has the same type of identity store as the running server. For example, a backup from a server using local authentication can be restored to a Tableau Server initialized with local authentication, but a backup from a server using Active Directory authentication cannot be restored to a server initialized with local authentication.

Restore Tableau Server from a backup file

**Note:** This operation includes steps that you may need to perform using the TSM command line.

1. (Optional) Copy the .tsbak file to the default file location.

   **Note:** If you are restoring a backup that was copied into the backups folder, ensure that the Run As service account, which can be found in TSM Web UI under **Security**, has at least Read access to the backup file. Otherwise, the restore process may not be able to unzip the backup file and the restore will fail.

2. Stop the server. At a command prompt, type:

   ```
   tsm stop
   ```

3. Restore from a backup file. At a command prompt, type:

   ```
   tsm maintenance restore --file <file_name>
   ```

   In the above line, replace `<file_name>` with the name of the backup file you want to restore from.
4. Restart the server:

   tsm start

When you restore a .tsbak file, Tableau Server automatically creates a copy of its current data folder, names it tabsvc.bak-*, and places it in /var/-opt/tableau/tableau_server/data. This folder is an emergency backup of Tableau Server that Tableau Support may be able to use in case something goes wrong during backup restoration.

When the restore is complete and you have verified that Tableau Server is running correctly with all the expected data, it's safe to remove any tabsvc.bak-* folders from /var/-opt/tableau/tableau_server/data to free additional disk space. In Tableau Server clusters, tabsvc.bak-* folders are created on each machine running Tableau Server.

**Important:** Only remove the tabsvc.bak-* folders. Do not remove the tabsvc folder, which is also located under /var/opt/tableau/tableau_server/data. It contains necessary Tableau Server data.

**Server Maintenance**

As an administrator, you will want to check the status of the server, analyze and monitor the activity on the server, manage scheduled tasks, or perform certain maintenance activities such as clearing saved data connection passwords. In addition, there are several settings that you may want to specify to customize the user experience for people using the server. You can do some of these tasks from the General page of the Status page and others from the Settings page.
View Server Process Status

There are two locations in Tableau Server or Tableau Services Manager (TSM) where administrators can view the state of Tableau processes. You may be able to access one or both of these locations, depending on how your account and server are set up. Most of the process status information that displays is duplicated on both Status pages. This article explains each page, and identifies what is unique for each one.

- The Tableau Services Manager (TSM) status page is accessible in TSM and can be viewed by TSM administrators. You must be able to log into TSM to see this page. For information about signing into TSM, see Sign in to Tableau Services Manager Web UI.

- The Tableau Server status page appears in the Tableau Server web UI and is accessible by Tableau Server administrators. This page includes Tableau Server processes, along with links to troubleshooting documentation if a process is not running as expected. If you hover your mouse pointer over the status indicator for a process, a tooltip shows the node name and the port the process is running on. The Tableau Server status page does not show TSM processes. For information about signing into Tableau Server as an administrator, see Sign in to the Tableau Server Admin Area.

Tableau Services Manager (TSM) Status page

The TSM Status page shows you the state of server processes, including TSM Controller and License Server. These two processes do not display on the Tableau Server Status page.
### Possible status indicators are listed at the bottom of the table:

- **Active**
- **Busy**
- **Degraded**
- **Error**
- **Stopped**
Tableau Server Status page

Possible status indicators are listed at the bottom of the table:

- **Active** — The process is functioning as intended. See File Store in Troubleshoot Server Processes for details on possible active states.
- **Busy** — The process is completing some task. See File Store and Repository in Troubleshoot Server Processes for more information.
Passive—The repository is in passive mode
Unlicensed—The process is unlicensed.
Down—The process is down. The implications of this differ depending on the process.
Status unavailable—Tableau Server is unable to determine the status of the process.

If there is additional information, a message displays below the status icon and links to appropriate documentation:

![Ready for removal]

For more information about troubleshooting process status, see Troubleshoot Server Processes.

Access Status Remotely

**Note:** The information in this article refers to the Tableau Server status page. For information about the Tableau Server status page and the TSM status page, see View Server Process Status.

You must be a Tableau Server administrator to see the Server Status page, but you can grant remote access to other computers to allow access to a machine-readable (XML) version of the Status table by non-admin users and by computers other than the initial Tableau Server node. One reason you might do this is as part of a remote monitoring process.

To grant remote access to Tableau Server status:

1. Open a command prompt as an administrator and type the following:

   ```
   tsm configuration set -k wgserver.systeminfo.allow_referer_ips -v <ip address>
   ```

   In the above command, `<ip address>` is the IPv4 address of the computer for
which you want to enable remote access to the Tableau Server status XML.

For example:

```bash
tsm configuration set -k wgserver.systeminfo.allowreferer_ips -v 10.32.139.31
```

If you are enabling remote access for more than one computer, use commas to separate each IP address.

```bash
tsm configuration set -k wgserver.systeminfo.allowreferer_ips -v 10.32.139.31,10.32.139.35
```

2. Commit the configuration change:

```bash
tsm pending-changes apply
```

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

Now, users of computers with the IP addresses that have been added can view Tableau process status by entering the URL `http://<server>/admin/systeminfo.xml` in a browser or from a command line (for example, `curl http://jsmith/admin/systeminfo.xml`).

If Tableau Server has been configured to work with a load balancer or proxy server, use the hostname or IP address of the initial Tableau Server node to access the XML version of the status page.

For details on the XML that is returned, see Get Process Status as XML.

Get Process Status as XML

To get a machine-readable version of the server process status, that is, a version of the status formatted in XML, use the following URL:
You must be signed in to Tableau Server to view the machine-readable process status, or have enabled remote access.

The server returns a status report similar to the following:

```xml
<systeminfo xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <machines>
    <machine name="my_tableau_server">
      <repository worker="my_tableau_server:8060" status="Active" preferred="false"/>
      <dataengine worker="my_tableau_server:27042" status="Active"/>
      <applicationserver worker="my_tableau_server:8600" status="Active"/>
      <apiserver worker="my_tableau_server:8000" status="Active"/>
      <vizqlserver worker="my_tableau_server:9100" status="Active"/>
      <dataserver worker="my_tableau_server:9700" status="Active"/>
      <backgrounder worker="my_tableau_server:8250" status="Active"/>
      <gateway worker="my_tableau_server:80" status="Active"/>
      <searchandbrowse worker="my_tableau_server:11000" status="Active"/>
      <cacheserver worker="my_tableau_server:6379" status="Active"/>
      <filestore worker="my_tableau_server:9345" status="Active" pendingTransfers="0" failedTransfers="0" syncTimestamp="2015-02-27T20:30:48.564Z"/>
      <clustercontroller worker="my_tableau_server:12012" status="Active"/>
    </machine>
  </machines>
</systeminfo>
```
<coordination worker="my_tableau_server:12000" status="Active"/>
</machine>
</machines>
<service status="Active"/>
</systeminfo>

Status values in the XML

- **<process> worker** - The name of the node running the process and the port the process is using.

- **status** - The status of the process on the node. Possible values are: Active, Passive, Unlicensed, Busy, Down, ReadOnly, ActiveSyncing, StatusNotAvailable, StatusNotAvailableSyncing, NotAvailable, DecommissionedReadOnly, DecomisioningReadOnly, and DecommissionFailedReadOnly

- **pendingTransfers** - A count of the workbook or data source extracts the node needs to get to be fully synced. These represent items that were published to this file store node, and items that were published to other file store nodes and need to be copied to this node.

- **failedTransfers** - A count of the workbooks or data sources that did not transfer successfully to this file store node during the last automated job. The automated job normally runs about every 15 to 30 minutes, but may take longer when transferring a large number of extracts or large extracts.

  Failed transfers do not necessarily indicate a problem with Tableau Server. The recurring automated job will normally transfer files that failed during the previous sync. Reasons for failed file transfers are listed in the logs.

- **syncTimestamp** - The time in UTC of the last automated job that ran and synchronized files.
Troubleshoot Server Processes

**Note:** The information in this article refers to the Tableau Server status page. For information about the Tableau Server status page and the TSM status page, see View Server Process Status.

When Tableau Server is functioning properly, processes will show as Active, Busy or Passive (Repository). If there is additional information, a message appears below the status icon:

![Ready for removal](image)

Possible status indicators are:

![Status icons](image)

The following sections provide troubleshooting recommendations for status messages that you may see.

**Cluster Controller**

This message will only display if you have more than two nodes.

**Status: Down; Message: "Node degraded"**

One or more of the following are true:

- Repository on the node is stopped.
- Node cannot respond to failover elsewhere on the cluster.
- If Tableau Server is configured for high availability and this is the active repository, failover to the second repository occurs.
- No status available for repository or file store on this node.
No action is necessary unless the cluster controller is regularly down or is down for an extended period of time.

If that occurs, take the following actions, in order, until the problem is resolved:

1. Check disk space. If disk space is limited, save the log files (use tsm maintenance ziplogs) in case you need them for Support, then remove unnecessary files.
2. Restart Tableau Server.
3. If Cluster Controller continues to show as down, save the log files (tsm maintenance ziplogs) and contact Support.

File Store

File Store status only reflects the state of the file store when the page was loaded.

An active status (✔️) with no message indicates that no extracts were being synchronized when the page was loaded. It is possible that the recurring "catch-all" job is running and synchronizing extracts.

estatus: Busy; Message: "Synchronizing"

"Synchronizing," usually indicates that extracts were being synchronized across file store nodes when the page was loaded.

However, the "synchronizing" message is also returned following installation (both single-node and multi-node). After Tableau initializes the status should disappear within 15 or 20 minutes.

estatus: Down; "Data Extracts unavailable"

On a single-node installation: "Data Extracts unavailable" indicates that existing extracts may be available but publish/refresh will fail. On multi-node installations, this message indicates that extract synchronization will fail for this node.

No action is necessary unless the file store is regularly down or is down for an extended period of time.
If that occurs, take the following actions, in order, until the problem is resolved:

1. Check disk space. If disk space is limited, save the log files (use `tsm maintenance ziplogs`) in case you need them for Support, then remove unnecessary files.
2. Restart Tableau Server.
3. If Cluster Controller continues to show as down, save the log files (`tsm maintenance ziplogs`) and contact Support.

**Status: Busy; "Decommissioning"**

This message indicates that this File Store is in read-only mode and that any unique files on this node are being replicated to other file store nodes.

To remove this node, wait until the status message changes to "Ready for removal".

**Status: Active; "Ready for removal"**

This message indicates that the File store is in read-only mode.

You can safely stop (`tsm stop`) the cluster and remove File Store processes, or remove entire node.

**Status: Active; "Decommission failed"**

This message indicates that the File store is in read-only mode, and that at least one unique file failed to replicate to another file store node.

To resolve a failed decommissioning:

1. Run the `tsm topology filestore decommission` command again.
2. Check disk space on other file store nodes. Decommissioning will fail if another file store node does not have enough space to store all the extracts.
3. Check the `tsm.log` file on the initial node and additional nodes for errors.
4. Stop Tableau Server (`tsm stop`) and then try running the `tsm topology filestore decommission` command again.
5. Put the file store node back into read/write mode (`tsm topology filestore recommission`), collect logs, and then contact Support.
6. With Support: copy and merge `extracts` directory from this file store node to the same directory on another file store node.

Repository

⚠️ Status: Busy; Message: "Setting up"

The "Setting up" message indicates one or more of the following states:

- Passive repository is being synchronized with active repository.
- Repository is not ready to handle failover.
- Repository may have gotten more than two minutes behind active repository and is being setup again (this is faster than waiting for a sync).
- Failover occurred and this former active repository is rejoining the cluster.

Wait until the repository status message changes to "Passive".

If this message does not appear, or if it is taking a long time:

1. Check disk space and free space if possible.
2. Check cluster controller logs for errors.
3. Restart node.

⚠️ Status: Busy; Message: "Synchronizing"

Repository is synchronizing, for example after a failover.

🚫 Status: Down; Message: n/a

When the Repository shows a status of down and there is no message, then the Repository is in one of the following states:

- If the installation is configured for high availability, failover of the repository occurred.
- Processes are restarting with updated database connection configurations after failover.
- If another active repository is not available, Tableau Server is down.

Take these actions in order until a step resolves the problem:
1. Wait several minutes for cluster controller to attempt to restart.
2. Restart Tableau Server (**tsm restart**).
3. Check disk space. If disk space is limited, save the log files (**tsm maintenance ziplogs**) in case you need them for Support, then remove unnecessary files.
4. Restart Tableau Server.
5. If repository continues to show as down, save the log files (**tsm maintenance ziplogs**) and contact Support.

**Status:** Passive; **Message:** n/a

A passive status with no message indicates that the node is working as intended and that it is ready for failover if needed.

**VizQL Server**

**Status:** Unlicensed; **Message:** n/a

For information about unlicensed status for a VizQL Server process, see Handle an Unlicensed VizQL Server Process.

**Clear Saved Data Connection Passwords**

As the administrator, if you enable users to save data source passwords, server users can save data source passwords across multiple visits and browsers so they are no prompted for their credentials each time they connect to a data source.

You can reset the data source passwords for all Tableau Server users. Doing this forces them to sign in to the data sources the next time they visit a view that requires database authentication. Server users can also clear their saved data connection passwords on an individual basis using their User Preferences page.
To clear saved data connection passwords for all server users:

1. In a site, click **Settings > General**.

2. Under Saved Credentials, click **Clear All Saved Credentials**.

Synchronize All Active Directory Groups on the Server

As a server administrator, you can synchronize all Active Directory groups (that have been configured on Tableau Server) on a regular schedule or on-demand on the **General** tab of the **Settings** page for the server.
**Note:** If you run Tableau Server on Linux, all external directory communication is configured and managed with a LDAP identity store. In the context of user and group synchronization, Tableau Server configured with LDAP identity store is equivalent to Active Directory. Active Directory synchronization features in Tableau Server function seamlessly with properly configured LDAP directory solutions.

Before you begin

Before synchronizing groups as described in this topic, you must first import the Active Directory group into Tableau Server. See Create Groups via Active Directory.

Synchronize Active Directory groups on a schedule

1. **Single-site:** Click **Settings > General**.

   **Multisite:** In the site menu, click **Manage All Sites** and then click **Settings > General**.

2. Scroll down the page to **Active Directory Synchronization**, and then select **Synchronize Active Directory groups on a regular schedule**.
3. Select the frequency and time of synchronization.

4. Click **Save**.

Synchronize all Active Directory groups on demand

At any time, you can synchronize Active Directory groups with Tableau Server to ensure that new users and changes in Active Directory are reflected in all Active Directory groups on Tableau Server.

1. **Single-site**: Click **Settings > General**.

    **Multisite**: In the site menu, click **Manage All Sites**, and then click **Settings > General**.

2. Under **Active Directory Synchronization**, click **Synchronize All Groups**.

View synchronization activity

You can view the results of synchronization jobs in the **Background Tasks for Non Extracts** administrative view. **Queue Active Directory Groups Sync** is the task that queues and indicates the number of **Sync Active Directory Group** tasks to be run.
1. **Single-site**: Click **Status**.

   **Multisite**: In the site menu, click **Manage All Sites** and then click **Status**.

2. Click the **Background Tasks for Non Extracts** link.

3. Set the **Task** filter to include **Queue Active Directory Groups Sync** and **Sync Active Directory Group**.

You can quickly navigate to this administrative view by clicking the **View synchronization activity** link in the **Settings** page for the server.

Set the minimum site role for users in an Active Directory group

In the **Groups - Details** page, you can set the minimum site role for group users to be applied during Active Directory synchronization.

This setting does not run synchronization; instead, it sets the minimum site role to applied to the group every time synchronization runs. The result is that when you synchronize Active Directory groups, new users are added to the site with the minimum site role. If a user already exists, the minimum site role is applied if it gives the user more access in a site. If you don’t set a minimum site role, new users are added as **Unlicensed** by default.

**Note**: A user’s site role can be promoted but never demoted based on the minimum site role setting. If a user already has the ability to publish, that ability will always be maintained. For more information on minimum site role, see Site roles and Active Directory import and synchronization.

1. In a site, click **Groups**.

2. On the Groups page, select a group.

   Click **Actions > Minimum Site Role**.
3. Select the minimum site role, and then click **Change Site Role**.

What happens when users are removed in the source Active Directory?

Users cannot be automatically removed from the Tableau Server through an Active Directory sync operation. Users that are disabled, deleted, or removed from groups in Active Directory remain on Tableau Server so that administrators can audit and reassign the user’s content before removing the user’s account completely. For more information, see Sync behavior when removing users from Active Directory.

Improving group synchronization performance

Active Directory synchronization is performed by the backgrounder process. The Backgrounder process is the same process that is used for managing and creating extracts, and is also used to generate subscription content. In large organizations with dynamic group membership and heavy extract usage, the Active Directory group synchronization process may be disruptive. We recommend running group synchronization during non-business hours.

By default, the Backgrounder process performs synchronization in a serial operation. This means that each group is synchronized, one after the other, in a single Backgrounder process. If you are running multiple instances of Backgrounder processes either on a single Tableau Server or across a distributed deployment, consider enabling parallel processing for
Active Directory synchronization. When parallel Backgrounder processing is enabled, the group synchronization is distributed across multiple Backgrounder processes for better performance.

To enable parallel backgrounder processing for group synchronization, open TSM CLI and enter the following commands:

```
  tsm configuration set -k backgrounder.enable_parallel_adsync -v true
  tsm pending-changes apply
```

Set the Default Start Page for All Users

In a new deployment, when users sign in to the Tableau Server web authoring environment, they are taken to the Content tab. By default, this tab shows all of the site's top-level projects. As the server administrator, you can change users' default landing page. For example, you can show all workbooks, and when the user signs in, they see the workbooks they have access to.

To set the default start page for all users

1. Display the page or filtered view you want to be the default page users see when they sign in to the site.

2. Select your initials in the upper right area of the page.
3. Select **Make This the Start Page for All Users**.

![Admin Menu](image)

Users can also specify their own start pages in their account settings (for information, search for “Access Your Profile and Account Settings” in the online Tableau Server Help for your operating system).

**Disable Automatic Client Authentication**

After Tableau Desktop clients first successfully sign in to Tableau Server, they are automatically authenticated in the future. Client sessions are managed by OAuth access and refresh tokens.

By default, all client tokens reset after a year. If a client token has not been used in 14 days, then it will expire. You can change these values by setting the `refresh_token.absolute_expiry_in_seconds` and `refresh_token.idle_expiry_in_seconds` options. See `tsm configuration set Options`.

As a Tableau Server administrator can also disable automatic authentication.

To immediately disconnect all clients from Tableau Server and require users to sign in every time they connect:

1. In the site menu, click **Manage All Sites**, and then click **Settings > General**.

2. Under **Connected Clients**, clear the option **Allow clients to automatically**
connect to Tableau Server.

3. Click Save.

Remove Unneeded Files

As a best practice, you should monitor space usage on your server. If you need to make more space available, you can use the `tsm maintenance cleanup` command to remove Tableau Server log files, temporary files, and rows from the `http_requests` table of the Tableau Server PostgreSQL database.

You should run the `tsm maintenance cleanup` command regularly.

Server Settings (General)

The following settings are available on the General page in Server - Settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded Credentials - Allow publishers to embed data source credentials in a workbook</td>
<td>Allows publishers to attach passwords to published workbooks that will automatically authenticate web users to connect to data sources. The passwords are attached to workbooks and are only accessible on server. That is, when the workbook is opened in Tableau Desktop, users will still need to enter a user name and password to connect to the data source. When this setting is turned off, all existing embedded passwords are saved but are not used for authentication. If you turn the setting back on, users don't have to re-embed the passwords.</td>
</tr>
<tr>
<td>Embedded Credentials - Allow publishers to schedule data extract refreshes</td>
<td>Allows publishers to assign workbooks to schedules. This option is only available if Allow publishers to embed data source credentials in a workbook is enabled. When this setting is enabled, publishers will see scheduling options in the Publish dialog box.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Saved Credentials - Allow users to save passwords for data sources</strong></td>
<td>Allows users to choose &quot;Remember my password&quot; and save data source passwords across multiple visits, browsers, and devices. (By default, users can choose to &quot;Remember my password until I sign out,&quot; which lets them save their password only for a single browser session.) As an administrator, you can clear all saved passwords at any time. In addition, users can clear their own saved passwords.</td>
</tr>
<tr>
<td><strong>Saved Credentials - Allow users to save OAuth access tokens for data sources</strong></td>
<td>Allows users to store access tokens with their user preferences. Access tokens are provided by cloud data sources that support OAuth connections, and they are used instead of user names and passwords to grant access to the data.</td>
</tr>
<tr>
<td><strong>Connected Devices - Allow devices to automatically connect to Tableau Server</strong></td>
<td>Controls whether mobile users must sign in and provide their credentials every time they connect to Tableau Server, or if users can connect with their devices to Tableau Server without providing credentials after they authenticate their device successfully the first time. For more information, see Disable Automatic Client Authentication.</td>
</tr>
<tr>
<td><strong>Guest Access - Enable Guest account</strong></td>
<td>Allows users to view and interact with embedded views without having to sign in to a Tableau Server account. Permission can be assigned to the Guest User account to control the interactivity allowed for each view. This option is only available if you have a core-based server license.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Default Start Page</strong></td>
<td>Takes you to the server’s current default start page for all users. For more information on how to change the default start page, see Set the Default Start Page for All Users. Individual users will be able to override this setting (search for &quot;Access Your Profile and Account Settings&quot; in the Tableau Server Help for details).</td>
</tr>
<tr>
<td><strong>Language and Locale</strong></td>
<td>Controls the language used for the server user interface and the locale used for views. Individual users can override this setting on their Account Settings page. Also, web browser settings are evaluated first to determine which language and locale should be used. For more information, see Language and Locale for Tableau Server.</td>
</tr>
<tr>
<td><strong>Active Directory Synchronization</strong></td>
<td>Controls the synchronization of all Active Directory groups in Tableau Server based on a schedule that you specify after you select the option <strong>Synchronize Active Directory groups on a regular schedule</strong>. For more information, see Synchronize All Active Directory Groups on the Server.</td>
</tr>
<tr>
<td><strong>Recommendations Trainer</strong></td>
<td>Suggests server content, such as data sources and tables, to Tableau Desktop users. Content suggestions are based on popularity of the content or on content frequently used by other users who are similar to the current user. Scheduling options control how often the server checks for new content and new usage information to keep the recommendations up to date.</td>
</tr>
</tbody>
</table>
date. New content includes new and updated data sources. New usage information includes information such as "Laura Rodriguez used the Food Catering data source" and "Henry Wilson used the Monthly Sales data source."

If you notice any impact on server performance, schedule this process to occur at a time when the server load is low. To track performance impact, look for the "Recommendations Trainer" task in the Background Tasks for Non Extracts view.

If you want to disable Recommendations, change the tsm configuration set Options option, "recommendations.enabled", to false.

| Reset to Default Settings | Returns any server settings that have been changed since setup to their original state. |

**Stop or Restart the Tableau Server Computer**

As a best practice, you should *always* stop Tableau Server before you stop or restart the computer it is running on. This is true whether you are running Tableau on virtual machines (VMs), or on dedicated hardware. You should never turn off a computer without first stopping Tableau Server. Shutting down the computer while Tableau is running can cause problems restarting Tableau Server, and may result in unexpected results.

To be safe, follow these steps, whether you have a scripted process to shut down your systems, or manually shut down your computers:

1. Stop Tableau Server.
You can do this either from the command line, using the `tsm stop` command, or from the TSM Web UI, by clicking **Tableau Server is running**, and selecting **Stop Tableau Server**.

**Note:** Some TSM processes will continue to run, even after you stop Tableau Server. This is normal, and you can go ahead and stop your computer. The running services are designed to shut themselves off when the computer is stopped.

2. Once Tableau is stopped, stop your computer.

3. When you are ready, restart your computer. This might be after you have completed planned maintenance, or after leaving the computer off for some extended period of down time.


   You can do this either from the command line, using the `tsm start` command, or from the TSM Web UI, by clicking **Tableau Server is stopped**, and selecting **Start Tableau Server**.

   TSM will start automatically when the computer starts, so you can run tsm commands even though Tableau Server is stopped.

### tsm Command Line Reference

The topics in this section include reference content for Tableau Services Manager (TSM) command line interface (CLI) to support Tableau Server.

TSM is used to manage installation and configuration of Tableau Server. To learn more about TSM, see Tableau Services Manager Overview.

You can automate the installation and configuration tasks supported by the TSM CLI using the TSM API. To learn more about the prerelease (Alpha) TSM API, see Tableau Services Manager API.
Looking for tsm commands for Tableau Server on Windows? See tsm Commands.

Using the tsm CLI

You can run tsm commands on the initial node (the node where TSM is installed), or on any additional node in the cluster.

To run tsm commands, you need to open a command prompt.

1. Open a command prompt with an account that is a member of the tsmadmin group on a node in the cluster.

2. Run the command you want. If you are running the command from a node other than the initial node, include the -s option to specify the URL of the initial node by name (not IP address), and include the TSM port, 8850.

To see the version of TSM and Tableau Server from the initial node:

   tsm version

To see the version of TSM and Tableau Server from an additional node:

   tsm version -s https://<initial_node_name>:8850

   For example:

   tsm version -s https://myTableauHost:8850

Viewing help content in the shell

To view minimal help content from a command line, use the tsm help category.

Synopsis

   tsm help [category] [command]
Commands

`tsm help`

Help for all tsm commands

`tsm help <category>`

Show help for a specific command category. For example, `tsm help authentication`.

`tsm help <category> <command>`

Show help for a specific command. For example, `tsm help authentication open-id`.

`tsm help command`

List all top-level commands or categories.

Categories

`tsm authentication`

You can use the `tsm authentication` commands to enable, disable, and configure user authentication options for Tableau Server.

- `kerberos`
  - configure
  - disable
  - enable
- `list`
Enable, disable, and configure Kerberos user authentication on Tableau Server. See Configure Kerberos.

Synopsis

```sh
tsm authentication kerberos configure --keytab-file <keytab_file.keytab> [global options]

tsm authentication kerberos enable [global options]

tsm authentication kerberos disable [global options]
```
Options for kerberos configure

-kt, --keytab-file <keytab_file.keytab>

   Required.
   Specifies the service.keytab file used for requests to the KDC.

\textbf{tsm authentication list}

List the server’s existing authentication-related configuration settings.

\textbf{Synopsis}

\texttt{tsm authentication list [--verbose][global options]}

\textbf{Options}

\texttt{v, --verbose}

   Optional.
   Show all configured parameters.

\textbf{tsm authentication mutual-ssl <commands>}

Enable, disable, and configure mutual SSL for user authentication on Tableau Server. To learn more about mutual SSL, see Configure Mutual SSL Authentication.

Before you enable mutual SSL, you must enable and configure SSL for external communication. For information, see Configure SSL for External HTTP Traffic to and from Tableau Server.

\textbf{Synopsis}

\texttt{tsm authentication mutual-ssl configure [options]}
\texttt{[global options]}

\texttt{tsm authentication mutual-ssl disable [global options]}

\textbf{Tableau Server on Linux Administrator Guide}
tsm authentication mutual-ssl enable [global options]

Options

-cf, --ca-cert <certificate-file.crt>

Optional.

Specifies the location and file name for the certificate file. The file must be a valid, trusted certificate from a Certificate Authority (for example, Verisign).

-fb, --fallback-to-basic <true | false>

Optional.

Specifies whether Tableau Server should accept user name and password for authentication if SSL authentication fails.

Default value is false, to indicate that when configured for mutual SSL, Tableau Server does not allow a connection when SSL authentication fails. However, Tableau Server accepts username and password authentication from REST API clients, even if this option is set to false.

-m, --user-name-mapping <upn | ldap | cn>

Optional.

Specifies the user name syntax (UPN, LDAP or CN) to retrieve from identity store or directory. The syntax must match the format for Subject or Subject Alternative Name on the user certificate.

-rf, --revocation-file <revoke-file.pem>

Optional.

Specifies the location and file name for the certificate revocation list file. This file can be a .pem or .der file.
tsm authentication openid <commands>

Enable, disable, and configure OpenID Connect (OIDC) user authentication on Tableau Server.

Synopsis

tsm authentication openid configure [options] [global options]

 tsm authentication openid disable [global options]

 tsm authentication openid enable [global options]

 tsm authentication openid get-redirect-url [global options]

 tsm authentication openid map-claims [options] [global options]

Options for openid configure

-a, --client-authentication <string>

 Optional.

 Specifies custom client authentication method for OpenID Connect.

 To configure Tableau Server to use the Salesforce IdP, set this value to client_secret_post.

-cs, --client-secret <string>

 Optional.

 Specifies the provider client secret. This is a token that is used by Tableau to verify the authenticity of the response from the IdP. This value is a secret and should be kept securely.

-cu, --config-url <CONFIG-URL>

 Optional.
Tableau Server on Linux Administrator Guide

Specifies the provider configuration URL. The default value is constructed based on the name of the server (gateway.public.host), and the gateway port, if any (gateway.public.port). In addition, by default the protocol is set to https:// if SSL is enabled for the server.

-mf, --config-file <config-file.json>

Optional.

Specifies the local path to the static OIDC discovery JSON document.

-i, --client-id <CLIENT-ID>

Optional.

Specifies the provider client ID that your IdP has assigned to your application.

-id, --ignore-domain <true | false>

Optional. Default: false

Set this to true if the following are true:

- You are using email addresses as usernames in Tableau Server
- You have provisioned users in the IdP with multiple domain names
- You want to ignore the domain name portion of the email claim from the IdP

Before you proceed, review the user names that will be used as a result of setting this option to true. User name conflicts may occur. In the case of a user name conflict, the risk of information disclosure is high. See Requirements for Using OpenID Connect.

-if, --iframed-idp-enabled <true | false>

Optional. Default: false
Specifies if IdP is allowed inside of an iFrame. The IdP must disable clickjack protection to allow iFrame presentation.

-ij, --ignore-jwk <true | false>

Optional. Default: false

Set this to true if your IdP does not support JWK validation. In this case, we recommend authenticating communication with your IdP using mutual TLS or another network layer security protocol.

-r, --return-url <return-url>

The URL of your server. This is typically the public name of your server, such as "http://example.tableau.com".

-sn, --custom-scope-name <string>

Optional.

Specifies a custom scope user-related value that you can use to query the IdP. See Requirements for Using OpenID Connect.

Options for openid map-claims

Use these options to change the default OIDC claims Tableau Server will use when communicating with your IdP. See Requirements for Using OpenID Connect.

-i, --id <string>

Optional. Default: sub

Change this value if your IdP does not use the sub claim to uniquely identify users in the ID token. The IdP claim that you specify should contain a single, unique string.

-un, --user-name <string>

Optional. Default: email
Change this value to the IdP claim that your organization will use to match user names as stored in Tableau Server.

`tsm authentication saml <commands>`

Configure Tableau Server to support single-sign on using the SAML 2.0 standard, enable or disable SAML for a site, map assertion attribute names between Tableau Server and the identity provider (IdP).

Available commands

- `tsm authentication saml configure [options] [global options]`
- `tsm authentication saml disable [options] [global options]`
- `tsm authentication saml enable [options] [global options]`
- `tsm authentication saml export-metadata [options] [global options]`
- `tsm authentication saml map-assertions [options]`

`tsm authentication saml configure`

Configure the SAML settings for the server. Specify the SAML certificate and metadata files, provide additional required information, set additional options.

If you are configuring SAML for the first time or have previously disabled it, you must run this command with `tsm authentication saml enable`. For more information, see Configure Server-Wide SAML.

Synopsis

`tsm authentication saml configure [options] [global options]`

Options

- `-e, --idp-entity-id <id>`
Required for initial SAML configuration; otherwise optional. IdP entity ID value.

Typically this is the same as the Tableau Server return URL (specified in the --idp-return-url parameter). The entity ID that you enter is used as a base for generating site-specific entity IDs. For example, if you enter the following:

http://tableau-server

A site configured for SAML might display the following entity ID:

http://tableau-server/samlservice/public/sp/metadata?alias=48957410-9396-430a-967c-75bdb6e002a0

To find a site’s entity ID, go to the site’s Settings page, and select the Authentication tab. When SAML is enabled, the entity ID is shown under the first step for configuring site-specific SAML, exporting metadata.

-r, --idp-return-url <idp-return-url>

Required for initial SAML configuration; otherwise optional. The SAML return URL configured in the IdP. This is typically the Tableau Server external URL; for example, https://tableau-server.

Notes

- http://localhost does not work for an external server.
- Adding a trailing slash to the URL (https://tableau-server/) is not supported.

-i, --idp-metadata <idp-metadata.xml>

Required for initial SAML configuration; otherwise optional. Provide the location and name of the XML metadata file you exported from the IdP’s settings.

For example, /var/opt/tableau/tableau_server/data/saml/<metadata-file.xml>

-cf, --cert-file <certificate.crt>
Tableau Server on Linux Administrator Guide

Required for initial SAML configuration; otherwise optional. The location and file name for the x509 certificate file for SAML. For requirements for the certificate file, see SAML Requirements.

For example, /var/opt/tableau/tableau_server/data/saml/<file.crt>

-kf, --key-file <certificate.key>

Required for initial SAML configuration; otherwise optional. Location and name of the key file that goes along with certificate.

For example, /var/opt/tableau/tableau_server/data/saml/<file.key>

-a, --max-auth-age <max-auth-age>

Optional. Default value is 7200 (2 hours).

The maximum number of seconds allowed between a user’s authentication and processing of the AuthNResponse message.

-d, --desktop-access <enable | disable>

Optional. Default value is enable.

Use SAML to sign in to the server from Tableau Desktop. If single sign-on from Tableau client applications does not work with your IdP, you can set this to disable.

-m, --mobile-access <enable | disable>

Optional. Default value is enable.

Allow using SAML to sign in from older versions of Tableau Mobile app. Devices running Tableau Mobile app version 19.225.1731 and higher ignore this option. To disable devices running Tableau Mobile app version 19.225.1731 and higher, disable SAML as a client login option on Tableau Server.

-so, --signout <enable | disable>
Optional. Enabled by default.

Enable or disable SAML sign out for Tableau Server.

-su, --signout-url <url>

Optional. Enter the URL to redirect to after users sign out of the server. By default this is the Tableau Server sign-in page. You can specify an absolute or a relative URL.

Example


tsm authentication saml enable and saml disable

Enable or disable server-wide SAML authentication. In this context, all sites and users that you enable for SAML go through a single identity provider.

Synopsis

tsm authentication saml enable [global options]

tsm authentication saml disable [global options]

tsm authentication saml export-metadata

Export the Tableau Server .xml metadata file that you will use to configure the SAML IdP.

Synopsis

tsm authentication saml export-metadata [options]
[global options]
Tableau Server on Linux Administrator Guide

Options

-f, --file [/path/to/file.xml]

Optional.

Specifies the location and file name in which the metadata will be written. If you don’t include this option, `export-metadata` saves the file to the current directory, and names it `samlmetadata.xml`.

-o, --overwrite

Optional.

Overwrites an existing file of the same name specified in -f, or of the default name if -f is not included. If a file specified in -f exists, and -o is not included, the command does not overwrite the existing file.

tsm authentication saml map-assertions

Maps attributes between the IdP and Tableau Server. Provide the name that the IdP uses for the attribute specified in each argument.

Synopsis

```
tsm authentication saml map-assertions --user-name <user-name>
[global options]
```

Options

-r, --user-name <user-name-attribute>

Optional. The attribute in which the IdP stores the user name. On Tableau Server this is the display name.

-e, --email <email-name-attribute>

Optional. The name of the attribute in which the IdP stores email addresses.
Optional. The attribute in which the IdP stores the domain name.

Optional. The attribute in which the IdP stores the domain name.

Example for saml map-assertions

tsm authentication saml map-assertions --email=Email --user-name=DisplayName

tsm authentication sitesaml enable and sitesaml disable

Set the server to allow or disallow SAML authentication at the site level. Enabling site-specific SAML gives you access to the Settings > Authentication tab in the Tableau Server web UI. The Authentication tab contains the site-specific SAML configuration settings.

Use the sitesaml enable command with saml configure if you haven't yet configured the server to allow site-specific SAML. For more information, see Configure Site-Specific SAML.

Synopsis

tsm authentication sitesaml enable [global options]

tsm authentication sitesaml disable [global options]

This command will only work on Tableau Server on Windows. If you attempt to enable SSPI on Tableau Server on Linux, an error will be returned.

Enable or disable automatic sign-in using Microsoft SSPI.

If you use Active Directory for authentication, you can optionally enable automatic logon, which uses Microsoft SSPI to automatically sign in your users based on their Windows
username and password. This creates an experience similar to single sign-on (SSO). Do not enable SSPI if you plan to configure Tableau Server for SAML, trusted authentication, or for a proxy server.

Synopsis

```
 tsm authentication sspi disable [global options]
```

```
 tsm authentication sspi enable [global options]
```

**tsm authentication trusted <commands>**

Configure trusted authentication (trusted tickets) for user authentication on Tableau Server.

Synopsis

```
 tsm authentication trusted configure [options] [global options]
```

Options

```
-th, --hosts <string>
```

Optional.

Specifies the trusted host names (or IPv4 addresses) of the web servers that will be hosting pages with Tableau content.

For multiple values, enter the names in a comma-separated list where each value is encapsulated in double-quotes.

For example:

```
 tsm authentication trusted configure -th "192.168.1.101", "192.168.1.102", "192.168.1.103"
```

or

```
 tsm authentication trusted configure -th "webserv1", "webserv2", "webserv3"
```
-t, --token-length <integer>

Optional.

Determines the number of characters in each trusted ticket. The default setting of 24 characters provides 144 bits of randomness. The value can be set to any integer between 9 and 255, inclusive.

Global options

-h, --help

Optional.

Show the command help.

-p, --password <password>

Required, along with -u or --username if no session is active.

Specify the password for the user specified in -u or --username.

If the password includes spaces or special characters, enclose it in quotes:

--password 'my password'

-s, --server <url_to_tsm>

Optional.

Use the specified address for Tableau Services Manager. The URL must start with https, include port 8850, and use the server name not the IP address, for example https://mytableauhost:8850. If no server is specified, https://localhost | dnsname>:8850 is assumed.

--trust-admin-controller-cert

Optional.
Use this flag to trust the self-signed certificate on the TSM controller. For more information about certificate trust and CLI connections, see Connecting TSM clients.

-u, --username <user>

Required if no session is active, along with -p or --password.

Specify a user account. If you do not include this option, the command is run using credentials you signed in with.

**tsm configuration**

You can use the `tsm configuration` commands to get, set, and update configuration values.

For specific configuration keys you can set, see `tsm configuration set Options`.

- `get`
- `set`

**tsm configuration get**

View the current server configuration and topology.

**Synopsis**

```bash
tsma configuration get --key <config.key> [global options]
```

**Option**

- `--key`

Required.

Get the current value of the specified configuration key.
tsm configuration set

Set or import server configuration or topology.

Quotes around the `<config.key>` and the `<config_value>` are optional unless there are spaces, in which case you must use quotes around the key or value.

**Note:** After setting a configuration key value you must apply the pending configuration changes using `tsm pending-changes apply`. Until you do, the new value will not be used by Tableau or show up in the results of a `tsm configuration get` command. You can view pending changes using `tsm pending-changes list`. For more information, see `tsm pending-changes`.

Synopsis

```
  tsm configuration set --key <config.key> --value <config_value>
  [global options]
```

Options

- `k,--key <config.key>`
  
  Required.

  Configuration key.

- `v,--value <config_value>`
  
  Required.

  Configuration value.

- `d`
  
  Optional.
Tableau Server on Linux Administrator Guide

Reset the configuration value to its default.

-\texttt{frc, \--force-keys}

Optional.

Force a key to be added to configuration even if it did not previously exist.

Global options

-\texttt{h, \--help}

Optional.

Show the command help.

-\texttt{p, \--password <password>}

Required, along with -\texttt{u or \--username} if no session is active.

Specify the password for the user specified in -\texttt{u or \--username}.

If the password includes spaces or special characters, enclose it in quotes:

-\texttt{--password 'my password'}

-\texttt{s, \--server <url_to_tsm>}

Optional.

Use the specified address for Tableau Services Manager. The URL must start with https, include port 8850, and use the server name not the IP address, for example https://mytableauhost:8850. If no server is specified, https://<localhost \mid dnsname>:8850 is assumed.

-\texttt{--trust-admin-controller-cert}

Optional.
Use this flag to trust the self-signed certificate on the TSM controller. For more information about certificate trust and CLI connections, see Connecting TSM clients.

-u, --username <user>

Required if no session is active, along with -p or --password.

Specify a user account. If you do not include this option, the command is run using credentials you signed in with.

tsm configuration set Options

You can use the following configuration options with the `tsm configuration set` command.

Essential syntax is:

```
tsm configuration set -k <config.key> -v <config_value>
```

After setting a configuration key value you must apply the pending configuration changes using `tsm pending-changes apply`. Until you do, the new value will not be used by Tableau or show up in the results of a `tsm configuration get` command. You can view pending changes using `tsm pending-changes list`. For more information, see `tsm pending-changes`.

To reset a configuration key back to its default value, use the `-d` option:

```
tsm configuration set -k <config.key> -d
```

**Note:** Configuration keys are case-sensitive.

Options

`adminviews.disabled`

Default value: `false`
Disables access to the Tableau Administrative views. By default, access to views is enabled (this option is set to "false").

**api.server.enabled**

*Default value: true*

Allows access to the Tableau Server REST API. By default, this functionality is enabled.

**auditing.enabled**

*Default value: true*

Allows access to the PostgreSQL (Tableau Server's own database) historical auditing tables.

**backgrounder.enable_sort_jobs_by_job_rank**

*Default value: true*

Enables Backgrounder to use the calculated job rank to determine when to queue a job. For optimal performance for managing the job queue, Tableau recommends you leave this configuration set to true.

**backgrounder.enable_task_run_time_and_job_rank**

*Default value: true*

Allows a task's last run time to be stored in the Workgroup database. This value is then used as a parameter in calculating a job's job rank. For optimal performance for managing the job queue, Tableau recommends you leave this configuration set to true.

**backgrounder.externalquerycachewarmup.enabled**

*Default value: true*

Controls the caching of workbook query results after scheduled extract refresh tasks.
backgrounder.externalquerycachewarmup.view_threshold

Default value: 2.0

The threshold for caching workbook query results after scheduled extract refresh tasks. The threshold is equal to the number of views that a workbook has received in the past seven days divided by the number of refreshes scheduled in the next seven days.

The following two backgrounder command options determine how long a flow task can run before the flow background task is canceled. These two commands together determine the total timeout value for flow tasks.

backgrounder.extra_timeout_in_seconds

Default value: 1800 or 30 minutes

The number of seconds beyond the setting in backgrounder.querylimit before a background task is canceled. This setting makes sure that tasks do not hold up subsequent jobs if they are stalled. The setting applies to processes listed in backgrounder.timeout_tasks.

backgrounder.default_timeout.run_flow

Default value: 14400 seconds or 4 hours

The number of seconds for a flow run task is canceled.

backgrounder.failure_threshold_for_run_prevention

Default value: 5

The number of consecutive failures of a subscription, extract, or flow run job before that job is suspended. Suspending continuously failing jobs helps preserve background resources for other jobs. To disable suspension of failing background tasks, set this to -1.
backgrounder.querylimit

Default value: 7200

Longest allowable time, in seconds, for completing a single extract refresh task or subscription task. 7200 seconds = 2 hours.

Note: If a background task reaches this time limit, it may continue to run for an additional several minutes while being canceled.

backgrounder.notifications_enabled

Default value: true

Controls whether extract refresh and flow run alerts are enabled for all sites on the server. By default alerts are enabled. To disable the alerts for all sites on a server, set this to false.

Extract alerts can be enabled or disabled on a site basis by site administrators in site settings, or at the user level in user settings.

backgrounder.sort_jobs_by_type_schedule_boundary_heuristics_milliSeconds

Default value: 60000

Controls the time window that identifies backgrounder jobs which are determined to have the same scheduled start time.

The backgrounder process orders work that is scheduled at the same time to be executed by job type, running the fastest category of jobs first: Subscriptions, then Incremental Extracts, then Full Extracts.

Jobs are batched to determine which jobs are scheduled at the “same time”. A value 60,000 milliseconds (the default) indicates jobs for schedules starting within a 1 minute window should be classified in the same batch and so are ordered by type within that batch.

backgrounder.subscription_failure_threshold_for_run_prevention
Determines the number of consecutive subscription failures that must occur before alerting for a condition is suspended. When set to the default of 5, alerting is suspended after 5 consecutive subscription failures. This threshold is server-wide, so applies to all subscriptions defined on the server.

`backgrounder.subscription_image_caching`

**Default value:** true

Controls whether backgrounder will cache images that are generated for subscriptions. Cached images do not have to be regenerated each time so caching improves subscription performance. By default image caching is enabled. To disable image caching for all sites on a server, set this to false.

`backgrounder.timeout_tasks`

**Default value:** `refresh_extracts, increment_extracts, subscription_notify, single_subscription_notify, check_data_alert, run_flow, encrypt_extracts, decrypt_extracts, rekey_extracts, extract_encryption_maintenance`

The list of tasks that can be canceled if they run longer than the combined values in `backgrounder.query_limit` and `backgrounder.extra_timeout_in_seconds`. The list of tasks is delimited with commas. The default list represents all the possible values for this setting.

`clustercontroller.zk_session_timeout_ms`

**Default value:** 300000
Tableau Server on Linux Administrator Guide

The length of time, in milliseconds, that Cluster Controller will wait for the Coordination Service (ZooKeeper), before determining that failover is required.

dataAlerts.checkIntervalInMinutes

Default value: 60

The frequency, in minutes, at which Tableau Server checks to determine if data-alert conditions are true.

(The server also checks whenever extracts related to data alerts are refreshed.)

dataAlerts.retryFailedAlertsAfterCheckInterval

Default value: true

Determines how often Tableau Server rechecks failing data alerts. When set to true, the server rechecks failing alerts at the frequency defined by dataAlerts.checkIntervalInMinutes. When set to false, the server rechecks failing alerts every five minutes, more quickly notifying alert recipients if data conditions have changed, but reducing server performance.

(The server also checks whenever extracts related to data alerts are refreshed.)

DataServerRefreshMetadataPerSession

Default value: false

Determines whether Tableau Server will make additional queries to get updated schema data for a published data source when there have been changes in the underlying schema structure. This is disabled by default for performance reasons, and there is a delay in the display of schema changes. If you want changes in the schema of a live published data source to be reflected quickly, or if you see errors (for example, "An error occurred while communicating with the data source: Invalid column name. Statement could not be prepared.") set this to true. When set to true, Tableau Server makes additional queries to update the schema.
**elasticserver.vmopts**

**Default value:** `-Xmx256m -Xms256m`

Controls the Elastic Server heap size. Tuning these values may help to improve performance. The heap size should usually be less than half of the full machine memory. As a general rule, set initial heap size (-Xms) equal to the maximum heap size (-Xmx) to minimize garbage collections. The default size for these values is measured in bytes. Append the letter 'k' or 'K' to the value to indicate kilobytes, 'm' or 'M' to indicate megabytes, and 'g' or 'G' to indicate gigabytes.

**excel.shadow_copy_all_remote.enabled**

**Default value:** `false`

Controls whether Tableau Server creates a "shadow copy" of a shared Excel spreadsheet (.xlsx or .xlsm) that is being used as a live data source. When enabled, this option prevents Excel users from seeing a "Sharing Violation Error" and a message that the file is "currently in use." This option can have a performance impact with large Excel files. If Excel users do not need to edit the shared file, you do not need to enable this option.

**Note:** Tableau Server always attempts to create a shadow copy of a .xls file. This option does not change that behavior.

This option was added beginning with Tableau Server version: 2019.1.5.

**features.DesktopReporting**

**Default value:** `false`

Controls whether Desktop License Reporting is enabled on the server. When set to `false` (the default), no Administrative Views related to desktop licenses are available. Set this to `true` to enable license reporting and make license usage and expiration Administrative Views visible on the Server Status page.
features.PasswordReset

Default value: false

Applies only to servers that use local authentication. Set to true to let users reset their passwords with a "Forgot password" option on the sign-in page.

features.SelfServiceSchedules

Default value: false

Set to true to enable subscription custom schedules. With this enabled, custom schedules must then be enabled at the site level. For more information, see Enable Custom Schedules for Subscriptions.

gateway.http.cachecontrol.updated

Default value: false

The Cache-Control HTTP header specifies whether the client browser should cache content sent from Tableau Server. To disable caching of Tableau Server data on the client, set this option to true.

gateway.http.hsts

Default value: false

The HTTP Strict Transport Security (HSTS) header forces browsers to use HTTPS on the domain where it is enabled.

gateway.http.hsts_options

Default value: "max-age=31536000"

By default, HSTS policy is set for one year (31536000 seconds). This time period specifies the amount of time in which the browser will access the server over HTTPS.
**gateway.http.request_size_limit**

Default value: 16380

The maximum size (bytes) of header content that is allowed to pass through the Apache gateway on HTTP requests. Headers that exceed the value set on this option will result in browser errors, such as HTTP Error 413 (Request Entity Too Large) or authentication failures.

A low value for `gateway.http.request_size_limit` can result in authentication errors. Single sign-on solutions that integrate with Active Directory (SAML and Kerberos) often require large authentication tokens in HTTP headers. Be sure to test HTTP authentication scenarios before deploying into production.

We recommend setting `tomcat.http.maxrequestsize` option to the same value that you set for this option.

**gateway.http.x_content_type_nosniff**

Default value: `true`

The X-Content-Type-Options response HTTP header specifies that the MIME type in the Content-Type header should not be changed by the browser. In some cases, where MIME type is not specified, a browser may attempt to determine the MIME type by evaluating the characteristics of the payload. The browser will then display the content accordingly. This process is referred to as "sniffing." Misinterpreting the MIME type can lead to security vulnerabilities. The X-Content-Type-Options HTTP header is set to 'nosniff' by default with this option.

**gateway.http.x_xss_protection**

Default value: `true`

The HTTP X-XSS-Protection response header is sent to the browser to enable cross-site scripting (XSS) protection. The X-XSS-Protection response header overrides con-
Tableau Server on Linux Administrator Guide

Figurations in cases where users have disabled XXS protection in the browser. The X-XSS-Protection response header is enabled by default with this option.

gateway.public.host

Default value: <hostname>

The name (URL) of the server, used for external access to Tableau Server. If Tableau Server is configured to work with a proxy server or external load balancer, it is the name entered in a browser address bar to reach Tableau Server. For example, if Tableau Server is reached by entering tableau.example.com, the name for gateway.public.host is tableau.example.com.

gateway.public.port

Default value: 80 (443 if SSL)

Applies to proxy server environments only. The external port the proxy server listens on.

gateway.slow_post_protection.enabled

Default value: false

Enabling this can provide some help in protecting against slow POST (Denial-of-Service) attacks by timing out POST requests that transfer data at extremely slow rates. **Note:** This will not eliminate the threat of such attacks, and could have the unintended impact of terminating slow connections.

gateway.slow_post_protection.request_read_timeout

Default value: header=15-20,MinRate=500 body=10,MinRate=500

When enabled by the preceding option, gateway.slow_post_protection.enabled, this option sets the Apache httpd ReadRequestTimeout. The httpd directive is documented at Apache Module mod_reqtimeout. The primary use of
this option is as a defense the Slowloris attack. See the Wikipedia entry, Slowloris (computer security).

gateway.timeout

Default value: 1800

Longest amount of time, in seconds, that the gateway will wait for certain events before failing a request (1800 seconds = 30 minutes).

gateway.trusted

Default value: IP address of proxy server machine

Applies to proxy server environments only. The IP address(es) or host name(s) of the proxy server.

gateway.trusted_hosts

Default value: Alternate names of proxy server

Applies to proxy server environments only. Any alternate host name(s) for the proxy server.

hyper.file_partition_size_limit

Default value: 0

When set to 0, the size is set to unlimited and will use all the disk space that is available.

This option is used to set the disk space limit for a query that spools to disk. If your disk space usage by the spool.<id>.tmp file is higher than where you need it to be for your environment, it means that queries are spooling and taking up disk space. Use this option to limit the amount of disk space that any one query can use. The spool.<id>.tmp file can be found in the temp folder of the user account running
Tableau Server on Linux Administrator Guide

Tableau Server. You can specify this value in K(KB), M(MB), G(GB), or T(TB) units. For example, you can specify the size limit as 100G when you want to limit the disk space usage to 100 GB.

For more information about spooling see the Memory and CPU Usage section in Tableau Server Data Engine.

hyper.global_file_partition_size_limit

Default value: 0

When set to 0, the size is set to unlimited and will use all the disk space that is available.

This option is used to set the disk space limit for all queries that spool to disk. If your disk space usage by the spool.<id>.tmp file is higher than where you need it to be for your environment, it means that queries are spooling and taking up disk space. The spool.<id>.tmp file can be found in the temp folder of the user account running Tableau Server. Use this option to limit the amount of disk space in sum total that all queries use when spooling to disk. You can specify this value in K(KB), M(MB), G(GB), or T(TB) units. For example, you can specify the size limit as 100G when you want to limit the disk space usage to 100 GB. Tableau recommends that you start with this configuration when fine tuning your spooling limits.

For more information about spooling see the Memory and CPU Usage section in Tableau Server Data Engine.

hyper.log_queries

Default value: true

When set to true, query information is logged.

By default query information is logged. If however you find that the log files are too large for the amount of disk space available, you can set it to false to disable logging query information. Tableau recommends leaving this configuration set to true.
hyper.log_query_cpu

Default value: false
Use this setting to log how much time each query takes and the CPU usage.

hyper.log_timing

Default value: false
This setting is useful to find out more information about the queries, like compilation and parsing times. By default this setting is disabled. You can turn this by setting the value to true to collect more details about your queries. Note, however that this will increase the size of your data engine log files (\logs\hyper).

hyper.log_troublesome_query_plans

Default value: true
When set to true, logs query plans of query that are identified as problematic. Queries that are either canceled, running slower than 10 seconds, or if the queries are spooling to disk fall into this category. The information in the logs can be useful to troubleshoot problematic queries. You can change the setting to false if you are concerned about the size of the logs.

hyper.hard_concurrent_query_thread_limit

Default value: 100%
Use this option to set the maximum number of threads Data Engine should use for running queries. Since this is a hard limit, use this to when you want to set a hard limit on the CPU usage. This setting will make sure that Data Engine does not use more CPU than this set limit.
It is important to consider that this setting controls the number of concurrent queries that can be executed. So, if you decrease this setting, the chance of queries needing
to wait in a queue and wait for currently running queries to complete increases, which may affect workbook load times.

hyper.soft_concurrent_query_thread_limit

Default value: 100%

Use this option to specify the number of threads that a single query can be parallelized across, which is the set limit minus the number of active threads already in use. To illustrate this, here is a simplified example:

Let’s say you set this value to 10 threads, this means queries can be parallelized up to 10 threads. If only 2 queries are running, the remaining 8 threads are used to parallelize the 2 queries.

This soft limit makes sure that the Data Engine does not utilize CPU over that limit, unless there are queries waiting to be queued even when at the limit. This is useful when you have queries that are CPU intensive, you can parallelize these across multiple threads so they complete faster.

The hyper. hard_concurrent_query_thread_limit, and hyper.soft_concurrent_query_thread_limit options work together to give you some options to manage your CPU usage while maximizing available CPU resources to complete queries faster. If you don't want the Data Engine to use all the available CPU on the machine, change it to less than 100% to a percentage that is optimal for your environment. The soft limit is a way for you to limit CPU usage but allow it to go beyond the soft limit up to the hard limit if necessary.

Note: The hyper.hard_concurrent_query_thread_limit and hyper.soft_concurrent_query_thread_limit options replace hyper.num_job_worker_threads and hyper.num_task_worker_threads options available in Tableau Server versions 2018.3 and earlier, and are deprecated in the current version. For information on the hyper.num_job_
worker_threads and hyper.num_task_worker_threads, see `tsm configuration set` Options.

```

hyper.use_spoolingFallback

Default value: true

When set to true, it allows spooling to disk when querying extracts exceeds set RAM usage (80% of installed RAM).

Tableau recommends that you use the default setting. You can turn this off by setting the value to false if you are concerned about disk usage. If you turn this setting off, queries that use more than 80% of installed RAM will be canceled.

For more information about spooling see the Memory and CPU Usage section in Tableau Server Data Engine.

install.firewall.allowedprograms.manage

Default value: true

Controls whether Tableau Server can add firewall rules. When set to true (the default), Tableau Server will add new firewall rules to allow its processes to make connections through Windows Firewall. Change this to false if you want to manage all firewall rules yourself and do not want Tableau Server to add new rules.

java.heap.size

Default value: 128m

Size of heap for Tomcat (repository and solr). This generally does not need to change except on advice from Tableau.

maestro.input.allowed_paths

Default value: ""

1090 Version: 2019.1 Tableau Software
By default, access to any directory will be denied, and only publishing to Tableau Server with content that is included in the tflx file is allowed.

A list of allowed network directories for flow input connections. You must enable Tableau Prep Conductor to run flows on your Tableau Server. For more information, see Tableau Prep Conductor.

The following rules apply and must be considered when configuring this setting:

- Paths should be accessible by Tableau Server. These paths are verified during server startup and at flow run time.

- Network directory paths have to be absolute and cannot contain wildcards or other path traversing symbols. For example `\myhost\myShare\*` or `\my-host\myShare*` are invalid paths and would result in all the paths as disallowed. The correct way to safelist any folder under `myShare` would be `\myhost\myShare` or `\myhost\\myShare`.

  **Note:** The `\myhost\myShare` configuration will not allow `\my-host\myShare1`. In order to safe list both of these folders one would have safe list them as `\myhost\myShare`; `\myhost\myShare1`.

- The value can be either `*` meaning that any path, including local (with the exception of some system paths configured using “native_api.internal_disallowed_paths”), or a list of paths, delimited by “;”.

  **Note:** If a path is both on the flows allowed list and internal_disallowed list, internal_disallowed takes precedence.

**Important:**
This command overwrites existing information and replaces it with the new information you provided. If you want to add a new location to an existing list, you must provide a list of all the locations, existing and the new one you want to add. Use the following commands to see the
current list of input and output locations:

```bash
tsm configuration get -k maestro.input.allowed_paths
tsm configuration get -k maestro.output.allowed_paths
```

For more information and details about configuring allowed directories for flow input and output connections, see [Safe list Input and Output Locations](#).

`maestro.output.allowed_paths`

Default value: `""

By default, access to any directories will be denied.

A list of allowed network directories for flow output connections. You must enable Tableau Prep Conductor to run flows on your Tableau Server. For more information, see Tableau Prep Conductor.

The following rules apply and must be considered when configuring this setting:

- Paths should be accessible by Tableau Server. These paths are verified during server startup and at flow run time.

- Network directory paths have to be absolute and cannot contain wildcards or other path traversing symbols. For example `\myhost\myShare\*` or `\myhost\myShare*` are invalid paths and would result in all the paths as disallowed. The correct way to safelist any folder under `myShare` would be `\myhost\myShare` or `\myhost\myShare/`.

> **Note:** The `\myhost\myShare` configuration will not allow `\myhost\myShare1`. In order to safe list both of these folders one would have safe list them as `\myhost\myShare; \myhost\myShare1`.

- The value can be either `*` meaning that any path, including local (with the
exception of some system paths configured using "native_api.internal_disallowed_paths"), or a list of paths, delimited by ";".

**Note:** If a path is both on the flows allowed list and internal_disallowed list, internal_disallowed takes precedence.

For more information and details about configuring allowed directories for flow input and output connections, see [Safe list Input and Output Locations](#).

**monitoring.dataengine.connection_timeout**

Default value: 30000

The length of time, in milliseconds, that Cluster Controller will wait for the data engine, before determining that a connection timeout occurred. The default is 30,000 milliseconds (30 seconds).

**native_api.connection.limit.<connection class>**

Set parallel query limit for the specified data source (connection class). This overrides the global limit for the data source.

**native_api.connection.globallimit**

Default value: 16

Global limit for parallel queries. Default is 16 except for Amazon Redshift which has a default of 8.

**native_api.ProtocolTransitionLegacyFormat**

Default value: `false`

Use the legacy name format for constrained delegation.

The name format was changed in version 10.1 to allow cross-domain protocol transition (S4U). If this causes problems with existing configurations and you don't need
cross-domain protocol transition, configure Tableau Server to use the old behavior by setting this to `true`.

`native_api.unc_mountpoints`

Default value: `none`

Specifies UNC and FQDN path for shared Windows directories that are accessed by Tableau Server on Linux. Each path must also be referenced in a corresponding `auto.cifs` file. Separate each path by a semicolon, for example:

```
'/files-rv01/development;/mnt/filesrv01/development;/filesrv01.example.lan/development;/mnt/filesrv01/development'
```

Subsequent updates to the `native_api.unc_mountpoints` value will overwrite the existing value. Therefore, each time you add a Windows share, you must include all shares in the updated value.

For more information, see the Community wiki topic, *Connecting to a Windows Shared Directory*.

`pgsql.port`

Default value: `8060`

Port that PostgreSQL listens on.

`pgsql.preferred_host`

Specifies the computer name of the node with the preferred repository installed. This value is used if the `--preferred` or `-r` option is specified with the `tsm topology fail-over-repository` command.

Example:

```
tsm configuration set -k pgsql.preferred_host -v "<host_name>"
```
Note: The host_name is case-sensitive and must match the node name shown in the output of tsm status -v.

pgsql.verify_restore.port

Default value: 8061

Port used to verify the integrity of the PostgreSQL database. See tsm maintenance backup for more information.

recommendations.enabled

Default value: true

Suggests server content, such as data sources and tables, to Tableau Desktop users. Content suggestions are based on popularity of the content or on content frequently used by other users who are similar to the current user.

refresh_token.absolute_expiry_in_seconds

Default value: 31536000

Specifies the number of seconds for absolute expiry of OAuth refresh and access tokens. The OAuth tokens are used by clients for authentication to Tableau Server after initial sign-in. To remove limits set to -1. To disable OAuth tokens, see Disable Automatic Client Authentication.

refresh_token.idle_expiry_in_seconds

Default value: 1209600

Specifies the number of seconds when idle OAuth tokens will expire. The OAuth tokens are used by clients for authentication to Tableau Server after initial sign-in. To remove limits set to -1.
refresh_token.max_count_per_user

Default value: 24

Specifies the maximum number of refresh tokens that can be issued for each user. If user sessions are expiring more quickly than you expect, either increase this value or set it to -1 to entirely remove token limits.

rsync.timeout

Default value: 600

Longest allowable time, in seconds, for completing file synchronization (600 seconds = 10 minutes). File synchronization occurs as part of configuring high availability, or moving the data engine and repository processes.

schedules.display_schedule_description_as_name

Default value: false

Controls whether a schedule name displays when creating a subscription or extract refresh (the default), or the "schedule frequency description" name describing the time and frequency of the schedule displays. To configure Tableau Server to display timezone-sensitive names for schedules, set this value to true.

When true, the "schedule frequency description" is also displayed after the schedule name on the schedule list page.

schedules.display_schedules_in_client_timezone

Default value: true

Shows the "schedule frequency description" in the timezone of the user when true (uses the client browser timezone to calculate the "schedule frequency description").

service.jmx_enabled
Tableau Server on Linux Administrator Guide

Default value: false

Setting to true enables JMX ports for optional monitoring and troubleshooting.

service.max_procs

Default value: <number>

Maximum number of server processes.

service.port_remapping.enabled

Default value: true

Determines whether or not Tableau Server will attempt to dynamically remap ports when the default or configured ports are unavailable. Setting to false disables dynamic port remapping.

session.ipsticky

Default value: false

Makes client sessions valid only for the IP address that was used to sign in. If a request is made from an IP address different from that associated with the session token, the session token is considered invalid.

In certain circumstances—for example, when Tableau Server is being accessed by computers with known and static IP addresses—this setting can yield improved security.

Note: Consider carefully whether this setting will help your server security. This setting requires that the client have a unique IP address and an IP address that stays the same for the duration of the session. For example, different users who are behind a proxy might look like they have the same IP address (namely, the IP address of the proxy); in that case, one user might have access to another user’s
session. In other circumstances, users might have a dynamic IP address, and their address might change during the course of the session. If so, the user has to sign in again.

**sheet_image.enabled**

Default value: true

Controls whether you can get images for views with the REST API. For more information, see REST API Reference.

**solr.rebuild_index_timeout**

Default value: 7200

When Tableau Server is upgraded or when a .tsbak file is restored, the background task rebuilds the search index. This setting, in seconds, controls the timeout setting for that task (7200 seconds = 120 minutes).

**subscriptions.enabled**

Default value: false

Controls whether subscriptions are configurable system-wide. See Set Up a Site for Subscriptions.

**subscriptions.timeout**

Default value: 1800

Longest allowable time, in seconds, for a single view in a workbook subscription task to be rendered before the task times out. This value applies separately to each view in the workbook, so the total length of time to render all the views in a workbook (the full subscription task) may exceed this timeout value. 1800 seconds = 30 minutes.
tomcat.http.maxrequestsize

Default value: 16380

The maximum size (bytes) of header content that is allowed to pass through the Apache gateway on HTTP requests. Headers that exceed the value set on this option will result in browser errors, such as HTTP Error 413 (Request Entity Too Large) or authentication failures.

A low value for tomcat.http.maxrequestsize may result in authentication errors. Single sign-on solutions that integrate with Active Directory (SAML and Kerberos) often require large authentication tokens in HTTP headers. Be sure to test HTTP authentication scenarios before deploying into production.

We recommend setting gateway.http.request_size_limit option to the same value that you set for this option.

tomcat.https.port

Default value: 8443

SSL port for Tomcat (unused).

tomcat.server.port

Default value: 8085

Port that tomcat listens on for shutdown messages.

vizportal.adsync.update_system_user

Default value: false

Specifies whether email addresses and display names of users are changed (even when changed in Active Directory) when an Active Directory group is synchronized in Tableau Server. To ensure that user email addresses and display names are updated
during synchronization, set `vizportal.adsync.update_system_user` to `true`, and then restart the server.

**vizportal.commenting.delete_enabled**

**Default value:** `true`

When set to `true`, lets users delete comments on views. You can delete a comment if you created it, are the content owner, a project leader with an appropriate site role, or are an administrator. To learn which site roles are required for full project leader access, see Project-level administration.

**vizportal.csv_user_mgmt.index_site_users**

**Default value:** `true`

Specifies whether indexing of site users is done user by user when importing or deleting users with a CSV file. When set to `true` (the default) indexing is done as each user is added or deleted. To delay the indexing of the site users until after the entire CSV file has been processed, set this to `false`.

**vizportal.log.level**

**Default value:** `info`

The logging level for vizportal Java components. Logs are written to `/var/opt/tableau/tableau_server/data/tabsvc/logs/vizportal/*.log`. Set to `debug` for more information. Using the debug setting can significantly impact performance, so you should only use this setting when directed to do so by Tableau Support.

**vizportal.openid.client_authentication**

Specifies custom client authentication method for OpenID Connect.
To configure Tableau Server to use the IdPs that require the `client_secret_post`, set this value to `client_secret_post`.

An example would be when connecting to the Salesforce IDP, which requires this.

```
vizportal.rest_api.cors.allow_origin
```

Specifies the origins (sites) that are allowed access to the REST API endpoints on Tableau Server when `vizportal.rest_api.cors.enabled` is set to `true`. You can specify more than one origin by separating each entry with a comma (,).

```
tsm configuration set vizportal.rest_api.cors.allow_origin
```

If `vizportal.rest_api.cors.enabled` is `false`, the origins listed by this option are ignored. For more information, see Enabling CORS on Tableau Server.

**Note:** You can use an asterisk (*) as a wild card to match all sites. This is not recommended as it allows access from any origin that has access to the server and can present a security risk. Do not use an asterisk (*) unless you fully understand the implications and risks for your site.

```
vizportal.rest_api.cors.enabled
```

Default value: `false`

Controls whether Tableau Server allows Cross Origin Resource Sharing (CORS). When set to `true`, the server allows web browsers to access the Tableau REST API endpoints. You can use this option and the REST API to create custom portals. By default, this functionality is not enabled. To specify which origins (sites) have access, use the `vizportal.rest_api.cors.allow_origin` option. Only the origins specified with this option are allowed to make requests to the Tableau Server REST API. For more information, see Enabling CORS on Tableau Server.

```
vizportal.rest_api.view_image.max_age
```
The amount of time, in minutes, to cache images that are generated by the Query View Image method of the REST API. For more information, see the REST API Reference in the REST API help.

vizqlserver.allow_insecure_scripts

Default value: false

Allows a workbook to be published to the server from Tableau Desktop, and to be opened from the server, even if the workbook contains SQL or R expressions that are potentially unsafe (for example, a SQL expression that could potentially allow SQL injection). When this setting is false (the default), publishing a workbook or opening it from the server results in an error message, and the workbook is blocked. Before you set this value to true review the Knowledge Base article, Blocking or Allowing Insecure Scripts in Tableau Server.

vizqlserver.browser.render

Default value: true

Views under the threshold set by vizqlserver.browser.render_threshold or vizqlserver.browser.render_threshold_mobile are rendered by the client web browser instead of by the server. See About Client-Side Rendering for details.

vizqlserver.browser.render_threshold

Default value: 100

The default value represents a high level of complexity for a view displayed on a PC. Complexity factors include number of marks, headers, reference lines, and annotations. Views that exceed this level of complexity are rendered by the server instead of in the PC's web browser.

vizqlserver.browser.render_threshold_mobile
The default value represents a high level of complexity for a view displayed on a tablet. Complexity factors include number of marks, headers, reference lines, and annotations. Views that exceed this level of complexity are rendered by the server instead of in the tablet's web browser.

```
vizqlserver.clear_session_on_unload
```

**Default value:** `false`

Determines whether or not VizQL sessions are kept in memory when a user navigates away from a view or closes their browser. The default value (false) keeps sessions in memory. To close VizQL sessions on leaving a view or closing a browser, set this to true.

```
vizqlserver.geosearch_cache_size
```

**Default value:** `5`

Sets the maximum number of different geographic search locale/language data sets that can be loaded into server memory at the same time. When the server receives a geographic search request for locale/language data set that is not in memory, it will load the set into memory. If loading the data set will exceed the specified limit, the least recently used locale/language data set is cleared from memory so the requested one can be loaded. The minimum value is 1. Each cache takes approximately 60 MB in memory (so if you set this to 10, the memory usage would be 600 MB (60 * 10)).

```
vizqlserver.initialsql.disabled
```

**Default value:** `false`

Specify whether to ignore initial SQL statements for all data sources. Set this to true to ignore initial SQL:
tsm configuration set -k vizqlserver.initialsql.disabled -v true

vizqlserver.log.level

Default value: info

The logging level for vizportal Java components. Logs are written to /var/opt/tableau/tableau_server/data/tabsvc/logs/vizportal/*.log.

Set to debug for more information. Using the debug setting can significantly impact performance, so you should only use it when directed to do so by Tableau Support.

vizqlserver.NumberOfWorkbookChangesBetweenAutoSaves

Default value: 5

Auto recover configuration for web authoring. Specifies the number of changes that a user must make to trigger auto save. Take care when changing this value. Auto recover functionality may impact the performance of web authoring and other viz-related operations on Tableau Server. We recommend tuning this value by making incremental adjustments over time.

vizqlserver.port

Default value: 9100

Base port for the VizQL servers.

vizqlserver.protect_sessions

Default value: true

When set to true, prevents VizQL sessions from being reused after the original user signs out.

vizqlserver.querylimit
Tableau Server on Linux Administrator Guide

Default value: 1800

Longest allowable time for updating a view, in seconds.

vizqlserver.RecoveryAttemptLimitPerSession

Default value: 3

Auto recover configuration for web authoring. The maximum number of attempts to recover the same session. Take care when changing this value. Auto recover functionality may impact the performance of web authoring and other viz-related operations on Tableau Server. We recommend tuning this value by making incremental adjustments over time.

vizqlserver.session.expiry.minimum

Default value: 5

Number of minutes of idle time after which a VizQL session is eligible to be discarded if the VizQL process starts to run out of memory.

vizqlserver.session.expiry.timeout

Default value: 30

Number of minutes of idle time after which a VizQL session is discarded.

vizqlserver.showdownload

Default value: true

Controls the display of the Tableau Workbook option of the Download menu in views. When set to false, the Tableau Workbook option is unavailable.

vizqlserver.showshare

Default value: true
Controls the display of Share options in views. To hide these options, set to false.

**Note:** Users can override the server default by setting the "showShareOptions" JavaScript or URL parameter.

**vizqlserver.url_scheme_whitelist**

Specifies one or more URL schemes to whitelist when using URL actions on views and dashboards. The schemes `http, https, gopher, mailto, news, sms, tel, tsc, and tsl` are whitelisted by default. This command can contain multiple comma and space-separated values, as in this example:

```bash
tsm configuration set -k vizqlserver.url_scheme_whitelist -v scheme1, scheme2
```

The values you specify overwrite previous settings. Therefore, you must include the full list of schemes in the `set` command. (You cannot amend the list of schemes by running the `set` command repeatedly.)

**vizqlserver.WorkbookTooLargeToCheckpointSizeKiB**

Default value: 1024

Auto recover configuration for web authoring. Size limit (KB) for a workbook that will auto save. Workbooks larger than this value will not be auto-saved. Take care when changing this value. Auto recover functionality may impact the performance of web authoring and other viz-related operations on Tableau Server. We recommend tuning this value by making incremental adjustments over time.

**webdataconnector.refresh.enabled**

Deprecated. Use `tsm data-access web-data-connectors allow` instead.
Tableau Server on Linux Administrator Guide

Determines whether extract refreshes for web data connectors (WDCs) are enabled in Tableau Server. To disable refresh for all WDCs, set the value for this key to false, as shown below:

```sh
tsm configuration set --key webdataconnector.refresh.enabled --value false
```

To learn more, see Web Data Connectors in Tableau Server.

**webdataconnector.whitelist.fixed**

Deprecated. Use `tsm data-access web-data-connectors add` instead.

Specifies one or more web data connectors (WDCs) that can be used by to access data connections that are accessible over HTTP or HTTPS. This command is formatted as JSON data on a single line, with all double-quotes (") escaped using a backslash (\).

For example to add a San Francisco Film Locations WDC to the safe list:

```sh
tsm configuration set --key webdataconnector.whitelist.fixed --value "'{"https://tableau.data.world:443": {"properties": { "secondary_whitelist": [{"(https://data.world/)(.*)"] } }}}"'
```

To learn more, see Web Data Connectors in Tableau Server.

**webdataconnector.enabled**

Deprecated. Use `tsm data-access web-data-connectors allow` instead.

Default value: true

When set to true, you can use `tsm` commands to manage web data connectors on the server.

**webdataconnector.whitelist.mode**

Default value: mixed
Determines how Tableau Server can run web data connectors. Supported modes are:

- **fixed.** Users can run connectors that are on a safe list (whitelist) of URLs.
- **insecure.** Users can run any connector.

**Important:** Use the `insecure` option *only* for development and testing. Because connectors run custom code, running connectors that have not been vetted can pose a security threat.

---

**wgserver.audit_history_expiration_days**

Default value: 183

Specifies the number of days after which historical events records are removed from the PostgreSQL database (the Tableau Server database).

**wgserver.change_owner.enabled**

Default value: true

Controls whether the ownership of a workbook, data source or project can be changed. Other options include false and adminonly.

**wgserver.clickjack_defense.enabled**

Default value: true

When set to `true`, helps prevent a malicious person from "clickjacking" a Tableau Server user. In a clickjack attack, the target page is displayed transparently over a second page, and the attacker gets the user to click or enter information in the target page while the user thinks he or she is interacting with the second page.

For more information, see Clickjack Protection.
wgserver.domain.ldap.domain_custom_ports

Default value: null

Allows you to map child domains and their LDAP ports. Domain and port are separated by a colon (:) and each domain:port pair is separated by a comma (,) using this format: FQDN1:port,FQDN2:port


wgserver.extended_trusted_ip_checking

Default value: false

Enforces IP client matching for trusted ticket requests.

wgserver.restrict_options_method

Default value: true

Controls whether Tableau Server accepts HTTP OPTIONS requests. If this option is set to true, the server returns HTTP 405 (Method Not Allowed) for HTTP OPTIONS requests.

wgserver.saml.idpattribute.username

Specifies the name of the attribute in which your SAML IdP stores user names. By default, this is set to username. If the attribute name that your IdP uses contains spaces, enclose it in quotation marks. For more information, see Configure Server-Wide SAML or Configure Site-Specific SAML.

wgserver.saml.iframed_idp.enabled

Default value: false
Default of false means that when users select the sign-in button on an embedded view, the IdP’s sign-in form opens in a pop-up window.

When you set it to true, and a server SAML user who is already signed in navigates to a web page with an embedded view, the user will not need to sign in to see the view.

You can set this to true only if the IdP supports signing in within an iframe. The iframe option is less secure than using a pop-up, so not all IdPs support it. If the IdP sign-in page implements clickjack protection, as most do, the sign-in page cannot display in an iframe, and the user cannot sign in.

If your IdP does support signing in via an iframe, you might need to enable it explicitly. However, even if you can use this option, it disables Tableau Server clickjack protection for SAML, so it still presents a security risk.

**wgserver.saml.maxassertiontime**

Default value: 3000

Specifies the maximum number of seconds, from creation, that a SAML assertion is usable.

**wgserver.saml.responseskew**

Default value: 180

Sets the maximum number of seconds difference between Tableau Server time and the time of the assertion creation (based on the IdP server time) that still allows the message to be processed.

**wgserver.session.apply_lifecycle_limit**

Default value: false

Controls whether there is a session lifetime for server sessions. Set this to true to configure a server session lifetime.
Tableau Server on Linux Administrator Guide

wgserver.session.idle_limit

Default value: 240

The number of minutes of idle time before a sign-in to the web application times out.

wgserver.session.lifetime_limit

Default value: 1440

The number of minutes a server session lasts if a session lifetime is set. The default is 1440 minutes (24 hours). If `wgserver.session.apply_lifetime_limit` is false (the default) this is ignored.

wgserver.unrestricted_ticket

Default value: false

Specifies whether to extend access to server resources for users authenticated by trusted tickets. Default behavior allows users to access views only. Setting this to true allows users with valid trusted tickets to access server resources (projects, workbooks, and so on) as if they had signed in using their credentials.

workerX.gateway.port

Default value: 80 (443 if SSL)

External port that Apache listens on for workerX (where a “worker” is the term used for subsequent server nodes in the cluster). worker0.gateway.port is Tableau Server’s external port. In a distributed environment, worker0 is the initial Tableau Server node.

workerX.vizqlserver.procs

Default value: <number>

Number of VizQL servers.
zookeeper.config.snapCount

Specifies the number of transactions necessary to cause the Coordination Service to create a snapshot of the logs. By default this value is 100,000 transactions. If your Coordination Service is not writing enough transactions to result in snapshots, the automatic cleanup of snapshots older than five days will not take place, and you may lose disk space to the transaction logs. By default transaction logs and snapshots are created in the Tableau data directory.

tsm customize

You can use the tsm customize command to customize the look and feel of the Tableau Server client browser experience.

<table>
<thead>
<tr>
<th>Logo</th>
<th>Option flag</th>
<th>Minimum size/Maximum size, in pixels</th>
<th>Recommended size, in pixels</th>
</tr>
</thead>
<tbody>
<tr>
<td>A - Window tab logo</td>
<td>cannot be changed</td>
<td>cannot be changed</td>
<td>cannot be changed</td>
</tr>
<tr>
<td>B - Server name</td>
<td>--server-name</td>
<td>does not apply</td>
<td>does not apply</td>
</tr>
</tbody>
</table>
The image files you use should be in GIF, JPEG, or PNG format.

The background colors on the header and sign in page are not the same. If you use the same image for both locations (if you use the --logo option, for example) your logo might look different depending on where it appears in the server interface.

Synopsis

```
  tsm customize [options] [global options]
```

After you run the customize command, you must run the following command to apply changes:

```
  tsm pending-changes apply
```

Options

```
  --header-logo "<path-to-logo>"
```

Optional.

Specify a path to the image file that will be displayed in the header only.
**Note:** Use quotation marks around the path and image file if they include any spaces.

```
--logo "<path-to-logo>"
```

Optional.

Path to a single image file that will display for both the header and the sign-in window.

**Note:** Use quotation marks around the path and image file if they include any spaces.

```
--restore-defaults
```

Optional.

Reset all customization options to default install state.

```
--server-name <server_name>
```

Optional.

Server name that appears in the browser tab, tooltips, and messages.

```
--signin-logo "<path-to-logo>"
```

Optional.

Specify a path to the image file that will be displayed for sign-in window only.

**Note:** Use quotation marks around the path and image file if they include any spaces.
Global options

-h, --help

Optional.
Show the command help.

-p, --password <password>

Required, along with -u or --username if no session is active.
Specify the password for the user specified in -u or --username.
If the password includes spaces or special characters, enclose it in quotes:
--password 'my password'

-s, --server <url_to_tsm>

Optional.
Use the specified address for Tableau Services Manager. The URL must start with https, include port 8850, and use the server name not the IP address, for example https://mytableauhost:8850. If no server is specified, https://<localhost | dnsname>:8850 is assumed.

--trust-admin-controller-cert

Optional.
Use this flag to trust the self-signed certificate on the TSM controller. For more information about certificate trust and CLI connections, see Connecting TSM clients.

-u, --username <user>

Required if no session is active, along with -p or --password.
Specify a user account. If you do not include this option, the command is run using credentials you signed in with.

**tsm data-access**

You can use the `tsm data-access` commands to configure data caching, enable or disable data repository access, enable SAML for single sign-on, and configure settings for Web Data Connectors (WDCs).

- caching
  - data-access caching list
  - data-access caching set
- repository
  - repository-access disable
  - repository-access enable
  - repository-access list
- set-saml-delegation
  - set-saml-delegation configure
  - set-saml-delegation disable
  - set-saml-delegation enable
- web-data-connectors
  - web-data-connectors add
  - web-data-connectors allow
  - web-data-connectors delete
  - web-data-connectors list

**tsm data-access caching list**

Displays data connection caching settings. To learn more about data connection caching settings, see Configure Data Cache.

**Synopsis**

```
tsm data-access caching list [global options]
```
tsm data-access caching set

Sets data connection caching settings. To learn more about data connection caching settings, see Configure Data Cache.

Synopsis

tsma data-access caching set [options] [global options]

Options

-r, --refresh-frequency

Optional.

Sets the frequency to refresh cached data with a new query to the underlying data source. You can specify a number to define the maximum number of minutes that data should be cached. You can also specify low to cache and reuse data for as long as possible, or always (equivalent to 0) to refresh data each time that a page is loaded. If this option is not specified, it defaults to low.

tsm data-access repository-access disable

Disable external access to the Tableau PostgreSQL database for the default remote user. This will not disable access from localhost.

Synopsis

tsma data-access repository-access disable [options]
[global options]

Options

--repository-username <username>

Required.

The username, either tableau or readonly, with access to the data repository.
--request-timeout <timeout in seconds>

Optional.

Wait the specified amount of time for the command to finish. Default value is 1800 (30 minutes).

--ignore-prompt

Optional.

Suppress the prompt for restart and restart Tableau Server.

tsm data-access repository-access enable

Enables access to the Tableau PostgreSQL database.

By default, PostgreSQL traffic uses port 8060 (TCP). If you are running a local firewall, be sure to allow traffic for this port. To change the PostgreSQL port, see Ports that are not dynamically mapped.

Synopsis

tsm data-access repository-access enable [options]
[global options]

Options

--repository-password <password>

Required.

Sets (or changes) the password to access the data repository for the specified username.

--repository-username <username>

Required.
The username, either **tableau** or **readonly**, with access to the data repository.

```
--request-timeout <timeout in seconds>
```

Optional.

Wait the specified amount of time for the command to finish. Default value is 1800 (30 minutes).

```
--ignore-prompt
```

Optional.

Suppress the prompt for restart and restart Tableau Server.

**tsm data-access repository-access list**

Lists users who have access to the Tableau PostgreSQL database.

**Synopsis**

```
tsml data-access repository-access list [global options]
```

**tsm data-access set-saml-delegation configure**

Setup single sign-on for SAML SAP HANA so that Tableau Server functions as an Identity Provider (IdP) that provides single sign-on for users making SAP HANA data connections.

**Synopsis**

```
tsml data-access set-saml-delegation configure [options] [global options]
```

**Options**

```
-kf, --cert-key <cert-key>
```

Optional.
The SAML certificate key file.

- cf, --cert-file <file-path>

Optional.

The location of the SAML certificate file.

- uf, --username-format <username-format>

Optional.

Username format. Valid format keys are: 'username', 'domain_and_username', and 'email'.

- uc, --username-case <username-case>

Optional.

Username case. Valid case keys are: 'lower', 'upper', and 'preserve'.


**tsm data-access set-saml-delegation disable**

Disable single sign-on for SAML SAP HANA.

**Synopsis**

```
tsm data-access set-saml-delegation disable [global options]
```

**tsm data-access set-saml-delegation enable**

Enable single sign-on for SAML SAP HANA.

**Synopsis**

```
tsm data-access set-saml-delegation enable [global options]
```
Add a web data connector (WDC) to the WDC safe list ("whitelist").

Synopsis

tsm data-access web-data-connectors add [options]
[global options]

Options

-n, --name <name>

Required.

The name for the WDC that will be displayed in the Tableau Server data source list. This name must be enclosed in single quotes (') or double quotes (").

-sec, --secondary <secondary-URL-1>, <secondary-URL-2>

Optional.

A comma-delimited list of URLs that indicates which domains the connector can make requests to or receive data from. To add a domain to this secondary safe list, use a wildcard character (*), as follows: https://www.example.com/*

--url <URL>

Required.

The URL for the WDC (formatted as <scheme>://<host>:<port>/<path>, for example https://www.tableau.com:80/example/). For many WDCs, the <port> value is 443 or 80, but you can check the value for your connector by looking at the data source details on Tableau Server or Tableau Online.
**tsm data-access web-data-connectors allow**

Enable or disable WDC refreshes. Also, enable or disable the use of WDCs on Tableau Server.

**Synopsis**

```
 tsm data-access web-data-connectors allow [options]
 [global options]
```

**Options**

```
-r, --refreshes <refreshes-allowed>
```

Optional.

Set to false to disallow WDC refreshes. Defaults to true.

```
-t, --type <WDC-allowed>
```

Optional.

Set to none to disallow the use of WDCs on Tableau Server (and omit WDCs from backups). Defaults to all, which allows the use of WDCs.

**tsm data-access web-data-connectors delete**

Delete a specified WDC, or all WDCs, from the Tableau Server safe list ("whitelist").

**Synopsis**

```
 tsm data-access web-data-connectors delete [options]
 [global options]
```

**Options**

```
--all
```

Optional.
This option will delete all WDCs.

```
--url <URL>
```

Optional.

The URL for the WDC to delete.

tsm data-access web-data-connectors list

List all WDCs currently on the safe list ("whitelist").

Synopsis

```
tsm data-access web-data-connectors list [options]
[global options]
```

Options

Global options

```
-h, --help
```

Optional.

Show the command help.

```
-p, --password <password>
```

Required, along with -u or --username if no session is active.

Specify the password for the user specified in -u or --username.

If the password includes spaces or special characters, enclose it in quotes:

```
--password 'my password'
```

```
-s, --server <url_to_tsm>
```

Optional.
Use the specified address for Tableau Services Manager. The URL must start with https, include port 8850, and use the server name not the IP address, for example https://mytableauhost:8850. If no server is specified, https://<localhost | dnsname>:8850 is assumed.

--trust-admin-controller-cert

Optional.

Use this flag to trust the self-signed certificate on the TSM controller. For more information about certificate trust and CLI connections, see Connecting TSM clients.

-u, --username <user>

Required if no session is active, along with -p or --password.

Specify a user account. If you do not include this option, the command is run using credentials you signed in with.

tsm initialize

You can use the tsm initialize command to initialize Tableau Server.

Note: You must apply or discard pending changes before running tsm initialize or the initialize will fail. Apply pending changes using the tsm pending-changes apply command. Discard any pending changes you do not want to apply using tsm pending-changes discard.

Synopsis

tsm initialize [options] [global options]

Options

-r,--start-server
Optional. Leave the server running after initialization is complete.

Global options

-h, --help

Optional.
Show the command help.

-p, --password <password>

Required, along with -u or --username if no session is active.
Specify the password for the user specified in -u or --username.
If the password includes spaces or special characters, enclose it in quotes:
--password 'my password'

-s, --server <url_to_tsm>

Optional.
Use the specified address for Tableau Services Manager. The URL must start with https, include port 8850, and use the server name not the IP address, for example https://mytableauhost:8850. If no server is specified, https://<localhost | dnsname>:8850 is assumed.

--trust-admin-controller-cert

Optional.
Use this flag to trust the self-signed certificate on the TSM controller. For more information about certificate trust and CLI connections, see Connecting TSM clients.

-u, --username <user>

Required if no session is active, along with -p or --password.
Specify a user account. If you do not include this option, the command is run using credentials you signed in with.

**tsm jobs**

You can use the `tsm jobs` commands to list, reconnect to, and cancel jobs.

- `cancel`
- `list`
- `reconnect`

**tsm jobs cancel**

Cancel a job on the server. Any job can be canceled before it starts running (when queued), but only backup and cleanup jobs can be canceled when they are already running.

**Synopsis**

`tsm jobs cancel --id <jobID> [global options]`

**Options**

-`-i,--id <jobID>`
  
  Required.
  
  Id of the job to cancel.

**tsm jobs list**

List asynchronous jobs on the server.

**Synopsis**

`tsm jobs list [--status <status>] [global options]`
Options

-t, --status <status>

Optional.
Filter for jobs that match the given status.

tsm jobs reconnect

Reconnect to an asynchronous job to display its progress. If no job id is specified, it reconnects to the latest job.

Synopsis

tsm jobs reconnect[--id <jobID>] [global options]

Options

-i, --id <jobID>

Optional.
Specifies the id of the job that should be reconnected.

Global options

-h, --help

Optional.
Show the command help.

-p, --password <password>

Required, along with -u or --username if no session is active.
Specify the password for the user specified in -u or --username.
If the password includes spaces or special characters, enclose it in quotes:

```
--password 'my password'
```

-s, --server <url_to_tsm>

Optional.

Use the specified address for Tableau Services Manager. The URL must start with https, include port 8850, and use the server name not the IP address, for example https://mytableauhost:8850. If no server is specified, https://<localhost | dnsname>:8850 is assumed.

--trust-admin-controller-cert

Optional.

Use this flag to trust the self-signed certificate on the TSM controller. For more information about certificate trust and CLI connections, see Connecting TSM clients.

-u, --username <user>

Required if no session is active, along with -p or --password.

Specify a user account. If you do not include this option, the command is run using credentials you signed in with.

**tsm licenses**

You can use the tsm licenses commands to manage server license tasks like activating or deactivating a Tableau Server product key on- or off-line, and getting associated files for offline activation or deactivation.

- tsm licenses activate
- tsm licenses deactivate
- tsm licenses get-offline-activation-file
Tableau Server on Linux Administrator Guide

- tsm licenses get-offline-deactivation-file
- tsm licenses list
- tsm licenses refresh

**tsm licenses activate**

Activates a Tableau Server product key.

**Synopsis**

```
 tsm licenses activate --license-key <product-key>
 [global options]
```

**Options**

- `-f, --license-file <file.tlf>`

  Required if doing offline activation.

  Specifies the license file (<file>.tlf) used for offline activation.

- `-k, --license-key <product-key>`

  Required if activating a valid product key.

  Specifies the product key to use for online activation.

- `-t, --trial`

  Required if activating a trial license.

  Activate a trial license.

**tsm licenses deactivate**

Deactivates a Tableau Server product key either online or offline.
Synopsis

`tsm licenses deactivate --license-key <product-key>`
[global options]

Options

- `-f, --license-file <return_file.tlr>`
  Required if doing offline deactivation.
  Specifies the license file (<file>.tlf) used for offline deactivation.

- `-k, --license-key <product-key>`
  Required if deactivating a product key.
  Specifies the product key to use for online deactivation.

`tsm licenses get-offline-activation-file`

Generate an offline activate file to use for activating Tableau Server offline. To learn more, see Activate Tableau Server Offline - Adding a License.

Synopsis

`tsm licenses get-offline-activation-file --license-key <product-key> --output-dir <path> [global options]`

Options

- `-k, --license-key <product-key>`
  Required.
  Specifies the product key to use for offline activation.

- `-o, --output-dir <path>`
Required.
The location where the offline activation file should be saved. This location must exist.

**tsm licenses get-offline-deactivation-file**

Generate an offline deactivation file to use for deactivating Tableau Server offline. To learn more, see Deactivate Tableau Server Offline.

**Synopsis**

```bash
tsm licenses get-offline-deactivation-file --license-key <product-key> --output-dir <path> [global options]
```

**Options**

- `-k, --license-key <product-key>`
  
  Required.
  Specifies the product key to use for offline deactivation.

- `-o, --output-dir <path>`
  
  Required.
  The existing location where the offline deactivation file should be saved.

**tsm licenses list**

Lists licenses that are activated on the Tableau Server deployment.

For example, a server with five Creator licenses, five Explorer licenses, 100 Viewer licenses, and a Data Management Add-on would provide command output similar to the following:

<table>
<thead>
<tr>
<th>Key</th>
<th>Type</th>
<th>Creator</th>
<th>Explorer</th>
<th>Viewer</th>
<th>Data Management</th>
<th>Add-on</th>
<th>Guest Access Lic Exp</th>
<th>Maint Exp</th>
<th>Valid</th>
</tr>
</thead>
<tbody>
<tr>
<td>T531-00000</td>
<td>Tier</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>false</td>
<td>false</td>
<td>12/31/19</td>
<td>N/A</td>
<td>true</td>
</tr>
<tr>
<td>T511-00000</td>
<td>Tier</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>false</td>
<td>false</td>
<td>12/31/19</td>
<td>N/A</td>
<td>true</td>
</tr>
<tr>
<td>T506-00000</td>
<td>Tier</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>false</td>
<td>false</td>
<td>12/31/19</td>
<td>N/A</td>
<td>true</td>
</tr>
</tbody>
</table>

The following fields are returned:
• **KEY**: A globally unique 16-character string that identifies the license.
• **TYPE**: Describes the type of license
  - Term: Term licenses map to a subscription schedule and must be renewed. The expiration date is listed under the LIC EXP field.
  - Perpetual: Perpetual licenses are purchased once and do not need to be renewed but must be refreshed to update the MAINT EXP or maintenance expiration date.
  - Cores: Core licenses are licenses that map to the number of cores on the computers running specific Tableau Server services. Core licensing allows for a guest user access to views on the server or embedded on other web servers. Core licenses also allow for unlimited Explorer and Viewer users.
• **CREATOR**: The number of Creator licenses issued to the Tableau Server deployment.
• **EXPLORER**: The number of Explorer licenses issued to the Tableau Server deployment.
• **VIEWER**: The number of Viewer licenses issued to the Tableau Server deployment.
• **DATA MANAGEMENT ADD-ON**: Tableau Server is licensed for the Data Management Add-on (True/False). See Data Management Add-On.
• **GUEST ACCESS**: Tableau Server is licensed for a Guest User. See Guest User. The ability to leverage a Guest User requires Core licensing. See TYPE field.
• **LIC EXP**: The date that the license expires and Tableau Server will stop working. Term licenses expire. See TYPE field. Visit the Tableau Customer Portal to refresh licenses.
• **MAINT EXP**: Applies only to legacy perpetual licenses (TYPE = Perpetual). For Term licenses, this field will output, N/A. MAINT EXP displays the date that the maintenance contract for the Tableau Server deployment expires. To update the license maintenance key see Refresh Expiration Date for the Product Key. Visit the Tableau Customer Portal to view maintenance purchase history and to purchase additional maintenance.
• **VALID**: Specifies if the license is valid (True/False). Invalid licenses will cause server failure.

**Synopsis**

```
tsm licenses list [global options]
```
tsm licenses refresh

Update the maintenance expiration date of all product keys on Tableau Server.

Synopsis

tsm licenses refresh [global options]

Global options

-h, --help

Optional.
Show the command help.

-p, --password <password>

Required, along with -u or --username if no session is active.
Specify the password for the user specified in -u or --username.
If the password includes spaces or special characters, enclose it in quotes:
--password 'my password'

-s, --server <url_to_tsm>

Optional.
Use the specified address for Tableau Services Manager. The URL must start with https, include port 8850, and use the server name not the IP address, for example https://mytableauhost:8850. If no server is specified, https://<localhost | dnsname>:8850 is assumed.

--trust-admin-controller-cert

Optional.
Use this flag to trust the self-signed certificate on the TSM controller. For more information about certificate trust and CLI connections, see Connecting TSM clients.

-\texttt{u, --username <user>}

Required if no session is active, along with -\texttt{p} or --\texttt{password}.

Specify a user account. If you do not include this option, the command is run using credentials you signed in with.

\textbf{tsm login}

Use the \texttt{tsm login} command to log in to Tableau Services Manager. You need to authenticate to TSM before running any TSM command.

\textbf{Synopsis}

\texttt{tsm login [global options]}

\textbf{Global options}

-\texttt{h, --help}

Optional.

Show the command help.

-\texttt{p, --password <password>}

Required, along with -\texttt{u or --username} if no session is active.

Specify the password for the user specified in -\texttt{u or --username}.

If the password includes spaces or special characters, enclose it in quotes:

-\texttt{--password 'my password'}

-\texttt{s, --server <url_to_tsm>
Optional.

Use the specified address for Tableau Services Manager. The URL must start with https, include port 8850, and use the server name not the IP address, for example https://mytableauhost:8850. If no server is specified, https://<localhost | dnsname>:8850 is assumed.

--trust-admin-controller-cert

Optional.

Use this flag to trust the self-signed certificate on the TSM controller. For more information about certificate trust and CLI connections, see Connecting TSM clients.

-u, --username <user>

Required if no session is active, along with -p or --password.

Specify a user account. If you do not include this option, the command is run using credentials you signed in with.

**tsm logout**

You can use the `tsm logout` command to log out of Tableau Services Manager (TSM).

**Synopsis**

```
tsm logout [global options]
```

**Global options**

--h, --help

Optional.

Show the command help.
-p, --password <password>

Required, along with -u or --username if no session is active.

Specify the password for the user specified in -u or --username.

If the password includes spaces or special characters, enclose it in quotes:

--password 'my password'

-s, --server <url_to_tsm>

Optional.

Use the specified address for Tableau Services Manager. The URL must start with https, include port 8850, and use the server name not the IP address, for example https://mytableauhost:8850. If no server is specified, https://<localhost | dnsname>:8850 is assumed.

--trust-admin-controller-cert

Optional.

Use this flag to trust the self-signed certificate on the TSM controller. For more information about certificate trust and CLI connections, see Connecting TSM clients.

-u, --username <user>

Required if no session is active, along with -p or --password.

Specify a user account. If you do not include this option, the command is run using credentials you signed in with.

tsm maintenance

You can use the tsm maintenance commands to manage server maintenance tasks like creating regular backups or restoring Tableau Server from a previously created backup.
Tableau Server on Linux Administrator Guide

- tsm maintenance backup
- tsm maintenance cleanup
- tsm maintenance reindex-search
- tsm maintenance reset-searchserver
- tsm maintenance restore
- tsm maintenance send-logs
- tsm maintenance validate-resources
- tsm maintenance ziplogs

tsm maintenance backup

Creates a backup of the data managed by Tableau Server. This data includes the Tableau PostgreSQL database (the repository) which contains workbook and user metadata, and extract (.tde or .hyper) files. This data does not include configuration data. See Perform a Full Backup and Restore of Tableau Server.

Locating the repository (pgsql) and the File Store on the same node as the Administration Controller can reduce the length of time it takes to back up Tableau Server. The Administration Controller is usually on the initial node, unless you have had an initial node failure and had to move the controller to another node.

When the repository is co-located with the controller it eliminates or greatly reduces the need to compress and transfer data between nodes during the backup process. This is also true with the File Store, especially if your organization uses extracts heavily.

Synopsis

```
tsm maintenance backup --file <backup_file> [options]
[global options]
```
Options

-d, --append-date

Optional.

Append the current date to the backup file name.

-f, --file <backup_file>

Required.

Write the backup to the specified file. An extension of .tsbak is automatically used.
The file is written to the directory defined in the TSM base-filepath.backuprestore variable. By default:

/var/opt/tableau/tableau_server/data/tabsvc/files/backups/

For more information about file paths and how to change them, see tsm File Paths.

-i, --description <string>

Optional.

Include the specified description of the backup file.

--skip-compression

Optional.

Create a backup without using compression. This results in a larger backup file but can reduce the amount of time it takes to complete the backup. If using this in a multi-node installation, we strongly recommend you have a File Store instance configured on your initial node.

-k, --skip-verification

Optional.
Do not verify the integrity of the database backup.

--override-disk-space-check

Optional.

Attempt to create a backup even when there is a low disk space warning.

-po, --pg-only

Optional.

Generates only the repository backup.

--request-timeout <timeout in seconds>

Optional.

Wait the specified amount of time for the command to finish. Default value is 1800 (30 minutes).

Examples

This example creates a backup called ts_backup-<yyyy-mm-dd>.tsbak in the /var/-
opt/tableau/tableau_server/data/tabsvc/files/backups/ directory:

tsm maintenance backup -f ts_backup -d

ts maintenance cleanup

Deletes old log files and temporary files.

If you are running Tableau Server on a distributed deployment, run this command on the
node that is running the Administration Controller (also referred to as the TSM Controller)pro-
cess. By default, the controller is on the initial node in the cluster.

The purpose of this command is to create free space on the Tableau deployment by deleting
old files. Therefore, running this command when the server is started will remove the
majority of old content for this scenario. To remove current log files, then you must stop the server before running this command.

**Note:** This command was added in Tableau Server version 10.5.1 and some options were added in version 2018.1.

Synopsis

```bash
tsrm maintenance cleanup [options] [global options]
```

Options

- `--all`
  
  Optional.
  
  Perform all cleanup operations with default retention values. Equivalent to running the `cleanup` command with the following options: `-l -t -r -q`.

- `--http-requests-table-retention <# of days>`
  
  Optional.
  
  Default: 7 days

  Specify the number of days of `http_requests` table entries that should be retained. Entries older than the specified number of days are deleted. This option specifies the retention age but does not delete table entries. To delete entries, use the `-q` option in addition to this option.

- `--log-files`
  
  Optional.
Delete log files that are older than the retention-period. Files in the subdirectories under `data/tabsvc/logs` will be deleted.

```
--log-files-retention <# of days>
```

Optional.

Default: 1 (24 hours)

Delete logs older than this number of days. This command does not apply to temporary files.

```
-q, --http-requests-table
```

Optional.

Delete old `http_requests` table entries. Tableau Server must be running for table entries to be deleted. This option is ignored if Tableau Server is stopped.

```
-r, --redis-cache
```

Optional.

Clear the Redis cache.

```
--request-timeout <timeout in seconds>
```

Optional.

Wait the specified amount of time for the command to finish. Default value is 1800 (30 minutes).

```
-t, --temp-files
```

Optional.

Delete all files and subdirectories in the following directories:
Only directories that are storing files for expired (not running) sessions are deleted.

- /var/opt/tableau/tableau_server/data/tabsvc/httpd/temp
- /var/opt/tableau/tableau_server/temp

-v, --verbose

Optional.

Show details of what was cleaned.

Examples

This example cleans up all log files older than 2 days old:

```bash
tsm maintenance cleanup -l --log-files-retention 2
```

tsm maintenance reindex-search

Use the reindex-search command to rebuild the search index.

Synopsis

```bash
tsm maintenance reindex-search [options] [global options]
```

Option

--request-timeout <timeout in seconds>

Optional.

Wait the specified amount of time for the command to finish. Default value is 1800 (30 minutes).
tsm maintenance reset-searchserver

Resets the search server to a clean state, deleting search information and rebuilding the search index.

Synopsis

tsm maintenance reset-searchserver [options] [global options]

Option

--request-timeout <timeout in seconds>

Optional.

Wait the specified amount of time for the command to finish. Default value is 1800 (30 minutes).

tsm maintenance restore

Restore Tableau Server using the specified backup file. Restoring a backup file does not restore any configuration data. See Perform a Full Backup and Restore of Tableau Server.

You can only restore from a backup that has the same type of identity store as the running server. For example, a backup from a server using local authentication can be restored to a Tableau Server initialized with local authentication, but a backup from a server using Active Directory authentication cannot be restored to a server initialized with local authentication.

Synopsis

tsm maintenance restore --file <file_name> [--restart-server] [global options]

Options

-ak, --asset-key-file <file_name>

Optional. Specify this option only if you are restoring from assets that were created by
tabadmin on Tableau Server (versions 2018.1 and earlier).

Name of asset key file to restore from. The asset key file is created by the tabadmin assetkeys command. The file must be in the predefined backup/restore location on the server.

-\texttt{f, \textbf{--file} <file\_name>}

Required.

Specifies the backup file to restore from.

The restore command expects a backup file in the directory defined in the TSM basefilepath.backuprestore variable. By default:

\texttt{/var/opt/tableau/tableau_server/data/tabsvc/files/backups/}

For more information about file paths and how to change them, see tsm File Paths.

-\texttt{k, \textbf{--skip-identity-store-verification} }

Optional. Specify this option only if you are restoring from a backup file that was created by tabadmin on Tableau Server (versions 2018.1 and earlier).

Do not use this key in an attempt to change identity store type from Tableau Sever that created original backup file. To change the identity store, see Changing the Identity Store.

-\texttt{p, \textbf{--pg-only} }

Optional.

Restores only the repository.

-\texttt{r, \textbf{--restart-server} }

Optional.
Restart the server after the restore.

--request-timeout <timeout in seconds>

Optional.

Wait the specified amount of time for the command to finish. Default value is 1800 (30 minutes).

tsm maintenance send-logs

Upload the specified file to Tableau and associate it with a support case. To successfully upload files to Tableau, your Tableau Server must be able to communicate with the send-logs server at https://report-issue.tableau.com.

Synopsis

tsm maintenance send-logs --case <case_number> --email <contact_email> --file <path/to/file> [global options]

Options

-c, --case <case_number>

Required.

Support case number.

-e, --email <contact_email>

Required.

Contact email.

-f, --file <path/to/file>

Required.
Specifies the location and name of the log file archive to send.

```
--request-timeout <timeout in seconds>
```

Optional.
Wait the specified amount of time for the command to finish. Default value is 1800 (30 minutes).

### tsm maintenance validate-resources

Validate workbooks and data sources for a site.

**Synopsis**

```
tsm maintenance validate-resources --site-id <site ID>
[global options]
```

**Options**

```
-id,--site-id <site ID>
```
Required.
ID for the site whose resources you are validating.

```
-r,--repair
```
Optional.
Repair invalid resources.

```
--request-timeout <timeout in seconds>
```
Optional.
Wait the specified amount of time for the command to finish. Default value is 1800 (30 minutes).
tsm maintenance ziplogs

Use the `ziplogs` command to create an archive of Tableau Server log files.

**Note:** If you cannot run the `ziplogs` command successfully, you can manually zip the Tableau Server logs. For more information, see Troubleshoot Tableau Server on Linux.

**Synopsis**

```
  tsm maintenance ziplogs [options] [global options]
```

**Options**

- `-a`, `--all`
  
  Optional.
  
  Include all files except PostgreSQL data.

- `-d`, `--with-postgresql-data`
  
  Optional.
  
  Include the PostgreSQL data folder if Tableau Server is stopped or PostgreSQL dump files if Tableau Server is running.

- `-f`, `--file <name>`
  
  Optional.
  
  Specify a name for the zipped archive file. If no name is provided the archive is created as `logs.zip`. The file is written to the directory defined in the TSM `basefilepath.log_archive` variable. By default:

  `/var/opt/tableau/tableau_server/data/tabsvc/files/log-archives/`

  For more information about file paths and how to change them, see tsm File Paths.
-i, --description <string>
Optional.
Include the specified description of the archive file.

-l, --with-latest-dump
Optional.
When any service crashes, Tableau Server generates a dumpfile. Set this option to include the most recent service crash dumpfile. If you do not set this option, then no dumpfile will be included in the resulting ziplog.

-m, --minimumdate <date>
Optional.
Earliest date of log files to be included. If not specified, a maximum of two days of log files are included. Format of date should be "mm/dd/yyyy".

-o, --overwrite
Optional.
For an overwrite of an existing ziplog file. If a file by the same name already exists and this option is not used, the ziplogs command will fail.

By default the file is written to:

/var/opt/tableau/tableau_server/data/tabsvc/files/log-archives/

For more information about file paths and how to change them, see tsm File Paths.

--request-timeout <timeout in seconds>
Optional.
Wait the specified amount of time for the command to finish. Default value is 7200 (120 minutes).

-t, --with-netstat-info

Optional.

Include netstat information.

Global options

-h, --help

Optional.

Show the command help.

-p, --password <password>

Required, along with -u or --username if no session is active.

Specify the password for the user specified in -u or --username.

If the password includes spaces or special characters, enclose it in quotes:

--password 'my password'

-s, --server <url_to_tsm>

Optional.

Use the specified address for Tableau Services Manager. The URL must start with https, include port 8850, and use the server name not the IP address, for example https://mytableauhost:8850. If no server is specified, https://<localhost | dnsname>:8850 is assumed.
trust-admin-controller-cert

Optional.

Use this flag to trust the self-signed certificate on the TSM controller. For more information about certificate trust and CLI connections, see Connecting TSM clients.

-u, --username <user>

Required if no session is active, along with -p or --password.

Specify a user account. If you do not include this option, the command is run using credentials you signed in with.

tsm pending-changes

You can use the tsm pending-changes commands to apply, discard, or view pending configuration and topology changes to Tableau Server.

- tsm pending-changes apply
- tsm pending-changes discard
- tsm pending-changes list

tsm pending-changes apply

You can use the tsm pending-changes apply command to apply pending configuration and topology changes to Tableau Server.

A prompt warns you that the command will restart Tableau Server. If Tableau Server is currently running it is restarted, and if it is stopped it is left in a stopped state with no restart. You can suppress the prompt using the --ignore-prompt option, but this does not change the restart behavior.
Tableau Server on Linux Administrator Guide

Synopsis

tsm pending-changes apply [global options]

Options

- iw, --ignore-warnings

  Optional.

  Ignore warning level constraints.

--ignore-prompt

  Optional.

  Suppress the prompt for restart. This only suppresses the prompt. The restart behavior is unchanged.

--request-timeout <timeout in seconds>

  Optional.

  Wait the specified amount of time for the command to finish. Default value is 1800 (30 minutes).

**tsm pending-changes discard**

You can use the tsm pending-changes discard command to discard pending configuration and topology changes to Tableau Server.

Synopsis

_tsm pending-changes discard [options] [global options]

Options

--config-only
Optional.

Discard only pending configuration changes.

--topology-only

Optional.

Discard only pending topology changes.

tsm pending-changes list

You can list pending configuration and topology changes to Tableau Server.

Synopsis

tsm pending-changes list [options] [global options]

Options

--config-only

Optional.

List only pending configuration changes.

--topology-only

Optional.

List only pending topology changes.

Global options

-h, --help

Optional.

Show the command help.
-p, --password <password>

Required, along with -u or --username if no session is active.

Specify the password for the user specified in -u or --username.

If the password includes spaces or special characters, enclose it in quotes:

--password 'my password'

-s, --server <url_to_tsm>

Optional.

Use the specified address for Tableau Services Manager. The URL must start with https, include port 8850, and use the server name not the IP address, for example https://mytableauhost:8850. If no server is specified, https://<localhost | dnsname>:8850 is assumed.

--trust-admin-controller-cert

Optional.

Use this flag to trust the self-signed certificate on the TSM controller. For more information about certificate trust and CLI connections, see Connecting TSM clients.

-u, --username <user>

Required if no session is active, along with -p or --password.

Specify a user account. If you do not include this option, the command is run using credentials you signed in with.

tsm register

You can use the tsm register command to register Tableau Server. This command lets you either display the registration file template (using the --template option) or provide
the path to a completed registration file (using the --file option). You must use one of these two options when calling the tsm register command.

Synopsis

```
tsm register --template | --file <registration-filename>
[global options]
```

Options

```
--file <registration-filename>
  Required.
  Path to the file that contains the registration data.

--template
  Required.
  Display registration file template.
```

Global options

```
-h, --help
  Optional.
  Show the command help.

-p, --password <password>
  Required, along with -u or --username if no session is active.
  Specify the password for the user specified in -u or --username.
  If the password includes spaces or special characters, enclose it in quotes:
  --password 'my password'
```
Optional.

Use the specified address for Tableau Services Manager. The URL must start with https, include port 8850, and use the server name not the IP address, for example https://mytableauhost:8850. If no server is specified, https://<localhost | dnsname>:8850 is assumed.

Optional.

Use this flag to trust the self-signed certificate on the TSM controller. For more information about certificate trust and CLI connections, see Connecting TSM clients.

Required if no session is active, along with -p or --password.

Specify a user account. If you do not include this option, the command is run using credentials you signed in with.

**tsm reset**

Use the `tsm reset` command to clear the initial admin user so that you can enter a new one. After you run `tsm reset` you must rerun the `tabcmd initialuser` command to create a new initial admin. The new name cannot be the same username as the previous admin user.

**Note:** This command was added in Tableau Server version 2018.1.

**Synopsis**

```
  tsm reset[option] [global options]
```
Option

-d, --delete-all-sessions

Optional.

Delete all active user sessions when the server is reset.

--request-timeout <timeout in seconds>

Optional.

Wait the specified amount of time for the command to finish. Default value is 1800 (30 minutes).

Global options

-h, --help

Optional.

Show the command help.

-p, --password <password>

Required, along with -u or --username if no session is active.

Specify the password for the user specified in -u or --username.

If the password includes spaces or special characters, enclose it in quotes:

--password 'my password'

-s, --server <url_to_tsm>

Optional.
Use the specified address for Tableau Services Manager. The URL must start with https, include port 8850, and use the server name not the IP address, for example https://mytableauhost:8850. If no server is specified, https://<localhost | dnsname>:8850 is assumed.

--trust-admin-controller-cert

Optional.

Use this flag to trust the self-signed certificate on the TSM controller. For more information about certificate trust and CLI connections, see Connecting TSM clients.

-u, --username <user>

Required if no session is active, along with -p or --password.

Specify a user account. If you do not include this option, the command is run using credentials you signed in with.

tsm restart

You can use the tsm restart command to restart Tableau Server. The command stops the server if necessary, and then starts it.

Synopsis

tsm restart [global options]

Option

--request-timeout <timeout in seconds>

Optional.

Wait the specified amount of time for the command to finish. Default value is 1800 (30 minutes).
Global options

-h, --help
Optional.
Show the command help.

-p, --password <password>
Required, along with -u or --username if no session is active.
Specify the password for the user specified in -u or --username.
If the password includes spaces or special characters, enclose it in quotes:
--password 'my password'

-s, --server <url_to_tsm>
Optional.
Use the specified address for Tableau Services Manager. The URL must start with https, include port 8850, and use the server name not the IP address, for example https://mytableauhost:8850. If no server is specified, https://<localhost | dnsname>:8850 is assumed.

--trust-admin-controller-cert
Optional.
Use this flag to trust the self-signed certificate on the TSM controller. For more information about certificate trust and CLI connections, see Connecting TSM clients.

-u, --username <user>
Required if no session is active, along with -p or --password.
Specify a user account. If you do not include this option, the command is run using credentials you signed in with.

**tsm security**

Use the `tsm security` commands to configure Tableau Server support for external (gateway) SSL or repository (Postgres) SSL. Repository SSL configuration includes the option to enable SSL over direct connections from Tableau clients—including Tableau Desktop, Tableau Mobile, and web browsers—to the repository.

- `tsm security external-ssl`
  - `tsm security external-ssl disable`
  - `tsm security external-ssl enable`
  - `tsm security external-ssl list`
- `tsm security regenerate-internal-tokens`
- `tsm security repository-ssl`
  - `tsm security repository-ssl disable`
  - `tsm security repository-ssl enable`
  - `tsm security repository-ssl get-certificate-file`
  - `tsm security repository-ssl list`
- `tsm security vizql-extsvc-ssl`
  - `tsm security vizql-extsvc-ssl disable`
  - `tsm security vizql-extsvc-ssl enable`
  - `tsm security vizql-extsvc-ssl list`

**Prerequisites**

Before you configure SSL, you must acquire certificates, and then copy them to the computer that runs the Tableau Server gateway process. Additional preparation is required for enabling direct connections from clients. To learn more, see the following articles:

Configure SSL for External HTTP Traffic to and from Tableau Server

Configure SSL for Internal Postgres Communication
Note: For information about mutual (two-way) SSL, see Configure Mutual SSL Authentication and tsm authentication mutual-ssl commands.

tsm security external-ssl disable

Removes the server’s existing SSL configuration settings and stops encrypting traffic between external clients and the server.

Synopsis

tsm security external-ssl disable [global options]

tsm security external-ssl enable

Enable and specify certificate and key files for SSL over external HTTP communication.

Synopsis

tsm security external-ssl enable --cert-file <file.crt> --key-file <file.key> [options] [global options]

Options

--cert-file <file.crt>
Required. Specify the name of a valid PEM-encoded x509 certificate with the extension .crt.

--key-file <file.key>
Required. Specify a valid RSA or DSA private key file, with the extension .key by convention.

--chain-file <chainfile.crt>
Specify the certificate chain file (.crt)
A certificate chain file is required for Tableau Desktop on the Mac. In some cases, a certificate chain file may be required for Tableau Mobile.

Some certificate providers issue two certificates for Apache. The second certificate is a chain file, which is a concatenation of all the certificates that form the certificate chain for the server certificate.

All certificates in the file must be x509 PEM-encoded and the file must have a .crt extension (not .pem).

--passphrase

Optional. Passphrase for the certificate file. The passphrase you enter will be encrypted while at rest.

**Note:** If you create a certificate key file with a passphrase, you cannot reuse the SSL certificate key for SAML.

--protocols <list protocols>

Optional. List the Transport Layer Security (TLS) protocol versions you want to allow or disallow.

TLS is an improved version of SSL. Tableau Server uses TLS to authenticate and encrypt connections. Accepted values include protocol versions supported by Apache. To disallow a protocol, prepend the protocol version with a minus (-) character.

**Default setting:** "all, -SSLv2, -SSLv3"

This default explicitly does not allow clients to use SSL v2 or SSL v3 protocols to connect to Tableau Server. However, we recommend that you also disallow TLS v1 and TLS v1.1.

Before you deny a specific version of TLS, verify that the browsers from which your users connect to Tableau Server support TLS v1.2. You might need to preserve support for TLSv1.1 until browsers are updated.
If you do not need to support TLS v1 or v1.1, use the following command to allow TLS v1.2 (using the value all), and explicitly deny SSL v2, SSL v3, TLS v1, and TLS v1.1.

tsm security external-ssl enable --cert-file file.crt --key-file file.key --protocols "all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1"

tsm security external-ssl list

Displays a list of settings related to the configuration of gateway external SSL. The list includes the names of the certificate files in use, but not their location.

Synopsis

tsm security external-ssl list [global options]

tsm security regenerate-internal-tokens

This command performs the following operations:

1. Generates new internal SSL certificates for Postgres repository the search server.
2. Generates new passwords for all of the internally managed passwords.
3. Updates all Postgres repository passwords.
4. Generates a new encryption key for asset key management and encrypts the asset key data with the new key.
5. Generates a new encryption key for configuration secrets (master key) and encrypts the configuration with it.
6. Reconfigures and updates Tableau Server with all of these secrets. In a distributed deployment, this command also distributes the reconfiguration and updates across all nodes in the cluster.
7. Stops the server.
8. Regenerates a new master key, adds it to the master keystore file, and then creates
new security tokens for internal use.

9. Starts the server.

If you plan to add a node to your cluster after you have run this command, then you will need to generate a new node configuration file to update the tokens, keys, and secrets that are generated by this command. See Install and Configure Additional Nodes.

Synopsis

```
tsm security regenerate-internal-tokens [options] [global options]
```

Options

```
--request-timeout <timeout in seconds>
```

Optional.

Wait the specified amount of time for the command to finish. Default value is 1800 (30 minutes).

`tsm security repository-ssl disable`

Stop encrypting traffic between the repository and other server components, and stop support for direct connections from Tableau clients.

Synopsis

```
tsm security repository-ssl disable [global-options]
```

`ttsm security repository-ssl enable`

Enables SSL and generates the server’s .crt and .key files used for encrypted traffic between the Postgres repository and other server components. Enabling this also gives you the option to enable SSL over direct connections from Tableau clients to the server.
Synopsis

`tsm security repository-ssl enable [options] [global options]`

Options

`-i, --internal-only`

Optional. When set to `--internal-only`, Tableau Server uses SSL between the repository and other server components, and it supports but does not require SSL for direct connections through `tableau` or `readonly` users.

If this option is not set, Tableau Server requires SSL for traffic between the repository and other server components, as well as for direct connections from Tableau clients (for connections through the `tableau` or `readonly` users).

When you specify this option, you must also complete the steps described in Configure Postgres SSL to Allow Direct Connections from Clients.

`tsm security repository-ssl get-certificate-file`

Get the public certificate file used for SSL communication with the Tableau repository. SSL must be enabled for repository communication before you can retrieve a certificate. The certificate file is distributed automatically to internal clients of the repository in the Tableau Server cluster. To enable remote clients to connect over SSL to the repository, you must copy the public certificate file to each client.

Synopsis

`tsm security repository-ssl get-certificate-file [global-options]`

Options

`-f, --file`

Required.
tsm security repository-ssl list

Returns the existing repository (Postgres) SSL configuration.

Synopsis

tsm security repository-ssl list [global-options]

tsm security vizql-extsvc-ssl disable

Disables the connection to Rserve or TabPy external service.

Synopsis

tsm security vizql-extsvc-ssl disable [global options]

tsm security vizql-extsvc-ssl enable

Enables and configures connection to Rserve external service.

If you are updating or changing an existing external services configuration, run the tsm security vizql-extsvc-ssl disable command to clear the settings before you run this command.

Synopsis

tsm security vizql-extsvc-ssl enable --connection-type <type> --extsvc-host <host_name> --extsvc-port <port> [options] [global options]

Options

--connection-type <type>

Specify the external service type that you are configuring. Valid values are: ext-svc-
rserve-secure or ext-svc-rserve.

--extsvc-host <host_name>

Required. Specify the host name or IP address of the server in your organization that is hosting the external service.

--extsvc-port <port_number>

Required. Specify the port that is used to connect to the external service. Default value for Rserve is typically 6311.

-cf, --cert-file <file.crt>

Optional. Specify the path and filename of a valid PEM-encoded x509 certificate with the extension .crt.

--extsvc-username <user_name>

Optional. If the connection to the external service requires authentication, specify the user name.

--extsvc-password <password>

Optional. If the connection to the external service requires authentication, specify the password.

--connect-timeout-ms <milliseconds>

Optional. Connection timeout in milliseconds. Default is 1000. Raise the value of this setting if Tableau is timing out before the external server can respond.

--script-disabled

This option is not supported. To disable scripts, run tsm security vizql-extsvc-
ssl disable.

tsm security vizql-extsvc-ssl list

Displays a list of settings related to the configuration of external service SSL. The list includes the names of the certificate files in use, host name, port, user name, timeout duration, and other details.

Synopsis

tsm security vizql-extsvc-ssl list [global options]

Global options

-h, --help

Optional.
Show the command help.

-p, --password <password>

Required, along with -u or --username if no session is active.
Specify the password for the user specified in -u or --username.
If the password includes spaces or special characters, enclose it in quotes:

--password 'my password'

-s, --server <url_to_tsm>

Optional.
Use the specified address for Tableau Services Manager. The URL must start with https, include port 8850, and use the server name not the IP address, for example https://mytableauhost:8850. If no server is specified, https://<localhost | dnsname>:8850 is assumed.
--trust-admin-controller-cert

Optional.

Use this flag to trust the self-signed certificate on the TSM controller. For more information about certificate trust and CLI connections, see Connecting TSM clients.

-u, --username <user>

Required if no session is active, along with -p or --password.

Specify a user account. If you do not include this option, the command is run using credentials you signed in with.

tsm settings

You can use the tsm settings commands to export (get) and import (set) configuration values.

- tsm settings export
- tsm settings import

Important: The server configuration file referenced in this topic includes a copy of the master keystore file used for encrypting configuration secrets. We strongly recommend that you take additional measures to secure the node configuration file, using mechanisms as described in Securing secrets for import and export operations.

tsm settings export

Export the current server configuration and topology to a file.

Synopsis

tsm settings export --output-config-file <path/to/output_file.json> [global options]
Options

-f, --output-config-file <file>

Required.

Specifies the location and name of the file created by this operation.

tsm settings import

Import server configuration or topology.

Synopsis

tsm settings import --import-config-file <path/to/import_file.json> [global options]

Options

-f, --import-config-file <FILE>

Required.

Path to input file.

--config-only

Optional.

--topology-only

Optional.

-frc, --force-keys

Optional.
Force a key to be added to configuration even if it did not previously exist.

Global options

-h, --help

Optional.
Show the command help.

-p, --password <password>

Required, along with -u or --username if no session is active.
Specify the password for the user specified in -u or --username.
If the password includes spaces or special characters, enclose it in quotes:

--password 'my password'

-s, --server <url_to_tsm>

Optional.
Use the specified address for Tableau Services Manager. The URL must start with https, include port 8850, and use the server name not the IP address, for example https://mytableauhost:8850. If no server is specified, https://<localhost | dnsname>:8850 is assumed.

--trust-admin-controller-cert

Optional.
Use this flag to trust the self-signed certificate on the TSM controller. For more information about certificate trust and CLI connections, see Connecting TSM clients.

-u, --username <user>

Required if no session is active, along with -p or --password.
Specify a user account. If you do not include this option, the command is run using credentials you signed in with.

**tsm sites**

You can use the tsm sites commands to export an existing site for import to a new site (also referred to as site migration), and to import the new site. An unlock command is available in case an error leaves a site locked.

The tsm sites commands will use your local file store to hold the export and import data. If you are running a multinode Tableau cluster, then you must run the tsm sites commands on a Tableau Server that is running the Data Engine process. For information about the Data Engine process and the processes that require it, see Tableau Server Processes.

For comprehensive steps for migrating a site, see Export or Import a Site.

- tsm sites export
- tsm sites import
- tsm sites import-verified
- tsm sites unlock

**tsm sites export**

Export a specified Tableau Server site to a .zip file. You can export a site to archive its settings at a specific point in time, or to complete the first step of a site migration process.

**Note:** The tsm sites import and tsm sites export commands can leave a site in a locked state if an error occurs. To unlock a site, use the tsm sites unlock command.
Synopsis

```
tsm sites export --site-id <source-siteID> --file <export-file> [options] [global options]
```

Options

- **-f, --file <export-file>**

  Required.

  Specify the name of the file to which Tableau Server saves all of the site’s information.

  This file is generated to the directory defined in the TSM `basefilepath.site_export.exports` variable. By default:

  `/var/opt/tableau/tableau_server/data/tabsvc/files/siteexports`

  For more information about file paths and how to change them, see `tsm File Paths`.

- **-id, --site-id <source-siteID>**

  Required.

  The site ID for the site you are exporting. You can get the site ID from the URL when you're signed in to the site from a web browser. For information about locating the site ID, see Prepare the source and target sites.

- **-ow, --overwrite**

  Optional.

  Overwrite an export file of the same name that already exists.

- **--request-timeout <timeout in seconds>**

  Optional.
Wait the specified amount of time for the command to finish. Default value is 1800 (30 minutes).

**tsm sites import**

This command uses the .zip file you created using `tsm sites export` to generate a set of .csv files that show how the exported source site settings will map to the new target site.

By default, the .zip file is generated and saved to the `siteexports` directory at:

```
/var/opt/tableau/tableau_server/data/tabsvc/files/siteexports
```

Before you use this command, you must copy the .zip file to the directory in which Tableau will expect it. This location is defined in the TSM `basefilepath.site_import.-exports` variable. By default, the import directory is:

```
/var/opt/tableau/tableau_server/data/tabsvc/files/siteimports
```

For more information about file paths and how to change them, see tsm File Paths.

**Note:** The `tsm sites import` and `tsm sites export` commands can leave a site in a locked state if an error occurs. To unlock a site, use the `tsm sites unlock` command.

**Synopsis**

```
tsm sites import --file <export-file.zip> --site-id <target-siteID> [options] [global options]
```

**Options**

```
-f,--file <export-file.zip>
```

Required.
Name of the .zip file created by the \texttt{tsm sites export} process, and which you must copy to the import directory. By default:

\texttt{/var/opt/tableau/tableau_server/data/tabsvc/files/siteimports}

\texttt{-id,--site-id <target-siteID>}

Required.

The site ID for the new site you are importing to (the target site). For information about locating the site ID, see \textit{Prepare the source and target sites}.

\texttt{-c,--continue-on-ignorable-errors}

Optional.

Continue site import if errors occur which can be ignored. These errors can indicate issues with the import of a specific workbook or data source.

\texttt{-k,--no-verify}

Optional.

Skip verification of mapping files.

\texttt{-m, --override-schedule.mapper <mapping-file.csv>}

Optional.

Schedule mapping file to override the normal mapping by name.

\texttt{--request-timeout <timeout in seconds>}

Optional.

Wait the specified amount of time for the command to finish. Default value is 1800 (30 minutes).
tsm sites import-verified

Specify the directory that contains an exported site’s .csv mapping files, to import to a new site. This is the final step of a site migration process.

Synopsis

tsm sites import-verified --import-job-dir <importjob-directory> --site-id <target-siteID> [options] [global options]

Options

-id, --site-id <target-siteID>

Required.

The site ID for the new site you are importing to (the target site). For information about locating the site ID, see Prepare the source and target sites.

-w, --import-job-dir <importjob-directory>

Required.

The parent of the mappings directory that contains the .csv files from the exported (source) site. The name of this parent directory includes the import id and date and time. For example:

/var/opt/tableau/tableau_server-/data/tabsvc/files/siteimports/working/import_ff00_20180102022014457

--request-timeout <timeout in seconds>

Optional.

Wait the specified amount of time for the command to finish. Default value is 1800 (30 minutes).
tsm sites unlock

Use this command to unlock a site.

Options

-id, --site-id <target-siteID>

Required.

The site ID for the site you are unlocking. For information about locating the site ID, see Prepare the source and target sites.

-d, --desired-state <state to leave unlocked site in>

Optional.

The state the site should be left in after it is unlocked. Options are "active" and "suspended". The default is "active" if not specified.

For example:

tsm sites unlock -id mysite -d suspended

--request-timeout <timeout in seconds>

Optional.

Wait the specified amount of time for the command to finish. Default value is 1800 (30 minutes).

Global options

-h, --help

Optional.

Show the command help.
Tableau Server on Linux Administrator Guide

-p, --password <password>

Required, along with -u or --username if no session is active.

Specify the password for the user specified in -u or --username.

If the password includes spaces or special characters, enclose it in quotes:

--password 'my password'

-s, --server <url_to_tsm>

Optional.

Use the specified address for Tableau Services Manager. The URL must start with https, include port 8850, and use the server name not the IP address, for example https://mytableauhost:8850. If no server is specified, https://<localhost | dnsname>:8850 is assumed.

--trust-admin-controller-cert

Optional.

Use this flag to trust the self-signed certificate on the TSM controller. For more information about certificate trust and CLI connections, see Connecting TSM clients.

-u, --username <user>

Required if no session is active, along with -p or --password.

Specify a user account. If you do not include this option, the command is run using credentials you signed in with.

**tsm start**

You can use the tsm start command to start Tableau Server. If the server is already running this command does nothing.
Synopsis

`tsm start [option][global options]`

Option

`--request-timeout <timeout in seconds>`

Optional.

Wait the specified amount of time for the command to finish. Default value is 1800 (30 minutes).

Global options

`-h, --help`

Optional.

Show the command help.

`-p, --password <password>`

Required, along with `-u` or `--username` if no session is active.

Specify the password for the user specified in `-u` or `--username`.

If the password includes spaces or special characters, enclose it in quotes:

`--password 'my password'`

`s, --server <url_to_tsm>`

Optional.

Use the specified address for Tableau Services Manager. The URL must start with `https`, include port 8850, and use the server name not the IP address, for example
Tableau Server on Linux Administrator Guide


--trust-admin-controller-cert

Optional.

Use this flag to trust the self-signed certificate on the TSM controller. For more information about certificate trust and CLI connections, see Connecting TSM clients.

-u, --username <user>

Required if no session is active, along with -p or --password.

Specify a user account. If you do not include this option, the command is run using credentials you signed in with.

**tsm status**

You can use the tsm status command to display the status of Tableau Server.

**Synopsis**

```bash
tsm status [global options]
```

**Options**

-v, --verbose

Optional.

Display status for every node in the Tableau Server cluster.

```bash
tsm status will return one of four potential statuses for a Tableau Server node:
```
The node is running without error statuses for any service.

A primary service - such as the repository - is in an error state.

One or more services is in an error state.

The node is stopped.

When running `tsm status` with the `--verbose` option, TSM will return a status for each individual service. There are four status messages:

- **is running**: The service is running.
- **status is unavailable**: The status is not returned - such as when processes are starting up.
- **is in an error state**: The process is running, but returning errors. This status indicates the process failed to install properly, or has not been configured.
- **is stopped**: The process is stopped.

### Global options

- `-h, --help`

  Optional.

  Show the command help.

- `-p, --password <password>`

  Required, along with `-u` or `--username` if no session is active.

  Specify the password for the user specified in `-u` or `--username`.

  If the password includes spaces or special characters, enclose it in quotes:

  `--password 'my password'`
Optional.

Use the specified address for Tableau Services Manager. The URL must start with https, include port 8850, and use the server name not the IP address, for example https://mytableauhost:8850. If no server is specified, https://<localhost | dnsname>:8850 is assumed.

Optional.

Use this flag to trust the self-signed certificate on the TSM controller. For more information about certificate trust and CLI connections, see Connecting TSM clients.

Required if no session is active, along with -p or --password.

Specify a user account. If you do not include this option, the command is run using credentials you signed in with.

You can use the tsm stop command to stop Tableau Server. If Tableau Server is already stopped, this command does nothing.

Option

Optional.
Wait the specified amount of time for the command to finish. Default value is 1800 (30 minutes).

Global options

-h, --help

Optional.

Show the command help.

-p, --password <password>

Required, along with -u or --username if no session is active.

Specify the password for the user specified in -u or --username.

If the password includes spaces or special characters, enclose it in quotes:

--password 'my password'

-s, --server <url_to_tsm>

Optional.

Use the specified address for Tableau Services Manager. The URL must start with https, include port 8850, and use the server name not the IP address, for example https://mytableauhost:8850. If no server is specified, https://<localhost | dnsname>:8850 is assumed.

--trust-admin-controller-cert

Optional.

Use this flag to trust the self-signed certificate on the TSM controller. For more information about certificate trust and CLI connections, see Connecting TSM clients.

-u, --username <user>
Required if no session is active, along with -p or --password.

Specify a user account. If you do not include this option, the command is run using credentials you signed in with.

tsm topology

You can use the tsm topology commands to prepare File Store nodes for safe removal or to put them back into read-write mode. You can also initiate a repository failover, get a list of nodes or ports, get the bootstrap configuration file required to add additional nodes to your cluster, and remove nodes.

- cleanup-coordination-service
- deploy-coordination-service
- failover-repository
- filestore
  - decommission
  - recommission
- list-nodes
- list-ports
- nodes
  - get-bootstrap-file
- remove-nodes
- tsm topology set-node-role
- set-ports
- set-process
- toggle-coordination-service

tsm topology cleanup-coordination-service

Use the tsm topology cleanup-coordination-service command to remove the non-production Tableau Server Coordination Service ensemble after you deploy a new ensemble. This command removes the old Coordination Service instances on all nodes in
the non-production Coordination Service ensemble and is required after you deploy a new Coordination Service ensemble. To learn more about Coordination Service ensembles, see Deploy a Coordination Service Ensemble.

Synopsis

tsm topology cleanup-coordination-service [option]
[global options]

Option

--request-timeout <timeout in seconds>

Optional.

Wait the specified amount of time for the command to finish. Default value is 2700 (45 minutes).

tsm topology deploy-coordination-service

You can use the tsm topology deploy-coordination-service command to deploy the Tableau Server Coordination Service. This command deploys a Coordination Service ensemble, which is a set of Coordination Service instances that run on specified nodes in your server cluster. To learn more about Coordination Service ensembles, including how many nodes in your cluster should have a Coordination Service instance, see Deploy a Coordination Service Ensemble.

Synopsis

tsm topology deploy-coordination-service --nodes
<nодеID,nodeID,...> [option] [global-options]

Options

-n, --nodes <nodeID,nodeID,...>

Required.
Node IDs of nodes to include in the new Coordination Service ensemble, separated by commas. You can specify 1, 3, or 5 Coordination Service nodes, depending on the total number of nodes in your cluster. For more information, see The Coordination Service Quorum.

--request-timeout <timeout in seconds>

Optional.

Wait the specified amount of time for the command to finish. Default value is 2700 (45 minutes).

tsm topology failover-repository

You can use the tsm topology failover-repository to manually initiate a repository failover from the current active repository to the second, passive repository.

The tsm topology failover-repository command is persistent. The failover repository remains the active repository until you issue the command again, or, if Tableau Server is configured for it, until automatic failover occurs. If you have a preferred active repository configured, use the --preferred option to switch back to that repository. For more information about configuring a preferred active repository, see Tableau Server Repository. If Tableau Server is configured for high availability, failover of the repository is automatic when necessary. Use the failover-repository command to manually fail over the repository.

Synopsis

tsm topology failover-repository --preferred | --target <node_id> [global options]

Options

-r, --preferred

Required if -t or --target is not used.

Use the configured preferred node as the target for repository failover.
--request-timeout <timeout in seconds>

Optional.
Wait the specified amount of time for the command to finish. Default value is 1800 (30 minutes).

-t, --target <node_id>

Required if -r or --preferred is not used.
The node id of the target node onto which failover will occur. Find the node id by using the tsm topology list-nodes command.

tsm topology filestore decommission

You must use the tsm topology filestore decommission command to prepare a file store node or nodes for safe removal. This command puts the specified nodes into read-only mode and ensures there is no unique content on the specified nodes.

If decommissioning results in a single file store node, you must use the --override option or the decommission will fail.

Synopsis

`tsm topology filestore decommission --nodes <nodeID,nodeID,...> [options] [global options]`

Options

-n, --nodes <nodeID,nodeID,...>

Required.
List of one or more nodes to decommission, specified by node ID and separated by commas.

--delete-filestore
Optional.

Forces the removal of the file store, even if it has not been decommissioned. You should only use this option if the node the file store is on is in an error state and decommissioning cannot be done. Any unique files on the node will be permanently deleted.

-o, --override

Optional.

Overrides warnings or failures that would normally occur if removing the target File Store node would reduce the number of remaining file store nodes to one.

--request-timeout <timeout in seconds>

Optional.

Wait the specified amount of time for the command to finish. Default value is 1800 (30 minutes).

tsm topology filestore recommission

Use the tsm topology filestore recommission command to revert any decommissioned nodes back to read-write mode.

Synopsis

tsm topology filestore recommission --nodes <nodeID,nodeID,...> [global options]

Options

-n, --nodes <nodeID,nodeID,...>

Required.

List of one or more nodes to recommission, specified by node ID and separated by commas.
You can use the `tsm topology nodes get-bootstrap-file` command to get the bootstrap file that is required to add a new node to the cluster.

**Important:** The bootstrap file contains a copy of the master keystore file used for encrypting the configuration secrets. We strongly recommend that you take additional measures to secure the bootstrap file using mechanisms as described in Securing secrets for import and export operations.

### Synopsis

```
tsml topology nodes get-bootstrap-file --file <path\file>.json
```

**Options**

- **-f, --file <file>**
  
  Required.

  Full path and file name where the configuration file will be saved. If a duplicate file exists it will be overwritten.

---

### tsm topology list-nodes

Display the nodes in the cluster and (optionally) the services on each node.

**Synopsis**

```
tsml topology list-nodes [options] [global options]
```

**Options**

- **-v, --verbose**
Optional.

Shows each node ID, the node role (for more information, see `set-node-role` below), the node address, and the processes on each node.

tsm topology set-node-role

Set the Backgrounder node roles. This determines the type of tasks that Backgrounder will perform on the nodes. The following node roles are useful if you have a Tableau Prep Conductor license for your Tableau Server Deployment. For more information, see Tableau Prep Conductor.

Synopsis

```
tsm topology set-node-role [options] [global options]
```

Options

- `-n, --nodes <nodeID,nodeID,...>`
  
  Required.

  List of one or more nodes to set node roles for, specified by node ID and separated by commas.

- `-r --role <all-jobs,flows,no-flows>`
  
  Required

  Sets the role for the nodes specified. The valid values for this option are:

  - all-jobs: backgrounder will perform all types of jobs.
  - flows: backgrounder will perform flow run jobs.
  - no-flows: backgrounder will not perform flow run jobs.


tsm topology list-ports

Display the ports in the cluster.
Synopsis

`tsm topology list-ports [options] [global options]`

Options

`--node-name <nodeID>`

Optional.

Specify the node to list ports for.

`--service-name`

Optional.

Specify the service to list ports for.

tsm topology remove-nodes

Remove nodes from the cluster.

To complete removal of a node, you also must run the `tsm pending-changes apply` command. Some scenarios require that you move or redeploy processes before removing nodes. See Remove a Node.

If you remove a node and want to re-add it to the cluster, you need to first run the obliterate script to clean Tableau off it, then reinstall the node using the normal process for adding a new node. For more information, see Remove Tableau Server from Your Computer and Install and Configure Additional Nodes.

**Note:** To remove a node from a cluster it must have been configured with a process at some point in the past. If you are removing a node on which you've not configured any
processes, then you must add a process on it, run `tsm pending-changes apply`, and then remove the node.

**Synopsis**

```bash
tsrm topology remove-nodes --nodes <nodeID,nodeID,...> [global options]
```

**Options**

- `-n, --nodes <nodeID,nodeID,...>`

  Required.

  Specify the node or nodes to remove. If specifying multiple nodes, separate node IDs with a comma.

**tsm topology set-ports**

Set the ports for a service instance.

**Synopsis**

```bash
tsrm topology set-ports --node-name <nodeID> --port-name <port_name> --port-value <port_value> [options] [global options]
```

**Options**

- `-i, --instance <instance_id>`

  Optional.

  Specifies the instance id of the service. Defaults to 0 (zero) if not specified.

- `-n, --node-name <nodeID>`
Required.

Specifies the node ID of the node.

`-pn, --port-name <port_name>`

Required.

The name of the port to be set, in this format: `service_name:port_type`. If no port type is specified, the primary port is assumed. For port name syntax, see Dynamically mapped ports.

`-pv, --port-value <port_value>`

Required.

The port to set.

`-r, --restart`

Optional.

Suppress the prompt for restart and restart Tableau Server when necessary.

tsm topology set-process

Set the number of instances of a process on a node. If a node already has the specified process, the number is updated to match the specified count.

You can only set one process at a time. If you specify more than one process, any process after the first one will be silently ignored.

**Note:** For a complete list of process names, see Tableau Server Processes.
Synopsis

`tsm topology set-process --count <process_count> --node <nodeID> --process <process_name> [global options]`

Options

-c, --count <process_count>

Required.

The process count (number of instances) to set.

-n, --node <nodeID>

Required.

Specifies the node ID of the node on which to set the process.

-pr, --process <process_name>

Required.

The name of the process to be set.

tsml topology toggle-coordination-service

You can use the `tsm topology toggle-coordination-service` command to switch between coordination service ensembles. To learn more about Coordination Service ensembles, see Deploy a Coordination Service Ensemble.

Synopsis

`tsm topology toggle-coordination-service [option] [global options]`
Option

--request-timeout <timeout in seconds>

Optional.

Wait the specified amount of time for the command to finish. Default value is 1800 (30 minutes).

Global options

-h, --help

Optional.

Show the command help.

-p, --password <password>

Required, along with -u or --username if no session is active.

Specify the password for the user specified in -u or --username.

If the password includes spaces or special characters, enclose it in quotes:

--password 'my password'

-s, --server <url_to_tsm>

Optional.

Use the specified address for Tableau Services Manager. The URL must start with https, include port 8850, and use the server name not the IP address, for example https://mytableauhost:8850. If no server is specified, https://<localhost | dnsname>:8850 is assumed.

--trust-admin-controller-cert

Optional.
Use this flag to trust the self-signed certificate on the TSM controller. For more information about certificate trust and CLI connections, see Connecting TSM clients.

-\texttt{u, \--username <user>}

Required if no session is active, along with \texttt{-p or \--password}.

Specify a user account. If you do not include this option, the command is run using credentials you signed in with.

\texttt{tsm user-identity-store}

You can use the \texttt{tsm user-identity-store} commands to modify the settings of the identity store for Tableau Server after the initial configuration.

The initial configuration of the identity store is part of the installation process. See Configure Initial Node Settings.

For introduction to identity store concepts, see Identity Store.

For LDAP/Active Directory configuration reference table, see LDAP Configuration Reference.

- \texttt{get-group-mappings}
- \texttt{get-user-mappings}
- \texttt{list}
- \texttt{set-connection}
- \texttt{set-group-mappings}
- \texttt{set-user-mappings}
- \texttt{verify-group-mappings}
- \texttt{verify-user-mappings}

\texttt{tsm user-identity-store get-group-mappings [options]}

Displays identity store group mappings.
Synopsis

```
tsm user-identity-store get-group-mappings [global options]
```

tsm user-identity-store get-user-mappings [options]
Displays identity store user mappings.

Synopsis

```
tsm user-identity-store get-user-mappings [global options]
```

```
tsm user-identity-store list [options]
```
Lists user-identity configuration.

Synopsis

```
tsm user-identity-store list [options] [global options]
```

Options

```
-v, --verbose
```
Optional.

Lists all configuration parameters.

```
tsm user-identity-store set-connection [options]
```
Sets identity store connection parameters.

Synopsis

```
tsm user-identity-store set-connection --kerbkeytab <kerb-keytab> [options] [global options]
```

Options

```
-b, --bind <username and password | Kerberos>
```
Optional.

Set LDAP bind type.

-d,--domain <domain>

Optional.

Domain name.

-hn,--hostname <hostname>

Optional.

The hostname of the LDAP server. You can enter a hostname or an IP address for this value. The host that you specify here will be used for user/group queries on the primary domain. In the case where user/group queries are in other domains, Tableau Server will query DNS to identify the appropriate domain controller.

-kc,--kerbconfig <kerbconfig>

Optional.

Kerberos configuration file path.

-kp,--kerbprincipal <kerbprincipal>

Optional.

Kerberos Principal.

-kt,--kerbkeytab <kerbkeytab>

Required.

Kerberos keytab file path.
-l,--port <port>
  Optional.
  Set LDAP Port value.

-lp,--ldappassword <ldappassword>
  Optional.
  LDAP Password.

-lu,--ldapusername <ldapusername>
  Optional.
  Set LDAP Username value.

-n,--nickname <nickname>
  Optional.
  NetBIOS name (nickname).

**tsm user-identity-store set-group-mappings [options]**

Sets identity store group mappings and configures LDAP directories that implement an arbitrary or custom schema.

**Synopsis**

```
  tsm user-identity-store set-group-mappings [options]
  [global options]
```

**Options**

-\b,--basefilter <groupbasefilter>
  Optional.
Set group BaseFilter value.

- cn, --classnames <group_classnames>
  Optional.
  Override default user classname values (contains "group" string) with the values you set here. You can provide multiple classnames separated by commas.

- d, --description <description>
  Optional.
  Group description.

- e, --groupemail <groupemail>
  Optional.
  Group email value.

- m, --member <member>
  Optional.
  Set the group members.

- n, --groupname <groupname>
  Optional.
  Name of the group.

tsm user-identity-store set-user-mappings [options]

Sets identity store user mappings and configures LDAP directories that implement an arbitrary or custom schema.
Synopsis

```bash
tsm user-identity-store set-user-mappings --certificate <certificate> [options] [global options]
```

Options

- `-c, --certificate <certificate>`
  - Optional.
  - Users' certificate file location.

- `-cn, --classnames <user_classnames>`
  - Optional.
  - Override default user classname values ("user" and "inetOrgPerson") with the values you set here. You can provide multiple classnames separated by commas.

- `-dn, --displayname <displayname>`
  - Optional.
  - Display name of the user.

- `-e, --email <email>`
  - Optional.
  - Users' email address.

- `-jp, --jpegphoto <jpegfile>`
  - Optional.
  - Users' jpeg image location.

- `-m, --memberof <groupname>"
Optional.

Group that the user is a member of.

-t,--thumbnail <thumbnail>

Optional.

Users' thumbnail location.

-ub,--basefilter <userbasefilter>

Optional.

Users' BaseFilter.

-uu,--ldapusername <ldapusername>

Optional.

User name.

tsm user-identity-store verify-group-mappings [options]

Validates configuration for LDAP group mapping.

Synopsis

tsm user-identity-store verify-group-mappings --verify <group_name> [global options]

Options

-v,--verify <group_name>

Optional.

Name of group to search for.
tsm user-identity-store verify-user-mappings [options]

Validates configuration for LDAP user mapping.

Synopsis

```
tsm user-identity-store verify-user-mappings --verify <user_name> [global options]
```

Options

```
-v, --verify <user_name>
```

Optional.

Name of user to search for.

Global options

```
-h, --help
```

Optional.

Show the command help.

```
-p, --password <password>
```

Required, along with -u or --username if no session is active.

Specify the password for the user specified in -u or --username.

If the password includes spaces or special characters, enclose it in quotes:

```
--password 'my password'
```

```
-s, --server <url_to_tsm>
```

Optional.
Tableau Server on Linux Administrator Guide

Use the specified address for Tableau Services Manager. The URL must start with https, include port 8850, and use the server name not the IP address, for example https://mytableauhost:8850. If no server is specified, https://<localhost | dnsname>:8850 is assumed.

--trust-admin-controller-cert

Optional.

Use this flag to trust the self-signed certificate on the TSM controller. For more information about certificate trust and CLI connections, see Connecting TSM clients.

-u, --username <user>

Required if no session is active, along with -p or --password.

Specify a user account. If you do not include this option, the command is run using credentials you signed in with.

tsm version

You can use the tsm version command to get the versions of TSM and Tableau Server.

Synopsis

tsm version [global options]

Global options

-h, --help

Optional.

Show the command help.

-p, --password <password>

Required, along with -u or --username if no session is active.
Specify the password for the user specified in -u or --username.

If the password includes spaces or special characters, enclose it in quotes:

--password 'my password'

-s, --server <url_to_tsm>

Optional.

Use the specified address for Tableau Services Manager. The URL must start with https, include port 8850, and use the server name not the IP address, for example https://mytableauhost:8850. If no server is specified, https://<localhost | dnsname>:8850 is assumed.

--trust-admin-controller-cert

Optional.

Use this flag to trust the self-signed certificate on the TSM controller. For more information about certificate trust and CLI connections, see Connecting TSM clients.

-u, --username <user>

Required if no session is active, along with -p or --password.

Specify a user account. If you do not include this option, the command is run using credentials you signed in with.

tsm File Paths

Certain tsm commands read files from or write files to default locations. These default locations are determined by basefilepath variables defined for each command. You can use tsm to view the current value of the variables, and to change the locations.
Default locations for files

During the `tsm maintenance backup, restore, send-logs, and ziplogs` processes, and the `tsm sites export and sites import` processes, Tableau Server uses default locations for the files created or used by these commands.

By default:

- **tsm maintenance commands:**
  - **backup**—The backup `.tsbak` file is generated in:
    
    /var/opt/tableau/tableau_server-
    /data/tabsvc/files/backups
  
  - **restore**—The restore process restores a backup file from:
    
    /var/opt/tableau/tableau_server-
    /data/tabsvc/files/backups
  
  - **send-logs**—The send-logs sends the logs file from:
    
    /var/opt/tableau/tableau_server-
    /data/tabsvc/files/backups
  
  - **ziplogs**—The ziplogs file is generated in:
    
    /var/opt/tableau/tableau_server/data/tabsvc/files/log-archives

- **tsm sites**
  - **export**—The export `.zip` file is generated to the following directory:
    
    /var/opt/tableau/tableau_server-
    /data/tabsvc/files/siteexports
import—During the import process, Tableau Server looks for files in:

/var/opt/tableau/tableau_server-
/data/tabsvc/files/siteimports

Get the current file location

You can see the current file location for a specific command using `tsm configuration get`:

- For tsm maintenance commands:
  - backup, restore, and send-logs:
    
    `tsm configuration get -k basefilepath.backuprestore`
  - ziplogs:
    
    `tsm configuration get -k basefilepath.log_archive`

- For tsm sites commands:
  - export
    
    `tsm configuration get -k basefilepath.site_export.-exports`
  - import
    
    `tsm configuration get -k basefilepath.site_import.-exports`

Change the current file location

You can change the expected file locations using the `tsm configuration set command` to update the `basefilepath` variables.
Changing a basefilepath variable does not move existing files from the original directory to the new directory. If you want existing backup, restore, log files, or site export or import files to reside in the new directory you specify, you must move them manually. You are responsible for creating the new location and for setting the correct permissions to allow tsm access to any files that will be placed there, and to the directory structure containing those files. For more information about permissions and tsm, see Files and Permissions in TSM.

- For tsm maintenance commands:
  - To change the backup, restore, or send-logs directory, run the following command:

    ```bash
tsm configuration set -k basefilepath.backuprestore -v "/new/directory/path"
    ```

  - To change the ziplogs directory:

    ```bash
tsm configuration set -k basefilepath.log_archive -v "/new/directory/path"
    ```

- For tsm sites commands:
  - To change the sites export directory:

    ```bash
tsm configuration set -k basefilepath.site_export.exports -v "/new/directory/path"
    ```

  - To change the sites import directory:

    ```bash
tsm configuration set -k basefilepath.site_import.exports -v "/new/directory/path"
    ```

After you change a default file location you need to do the following:
1. Apply pending changes:

    tsm pending-changes apply

2. Stop Tableau Server:

    tsm stop

3. Restart the TSM Controller (as tableau system account):

    sudo su -l tableau -c "systemctl --user restart tabadmincontroller_0.service"

4. Wait several minutes for the controller to restart. You can confirm the controller has restarted with this command:

    tsm status -v

    When you can run that command and the Tableau Server Administration Controller is listed as 'running' the controller has restarted.

5. Start Tableau Server:

    tsm start

---

**Migrate from Tabadmin to the TSM CLI**

The Tableau Services Manager (TSM) command-line interface (CLI) replaces the tabadmin CLI in Tableau Server on Linux, and in Tableau Server on Windows version 2018.2. This page maps tabadmin commands to TSM commands to help you to migrate to the TSM CLI.

To learn more about the TSM CLI, see tsm Command Line Reference.

Tabadmin commands with a corresponding TSM CLI command

The following table shows which tabadmin commands correspond to commands available in the TSM CLI.

<table>
<thead>
<tr>
<th>Command Description</th>
<th>Tabadmin Command(s)</th>
<th>Comparable TSM CLI Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activate a license</td>
<td>tabadmin activate --activate</td>
<td>tsm licenses activate</td>
</tr>
<tr>
<td>Deactivate licenses</td>
<td>tabadmin activate --return</td>
<td>tsm licenses deactivate</td>
</tr>
<tr>
<td>Activate a trial license</td>
<td>tabadmin activate --trial</td>
<td>tsm licenses activate --trial</td>
</tr>
<tr>
<td>Create a backup of the data managed by Tableau Server</td>
<td>tabadmin backup</td>
<td>tsm maintenance backup</td>
</tr>
<tr>
<td>Clear the server cache</td>
<td>tabadmin clearcache</td>
<td>tsm maintenance cleanup -r</td>
</tr>
<tr>
<td>Clean up temporary files and old log files</td>
<td>tabadmin cleanup</td>
<td>tsm maintenance cleanup</td>
</tr>
<tr>
<td>Update the</td>
<td>tabadmin configure</td>
<td>tsm pending-changes</td>
</tr>
</tbody>
</table>

A backup created using TSM does not include any server configuration data. There is no option to include server configuration data.

Note: This command was added in version 10.5.1
<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customize the server name and logos</td>
<td><code>tabadmin customize</code></td>
</tr>
<tr>
<td>Enable access to the repository</td>
<td><code>tabadmin dbpass</code></td>
</tr>
<tr>
<td>Disable access to the repository</td>
<td><code>tabadmin dbpass --disable</code></td>
</tr>
<tr>
<td>Set a file store instance to read-only mode</td>
<td><code>tabadmin decommission</code></td>
</tr>
<tr>
<td>Delete one or more Web Data Connectors (WDCs) from Tableau Server</td>
<td><code>tabadmin delete_web-dataconnector</code></td>
</tr>
<tr>
<td>Add a Web Data Connector (WDC) to Tableau Server</td>
<td><code>tabadmin import_web-dataconnector</code> and <code>tabadmin whitelist_web-dataconnector</code></td>
</tr>
</tbody>
</table>

**Note**: TSM does not support importing WDCs, instead it lets you add WDCs to a safe list (or "whitelist"). To learn more, see Web Data Connectors in Tableau Server.
## Tableau Server on Linux Administrator Guide

<table>
<thead>
<tr>
<th>Task</th>
<th>Tabadmin Command</th>
<th>Tsm Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>List Web Data Connectors (WDCs) used by Tableau Server</td>
<td><code>tabadmin list_web-dataconnectors</code></td>
<td><code>tsm data-access web-data-connectors list</code></td>
</tr>
<tr>
<td>To learn more, see Web Data Connectors in Tableau Server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Export a site from Tableau Server</td>
<td><code>tabadmin exportsite</code></td>
<td><code>tsm sites export</code></td>
</tr>
<tr>
<td>Initiate a repository failover</td>
<td><code>tabadmin failoverrepository</code></td>
<td><code>tsm topology failoverrepository</code></td>
</tr>
<tr>
<td>Get a configuration option</td>
<td><code>tabadmin get</code></td>
<td><code>tsm configuration get</code></td>
</tr>
<tr>
<td>Get the OpenID redirect URL</td>
<td><code>tabadmin get_openid_redirect_url</code></td>
<td><code>tsm authentication openid get-redirect-url</code></td>
</tr>
<tr>
<td>Import site .csv files into Tableau Server</td>
<td><code>tabadmin importsite</code></td>
<td><code>tsm sites import</code></td>
</tr>
<tr>
<td>Import a site into Tableau Server using .csv files</td>
<td><code>tabadmin importsite_verbified</code></td>
<td><code>tsm sites import-verbified</code></td>
</tr>
<tr>
<td>Display license information for Tableau Server</td>
<td><code>tabadmin licenses</code></td>
<td><code>tsm licenses list</code></td>
</tr>
<tr>
<td><strong>Note:</strong> For more information about the output of this command, see View Server Licenses.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Move a file store from</td>
<td><code>tabadmin recommission</code></td>
<td><code>tsm topology filestore recommission</code></td>
</tr>
<tr>
<td>Operation</td>
<td>Tabadmin Command</td>
<td>TSM Command</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Read-only mode to an active read/write state</td>
<td><code>tabadmin regenerate_internal_tokens</code></td>
<td><code>tsm security regenerate-internal-tokens</code></td>
</tr>
<tr>
<td>Regenerate internal security tokens</td>
<td><code>tabadmin register</code></td>
<td><code>tsm register</code></td>
</tr>
<tr>
<td>Register Tableau Server</td>
<td><code>tabadmin reindex</code></td>
<td><code>tsm maintenance reindex-search</code></td>
</tr>
<tr>
<td>Rebuild the search index for Tableau Server</td>
<td><code>tabadmin reindex</code></td>
<td></td>
</tr>
<tr>
<td>Rebuild the search index for Tableau Server</td>
<td><code>tabadmin reindex</code></td>
<td></td>
</tr>
<tr>
<td>Reset the Tableau Server administrator account</td>
<td><code>tabadmin reset</code></td>
<td><code>tsm reset</code></td>
</tr>
<tr>
<td>Reset the Tableau Server administrator account</td>
<td><code>tabadmin reset</code></td>
<td></td>
</tr>
<tr>
<td>Stop and restart all Tableau Server processes</td>
<td><code>tabadmin restart</code></td>
<td><code>tsm restart</code></td>
</tr>
<tr>
<td>Stop and restart all Tableau Server processes</td>
<td><code>tabadmin restart</code></td>
<td></td>
</tr>
<tr>
<td>Restore from a Tableau Server backup file</td>
<td><code>tabadmin restore</code></td>
<td><code>tsm maintenance restore</code></td>
</tr>
<tr>
<td>Restore from a Tableau Server backup file</td>
<td><code>tabadmin restore</code></td>
<td></td>
</tr>
<tr>
<td>Set a configuration option</td>
<td><code>tabadmin set</code></td>
<td><code>tsm configuration set</code></td>
</tr>
<tr>
<td>Set a configuration option</td>
<td><code>tabadmin set</code></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Added in version 2018.1.

The restore command does not restore any server configuration data. This is true whether you are using a backup created with TSM or a backup created with tabadmin.
Tabadmin commands with no corresponding TSM CLI command

The following table lists the tabadmin commands for which a comparable TSM CLI command is not available.

<table>
<thead>
<tr>
<th>Command Description</th>
<th>Tabadmin Command</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add or remove a user from the system administrator group</td>
<td>tabadmin administrator</td>
<td>You can use the Tableau Server REST API Add User to Group and Remove User from Group methods to add or remove a user from the system administrator group.</td>
</tr>
<tr>
<td>Task</td>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Create a new key to encrypt sensitive information stored in the repository</td>
<td><code>tabadmin assetkeys</code></td>
<td>Use the <code>tsm security regenerate-internal-tokens</code> command to create or regenerate secrets and master keys.</td>
</tr>
<tr>
<td>Specify whether Tableau Server starts at system start-up time</td>
<td><code>tabadmin autostart</code></td>
<td>Tableau Server returns to the state it was in prior to a system restart. If it was running, it will restart. If it was stopped it will be stopped after the system starts.</td>
</tr>
<tr>
<td>Identify a second server node for backup</td>
<td><code>tabadmin failoverprimary</code></td>
<td>TSM does not have primary nodes, so a TSM equivalent to this command is not needed.</td>
</tr>
<tr>
<td>Manage credentials for delegated data access on Tableau Server</td>
<td><code>tabadmin manage_global_credentials</code></td>
<td>We recommend that you use Kerberos delegation to Apache Impala for global credential management. To learn more, see Kerberos and Enable Kerberos Delegation for Hive/Impala in the Tableau Community.</td>
</tr>
<tr>
<td>Reset the password for a Tableau Server account</td>
<td><code>tabadmin passwd</code></td>
<td>If your server uses local authentication, you can use the Tableau Server REST API Update User method to reset the password for a user account.</td>
</tr>
<tr>
<td>Reset binding between Tableau Server user ID and Open ID Connect identity profile</td>
<td><code>tabadmin reset_openid_sub</code></td>
<td></td>
</tr>
</tbody>
</table>
Determine whether your environment meets the minimum requirements to run Tableau Server

Verify that a backup of the Tableau Server repository will restore successfully

Prepare VizQL processes for fast load times after a Tableau Server restart

Entity Definitions and Templates

Configuration File Example

This article provides an example of a complete JSON configuration file, with gatewaySettings and identityStore entities specified. In addition, a configuration key sets the gateway timeout to 900 seconds.
Your configuration file will look different depending on the options you need to set.

You might set multiple .json configuration files during installation. To set the values for each file in Tableau Server, you run the following command, once for each configuration file:

```bash
tsm settings import -f path-to-file.json
```

After you set the configuration files, run tsm pending-changes apply to apply the changes from all of the .json files you’ve set.

```json
{
  "configEntities": {
    "gatewaySettings": {
      "_type": "gatewaySettingsType",
      "port": 80,
      "firewallOpeningEnabled": true,
      "sslRedirectEnabled": true,
      "publicHost": "localhost",
      "publicPort": 80
    },
    "identityStore": {
      "_type": "identityStoreType",
      "type": "local",
      "domain": "example.lan",
      "nickname": "EXAMPLE"
    }
  },
  "configKeys": {
    "gateway.timeout": "900"
  }
}
```

**Entities vs keys**

As shown in the example above, there are two classes of configuration parameters: configEntities and configKeys.
configEntities

Certain types of configuration are done through entity sets that map to specific scenarios, such as the identity store and gateway configurations. When you pass a set of configEntities with the `tsm settings import -f path-to-file.json` command, TSM validates the configuration. If values passed are invalid, TSM will provide an error. This enables you to make changes during the configuration process, rather than experience a configuration failure at initialization or run time.

Entities can be set only by including a configEntities block in a .json file.

**Important:** All files that are referenced in configEntities must be located on the local computer. Do not specify UNC paths.

cfgKeys

Entities cover only a small portion of the configuration values that can be set. Hundreds of keys correspond to parameters stored in .yaml files. Tableau Server uses these parameters to store all of the configuration information for all services.

You can set individual keys with the `tsm configuration` command. But during deployment, setting them along with other configuration scenarios in JSON files, as shown above, is more convenient.

Unlike configEntities, configKeys are not validated.

**Note:** We do not recommend setting parameters that are not documented in tsm configuration set Options.

gatewaySettings Entity

You must configure the gateway settings for the Tableau Server computer.
Use the configuration file template below to create a json file. After you have filled in the options with the appropriate values, pass the json file and apply settings with the following commands:

```bash
tsm settings import -f /path/to/file.json

tsm pending-changes apply
```

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

Gateway settings

The gateway settings in the template below specify the HTTP settings for Tableau Server. We recommend using SSL/TLS. Tableau Server is hard-coded to use port 443 for SSL/TLS. Therefore, if you enable SSL, you do not need to update the `gatewaySettings` entity.

Configuration template

Use this template to configure the gateway settings.

All entity options are case sensitive.

For more explanation about configuration files, entities, and keys see Configuration File Example.

```json
{
   "configEntities": {
      "gatewaySettings": {
         "_type": "gatewaySettingsType",
         "port": 80,
         "sslRedirectEnabled": true,
         "publicHost": "localhost"
      }
   }
}
```
This table includes all of the options that can be included with the "gatewaySettings" entity set.

_type

Required.

**Value:** "gatewaySettingsType"

Do not change.

_port

Specifies HTTP port. Default is port 80.

_sslRedirectEnabled

**Options:** true or false.

_publicHost

Specifies host name for http/s service.

_trustedIPs

Specifies trusted IP addresses that communicate with Tableau Server. Trusted IP addresses include upstream proxy servers and servers that are used for trusted authentication with Tableau Server. See Configuring Proxies for Tableau Server and Add Trusted IP Addresses or Host Names to Tableau Server.

If you are running Tableau Server in a cluster then all other nodes of the cluster will automatically be included in the corresponding configuration file that this entity
updates. Therefore, if you specify a new value for trustedIPs, then you must include the IP addresses for the other nodes in the value.

This option takes a list of strings, which requires passing each IP or host in quotes, separated by a comma (no space) and within brackets. For example:

["192.168.1.101","192.168.1.102","192.168.1.103"] or ["web-serv1","webserv2","webserv3"].

trustedHosts

Specifies trusted IP addresses that communicate with Tableau Server. Typically, this value contains a list of upstream proxy servers. The values in trustedHosts are used to determine client request targets.

If you are running Tableau Server in a cluster then all other nodes of the cluster will automatically be included in the corresponding configuration file that this entity updates. Therefore, if you specify a new value for trustedIPs, then you must include the IP addresses for the other nodes in the value.

This option takes a list of strings, which requires passing each IP or host in quotes, separated by a comma (no space) and within brackets. For example:

["192.168.1.101","192.168.1.102","192.168.1.103"] or ["web-serv1","webserv2","webserv3"].

identityStore Entity

Tableau Server requires an identity store to store user and group information. Review Authentication and Identity Store topics before configuring the identity store for the first time. After you have installed the identity store on Tableau Server, you cannot change it without reinstalling the server.

All entity options are case sensitive.

Before you begin

Review the following information:
If you plan to enable OpenID Connect then you must configure the local identity store.

If you will not be using the local identity store, then you will be using some version of LDAP. In this case, work with your directory/LDAP administrator to configure Tableau Server for your LDAP schema and bind requirements.

Tableau Server configuration is optimized for Active Directory. If you are installing into Active Directory, we recommend configuring the identity store with Configure Initial Node Settings. Alternatively, if you are configuring with TSM CLI, use the LDAP - Active Directory template in this topic to configure identity store. For a full accounting of LDAP configuration options, see LDAP Configuration Reference.

LDAP bind is independent of user authentication. For example, you can configure Tableau Server to use simple bind to authenticate to the LDAP directory and then configure Tableau Server to authenticate users with Kerberos after installation.

Do not connect to LDAP with simple bind over a unsecured connection. We recommend LDAPS for simple bind. See LDAP over SSL.

To use Kerberos authentication for the Tableau Server service, then you'll need a keytab file for GSSAPI bind, as described in the sections below. See also, Understanding Keytab Requirements. In the context of Kerberos, GSSAPI bind is all you need during the base installation of Tableau Server. After you install the server, you can then configure Kerberos for user authentication and Kerberos delegation to data sources.

In this topic, we make the distinction between LDAP (the protocol for connecting to directory services) and an LDAP server (an implementation of a directory service). For example, slapd is an LDAP server that is part of the OpenLDAP project.

We recommend validating the LDAP configuration before initializing the server, see Configure Initial Node Settings.
Use one of the configuration file templates below to create a json file. After you have filled in the options with the appropriate values, pass the json file and apply settings with the following commands:

```
tsm settings import -f path-to-file.json

tsm pending-changes apply
```

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

**Configuration templates**

Select an identity store configuration template to edit:

- Local
- LDAP - Active Directory
- OpenLDAP - GSSAPI Bind
- OpenLDAP - Simple Bind

For more explanation about configuration files, entities, and keys see Configuration File Example.

Consider using the Tableau Identity Store Configuration Tool to generate your LDAP json configuration file. The tool itself is not supported by Tableau. However, using a JSON file created by the tool instead of creating a file manually does not change the supported status of your server.

Local

Configure local as the identity store type if your organization does not already have an Active Directory or LDAP server for user authentication. When you select local as the identity store type, you use Tableau Server to create and manage users.
Important

The LDAP configuration templates below are examples. The templates, as presented, will not configure LDAP connectivity in your organization. You must work with your directory administrator to edit the LDAP template values for a successful deployment.

Additionally, all files that are referenced in configEntities must be located on the local computer. Do not specify UNC paths.

LDAP - Active Directory

Configure this option to connect to Active Directory with GSSAPI (Kerberos) bind. Tableau Server uses the LDAP protocol to connect to Active Directory. GSSAPI (Kerberos) bind is used to authenticate Tableau Server service to Active Directory. Tableau Server includes support for Active Directory schema. Therefore, if you set the "directoryServiceType" option to "activedirectory" then you do not need to provide schema info in the "identityStoreSchemaType" option.

If you are installing Tableau Server for Linux into Active Directory, and the computer where you are installing Tableau Server is already joined to the domain, then the computer will already have a Kerberos configuration file and a keytab file. Strictly speaking, you can use these files for GSSAPI bind, but we don’t recommend using them. Instead, contact your Active Directory administrator and request a keytab specifically for the Tableau Server service.
We recommend binding to Active Directory with GSSAPI. However, you can connect with simple bind and LDAPS. To connect with simple bind, change `bind` to `simple`, remove the three Kerberos entities, and add the `port/sslPort`, `username`, and `password` options. The following example shows Active Directory with simple bind json.

```json
{
  "configEntities":{
    "identityStore": {
      "_type": "identityStoreType",
      "type": "activedirectory",
      "domain": "your-domain.lan",
      "nickname": "YOUR-DOMAIN-NICKNAME",
      "directoryServiceType": "activedirectory",
      "bind": "simple",
      "hostname": "optional-ldap-server",
      "sslPort": "636",
      "username": "username",
      "password": "password"
    }
  }
}
```
OpenLDAP - GSSAPI bind

Use the template below to configure OpenLDAP with GSSAPI bind. Do not use this template if your organization is running Active Directory. If you are installing into Active Directory, use the template above, LDAP - Active Directory.

In most cases, organizations that use OpenLDAP with GSSAPI (Kerberos) will use a keytab file to store credentials. In the following example, a keytab file is used for authentication credentials.

However, you can provide credentials through the `username` and `password` entities.

You can also specify both a keytab and a username and password pair. In this case, Tableau Server will attempt to use the keytab, but if authentication fails for any reason it will fallback and use the username and password credentials.

```json
{
    "configEntities": {
        "identityStore": {
            "_type": "identityStoreType",
            "type": "activedirectory",
            "domain": "your-domain.lan",
            "nickname": "YOUR-DOMAIN-NICKNAME",
            "directoryServiceType": "openldap",
            "bind": "gssapi",
            "kerberosKeytab": "<path to local key tab file>",
            "kerberosConfig": "/etc/krb5.conf",
            "kerberosPrincipal": "your-principal@YOUR.DOMAIN",
            "identityStoreSchemaType": {
                "userBaseFilter": "(objectClass=inetOrgPerson)",
                "userUsername": "user",
                "userDisplayName": "displayname",
            }
```
"userEmail": "email",
"userCertificate": "certificate",
"userThumbnail": "thumbnail",
"userJpegPhoto": "photo",
"groupBaseFilter": "(objectClass=groupofNames)",
"groupName": "groupname",
"groupEmail": "groupemail",
"groupDescription": "groupdescription",
"member": "member",
"distinguishedNameAttribute": "",
"serverSideSorting": "",
"rangeRetrieval": "",
"userClassNames": ["inetOrgPerson","someClass2"],
"groupClassNames": ["groupOfUniqueNames1","groupOfUniqueNames2"]
}
}
}

OpenLDAP - Simple bind
{
  "configEntities": {
    "identityStore": {
      "_type": "identityStoreType",
      "type": "activedirectory",
      "domain": "my.root",
      "nickname": "",
      "hostname": "optional-ldap-server",
      "port": "389",
      "directoryServiceType": "openldap",
      "bind": "simple",
      "username": "cn=username,dc=your,dc=domain",
    }
  }
}
"password": "password",
"identityStoreSchemaType": {
  "userBaseFilter": "(objectClass/inetOrgPerson)",
  "userUsername": "user",
  "userDisplayName": "displayname",
  "userEmail": "email",
  "userCertificate": "certificate",
  "userThumbnail": "thumbnail",
  "userJpegPhoto": "photo",
  "groupBaseFilter": "(objectClass=groupofNames)",
  "groupName": "groupname",
  "groupEmail": "groupemail",
  "groupDescription": "groupdescription",
  "member": "member",
  "distinguishedNameAttribute": "",
  "serverSideSorting": "",
  "rangeRetrieval": "",
  "userClassNames": ["inetOrgPerson","someClass2"],
  "groupClassNames": ["groupOfUniqueNames1","groupOfUniqueNames2"]
}
}
}

Configuration template reference

Shared identity store options

type
  Where you want to store user identity information. Either local or activedirectory.
  (If you want to connect to any LDAP server, select activedirectory.)

domain
The domain of the computer where you installed Tableau Server.

**nickname**

The nickname of the domain. This is also referred to as the NetBIOS name in Windows environments. The **nickname** option is required for all LDAP entities. If your organization does not require a nickname/NetBIOS, then pass a blank key, for example: "nickname": "".

**LDAP GSSAPI bind options**

**directoryservicetype**

The type of directory service that you want to connect to. Either `activedirectory` or `openldap`.

**kerberosConfig**

The path to the Kerberos configuration file on the local computer. If you are installing into Active Directory, we don't recommend using the existing Kerberos configuration file or keytab file that may already be on the domain-joined computer. See Identity Store.

**kerberosKeytab**

The path to the Kerberos keytab file on the local computer. It is recommended that you create a keytab file with keys specifically for Tableau Server service and that you do not share the keytab file with other applications on the computer. For example, on Linux, you might place the keytab file in the `/var/opt/tableau/keytab` directory.

**kerberosPrincipal**

The service principal name for Tableau Server on the host machine. The keytab must have permission for this principal. Do not use the existing system keytab at `/etc/krb5.keytab`. Rather, we recommend that you register a new service principal name. To see principals in a given keytab, run the `klist -k` command. See Understanding Keytab Requirements.
LDAP simple bind options

directoryservicetype
The type of directory service that you want to connect to. Either `activedirectory` or `openldap`.

hostname
The hostname of the LDAP server. You can enter a hostname or an IP address for this value. The host that you specify here will be used for user/group queries on the primary domain. In the case where user/group queries are in other domains, Tableau Server will query DNS to identify the appropriate domain controller.

port
Use this option to specify the non-secure port of the LDAP server. Plaintext is usually 389.

sslPort
Use this option to specify the secure port of the LDAP server. We recommend secure LDAP for simple bind. LDAPS is usually port 636.

username
The user name that you want to use to connect to the directory service. The account that you specify must have permission to query the directory service. For Active Directory, enter the username, for example, `jsmith`. For LDAP servers, enter the distinguished name (DN) of the user that you want to use to connect. For example, you might enter `cn=username,dc=your-local-domain,dc=lan`.

password
The password of the user that you want to use to connect to the LDAP server.

Shared LDAP options

The following options can be set for generic LDAP, OpenLDAP, or Active Directory implementations.
bind

The way that you want to authentication communication from the Tableau Server service to the LDAP directory service. Enter gssapi for GSSAPI (Kerberos).

domain

In Windows Active Directory environments, specify the domain where Tableau Server is installed, for example, "example.lan". In LDAP directories, specify the root domain name in the same format. For example, if your root is "dc=my,dc=root", specify "my.root".

root

LDAP only. Do not specify for Active Directory.
If you do not use a dc component in the LDAP root or you want to specify a more complex root you need to set the LDAP root. Use the "o=my,u=root" format. For example, for the domain example.lan, the root would be "o=example,u=lan".

membersRetrievalPageSize

This option determines the maximum number of results returned by an LDAP query. For example, consider a scenario where Tableau Server is importing an LDAP group that contains 50,000 users. Attempting to import such a large number of users in a single operation is not a best practice. When this option is set to 1500, Tableau Server imports the first 1500 users in the first response. After those users are processed, Tableau Server requests the next 1500 users from the LDAP server, and so forth. We recommend that you modify this option only to accommodate the requirements of your LDAP server.

identityStoreSchemaType options

If you configure an LDAP connection to an LDAP server, you can enter schema information specific to your LDAP server in the identityStoreSchemaType object. If you are connecting to Active Directory ("directoryServiceType": "activedirectory"), then do not configure these options.

userBaseFilter
The filter that you want to use for users of Tableau Server. For example, you might specify an object class attribute and an organization unit attribute.

userUsername
The attribute that corresponds to user names on your LDAP server.

userDisplayName
The attribute that corresponds to user display names on your LDAP server.

userEmail
The attribute that corresponds to user email addresses on your LDAP server.

userCertificate
The attribute that corresponds to user certificates on your LDAP server.

userThumbnail
The attribute that corresponds to user thumbnail images on your LDAP server.

userJpegPhoto
The attribute that corresponds to user profile images on your LDAP server.

groupBaseFilter
The filter that you want to use for groups of users of Tableau Server. For example, you might specify an object class attribute and an organization unit attribute.

groupName
The attribute that corresponds to group names on your LDAP server.

groupEmail
The attribute that corresponds to group email addresses on your LDAP server.
The attribute that corresponds to group descriptions on your LDAP server.

**member**
The attribute that describes the list of users in a group.

**distinguishedNameAttribute**
The attribute that stores the distinguished names of users. This attribute is optional, but it greatly improves the performance of LDAP queries.

**serverSideSorting**
Whether the LDAP server is configured for server-side sorting of query results. If your LDAP server supports server-side sorting, set this option to true. If you are unsure whether your LDAP server supports this, enter false, as misconfiguration may cause errors.

**rangeRetrieval**
Whether the LDAP server is configured to return a range of query results for a request. This means that groups with many users will be requested in small sets instead of all at once. LDAP servers that support range retrieval will perform better for large queries. If your LDAP server supports range retrieval, set this option to true. If you are unsure whether your LDAP server supports range retrieval, enter false, as misconfiguration may cause errors.

**groupClassNames**
By default Tableau Server looks for LDAP group object classes containing the string "group". If your LDAP group objects do not fit the default class name, override the default by setting this value. You can provide multipleclassnames separated by commas. This option takes a list of strings, which requires passing each class in quotes, separated by a comma (no space) and within brackets. For example: ["basegroup","othergroup"].

**userClassNames**
By default Tableau Server looks for LDAP user object classes containing the string "user" and "inetOrgPerson". If your LDAP user objects do not use these default class
names, override the default by setting this value. You can provide multiple classnames separated by commas. This option takes a list of strings, which requires passing each class in quotes, separated by a comma (no space) and within brackets. For example: 
["userclass1","userclass2"].

**kerberosSettings Entity**

Before you configure Kerberos authentication, review Kerberos Requirements.

Use the configuration file template below to create a json file. After you have filled in the options with the appropriate values, pass the json file and apply settings with the following commands:

```bash
  tsm settings import -f /path/to/file.json
  tsm pending-changes apply
```

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see tsm pending-changes apply.

**Configuration template**

Use this template to configure Kerberos settings.

All entity options are case sensitive.

For more explanation about configuration files, entities, and keys see Configuration File Example.

After you have finished with the initial configuration of Kerberos authentication, use the tsm authentication kerberos `<commands>` sub-category to set additional values.

```
```
"kerberosSettings": {
  "_type": "kerberosSettingsType",
  "enabled": "true",
  "keytabFile": "/path/to/keytab_file"
}
}

Configuration file reference

The following list includes all of the options that can be included with the "kerberosSettings" entity set.

Option | Value
---|---
enabled | Options: true or false.
          | Enables Kerberos authentication.
keytabFile | Required.
            | Path to valid Kerberos keytab file.
dBClasses | Comma-separated list of database classes for global credentials. May be required for connecting to Cloudera data sources.

**mutualSSLSettings Entity**

Before you configure mutual SSL, review Configure SSL for External HTTP Traffic to and from Tableau Server.
The **mutualSSLSettings** entity combines both SSL and mutual SSL configuration. Mutual SSL requires that external SSL has been enabled and properly configured.

The TSM entities use JSON and key-value pairs. Use the configuration file template below to create a .json file. Provide values for the appropriate keys for your environment, and then pass the .json file to Tableau Server with the following commands:

```shell
 tsm settings import -f <path-to-file.json>

 tsm pending-changes apply
```

The **pending-changes apply** command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the **--ignore-prompt** option, but this does not change the restart behavior. For more information, see **tsm pending-changes apply**.

**Configuration template**

Use this template to configure mutual SSL settings.

All entity options are case sensitive.

For more explanation about configuration files, entities, and keys see Configuration File Example.

```json
{
  "configEntities": {
    "mutualSSLSettings": {
      "_type": "mutualSSLSettingsType",
      "sslEnabled": true,
      "proxyLogin": false,
      "clientCertRequired": true,
      "caCertFile": "required",
      "keyFileName": "required",
```

Tableau Server on Linux Administrator Guide

Tableau Software  Version: 2019.1  1235
"keyPassphrase": "",
"chainFile": "",
"revocationFile": "",
"redirect": false,
"fallbackToPassword": true,
"protocols": "",
"cipherSuite": "",
"forceHttpsForPublicEmbed": false
}
}
}

Configuration file reference

sslEnabled

Enable SSL. This is a prerequisite to enabling mutual SSL.

clientCertRequired (MutualSSL)

Set to true to enable mutual SSL authentication. Set to false to disable.

cacertFile (MutualSSL)

Required.

Specify the CA-issued certificate file for two-way SSL. The file path must be readable by Tableau Server.

certFileName

Specify the file that contains the concatenation of PEM encoded CA certificates that form the certificate chain for the server certificate.
Alternatively the referenced file can be the same as caCertFile when the CA certificates are directly appended to the server certificate for convenience.

**keyFileName**

If the key is not combined with the certificate, use this configuration key to point to the key file. If you have both an RSA and a DSA private key, you can configure both in parallel (for example, to also allow the use of DSA ciphers).

**keyPassphrase**

Optional. Passphrase for the certificate file. The passphrase you enter will be encrypted while at rest.

**Note:** If you create a certificate key file with a passphrase, you cannot reuse the SSL certificate key for SAML.

**revocationFile**

Specifies the file path for an SSL CA Certificate Revocation List (.crl) file.

**Redirect**

Default: true. Specifies whether Tableau Server should redirect http requests as https requests to the appropriate endpoint.

**clientCertMapping (MutualSSL)**

Specifies the method for retrieving the user name from the certificate.

**Accepted values:** ldap, upn, cn

- For a server using local authentication, the default setting is upn (User Principal Name).
- When Tableau Server authentication is configured for Active Directory (AD), the
default is `ldap` (Lightweight Directory Access Protocol). This tells the server to go to AD to validate the user, and it ignores the names inside the certificate.

You can set `cn` for either authentication type to use the CN in the Subject DN in the certificate.

For more information, see Mapping a Client Certificate to a User During Mutual Authentication.

`fallbackToPassword` (MutualSSL)

Set to true to give users the option to sign in to Tableau Server through their user name and password if mutual SSL authentication fails. Set to false to disallow this fallback option.

`protocols`

List the Transport Layer Security (TLS) protocol versions you want to allow or disallow.

**Default value:** "all -SSLv2 -SSLv3"

However, we recommend the using the following setting:

"all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1"

For more information, see tsm security external-ssl enable. For general information, see the Apache online documentation.

`cipherSuite`

List ciphers to allow or disallow for SSL.

**Default value:** "HIGH:MEDIUM:!aNULL:!MD5:!RC4"

However, we recommend that you add Triple-DES to the list of disabled cipher suites, and set this key to:

"HIGH:MEDIUM:!aNULL:!MD5:!RC4:!3DES"
proxyLogin

Default: false. Indicates that Tableau Server uses a proxy for SSL on sign-in only. It controls the protocol the server reports to Tableau Desktop for sign-in APIs.

forceHTTPForPublicEmbed

Default value: false. Forces the code for embedded views to use SSL.

openIDSettings Entity

Before you configure OpenID authentication, review Requirements for Using OpenID Connect.

Use the configuration file template below to create a json file. After you have filled in the options with the appropriate values, pass the json file and apply settings with the following commands:

```
  tsm settings import -f path-to-file.json
  tsm pending-changes apply
```

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

Configuration template

Use this template to configure OpenID settings.

All entity options are case sensitive.
For more explanation about configuration files, entities, and keys see Configuration File Example.

After you have finished with the initial configuration of OIDC, use the tsm authentication openid <commands> sub-category to set additional values.

```
{
   "configEntities": {
      "openIDSettings": {
         "_type": "openIDSettingsType",
         "enabled": true,
         "clientId": "required",
         "clientSecret": "required",
         "configURL": "required if staticFile value is not set",
         "staticFile": "required if configURL value is not set",
         "externalURL": "required"
      }
   }
}
```

Configuration file reference

The following list includes all of the options that can be included with the "openIDSettings" entity set.

_type

Required.

Do not change.

enabled

Required.

Set to true.
clientId

Required.

Specifies the provider client ID that your IdP has assigned to your application. For example, "laakjwdlnaolodjkw".

clientSecret

Required.

Specifies the provider client secret. This is a token that is used by Tableau to verify the authenticity of the response from the IdP. This value is a secret and should be kept securely.

For example, "fwahfkjaw72123=".

cfgURL

Required.

Specifies provider configuration URL. If you do not specify a configuration URL, then delete this option and specify a path and file name for staticFile instead.

staticFile

Required.

Specifies the local path to the static OIDC discovery JSON document. If you do not specify a static file, then delete this option and specify a url for configURL instead.

e externalURL

Required.

The URL of your server. This is typically is the public name of your server, such as http://example.tableau.com.

connectionTimeout
Optional.

Specifies connection timeout span in seconds. Default is 10.

readTimeout

Optional.

Specifies read timeout span in seconds. Default is 30.

ignoreDomain

Set this to true if the following are true:

- You are using email addresses as usernames in Tableau Server
- You have provisioned users in the IdP with multiple domain names
- You want to ignore the domain name portion of the email claim from the IdP

Before you proceed, review the user names that will be used as a result of setting this option to true. User name conflicts may occur. In the case of a user name conflict, the risk of information disclosure is high. See Requirements for Using OpenID Connect.

ignoreJWK

Set this to true if your IdP does not support JWK validation. In this case, we recommend authenticating communication with your IdP using mutual TLS or another network layer security protocol. Default is false.

customScope

Specifies a custom scope user-related value that you can use to query the IdP. See Requirements for Using OpenID Connect.

idClaim

Change this value if your IdP does not use the sub claim to uniquely identify users in the ID token. The IdP claim that you specify should contain a single, unique string.
usernameClaim

Change this value to the IdP claim that your organization will use to match user names as stored in Tableau Server.

clientAuthentication

Specifies custom client authentication method for OpenID Connect.

To configure Tableau Server to use the Salesforce IdP, set this value to client_secret_post.

iFramedIDPEnabled

Set to true to allow IdP displayed in an iFrame. The IdP must disable clickjack protection to allow iFrame presentation.

samlSettings Entity

This article contains a template and reference for configuring server-wide SAML on Tableau Server, using a configuration file with keys and values for the samlSettings entity. This information supplements the SAML configuration steps in Configure Server-Wide SAML.

To create a SAML configuration template and apply it to Tableau Server, you complete the following steps:

1. Review the following two sections that describe the template and how it’s structured (Template categories and definitions and samlSettings configuration template).

2. Paste the JSON code shown in the template into a new text file, and save it using a .json extension.

3. Use the SAML configuration entity reference to help you provide values where required.

4. Add optional key/value pairs specific to your environment. For example, if your SAML
certificate key file requires a passphrase, you will need to specify the password in the
wgserver.saml.key.passphrase parameter using the tsm configuration set command.

5. Pass the configuration file to Tableau Server.

Template categories and definitions

The template uses placeholders for each key value. These placeholders are categorized as follows:

- **Required**: Attributes with the "required" value must be replaced with valid data before you run the configuration command. Review the configuration file reference for valid values.

- **Hard-coded**: Attribute names that are prepended with an underscore (_), for example "_type" hold hard-coded values. Do not change these values.

- **Default values**: Attributes that are set to a value that is not "required" are default values. These are required attributes that you can change as appropriate for your environment.

- **Empty sets**: Values that are empty ("") can be passed as they are, or you can provide a value for your installation.

All entity options are case sensitive.

samlSettings configuration template

Paste this code into a text file and customize it for your environment, using the reference below.

```json
{
  "configEntities": {
    "samlSettings": {
```
SAML configuration entity reference

The following table includes all of the options you can include with the "samlSettings" entity set.

idpMetadataFile

Required. The path and file name for the XML file generated by the IdP. The XML metadata must include the user name attribute (assertion).

If you completed the steps described in Configure Server-Wide SAML the value you enter here would be:

/var/opt/tableau/tableau_server/data/saml/<metadata-file.xml>

enabled

true | false

Required. Indicates whether SAML authentication is enabled and can be configured on the server.
**returnURL**

The SAML return URL configured in the IdP. This is typically the external URL that Tableau Server users enter in their browser to access the server, such as http://tableau_server.

**Notes**

- http://localhost does not work for an external server.
- Adding a trailing slash to the URL (http://tableau-server/) is not supported.

**entityId**

Required. IdP entity ID value.

Typically the same as the Tableau Server return URL. The entity ID that you enter is used as a base for generating site-specific entity IDs. For example, if you enter "http://tableau-server", an individual site configured for SAML might display an entity ID something like the following:

http://tableau-server-/saml/service/public/sp/metadata?alias=48957410-9396-430a-967c-75b-db6e002a0

**certFile**

Enter the location and file name of the x509 certificate (.crt) file for SAML. For example:

/var/opt/tableau/tableau_server/data/saml/<file.crt>

For more information, see SAML Requirements and Configure Server-Wide SAML.

**keyFile**

Specify the location of the RSA or DSA private key (.key) file that accompanies the certificate file and is not password protected. For example:
For more information, see SAML Requirements and Configure Server-Wide SAML.

idpDomainAttribute

Optional. This value is used when Tableau Server includes user accounts from multiple domains. Specify the fully qualified domain name (FQDN) of the domain you want to be the default. For example tableauserver.mycompany.com.

If you do not provide a value for this key, the value used depends on the Tableau Server user authentication setting:

- For local authentication, the value local is used.
- For Active Directory, Tableau uses the FQDN from the configuration setting wgserver.domain.default.

To get the value for wgserver.domain.default, you can run the following command:

```bash
tsm configuration get --key wgserver.domain.default
```

idpUsernameAttribute

Required. In the IdP metadata, find the attribute that is used to specify user name values, and enter the name of that attribute. For example, username.

idpEmailAttribute

Optional. In the IdP metadata, the name of the attribute the IdP uses to specify users’ email addresses.

idpDisplayNameAttribute

Optional. In the IdP metadata, the name of the attribute the IdP uses to specify users’ display names.
idpAttributeUseDefaultDomain

true | false

Optional. The default value is true for a single domain or for multiple domains when you do not specify a value for idpDomainAttribute. The default value is false if you specify a non-default value for idpDomainAttribute.

desktopNoSAML

true | false

Allow users to use SAML authentication when they sign in from Tableau Desktop.

By default this is not set, so the effective behavior is equivalent to setting it to false. If single sign-on from Tableau client applications does not work with your IdP, you can set this to true to disable SAML authentication through Tableau Desktop.

appNoSAML

true | false

Allow using SAML to sign in from older versions of Tableau Mobile app. Devices running Tableau Mobile app version 19.225.1731 and higher ignore this option. To disable devices running Tableau Mobile app version 19.225.1731 and higher, disable SAML as a client login option on Tableau Server.

logoutEnabled

true | false

Specifies whether the logout UI option is displayed for users who have logged on with SAML. The default is true. This setting applies only if SAML authentication is enabled for the server.

logoutUrl

Enter the URL to redirect to after users sign out of the server. By default this is the
Tableau Server sign-in page. You can specify an absolute or a relative URL.

maxAuthenticationAge

Specifies the maximum number of seconds allowed between a user's authentication and processing of the AuthNResponse message. The default value is 7200 (2 hours).

maxAssertionTime

Specifies the maximum number of seconds, from creation, that a SAML assertion is usable. Default value is 3000 (50 minutes).

sha256Enabled

true | false

Indicates whether the SAML certificate is an SHA-2 (256 or 512 bit) certificate. Default value is false. If you use the same certificate for SAML as you do for SSL, you will most likely set this to true.

signRequests

true | false

Default value is true.

Tableau Server requires a certificate-key pair to sign the request that is sent to the IdP. This reduces the threat of a man-in-the-middle attack given the difficulty of spoofing a signed request. Additionally, Tableau Server verifies that the AuthNResponse it receives from the trusted IdP. Signed requests are not always necessary for all IdPs. We recommend signing requests to ensure the most secure option when configuring SAML. To disable signed requests, set this option to false.

iFramedIdpEnabled

true | false
Default value is false, meaning that when users select the sign-in button on an embedded view, the IdP’s sign-in form opens in a pop-up window.

When you set it to true, and a server SAML user who is already signed in navigates to a web page with an embedded view, the user will not need to sign in to see the view.

You can set this to true only if the IdP supports signing in within an iframe. The iframe option is less secure than using a pop-up, so not all IdPs support it. If the IdP sign-in page implements clickjack protection, as most do, the sign-in page cannot display in an iframe, and the user cannot sign in.

If your IdP does support signing in via an iframe, you might need to enable it explicitly. However, even if you can use this option, it disables Tableau Server clickjack protection for SAML, so it still presents a security risk.

**port**

The port that handles SAML authentication traffic.

Default value: 80

If your server is configured for SSL (recommended), set this to 443.

**singleLogoutSupported**

true | false

Enable or disable SAML single logout (SLO). This value is not set by default, so effectively it behaves as if the value were set to false. To set it to true, the IdP must support SLO.

**siteSpecific**

enabled | disabled

Specifies whether the server is configured to support site-specific SAML authentication, in which you can configure sites to use different IdPs or IdP applications. Set to disabled by default. If you set to enabled, you then configure a
Pass the configuration file to Tableau Server

After you have provided an appropriate value for each entity you include in the configuration template, use the following commands to pass the .json file and apply settings to Tableau Server.

```
tsm settings import -f path-to-file.json

 tsm pending-changes apply
```

See also

After you complete the initial SAML configuration, use tsm authentication mutual-ssl <commands> to set additional values.

For the command-line reference for configuring SAML, see tsm authentication saml <commands>.

**sapHanaSettings Entity**

Use the sapHanaSettings entity to configure SAML delegation for SAP HANA.

Review Configure SAP HANA SSO before you continue.

Use the configuration file template below to create a json file. After you have filled in the options with the appropriate values, pass the json file and apply settings with the following commands:

```
tsm settings import -f path-to-file.json

 tsm pending-changes apply
```
The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

SAP HANA SAML settings

The settings in the template below specify the settings for Tableau Server in a SAML delegation scenario with SAP HANA.

Configuration template

Use this template to configure trusted authentication settings.

All that are referenced in `configEntities` must be located on the local computer. Do not specify UNC paths.

All entity options are case sensitive.

For more explanation about configuration files, entities, and keys see Configuration File Example.

```json
{
    "configEntities": {
        "sapHanaSettings": {
            "_type": "sapHanaSettingsType",
            "enabled": "true",
            "usernameFormat": "username",
            "usernameCase": "preserve",
            "certFile": "path-to-cert_file",
            "keyFile": "path-to-key_file"
        }
    }
}
```
This table includes all of the options that can be included with the "gatewaySettings" entity set.

**enabled**

Required.

**Values:** true or false

**usernameFormat**

**Values:** username, domain_and_username, or email

Specifies user name credential format.

**usernameCase**

**Values:** lower, upper, or preserve

Specifies user input name case.

**certFile**

Specifies file path and name for the certificate file on the local computer.

*For example,* 
"/var/opt/tableau/tableau_server/data/saml/saml_cert.t.crt".

**keyFile**

Specifies file path and name for the certificate key on the local computer.

*For example,* 
"/var/opt/tableau/tableau_server/data/saml/saml_key.der".
trustedAuthenticationSettings Entity

Before you configure trusted authentication, review Trusted Authentication.

Use the configuration file template below to create a json file. After you have filled in the options with the appropriate values, pass the json file and apply settings with the following commands:

```shell
  tsm settings import -f /path/to/file.json

  tsm pending-changes apply
```

The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the `--ignore-prompt` option, but this does not change the restart behavior. For more information, see `tsm pending-changes apply`.

Configuration template

Use this template to configure trusted authentication settings.

All entity options are case sensitive.

For more explanation about configuration files, entities, and keys see Configuration File Example.

After you have finished with the initial configuration of trusted authentication, use the `tsm authentication trusted <commands>` sub-category to set additional values.

```json
{
  "configEntities": {
    "trustedAuthenticationSettings": {
      "_type": "trustedAuthenticationSettingsType",
      "trustedHosts": ["webserv1","webserv2","webserv3"]
    }
  }
}
```
Configuration file reference

The following list includes all of the options that can be included with the "trustedAuthenticationSettings" entity set.

trustedHosts

Required.

IP address or host names of web servers that request trusted tickets from Tableau Server.

This option takes a list of strings, which requires passing each IP or host in quotes, separated by a comma (no space) and within brackets. For example:

["192.168.1.101","192.168.1.102","192.168.1.103"] or ["webserv1","webserv2","webserv3"].

The values you specify overwrite previous settings. Therefore, you must include the full list of hosts when you configure this value.

tokenLength

Optional.

The value can be set to any integer between 9 and 255, inclusive.

Determines the number of characters in each trusted ticket. The default setting of 24 characters provides 144 bits of randomness. This option is ignored unless `useV2Tickets` is set to true, which is not a recommended best practice.

logLevel

Optional.

all | debug | info | warn | error | fatal | off
Default: info

Specifies logging level for processes related to creating and redeeming trusted tickets. See Change Logging Levels.

timeoutInSeconds

Optional.

Default: 180

Specifies the length of time (in seconds) to invalidate trusted tickets after they are created.

tryCount

Optional.

Integer.

Default: 10

Specifies the number of times to attempt to create a trusted ticket entry.

use9DigitToken

Optional.

true | false

Default: false

When set to true, tickets are 9 digits long (as in version 8.0 and earlier) and the option tokenLength is ignored. This option is intended for temporary support of legacy code.

**Warning:** Setting this option to true severely and negatively impacts the security strength of trusted ticket authentication.
useV2Tickets

Optional.

true | false

Default: false

Specifies whether Tableau Server should return a legacy URL format for trusted ticket requests. The legacy URL format includes a 24 character, Base64-encoded string. Beginning with Tableau Server 10.3, the URL that is returned has been updated and includes a Base64-encoded UUID and a 24 character secure random string. Only set this option to true if you have deployed trusted tickets with custom code that requires the legacy URL format. We recommend instead, updating your custom code to accept the new URL format.

web-data-connector-settings Entity

This entity is used to manage web data connector (WDC) settings. To learn more about using WDCs in Tableau Server, see Web Data Connectors in Tableau Server and tsm data-access.

Use the configuration file template below to create a .json file. After you have filled in the options with the appropriate values, pass the .json file and apply settings with the following commands:

tsm settings import -f /path/to/file.json

tsm pending-changes apply

The pending-changes apply command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the --ignore-prompt option, but this does not change the restart behavior. For more information, see tsm pending-changes apply.
Web data connector settings

The web data connector (WDC) settings in the template below specify whether WDCs are enabled, whether refresh of WDCs is enabled, and the primary and secondary safe lists. The safe lists (or "whitelists") indicate which WDC URLs are approved for use in your Tableau Server installation, and the domains or URLs that a connector can send requests to and receive requests from.

Configuration template

Use this template to configure the WDC settings.

All entity options are case sensitive.

For more explanation about configuration files, entities, and keys see Configuration File Example.

```
{
  "configEntities": {
    "web-data-connector-settings": {
      "_type": "webDataConnectorSettingsType",
      "refreshEnabled": true,
      "whitelist": {
        "https://dtreskunov.github.io:80/wta-wdc/": {
          "secondaryWhitelist": [
            "(https://dtreskunov.github.io/*/"
          ]
        }
      },
      "enabled": true
    }
  }
}
```
This table includes all of the options that can be included with the "web-data-connector-settings" entity set.

_type

Required.

Value: "web-data-connector-settings"

Do not change.

refreshEnabled

Set to false to disable refresh of WDCs. Defaults to true.

whitelist

Required.

Can contain one or more matching sets of safe lists and secondary safe lists (one set per WDC). The first URL provided is the safe list, where you specify the WDC URL and port, formatted as follows:

<scheme>://<host>:<port>/<path>

For many WDCs, the <port> value is 443 or 80, but you can check the value for your connector by looking at the data source details on Tableau Server or Tableau Online.

secondaryWhitelist

Required.

Specifies the domains or URLs that a connector can send requests to and receive requests from. To specify a domain, use a wildcard character (*), as in the following example:

https://dtreskunov.github.io/*
enabled

Set to false to disable use of WDCs. Defaults to true.

**tabcmd**

Tableau provides the tabcmd command-line utility which you can use to automate site administration tasks on your Tableau Server site. For example, creating or deleting users, projects, and groups.

This utility is included with Tableau Server, and is automatically installed on the initial server node. You can also run it from other computers, even computers that are not part of your Tableau Server installation, but to do so you need to download the tabcmd installer from the Tableau website. For more information, see Install tabcmd below.

**Install tabcmd**

When Tableau Server or Tableau Online is upgraded to a new version, if an updated version of tabcmd is required, you can download it from the Tableau Releases page on the Tableau website, to avoid issues caused by version incompatibilities. Using an out of date version of tabcmd can cause errors and unpredictable results.

1. Open a web browser and go to the Tableau Server Releases page (do this even if you use Tableau Online).

2. **For Tableau Online**: select the latest release.

   **For Tableau Server (Windows or Linux)**: select the release that matches your server version.

   If the expanded information shows maintenance releases, select the latest maintenance release or the one that matches your server version.
This takes you to the release notes page, where you can read about security improvements and resolved issues.

3. Scroll to the **Download Files** section under the resolved issues, select the `tabcmd` download link that is compatible with the computer on which you’ll run the `tabcmd` commands.

   The remaining steps refer to this computer as “the `tabcmd` computer.”

4. Save the installer to the `tabcmd` computer, or a location accessible from that computer.
5. Complete the installation steps as appropriate for the operating system of the tabcmd computer:

**Windows**

Run the installer.

We recommend that you install tabcmd to a folder named `tabcmd` at the root of the C:\ drive (`C:\tabcmd`), for convenience when using tabcmd, and to accommodate some limitations with the Windows operating system.

**Note** The tabcmd Setup program does not add the tabcmd directory to the Windows PATH variable. You can add it manually, or you can include the full path to tabcmd each time you call it.

**Linux**

a. Log on as a user with sudo access to the tabcmd computer.

b. Navigate to the directory where you copied the `.rpm` or `.deb` package that you downloaded.

   - On RHEL-like distributions, including CentOS, run the following command:

     ```bash
     sudo yum install tableau-tabcmd-<version>.noarch.rpm
     ```

   - On Ubuntu, run the following command:

     ```bash
     sudo gdebi -n tableau-tabcmd-<version>_all.deb
     ```
How to use tabcmd

The basic steps for using tabcmd are as follows:

1. Open the Command Prompt as an administrator.

2. On a Windows computer, if you installed tabcmd on a computer other than the initial node, change to the directory where you installed tabcmd.

   On a Linux computer, you do not need to change to the install directory.

3. Run the tabcmd command.

When you use tabcmd, you must establish an authenticated server session. The session identifies the server or Tableau Online site and the user running the session. You can start a session first, and then specify your command next, or you can start a session and execute a command all at once.

**Important:** If you are using tabcmd to perform more than one task, you must run tasks one after another (serially), rather than at the same time (in parallel).

Commands (such as `login`) and the options (such as `-s`, `-u`, etc.) are not case sensitive, but the values you provide (such as `User@Example.com`) are case sensitive.

**Examples**

The following command demonstrates starting a session with the Tableau Server named `tab-server.mycompany.com`:

```
tabcmd login -s http://tabserver.mycompany.com -u admin -p mypassword
```

The next example shows a command that deletes a workbook named `Sales_Workbook`:

```
tabcmd delete "Sales_Workbook"
```
Here’s how to accomplish all of the above with one command—note that you do not need login here:

```
tagcmd delete "Sales_Workbook" -s http://tabserver.mycompany.com -u admin -p mypassword
```

A Tableau Server can run multiple sites. When a workbook is on the Default site of a multi-site server you don't need to specify Default, the above command is sufficient. However, if the command applies to something on a site other than Default, you need to specify the site ID for that site (see login). Here’s the same command for a workbook that’s on the West Coast Sales site (site ID wsales):

```
tagcmd delete "Sales_Workbook" -s http://tabserver.mycompany.com -t wsales -u admin -p mypassword
```

The options -s, -t, -u, and -p are among the tabcmd global variables, which can be used with any command.

For more information, see tabcmd Commands.

**tabcmd Commands**

Looking for Tableau Server on Windows? See [tabcmd Commands](#).

You can use the following commands with the tabcmd command line tool:

- `addusers` (to group)
- `creategroup`
- `createproject`
- `createsite`
- `createsiteusers`
- `createusers`
- `delete workbook-name or datasource-name`
- `deletegroup`
- `deleteproject`
- `deletesite`
addusers *group-name*

Adds users to the specified group.

**Example**

tabcmd addusers "Development" --users "users.csv"

**Options**

--users

Add the users in the given .csv file to the specified group. The file should be a simple list with one user name per line. User names are not case sensitive. The users should already be created on Tableau Server.
For more information, see CSV Import File Guidelines.

--[no-]complete

When set to complete this option requires that all rows be valid for any change to succeed. If not specified, --complete is used.

Global options

The following options are used by all tabcmd commands. The --server, --user, and --password options are required at least once to begin a session. An authentication token is stored so subsequent commands can be run without including these options. This token remains valid for five minutes after the last command that used it.

-h, --help

Displays the help for the command.

-c, --use-certificate

Use client certificate to sign in. Required when mutual SSL is enabled.

For information about configuring the certificate, start with the following topic appropriate for your Tableau Server OS:

- **Windows**: Configure Mutual SSL
- **Linux**: Configure Mutual SSL

-s, --server

The Tableau Server URL, which is required at least once to begin session.

-u, --user
Tableau Server on Linux Administrator Guide

The Tableau Server username, which is required at least once to begin session.

-p, --password

The Tableau Server password, which is required at least once to begin session.

--password-file

Allows the password to be stored in the given .txt file rather than the command line for increased security.

-t, --site

Indicates that the command applies to the site specified by the Tableau Server site ID. If you do not specify a site, the Default site is assumed. Applies only to servers with multiple sites.

-x, --proxy

Host:Port

Uses the specified HTTP proxy.

--no-prompt

When specified, the command will not prompt for a password. If no valid password is provided the command will fail.

--no-proxy

When specified, an HTTP proxy will not be used.

--no-certcheck

When specified, tabcmd (the client) does not validate the server’s SSL certificate.
--[no-]cookie

When specified, the session ID is saved on login so subsequent commands will not need to log in. Use the no- prefix to not save the session ID. By default the session is saved.

--timeout

Waits the specified number of seconds for the server to complete processing the command. By default the process will timeout in 30 seconds.

--

Specifies the end of options on the command line. You can use -- to indicate to tabcmd that anything that follows -- should not be interpreted as an option setting and can instead be interpreted as a value for the command. This is useful if you need to specify a value in the command that includes a hyphen. The following example shows how you might use -- in a tabcmd command, where -430105/Sheet1 is a required value for the export command.

```
tabcmd export --csv -f "D:\export10.csv" -- -430105/Sheet1
```

creategroup group-name

Creates a group. Use addusers (for local groups) and syncgroup (for Active Directory groups) commands to add users after the group has been created.

Example

```
tabcmd creategroup "Development"
```

Global options

The following options are used by all tabcmd commands. The --server, --user, and --password options are required at least once to begin a session. An authentication token is stored so subsequent commands can be run without including these options. This token
remains valid for five minutes after the last command that used it.

-h, --help

Displays the help for the command.

-c, --use-certificate

Use client certificate to sign in. Required when mutual SSL is enabled.

For information about configuring the certificate, start with the following topic appropriate for your Tableau Server OS:

- **Windows**: Configure Mutual SSL
- **Linux**: Configure Mutual SSL

-s, --server

The Tableau Server URL, which is required at least once to begin session.

-u, --user

The Tableau Server username, which is required at least once to begin session.

-p, --password

The Tableau Server password, which is required at least once to begin session.

--password-file

Allows the password to be stored in the given .txt file rather than the command line for increased security.

-t, --site

Indicates that the command applies to the site specified by the Tableau Server site ID.
If you do not specify a site, the Default site is assumed. Applies only to servers with multiple sites.

-x, --proxy

Host:Port

Uses the specified HTTP proxy.

--no-prompt

When specified, the command will not prompt for a password. If no valid password is provided the command will fail.

--no-proxy

When specified, an HTTP proxy will not be used.

--no-certcheck

When specified, tabcmd (the client) does not validate the server's SSL certificate.

--[no-]cookie

When specified, the session ID is saved on login so subsequent commands will not need to log in. Use the no- prefix to not save the session ID. By default the session is saved.

--timeout

Waits the specified number of seconds for the server to complete processing the command. By default the process will timeout in 30 seconds.

--

Specifies the end of options on the command line. You can use -- to indicate to
Tableau Server on Linux Administrator Guide

tabcmd that anything that follows -- should not be interpreted as an option setting and can instead be interpreted as a value for the command. This is useful if you need to specify a value in the command that includes a hyphen. The following example shows how you might use -- in a tabcmd command, where -430105/SHEET1 is a required value for the export command.

    tabcmd export --csv -f "D:\export10.csv" -- -430105/SHEET1

createproject project-name

Creates a project.

Example

    tabcmd createproject -n "Quarterly_Reports" -d "Workbooks showing quarterly sales reports."

Options

-n, --name

    Specifies the name of the project that you want to create.

--parent-project-path

    Specifies the name of the parent project for the nested project as specified with the -n option. For example, to specify a project called "Nested" that exists in a "Main" project, use the following syntax: --parent-project-path "Main" -n "Nested".

-d, --description

    Specifies a description for the project.

Global options

The following options are used by all tabcmd commands. The --server, --user, and --
password options are required at least once to begin a session. An authentication token is stored so subsequent commands can be run without including these options. This token remains valid for five minutes after the last command that used it.

- **h, --help**
  
  Displays the help for the command.

- **c, --use-certificate**
  
  Use client certificate to sign in. Required when mutual SSL is enabled.

  For information about configuring the certificate, start with the following topic appropriate for your Tableau Server OS:

  - **Windows**: Configure Mutual SSL
  
  - **Linux**: Configure Mutual SSL

- **s, --server**
  
  The Tableau Server URL, which is required at least once to begin session.

- **u, --user**
  
  The Tableau Server username, which is required at least once to begin session.

- **p, --password**
  
  The Tableau Server password, which is required at least once to begin session.

- **--password-file**
  
  Allows the password to be stored in the given .txt file rather than the command line for increased security.
-t, --site

Indicates that the command applies to the site specified by the Tableau Server site ID.
If you do not specify a site, the Default site is assumed. Applies only to servers with multiple sites.

-x, --proxy

Host:Port

Uses the specified HTTP proxy.

--no-prompt

When specified, the command will not prompt for a password. If no valid password is provided the command will fail.

--no-proxy

When specified, an HTTP proxy will not be used.

--no-certcheck

When specified, tabcmd (the client) does not validate the server's SSL certificate.

--[no-]cookie

When specified, the session ID is saved on login so subsequent commands will not need to log in. Use the no- prefix to not save the session ID. By default the session is saved.

--timeout

Waits the specified number of seconds for the server to complete processing the command. By default the process will timeout in 30 seconds.
Specifies the end of options on the command line. You can use `--` to indicate to `tabcmd` that anything that follows `--` should not be interpreted as an option setting and can instead be interpreted as a value for the command. This is useful if you need to specify a value in the command that includes a hyphen. The following example shows how you might use `--` in a `tabcmd` command, where `-430105/SHEET1` is a required value for the `export` command.

```
tabcmd export --csv -f "D:\export10.csv" -- -430105/SHEET1
```

createsite `site-name`

Creates a site.

Examples

Create a site named West Coast Sales. A site ID of `WestCoastSales` will be automatically created, the site will have no storage quota limit, and site administrators will be able to add and remove users:

```
tabcmd createsite "West Coast Sales"
```

Create a site named West Coast Sales with a site ID of `wsales`:

```
tabcmd createsite "West Coast Sales" -r "wsales"
```

Prevent site administrators from adding users to the site:

```
tabcmd createsite "West Coast Sales" --no-site-mode
```

Set a storage quota, in MB:

```
tabcmd createsite "West Coast Sales" --storage-quota 100
```

Options

```
-r, --url
```
Tableau Server on Linux Administrator Guide

Used in URLs to specify the site. Different from the site name.

--user-quota

Maximum number of users that can be added to the site.

--[no-]site-mode

Allows or denies site administrators the ability to add users to or remove users from the site.

--storage-quota

In MB, the amount of workbooks, extracts, and data sources that can be stored on the site.

Global options

The following options are used by all `tabcmd` commands. The `--server`, `--user`, and `--password` options are required at least once to begin a session. An authentication token is stored so subsequent commands can be run without including these options. This token remains valid for five minutes after the last command that used it.

-h, --help

Displays the help for the command.

-c, --use-certificate

Use client certificate to sign in. Required when mutual SSL is enabled.

For information about configuring the certificate, start with the following topic appropriate for your Tableau Server OS:
-s, --server

The Tableau Server URL, which is required at least once to begin session.

-u, --user

The Tableau Server username, which is required at least once to begin session.

-p, --password

The Tableau Server password, which is required at least once to begin session.

--password-file

Allows the password to be stored in the given .txt file rather than the command line for increased security.

-t, --site

Indicates that the command applies to the site specified by the Tableau Server site ID. If you do not specify a site, the Default site is assumed. Applies only to servers with multiple sites.

-x, --proxy

Host:Port

Uses the specified HTTP proxy.

--no-prompt

When specified, the command will not prompt for a password. If no valid password is
provided the command will fail.

```
--no-proxy
```

When specified, an HTTP proxy will not be used.

```
--no-certcheck
```

When specified, `tabcmd` (the client) does not validate the server's SSL certificate.

```
--[no-]cookie
```

When specified, the session ID is saved on login so subsequent commands will not need to log in. Use the `no-` prefix to not save the session ID. By default the session is saved.

```
--timeout
```

Waits the specified number of seconds for the server to complete processing the command. By default the process will timeout in 30 seconds.

```

```
```

Specifies the end of options on the command line. You can use `--` to indicate to `tabcmd` that anything that follows `--` should not be interpreted as an option setting and can instead be interpreted as a value for the command. This is useful if you need to specify a value in the command that includes a hyphen. The following example shows how you might use `--` in a `tabcmd` command, where `-430105/SHEET1` is a required value for the `export` command.

```
tabcmd export --csv -f "D:\export10.csv" -- -430105/SHEET1
```

**createsiteusers** `filename.csv`

Adds users to a site, based on information supplied in a comma-separated values (CSV) file. If the user is not already created on the server, the command creates the user before adding that user to the site.
The CSV file must contain one or more user names and can also include (for each user) a password, full name, license type, administrator level, publisher (yes/no), and email address. For information about the format of the CSV file, see CSV Import File Guidelines.

As an alternative to including administrator level and publisher permissions in the CSV file, you can pass access level information by including the \--role option and specifying the site role you want to assign users listed in the CSV file.

By default, users are added to the site that you are logged in to. To add users to a different site, include the global \--site option and specify that site. (You must have permissions to create users on the site you specify.)

If the server contains multiple sites, you cannot add server (system) administrators through the `createSiteUsers` command. Use `createusers` instead. If you specify the `ServerAdministrator` site role for the \--role option, the command returns an error. If the CSV file includes `System` as value for administrator, the value is ignored and the user is assigned the Unlicensed license type.

If the server contains only one site (the default site), you can specify `system` for the administrator value for a user, or even assign the `ServerAdministrator` site role using the \--role option, if you want all users in the CSV file to be server administrators.

By default, this command creates users using a synchronous operation (it waits for all operations to complete before proceeding). You can use the \--no-wait option to specify an asynchronous operation.

Local authentication

If the server is configured to use local authentication, the information in the CSV file is used to create users.

Active Directory authentication

If the server is configured to use Active Directory authentication, user information is imported from Active Directory, and password and friendly name information in the CSV file is ignored. Further, if a user is specified in the CSV file but no corresponding user exists in
Active Directory, the user is not added to Tableau Server. For Active Directory users, because the user name is not guaranteed to be unique across domains, you must include the domain as part of the user name. You can specify this as either `domain/username` or `username@domain.com`; however, we recommend using the `domain/username` format. For more information, see User Management in Active Directory Deployments.

**Example**

```
tabcmd createsiteusers "users.csv" --role "Explorer"
```

**Options**

`--admin-type`

Deprecated. Use the `--role` option instead.

`--complete`

Requires that all rows be valid for any change to succeed. This is the default setting.

`--no-complete`

Specifies that the command should make changes on the server even if not all rows contain valid information. Rows that contain invalid information are skipped.

`--no-publisher`

Deprecated. Use the `--role` option instead.

`--nowait`

Do not wait for asynchronous jobs to complete.

`--publisher`

Deprecated. Use the `--role` option instead.
--role

Specifies a site role for all users in the .csv file. When you want to assign site roles using the --role option, create a separate CSV file for each site role.

Valid values are ServerAdministrator, SiteAdministratorCreator, SiteAdministratorExplorer, Creator, ExplorerCanPublish, Explorer, Viewer, ReadOnly, and Unlicensed.

The default is Unlicensed for new users and unchanged for existing users. Users are added as unlicensed also if you have a user-based server installation, and if the createsiteusers command creates a new user, but you have already reached the limit on the number of licenses for your users.

**Note:** On a multi-site Tableau Server, if you want to assign the ServerAdministrator site role using the --role option, use the createusers command instead of createsiteusers.

--silent-progress

Do not display progress messages for the command.

Global options

The following options are used by all tabcmd commands. The --server, --user, and --password options are required at least once to begin a session. An authentication token is stored so subsequent commands can be run without including these options. This token remains valid for five minutes after the last command that used it.

-h, --help

Displays the help for the command.
-c, --use-certificate

Use client certificate to sign in. Required when mutual SSL is enabled.

For information about configuring the certificate, start with the following topic appropriate for your Tableau Server OS:

- **Windows**: Configure Mutual SSL
- **Linux**: Configure Mutual SSL

-s, --server

The Tableau Server URL, which is required at least once to begin session.

-u, --user

The Tableau Server username, which is required at least once to begin session.

-p, --password

The Tableau Server password, which is required at least once to begin session.

--password-file

Allows the password to be stored in the given .txt file rather than the command line for increased security.

-t, --site

Indicates that the command applies to the site specified by the Tableau Server site ID. If you do not specify a site, the Default site is assumed. Applies only to servers with multiple sites.

-x, --proxy

Host:Port
Uses the specified HTTP proxy.

--no-prompt

When specified, the command will not prompt for a password. If no valid password is provided the command will fail.

--no-proxy

When specified, an HTTP proxy will not be used.

--no-certcheck

When specified, tabcmd (the client) does not validate the server's SSL certificate.

--[no-]cookie

When specified, the session ID is saved on login so subsequent commands will not need to log in. Use the no- prefix to not save the session ID. By default the session is saved.

--timeout

Waits the specified number of seconds for the server to complete processing the command. By default the process will timeout in 30 seconds.

--

Specifies the end of options on the command line. You can use -- to indicate to tabcmd that anything that follows -- should not be interpreted as an option setting and can instead be interpreted as a value for the command. This is useful if you need to specify a value in the command that includes a hyphen. The following example shows how you might use -- in a tabcmd command, where -430105/Sheet1 is a required value for the export command.

tabcmd export --csv -f "D:\export10.csv" -- -430105/Sheet1
createusers filename.csv

Create users in Tableau Server, based on information supplied in a comma-separated values (CSV) file.

The CSV file must contain one or more user names and can also include (for each user) a password, full name, license type, administrator level, publisher (yes/no), and email address. For information about the format of the CSV file, see CSV Import File Guidelines.

As an alternative to including administrator level and publisher permissions in the CSV file, you can pass access level information by including the --role option and specifying the site role you want to assign users listed in the CSV file.

If the server has only one site (the default site), the user is created and added to the site. If the server has multiple sites, the user is created but is not added to any site. To add users to a site, use createsiteusers.

If you have a user-based server installation, and if the command creates a new user but you have already reached the limit on the number of licenses for your users, the user is added as an unlicensed user.

Local authentication

If the server is configured to use local authentication, the information in the CSV file is used to create users.

Active Directory authentication

If the server is configured to use Active Directory authentication, user information is imported from Active Directory, and password and friendly name information in the CSV file is ignored. Further, if a user is specified in the CSV file but no corresponding user exists in Active Directory, the user is not added to Tableau Server. For Active Directory users, because the user name is not guaranteed to be unique across domains, you must include the domain as part of the user name. You can specify this as either domain/username or user-
name@domain.com; however, we recommend using the domain/username format. For more information, see User Management in Active Directory Deployments.

Example

```bash
tabcmd createusers "users.csv" --role "ServerAdministrator"

tabcmd createusers "users.csv"
```

Options

--admin-type

Deprecated. Use the --role option instead.

--complete

Requires that all rows be valid for any change to succeed. This is the default setting.

--no-complete

Specifies that the command should make changes on the server even if not all rows contain valid information. Rows that contain invalid information are skipped.

--no-publisher

Deprecated. Use the --role option instead.

--nowait

Do not wait for asynchronous jobs to complete.

--publisher

Deprecated. Use the --role option instead.
-r, --role

Specifies a site role for all users in the .csv file. When you want to assign site roles using the --role option, create a separate CSV file for each site role.

Valid values are ServerAdministrator, SiteAdministratorCreator, SiteAdministratorExplorer, Creator, ExplorerCanPublish, Explorer, Viewer, ReadOnly, and Unlicensed.

On a multi-site server, the command does not assign the user to a site. Therefore, the only site roles the command can successfully assign are ServerAdministrator and Unlicensed. If you specify any other site role, the command assigns the Unlicensed role.

On a single-site server, the user is created and added to the default site using the role that you specify.

If you have a user-based server installation, and if the command creates a new user but you have already reached the limit on the number of licenses for your users, the user is added as an unlicensed user.

--silent-progress

Do not display progress messages for the command.

Global options

The following options are used by all tabcmd commands. The --server, --user, and --password options are required at least once to begin a session. An authentication token is stored so subsequent commands can be run without including these options. This token remains valid for five minutes after the last command that used it.

-h, --help

Displays the help for the command.
-c, --use-certificate

Use client certificate to sign in. Required when mutual SSL is enabled.

For information about configuring the certificate, start with the following topic appropriate for your Tableau Server OS:

- **Windows**: [Configure Mutual SSL](#)
- **Linux**: [Configure Mutual SSL](#)

-s, --server

The Tableau Server URL, which is required at least once to begin session.

-u, --user

The Tableau Server username, which is required at least once to begin session.

-p, --password

The Tableau Server password, which is required at least once to begin session.

--password-file

Allows the password to be stored in the given .txt file rather than the command line for increased security.

-t, --site

Indicates that the command applies to the site specified by the Tableau Server site ID. If you do not specify a site, the Default site is assumed. Applies only to servers with multiple sites.

-x, --proxy

Host:Port
Uses the specified HTTP proxy.

--no-prompt
When specified, the command will not prompt for a password. If no valid password is provided the command will fail.

--no-proxy
When specified, an HTTP proxy will not be used.

--no-certcheck
When specified, tabcmd (the client) does not validate the server's SSL certificate.

--[no-]cookie
When specified, the session ID is saved on login so subsequent commands will not need to log in. Use the no- prefix to not save the session ID. By default the session is saved.

--timeout
Waits the specified number of seconds for the server to complete processing the command. By default the process will timeout in 30 seconds.

--
Specifies the end of options on the command line. You can use -- to indicate to tabcmd that anything that follows -- should not be interpreted as an option setting and can instead be interpreted as a value for the command. This is useful if you need to specify a value in the command that includes a hyphen. The following example shows how you might use -- in a tabcmd command, where -430105/SHEET1 is a required value for the export command.

```
tabcmd export --csv -f "D:\export10.csv" -- -430105/SHEET1
```
delete **workbook-name** or **datasource-name**

Deletes the specified workbook or data source from the server.

This command takes the name of the workbook or data source as it is on the server, not the file name when it was published.

**Example**

```
tabcmd delete "Sales_Analysis"
```

**Options**

- **-r, --project**

  The name of the project containing the workbook or data source you want to delete. If not specified, the “Default” project is assumed.

- **--parent-project-path**

  Specifies the name of the parent project for the nested project as specified with the `-r` option. For example, to specify a project called "Nested" that exists in a "Main" project, use the following syntax: `--parent-project-path "Main" -r "Nested"`.

- **--workbook**

  The name of the workbook you want to delete.

- **--datasource**

  The name of the data source you want to delete.

**Global options**

The following options are used by all `tabcmd` commands. The `-server`, `-user`, and -
-password options are required at least once to begin a session. An authentication token is stored so subsequent commands can be run without including these options. This token remains valid for five minutes after the last command that used it.

-h, --help

Displays the help for the command.

-c, --use-certificate

Use client certificate to sign in. Required when mutual SSL is enabled.

For information about configuring the certificate, start with the following topic appropriate for your Tableau Server OS:

- **Windows**: Configure Mutual SSL
- **Linux**: Configure Mutual SSL

-s, --server

The Tableau Server URL, which is required at least once to begin session.

-u, --user

The Tableau Server username, which is required at least once to begin session.

-p, --password

The Tableau Server password, which is required at least once to begin session.

--password-file

Allows the password to be stored in the given .txt file rather than the command line for increased security.
-t, --site

Indicates that the command applies to the site specified by the Tableau Server site ID. If you do not specify a site, the Default site is assumed. Applies only to servers with multiple sites.

-x, --proxy

Host:Port

Uses the specified HTTP proxy.

--no-prompt

When specified, the command will not prompt for a password. If no valid password is provided the command will fail.

--no-proxy

When specified, an HTTP proxy will not be used.

--no-certcheck

When specified, tabcmd (the client) does not validate the server's SSL certificate.

--[no-]cookie

When specified, the session ID is saved on login so subsequent commands will not need to log in. Use the no- prefix to not save the session ID. By default the session is saved.

--timeout

Waits the specified number of seconds for the server to complete processing the command. By default the process will timeout in 30 seconds.
Specifies the end of options on the command line. You can use -- to indicate to tabcmd that anything that follows -- should not be interpreted as an option setting and can instead be interpreted as a value for the command. This is useful if you need to specify a value in the command that includes a hyphen. The following example shows how you might use -- in a tabcmd command, where -430105/Sheet1 is a required value for the export command.

```
tabcmd export --csv -f "D:\export10.csv" -- -430105/Sheet1
```

deletegroup group-name

Deletes the specified group from the server.

**Example**

```
tabcmd deletegroup "Development"
```

**Global options**

The following options are used by all tabcmd commands. The --server, --user, and --password options are required at least once to begin a session. An authentication token is stored so subsequent commands can be run without including these options. This token remains valid for five minutes after the last command that used it.

- **-h, --help**

  Displays the help for the command.

- **-c, --use-certificate**

  Use client certificate to sign in. Required when mutual SSL is enabled.
For information about configuring the certificate, start with the following topic appropriate for your Tableau Server OS:

- **Windows**: Configure Mutual SSL
- **Linux**: Configure Mutual SSL

- `s, --server`
  
The Tableau Server URL, which is required at least once to begin session.

- `u, --user`
  
The Tableau Server username, which is required at least once to begin session.

- `p, --password`
  
The Tableau Server password, which is required at least once to begin session.

- `--password-file`
  
  Allows the password to be stored in the given .txt file rather than the command line for increased security.

- `t, --site`
  
  Indicates that the command applies to the site specified by the Tableau Server site ID. If you do not specify a site, the Default site is assumed. Applies only to servers with multiple sites.

- `x, --proxy`
  
  Host:Port

  Uses the specified HTTP proxy.
When specified, the command will not prompt for a password. If no valid password is provided the command will fail.

--no-proxy

When specified, an HTTP proxy will not be used.

--no-certcheck

When specified, tabcmd (the client) does not validate the server’s SSL certificate.

--[no-]cookie

When specified, the session ID is saved on login so subsequent commands will not need to log in. Use the no- prefix to not save the session ID. By default the session is saved.

--timeout

Waits the specified number of seconds for the server to complete processing the command. By default the process will timeout in 30 seconds.

--

Specifies the end of options on the command line. You can use -- to indicate to tabcmd that anything that follows -- should not be interpreted as an option setting and can instead be interpreted as a value for the command. This is useful if you need to specify a value in the command that includes a hyphen. The following example shows how you might use -- in a tabcmd command, where -430105/Sheet1 is a required value for the export command.

```
  tabcmd export --csv -f "D:\export10.csv" -- -430105/Sheet1
```

**deleteproject project-name**

Deletes the specified project from the server.
Using `tabcmd`, you can specify only a top-level project in a project hierarchy. To automate tasks you want to perform on a project within a parent project, use the equivalent Tableau REST API call.

**Example**

```
tabcmd deleteproject "Designs"
```

**Option**

`--parent-project-path`

Specifies the name of the parent project for the nested project as specified with the command. For example, to specify a project called "Designs" that exists in a "Main" project, use the following syntax: `--parent-project-path "Main" "Designs"`.

**Global options**

The following options are used by all `tabcmd` commands. The `--server`, `--user`, and `--password` options are required at least once to begin a session. An authentication token is stored so subsequent commands can be run without including these options. This token remains valid for five minutes after the last command that used it.

`-h, --help`

Displays the help for the command.

`-c, --use-certificate`

Use client certificate to sign in. Required when mutual SSL is enabled.

For information about configuring the certificate, start with the following topic appropriate for your Tableau Server OS:
Tableau Server on Linux Administrator Guide

- **Windows:** Configure Mutual SSL

- **Linux:** Configure Mutual SSL

- `-s, --server`

  The Tableau Server URL, which is required at least once to begin session.

- `-u, --user`

  The Tableau Server username, which is required at least once to begin session.

- `-p, --password`

  The Tableau Server password, which is required at least once to begin session.

- `--password-file`

  Allows the password to be stored in the given .txt file rather than the command line for increased security.

- `-t, --site`

  Indicates that the command applies to the site specified by the Tableau Server site ID. If you do not specify a site, the Default site is assumed. Applies only to servers with multiple sites.

- `-x, --proxy`

  Host:Port

  Uses the specified HTTP proxy.

- `--no-prompt`

  When specified, the command will not prompt for a password. If no valid password is
provided the command will fail.

--no-proxy

When specified, an HTTP proxy will not be used.

--no-certcheck

When specified, tabcmd (the client) does not validate the server's SSL certificate.

--[no-]cookie

When specified, the session ID is saved on login so subsequent commands will not need to log in. Use the no- prefix to not save the session ID. By default the session is saved.

--timeout

Waits the specified number of seconds for the server to complete processing the command. By default the process will timeout in 30 seconds.

--

Specifies the end of options on the command line. You can use -- to indicate to tabcmd that anything that follows -- should not be interpreted as an option setting and can instead be interpreted as a value for the command. This is useful if you need to specify a value in the command that includes a hyphen. The following example shows how you might use -- in a tabcmd command, where -430105/Sheet1 is a required value for the export command.

```
  tabcmd export --csv -f "D:\export10.csv" -- -430105/Sheet1
```

deletesite site-name

Deletes the specified site from the server.

Example
Global options

The following options are used by all `tabcmd` commands. The `--server`, `--user`, and `--password` options are required at least once to begin a session. An authentication token is stored so subsequent commands can be run without including these options. This token remains valid for five minutes after the last command that used it.

-h, --help

Displays the help for the command.

-c, --use-certificate

Use client certificate to sign in. Required when mutual SSL is enabled.

For information about configuring the certificate, start with the following topic appropriate for your Tableau Server OS:

- **Windows**: Configure Mutual SSL
- **Linux**: Configure Mutual SSL

-s, --server

The Tableau Server URL, which is required at least once to begin session.

-u, --user

The Tableau Server username, which is required at least once to begin session.

-p, --password

The Tableau Server password, which is required at least once to begin session.
--password-file

Allows the password to be stored in the given .txt file rather than the command line for increased security.

-t, --site

Indicates that the command applies to the site specified by the Tableau Server site ID. If you do not specify a site, the Default site is assumed. Applies only to servers with multiple sites.

-x, --proxy

Host:Port

Uses the specified HTTP proxy.

--no-prompt

When specified, the command will not prompt for a password. If no valid password is provided the command will fail.

--no-proxy

When specified, an HTTP proxy will not be used.

--no-certcheck

When specified, tabcmd (the client) does not validate the server's SSL certificate.

[--no-]cookie

When specified, the session ID is saved on login so subsequent commands will not need to log in. Use the no- prefix to not save the session ID. By default the session is saved.
--timeout

Waits the specified number of seconds for the server to complete processing the command. By default the process will timeout in 30 seconds.

--

Specifies the end of options on the command line. You can use -- to indicate to tabcmd that anything that follows -- should not be interpreted as an option setting and can instead be interpreted as a value for the command. This is useful if you need to specify a value in the command that includes a hyphen. The following example shows how you might use -- in a tabcmd command, where --430105/SHEET1 is a required value for the export command.

tabcmd export --csv -f "D:\export10.csv" -- -430105/SHEET1

 deletesiteusers filename.csv

Removes users from from the site that you are logged in to. The users to be removed are specified in a file that contains a simple list of one user name per line. (No additional information is required beyond the user name.)

By default, if the server has only one site, or if the user belongs to only one site, the user is also removed from the server. On a Tableau Server Enterprise installation, if the server contains multiple sites, users who are assigned the site role of Server Administrator are removed from the site but are not removed from the server.

If the user owns content, the user’s role is change to Unlicensed, but the user is not removed from the server or the site. The content is still owned by that user. To remove the user completely, you must change the owner of the content and then try removing the user again.

If the user was imported from Active Directory, the user is removed from the site and possibly from the server. However, the user is not deleted from Active Directory.

Example
tabcmd deletesiteusers "users.csv"

Global options

The following options are used by all `tabcmd` commands. The `--server`, `--user`, and `--password` options are required at least once to begin a session. An authentication token is stored so subsequent commands can be run without including these options. This token remains valid for five minutes after the last command that used it.

- `h`, `--help`

  Displays the help for the command.

- `c`, `--use-certificate`

  Use client certificate to sign in. Required when mutual SSL is enabled.

  For information about configuring the certificate, start with the following topic appropriate for your Tableau Server OS:

  - **Windows**: [Configure Mutual SSL](#)
  - **Linux**: [Configure Mutual SSL](#)

- `s`, `--server`

  The Tableau Server URL, which is required at least once to begin session.

- `u`, `--user`

  The Tableau Server username, which is required at least once to begin session.

- `p`, `--password`

  The Tableau Server password, which is required at least once to begin session.
--password-file

Allows the password to be stored in the given .txt file rather than the command line for increased security.

-t, --site

Indicates that the command applies to the site specified by the Tableau Server site ID. If you do not specify a site, the Default site is assumed. Applies only to servers with multiple sites.

-x, --proxy

Host:Port

Uses the specified HTTP proxy.

--no-prompt

When specified, the command will not prompt for a password. If no valid password is provided the command will fail.

--no-proxy

When specified, an HTTP proxy will not be used.

--no-certcheck

When specified, tabcmd (the client) does not validate the server’s SSL certificate.

--[no-]cookie

When specified, the session ID is saved on login so subsequent commands will not need to log in. Use the no- prefix to not save the session ID. By default the session is saved.
--timeout

Waits the specified number of seconds for the server to complete processing the command. By default the process will timeout in 30 seconds.

--

Specifies the end of options on the command line. You can use -- to indicate to tabcmd that anything that follows -- should not be interpreted as an option setting and can instead be interpreted as a value for the command. This is useful if you need to specify a value in the command that includes a hyphen. The following example shows how you might use -- in a tabcmd command, where -430105/SHEET1 is a required value for the export command.

tabcmd export --csv -f "D:\export10.csv" -- -430105/SHEET1

deleteusers filename.csv

Deletes the users listed in the specified comma-separated values (.csv) file.

The .csv file should contain a simple list of one user name per line.

Example

tabcmd deleteusers "users.csv"

Options

--[no-]complete

When set to --complete this option requires that all rows be valid for any change to succeed. If not specified, --complete is used.

Global options

The following options are used by all tabcmd commands. The --server, --user, and --
-password options are required at least once to begin a session. An authentication token is stored so subsequent commands can be run without including these options. This token remains valid for five minutes after the last command that used it.

-h, --help
Displays the help for the command.

-c, --use-certificate
Use client certificate to sign in. Required when mutual SSL is enabled.
For information about configuring the certificate, start with the following topic appropriate for your Tableau Server OS:

- Windows: Configure Mutual SSL
- Linux: Configure Mutual SSL

-s, --server
The Tableau Server URL, which is required at least once to begin session.

-u, --user
The Tableau Server username, which is required at least once to begin session.

-p, --password
The Tableau Server password, which is required at least once to begin session.

--password-file
Allows the password to be stored in the given .txt file rather than the command line for increased security.
-t, --site

Indicates that the command applies to the site specified by the Tableau Server site ID. If you do not specify a site, the Default site is assumed. Applies only to servers with multiple sites.

-x, --proxy

Host:Port

Uses the specified HTTP proxy.

--no-prompt

When specified, the command will not prompt for a password. If no valid password is provided the command will fail.

--no-proxy

When specified, an HTTP proxy will not be used.

--no-certcheck

When specified, tabcmd (the client) does not validate the server's SSL certificate.

--[no-]cookie

When specified, the session ID is saved on login so subsequent commands will not need to log in. Use the no- prefix to not save the session ID. By default the session is saved.

--timeout

Waits the specified number of seconds for the server to complete processing the command. By default the process will timeout in 30 seconds.
Specifies the end of options on the command line. You can use -- to indicate to \texttt{tabcmd} that anything that follows -- should not be interpreted as an option setting and can instead be interpreted as a value for the command. This is useful if you need to specify a value in the command that includes a hyphen. The following example shows how you might use -- in a \texttt{tabcmd} command, where \texttt{-430105/Sheet1} is a required value for the \texttt{export} command.

\begin{verbatim}
tabcmd export --csv -f "D:\export10.csv" -- -430105/Sheet1
\end{verbatim}

\textbf{editdomain}

Changes the nickname or full domain name of an Active Directory domain on the server. A domain “nickname” is the Windows NetBIOS domain name.

You can modify the nickname for any domain the server is using. In general, you can modify the full domain name for any domain except the one that you used to sign in. However, if the user name that you are currently signed in with exists in both the current domain and the new domain, you can modify the full name for the current domain.

Review User Management in Active Directory Deployments to understand how multiple domains, domain name mapping, and user names interact with Tableau Server.

To see a list of domains, use \texttt{listdomains}.

\textbf{Examples}

\begin{verbatim}
tabcmd editdomain --id 2 --nickname "new-nickname"

tabcmd editdomain --id 3 --name "new-name"
\end{verbatim}

\textbf{Options}

\begin{verbatim}
--id
\end{verbatim}

The ID of domain to change. To get a list of domain IDs, use \texttt{listdomains}.
--name

The new name for the domain.

--nickname

The new nickname for the domain.

Global options

The following options are used by all `tabcmd` commands. The `--server`, `--user`, and `--password` options are required at least once to begin a session. An authentication token is stored so subsequent commands can be run without including these options. This token remains valid for five minutes after the last command that used it.

-h, --help

Displays the help for the command.

-c, --use-certificate

Use client certificate to sign in. Required when mutual SSL is enabled.

For information about configuring the certificate, start with the following topic appropriate for your Tableau Server OS:

- **Windows**: Configure Mutual SSL
- **Linux**: Configure Mutual SSL

-s, --server

The Tableau Server URL, which is required at least once to begin session.
-u, --user

The Tableau Server username, which is required at least once to begin session.

-p, --password

The Tableau Server password, which is required at least once to begin session.

--password-file

Allows the password to be stored in the given .txt file rather than the command line for increased security.

-t, --site

Indicates that the command applies to the site specified by the Tableau Server site ID. If you do not specify a site, the Default site is assumed. Applies only to servers with multiple sites.

-x, --proxy

Host:Port

Uses the specified HTTP proxy.

--no-prompt

When specified, the command will not prompt for a password. If no valid password is provided the command will fail.

--no-proxy

When specified, an HTTP proxy will not be used.

--no-certcheck
When specified, tabcmd (the client) does not validate the server's SSL certificate.

--[no-]cookie

When specified, the session ID is saved on login so subsequent commands will not need to log in. Use the no- prefix to not save the session ID. By default the session is saved.

--timeout

Waits the specified number of seconds for the server to complete processing the command. By default the process will timeout in 30 seconds.

--

Specifies the end of options on the command line. You can use -- to indicate to tabcmd that anything that follows -- should not be interpreted as an option setting and can instead be interpreted as a value for the command. This is useful if you need to specify a value in the command that includes a hyphen. The following example shows how you might use -- in a tabcmd command, where -430105/S01 is a required value for the export command.

    tabcmd export --csv -f "D:\export10.csv" --430105/S01

editsite site-name

Changes the name of a site or its web folder name. You can also use this command to allow or deny site administrators the ability to add and remove users. If site administrators have user management rights, you can specify how many users they can add to a site.

Examples

    tabcmd editsite wc_sales --site-name "West Coast Sales"

    tabcmd editsite wc_sales --site-id "wsales"

    tabcmd editsite wsales --status ACTIVE
Tableau Server on Linux Administrator Guide

tabcmd editsite wsales --user-quota 50

Options

--site-name

The name of the site that's displayed.

--site-id

Used in the URL to uniquely identify the site.

--user-quota

Maximum number of users who can be members of the site.

--[no-]site-mode

Allow or prevent site administrators from adding users to the site.

--status

Set to **ACTIVE** to activate a site, or to **SUSPENDED** to suspend a site.

--storage-quota

In MB, the amount of workbooks, extracts, and data sources that can be stored on the site.

Global options

The following options are used by all tabcmd commands. The **--server**, **--user**, and **--password** options are required at least once to begin a session. An authentication token is stored so subsequent commands can be run without including these options. This token
remains valid for five minutes after the last command that used it.

-h, --help

Displays the help for the command.

-c, --use-certificate

Use client certificate to sign in. Required when mutual SSL is enabled.

For information about configuring the certificate, start with the following topic appropriate for your Tableau Server OS:

- **Windows**: Configure Mutual SSL
- **Linux**: Configure Mutual SSL

-s, --server

The Tableau Server URL, which is required at least once to begin session.

-u, --user

The Tableau Server username, which is required at least once to begin session.

-p, --password

The Tableau Server password, which is required at least once to begin session.

--password-file

Allows the password to be stored in the given .txt file rather than the command line for increased security.

-t, --site

Indicates that the command applies to the site specified by the Tableau Server site ID.
If you do not specify a site, the Default site is assumed. Applies only to servers with multiple sites.

-x, --proxy

Host:Port

Uses the specified HTTP proxy.

--no-prompt

When specified, the command will not prompt for a password. If no valid password is provided the command will fail.

--no-proxy

When specified, an HTTP proxy will not be used.

--no-certcheck

When specified, tabcmd (the client) does not validate the server’s SSL certificate.

--[no-]cookie

When specified, the session ID is saved on login so subsequent commands will not need to log in. Use the no- prefix to not save the session ID. By default the session is saved.

--timeout

Waits the specified number of seconds for the server to complete processing the command. By default the process will timeout in 30 seconds.

--

Specifies the end of options on the command line. You can use -- to indicate to
tabcmd that anything that follows -- should not be interpreted as an option setting and can instead be interpreted as a value for the command. This is useful if you need to specify a value in the command that includes a hyphen. The following example shows how you might use -- in a tabcmd command, where -430105/SHEET1 is a required value for the export command.

```bash
tabcmd export --csv -f "D:\export10.csv" -430105/SHEET1
```

**export**

Exports a view or workbook from Tableau Server and saves it to a file. This command can also export just the data used for a view.

Note the following when you use this command:

- **Permissions**: To export, you must have the `Export Image` permission. By default, this permission is Allowed or Inherited for all roles, although permissions can be set per workbook or view.

- **Exporting data**: To export just the data for a view, use the `--csv` option. This exports the summary data used in a view to a .csv file.

- **Specifying the view, workbook, or data to export**:
  
  - Use part of the URL to identify what to export, specifically the "workbook/view" string as it appears in the URL for the workbook or view. Do not use the "friendly name," and exclude the :iid=<n> session ID at the end of the URL.

  For example, the Tableau sample view *Global Temperatures* in the *Regional* workbook has a URL similar to this: `<server_name>/#/views/Regional/GlobalTemperatures?:iid=3`

  To export the *Global Temperatures* view, use the string `Regional/GlobalTemperatures`. 
Do not use Regional/Global Temperatures, or Region-
al/GlobalTemperatures?iid=3.

- If the server is running multiple sites and the view or workbook is on a site other than Default, Use -t <site_id>.

- To export a workbook, get the URL string by opening a view in the workbook, and include the view in the string you use.

  In the above example, to export the Regional workbook, use the string Regional/GlobalTemperatures.

- To export a workbook, it must have been published with Show Sheets as Tabs selected in the Tableau Desktop Publish dialog box.

- The saved file's format: Your format options depend on what’s being exported. A workbook can only be exported as a PDF using the --fullpdf argument. A view can be exported as a PDF (--pdf) or a PNG (--png).

- The saved file's name and location (optional): If you don't provide a name, it will be derived from the view or workbook name. If you don't provide a location, the file will be saved to your current working directory. Otherwise, you can specify a full path or one that's relative to your current working directory.

  Note: You must include a file name extension such as .csv or .pdf. The command does not automatically add an extension to the file name that you provide.

- Dashboard web page objects not included in PDF exports: A dashboard can optionally include a web page object. If you are performing an export to PDF of a dashboard that includes a web page object, the web page object won't be included in the PDF.

- Non-ASCII and non-standard ASCII characters and PDF exports: If you are
exporting a view or workbook with a name that includes a character outside the
ASCII character set, or a non-standard ASCII character set, you need to
URL encode (percent-encode) the character.

For example if your command includes the city Zürich, you need to URL encode it
as Z%C3%BCrich:

```bash
tabcmd export "/Cities/Sheet1?locationCity=Z%C3%BCrich" -
fullpdf
```

Clearing the Cache to Use Real-Time Data

You can optionally add the URL parameter `?:refresh=yes` to force a fresh data query
instead of pulling the results from the cache. If you are using tabcmd with your own scripting
and the `refresh` URL parameter is being used a great deal, this can have a negative
impact on performance. It's recommended that you use `refresh` only when real-time data
is required—for example, on a single dashboard instead of on an entire workbook.

Examples

Views

```bash
tabcmd export "Q1Sales/Sales_Report" --csv -f "Weekly-
Report.csv"
```

```bash
tabcmd export -t Sales "Sales/Sales_Analysis" --pdf -f "C:\T-
ableau_Workbooks\Weekly-Reports.pdf"
```

```bash
tabcmd export "Finance/InvestmentGrowth" --png
```

```bash
tabcmd export "Finance/InvestmentGrowth?:refresh=yes" --png
```

Workbooks

```bash
tabcmd export "Q1Sales/Sales_Report" --fullpdf
```
tabcmd export "Sales/Sales_Analysis" --fullpdf --pagesize tabloid -f "C:\Tableau_Workbooks\Weekly-Reports.pdf"

Options

-f, --filename

Saves the file with the given filename and extension.

--csv

View only. Export the view's data (summary data) in .csv format.

--pdf

View only. Export as a PDF.

--png

View only. Export as an image in .png format.

--fullpdf

Workbook only. Export as a PDF. The workbook must have been published with Show Sheets as Tabs enabled.

--pagelayout

Sets the page orientation (landscape or portrait) of the exported PDF. If not specified, its Tableau Desktop setting will be used.

--pagesize

Sets the page size of the exported PDF as one of the following: unspecified, letter, legal, note folio, tabloid, ledger, statement, executive, a3, a4, a5,
b4, b5, or quarto. Default is letter.

--width

Sets the width in pixels. Default is 800 px.

--height

Sets the height in pixels. Default is 600 px.

Global options

The following options are used by all tabcmd commands. The --server, --user, and --password options are required at least once to begin a session. An authentication token is stored so subsequent commands can be run without including these options. This token remains valid for five minutes after the last command that used it.

-h, --help

Displays the help for the command.

-c, --use-certificate

Use client certificate to sign in. Required when mutual SSL is enabled.

For information about configuring the certificate, start with the following topic appropriate for your Tableau Server OS:

- Windows: Configure Mutual SSL
- Linux: Configure Mutual SSL

-s, --server

The Tableau Server URL, which is required at least once to begin session.
-u, --user

The Tableau Server username, which is required at least once to begin session.

-p, --password

The Tableau Server password, which is required at least once to begin session.

--password-file

Allows the password to be stored in the given .txt file rather than the command line for increased security.

-t, --site

Indicates that the command applies to the site specified by the Tableau Server site ID. If you do not specify a site, the Default site is assumed. Applies only to servers with multiple sites.

-x, --proxy

Host:Port

Uses the specified HTTP proxy.

--no-prompt

When specified, the command will not prompt for a password. If no valid password is provided the command will fail.

--no-proxy

When specified, an HTTP proxy will not be used.

--no-certcheck
When specified, tabcmd (the client) does not validate the server's SSL certificate.

`--[no-]cookie`

When specified, the session ID is saved on login so subsequent commands will not need to log in. Use the `no-` prefix to not save the session ID. By default the session is saved.

`--timeout`

Waits the specified number of seconds for the server to complete processing the command. By default the process will timeout in 30 seconds.

`--`

Specifies the end of options on the command line. You can use `--` to indicate to `tabcmd` that anything that follows `--` should not be interpreted as an option setting and can instead be interpreted as a value for the command. This is useful if you need to specify a value in the command that includes a hyphen. The following example shows how you might use `--` in a `tabcmd` command, where `--430105/SHEET1` is a required value for the `export` command.

```
tabcmd export --csv -f "D:\export10.csv" --430105/SHEET1
```

`get url`

Gets the resource from Tableau Server that's represented by the specified (partial) URL. The result is returned as a file.

Note the following when you use this command:

- **Permissions**: To get a file, you must have the `Download/Web Save As` permission. By default, this permission is allowed or inherited for all roles, although permissions can be set per workbook or view.

- **Specifying a view or workbook to get**: You specify a view to get using the
"/views/<workbookname>/<viewname>_<extension>" string, and specify a workbook to get using the
"/workbooks/<workbookname>_<extension>" string. Replace <workbookname> and <viewname> with the names of the workbook and view as they appear in the URL when you open the view in a browser and replace <extension> with the type of file you want to save. Do not use the session ID at the end of the URL (?:iid=<n>) or the "friendly" name of the workbook or view.

For example, when you open a view Regional Totals in a workbook named Metrics Summary, the URL will look similar to this:

/Views/MetricsSummary_1/RegionalTotals?iid=1

Use the string /views/MetricsSummary_1/RegionalTotals_<extension> to get the view.

Use the string /workbooks/MetricsSummary_1_<extension> to get the workbook.

- **File extension**: The URL must include a file extension. The extension determines what's returned. A view can be returned in PDF, PNG, or CSV (summary data only) format. A Tableau workbook is returned as a TWB if it connects to a published data source or uses a live connection, or a TWBX if it connects to a data extract.

  **Note**: If you are downloading a view to a PDF or PNG file, and if you include a --filename parameter that includes the .pdf or .png extension, you do not have to include a .pdf or .png extension in the URL.

- **The saved file's name and location** (optional): The name you use for --filename should include the file extension. If you don’t provide a name and file extension, both will be derived from the URL string. If you don't provide a location, the file is saved to your current working directory. Otherwise, you can specify a full path or one that's...
relative to your current working directory.

- **PNG size** (optional): If the saved file is a PNG, you can specify the size, in pixels, in the URL.

**Clearing the cache to use real-time data**

You can optionally add the URL parameter `?:refresh=yes` to force a fresh data query instead of pulling the results from the cache. If you are using tabcmd with your own scripting, using the `refresh` parameter a great deal can have a negative impact on performance. It's recommended that you use `refresh` only when real-time data is required—for example, on a single dashboard instead of on an entire workbook.

**Examples**

**Views**

tabcmd get "/views/Sales_Analysis/Sales_Report.png" --filename "Weekly-Report.png"

tabcmd get "/views/Finance/InvestmentGrowth.pdf" -f "Q1Growth.pdf"

tabcmd get "/views/Finance/InvestmentGrowth" -f "Q1Growth.pdf"

tabcmd get "/views/Finance/InvestmentGrowth.csv"

tabcmd get "/views/Finance/InvestmentGrowth.png?:size=640,480" -f growth.png

tabcmd get "/views/Finance/InvestmentGrowth.png?:refresh=yes" -f growth.png

**Workbooks**

tabcmd get "/workbooks/Sales_Analysis.twb" -f "C:\Tableau_Workbooks\Weekly-Reports.twb"
Global options

The following options are used by all `tabcmd` commands. The `--server`, `--user`, and `--password` options are required at least once to begin a session. An authentication token is stored so subsequent commands can be run without including these options. This token remains valid for five minutes after the last command that used it.

-h, --help

Displays the help for the command.

-c, --use-certificate

Use client certificate to sign in. Required when mutual SSL is enabled.

For information about configuring the certificate, start with the following topic appropriate for your Tableau Server OS:

- **Windows:** Configure Mutual SSL
- **Linux:** Configure Mutual SSL

-s, --server

The Tableau Server URL, which is required at least once to begin session.

-u, --user

The Tableau Server username, which is required at least once to begin session.

-p, --password

The Tableau Server password, which is required at least once to begin session.
--password-file

Allows the password to be stored in the given .txt file rather than the command line for increased security.

-t, --site

Indicates that the command applies to the site specified by the Tableau Server site ID. If you do not specify a site, the Default site is assumed. Applies only to servers with multiple sites.

-x, --proxy

Host:Port

Uses the specified HTTP proxy.

--no-prompt

When specified, the command will not prompt for a password. If no valid password is provided the command will fail.

--no-proxy

When specified, an HTTP proxy will not be used.

--no-certcheck

When specified, tabcmd (the client) does not validate the server’s SSL certificate.

--[no-]cookie

When specified, the session ID is saved on login so subsequent commands will not need to log in. Use the no- prefix to not save the session ID. By default the session is saved.
--timeout

Waits the specified number of seconds for the server to complete processing the command. By default the process will timeout in 30 seconds.

--

Specifies the end of options on the command line. You can use -- to indicate to tabcmd that anything that follows -- should not be interpreted as an option setting and can instead be interpreted as a value for the command. This is useful if you need to specify a value in the command that includes a hyphen. The following example shows how you might use -- in a tabcmd command, where -430105/SHEET1 is a required value for the export command.

```
tabcmd export --csv -f "D:\export10.csv" -- -430105/SHEET1
```

initialuser

Create the initial administrative user on a server that does not have an initial administrative user defined.

Enclose values in single quotes.

**Note:** The `tabcmd initialuser` command does not require authentication to Tableau Server, but you must run the command on the initial server node.

**Examples**

```
tabcmd initialuser --username 'admin' --password 'password' --server http://localhost
```

```
tabcmd initialuser --username 'admin' --password 'password' --friendly 'Tableau Admin' --server http://localhost
```

To prompt for the password in the shell, do not include the --password parameter in the command. For example:
tabcmd initialuser --username 'admin' --server http://localhost

Options

-f, --friendly

Creates the initial administrative user with the display name.

Global options

The following options are used by all tabcmd commands. The --server, --user, and --password options are required at least once to begin a session. An authentication token is stored so subsequent commands can be run without including these options. This token remains valid for five minutes after the last command that used it.

-h, --help

Displays the help for the command.

-c, --use-certificate

Use client certificate to sign in. Required when mutual SSL is enabled.

For information about configuring the certificate, start with the following topic appropriate for your Tableau Server OS:

- **Windows:** [Configure Mutual SSL](#)
- **Linux:** [Configure Mutual SSL](#)

-s, --server

The Tableau Server URL, which is required at least once to begin session.
Tableau Server on Linux Administrator Guide

-u, --user

The Tableau Server username, which is required at least once to begin session.

-p, --password

The Tableau Server password, which is required at least once to begin session.

--password-file

Allows the password to be stored in the given .txt file rather than the command line for increased security.

-t, --site

Indicates that the command applies to the site specified by the Tableau Server site ID. If you do not specify a site, the Default site is assumed. Applies only to servers with multiple sites.

-x, --proxy

Host:Port

Uses the specified HTTP proxy.

--no-prompt

When specified, the command will not prompt for a password. If no valid password is provided the command will fail.

--no-proxy

When specified, an HTTP proxy will not be used.

--no-certcheck
When specified, tabcmd (the client) does not validate the server’s SSL certificate.

--[no-]cookie

When specified, the session ID is saved on login so subsequent commands will not need to log in. Use the no- prefix to not save the session ID. By default the session is saved.

--timeout

Waits the specified number of seconds for the server to complete processing the command. By default the process will timeout in 30 seconds.

--

Specifies the end of options on the command line. You can use -- to indicate to tabcmd that anything that follows -- should not be interpreted as an option setting and can instead be interpreted as a value for the command. This is useful if you need to specify a value in the command that includes a hyphen. The following example shows how you might use -- in a tabcmd command, where -430105/SHEET1 is a required value for the export command.

    tabcmd export --csv -f "D:\export10.csv" -- -430105/SHEET1

listdomains

Displays a list of the Active Directory domains that are in use on the server, along with their nicknames and IDs. If the server is configured to use local authentication, the command returns only the domain name local.

Example

    tabcmd listdomains

Global options
Tableau Server on Linux Administrator Guide

The following options are used by all `tabcmd` commands. The `--server`, `--user`, and `--password` options are required at least once to begin a session. An authentication token is stored so subsequent commands can be run without including these options. This token remains valid for five minutes after the last command that used it.

- **h, --help**
  Displays the help for the command.

- **c, --use-certificate**
  Use client certificate to sign in. Required when mutual SSL is enabled.
  
  For information about configuring the certificate, start with the following topic appropriate for your Tableau Server OS:
  
  - **Windows:** [Configure Mutual SSL](https://tableausoftware.com/help/)
  - **Linux:** [Configure Mutual SSL](https://tableausoftware.com/help/)

- **s, --server**
  The Tableau Server URL, which is required at least once to begin session.

- **u, --user**
  The Tableau Server username, which is required at least once to begin session.

- **p, --password**
  The Tableau Server password, which is required at least once to begin session.

- **--password-file**
  Allows the password to be stored in the given `.txt` file rather than the command line for increased security.
-t, --site

Indicates that the command applies to the site specified by the Tableau Server site ID. If you do not specify a site, the Default site is assumed. Applies only to servers with multiple sites.

-x, --proxy

Host:Port

Uses the specified HTTP proxy.

--no-prompt

When specified, the command will not prompt for a password. If no valid password is provided the command will fail.

--no-proxy

When specified, an HTTP proxy will not be used.

--no-certcheck

When specified, tabcmd (the client) does not validate the server’s SSL certificate.

--[no-]cookie

When specified, the session ID is saved on login so subsequent commands will not need to log in. Use the no- prefix to not save the session ID. By default the session is saved.

--timeout

Waits the specified number of seconds for the server to complete processing the command. By default the process will timeout in 30 seconds.
Specifies the end of options on the command line. You can use `--` to indicate to tabcmd that anything that follows `--` should not be interpreted as an option setting and can instead be interpreted as a value for the command. This is useful if you need to specify a value in the command that includes a hyphen. The following example shows how you might use `--` in a tabcmd command, where `-430105/SHEET` is a required value for the `export` command.

```
tabcmd export --csv -f "D:\export10.csv" -- -430105/SHEET
```

listsites

Returns a list of sites to which the logged in user belongs.

Example

```
tabcmd listsites --username adam --password mypassword
```

Global options

The following options are used by all tabcmd commands. The `--server`, `--user`, and `--password` options are required at least once to begin a session. An authentication token is stored so subsequent commands can be run without including these options. This token remains valid for five minutes after the last command that used it.

```
-h, --help

Displays the help for the command.

-c, --use-certificate

Use client certificate to sign in. Required when mutual SSL is enabled.
```
For information about configuring the certificate, start with the following topic appropriate for your Tableau Server OS:

- **Windows**: Configure Mutual SSL
- **Linux**: Configure Mutual SSL

-s, --server

The Tableau Server URL, which is required at least once to begin session.

-u, --user

The Tableau Server username, which is required at least once to begin session.

-p, --password

The Tableau Server password, which is required at least once to begin session.

--password-file

Allows the password to be stored in the given .txt file rather than the command line for increased security.

-t, --site

Indicates that the command applies to the site specified by the Tableau Server site ID. If you do not specify a site, the Default site is assumed. Applies only to servers with multiple sites.

-x, --proxy

Host:Port

Uses the specified HTTP proxy.
--no-prompt

When specified, the command will not prompt for a password. If no valid password is provided the command will fail.

--no-proxy

When specified, an HTTP proxy will not be used.

--no-certcheck

When specified, tabcmd (the client) does not validate the server’s SSL certificate.

--[no-]cookie

When specified, the session ID is saved on login so subsequent commands will not need to log in. Use the no- prefix to not save the session ID. By default the session is saved.

--timeout

Waits the specified number of seconds for the server to complete processing the command. By default the process will timeout in 30 seconds.

--

Specifies the end of options on the command line. You can use -- to indicate to tabcmd that anything that follows -- should not be interpreted as an option setting and can instead be interpreted as a value for the command. This is useful if you need to specify a value in the command that includes a hyphen. The following example shows how you might use -- in a tabcmd command, where -430105/Sheet1 is a required value for the export command.

```
tabcmd export --csv -f "D:\export10.csv" -- -430105/Sheet1
```

login

Logs in a Tableau Server user.
Use the `--server`, `--site`, `--username`, `--password` global options to create a session.

**Note:** When you use the `tabcmd login` command, you cannot use SAML single sign-on (SSO), even if the server is configured to use SAML. To log in, you must pass the user name and password of a user who has been created on the server. You will have the permissions of the Tableau Server user that you're signed in as. For more information, see Set Users' Site Roles and Content Permissions and Ownership.

If you want to log in using the same information you've already used to create a session, just specify the `--password` option. The server and user name stored in the cookie will be used.

If the server is using a port other than 80 (the default), you will need to specify the port.

You need the `--site (-t)` option only if the server is running multiple sites and you are logging in to a site other than the Default site. If you do not provide a password you will be prompted for one. If the `--no-prompt` option is specified and no password is provided the command will fail.

Once you log in, the session will continue until it expires on the server or the `logout` command is run.

**Example**

Logs user jsmith in to the Tableau Server running on their local machine:

```bash
tabcmd login -s http://localhost -u jsmith -p password
```

Logs administrator in to the Sales site on sales-server:

```bash
tabcmd login -s http://sales-server -t Sales -u administrator -p password
```
Tableau Server on Linux Administrator Guide

`tabcmd login -s http://sales-server:8000 -t Sales -u administrator -p password`

Logs administrator in to the Sales site on sales-server using SSL, but does not validate the server’s SSL certificate:

`tabcmd login --no-certcheck -s https://sales-server -t Sales -u administrator -p password`

Establishes a forward proxy and port for localhost:

`tabcmd login --proxy myfwdproxyserver:8888 -s http://localhost -u jsmith -p password`

Logs user jsmith in to the reverse proxy using SSL:

`tabcmd login -s https://myreverseproxy -u jsmith -p password`

Options

-s, --server

If you are running the command from a Tableau Server computer that’s on your network, you can use `http://localhost`. Otherwise, specify the computer’s URL, such as `http://bigbox.myco.com` or `http://bigbox`.

For Tableau Online specify the URL `https://online.tableau.com`.

-t, --site

Include this option if the server has multiple sites, and you are logging in to a site other than the default site.

The site ID is used in the URL to uniquely identify the site. For example, a site named West Coast Sales might have a site ID of west-coast-sales.

-u, --username
The user name of the user logging in. For Tableau Online, the user name is the user’s email address.

-p, --password

Password for the user specified for --username. If you do not provide a password you will be prompted for one.

--password-file

Allows the password to be stored in the given filename.txt file rather than the command line, for increased security.

-x, --proxy

Use to specify the HTTP proxy server and port (Host:Port) for the tabcmd request.

--no-prompt

Do not prompt for a password. If no password is specified, the login command will fail.

--no-proxy

Do not use an HTTP proxy server.

--cookie

Saves the session ID on login. Subsequent commands will not require a login. This value is the default for the command.

--no-cookie

Do not save the session ID information after a successful login. Subsequent commands will require a login.
The number of seconds the server should wait before processing the login command. Default: 30 seconds.

Global options

The following options are used by all tabcmd commands. The --server, --user, and --password options are required at least once to begin a session. An authentication token is stored so subsequent commands can be run without including these options. This token remains valid for five minutes after the last command that used it.

-h, --help

Displays the help for the command.

-c, --use-certificate

Use client certificate to sign in. Required when mutual SSL is enabled.

For information about configuring the certificate, start with the following topic appropriate for your Tableau Server OS:

- **Windows**: Configure Mutual SSL
- **Linux**: Configure Mutual SSL

-s, --server

The Tableau Server URL, which is required at least once to begin session.

-u, --user

The Tableau Server username, which is required at least once to begin session.
-p, --password

The Tableau Server password, which is required at least once to begin session.

--password-file

Allows the password to be stored in the given .txt file rather than the command line for increased security.

-t, --site

Indicates that the command applies to the site specified by the Tableau Server site ID. If you do not specify a site, the Default site is assumed. Applies only to servers with multiple sites.

-x, --proxy

Host:Port

Uses the specified HTTP proxy.

--no-prompt

When specified, the command will not prompt for a password. If no valid password is provided the command will fail.

--no-proxy

When specified, an HTTP proxy will not be used.

--no-certcheck

When specified, tabcmd (the client) does not validate the server’s SSL certificate.

--[no-]cookie
When specified, the session ID is saved on login so subsequent commands will not need to log in. Use the no- prefix to not save the session ID. By default the session is saved.

--timeout

Waits the specified number of seconds for the server to complete processing the command. By default the process will timeout in 30 seconds.

--

Specifies the end of options on the command line. You can use -- to indicate to tabcmd that anything that follows -- should not be interpreted as an option setting and can instead be interpreted as a value for the command. This is useful if you need to specify a value in the command that includes a hyphen. The following example shows how you might use -- in a tabcmd command, where -430105/Sheet1 is a required value for the export command.

```
tabcmd export --csv -f "D:\export10.csv" -- -430105/Sheet1
```

logout

Logs out of the server.

Example

tabcmd logout

publish filename.twb(x), filename.tds(x), or filename.hyper

Publishes the specified workbook (.twb(x)), data source (.tds(x)), or extract (.hyper) to Tableau Server.

If you are publishing a workbook, by default, all sheets in the workbook are published without database user names or passwords.
The permissions initially assigned to the workbook or data source are copied from the project that the file is published to. Permissions for the published resource can be changed after the file has been published.

If the workbook contains user filters, one of the thumbnail options must be specified.

**Example**

```sh
tabcmd publish "analysis.twbx" -n "Sales_Analysis" --db-username "jsmith" --db-password "secret-password"
```

```sh
tabcmd publish "analysis_sfdc.hyper" -n "Sales Analysis" --oauth-username "username" --save-oauth
```

If the file is not in the same directory as tabcmd, include the full path to the file.

**Example**

```sh
tabcmd publish "\\computer\volume\Tableau Workbooks\analysis.twbx" -n "Sales_Analysis" --db-username "jsmith" --db-password "secret-password"
```

```sh
tabcmd publish "\\computer\volume\Tableau Workbooks\analysis_sfdc.hyper" -n "Sales Analysis" --oauth-username "username" --save-oauth
```

**Options**

- `-n, --name`

  Name of the workbook or data source on the server. If omitted, the workbook, data source, or data extract will be named after filename.

- `-o, --overwrite`

  Overwrites the workbook, data source, or data extract if it already exists on the server.
-r, --project

Publishes the workbook, data source, or data extract into the specified project. Publishes to the "Default" project if not specified.

--parent-project-path

Specifies the name of the parent project for the nested project as specified with the -r option. For example, to specify a project called "Nested" that exists in a "Main" project, use the following syntax: --parent-project-path "Main" -r "Nested".

--db-username

Use this option to publish a database user name with the workbook, data source, or data extract.

--db-password

Use this option to publish a database password with the workbook, data source, or extract.

--save-db-password

Stores the provided database password on the server.

--oauth-username

The email address of the user account. Connects the user through a preconfigured OAuth connection, if the user already has a saved access token for the cloud data source specified in --name. Access tokens are managed in user preferences.

For existing OAuth connections to the data source, use this option instead of --db-username and --db-password.
**--save-oauth**

Saves the credential specified by **--oauth-username** as an embedded credential with the published workbook or data source.

Subsequently, when the publisher or server administrator signs in to the server and edits the connection for that workbook or data source, the connection settings will show this OAuth credential as embedded in the content.

If you want to schedule extract refreshes after publishing, you must include this option with **--oauth-username**. This is analogous to using **--save-db-password** with a traditional database connection.

**--thumbnail-username**

If the workbook contains user filters, the thumbnails will be generated based on what the specified user can see. Cannot be specified when **--thumbnail-group** option is set.

**--thumbnail-group**

If the workbook contains user filters, the thumbnails will be generated based on what the specified group can see. Cannot be specified when **--thumbnail-username** option is set.

**--tabbed**

When a workbook with tabbed views is published, each sheet becomes a tab that viewers can use to navigate through the workbook. Note that this setting will override any sheet-level security.

**--append**

Append the extract file to the existing data source.
Tableau Server on Linux Administrator Guide

--replace

Use the extract file to replace the existing data source.

--disable-uploader

Disable the incremental file uploader.

--restart

Restart the file upload.

Global options

The following options are used by all \texttt{tabcmd} commands. The \texttt{--server}, \texttt{--user}, and \texttt{--password} options are required at least once to begin a session. An authentication token is stored so subsequent commands can be run without including these options. This token remains valid for five minutes after the last command that used it.

\texttt{-h, --help}

Displays the help for the command.

\texttt{-c, --use-certificate}

Use client certificate to sign in. Required when mutual SSL is enabled.

For information about configuring the certificate, start with the following topic appropriate for your Tableau Server OS:

- \textbf{Windows}: Configure Mutual SSL
- \textbf{Linux}: Configure Mutual SSL

\texttt{-s, --server}
The Tableau Server URL, which is required at least once to begin session.

-u, --user

The Tableau Server username, which is required at least once to begin session.

-p, --password

The Tableau Server password, which is required at least once to begin session.

--password-file

Allows the password to be stored in the given .txt file rather than the command line for increased security.

-t, --site

Indicates that the command applies to the site specified by the Tableau Server site ID. If you do not specify a site, the Default site is assumed. Applies only to servers with multiple sites.

-x, --proxy

Host:Port

Uses the specified HTTP proxy.

--no-prompt

When specified, the command will not prompt for a password. If no valid password is provided the command will fail.

--no-proxy

When specified, an HTTP proxy will not be used.
Tableau Server on Linux Administrator Guide

--no-certcheck

When specified, tabcmd (the client) does not validate the server's SSL certificate.

--[no-]cookie

When specified, the session ID is saved on login so subsequent commands will not need to log in. Use the no- prefix to not save the session ID. By default the session is saved.

--timeout

Waits the specified number of seconds for the server to complete processing the command. By default the process will timeout in 30 seconds.

--

Specifies the end of options on the command line. You can use -- to indicate to tabcmd that anything that follows -- should not be interpreted as an option setting and can instead be interpreted as a value for the command. This is useful if you need to specify a value in the command that includes a hyphen. The following example shows how you might use -- in a tabcmd command, where -430105/SHEET1 is a required value for the export command.

    tabcmd export --csv -f "D:\export10.csv" -- -430105/SHEET1

publishsamples

Description

Publishes Tableau Sample workbooks to the specified project. Any existing samples will be overwritten.

Syntax

    tabcmd publishsamples -n [project name] [Global options]

Example
Publish samples to the Inside Sales project on the Default site, as user jsmith.

tabcmd publishesamples -n "Inside Sales" -t "" -s localhost --username "jsmith" --password "secret-password"

Options

-n, --name

Required. Publishes the Tableau samples into the specified project. If the project name includes spaces, enclose the entire name in quotes.

--parent-project-path

Specifies the name of the parent project for the nested project as specified with the -n option. For example, to specify a project called "Nested" that exists in a "Main" project, use the following syntax: --parent-project-path "Main" -n "Nested".

Global options

The following options are used by all tabcmd commands. The --server, --user, and --password options are required at least once to begin a session. An authentication token is stored so subsequent commands can be run without including these options. This token remains valid for five minutes after the last command that used it.

-h, --help

Displays the help for the command.

-c, --use-certificate

Use client certificate to sign in. Required when mutual SSL is enabled.
Tableau Server on Linux Administrator Guide

For information about configuring the certificate, start with the following topic appropriate for your Tableau Server OS:

- **Windows**: Configure Mutual SSL

- **Linux**: Configure Mutual SSL

-s, --server

The Tableau Server URL, which is required at least once to begin session.

-u, --user

The Tableau Server username, which is required at least once to begin session.

-p, --password

The Tableau Server password, which is required at least once to begin session.

--password-file

Allows the password to be stored in the given .txt file rather than the command line for increased security.

-t, --site

Indicates that the command applies to the site specified by the Tableau Server site ID. If you do not specify a site, the Default site is assumed. Applies only to servers with multiple sites.

-x, --proxy

Host:Port

Uses the specified HTTP proxy.
When specified, the command will not prompt for a password. If no valid password is provided the command will fail.

When specified, an HTTP proxy will not be used.

When specified, tabcmd (the client) does not validate the server's SSL certificate.

When specified, the session ID is saved on login so subsequent commands will not need to log in. Use the no- prefix to not save the session ID. By default the session is saved.

Waits the specified number of seconds for the server to complete processing the command. By default the process will timeout in 30 seconds.

Specifies the end of options on the command line. You can use -- to indicate to tabcmd that anything that follows -- should not be interpreted as an option setting and can instead be interpreted as a value for the command. This is useful if you need to specify a value in the command that includes a hyphen. The following example shows how you might use -- in a tabcmd command, where -430105/Sheet1 is a required value for the export command.

tabcmd export --csv -f "D:\export10.csv" -- -430105/Sheet1
refreshextracts **workbook-name** or **datasource-name**

Performs a full or incremental refresh of extracts belonging to the specified workbook or data source.

This command takes the name of the workbook or data source as it appears on the server, not the file name when it was published. Only an administrator or the owner of the workbook or data source is allowed to perform this operation.

**Examples**

```
tabcmd refreshextracts --datasource sales_ds
```

```
tabcmd refreshextracts --project "Sales External" --datasource sales_ds
```

```
tabcmd refreshextracts --workbook "My Workbook"
```

```
tabcmd refreshextracts --url SalesAnalysis
```

```
tabcmd refreshextracts --workbook "My Workbook" --addcalculations
```

```
tabcmd refreshextracts --datasource sales_ds --removecalculations
```

**Options**

```
--incremental

    Runs the incremental refresh operation.
```

```
--synchronous

    Adds the full refresh operation to the queue used by the Backgrounder process, to be run as soon as a Backgrounder process is available. If a Backgrounder process is available, the operation is run immediately. The refresh operation appears on the
Background Tasks report.

During a synchronous refresh, `tabcmd` maintains a live connection to the server while the refresh operation is underway, polling every second until the background job is done.

`--workbook`

The name of the workbook containing extracts to refresh. If the workbook has spaces in its name, enclose it in quotes.

`--datasource`

The name of the data source containing extracts to refresh.

`--project`

Use with `--workbook` or `--datasource` to identify a workbook or data source in a project other than Default. If not specified, the Default project is assumed.

`--parent-project-path`

Specifies the name of the parent project for the nested project as specified with the `--project` option. For example, to specify a project called "Nested" that exists in a "Main" project, use the following syntax: `--parent-project-path "Main" --project "Nested"`.

`--url`

The name of the workbook as it appears in the URL. A workbook published as “Sales Analysis” has a URL name of “SalesAnalysis”.

`--addcalculations`

Use with `--workbook` to materialize calculations in the embedded extract of the
workbook or --datasource to materialize calculations in the extract data source. Adds the operation to the queue used by the Backgrounder process. If a Backgrounder process is available, the operation runs immediately. This operation appears on the Background Tasks for Extracts administrative view.

--removecalculations

Use with --workbook or --datasource to remove calculations that were previously materialized. Adds the operation to the queue used by the Backgrounder process. If a Backgrounder process is available, the operation runs immediately. This operation appears on the Background Tasks for Extracts administrative view.

Global options

The following options are used by all tabcmd commands. The --server, --user, and --password options are required at least once to begin a session. An authentication token is stored so subsequent commands can be run without including these options. This token remains valid for five minutes after the last command that used it.

-h, --help

Displays the help for the command.

-c, --use-certificate

Use client certificate to sign in. Required when mutual SSL is enabled.

For information about configuring the certificate, start with the following topic appropriate for your Tableau Server OS:

- **Windows**: Configure Mutual SSL

- **Linux**: Configure Mutual SSL

-s, --server
The Tableau Server URL, which is required at least once to begin session.

-u, --user

The Tableau Server username, which is required at least once to begin session.

-p, --password

The Tableau Server password, which is required at least once to begin session.

--password-file

Allows the password to be stored in the given .txt file rather than the command line for increased security.

-t, --site

Indicates that the command applies to the site specified by the Tableau Server site ID. If you do not specify a site, the Default site is assumed. Applies only to servers with multiple sites.

-x, --proxy

Host:Port

Uses the specified HTTP proxy.

--no-prompt

When specified, the command will not prompt for a password. If no valid password is provided the command will fail.

--no-proxy

When specified, an HTTP proxy will not be used.
--no-certcheck

When specified, tabcmd (the client) does not validate the server's SSL certificate.

--[no-]cookie

When specified, the session ID is saved on login so subsequent commands will not need to log in. Use the no- prefix to not save the session ID. By default the session is saved.

--timeout

Waits the specified number of seconds for the server to complete processing the command. By default the process will timeout in 30 seconds.

--

Specifies the end of options on the command line. You can use -- to indicate to tabcmd that anything that follows -- should not be interpreted as an option setting and can instead be interpreted as a value for the command. This is useful if you need to specify a value in the command that includes a hyphen. The following example shows how you might use -- in a tabcmd command, where -430105/Sheet1 is a required value for the export command.

```
tabcmd export --csv -f "D:\export10.csv" -- -430105/Sheet1
```

removeusers group-name

Removes users from the specified group.

Example

tabcmd removeusers "Development" --users "users.csv"

Options

--users
Remove the users in the given .csv file from the specified group. The file should be a simple list with one user name per line.

`--[no-]complete`

Requires that all rows be valid for any change to succeed. If not specified `--complete` is used.

Global options

The following options are used by all `tabcmd` commands. The `--server`, `--user`, and `--password` options are required at least once to begin a session. An authentication token is stored so subsequent commands can be run without including these options. This token remains valid for five minutes after the last command that used it.

`-h, --help`

Displays the help for the command.

`-c, --use-certificate`

Use client certificate to sign in. Required when mutual SSL is enabled.

For information about configuring the certificate, start with the following topic appropriate for your Tableau Server OS:

- **Windows**: Configure Mutual SSL
- **Linux**: Configure Mutual SSL

`-s, --server`

The Tableau Server URL, which is required at least once to begin session.

`-u, --user`
The Tableau Server username, which is required at least once to begin session.

-p, --password

The Tableau Server password, which is required at least once to begin session.

--password-file

Allows the password to be stored in the given .txt file rather than the command line for increased security.

-t, --site

Indicates that the command applies to the site specified by the Tableau Server site ID. If you do not specify a site, the Default site is assumed. Applies only to servers with multiple sites.

-x, --proxy

Host:Port

Uses the specified HTTP proxy.

--no-prompt

When specified, the command will not prompt for a password. If no valid password is provided the command will fail.

--no-proxy

When specified, an HTTP proxy will not be used.

--no-certcheck

When specified, tabcmd (the client) does not validate the server’s SSL certificate.
--[no-]cookie

When specified, the session ID is saved on login so subsequent commands will not need to log in. Use the no- prefix to not save the session ID. By default the session is saved.

--timeout

Waits the specified number of seconds for the server to complete processing the command. By default the process will timeout in 30 seconds.

--

Specifies the end of options on the command line. You can use -- to indicate to tabcmd that anything that follows -- should not be interpreted as an option setting and can instead be interpreted as a value for the command. This is useful if you need to specify a value in the command that includes a hyphen. The following example shows how you might use -- in a tabcmd command, where -430105/Sheet1 is a required value for the export command.

```
tabcmd export --csv -f "D:\export10.csv" -- -430105/Sheet1
```

runschedule schedule-name

Runs the specified schedule.

This command takes the name of the schedule as it is on the server.

For Tableau Online, the command can be run within the scope of a single site, using site administrator permissions.

Example

```
tabcmd runschedule "5AM Sales Refresh"
```

Global options

The following options are used by all tabcmd commands. The --server, --user, and --
-password options are required at least once to begin a session. An authentication token is stored so subsequent commands can be run without including these options. This token remains valid for five minutes after the last command that used it.

-h, --help

Displays the help for the command.

-c, --use-certificate

Use client certificate to sign in. Required when mutual SSL is enabled.

For information about configuring the certificate, start with the following topic appropriate for your Tableau Server OS:

- **Windows**: [Configure Mutual SSL](#)
- **Linux**: [Configure Mutual SSL](#)

-s, --server

The Tableau Server URL, which is required at least once to begin session.

-u, --user

The Tableau Server username, which is required at least once to begin session.

-p, --password

The Tableau Server password, which is required at least once to begin session.

--password-file

Allows the password to be stored in the given .txt file rather than the command line for increased security.
-t, --site

Indicates that the command applies to the site specified by the Tableau Server site ID. If you do not specify a site, the Default site is assumed. Applies only to servers with multiple sites.

-x, --proxy

Host:Port

Uses the specified HTTP proxy.

--no-prompt

When specified, the command will not prompt for a password. If no valid password is provided the command will fail.

--no-proxy

When specified, an HTTP proxy will not be used.

--no-certcheck

When specified, tabcmd (the client) does not validate the server's SSL certificate.

--cookie

When specified, the session ID is saved on login so subsequent commands will not need to log in. Use the no- prefix to not save the session ID. By default the session is saved.

--timeout

Waits the specified number of seconds for the server to complete processing the command. By default the process will timeout in 30 seconds.
Specifies the end of options on the command line. You can use -- to indicate to tabcmd that anything that follows -- should not be interpreted as an option setting and can instead be interpreted as a value for the command. This is useful if you need to specify a value in the command that includes a hyphen. The following example shows how you might use -- in a tabcmd command, where -430105/Sheet1 is a required value for the export command.

```bash
tabcmd export --csv -f "D:\export10.csv" -- -430105/Sheet1
```

**set setting**

Enables the specified setting on the server. Details about each setting can be seen on the Maintenance page on the server.

Use an exclamation mark in front of the setting name to disable the setting. You can enable or disable the following settings:

- allow_scheduling
- embedded_credentials
- remember_passwords_forever

**Example**

```bash
tabcmd set embedded_credentials
```

**Global options**

The following options are used by all tabcmd commands. The --server, --user, and --password options are required at least once to begin a session. An authentication token is stored so subsequent commands can be run without including these options. This token remains valid for five minutes after the last command that used it.
-h, --help
Displays the help for the command.

-c, --use-certificate
Use client certificate to sign in. Required when mutual SSL is enabled.
For information about configuring the certificate, start with the following topic appropriate for your Tableau Server OS:

- Windows: Configure Mutual SSL
- Linux: Configure Mutual SSL

-s, --server
The Tableau Server URL, which is required at least once to begin session.

-u, --user
The Tableau Server username, which is required at least once to begin session.

-p, --password
The Tableau Server password, which is required at least once to begin session.

--password-file
Allows the password to be stored in the given .txt file rather than the command line for increased security.

-t, --site
Indicates that the command applies to the site specified by the Tableau Server site ID. If you do not specify a site, the Default site is assumed. Applies only to servers with
multiple sites.

-x, --proxy

    Host:Port

    Uses the specified HTTP proxy.

--no-prompt

    When specified, the command will not prompt for a password. If no valid password is provided the command will fail.

--no-proxy

    When specified, an HTTP proxy will not be used.

--no-certcheck

    When specified, tabcmd (the client) does not validate the server's SSL certificate.

--[no-]cookie

    When specified, the session ID is saved on login so subsequent commands will not need to log in. Use the no- prefix to not save the session ID. By default the session is saved.

--timeout

    Waits the specified number of seconds for the server to complete processing the command. By default the process will timeout in 30 seconds.

--

    Specifies the end of options on the command line. You can use -- to indicate to tabcmd that anything that follows -- should not be interpreted as an option setting and can
instead be interpreted as a value for the command. This is useful if you need to specify a value in the command that includes a hyphen. The following example shows how you might use -- in a tabcmd command, where -430105/SHEET1 is a required value for the export command.

```
tabcmd export --csv -f "D:\export10.csv" -- -430105/SHEET1
```

**syncgroup group-name**

Synchronizes a Tableau Server group with an Active Directory group. If the Tableau Server group does not already exist, it is created and synchronized with the specified Active Directory group.

If the group name itself includes an "@" (other than as the domain separator) you need to refer to the symbol using the hex format "\0x40".

**Example**

```
tabcmd syncgroup "Development"
```

```
tabcmd syncgroup "Dev\0x40West"
```

**Note:** If you synchronize a group that you are a member of, changes that you make using this command do not apply to your user. For example, if you use this command to remove the administrator right from users in a group that you are a member of, you are still an administrator when the command finishes.

**Options**

--no-publisher

Deprecated. Use the --role option instead.

--overwritesiterole
Tableau Server on Linux Administrator Guide

Allows a user’s site role to be overwritten with a less privileged one when using 
--role. By default, a user site role can be promoted when using --role, but cannot 
be demoted. Because the --overwritesiterole option will demote user site roles, 
use it with caution.

--publisher

Deprecated. Use the --role option instead.

-r, --role

Specifies a site role for users in the group. The default is Unlicensed.

--silent-progress

Do not display progress messages for the command.

Global options

The following options are used by all tabcmd commands. The --server, --user, and -- 
password options are required at least once to begin a session. An authentication token is 
stored so subsequent commands can be run without including these options. This token 
remains valid for five minutes after the last command that used it.

-h, --help

Displays the help for the command.

-c, --use-certificate

Use client certificate to sign in. Required when mutual SSL is enabled.
For information about configuring the certificate, start with the following topic appropriate for your Tableau Server OS:

- **Windows**: Configure Mutual SSL
- **Linux**: Configure Mutual SSL

**-s, --server**

The Tableau Server URL, which is required at least once to begin session.

**-u, --user**

The Tableau Server username, which is required at least once to begin session.

**-p, --password**

The Tableau Server password, which is required at least once to begin session.

**--password-file**

Allows the password to be stored in the given `.txt` file rather than the command line for increased security.

**-t, --site**

Indicates that the command applies to the site specified by the Tableau Server site ID. If you do not specify a site, the Default site is assumed. Applies only to servers with multiple sites.

**-x, --proxy**

Host:Port

Uses the specified HTTP proxy.
--no-prompt

When specified, the command will not prompt for a password. If no valid password is provided the command will fail.

--no-proxy

When specified, an HTTP proxy will not be used.

--no-certcheck

When specified, tabcmd (the client) does not validate the server’s SSL certificate.

--[no-]cookie

When specified, the session ID is saved on login so subsequent commands will not need to log in. Use the no- prefix to not save the session ID. By default the session is saved.

--timeout

Waits the specified number of seconds for the server to complete processing the command. By default the process will timeout in 30 seconds.

--

Specifies the end of options on the command line. You can use -- to indicate to tabcmd that anything that follows -- should not be interpreted as an option setting and can instead be interpreted as a value for the command. This is useful if you need to specify a value in the command that includes a hyphen. The following example shows how you might use -- in a tabcmd command, where -430105/Sheet1 is a required value for the export command.

```
tabcmd export --csv -f "D:\export10.csv" -- -430105/Sheet1
```

version

Displays the version information for the current installation of the tabcmd utility.
Example

tabcmd version

Global options

The following options are used by all tabcmd commands. The --server, --user, and --password options are required at least once to begin a session. An authentication token is stored so subsequent commands can be run without including these options. This token remains valid for five minutes after the last command that used it.

-h, --help

Displays the help for the command.

-c, --use-certificate

Use client certificate to sign in. Required when mutual SSL is enabled.

For information about configuring the certificate, start with the following topic appropriate for your Tableau Server OS:

- Windows: Configure Mutual SSL
- Linux: Configure Mutual SSL

-s, --server

The Tableau Server URL, which is required at least once to begin session.

-u, --user

The Tableau Server username, which is required at least once to begin session.

-p, --password
The Tableau Server password, which is required at least once to begin session.

--password-file

Allows the password to be stored in the given .txt file rather than the command line for increased security.

-t, --site

Indicates that the command applies to the site specified by the Tableau Server site ID. If you do not specify a site, the Default site is assumed. Applies only to servers with multiple sites.

-x, --proxy

Host:Port

Uses the specified HTTP proxy.

--no-prompt

When specified, the command will not prompt for a password. If no valid password is provided the command will fail.

--no-proxy

When specified, an HTTP proxy will not be used.

--no-certcheck

When specified, tabcmd (the client) does not validate the server's SSL certificate.

--[no-]cookie

When specified, the session ID is saved on login so subsequent commands will not
need to log in. Use the no- prefix to not save the session ID. By default the session is saved.

--timeout

Waits the specified number of seconds for the server to complete processing the command. By default the process will timeout in 30 seconds.

--

Specifies the end of options on the command line. You can use -- to indicate to tabcmd that anything that follows -- should not be interpreted as an option setting and can instead be interpreted as a value for the command. This is useful if you need to specify a value in the command that includes a hyphen. The following example shows how you might use -- in a tabcmd command, where -430105/Sheet1 is a required value for the export command.

```
tabcmd export --csv -f "D:\export10.csv" -- -430105/Sheet1
```

Troubleshooting

Troubleshoot Tableau Server on Linux

Follow the suggestions in this topic to resolve common issues with Tableau Server. For additional troubleshooting steps based on process status viewed on the Status page, see Troubleshoot Server Processes.

The following table displays the default locations of the installation, data, logs, and scripts directories:

<table>
<thead>
<tr>
<th>Directory</th>
<th>Default location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation:</td>
<td>/opt/tableau/tableau_server</td>
</tr>
<tr>
<td>Data:</td>
<td>/var/opt/tableau/tableau_server/data</td>
</tr>
<tr>
<td>Directory</td>
<td>Default location</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td>Logs:</td>
<td>/var/opt/tableau/tableau_server/data/tabsvc/logs/</td>
</tr>
<tr>
<td>Scripts:</td>
<td>/opt/tableau/tableau_server-&lt;version_code&gt;/scripts.</td>
</tr>
</tbody>
</table>

**General Troubleshooting Steps**

Many Tableau Server issues can be addressed or tested with one or more of these basic steps:

**Clean install**

Install Tableau Server on Linux on a computer that has never had Tableau installed on it. If you are reusing a computer or VM that has had a previous version of Tableau Server installed, follow the steps in Remove Tableau Server from Your Computer to clean Tableau off your computer before you install the new version.

If you run into problems installing Tableau Server you may need to entirely remove Tableau from your computer and do a clean install. See Remove Tableau Server from Your Computer for details.

**Disk space**

Make sure there is enough disk space on each computer running Tableau Server. Limited disk space can cause a failure to install, a failure to upgrade, or problems running Tableau Server.

**Remove old log files**

If you are running out of disk space you can clean up old Tableau Server log files. These can take up space and as a best practice you should remove them regularly.

**Version 10.5.x**
If you have version 10.5.1 and higher, run this command at a terminal prompt to clean up log files you do not need:

```
tsm maintenance cleanup
```

**Version 10.5.0**

If you are running version 10.5.0 of Tableau Server on Linux, the cleanup command is not available and you need to run these commands at a terminal prompt:

```
sudo find /var/opt/tableau/tableau_server/data/tabsvc/temp/* -mtime +2 -type f -delete
```

```
sudo find /var/opt/tableau/tableau_server/data/tabsvc/logs/* -mtime +2 -type f -delete
```

**Important:** The Linux file system makes it possible to delete files that are open and if you do this the Tableau processes may not be able to recreate the files. This will result in empty log files. To fix this you can stop Tableau Server, restart the TSM Controller, and restart Tableau again:

1. **Stop Tableau Server:**
   
   `tsm stop`

2. **Restart the TSM Controller:**
   
   `sudo systemctl restart tabadmincontroller_0.service`

3. **Wait several minutes for the controller to restart. You can confirm the controller has restarted with this command:**
   
   `tsm status -v`

   When you can run that command and the Tableau Server Administration Controller is listed as 'running' the controller has restarted.
4. Start Tableau Server:

   tsm start

Manually gather logs

If you cannot run tsm maintenance ziplogs for any reason (for example, if you have a critical failure before you run tsm initialize), you can manually collect and zip the logs by running these commands in a terminal window:

   cd /var/opt/tableau/tableau_server/data/tabsvc/

   cp /var/opt/tableau/tableau_server/logs/app-install.log logs

   cp ~/.tableau/tsm/tsm.log logs

   tar -czvf ~/logs.tar.gz logs

This creates a file called logs.tar.gz in your home directory. You can upload or send this file to Tableau.

Restart server

Restart Tableau Server. Issues related to indexing and processes not fully started can be resolved by restarting Tableau Server in a controlled way. To restart Tableau Server, use the tsm restart command. This will stop all the processes associated with Tableau Server and then restart them.

Edit installation and configuration files using Linux

You should edit or create any files used to install or configure Tableau Server on Linux using a Linux operating system. Files created using Microsoft Windows will cause errors in Tableau Server on Linux installation and configuration because Linux operating systems end files with a line-feed (LF) character, whereas Windows ends files with a carriage-return character and a line-feed character (CR LF). Non-Linux (CR LF) file endings can cause errors during Automated Installation of Tableau Server if they appear in the config.json, reg_templ.json or secrets files used by the automated installer. Non-Linux (CR LF) file
endings can also cause errors during registration or when configuring identity store settings or gateway settings.

Check systemd logs

If Tableau Server will not start, and you do not find anything useful in the Tableau logs (see Work with Log Files for more information) you can check the logs at /var/-logs/messages for messages related to the TSM Service starting and stopping.

Installing Tableau Server

Install fails due to hardware requirements

Tableau Server cannot install if the computer you are installing on does not meet the minimum hardware requirements. For details on requirements, see Before you install....

Install fails due to timeouts

If you install Tableau Server on a computer with limited resources, for example, a computer that just meets the minimum hardware requirements, you can run into problems where tsm commands timeout due to slow response. You can specify a longer timeout by using the global --request-timeout option on all tsm commands. For more information on the --request-timeout option, see for example, tsm initialize.

Install fails with "Failed to initialize the instance of the temporary database"

Tableau Server on Linux only supports UTF-8 character encoding. If your Linux locale is missing the UTF-8 encoding, your installation can fail with an error similar to this one:

Failed to initialize the instance of the temporary database

To check if your locale is using UTF-8 encoding, run the localectl command at a command prompt. The resulting output should look something like this (your locale may be different):

```
[tableauserver-centos1a ~]$ localectl
System Locale: LANG=en_US.UTF-8
```

Tableau Server on Linux Administrator Guide

If the `LANG` value does not include `.UTF-8` then you need to run `localectl` to add it:

```
sudo localectl set-locale LANG=<your_locale>.UTF-8
```

**Note:** In some cases `localectl` may not complete (timeout) if your version of `systemd` is old. Updating `systemd` may fix this problem and allow you to set the UTF-8 encoding. On RHEL-like systems, use this command to update `systemd`:

```
sudo yum update systemd
```

Installation fails on a virtual machine in Parallels

Parallels is currently not supported. If you install Tableau Server on a Linux virtual machine in Parallels, the install might fail.

Tableau Server doesn't start

If Tableau Server does not start or is running in a degraded state, run the `tsm restart` command. This will shut down any processes that are running, and restart Tableau Server.

Cannot start Tableau Server after installation

Tableau Server might not start if your computer's hostname changes after installation. One of the main reasons why the hostname might change is if you use the `cloud-init` package on CentOS. If you use the cloud-init package, `reboot the computer` where you want to install Tableau Server before you begin the installation process. Alternatively, you can fix the hostname without rebooting by running the following command:

```
sudo hostnamectl set-hostname `hostnamectl --static`
```

The cloud-init package is commonly used to initialize new virtual machines, configure SSH public key authentication, and more. For example, some CentOS images use cloud-init, and cloud-init is commonly used in OpenStack deployments. However, the version of cloud-init included by default in the CentOS 7.x repositories (cloud-init 0.7.5-10.el7.centos.1) has a known issue that prevents your computer from displaying its Fully Qualified Domain Name (FQDN) along with its hostname until after it restarts.
Because the Tableau Server installation process uses your computer’s hostname to configure server processes and generate TLS certificates, Tableau Server might not start if it is configured to use a hostname without the FQDN.

To determine if your computer is displaying the correct hostname, run the `hostnamectl` command. In the following example, the command displays a transient hostname which indicates that it will not return the FQDN and must be restarted.

```
$ hostnamectl
  Static hostname: server01.example.com
  Transient hostname: server01
[...]
```

Alternatively, in the following example, the command displays the correct hostname and FQDN:

```
$ hostnamectl
  Static hostname: server01.example.com
[...]
```

```
Cannot create initial administrator account with multiple Active Directory (AD) domains
```

When you create the initial administrator account on Tableau Server, you might see the following error if you selected AD as the authentication type:

```
Failed to authenticate username and password
```

This occurs when Tableau Server attempts to connect to multiple AD domains. For example, you might see this error if you install Tableau Server on a computer that is part of one domain and you attempt to authenticate AD users that are part of another domain.

**Fonts**

Tableau Server uses the fonts installed on the system to render workbooks based on the fonts used when a workbook was created. When a font is not available, Tableau Server will use the closest equivalent based on font families; this is true for both Windows and Linux Servers. On Linux Servers missing fonts may be more obvious because Linux ships with
fewer included fonts than Windows and OS/X systems do. This matters because many workbooks are authored in Tableau Desktop on Windows or on Mac.

Tableau Server on Linux ships with the following fonts:

- Arial
- Courier
- Georgia
- Times New Roman
- Verdana
- Trebuchet MS
- Tableau Font

Workbooks which use fonts other than these may appear differently than expected when viewed on Tableau Server on Linux, due to missing fonts. To resolve this issue, install the appropriate fonts onto all nodes in your Tableau Server installation.

Support for Asian character sets

If you see empty boxes where you expect to see Asian characters in workbooks that are displayed on Tableau Server, then you should install the language-appropriate font packages in your Linux environment.

Initializing Tableau Server

TSM initialization fails because the `tableau` user account exists but is not a member of the group `tableau`

When you install and initialize Tableau Services Manager (TSM) and Tableau Server, the initialization script (`initialize-tsm`) creates the users and groups needed to run, or confirms that the existing ones are configured with the required characteristics. By default the script creates a user called `tableau` and adds it to a group called `tableau`. If a `tableau` user already exists but is not part of the `tableau` group, the script fails with a warning.

If this happens you can fix the conflict by using a `--unprivileged-user` flag to specify a different user, and the user will be created and added to the `tableau` group.
For example, to specify a user named `tableauserver`, you would run the script from the `/opt/tableau/tableau_server/packages/scripts.<version_code>` directory using this command:

```
sudo ./initialize-tsm --unprivileged-user="tableauserver" --accepteula
```

For a complete list of options that can be used with the `initialize-tsm` script, use the `-h` option:

```
sudo ./initialize-tsm -h
```

Error initializing Tableau Server on unsupported system locale

If you attempt to install Tableau Server on a computer with a locale that is not one of the eight supported locales, you will get an error during installation.

Tableau Server will run on a system using one of the following locales:

```
```

Any other locale will generate the error.

Error initializing Tableau Server when `en_US.utf8` is not included in locale list

If you attempt to install Tableau Server on a computer that does not have `en_US.utf8` in the locale list, the initialization will fail with an error. To see if `en_US.utf8` is included, type `locale -a` at a shell prompt.

If `en_US.utf8` is not listed, you can `en_us` to the locale list by typing `sudo locale-gen en_US.UTF-8` at a shell prompt on Ubuntu, or `sudo localedef -i en_US -f UTF-8` at a shell prompt on RHEL-like distributions.

Error: status 10 - initializing Tableau Server when data directory path includes a period

If you attempt to install Tableau Server and specify a data directory with a path that includes a period ("."), initialization will fail with errors including:

```
Connection timed out
```
ERROR: TSM services returned status 10

To avoid this issue, choose a data directory that does not include a period in its path.

Error initializing Tableau Server after reinstallation

If you uninstall and reinstall Tableau Server, you can encounter an error initializing Tableau Server. For example, you might see the following error:

```
ERROR com tableausoftware.tabadmin.webapp.asyncjobs.JobStepRunner - Running step WaitForConfigure failed
com tableausoftware.tabadmin.webapp.exceptions.ServiceFailedStateException
```

This error occurs when artifacts remain from a previous installation that cause services to fail to start. To prevent this error, use the `tableau-server-obliterate` script in the `/opt/tableau/tableau_server/packages/scripts.<version_code>` folder. For more information about completely removing Tableau Server, see Remove Tableau Server from Your Computer.

Activating Tableau Server

Tableau Server license activation fails

In certain cases activation of the Tableau product key using the `tsm licenses activate -k <product_key>` command fails with an error:

```
License Server not available
```

This can happen if your computer is unable to connect through TCP port 443 to the Tableau licensing server at `licensing.tableau.com`.  

Tableau Software

Version: 2019.1

1375
To resolve this you need to configure your network and/or host-based firewalls to allow access to that address and port, or activate Tableau offline. For more information, see Activate Tableau Server Offline - Adding a License.

Reindexing Tableau Server Search & Browse

Problems that can be solved by reindexing Search & Browse

Symptoms of an index that needs to be rebuilt include:

- A blank list of sites when a user attempts to log in
- A blank list of projects when a user tries to select a project
- Missing content (workbooks, views, dashboards)
- Unexpected or inaccurate alerts (for example, an "refresh failed" alert on a workbook that does not include an extract)

If you see any of these behaviors, rebuild the Search & Browse index using the `tsm maintenance reindex-search` command.

Restarting Tableau Server

Restarting Tableau Server or applying changes fails

If one of the Tableau Server services fails, you might see an error when you attempt to restart the server or apply configuration changes.

To see if a failed service is causing the error, type the following command:

```bash
tsm status -v
```

To find out why a service failed, view the tabadminagent and tabadmincontroller log files in the data directory. For example, a service might fail because of concurrency issues or port configuration issues. Please include any issues you encounter in your feedback.

As a workaround, you can attempt to resolve the failure by removing and re-adding the service in TSM. Once the service has started, you can retry your previous configuration change or retry restarting the server with the `tsm restart` command.
Tableau Server on Linux Administrator Guide

Error restarting Tableau Server after adding or configuring a node

If you add a or configure the node without a Gateway process, Tableau Server might fail to restart and you could see errors like these:

ERROR : com.tableausoftware.tabadmin.configuration.PortConfigurationExtractor
- Unable to find port config key worker1.gateway.port

and

Message: Missing port configuration value for key 'worker1.gateway.port'

These errors appear in the gateway.log file and occur when a Tableau Server node is configured with either an Application Server or VizQL Server but without a Gateway. A Gateway process is required if either Application Server or VizQL Server is running on a node.

Backup/Restore

Problems related to restoring a backup created by Tableau Server can be the result of permissions issues. Proper permissions are necessary for both the file that TSM is restoring, and the location of the file. When TSM handles the backup, it puts the file in a default location and sets permissions appropriately. You can run into permission problems if you are restoring a backup that was copied to your Linux server, or a backup from a non-default location on your server. For details about using a non-default location, including how to change the location, see tsm File Paths.

Errors may include:

Server Was Denied Access to File

or

Restoring the backup '<backup>.tsbak' was unsuccessful

or
Comparing authentication methods failed

The Tableau Server backup and restore processes must have:

- Read permission—The processes need to access the .tsbak backup file directly.
- Execute permission—The processes also require execute permissions to the directory structure in which the .tsbak file is placed.

When TSM creates a backup in the default location, it sets the permissions it needs. If you copy a file to the Linux server, or move it to a non-default directory, the permissions may not allow the TSM processes proper access. You need to verify that both the file, and the directory tree that contains it, allow access by the TSM user tableau. The file permissions must give the tableau user read access to the .tsbak file. You can do this by setting the group on the file to the tableau group, and giving that group read access. The directory permissions must give the tableau user read access. You can do this by setting the group on the directory to the tableau group, and giving that group read and execute access on the directories.

For detailed information about TSM and file permissions, see Files and Permissions in TSM.

File locations

Changing basefilepath does not change the location of an existing file

Several tsm commands write files to default locations. You can change these default locations for each command using a tsm set command, but doing so does not move any existing files from the original location to the new one, and it does not create the new location.

You are responsible for creating the new location, and for making sure it has the correct permissions to allow tsm access to any files in the location, and the entire directory structure that contains the files.

For more information about changing default locations for backup, restore, site import and export, and ziplogs files, see tsm File Paths.

For information about tsm permissions, see Files and Permissions in TSM.
TSM commands

TSM command line does not show progress for long-running tasks

If you run a tsm command such as restore or ziplogs that takes more than 2 hours to complete, the command will continue to run until completion on the server. To display the progress of the job, use the `tsm jobs reconnect` command.

Opening Firewall ports

Manually opening firewall ports on Ubuntu

The current version of Tableau Server does not support the `ufw` firewall that is used on Ubuntu. For customers that do not want to install `firewalld` on Ubuntu, another option is to manually open those ports. The following steps will confirm that `ufw` is running, and open TCP ports 8850 and 80 to connections from any source address:

1. Run the following command to confirm `ufw` is running:

   ```bash
   sudo ufw status
   ```

   If the result is `Status: inactive`, you will need to enable `ufw` and ensure that you can continue to connect via `ssh`, which is outside the scope of these release notes.

2. Run the following command to allow access to port 8850:

   ```bash
   sudo ufw allow 8850
   ```

3. Run the following command to allow access to port 80:

   ```bash
   sudo ufw allow 80
   ```

OpenID fails on first sign-in attempt

If you have configured Open ID Connect authentication for Tableau Server, the first sign-in attempt fails. To successfully log in, users must retry authentication after the initial failure.
Administrative views do not display

The Status tab of Tableau Server includes links to visualizations that display server metrics. These visualizations require the PostgreSQL driver to access the appropriate data from the Tableau Server repository. The PostgreSQL driver is not installed automatically, so if you have not installed the driver, the views will not display. For more information, see Database Drivers.

Note: To use administrative views, the PostgreSQL driver must be installed on any node that runs the VizQL Server process.

Changing locale on view

When you change your user locale after opening a view, any subsequent attempt to open the view will fail with an "unexpected error." You can still open views that you have not previously opened.

To work around this issue, sign out of Tableau Server after changing your locale, and then sign back in. All views will display properly.

Work with Log Files

Tableau Server creates log files as a normal part of its activities. You may need to use the server log files when you are troubleshooting issues with Tableau Server or if Tableau Support requests logs from you to help you resolve an issue.

You can create a zipped log file archive using the tsm maintenance ziplogs command. The zipped archive contains copies of the logs you can unzip and look at, or send to Tableau Support. Once you have a copy of the archive, you can delete the archive from your server. For more information on log file archives, see Log File Snapshots (Archive Logs).
This collection of topics provides information about how to create log file archives, the contents of specific log files, and details about when and how you might want to look at a log.

Investigating Tableau Server Issues

The range and complexity of possible issues with Tableau Server means that there is no simple process you can use to investigate all problems, but a general approach would include these steps:

1. **Clean up** existing log files to reduce their size. For more information, see For more information, see Remove Unneeded Files.
2. **Set the appropriate logging level**. This is something that Tableau Support will instruct you on. For more information, see Change Logging Levels.
3. **Reproduce the issue** you are troubleshooting so the logs capture the events related to the problem.
4. **Create an archive** of the logs. For more information see Log File Snapshots (Archive Logs).

   **Important:** Use this archive when looking at the log files. You should not edit, move or delete any files directly on the server.

5. **Review the TSM Administration Controller log** (/tabadmincontroller/tabadmincontroller_node<n>-<n>.log) to understand any configuration or deployment done by TSM from the command line, Web UI, or API, including jobs started by TSM. Start with the controller log. This is where you'll get most useful information.

6. **Review the Apache logs** (/httpd/access.###_##_##_##_#.log and /httpd/error.log) for requests that may be related to the issue you are investigating.
The Apache logs will contain a fair amount of "noise" that does not apply to issues you are experiencing.

- If you find a request that seems to be related to your issue, search the `vizqlserver` directory for entries that include the unique request ID from the Apache logs.
- Look for the response code and message associated with the request ID.
- Search for the name of the workbook, view, dashboard, or data source that is related to your issue. Make sure to look for a relevant timestamp.
- If you find a request that seems to be related to your issue, look at the response code associated with the request. (200s are good, 500s indicate problems.)
- Locate the unique request ID associated with the request you've identified (the unique request ID is a 24 character alphanumeric string at the very end of the request).

7. **Review the log archive** further to search for other messages and possible errors.
   - Use the request ID from the Apache logs to search the `vizqlserver` folder of the log archive for files containing related log entries. Look for indications of a problem (for example, error messages or long-running queries).

8. **Review script logging**.

   Tableau Server includes logs for most of the bash scripts that are included in the `scripts` directory at `/opt/tableau/tableau_server-/packages/scripts.<version_code>/`. These logs are saved to the `/var/tmp` directory each time a script is run.
   - `<install_drive>\<install\path>\logs`
     by default:
   - `C:\ProgramData\Tableau\Tableau Server\logs`

9. **Contact support**

   If you are not able to solve the issue yourself, or if requested by Tableau Support, send the zipped archive to Tableau.
Server Log File Locations

By default, Tableau Server log file archives are gathered in a zip file called `logs.zip`, but you can specify a different filename when you create the archive with the `tsm maintenance ziplogs` command. You can copy the archive from the server to a local computer and open it there, or send it to Tableau Support.


When you unzip the archive, a series of zip files are created that start with the directory names shown below, and that end with a version number. These zip files contain the log files from the corresponding directories. The table in this topic explains the possible contents of these zip files, along with the original location the files came from on Tableau Server, the process that created the log files, and details about the files.

Tableau Server Log and Configuration File Locations

The Tableau Server log files are found in the following directory: `/var/-opt/tableau/tableau_server/data/tabsvc/logs/`

Logs not included in the ziplog archive

The `tsm maintenance ziplogs` command creates an archive of most of the Tableau Server logs, but some logs are not zipped up in the archive. Important logs not included in a log file archive:

- The TSM log. The `tsm.log` file is located in `/home dir`.<tableau>.	sm.
- The install log. The `app-install.log` file is located in `/var/-opt/tableau/tableau_server/logs`.
- The upgrade log. The `app-upgrade.log` file is located in `/var/-opt/tableau/tableau_server/logs`.
Bash script logging

Tableau Server includes logs for most of the bash scripts that are included in the scripts directory at /opt/tableau/tableau_server/packages/scripts.<version>. These logs are not included in the log file archive. Instead, the logs are saved to the /var/tmp directory each time a script is run.

System information

The log archives include system information gathered by running a number of system commands. The output for those commands are included in a subdirectory of the tabadminagent directory called sysinfo. See tabadminagent in the table below for more information.

Log Archive File Locations (unzipped archive)

<table>
<thead>
<tr>
<th>Log Archives in logs.zip</th>
<th>Details</th>
<th>Files</th>
<th>Generated by</th>
<th>Location on Tableau Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>app-zookeeper</td>
<td>Logs related to the Tableau Server Coordination Service.</td>
<td>appzookeeper-#.log, control_appzookeeper-#.log, spawn.#####.log</td>
<td>zookeeper.exe</td>
<td>/log-s/appzookeeper</td>
</tr>
<tr>
<td>backgrounder</td>
<td>Logs related to subscriptions and scheduled activities like extract refreshes, &quot;Run Now&quot;</td>
<td>backgrounder-#.log, spawn.#####.log, tomcat-#.#####-##-.log</td>
<td>backgrounder.exe</td>
<td>/log-s/backgrounder</td>
</tr>
</tbody>
</table>
### Tableau Server on Linux Administrator Guide

<table>
<thead>
<tr>
<th>Task Area</th>
<th>Logs Related</th>
<th>Logs Files</th>
<th>Directory Path</th>
</tr>
</thead>
</table>
| backuprestore | backup and restore scenarios. | control-backuprestore-#.log | /log-
s/backuprestore |
| cacheserver | Cache Server process. | control-cacheserver-#.log, redis_.log | /logs/cacheserver |
| clustercontroller | Cluster Controller process. | clustercontroller.log, clustercontroller.log-####-### | /log-
s/clustercontroller |
| database-maintenance | Database maintenance. | control-data-
basemaintenance-#.log, data-
basemaintenance-#.log, db-migrate.log, migration.log, spawn.####.log | /log-
s/data-
basemaintenance |
<p>| dataserver | Dataserver process. | dataserver-#.log | /logs/dataserver |</p>
<table>
<thead>
<tr>
<th>Connections to Tableau Server data sources.</th>
<th>Logs related to the Elastic Server process that is used by Ask Data.</th>
<th>/log-s/elasticserver</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>elasticserver</strong></td>
<td>control_elasticserver_node&lt;n&gt;.&lt;n&gt;.log</td>
<td>Elasticsearch.log</td>
</tr>
<tr>
<td></td>
<td>elasticsearch.log</td>
<td>Elasticsearch_deprecation.log</td>
</tr>
<tr>
<td></td>
<td>elasticsearch_index_indexing_slowlog.log</td>
<td>Elasticsearch_index_search_slowlog.log</td>
</tr>
<tr>
<td></td>
<td>stdout_elasticserver_node&lt;n&gt;.&lt;n&gt;.log</td>
<td>Stdout_elasticserver_node&lt;n&gt;.&lt;n&gt;.log</td>
</tr>
<tr>
<td><strong>filestore</strong></td>
<td>Logs related to the Tableau Server File Store process that controls the storage of extracts and</td>
<td>filestore.log</td>
</tr>
<tr>
<td></td>
<td>filestore.exe</td>
<td>/logs/filestore</td>
</tr>
</tbody>
</table>
Tableau Server on Linux Administrator Guide

<table>
<thead>
<tr>
<th>syncs extracts across nodes.</th>
<th>Apache logs. Look here for authentication entries. Each request in the Apache log will have a request ID associated with it. This request ID is used throughout the server logs and you can use it to associate log entries with a request.</th>
<th>access.####-##-#.#.##-##-##.log error.log startup.log</th>
<th>Apache daemon</th>
<th>/logs/httpd</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>Logs related to Tableau data engine. A log file is generated each day</td>
<td>checklicense.log control-hyper-0.log hyper_####<em>###</em>##<em>###</em>###.log</td>
<td>/logs/hyper</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>File Path</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interactive</td>
<td>Logs related to the Interactive Microservice Container.</td>
<td><code>control_interactive_&lt;node&gt;-&lt;instance&gt;-log</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>interactive_&lt;node&gt;-&lt;instance&gt;.log</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>stdout_interactive_&lt;node&gt;-&lt;instance&gt;.yyyy-mm-dd.log</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>tomcat_interactive_&lt;node&gt;-&lt;instance&gt;.yyyy-mm-dd.log</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Licenseservice</td>
<td>Logs related to licensing processes.</td>
<td><code>control-licenseservice.log</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>tabclicsrv.log</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NLP</td>
<td>Logs related to responses to VizQL server requests.</td>
<td><code>control_nlp_&lt;node&gt;&lt;n&gt;-&lt;n&gt;.log</code></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Tableau Server on Linux Administrator Guide**
<table>
<thead>
<tr>
<th>Logs related to the Ask Data service in Tableau Server.</th>
<th>stdout_nlp_node1-&lt;n&gt;-&lt;n&gt;.log</th>
<th>non-interactive Logs related to the Non-Interactive Microservice Container.</th>
<th>control_non-interactive_&lt;node&gt;-&lt;instance&gt;.log</th>
</tr>
</thead>
<tbody>
<tr>
<td>non-interactive</td>
<td>control_non-interactive_&lt;node&gt;-&lt;instance&gt;.log</td>
<td>non interactive_&lt;node&gt;-&lt;instance&gt;.log</td>
<td>stdout_non-interactive_&lt;node&gt;-&lt;instance&gt;.yyyy-mm-dd.log</td>
</tr>
<tr>
<td></td>
<td>non interactive_&lt;node&gt;-&lt;instance&gt;.log</td>
<td></td>
<td>tomcat_non-interactive_&lt;node&gt;-&lt;instance&gt;.yyyy-mm-dd.log</td>
</tr>
<tr>
<td>pgsql</td>
<td>Logs related to the PostgreSQL database (repository), including files related to launching server processes</td>
<td>control-pgsql-#.log</td>
<td>tabspawn</td>
</tr>
<tr>
<td></td>
<td></td>
<td>shut-downCommand.#####.log</td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>Logs Related to the Service</td>
<td>Logs File Path</td>
<td>Directory Path</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------</td>
<td>----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>samlservice</td>
<td>Logs related to the Security Assertion Markup Language (SAML) service in Tableau Server.</td>
<td>control-samlservice-#.log</td>
<td>/logs/samlservice</td>
</tr>
<tr>
<td>searchserver</td>
<td>Logs related to search indexing.</td>
<td>control-searchserver-#.log</td>
<td>/logs/searchserver</td>
</tr>
<tr>
<td>siteimportexport</td>
<td>Logs related to site import and export operations.</td>
<td>control-siteimportexport-0.log</td>
<td>/logs/siteimportexport</td>
</tr>
<tr>
<td>tabadminagent</td>
<td>Logs related to configuration and topology changes on each server node. Also included in a /sysinfo subdirectory is output from</td>
<td>control_tabadminagent_&lt;instance#&gt;.log</td>
<td>/logs/tabadminagent_&lt;instance#&gt;.&lt;version_code&gt;/config</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tabadminagent_&lt;instance#&gt;.log</td>
<td>/log-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>/log-</td>
</tr>
<tr>
<td>Directory</td>
<td>Description</td>
<td>File Paths</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>------------</td>
<td></td>
</tr>
<tr>
<td><code>various</code></td>
<td>System commands that provide details on the server machine and its state.</td>
<td><code>s/tabadmin_minagent_&lt;instance#&gt;.&lt;version_code&gt;/sysinfo</code></td>
<td></td>
</tr>
<tr>
<td>tabadmin-mincontroller</td>
<td>Logs related to the Tableau Services Manager (TSM) CLI and TSM API.</td>
<td><code>control-tabadmin-mincontroller-#.log</code>, <code>tabadmincontroller-#.log</code></td>
<td></td>
</tr>
<tr>
<td>tabsvc</td>
<td>Logs related to the startup and shutdown of other Tableau Server service processes.</td>
<td><code>control-tabsvc-#.log</code>, <code>tabsvc.log</code></td>
<td></td>
</tr>
<tr>
<td>vizportal</td>
<td>Logs related to administrative tasks, workbook and permissions management.</td>
<td><code>vizportal-0.log</code>, <code>vizportal-0.log.#####.###</code></td>
<td></td>
</tr>
</tbody>
</table>
authentication, sign-ins, initial view requests, and publishing requests.

These log files also include entries related to REST API requests. REST API log entries start with the receipt of the HTTP request, followed by information related to the processing of that request. If the request is completed, these log
entries end with the HTTP response code for that request.

| log | Logs related to displaying and interacting with views. When running multiple instances of VizQL Server, the instances are distinguished by port number. notify-production logs contain exceptional events. | control_vizqlserver_node##-0.log | tomcat_#.#####-##-.log | vizql-client-0.log#####-### | vizqlserver_node##-0.log | spawn#####.log | vizqlserver.exe | /logs/vizqlserver |
Log File Snapshots (Archive Logs)

Tableau Server includes functionality to generate a snapshot of log files for archival purposes. If you plan to clean up and delete old log files as part of regular server maintenance, you may consider archiving log files to an off-server storage location before deleting them.

Or, if you are working with Tableau Support on a case, the support engineer may request a server log file snapshot.

This topic describes:

- How to generate a log file snapshot
- How to send the snapshot directly to Tableau Support from the Tableau Server administration tools
- How to download the snapshot
- How to delete archived logs

Use the TSM web interface

1. Open TSM in a browser:

   https://<tsm-computer-name>:8850. For more information, see Sign in to Tableau Services Manager Web UI.

2. Click the Maintenance.

3. Generate a log file snapshot.


      An options dialog displays:
b. On the Options page, enter or select the options you want, including a **Description**, **time Range** of log files to be included, and the optional types of logs to be included (**Include Postgres Data**, **Include Recent Crash Dumps**), then click **Generate Log File Snapshot**.

The log file snapshot is saved to a fixed location on the computer where TSM and Tableau Server are installed. If you have a multi-node installation, the snapshot is saved to the initial node of the cluster. The location is specified by the `basefilepath_log_archives` variable.

By default the snapshot is saved to:

```
/var/opt/tableau/tableau_server/data/tabsvc/files/log-archives
```

You can find the current location by querying the `basefilepath.log_archives` setting, and change the location by specifying a new value for `basefilepath.log_archive`. For more information, see `tsm File Paths`.

4. After you generate the snapshot, you can select it and upload it to Technical Support, download it to your local machine, or delete it:
5. To download a local copy of the snapshot or to delete it, select the snapshot under Log Files and then select the appropriate Action.

Uploading log snapshots for Tableau Support

1. Click the Maintenance tab.

2. Select the snapshot you want to send.

3. Click Upload to Technical Support Case.

4. In the dialog that displays, enter the Support Case Number and your Contact.
Email Address, then click **Upload Snapshot**.

Use the TSM CLI

You create a snapshot archive of Tableau Server log files using the `tsm maintenance ziplogs` command.

By default, this command creates a zip file containing all of the log files. If you are running a distributed installation of Tableau Server, perform this step from the initial node. Logs from all nodes will be included in the zip file.

**Note:** If you cannot run the `ziplogs` command successfully, you can manually zip the Tableau Server logs. For more information, see Troubleshoot Tableau Server on Linux.

To create a log file snapshot:
1. On the initial node, open a terminal session.

2. Type the following command:

   tsm maintenance ziplogs -l -f <filename>

   where <filename> is name of the zipped archive file you want to create. Choose a unique name with no spaces. If an existing ziplog with the same file name already exists the creation of the file will fail unless you include the -o option to force an overwrite, delete the existing file, or specify a different name in the command.

   You can specify a time range for the snapshot and you can also specify which types of logs to include. For more information, see tsm maintenance ziplogs.

   The log file snapshot is saved to a fixed location on the computer where TSM and Tableau Server are installed. If you have a multi-node installation, the snapshot is saved to the initial node of the cluster. The location is specified by the basefilepath_log_archives variable.

   By default the log file snapshot is saved to:

   /var/opt/tableau/tableau_server/data/tabsvc/files/log-archives

   You can find the current location by querying the basefilepath.log_archives setting, and change the location by specifying a new value for basefilepath.log_archive. For more information, see tsm File Paths.

Sending log archives to Tableau Support

You can send log files to Tableau Support as a part of a customer support case (a customer support case number is required). Before sending a log file, use tsm maintenance ziplogs command to combine the log files into a single zip file archive. If you are creating the archive to send to Tableau Support, see the Knowledge Base for information about how to upload large files.
In a terminal session, type the following command:

```
  tsm maintenance send-logs -f <zip file name> -c <case number> -e <email address>
```

where `<case number>` is your support case number, `<email address>` is your contact email for this support case, and `<zip file name>` is the file name of your archive with .zip file extension.

Change Logging Levels

By default, Tableau Server logs events at the **Info** level. You can change this if you need to gather more information (if you are working with Tableau Support, for example). As a best practice you should not increase logging levels except when troubleshooting an issue.

Increasing the log level to debug or trace increases the amount of information being logged and can have a significant impact to performance. You should only set a logging level to debug when investigating a specific issue. Reproduce the issue and then reset the logging level back to info.

Logging Levels

The following logging levels are listed in order of increasing amount of information logged:

- off
- fatal
- error
- warn
- info (the default)
- debug
- trace

**Note:** Logging levels for new TSM processes are set at info and cannot be changed easily. If you are working with Tableau Technical Support and they determine that logs for these processes are needed, they can help you change the logging level temporarily.
Processes impacted by this limitation include: Administration Agent, Administration Controller, Client File Service, Service Manager, Database Maintenance, and Backup/Restore.

Change Logging Levels

Set logging levels for Tableau Server using one of several `tsm configuration set` commands. The command you use depends on which component of Tableau Server you want to change the logging level for.

<table>
<thead>
<tr>
<th>Configuration key</th>
<th>Location of affected logs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(path begins with /var/-opt/tableau/tableau_server-</td>
</tr>
<tr>
<td></td>
<td>/data/tabsvc/logs/)</td>
</tr>
<tr>
<td>&lt;process&gt;.native_api.log.level</td>
<td>/vizqlserver/*.txt</td>
</tr>
<tr>
<td></td>
<td>/vizqlserver/*.log</td>
</tr>
<tr>
<td></td>
<td>/vizqlserver./*.log</td>
</tr>
</tbody>
</table>

Valid process names are backgrounder, vizportal, vizqlserver, or data-server.

For more information, see `tsm configuration set Options`.

You need to stop Tableau Server before changing the logging levels, and restart it afterward. If you are running a distributed installation of Tableau Server, set logging levels from the initial node.

To change the logging level:
1. Stop Tableau Server by typing:

   tsm stop

2. Set the logging level to by typing tsm configuration set -k <config.key> -v <config_value>

   where <config.key> is <process>.native_api.log.level, viz-portal.log.level, or vizqlserver.log.level

   and <config_value> is a valid logging level.

   Examples:
   
   • tsm configuration set -k backgrounder.native_api.log.level -v debug
   • tsm configuration set -k vizqlserver.log.level -v warn
   • tsm configuration set -k vizportal.log.level -v debug

3. Apply pending changes by running the tsm pending-changes apply command.

4. Start Tableau Server by running the following command:

   tsm start

Reset Logging Levels

After you gather the information related to the issue you are investigating, reset the logging levels so there is no lingering performance impact.

Reset the logging level back to its default (info) using the appropriate command with a -d option.

Examples:

• tsm configuration set -k backgrounder.native_api.log.level -d
• tsm configuration set -k vizportal.log.level -d
• tsm configuration set -k vizqlserver.log.level -d

Troubleshoot Tableau Server Install and Upgrade

Follow the suggestions in this topic to resolve common issues with Tableau Server. For additional troubleshooting steps based on process status viewed on the Status page, see Troubleshoot Server Processes.

General Troubleshooting Steps

Many Tableau Server issues can be addressed with some basic steps:

1. Make sure there is enough disk space on each computer running Tableau Server. Limited disk space can cause a failure to install, a failure to upgrade, or problems running Tableau Server.

2. Restart Tableau Server. Issues related to indexing and processes not fully started can be resolved by restarting Tableau Server in a controlled way. To restart Tableau Server, use the tsm restart command. This will stop all the processes associated with Tableau Server and then restart them.

3. Reindex Tableau Server. Issues related to indexing can be resolved by reindexing Tableau Server. To reindex Tableau Server, use the tsm maintenance rein-dex-search command. For more information, see Reindexing Tableau Server Search & Browse below.

4. Restart the computer on which Tableau Server is running. Some issues, such as those related to data source connectivity, can be resolved by restarting the server computer.
Tableau Server on Linux Administrator Guide

Common Tableau Server Install Issues

Installation logs location

The install log, app-install.log, is located in /var/opt/tableau/tableau_server/logs.

The upgrade log, app-upgrade.log, is located in /var/opt/tableau/tableau_server/logs.

Unable to log into TSM or Tableau Server (sign in screen redisplayed after entering credentials)

Using Internet Explorer or Edge, if you enter your credentials into the TSM or Tableau Server sign-in screen and the page redisplayed without signing you in, verify that the hostname or domain in your URL does not include an underscore (_). If the hostname or domain of the Tableau Server computer includes an underscore (_) Internet Explorer or Edge browsers will not set a cookie, so the page will re-display without signing you in. To work around this, use "localhost" or the IP address of the computer in the URL. For example: https://localhost:8850.

For more information, see the Tableau Knowledge Base.

Multiple install attempts fail

If you attempt to install Tableau Server and the install fails, any subsequent installation attempts are likely to fail unless you run the tableau-server-obliterate script to clean Tableau off the computer.

A failed install attempt can leave the computer in a state that causes subsequent attempts to also fail with errors that don’t seem directly related to a previous install attempt. One possible error is:

Enabling and starting all services
+ services=(appzookeeper* tabadmincontroller* tabsvc* licenseservice* fnplicenseservice* tabadminagent* clientfileservice*)
+ systemctl_user enable appzookeeper_0.service 'tabadmincontroller*' 'tabsvc*' 'licenseservice*' fnplienceservice_0.service 'tabadminagent*' 'clientfileservice*' 
++ id -ru a_tabadminpoc 
+ local unprivileged_uid=222954 
+ su -l a_tabadminpoc -c 'XDG_RUNTIME_DIR=/run/user/222954 systemctl --user enable appzookeeper_0.service tabadmincontroller* tabsvc* licenseservice* fnplienceservice_0.service tabadminagent* clientfileservice*' 
Failed to execute operation: No such file or directory 

To fix this problem, run the tableau-server-obliterate script to clean up any left over remnants of the previous install attempt and then restart the computer. For more information, see Running the tableau-server-obliterate script.

Important: If you created a backup of Tableau (<file>.tsbak) you want to keep (for example, to restore to your new installation), copy that file to a safe location on another computer to guarantee it is not removed when you clean up your Tableau computer.

Install fails due to hardware requirements 

Tableau Server cannot install if the computer you are installing on does not meet the minimum hardware requirements. The requirements apply to all computers on which you are installing Tableau Server. For details on minimum hardware requirements, see Minimum Hardware Requirements and Recommendations for Tableau Server.

Common Tableau Server Upgrade Issues

Upgrade logs location 

The upgrade log, app-upgrade.log, is located in /var/opt/tableau/tableau_server/logs.
Upgrade multi-node, initializing additional node fails with "Enter your credentials again" error

If you attempt to initialize an additional node when upgrading Tableau Server and see this error:

Enter your credentials again. The credentials you enter must provide administrative access to the computer where you generated the configuration file.

This is an indication that the node is unable to connect to or communicate with the initial node. This can happen for multiple reasons:

- The credentials you entered are not valid or you mistyped them. The credentials must be for a user who has administrative permissions on the computer where Tableau Server was first installed. You do not need to use the credentials of the user who created the bootstrap file but doing so will ensure you are using valid credentials.

- The local firewall of the computer you are trying to add is not allowing communication to the initial node. For more information, see Local firewall configuration.

- The nodes are on different subnets. In distributed installations, all nodes should be installed on the same subnet. For more information, see Distributed Requirements.

Upgrading fails due to lack of disk space

If there is not enough disk space for the Tableau Server Setup program to run and do the upgrade, the installation will fail. The amount of disk space required will depend on the size of your repository database and the number and size of your extracts. As a part of upgrading to version 9.0, the Setup program migrates extracts to the new File Store and this takes space.

To free up disk space:

1. Create a log archive snapshot using the `tsm maintenance ziplogs` command.

   After you create the ziplogs file, save it to a safe location that is not part of your Tableau Server installation.
2. Clean up unnecessary files using the `tsm maintenance cleanup` command.
   For more information, see Remove Unneeded Files.

Starting Tableau Server

Tableau Server cannot determine if it fully started

In some instances Tableau Server may report that it could not determine if all components started properly on startup. A message displays: "Unable to determine if all components of the service started properly."

If you see this message after starting, verify that Tableau Server is running as expected by using a `tsm status -v` command.

If the status shows as running ("Status: RUNNING"), then the server successfully started and you can ignore the message. If the status is DEGRADED or STOPPED, see "Tableau Server doesn't start" in the next section.

Tableau Server doesn't start

If Tableau Server does not start or is running in a degraded state, run the `tsm restart` command from a command prompt. This will shut down any processes that are running, and restart Tableau Server.

Reindexing Tableau Server Search & Browse

Problems that can be solved by rebuilding Search & Browse index

Symptoms of an index that needs to be rebuilt include:

- A blank list of sites when a user attempts to log in
- A blank list of projects when a user tries to select a project
- Missing content (workbooks, views, dashboards)
- Unexpected or inaccurate alerts (for example, an "refresh failed" alert on a workbook that does not include an extract)
If you see any of these behaviors, reset and rebuild the Search & Browse index using the `tsm maintenance reset-searchserver` command.

Activating Tableau Server

Tableau Server license activation fails

In some instances Tableau Server license activation may fail. Error messages can range from a very generic one:

- An error has occurred

To more specific messages:

- `Function flxActCommonLicSpcPopulateFromTS returned error 50030, 71521`
- `No license found for 'Tableau Server'

To resolve this issue, try these solutions in the order listed:

Confirm you can access the licensing server

The Tableau licensing service was moved to a new data center on October 6, 2018. This means any environments that required special configuration (static IP safe listing for example) to access licensing.tableau.com or licensing.tableausoftware.com will need to be updated before you can activate, refresh, or deactivate a Tableau product key.

Tableau Server needs to connection to the following internet locations for licensing purposes:

- licensing.tableau.com:443
- atr.licensing.tableau.com:443
- o.ss2.us
- ocsp.rootg2.amazontrust.com
Requests to the above domains may be on port 80 or 443.

Verify the date and time

Verify the date and time on the initial Tableau Server computer is correct. If the clock is set to a time and date earlier than the current date, Tableau Server cannot be activated.

Force the product key to be read again

1. On the initial Tableau Server computer, sign in as administrator and open a command prompt.
2. Change to the Tableau Server bin directory. By default this is:

```
/opt/tableau/tableau_server/packages/bin.<version_code>/
```

3. Type the following commands:

```
tsm stop
./lmreread
tsm start
```

Send the contents of trusted storage to Tableau Support

If FlexNet Licensing Services is installed and running but you're still seeing an error, there might be a problem with the Tableau product key information. To resolve this issue, complete the following steps to create a file of the key information located in trusted storage.

1. On the initial Tableau Server computer, sign in as administrator and open a command prompt.

2. Type the following command:

```
serveractutil -view > <machine_name>-LicResults.txt
```

   **This creates the** `<machine_name>-LicResults.txt` **file in your current directory. If you don't have write permissions for that location and see an error, change to a location where you do have permission to create a file and run the command again.**

3. Contact Tableau Support ([http://www.tableau.com/support/request](http://www.tableau.com/support/request)) and include the `<machine_name>-LicResults.txt` file that you created.

**Troubleshoot Server Sign in Problems**

There are several different sign in options between Tableau Services Manager (TSM) and Tableau Server.
• **TSM**—If you are not able to sign into TSM, make sure you are using credentials for a user who has administrative rights to the computer where TSM is installed. This user may or may not also be a Tableau Server administrator. This is true whether you are signing in to the Web UI or the CLI. For more information, see Sign in to Tableau Services Manager Web UI.

• **Tableau Server**—
  • Administrators: if you are signing into Tableau Server as an administrator, you must use credentials for a user who has an administrator role in Tableau Server. You create the initial administrator when you first install Tableau, but can add other users as administrators once Tableau is installed and running. For more information, see Sign in to the Tableau Server Admin Area.
  • Non-administrative users: If you are signing into Tableau Server as a user, you need to use credentials for a user who has been added to Tableau Server. For more information, see Sign in to Tableau Server or Online.

**Note**: If users with valid credentials are unable to sign into Tableau Server, make sure you have not added a node without applying pending changes. If you have a pending new node, signing into Tableau Server may not be possible.

**Troubleshooting scenarios**

Unable to log into TSM or Tableau Server (sign in screen redisplay after entering credentials)

Using Internet Explorer or Edge, if you enter your credentials into the TSM or Tableau Server sign-in screen and the page redisplay without signing you in, verify that the hostname or domain in your URL does not include an underscore (_). If the hostname or domain of the Tableau Server computer includes an underscore (_), Internet Explorer or Edge browsers will not set a cookie, so the page will redisplay without signing you in. To work
around this, use "localhost" or the IP address of the computer in the URL. For example: https://localhost:8850.

For more information, see the Tableau Knowledge Base.

Troubleshoot Licensing

This topic includes instructions for troubleshooting issues related to Tableau Server licensing.

Handle an unlicensed server

Tableau offers two licensing models: user-based and core-based. To learn more about user-based and core-based licensing, see Licensing Overview.

User-based licensing requires each active user account to be covered by a license. User-based licenses have a defined capacity, or number of users that they allow. Each user is assigned a unique user name on the server and is required to identify themselves when connecting to the server.

Core-based licensing has no constraints on the number of user accounts in the system, but it does restrict the maximum number of processor cores that Tableau Server can use. You can install Tableau Server on one or more machines to create a cluster, with the restriction that the total number of cores in all the machines does not exceed the number of cores you have licensed and that all of the cores on a particular machine are covered by the license.

Unlicensed User-Based Server

The most common reason for a server that has user-based licensing to be unlicensed is an expired product key or an expired maintenance contract.

Unlicensed Core-Based Server

A core-based server can become unlicensed for a variety of reasons, such as when Tableau Server nodes running licensed processes cannot contact the Tableau Server node running
the License Manager service. To learn more about licensed processes, see Tableau Server Processes.

When the server is unlicensed you may not be able to start or administer the server. You can, however, manage your licenses using the tsm licenses command.

**Troubleshoot user-based licensing**

This section provides information about resolving issues that can occur when adding the user-based Viewer, Explorer and Creator licenses to Tableau Server or Tableau Online, or when these licenses expire. The highest available license type is Creator, followed by Explorer, and finally Viewer. To learn more about user-based licensing, see Licensing Overview.

A user or administrator is unlicensed due to license expiration

To avoid having users unexpectedly become unlicensed or move to another site role, you should always do one of the following before the license that they are currently using expires:

- Renew and activate a replacement license. If a user occupies a Creator, Explorer or viewer license and their license expires, they will use another license of the same type, if available.
- Change the site role of those users to allow the use of a license that is not due to expire.

To learn how site roles can be changed to require a different license, see Set Users’ Site Roles.

The reassignment of users to new licenses is governed by the following logic:

- When a Server Administrator user occupies a Creator license and their license expires (with no replacement licenses available), they are reassigned to an Explorer license if any Explorer licenses are available. This license reassignment occurs in order of most recent login. Server Administrators displace other users who might be currently using an Explorer license. If no Creator or Explorer licenses are available a Server Administrator becomes unlicensed.
When a non-Server Administrator user occupies a Creator license and their license expires (with no replacement licenses available), they become unlicensed. To avoid having these users become unlicensed, change their site role prior to license expiration. This is especially important for users in the Site Administrator Creator site role, who must move to the Site Administrator Explorer site role before their Creator license expires to avoid losing Site Administrator capabilities.

When a non-Server Administrator user occupies an Explorer or Viewer license and their license expires (with no replacement licenses available), they are upgraded to a higher license type, if licenses of that type are available. Specifically, the following occurs when a license expires:

- Users who occupy an Explorer license will move to a Creator license, if available (with no change to site role).
- Users who occupy a Viewer license will move to an Explorer license, if available. If no Explorer licenses are available, these users will move to a Creator license, if available (with no change to site role).
- If no licenses are available at the higher license types, those users are moved to Unlicensed.

Users are reassigned to a new license as described above in order of most recent login, with lower license types reassigned first (first Viewer, then Explorer, and then Creator).

For example: Two users with a Viewer license, a user with the Creator license, and two Server Administrators with a Creator license all have their licenses expire. Four unexpired Explorer licenses are available for these users. In this situation, the following occurs in the order shown below:

1. The user with a Viewer license who logged in most recently is reassigned to an Explorer license.
2. The second user with a Viewer license is reassigned to an Explorer license.
3. The Server Administrator user with a Creator license who logged in most recently is reassigned to an Explorer license, and then the second Server Administrator with a Creator license is reassigned to the remaining Explorer license.
4. The user with the Creator license becomes unlicensed.
Server Administrator site role is unchanged when using a Creator license

Server Administrators gain Creator capabilities if Creator licenses are available in Tableau Server, with no change to their site role name. All other Tableau Server and Tableau Online users gain Creator licenses only if assigned to a site role that includes Creator in its name.

Licenses are not immediately available

When you add a role-based license to Tableau Server, those licenses become available to all users when you restart Tableau Server. If you don’t restart Tableau Server, role-based licenses become available to all users within 24 hours.

A user with a Viewer license cannot open Tableau Server or Tableau Online workbooks from Tableau Desktop

A user with a Viewer license who also has a separate Tableau Desktop license will be unable to open workbooks on Tableau Server or Tableau Online using Tableau Desktop. To open workbooks such using Tableau Desktop, that user will need an Explorer or Creator license on Tableau Server or Tableau Online.

Handle an Unlicensed VizQL Server Process

There are several status indicators on the Tableau Server Status page that help you understand the state of Tableau Server processes. An orange-color status box, "Unlicensed", indicates that one of the VizQL server processes is unable to retrieve the Tableau Server license information.
There may be several reasons why the process is unable to access this information. For example, there may be network issues preventing a VizQL process, which is running on an additional node, from communicating with the initial node machine. Or, the process may be getting sent more requests than it can accept at that time and can't handle the licensing request. As a result, some of your users may be able to access views while others cannot.

To resolve the problem, stop, then start Tableau Server.

Tableau Services Manager (TSM) Command Timeout

When Tableau Server is configured with two instances of the repository and failover to the backup repository occurs, TSM attempts to restart the original repository so that it is available as a backup. If this cannot be done for any reason, subsequent TSM commands can fail due to timeouts while waiting for the original repository to recover.

Commands that can be impacted include:

- tsm maintenance restore
- tsm maintenance reindex-search
• tsm reset
• tsm security regenerate-internal-tokens
• tsm sites export
• tsm sites import

If any of these commands is failing, and you have a repository that is not recovering, remove the repository from the server topology, apply pending changes, and re-add it.

Tableau Services Manager (TSM) Backup Timeout

When you back up Tableau Server, one of the first steps taken is to confirm that key services are running, and, if they are not, to start them. If these services cannot be started:

• Active Repository
• File Store
• Cluster Controller

any attempt to back up Tableau Server will fail with one of the following errors:

An error occurred starting one or more of the following services: Active Repository, File Store, Cluster Controller.

One or more of the following services did not start in a timely fashion: Active Repository, File Store, Cluster Controller.

To successfully back Tableau Server up, make sure these processes can start.

Cookie Restriction Error

When a user signs in to Tableau Server, a session cookie is stored in their local browser. The stored cookie is how Tableau Server maintains that the signed in user has been authenticated and can access the server. Because the cookie is set with the same domain or sub-domain as the browser’s address bar, it is considered a first-party cookie. If a user's browser is configured to block first-party cookies, they will be unable to sign in to Tableau Server.
When a user signs in to Tableau Server via an embedded view, or in an environment where trusted authentication has been configured, the same thing happens: a cookie is stored. In this case, however, the browser treats the cookie as a third-party cookie. This is because the cookie is set with a domain that's different from the one shown in the browser’s address bar. If a user's web browser is set to block third-party cookies, authentication to Tableau Server will fail. To prevent this from occurring, web browsers must be configured to allow third-party cookies.

Troubleshoot Subscriptions

"The view snapshot in this email could not be properly rendered."

If you receive a subscription with this error message, there could be several reasons:

- **Missing credentials**: Some views are published with embedded credentials. You may receive the above error if the embedded credentials are now out-of-date, or if the view was republished without the embedded credentials.

- **Database temporarily down**: If the view has a live database connection and the database was temporarily down when the subscription was being generated, you might receive the above error.

- **Background process timeout**: By default, the background process that handles subscriptions times out after 30 minutes. In the majority of cases, this is plenty of time. However, if the background process is handling an extraordinarily large and complex dashboard, that may not be enough time. You can check the Background Tasks for Non Extracts admin view to see if that’s the case. To increase the timeout threshold, use the `tsm configuration set subscriptions.timeout` command.

Can't see images in email

For images of content to display in a subscription email, users subscribed to views, in addition to **View** permissions, must also have **Download Image/PDF** permissions. For more information, see View or Edit Permissions.
Can't subscribe

If you can see a view on Tableau Server and it has a subscription icon () in the upper right corner, you can subscribe to it.

To subscribe to a view, Tableau Server needs to be correctly configured (described in Manage Subscriptions) and the view you’re subscribing to must either have embedded credentials for its data source or not rely on credentials at all. Examples of the latter include a workbook that connects to an extract that isn’t being refreshed, or a workbook whose data is in a file that was included with the workbook at publish time. Embedding credentials is a step that happens in Tableau Desktop (see the Tableau Help for details).

No subscription icon

It’s possible to see a view but be unable to subscribe to it. This can happen for several reasons:

- **No subscriptions have been scheduled**: If no subscriptions have been scheduled, the subscription icon will not appear. To set a schedule for subscriptions, see Create or Modify a Schedule.
- **The view uses a live database connection**: Views with live database connections, where you’re prompted for your database credentials when you first click the view, aren’t available for subscription. A subscription includes a view (or workbook), data, and a schedule. To deliver the data required for the view, Tableau Server either needs embedded database credentials or data that doesn’t require credentials. Where live database connections are concerned, Tableau Server doesn’t have the credentials, only the individual users do. This is why you can only subscribe to views that either don’t require credentials or have them embedded.
- **Tableau Server is configured for trusted authentication**: You may also be able to see a view but be unable to subscribe to it (no subscription icon) if Tableau Server is configured for trusted authentication. See Ensure Access to Subscriptions for more information.
Receiving invalid or "broken" subscriptions

If you configured subscriptions on test or development instances of Tableau Server in addition to your in-production instance, disable subscriptions on your non-production instances. Keeping subscriptions enabled on all instances can result in your users receiving subscriptions that appear to be valid, but which don't work, or receiving subscriptions even though they've unsubscribed from the view or workbook.

Suspended Subscriptions

By default, a subscription is suspended after 5 consecutive subscription failures. To change the threshold number of subscription failures that can occur before they are suspended, use the tsm configuration set option, `backgrounder.subscription_failure_threshold_for_run_prevention`. This sets the threshold for the number of consecutive failed subscriptions necessary before suspending the subscription. This is a server-wide setting.

Only Server administrators can configure the threshold number of subscription failures before a subscription is suspended. For information on setting this threshold, see Set up a Server for Subscriptions.

By default, administrators are not emailed when a subscription is suspended, but can opt-in to suspension emails per site through My Account Settings.

Resume suspended subscriptions

Administrators and subscription owners can resume subscriptions in several ways:

- from My Subscription tab in Content Settings
- from the Subscriptions tab per workbook
- from the Subscriptions tab under Tasks (Server Admins only)

When a subscription is resumed, the alert failing count goes back to zero. The next evaluation of the subscription will occur at the next scheduled evaluation time.
Subscriptions not arriving ("Error sending email. Can't send command to SMTP host.")

You may see the above error in Windows Event Viewer if subscriptions aren't arriving and your SMTP server is using encrypted (SSL) sessions. Subscriptions are only supported for unencrypted SMTP connections. The solution is to use an unencrypted SMTP server. (If you’re experiencing this error, note that Tableau Server will still indicate that subscriptions are being sent in the Background Tasks for Non Extracts admin view.)

Custom scripts not working after upgrade to 8.1

To support better session management, starting with version 8.1, a hash tag (#) was added to the end of view URLs. If you had custom subscriptions scripting that generated views as PDFs or PNGs you may need to update your scripts to allow for the hash tag.

For example, prior to version 8.1, view URLs use this syntax: http://tableauserver/views/SuperStore/sheet1. To generate a view as a PNG, .png could be added to the end of the URL. For example, http://tableauserver/views/SuperStore/sheet1.png.

In versions 8.1, 8.2, or 8.3, view URLs use this syntax: http://tableauserver/views/SuperStore/sheet1#1. To generate a PNG, add .png before the hash tag. For example: http://tableauserver/views/SuperStore/sheet1.png#1

Custom scripts not working after upgrade to 9.0

In version 9.0, the session ID at the end of server URLs is indicated by an "iid" parameter, :iid=<n>. For example, http://localhost/#/views/Sales2015/SalesMarginsByAreaCode?:iid=1. This parameter replaces the hash tag "#<n>" used for the session ID in 8.x versions of Tableau Server.
If you use custom subscriptions scripts that generate views as PDFs or PNGs, you may need to update your scripts by removing the hash tag and number (#<n>), and inserting the ?:iid= session ID parameter before the number.


To generate a PNG in version 9.0 and later, add .png before the session ID: http://tableauserver/views/SuperStore/sheet1.png?iid=2

Troubleshoot Performance of Workbooks with Calculations

In most cases, you can expect to see similar or better performance after upgrading your Tableau Server from versions 10.4 or earlier to 10.5 or later. However, for workbooks that use complex calculations, you may see performance issues after you upgrade. This article describes how to test and troubleshoot performance issues for workbooks that have calculations and use extracts as the data source after you have upgraded your Tableau Server from versions 10.4 or earlier to 10.5 or later.

If you have not yet upgraded to Tableau Server 10.5 or later, we strongly recommend that you set up a test environment and test your workbook performance before you upgrade your production Tableau Server. For more details, see Test Workbook Performance.

If you have already upgraded to Tableau Server 10.5 or later, and you are experience slow response times, use the guidance provided in this topic to help troubleshoot performance issues.

Since Linux was first released in 10.5, this only applies when you are migrating from Tableau Server versions 10.4 or earlier on Windows to Linux 10.5 or later.

Here are the scenarios that most likely describe your environment after upgrading to Tableau Server 10.5 or later:

- Recently upgraded, and majority of the extracts are still in .tde format
- Recently upgraded and majority of extracts are in .hyper format
- Upgraded a while ago, workbooks have changed since upgrade
Scenario: You upgraded your Tableau Server recently. You are experiencing slow response times and the majority of your extracts have not been refreshed, so they are still in .tde format.

1. Disable any scheduled or automated extract refreshes.

2. Enable the following setting on Tableau Server to check the number of query nodes required for Tableau to generate the workbook and display an error when the set limit is exceeded. The error message might say something like: "Logical Query tree has 2348182 nodes, maximum number allowed is 1000000....".

   Use TSM CLI to run the following commands:

   tsm configuration set -k native_api.node_limit_checker_pre_rewrite_disable -v false
   tsm pending-changes apply

   **Note:** This setting is only available in Tableau Server 10.5.3 or later. While enabling this setting improves the reliability and stability of Tableau Server, you may see errors on a very small percentage of workbooks when you enable this setting. For example, the Tableau team saw errors on 0.01% of the workbooks with this setting enabled on Tableau Online.

3. Test the workbooks by viewing or interacting with them. You should see an error message informing you about exceeding the node limits on workbooks that have performance issues. The error message might say something like: "Logical Query tree has 2348182 nodes, maximum number allowed is 1000000....".

4. Use Tableau Desktop to troubleshoot your workbook performance. Run this command to enable the node limit check in your Tableau Desktop:

   tableau.exe -DNodeLimitCheckerPreRewriteDisable=false
Note: This setting is only available in Tableau Desktop 10.5.3 or later.

In Tableau Desktop, download and open the workbooks that displayed the error message about high node limits in step 2. Try optimizing the performance of workbooks using methods described in Best Practices for Creating Calculations in Tableau. If successful, publish these workbooks to Tableau Server. If you are still experiencing performance issues, continue to the next step.

5. For workbooks that load successfully, but the overall response times is slower after upgrade, try using the Compute Calculations Now option. If you have a large number of workbooks that fall under this category, consider enabling the server-wide setting to retain materialized calculations for all extracts when they are upgraded from .tde to .hyper:

Use TSM CLI to run the following commands:

```
tsm configuration set -k native_api.preserve_calculations_on_hyper_refresh_conversion -v true

 tsm pending-changes apply
```

Considerations for turning on this setting:

Turn this setting on only if the majority of your workbooks require calculations to be materialized. There are resource and time costs associated with this setting, which are as follows:

- When this setting is set to true, the extract file size will increase, affecting the overall disk space.
- Extracts with materialized calculations take a longer time to refresh than extracts without materialized calculations.
This setting only affects extracts that have not yet upgraded to .hyper. Extracts already upgraded to .hyper before turning on this setting, will not have the calculations materialized. This setting will also not affect workbooks and extracts published from Tableau Desktop, or any new extract refreshes published to Tableau Server that do not use the **Compute Calculations Now** option.

**Note:** This setting is only available in Tableau Server 10.5.3 or later.

6. Enable extract refresh schedules.

**Scenario:** You upgraded your Tableau Server recently. You are experiencing slow response times and a majority of your extracts have been refreshed and upgraded from .tde to .hyper.

1. Restore the backup you made before you upgraded your production Tableau Server.

    **Note:** This method assumes that your workbooks have not changed significantly since the upgrade and, or it is OK to go back to the state just before upgrade.

2. Disable any scheduled extract refreshes.

3. Enable the following setting on Tableau Server to check the number of query nodes required for Tableau to generate the workbook and display an error when the set limit is exceeded. The error message might say something like: "**Logical Query tree has 2348182 nodes, maximum number allowed is 1000000....**".

Use TSM CLI to run the following commands:

```
tsm configuration set -k native_api.node_limit_checker_pre_rewrite_disable -v false
tsm pending-changes apply
```
Note: This setting is only available in 10.5.3 or later. While enabling this setting improves the reliability and stability of Tableau Server, you may see errors on a very small percentage of workbooks with when you enable this setting. For example, the Tableau team saw errors on 0.01% of the workbooks with this setting enabled on Tableau Online.

4. Test the workbooks by viewing or interacting with them. You should see an error message informing you that you are exceeding the node limits on workbooks that have performance issues. The error message might say something like: "Logical Query tree has 2348182 nodes, maximum number allowed is 1000000....".

5. Use Tableau Desktop to troubleshoot your workbook performance. Run this command to enable the node limit check in your Tableau Desktop:

```
tableau.exe -DNodeLimitCheckerPreRewriteDisable=false
```

Download and open the workbooks that displayed the error message using Tableau Desktop. Try optimizing the performance of workbooks using methods described in Best Practices for Creating Calculations in Tableau. If successful, then publish them to Tableau Server. If you are still experiencing performance issues, continue to the next step.

6. For workbooks that load successfully, but the overall response time is slower after upgrade, try using the Compute Calculations Now option. If you have a large number of workbooks that fall under this category, consider enabling the server-wide setting to retain materialized calculations for all extracts when they are upgraded from .tde to .hyper:

Use TSM CLI to run the following commands:

```
tsm configuration set -k native_api.preserve_calculations_on_hyper_refresh_conversion -v true
```
tsm pending-changes apply

Considerations for turning on this setting:

Turn this setting on only if majority of your workbooks require calculations to be materialized. There are resource and time costs associated with this setting, which are as follows:

- When this setting is set to true, the extract file size will increase, affecting the overall disk space.
- Extracts with materialized calculations take a longer time to refresh than extracts without materialized calculations.

This setting only affects extracts that have not yet upgraded to .hyper. Extracts already upgraded to .hyper before turning on this setting will not have the calculations materialized. This setting will also not affect workbooks and extracts published from Tableau Desktop, or any new extract refreshes published to Tableau Server that do not use the Compute Calculations Now option.

**Note:** This setting is only available in 10.5.3 or later.

7. Enable extract refresh schedules.

Scenario: You upgraded your Tableau Server a while ago and you are experiencing slow response times. It is not practical for you to roll back using the backup you made prior to upgrade because your workbooks have changed since the upgrade, and the extracts have been upgraded to .hyper format.

If you fall under this scenario, and you find that your workbooks require materialized calculations, turning on the optimization setting on refresh will not work for you as this setting only works when upgrading from .tde to .hyper. You will need to test your workbooks indi-
Tableau Server on Linux Administrator Guide

Individually for performance issues, and optimize them manually and republish to Tableau Server.

1. If you see high memory and CPU consumption by VizQL Server when viewing workbooks with extracts, in addition to slower workbook response times, then you can enable the following setting on Tableau Server to help prevent the VizQL process from consuming the memory resources on the machine that might result in critical server issues. This setting checks the number of query nodes required for Tableau to generate the workbook and displays an error when the set limit is exceeded:

Use TSM CLI to run the following commands:

```
tsm configuration set -k native_api.node_limit_checker_pre_rewrite_disable -v false
tsm pending-changes apply
```

**Note:** While enabling this setting improves the reliability and stability of Tableau Server, you may see errors on a very small percentage of workbooks when you enable this setting. For example, the Tableau team saw errors on 0.01% of the workbooks with this setting enabled on Tableau Online.

2. Test the workbooks by viewing or interacting with them. Look for workbooks where you might see an error message that says something like: "**Logical Query tree has 2348182 nodes, maximum number allowed is 1000000....**".

3. Use Tableau Desktop to troubleshoot the workbooks that you identified in step 2. Run this command to enable the node limit check in your Tableau Desktop:

```
tableau.exe -DNodeLimitCheckerPreRewriteDisable=false
```

Download and open the workbooks that displayed the error message using Tableau Desktop. Try optimizing the performance of workbooks using methods described in
the Best Practices for Creating Calculations in Tableau topic and publish them to Tableau Server. If you are still seeing performance issues, continue to the next step.

4. Use the **Compute Now** option to materialize calculations in your extract.

Server Administrator Reference

Tableau Server Processes

This topic describes the options for setting the process configuration. To configure Tableau Server processes, you need to specify which processes and how many instances should run on each node. You do this using the `tsm topology set-process` command. For more information, see Changing the number of processes on a node.


Except where explicitly noted in the table below, applying changes in processes will stop Tableau Server if it is running when you apply those changes. After changes are applied, Tableau Server is returned to the state it was in before process configuration, so if the server was running, it will be restarted.

**Important:** Your process topology will depend on your organizational needs.

Licensed processes

Some of the processes that are installed as a part of Tableau Server are "licensed" processes. Licensed processes need a valid Tableau Server license in order to run. Other processes that are installed as a part of Tableau Server are not tied to a valid license. This has the following impact:
Every licensed process needs to regularly contact the Tableau Server License Manager service that runs on the initial Tableau Server computer to verify they are licensed. If they cannot confirm there is a valid license, for example, if the initial node is not available, the process will not run and Tableau Server may not function properly or reliably.

- If you have a core-based Tableau Server license, the cores on any node with a licensed process will count against the total count of licensed cores.

The "Licensed" column in the table below identifies those processes that require a valid license, and which impact the count of cores in core-based licenses.

**Tableau Server Processes**  These processes have a status of **running** when Tableau Server is running, and **stopped** when Tableau Server is stopped.

<table>
<thead>
<tr>
<th>Name shown in tsm status -v</th>
<th>Name used with tsm topology set-process</th>
<th>Purpose</th>
<th>Notes</th>
<th>Licensed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Server</td>
<td>vizportal</td>
<td>The Application Server (VizPortal) handles the web application, REST API calls, and supports browsing and searching.</td>
<td>When Application Server is installed, Data Engine is also installed, unless the node already has an instance of Data Engine.</td>
<td>Yes</td>
</tr>
<tr>
<td>Ask Data</td>
<td>Cannot be configured manually.</td>
<td>The Ask Data service is used by the Ask Data feature.</td>
<td>Runs automatically on all nodes where Data Server is running.</td>
<td>No</td>
</tr>
<tr>
<td>Backgrounder</td>
<td>backgrounder</td>
<td>The Backgrounder runs server tasks, including extract refreshes, subscriptions, ‘Run Now’ tasks, and tasks initiated from tabcmd.</td>
<td>When Backgrounder is installed, Data Engine is also installed, unless the node already has an instance of Data Engine. In most situations you can change the number of backgrounder instances on an existing node of a running server without causing a stop and restart the server. An exception is if you are adding backgrounder to an existing node that did not previously have backgrounder or any other process that also installs Data Engine. For more information, see Tableau Server Dynamic Topology Changes.</td>
<td>Yes</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Cache Server</td>
<td>cacheserver</td>
<td>The Cache Server is a query cache distributed and shared</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
across the server cluster. This in-memory cache speeds user experience across many scenarios. VizQL server, backgrounder, and data server (and application server to a lesser extent) make cache requests to the cache server on behalf of users or jobs. The cache is single-threaded, so if you need better performance you should run additional instances of cache server.

<table>
<thead>
<tr>
<th>Cluster Controller</th>
<th>cluster-controller</th>
<th>The Cluster Controller is</th>
<th>Required on each node. Not automatically</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>Responsibility</td>
<td>Installation Status</td>
<td>Installed Automatically?</td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>--------------------------</td>
<td></td>
</tr>
<tr>
<td>Data Engine</td>
<td>The Data Engine creates data extracts and processes queries.</td>
<td>Automatically installed when you install File Store, VizQL Server, Application Server (VizPortal), Data Server, or Backgrounder.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Data Server</td>
<td>The Data Server manages connections to Tableau Server data sources.</td>
<td>When Data Server is installed, Data Engine is also installed, unless the node already has an instance of Data Engine.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Elastic Server</td>
<td>Elastic Server is used by Ask Data to index and cache data.</td>
<td>Only one Elastic Server process can be running and it can optionally be moved to any node in the cluster. The Elastic Server heap size can be configured by using the elasticserver.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Type</td>
<td>Description</td>
<td>Required</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>File Store</td>
<td>filestore</td>
<td>The File Store automatically replicates extracts across Data Engine nodes.</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Gateway</td>
<td>gateway</td>
<td>The Gateway is a web server that handles all requests to Tableau Server from browsers, Tableau Desktop, and other clients.</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Repository</td>
<td>pgsql</td>
<td>The PostgreSQL repository is the main database for Tableau Server. It stores work-</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Service</td>
<td>Description</td>
<td>Status</td>
<td>Configured Automatically</td>
<td></td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>--------------------------</td>
<td></td>
</tr>
<tr>
<td>SAML Service</td>
<td>Cannot be configured manually.</td>
<td>The SAML Service acts as a proxy between Tableau Server and SAML Identity Providers (IdPs).</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Search And Browse</td>
<td><strong>searchserver</strong></td>
<td>The Search Service handles fast search, filter, retrieval, and display of content metadata on the server.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Tableau Prep Conductor</td>
<td><strong>flowprocessor</strong></td>
<td>The Tableau Prep Conductor runs a flow, checks connection credentials,</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Requires Data Management Add-on to enable this on Tableau Server. By default, it is automatically enabled on a node where back-</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
and sends alerts if a flow fails.

It leverages the scheduling and tracking functionality of Tableau Server so you can automate running flows to update the flow output.

If the node role is set to exclude flows, then Tableau Prep Conductor is not installed on that node. For more information, see Node Roles in Tableau Server.

| VizQL Server | vizqlserver | The VizQL Server loads and renders views, computes and executes queries. | When VizQL Server is installed, Data Engine is also installed, unless the node already has an instance of Data Engine.

In most situations you can change the number of VizQL instances on an existing node of a running server without causing a stop and restart the server. An exception is if you are adding VizQL to an | Yes |
existing node that did not previously have VizQL or any other process that also installs Data Engine. For more information, see Tableau Server Dynamic Topology Changes.

**Tableau Microservice Container Processes** These processes are automatically added when one of the microservices they contain is added to a node. Container status depends on the status of the microservices within the container. If all microservices are running, the container process has a status of running. If all microservices are stopped, the container process status is error. If one or more microservices is running while others are not, the container service has a status of degraded. For more information, see Tableau Server Microservice Containers.

| Interactive Microservice Container |  |
|-----------------------------------|  |
| Non-Interactive Microservice Container |  |

**Tableau Services Manager (TSM) Processes** These processes have a status of running once TSM has been initialized, and remain running even when Tableau Server is stopped.

<p>| Administration Agent | Cannot be configured manually. | The TSM Agent monitors the Coordination | Automatically installed on each node where you install Tableau Server. | No |</p>
<table>
<thead>
<tr>
<th>Service for changes to configuration or topology and delivers new configurations to each service (configuration) or deploys new services and removes old ones (topology)</th>
<th>You cannot configure the Administration Agent manually.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration Controller</td>
<td>Cannot be configured manually, except to move it to another node. For more information, see Recover from an Initial Node Failure.</td>
</tr>
<tr>
<td>The TSM Controller handles requests to TSM and orchestrates configuration and topology changes and workflow across service processes. The Controller also serves as the REST API endpoint (HTTPS).</td>
<td>Automatically installed when you install TSM on the initial node. You cannot configure the Administration Controller manually except to move it to another node. For more information, see Recover from an Initial Node Failure.</td>
</tr>
<tr>
<td>Client File Service</td>
<td>cli-entfileservice</td>
</tr>
</tbody>
</table>
File Service (CFS) manages most shared files in a multinode cluster. For example, authentication related certificates, keys, and files (OpenID, mutual SSL, SAML, and Kerberos), and customization files are managed by CFS.

On the initial node. No other instances are installed unless you explicitly configure them. See Configure Client File Service.

In multi-node deployments, we recommend you configure an instance of CFS on each of the nodes where you deploy the Coordination Service. Redeploying the Coordination Service does not have any impact on CFS.

CFS does not display in the Status page or the Configuration page but is visible in the output of the `tsm status -v` command.

To view or set instances of CFS, use the `tsm topology` command.

| Coordination Service | Cannot be set with `tsm topology` | The Coordination Service | Automatically installed on the initial node. No | No |
### Tableau Server on Linux Administrator Guide

| Service Manager | Cannot be configured manually. | The Service Manager serves as the single source of truth. | other instances are installed unless you explicitly deploy a new Coordination Service ensemble. For details, see Deploy a Coordination Service Ensemble. | No |
| License Manager | Cannot be configured manually. | The License Manager handles licensing. | Automatically installed on all nodes. You cannot configure the Service Manager manually. | No |

### Tableau Server Maintenance Processes

These processes have a status of **stopped** unless they are actively running to complete a job.

<p>| Database | Cannot be configured manually. | The Database | Automatically installed | No |</p>
<table>
<thead>
<tr>
<th><strong>Maintenance</strong></th>
<th>figured manually.</th>
<th>base Maintenance service is responsible for performing maintenance operations on the Tableau Server repository.</th>
<th>on each node where you install Tableau Server. Shows a status of stopped in output of tsm status -v unless it is actively performing database maintenance. Maintenance can include updates related to enabling remote access to the repository and changing passwords used to access the repository. You cannot configure the Database Maintenance service manually.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Backup/Restore</strong></td>
<td>Cannot be configured manually.</td>
<td>The Backup and Restore service is responsible for performing backup and restore operations on the data stored in the Tableau Server repository.</td>
<td>Automatically installed on each node where you install Tableau Server. Shows a status of stopped in output of tsm status -v unless it is performing a backup or restore operation. No</td>
</tr>
<tr>
<td>Site Import/Export</td>
<td>Cannot be configured manually.</td>
<td>The Site Import and Export service is responsible for migrating Tableau Server sites between server clusters.</td>
<td>Automatically installed on each node where you install Tableau Server. Shows a status of stopped in output of tsm status -v unless it is performing an import or export. You cannot configure the Site Import and Export service manually.</td>
</tr>
</tbody>
</table>

### Process workflow

The Tableau Server processes and how they interact depend on what action or activity is taking place. For example, the processes that are used, and how they interact, differ when you publish a workbook from those used when you sign in using SAML. For some interactive views on process workflow, see the below workbook. This allows you to select a particular workflow and follow it step by step from start to finish.

**Disclaimer:** This workbook is published on Tableau Public and is not maintained by Tableau documentation. We cannot guarantee that it is up-to-date with the latest version of Tableau Server.
Tableau Server Coordination Service

The Coordination Service is built on Apache ZooKeeper, an open-source project, and coordinates activities on the server, guaranteeing a quorum in the event of a failure, and serving as the source of "truth" regarding the server topology, configuration, and state. The service is installed automatically on the initial Tableau Server node, but no additional instances are installed as you add additional nodes. Because the successful functioning of Tableau Server depends on a properly functioning Coordination Service, we recommend that for server installations of three or more nodes, you add additional instances of the Coordination Service by deploying a new Coordination Service ensemble. This provides...
redundancy and improved availability in the event that one instance of the Coordination Service has problems.

The hardware for your cluster can have some effect on how well the Coordination Service runs. In particular:

- **Memory.** The Coordination Service maintains state information in memory. By design, the memory footprint is small, and is typically not a factor in overall server performance.

- **Disk speed.** Because the service stores state information on disk, it benefits from fast disk speed on the individual node computers.

- **Connection speed between nodes.** The service communicates continuously between cluster nodes; a fast connection speeds between nodes helps with efficient synchronization.

Configuration for the Coordination Service

The Coordination Service is installed automatically on the initial node of Tableau Server. If you are running a single-node installation, you do not need to do anything to deploy or configure the Coordination Service. If your installation includes three or more nodes, you'll be prompted to configure a Coordination Service ensemble when you add your third node. This is not required, but is highly recommended as the Coordination Service serves a key function for high availability, acting as the source of "truth" about server topology, configuration, and state.

To configure a Coordination Service ensemble, use the TSM CLI and add the Coordination Service to the nodes you want running it. For details on how to deploy a Coordination Service ensemble, see Deploy a Coordination Service Ensemble.

The Coordination Service Quorum

To ensure that the Coordination Service can work properly, the service requires a *quorum*—a minimum number of instances of the service. This means that the number of nodes in your
installation impacts how many instances of the Coordination Service you want to configure in your ensemble.

**Number of Coordination Service instances to use**

The maximum number of Coordination Service instances you can have in an ensemble on Tableau Server depends on how many Tableau Server nodes you have in your deployment. Configure a Coordination Service ensemble based on these guidelines:

<table>
<thead>
<tr>
<th>Total number of server nodes</th>
<th>Recommended number of Coordination Service nodes in ensemble (must be 1, 3, or 5)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-2 nodes</td>
<td>1 node</td>
<td>This is the default and requires no changes unless you want to move the Coordination Service off your initial node and onto your additional node.</td>
</tr>
<tr>
<td>3-4 nodes</td>
<td>3 nodes</td>
<td></td>
</tr>
<tr>
<td>5 or more nodes</td>
<td>5 nodes</td>
<td>Five is the maximum number of Coordination Service instances you can install.</td>
</tr>
</tbody>
</table>

If you reduce the number of nodes

If you reduce the nodes in your cluster from three (or more) to two nodes, a warning tells you Tableau Server can no longer support high availability:

*A minimum of three Tableau Server nodes are required for high availability. You can add a third node now, or continue with only two nodes. Continuing with only two nodes*
Tableau Server will not be highly available. You can always add a third node later. Click OK to continue with 2 nodes, or Cancel to go back and add a node.

If you continue, Tableau Server will run, but you will not have any automatic failover of the repository.

Viewing Coordination Service Status

The Coordination Service is not included in the listing when you View Server Process Status. To see the state of the service, you can use the tsm status command:

```
tsm status -v
```

The output from the command shows you whether the service is running:

```
node1: TABLEAUSVR01
Status: RUNNING
'Tableau Server Gateway 0' is running.
'Tableau Server Application Server 0' is running.
'Tableau Server VizQL Server 0' is running.
'Tableau Server VizQL Server 1' is running.
'Tableau Server VizQL Server 2' is running.
'Tableau Server VizQL Server 3' is running.
'Tableau Server Cache Server 0' is running.
'Tableau Server Cache Server 1' is running.
'Tableau Server Coordination Service 0' is running.
'Tableau Server Cluster Controller 0' is running.
'Tableau Server Search And Browse 0' is running.
'Tableau Server Backgrounder 0' is running.
'Tableau Server Backgrounder 1' is running.
'Tableau Server Data Server 0' is running.
'Tableau Server Data Server 1' is running.
'Tableau Server Data Engine 0' is running.
'Tableau Server File Store 0' is running.
'Tableau Server Repository 0' is running (Active Repository).
```
Tableau Server Administration Agent 0' is running.
'Tableau Server Administration Controller 0' is running.
'Tableau Server Service Manager 0' is running.
'Tableau Server License Manager 0' is running.
'Tableau Server Client File Service 0' is running.
'Tableau Server Database Maintenance 0' is stopped.
'Tableau Server Backup/Restore 0' is stopped.
'Tableau Server Site Import/Export 0' is stopped.
'Tableau Server SAML Service 0' is stopped.

Tableau Server Data Engine

Hyper is Tableau’s in-memory Data Engine technology optimized for fast data ingests and analytical query processing on large or complex data sets. Starting in Tableau 10.5 release, Hyper powers the Data Engine in Tableau Server, Tableau Desktop, Tableau Online, and Tableau Public. The Data Engine is used when creating, refreshing or querying extracts. It is also used for cross-database joins to support federated data sources with multiple connections.

Memory and CPU usage

The Data Engine is designed to leverage all available CPU and memory on the machine to provide the fastest response times.

CPU usage

Hyper technology leverages the new instruction sets in CPU and is capable of parallelizing and scaling to all the available cores. Hyper technology is designed to scale to many cores efficiently, and also to maximize the use of each single core as much as possible. This means that you can expect to see the CPU being fully used during query processing. Adding more CPU is expected to result in performance improvement.

Modern operating systems such as Microsoft Windows, Apple macOS, and Linux have mechanisms to make sure that even if a CPU is fully used, incoming and other active processes can run simultaneously. In addition, to manage overall resource consumption and to
prevent overloading and completely starving other processes running on the machine, the Data Engine monitors itself to stay within the limits set in the Tableau Server Resource Manager (SRM). Tableau Server Resource Manager monitors the resource consumption and notifies Data Engine to reduce the usage when it exceeds the predefined limit.

Since the Data Engine is designed to utilize the available CPU, it is normal to see spikes in CPU usage at times. If however, you see high CPU usage (ex: 95%) for extended periods of time (an hour or more), this can mean a couple of things:

- There is a high load of queries. This can happen if a server is under stress due to overload of multiple client requests and the queries are queuing up. If this happens often, it is an indication that more hardware is required to serve the clients. Adding more CPU in this case should help to improve performance.

- There is one long running query. In this case, the Tableau Server resource Manager will stop long running queries based on the timeout settings. This was also true for the Tableau Server versions earlier than version 10.5

For more information on Tableau Server Resource Manager, see General Performance Guidelines.

Memory usage

Memory usage of the Data Engine depends on the amount of data required to answer the query. The Data Engine will try to run this in-memory first. A working set memory is allocated to store an intermediate data structure during query processing. In most cases, systems have enough memory to do these types of processing, but if there isn't enough available memory, or if more than 80% of RAM is utilized, the Data Engine shifts to spooling by temporarily writing to disk. The temporary file get deleted after the query has been answered. Therefore, spooling is an indication that more memory may be needed. Memory usage should be monitored and upgraded appropriately to avoid performance issues caused by spooling.

To manage memory resources on the machine, the maximum memory limit for Data Engine is set by Tableau Server Resource Manager (SRM).
Server configuration, Scalability, and Performance

- A single instance of Data Engine is automatically installed per node where an instance of File Store, Application Server (VizPortal), VizQLServer, Data Server, or Backgrounder is installed. The Data Engine can scale by itself and uses as much CPU and memory as needed, thus removing the need for multiple instances of the Data Engine. For more information on the server processes, see Tableau Server Processes.

- The instance of Data Engine installed on the node where File Store is installed is used for querying data for view requests. The instance of Data Engine installed on the node where backgrounder is installed is used for extract creation and refreshes. This is an important consideration when you are doing performance tuning. For more information, see Performance Tuning Examples.

- Data Server, VizQL Server, and the Application Server (VizPortal) all use the local instance of Data Engine to do cross-database joins and create shadow extracts. Shadow extract files are only created when you work with workbooks that are based on non-legacy Excel or text, or statistical files. Tableau creates a shadow extract file in order to load the data more quickly.

- In Tableau Server 10.5 one instance of Data Engine is installed automatically when you install backgrounder. The backgrounder process uses the single instance of Data Engine (hyperd.exe) installed on the same node.

Scalability:

You can scale up with the new Data Engine: Since cores are fully utilized, adding more cores makes individual queries execute faster which in turn allows for more queries to execute in less time.

Memory usage should be monitored and upgraded appropriately to avoid the performance issues caused by spooling.
For more information on Scalability, see Tableau Server Scalability.

Performance:

As mentioned in the beginning of this topic, in most cases you can expect to see performance improvements when you upgrade to Tableau 10.5 or later. However, in some cases you may see performance issues like slower response times, especially for workbooks with complex calculations. To test your workbooks to see if should expect performance issues, we recommend that you test this before you upgrade. For more information, see Test Workbook Performance. If you have already upgraded your Tableau Server, see Troubleshoot Performance of Workbooks with Calculations.

For more information on performance, start with General Performance Guidelines, and Performance Tuning

Performance benefits

Starting in 10.5, Hyper technology has been integrated with Tableau Data Engine to give you the following key benefits:

- **Faster extract creation**: With Hyper technology, extracts are generated almost as fast as the source system can deliver data, no sorting needed.

- **Support for larger extracts**: Prior to this release, you might have not been able to get all your data into a single extract. With Hyper technology, much larger amounts of data can be included in a single extract.

- **Faster analysis of extracts**: In many cases you will see faster querying of data for larger extracts, or workbooks with complex calculations.

Here are some reasons why the Data Engine powered by Hyper performs better on larger or complex extracts and is optimized for faster querying:

- **Hyper technology is designed to consume data faster**: Unlike in previous versions, the Data Engine does not do any post processing like sorting. With Hyper, post
processing steps like sorting are not needed giving the Data Engine the ability to perform better with larger extracts.

- **Hyper technology is memory-optimized.** This means that when needed, all data lives in memory. This results in fast data access times.

- **Hyper technology is CPU optimized.** This means that Data Engine now fully parallelizes the query execution and utilizes available CPU in such a way that query execution time scales almost linearly with the number of cores in the machine.

- **Hyper is a compiling query engine.** Queries are either interpreted or compiled to the machine code for maximum performance and allowing the Data Engine to get most performance out of modern hardware (CPU, large main-memory capacities).

- **Hyper technology uses advanced query optimizations to make queries faster.** Along with many additional advanced techniques such as, materializing min and max values for each column, mini-indices to optimize search ranges, more granular data block-level dictionaries, advanced logic for join and sub-query performance optimizations, the new Data Engine offers many improvements over the previous Tableau Data Engine in terms of performance and scalability.

**Tableau Server File Store**

The Tableau Server File Store process controls the storage of extracts. When the file store is installed, an instance of the Data Engine is also installed unless the node already has an instance of the data engine. In highly available (HA) environments, the File Store ensures that extracts are synchronized to other file store nodes so they are available if one file store node stops running.

<table>
<thead>
<tr>
<th>Process</th>
<th>File Store</th>
</tr>
</thead>
<tbody>
<tr>
<td>File name</td>
<td>filestore.exe</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the File Store process is visible on the Status Page. For more information, see View Server Process Status</td>
</tr>
</tbody>
</table>
Logging

Logs generated by the repository are located in /var/opt/tableau/tableau_server/data/tabsvc/logs/filestore. For more information, see Server Log File Locations

The decommission Command

If you want or need to remove a file store you should decommission the file store first, using the tsm topology filestore decommission command. If you don’t decommission the filestore before you attempt to remove it, you will be prompted to do so. Decommissioning puts the file store into read-only mode and copies any unique data contained in the file store to the other file store(s) in the cluster. While a file store is being decommissioned, this shows on the Status page, and once all unique content has been copied to other file store nodes, the decommissioned node shows as ready to be removed.

Tableau Server Gateway Process

The Tableau Server gateway process is an Apache web server component (httpd.exe). Its role is to handle requests to the server from all clients—Tableau Desktop, mobile devices, a proxy, a load balancer, etc.

The server runs a single instance of the gateway process; you can’t run more than one per machine.

<table>
<thead>
<tr>
<th>Process</th>
<th>Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>File name</td>
<td>httpd.exe</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the Gateway is visible on the Status Page. For more information, see View Server Process Status</td>
</tr>
<tr>
<td>Logging</td>
<td>Logs generated by the repository are located in /var/opt/tableau/tableau_server/data/tabsvc/logs/filestore. For more information, see Server Log File Locations</td>
</tr>
</tbody>
</table>
Port assignment

By default, the gateway process listens for requests on port 80 (for HTTP requests) and 443 (for SSL requests). When you install Tableau Server on a computer, part of the server configuration makes sure that this port is open in the computer’s firewall. If the computer is running a different process that requires port 80 for HTTP, you can change the port assignment for the gateway process during installation. (You cannot change the SSL/HTTPS port.)

If you need to set the HTTP port after installation, then run the following TSM command, where `node` is the node number (for example, `node1`) and `nn` is the new port number:

```
 tsm topology set-ports --node-name node --port-name gateway:primary --port-value nn
```

If you are running Tableau Server with a reverse proxy server, you will need to configure other port and host-related settings on Tableau Server. See Configuring Proxies for Tableau Server.

Log files for the gateway process

The gateway process creates two sets of log files:

- Activity logs. The name for these log files has the format `access.yy_mm_dd_hh_mm_ss.log`.

- Error logs. All errors are logged in a single file named `error.log`.

For more information, see Log File Snapshots (Archive Logs).
Gateway processes in a cluster

If your server environment is distributed across multiple machines, you can run a single gateway process on each node of the cluster. The most common scenario for running a gateway process on multiple computers in the cluster is that you have a load balancer in front of the cluster. In this scenario, the load balancer distributes requests to any gateway in the cluster. If you need to take a node off line (for example, to perform maintenance on that node), you can disable the load balancer's routing to that machine. When the maintenance is complete, you can re-enable the node on the load balancer.

You must have a gateway process running on at least one computer in the cluster. If you remove the gateway process from the primary server, you must make sure that another computer in the cluster is running the gateway process. You must also make sure that that computer is reachable by clients.

If the Tableau Server is configured to use SSL, you must make sure that the certificate for SSL support is in the same location on each computer in the cluster that has the gateway process running. For more information about using SSL, see Configure SSL for External HTTP Traffic to and from Tableau Server.

Similarly, if the server installation uses a custom logo, the logo must be in the same location on every computer that is running the gateway process.

If you need to change the port number that the gateway process listens on, as explained earlier, you can use the configuration dialog box or run the following command for each worker computer that is running the gateway process:

```
tsm topology set-ports --node-name node --port-name gateway:primary --port-value nn
```

Additional information

Configuring Proxies for Tableau Server

Add a Load Balancer
Tableau Server Repository

Tableau Server Repository is a database that stores server data. This data includes information about Tableau Server users, groups and group assignments, permissions, projects, data sources, and extract metadata and refresh information.

<table>
<thead>
<tr>
<th>Process</th>
<th>Repository</th>
</tr>
</thead>
<tbody>
<tr>
<td>File name</td>
<td>postgres.exe</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the Repository is visible on the Status Page. For more information, see View Server Process Status</td>
</tr>
<tr>
<td>Logging</td>
<td>Logs generated by the repository are located in /var/-opt/tableau/tableau_server/data/tabsvc/logs/pgsql. For more information, see Server Log File Locations</td>
</tr>
</tbody>
</table>

Preferred active repository

When you configure Tableau Server you have the option to specify a node as the preferred active repository. When Tableau Server is configured for repository failover, the preferred active repository node is the one used for the active repository. This is an optional step, and if you do not specify a preferred active repository node, Tableau Server will select the active repository node on startup.

To configure the preferred active repository, use the `tsm configuration set` command to configure the `pgsql.preferred_host` option:

```
tsm configuration set -k pgsql.preferred_host -v "<host_name>"
```

**Note:** The `host_name` is case-sensitive and must match the node name shown in the output of `tsm status -v`.

Configure a preferred active repository node if you want Tableau Server to select a specific node on startup. You might want to do this if you have a particular server you want to use for
your active repository (a computer with more disk space or memory for example), or if you are using custom administrative views. Custom administrative views have embedded connection information that refers to the repository for which you created the views. For more information on connecting to the Tableau Server repository, see Collect Data with the Tableau Server Repository.

The failoverrepository Command

If failover occurs and your passive repository becomes the active repository, it remains the active repository until either Tableau Server restarts or you use the tsm topology failover-repository command to switch back. Specify the repository you want to be the active one, or specify that the preferred active repository (if configured) should be made active again. For more information, see tsm topology failover-repository.

Tableau Server Microservice Containers

The two Microservice Container processes, Interactive Microservice Container and Non-Interactive Microservice Container, are added automatically to a Tableau Server node when a microservice contained in one of these container processes is added to the server. The microservices within these container processes are internal to Tableau Server. You cannot add or configure a microservice or a Microservice Container directly.

Microservice Containers and the microservices:

- Interactive Microservice Container:
  - Relationship Query Microservice
  - Content Model Microservice

- Non-Interactive Microservice Container:
  - Relationship Ingestor Microservice
  - Content Provider Microservice
Viewing Microservice Container Status

You can see the status of the Microservice Container processes from the TSM Status page, or from the command line, using the `tsm status -v` command. When you use the TSM Status page to View Server Process Status, the status of each container process is visible, but you cannot see the status of any of the microservices in the containers. When you use the command line, more detail is shown, including the status of each individual microservice.

Microservice Container Status

The status of a container process depends on the status of the microservices within the container. When all microservices within a container process are running as expected, the container status is Active (on the TSM Status page) or running (when viewed from the TSM command line). If all microservices within a container process are stopped, the status for the container is Error (on the TSM Status page) or stopped (from the TSM command line). If a microservice is stopped but at least one other microservice is running, the container status is Degraded (on the TSM Status page) or degraded (from the TSM command line).

When all microservices within a container process have a status of running, the container status is Active. If any microservice in a container is in an error state (has a status of stopped) the container process status is degraded. If all microservices in a container are in an error state, the container status is error.

Use the TSM web interface

To view the Microservice Container status from the TSM Status page:

1. Open TSM in a browser:

   http://<tsm-computer-name>:8850

2. Click Status:
The page displays the status for the Interactive Microservice Container and Non-Interactive Microservice Container processes, as well as status for other processes running as part of TSM or Tableau Server.

You cannot see the status of any individual microservice within a container process, but if the container process has a status of Active (a green check), the microservices it contains are all running as expected. To see the status of individual microservices, use the TSM command line.

**Note:** The status of the container processes does not display on the older Tableau Server status page. For details about the two status pages and how they differ, see View Server Process Status.

Use the TSM CLI

To view the Microservice Container status from the TSM command line:

1. Open a command prompt as administrator on the initial node (the node where TSM is installed).

2. Run the following command:

   `tsm status -v`

   The output from the command shows you the status of the container services and the microservices in them:

   `-node1: TABLEAUSVR01-
   Status: RUNNING
   'Tableau Server Gateway 0' is running.
   'Tableau Server Application Server 0' is running.
   'Tableau Server Interactive Microservice Container 0' is running.`
'Relationship Query Microservice 0' is running.
'Content Model Microservice 0' is running.
'Tableau Server VizQL Server 0' is running.
'Tableau Server VizQL Server 1' is running.
'Tableau Server VizQL Server 2' is running.
'Tableau Server VizQL Server 3' is running.
'Tableau Server Cache Server 0' is running.
'Tableau Server Cache Server 1' is running.
'Tableau Server Coordination Service 0' is running.
'Tableau Server Cluster Controller 0' is running.
'Tableau Server Search And Browse 0' is running.
'Tableau Server Backgrounder 0' is running.
'Tableau Server Backgrounder 1' is running.
'Tableau Server Non-Interactive Microservice Container 0' is running.
'Relationship Ingestor Microservice 0' is running.
'Content Provider Microservice 0' is running.
'Tableau Server Data Server 0' is running.
'Tableau Server Data Server 1' is running.
'Tableau Server Data Engine 0' is running.
'Tableau Server File Store 0' is running.
'Tableau Server Repository 0' is running (Active Repository).
'Tableau Server Tableau Prep Conductor 0' is running.
'Tableau Server Elastic Server 0' is running.
'Tableau Server Ask Data 0' is running.
'Tableau Server Administration Agent 0' is running.
'Tableau Server Administration Controller 0' is running.
'Tableau Server Service Manager 0' is running.
'Tableau Server License Manager 0' is running.
'Tableau Server Client File Service 0' is running.
'Tableau Server Database Maintenance 0' is stopped.
'Tableau Server Backup/Restore 0' is stopped.
Tableau Prep Conductor

Overview

If you build flows in Tableau Prep, you can automate running your flows to refresh flow input and output data on a schedule using Tableau Server, instead of opening Tableau Prep Builder to run individual flows manually.

Tableau Prep Conductor is one of the process on Tableau Server. It runs flows, checks connection credentials, and sends alerts if a flow fails. Tableau Prep Conductor leverages the scheduling and tracking functionality of Tableau Server so you can automate running flows to update the flow output instead of logging into Tableau Prep Builder to manually run individual flows as your data changes.

Tableau Prep Conductor is licensed through the Data Management Add-on. To use Tableau Prep Conductor, you must have the Data Management product key activated on your server. For more information, see Licensing Tableau Prep Conductor.

Tableau Prep Conductor uses the following components to run flows:

- **Backgrounder**: Tableau Prep Conductor uses the Backgrounder process to run flows. Backgrounder is single threaded, so each instance of the Backgrounder process on a node can run one flow at a time. By adding more Backgrounders to a node, you can increase the number of flows that can be run in parallel on that node. The Backgrounder processes can be up to half the number of the physical cores of that node.

- **Connectors**: Prep Conductor uses the supported Tableau Data connectors to
connect to data. For a list of supported Connectors, see Supported Connectors.

- **Data Engine**: Any changes to data or transformation steps in your flow that cannot be pushed to the underlying data source are processed using the Data Engine process. For example, SQL Server does not natively support regular expressions. When connecting to SQL Server, Tableau Prep lets you write regular expression calculations. Tableau Prep Conductor uses Data Engine to temporarily load the data and then perform the regular expression.

**Performance and Scale Recommendations**

- **Isolate flows to a separate node**: Running Tableau Prep Conductor on a separate node will isolate flow workflows from other Tableau workloads. This is highly recommended since Prep flows are CPU and RAM intensive.

- **Manage flow schedules**: You can control flow execution by creating flow schedules. These schedules let you determine when flows run, how frequently they run, the priority of that schedule, and whether to run items in that schedule serially or in parallel.

- **Add resources**: When scaling your Tableau Prep Conductor environment, we recommend scaling up to an 8 physical cores box per node running as many as 4 backgrounders on each. As you need more resources, we recommend adding more nodes to your server environment.

You can monitor user activity and performance of flows using Administrative views. For more information, see Monitor Flow Health and Performance.

**Topology and Configuration**

By default, the installer enables Tableau Prep Conductor on all nodes that already have backgrounder enabled and where the following conditions are true:

- The Tableau Server has a valid Data Management product key.

- The node role is either set to allow all tasks or to allow only flows. For more
Enabling Tableau Prep Conductor on Tableau Server

To enable Tableau Prep Conductor, use the Tableau Data Management product key. Tableau Prep Conductor is now licensed and enabled at the server level.

Before you can start publishing flows to your Tableau Server, there are server-level and site-level settings you must configure or verify to prepare your Tableau Server to allow publishing, scheduling and monitoring flows.

Review the following topics to understand Tableau Prep Conductor licensing, and learn how to enable Tableau Prep Conductor:

- **Enable and Configure Tableau Prep Conductor on Tableau Server**: This topic provides step-by-step instructions on how to enable and configure Tableau Prep Conductor, and preparing your Tableau Server to allow publishing, scheduling, managing, and maintaining flows.

- **License Overview**: This topic describes the license concepts that Tableau Prep Conductor add-on licensing introduces.

Tableau Server Dynamic Topology Changes

With the introduction of TSM, Tableau Server also introduced the ability to make certain topology changes or updates without restarting the server. These are known as dynamic
topology changes, and are possible with the backgrounder and VizQL Server processes.

You can increase or decrease the number of backgrounder or VizQL Server instances on a node that already has at least one of these processes running, without any Tableau Server downtime. If you have a node already running backgrounder, you add additional instances of backgrounder or VizQL Server to the node without restarting Tableau. You can do the same with VizQL Server node running VizQL Server, adding or removing instances of either backgrounder or VizQL Server. You must be only changing the number of instances of backgrounder or VizQL Server. If you also add or remove another process, you need to restart Tableau Server. For example, if you have a node running four instances of VizQL Server, you can remove all those instances and add one or more instances of backgrounder instead, without restarting Tableau Server, taking advantage of dynamic topology changes.

Example Scenarios

To better understand why this might be useful, consider these examples:

- **Backgrounder**—At the end of a sales quarter your sales team is using Tableau Server to keep track of their numbers. Dashboards that depend on extracts are showing sales people how they are doing. Any delay in extract refreshes means your team is not seeing the most up-to-date numbers. You can add additional backgrounders to any node that already has at least one backgrounder or VizQL Server, and increase the throughput of extract refreshes, helping to guarantee the numbers are up-to-date as your team finished up their quarter. Later, after the quarterly push, you can reduce the backgrounder instances again to return Tableau Server to its original configuration.

- **VizQL Server**—Similarly, if Tableau Server is unable to keep up with view refreshes, you can quickly add additional VizQL Server instances to any node that already has at least one instance of either VizQL Server or backgrounder configured. In the above backgrounder example, you might want to remove VizQL Servers temporarily, to accommodate additional backgrounders, and then re-add them back before your users arrive in the morning.

Making dynamic topology changes

You can make dynamic topology changes using the TSM Web UI, or on the command line. To use the Web UI, sign in to TSM using a browser, and on the Configuration tab, update
the number of backgrounder or VizQL Server instances for the node you are updating. For details, see Configure Nodes. To make your changes using the TSM CLI, at a command prompt, run the tsm topology set-process command. For details, see Changing the number of processes on a node.

Impact of dynamic topology changes

When making dynamic topology changes that remove existing instances of VizQL Server or backgrounder, the instances are removed immediately. Be aware of the following potential impacts to users and currently running jobs:

- Backgrounder—Any currently running jobs are terminated. The normal Tableau Server retry logic will restart these jobs, using another backgrounder instance.

- VizQL Server—Any currently active sessions are terminated. Users may see an error message. Refreshing the browser should clear the error.

Best practices

Tableau recommends you test any dynamic topology changes you plan on using, before implementing them in your production environment. This will help you fully understand potential impacts to your users and scheduled refreshes and subscriptions, and allow you to most efficiently take advantage of the flexibility offered by dynamic topology.

Automating dynamic topology changes

You can automate dynamic topology changes. For example, if you have most of your extract refreshes scheduled overnight, and know your server has extra capacity because users are not signed in, you can use a script or other automated deployment tool to add backgrounder instances when they can be most efficiently used, and then remove them before the start of the work day.

To automatically get the status of processes, use the tsm status -v command and parse the output in your script. Alternately, you can use the TSM REST API get server status. The API is currently in alpha. For more details, see Get server status.

A sample script to set four instances of backgrounder on node2 might look like this:
echo Adding/Removing Processes
tsm topology set-process -pr backgrounder -n node2 -c 4
tsm pending-changes apply
echo Done!

Additional information

Tableau Server Processes

Server Process Limits

When you reconfigure processes for Tableau Server, there is a limit to the amount that you can increase the number of process instances. By default, the limit is set to eight. If your machine has enough RAM and CPU cores, and you want to go above this limit, you can change the limit using the `service.max_procs` configuration option. For each process instance, Tableau recommends that the machine running the process have at least 1 GB of RAM and 1 logical CPU core.

To change the maximum number of processes allowed:

1. Type the following command, where `number` is the maximum number of process instances you want to allow:

   ```
   tsm configuration set -k service.max_procs -v <number>
   ```

   For example:

   ```
   tsm configuration set -k service.max_procs -v 10
   ```

2. Next type:

   ```
   tsm pending-changes apply
   ```

   The `pending-changes apply` command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt
using the --ignore-prompt option, but this does not change the restart behavior. For more information, see tsm pending-changes apply.

Tableau Services Manager Ports

The processes and services that make up the components of Tableau Services Manager (TSM) and Tableau Server on Linux use various ports to communicate. By default, most these ports are assigned (mapped) dynamically from a predefined range of ports. The port assignments are made for each service or process when it is installed. You can control what ports are used in a variety of ways.

A small subset of processes do not use dynamic port mapping and behave uniquely. For more information, see Ports that are not dynamically mapped, below.

Note: This operation includes steps that you may need to perform using the TSM command line.

Firewall requirements

If you are running a firewall on the computer where you will be installing Tableau Server, then you will need to open the following default ports for Tableau Server traffic. All port numbers, except 443 can be changed.

<table>
<thead>
<tr>
<th>Port</th>
<th>TCP/UDP</th>
<th>Used by ...</th>
<th>TYPE OF INSTALLATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP</td>
<td>Gateway</td>
<td>All</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>SSL. When Tableau Server is configured for SSL, the application server redirects requests to this port. Do not change this</td>
<td>X</td>
</tr>
</tbody>
</table>
### Port assignment

There are two approaches you can use for port assignment or mapping in TSM:

- **Dynamic port assignment.** This is the default and requires the least intervention by the administrator.
- **Manual port assignment.** This option requires an administrator to individually assign each port.

If you change port assignments and you are running a local firewall, see Local firewall configuration.

---

<table>
<thead>
<tr>
<th>Port</th>
<th>TCP/UDP</th>
<th>Used by ...</th>
<th>TYPE OF INSTALLATION</th>
<th>Distributed / High Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>8850</td>
<td>TCP</td>
<td>Tableau Services Manager.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>8060</td>
<td>TCP</td>
<td>PostgreSQL database.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>8061</td>
<td>TCP</td>
<td>PostgreSQL backup verification port</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8000-9000</td>
<td>TCP</td>
<td>Range of ports reserved by default for dynamic mapping of Tableau processes</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>27000-27009</td>
<td>TCP</td>
<td>Range of ports used by Tableau Server for License service. This range must be open on the node running the License service and accessible from other nodes. By default, the initial node runs the License service.</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

See Configure Local Firewall.
Dynamic port assignment

You can control which ports are used by changing the range of ports available to the dynamic assignment process. Doing this leaves dynamic port assignment in place but restricts the ports that can be chosen. With dynamic port assignment in place, you can still choose to assign ports for certain processes manually. This approach enables you to assign specific ports to specific processes, while leaving the others to be mapped dynamically. Using dynamic mapping, with or without some individually assigned ports is the easiest approach, and should satisfy the requirements of most customers. Dynamically assigned ports are preserved if you export your Tableau Server configuration.

By default, ports are assigned for each service or process from available ports between 8000 to 9000. This assignment takes place when services are installed for the first time on a node. After Tableau Server is initialized, you can see which ports are being used by which services or processes by running this command:

```plaintext
tsm topology list-ports
```

If you have a multi-node cluster, ports on all nodes are listed.

Changing the port range

For organizations that have specific requirements for ports being used, the easiest way to control this is to change the range from which ports are dynamically selected. You need to do this at installation, by specifying a minimum and maximum port for the range in your configuration file.

**Note:** The minimum allowable size of your port range will depend on your server installation and how many services or processes you are running. As a general best practice you should not restrict the range too tightly because port assignment is done by selecting random ports within the range, and if you do not allow a large enough range, selection may fail to find an available port.
To limit the range from which available ports are chosen to those between 8300 and 8600, your configuration file would include an entry similar to this:

```
"configKeys": {
  "ports.range.min": "8300",
  "ports.range.max": "8600"
}
```

Disabling dynamic port assignment

If you need more control of port assignment than you can get through a combination of restricting port range and individually assigning ports, you can disable dynamic port mapping at initial server configuration. Disabling dynamic port mapping requires you to manually assign every port for every process, so we don't recommend this unless you need to control every single port assignment.

If you disable dynamic port mapping, you must configure the port for each process on each node of your installation.

To disable dynamic mapping, your configuration file would include an entry similar to this:

```
"configKeys": {
  "service.port_remapping.enabled": false
}
```

**Important:** When you disable dynamic port assignments, the License service port range is not included. This range (27000-27009) must be open on the node running the License service and accessible from other nodes. By default, the initial node runs the License service.

**Manual port assignment**

You can disable automatic port assignment entirely and assign a port for each process individually. If you do this, you must assign a port for every process on every node. You can assign ports either in a configuration file, when the processes are first installed, or after
installation, using a TSM command. Only ports assigned at process installation are preserved if you export your Tableau Server configuration.

You can specify individual ports for specific processes, whether or not dynamic mapping is enabled. You might do this if you want a process to use a particular port, or if you've disabled dynamic mapping. There are two ways to specify ports for processes: during installation or after installation.

Configuring ports during installation

We recommend configuring port assignment during the installation process as described here. Changing ports after installation is a much more labor-intensive process.

To configure ports during installation, create a json file that specifies your port configuration. This process is similar to defining a non-default port range, but instead you specify a particular port for a specific service or process. If you are going to assign specific ports, this approach is the most robust way to do so because the port mapping is preserved if you export the server configuration and topology settings using the `tsm settings export` command.

To define ports at installation, add information to your configuration file to specify the node (`workerN`), process (`servicename`) and instance ID (`instanceid`), port type (`porttype`), and the port to be used. The format looks like this:

```
workerN.{servicename}_{instanceid}.{porttype}.port:X
```

Where:

- `workerN` is an optional parameter and identifies the node for which the remapping applies. Node numbers start with zero (0). We recommend you do not include this parameter unless you need to map different ports for the same service on different nodes. If you leave this parameter off, you can map a service port on the initial node, or map the same service port on multiple nodes.
- `servicename` is the name of the process or service that will use the port.
- `instanceid` is the instance of the process. If you are going to be configuring multiple instances of a process on one node, you would need to increment this value for
each instance. Start the instanceid at zero (0) and increment it by one (1) for each instance of the process. For services that only install a single instance on any given node, this must be left off.

- **porttype** If setting the primary port, do not include this option.
- **port** is the port the process or service should use.

For example, to set the port for the first instance of the file store process on the initial node to 8500, you would include a configuration file entry similar to this:

```
"configKeys": {
   "filestore_0.port": "8500"
}
```

The example above does not include the optional workerN parameter, so sets the port on all nodes in the cluster. It also leaves off the porttype option because it is setting the primary filestore port.

**Important:** When specifying port changes with a configuration file, you must include the `--force-keys` parameter with the `tsm settings import` command.

Configuring ports after installation

If you need to change ports after you have installed Tableau Server, use the `tsm topology set-ports` command. This approach allows you to specify a port for a specific process after that process has been installed. You are restricted by these limits:

- You must set ports individually, on each node.
- After you set an individual port, you must run `tsm restart`.
- The port assignments are not preserved if you need to import a Tableau Server configuration using `tsm settings import`.
- Port names use a different syntax for `tsm` commands than the syntax that is required for `configKeys`. The table at the end of this topic provides a syntax reference.

For example, to set second instance of the file store on the initial node to use port 8500:
The following example shows how to use shorthand commands to set the JMX ports:

```
 tsm topology set-ports --node-name node1 --port-name filestore --port-value 8500 --instance 2

 tsm topology set-ports -n node1 --port-name vizqlserver:jmx.rmi -pv 9403 -i 1

 tsm topology set-ports -n node1 --port-name vizqlserver:jmx -pv 9404 -i 2
```

**Note:** Port entries are not validated when you enter them. Therefore, if you use a port that is already assigned, or if you mistype the syntax for a command, Tableau will not give an error until you restart. After restarting, you may see a generic error, *The reconfigure async job failed.*

If you add an incorrect portname:type with a valid port, you cannot delete the incorrect entry. To update the port, you must reassign an unused port to that value to free up the port again.

Ports that are not dynamically mapped

The Tableau Server repository uses two ports that are not dynamically mapped. These each have a default port that you can override using the `tsm configuration set` command and a process-specific parameter.

<table>
<thead>
<tr>
<th>Port names</th>
<th>Port (default)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pgsql.port</td>
<td>8060</td>
<td>Port for the Tableau Repository (PostgreSQL database).</td>
</tr>
</tbody>
</table>

To override this port:

```
 tsm configuration set -k pgsql.port <port>
```
Port names | Port (default) | Description
---|---|---
pgsql.verify_restore.port | 8061 | Port for verifying the integrity of a repository backup.

to override this port:

tsm configuration set -k pgsql.verify_restore.port <port>

Because these ports do not use the dynamic port mapping system, they do not show up in the output of the `tsm topology list-ports` command. To see the value of these you need to use the `tsm configuration get -k <config.value>` command. For example:

```
tsm configuration get -k pgsql.port
```

### Controlling port remapping with initialize-tsm

Port assignments are made when services are installed. This means that in order to manually map ports for the TSM-specific processes, you need to assign the ports when you run the `initialize-tsm` script. The script includes options to specify ports for individual TSM services, as well as options for defining the minimum and maximum of the port range used with dynamic mapping, and you can disable dynamic mapping.

The table below lists the options for ports when running the `initialize-tsm` script.

### Table: initialize-tsm script port options

<table>
<thead>
<tr>
<th>Script option</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-i</td>
<td>&lt;port&gt;</td>
<td>Sets the Coordination Service client</td>
</tr>
</tbody>
</table>
Tableau Server on Linux Administrator Guide

<table>
<thead>
<tr>
<th>Script option</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>port.</td>
</tr>
<tr>
<td>-e</td>
<td>&lt;port&gt;</td>
<td>Sets the Coordination Service peer port.</td>
</tr>
<tr>
<td>-m</td>
<td>&lt;port&gt;</td>
<td>Sets the Coordination Service leader port.</td>
</tr>
<tr>
<td>-n</td>
<td>&lt;port&gt;</td>
<td>Sets the TSM agent file transfer port.</td>
</tr>
<tr>
<td>-o</td>
<td>&lt;port&gt;</td>
<td>Sets the TSM Controller port.</td>
</tr>
<tr>
<td>-l</td>
<td>&lt;min-port&gt;</td>
<td>Sets the bottom of the port range used for dynamically mapping ports.</td>
</tr>
<tr>
<td>-r</td>
<td>&lt;max-port&gt;</td>
<td>Sets the top of the port range used for dynamically mapping ports.</td>
</tr>
<tr>
<td>--disable-port-remapping</td>
<td></td>
<td>Disables dynamic port mapping. If you do this you must assign ports for every service or process used by TSM and Tableau Server. For more information, see Manual port assignment above.</td>
</tr>
</tbody>
</table>

Dynamically mapped ports

This table lists the processes or services that use dynamically mapped ports.

<table>
<thead>
<tr>
<th>Port names: syntax for json file (configKeys)</th>
<th>Port names: syntax for tsm CLI</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>appzookeeper_0.client.port</td>
<td>appzookeeper:client</td>
<td>Coordination Service client port.</td>
</tr>
<tr>
<td>appzookeeper_0.peer.port</td>
<td>appzookeeper:peer</td>
<td>Coordination</td>
</tr>
<tr>
<td>Port names: syntax for json file (configKeys)</td>
<td>Port names: syntax for tsm CLI</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>--------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>appzookeeper_0.leader.port</td>
<td>appzookeeper:leader</td>
<td>Service peer port.</td>
</tr>
<tr>
<td>backgrounder_0.port</td>
<td>backgrounder</td>
<td>Backgrounder primary port.</td>
</tr>
<tr>
<td>backgrounder_0.debug.port</td>
<td>backgrounder:debug</td>
<td>Backgrounder debug port.</td>
</tr>
<tr>
<td>backgrounder_0.jmx.port</td>
<td>backgrounder:jmx</td>
<td>Backgrounder jmx port.</td>
</tr>
<tr>
<td>backgrounder_0.jmx.rmi.port</td>
<td>backgrounder:jmx.rmi</td>
<td>Backgrounder jmx rmi port.</td>
</tr>
<tr>
<td>backgrounder_0.recommendations.trainer.port</td>
<td>backgrounder:recommendations.trainer</td>
<td>Backgrounder recommendations port.</td>
</tr>
<tr>
<td>backuprestore.port</td>
<td>backuprestore</td>
<td>Backup/Restore service port.</td>
</tr>
<tr>
<td>cacheserver_0.port</td>
<td>cacheserver</td>
<td>Cache server port.</td>
</tr>
<tr>
<td>clustercontroller.status.port</td>
<td>clustercontroller:status</td>
<td>Cluster Controller status port.</td>
</tr>
<tr>
<td>clustercontroller.storage.port</td>
<td>clustercontroller:storage</td>
<td>Cluster Controller storage port.</td>
</tr>
<tr>
<td>Port names: syntax for json file (configKeys)</td>
<td>Port names: syntax for tsm CLI</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>--------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>databasemaintenance.port</code></td>
<td><code>databasemaintenance</code></td>
<td>Database Maintenance port.</td>
</tr>
<tr>
<td><code>dataserver_0.port</code></td>
<td><code>dataserver</code></td>
<td>Data server primary port.</td>
</tr>
<tr>
<td><code>dataserver_0.debug.port</code></td>
<td><code>dataserver:debug</code></td>
<td>Data server debug port.</td>
</tr>
<tr>
<td><code>dataserver_0.jmx.port</code></td>
<td><code>dataserver:jmx</code></td>
<td>Data server jmx port.</td>
</tr>
<tr>
<td><code>dataserver_0.jmx.rmi.port</code></td>
<td><code>dataserver:jmx.rmi</code></td>
<td>Data server jmx rmi port.</td>
</tr>
<tr>
<td><code>filestore.port</code></td>
<td><code>filestore</code></td>
<td>File store primary port.</td>
</tr>
<tr>
<td><code>filestore.status.port</code></td>
<td><code>filestore:status</code></td>
<td>File Store status port.</td>
</tr>
<tr>
<td><code>gateway.port</code></td>
<td><code>gateway</code></td>
<td>Gateway port. This defaults to 80, and if that is not available, to 8080. If that is not available, it tries 8000. That sequence is followed whether or not dynamic port assignment is enabled or not. If none of</td>
</tr>
<tr>
<td>Port names: syntax for json file (configKeys)</td>
<td>Port names: syntax for tsm CLI</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>--------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>those ports are available and dynamic mapping is enabled, it takes an available port within the defined range. The gateway port must be the same on all nodes in a multi-node cluster, so if port 80 is selected on the initial node this is the port that will be used on all nodes and if it is unavailable on one of the other nodes, gateway port selection will fail.</td>
</tr>
<tr>
<td>hyper.port</td>
<td>hyper</td>
<td>Data engine primary port.</td>
</tr>
<tr>
<td>hyper.connection.port</td>
<td>hyper:connection</td>
<td>Data engine connection port.</td>
</tr>
<tr>
<td>licenseservice.vendor_dae-mon.port</td>
<td>licenseservice:vendor_daemon</td>
<td>License service vendor daemon port. Used for</td>
</tr>
<tr>
<td>Port names: syntax for json file (configKeys)</td>
<td>Port names: syntax for tsm CLI</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>samlservice.port</td>
<td>samlservice</td>
<td>licensing-related communications between nodes in a multi-node installation.</td>
</tr>
<tr>
<td>searchserver.port</td>
<td>searchserver</td>
<td>SAML service port.</td>
</tr>
<tr>
<td>searchserver.debug.port</td>
<td>searchserver:debug</td>
<td>Search server debug port.</td>
</tr>
<tr>
<td>searchserver.jmx.port</td>
<td>searchserver:jmx</td>
<td>Search server jmx port.</td>
</tr>
<tr>
<td>searchserver.jmx.rmi.port</td>
<td>searchserver:jmx:rmi</td>
<td>Search server jmx rmi port.</td>
</tr>
<tr>
<td>searchserver.startup.port</td>
<td>searchserver:startup</td>
<td>Search server startup port.</td>
</tr>
<tr>
<td>siteimportexport.port</td>
<td>siteimportexport</td>
<td>Site Import/Export port.</td>
</tr>
<tr>
<td>tabadmincontroller.port</td>
<td>tabadmincontroller</td>
<td>TSM Controller port.</td>
</tr>
<tr>
<td>tabadminagent.columbo.port</td>
<td>tabadminagent:columbo</td>
<td>Administration Agent service discovery port</td>
</tr>
<tr>
<td>tabadminagent.filetransfer.port</td>
<td>tabadminagent:filetransfer</td>
<td>TSM Agent file transfer port.</td>
</tr>
<tr>
<td>Port names: syntax for json file (configKeys)</td>
<td>Port names: syntax for tsm CLI</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>--------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>vizportal_0.authentication.port</td>
<td>vizportal:authentication</td>
<td>Application server authentication port.</td>
</tr>
<tr>
<td>vizportal_0.authorization.port</td>
<td>vizportal:authorization</td>
<td>Application server authorization port.</td>
</tr>
<tr>
<td>vizportal_0.maintenance.port</td>
<td>vizportal:.maintenance</td>
<td>Application server maintenance port.</td>
</tr>
<tr>
<td>vizportal_0.microservice.extensions.port</td>
<td>vizportal:.microservice:extensions</td>
<td>Application server extensions port.</td>
</tr>
<tr>
<td>vizportal_0.monolith_grpc.port</td>
<td>vizporta:monolith_grpc</td>
<td>Application server GRPC port.</td>
</tr>
<tr>
<td>vizportal_0.publishing.port</td>
<td>vizportal:publishing</td>
<td>Application server publishing port.</td>
</tr>
<tr>
<td>vizportal_0.recommendations.port</td>
<td>vizportal:recommendations</td>
<td>Application server recommendations port.</td>
</tr>
<tr>
<td>vizportal_0.port</td>
<td>vizportal</td>
<td>Application server primary port.</td>
</tr>
<tr>
<td>vizportal_0.debug.port</td>
<td>vizportal:debug</td>
<td>Application server debug port.</td>
</tr>
</tbody>
</table>
Enable the JMX Ports

To help you work through a problem with Tableau Server, Tableau Support may ask you to enable the server’s JMX ports. These ports can be useful for monitoring and troubleshooting, usually with a tool like JConsole.

To enable the JMX ports on Tableau Server:

1. Stop the server.

2. Enter the following command:

   `tsm configuration set -k service.jmx_enabled -v true`

3. Apply pending changes:
tsm pending-changes apply

The pending-changes apply command displays a prompt to let you know this will restart Tableau Server if the server is running. The prompt displays even if the server is stopped, but in that case there is no restart. You can suppress the prompt using the --ignore-prompt option, but this does not change the restart behavior. For more information, see tsm pending-changes apply.

4. Start the server.

**Important** Enabling JMX ports can introduce some security risk. To mitigate this risk, it is important to limit access to the JMX ports to the fewest number of clients that's practical for your scenario. You typically limit access using the host's firewall rules, an external security device, or routing rules.

How the JMX Ports Are Determined

By default, the JMX ports assigned dynamically, from within a range of available ports. For details on how port assignment is done, and how to override dynamic mapping, see Tableau Services Manager Ports.

Help Output for initialize-tsm Script

The following help content is the output when you run the following command:

```
sudo ./initialize-tsm -h
```

The initialize-tsm script is installed to `/opt/tableau/tableau_server-/packages/scripts.<version_code>/`.

Output

**REQUIRED**

`--accepteula` Indicate that you have accepted the End User License Agreement (EULA).
You can find the EULA in `/opt/tableau/tableau_server-packages/docs.<version_code>`

**OPTIONAL**

- **c config-name**
  Set the service configuration name.
  If not set, the default is "tabsvc".

- **d data-directory**
  Set a custom location for the data directory
  if it's not already set. If not set, the default is "/var/opt/tableau/tableau_server".

- **b bootstrap-file**
  Optional. Location of the bootstrap file
downloaded from the Tableau Services Manager
  on existing node. Must be provided to join existing Tableau Server cluster.

- **u username**
  Name of the user with admin privileges on
  existing Tableau Services Manager.
  Required if -b option specified.

- **p password**
  Password for the Tableau Services Manager
  admin user.

- **f**
  Bypass warning messages.

- **g**
  Do NOT add the current user to the "tsmad-
  min" administrative
group, used for default access to Tableau Services Manager
  or
to the "tableau" group, used for easier access to log files.

- **a username**
  user to be added
  The provided username will be used as the
to the appropriate groups, instead of the user running the script. Providing both -a and -g is not allowed.

-q   Quiet, suppress output except for errors and warnings.

-i coordinationservice-client-port   Client port for the coordination service

-e coordinationservice-peer-port   Peer port for the coordination service

-m coordinationservice-leader-port   Leader port for the coordination service

-t licenseservice-vendordaemon-port   Vendor daemon port for the licensing service

-n agent-filetransfer-port   Filetransfer port for the agent service

-o controller-port   Https port for the controller service

-l port-range-min   Lower port bound for automatic selection

-r port-range-max   Upper port bound for automatic selection

--disable-port-remapping   Disable automatic port selection

--unprivileged-user=<value>   Name of the unprivileged
account to run Tableau Server.
Default: "tableau".

--tsm-authorized-group=<value> Name of the group(s) that
allows authorization to access Tableau Services Manager.
Default: "tsmadmin".

--disable-account-creation Do not create groups or
user accounts for Server and TSM authorization.
However, the values in: unprivileged-used
ized-group will still be used
in TSM configuration.

--debug Print each command as it is run for
debugging purposes. Produces extensive
output.

--http_proxy=<value> Http forward proxy for
Tableau Server. Its value should be http://<proxy_address>:<proxy_port>/
For example, --http_proxy=http://1.2.3.4:3128/

--https_proxy=<value> Https forward proxy for
Tableau Server. Its value should be http://<proxy_address>:<proxy_port>/
For example, --https_proxy=http://example.com:3128/
Take care to use
https_proxy environmental variable.
Do not specify
https_proxy environmental variable.

--no_proxy=<value> Environment variable that directs certain
URLs to bypass the forward proxy. For example,

```bash
--no_proxy=
y=localhost,127.0.0.1,localaddress,.localdomain.com
```

Related topics

- Controlling port remapping with initialize-tsm
- Install and Initialize TSM
- System user and groups
- Data directory

View Server Version

The version of Tableau Server you are running is important. It determines the functionality and capabilities you have access to. Version is also important when you are upgrading, because in some cases how you upgrade depends on which version you are upgrading from, and which version you are upgrading to. Knowing your version is easy, once you understand how to find it.

- Viewing version in Tableau Server—All server users can view the version of Tableau Server from the Help menu in the server web UI.

- Viewing version in Tableau Services Manager (TSM)—TSM administrators can view the versions of TSM and Tableau Server from the TSM command line (CLI).

Viewing the server version from the Tableau Server web UI

- While logged into Tableau Server, click the information icon (ℹ️) and **About Tableau Server**.
The version of Tableau Server is listed in the About Tableau Server dialog box:

Viewing the server version and TSM version from the TSM command line

1. Open a command prompt as administrator on the initial node (the node where TSM is installed).

2. Run the following command:

   tsm version

The output displays the versions of Tableau Services Manager (TSM) and Tableau Server.

For example:

   C:\> tsm version
   Tableau Services Manager command line version
   2018.2.5 (20182.18.1214.0751) 64-bit Linux
   Tableau Server version 20182.18.1214.0751.
Short version, long version, and version_code

In most cases, when you need to know your version number, you need to know the "short" version. This version number displays in the About Tableau Server dialog box and is made up of three parts: major, minor, and maintenance versions. The short version number has this format: nnnn.n.n. For example: 2018.2.5.

A longer version includes the major and minor version numbers, as well as other build-specific information, and has this format: nnnnn.nn.nnnn.nnnn, for example: 20182.18.1214.0751. When you see a reference to <version_code> in this documentation, it means this longer version. The most common reference to this version_code or long version in the documentation is when we are discussing install locations or paths to the scripts or bin directories.

Tableau Server is installed in a /packages directory, with subdirectories that include the long version in the path name. This means that when you are navigating to a location within the /packages directory, you need to include the long version. For example, the /scripts directory: /opt/tableau/tableau_server-/packages/scripts.<version_code>./.

For example: /opt/tableau/tableau_server-/packages/scripts.20182.18.1214.0751

Finding the long version number

This longer version also displays in the About Tableau Server dialog box, in parentheses:

<table>
<thead>
<tr>
<th>About Tableau Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tableau Server Version: 2018.2.5 (20182.18.1214.0751) 64-bit Linux</td>
</tr>
<tr>
<td>©2018 Tableau Software, Incorporated and its licensors. All rights reserved.</td>
</tr>
</tbody>
</table>
Manage Dashboard Extensions in Tableau Server

Dashboard extensions are web applications that run in custom dashboard zones and can interact with the rest of the dashboard using the Tableau Extensions API. Dashboard extensions give users the ability to interact with data from other applications directly in Tableau.

**Note:** You must be a server administrator to enable dashboard extensions on the server, or to block specific extensions from running. You must be a server administrator to add extensions to the safe list and to control the type of data the extensions can access. The server administrator can also configure whether users on the site will see prompts when they add or view extensions in a dashboard.

For information about using dashboard extensions in Tableau, see [Use Dashboard Extensions](#).

Looking for Tableau Online? See [Manage Dashboard Extensions in Tableau Online](#).

Before you run extensions on Tableau Server

Dashboard extensions are web applications and could be running on any computer set up as a web server. This includes local computers, computers in your domain, and third-party web sites. Because extensions could be hosted on third-party sites and could have access to the data in the dashboard, you want to only allow the extensions you trust. See [Test extensions for security](#).

For security, you can use the settings for dashboard extensions on Tableau Server to control and limit the dashboard extensions that are allowed to run.

- Be default, no extensions are allowed unless they have been explicitly added to the safe list.
- You can change the **Default behavior for Extensions** to also allow extensions that
haven't been added to the safe list. If you change the default to allow unknown or unspecified extensions to run, those extensions are also allowed, provided that they do not require full data (access to underlying data) from the view. If a user adds one of these unknown extensions to a dashboard, the user first sees a prompt where they can choose to allow or deny the extension permission to run.

- By default, only extensions that use the HTTPS protocol are allowed, which guarantees an encrypted channel for sending and receiving data (the only exception is for http://localhost).

- If the extension requires full data (access to the underlying data) the extension will not be able to run on Tableau Server unless you explicitly add the extension to the safe list and grant the extension access to full data.

Control dashboard extensions and access to data

Server administrators can control a global setting to allow extensions for all sites on the server. Server administrators can also put extensions on a global block list to prevent them from running (see Block specific extensions). By default, extensions are enabled on the server (with the constraints previously described). You can change the settings that enable and control dashboard extensions.

Change the global setting enabling extensions on the server

1. To change this setting for the server, go to Manage All Sites > Settings > Extensions. If the server just has a single site, the global controls appear on the settings page for the site.

2. Under Dashboard Extensions, select or clear the Enable users to run extensions on this server checkbox. If not selected, extensions are not allowed to run. This setting overrides the settings for each site.

Change the default settings for a site

Server administrators can control whether to enable extensions for the site and whether to enable the default behavior (or policy) for extensions. That is, if enabled, the default
behavior is that extensions that are not already on the safe list are allowed, provided that they do not request full data. And users will see prompts asking for permission to run those extensions.

1. To change these settings for the site, go to Settings > Extensions.

2. Under Dashboard Extensions, select **Enable users to run extensions on this site**.

3. Under Default behavior for Extensions, select **Enable unknown extensions to run, always displaying user prompts and without full data access**.

Server administrators can add or remove extensions from the safe list for a site. When you add an extension to the safe list, you can control whether to allow the extension to have access to full data. See Add extensions to the safe list and configure user prompts.

**Identifying an extension**

As a web application, an extension is associated with a URL. You use this URL to test and verify the extension. You also use the URL to add the extension to the safe list to allow full data access, or to the block list to prohibit any access.

If you have the extension manifest file (.trex), an XML file that defines properties for the extension, you can find the URL from the `<source-location>` element.

```
<source-location>
  <url>https://www.example.com/myExtension.html</url>
</source-location>
```

If you have added the extension to the dashboard, you can find the URL from the extension properties. From the **More Options** menu, click **About**.
The About dialog box lists the name of the extension, the author of the extension, the website of the author, along with the URL of the extension.

Add extensions to the safe list and configure user prompts

To ensure that users can use extensions that are trusted, you can add them to the safe list for the site.

On the safe list, you can control whether to grant the extension full data access. You can also control whether users will see a prompt asking them to allow the extension access to data. If the extension does not require full data access, you don’t need to add it to the safe list. However, you might want to add an extension to the safe list so that you can configure whether or not users see the prompts. When you hide the prompt from users, the extension can run immediately.
1. Go to **Settings > Extensions**.

2. Under **Enable Specific Extensions**, add the URL of the extension. See Identifying an extension.

3. Choose to **Allow** or **Deny** the extension **Full Data Access**.

   Full data access is access to the underlying data in the view, not just the summary or aggregated data. Full data access also includes information about the data sources, such as the names of the connection, fields, and tables. In most cases, if you are adding an extension to the safe list so that it can run, you will also want to allow the extension to have access to full data, if the extension requires it. Before adding extensions to the safe list, be sure to Test extensions for security.

4. Choose to **Show** or **Hide** the **User Prompts**.

   Users see the prompts by default when they are adding an extension to a dashboard, or when they are interacting with a view that has an extension. The prompt tells users details about the extension and whether the extension has access to full data. The prompt gives users the ability to allow or deny the extension from running. You can hide this prompt from users, allowing the extension to run immediately.

**Block specific extensions**

The default global policy allows unknown extensions to run, provided that they only access summary data. Server administrators can keep specific extensions from running by adding them to the block list for the server. If an extension is on the global block list it overrides any settings for the extension on the safe list for a site.

1. To add an extension to the blocked list for the server, go to **Manage All Sites > Settings > Extensions**. On single-site installations, the block list is on the site Extensions settings page.

2. Under **Block Specific Extensions**, add the URL of the extension. See Identifying an extension.
Test extensions for security

Dashboard extensions are web applications that interact with data in Tableau using the Extensions API. Dashboard extensions contain JavaScript and could be hosted on sites outside of your domain. Because of this and the potential vulnerabilities, such as cross-site scripting, you should test and vet dashboard extensions before users use them in dashboards on Tableau Desktop, and before you allow extensions on Tableau Server.

Examine the source files

Dashboard extensions are web applications and include various HTML, CSS, and JavaScript files, and an XML manifest file (*.trex) that defines the properties in the extension. In many cases, the code for a dashboard extension is publicly available on GitHub and can be examined there or downloaded. In the manifest file (*.trex), you can find the source location, or URL indicated where the extension is hosted, the name of the author, and the web site of the author or company to contact for support. The <source-location> element specifies in the URL, the <author> element, specifies the name of the organization and the web site to contact for support (website="SUPPORT_URL"). The web site is the Get Support link user see in the About dialog box for the extension.

Many dashboard extensions reference external JavaScript libraries, such as the jQuery library or API libraries for third parties. Validate that the URL for external libraries points to a trusted location for the library. For example, if the connector references the jQuery library, make sure that the library is on a site that is considered standard and safe.

All extensions are required to use HTTPS protocol (https://) for hosting their extensions. You should examine the source files for the extension to ensure that any reference to external libraries is also using HTTPS or is hosted on the same web site as the extension. The one exception to the requirement of HTTPS is if the extension is hosted on the same computer as Tableau (http://localhost).

To the extent possible, make sure you understand what the code is doing. In particular, try to understand how the code is constructing requests to external sites, and what information
is being sent in the request. In particular, check if any user-supplied data is validated to prevent cross-site scripting.

Understand data access

The Tableau Extensions API provides methods that can access the names of the active tables and fields in the data source, the summary descriptions of the data source connections, and the underlying data in a dashboard. If an extension uses any of these methods in a view, the extension developer must declare that the extension requires full data permission in the manifest file (.trex). The declaration looks like the following.

```xml
<permissions>
  <permission>full data</permission>
</permissions>
```

Tableau uses this declaration to provide a prompt to users at run time that gives them the option of allowing this access or not. If the extension uses any one of these four methods, without declaring full-data permission in the manifest file, the extension will load but the method calls will fail.

For information about how an extension accesses data from the dashboard, and the JavaScript methods used, see Accessing Underlying Data in the Tableau Extensions API. To get a better understanding about what the extension can find out about the data, you can use the DataSources sample dashboard extension (available from the Tableau Extensions API GitHub repository) to see what data is exposed when the `getDatasourcesAsync()` method is called.

Test the extension in an isolated environment

If possible, test the dashboard extension in an environment that is isolated from your production environment and from user computers. For example, add a dashboard extensions to a safe list on a test computer or virtual machine that's running a version of Tableau Server that is not used for production.
Monitor traffic created by the dashboard extension

When you test a dashboard extension, use a tool like Fiddler, Charles HTTP proxy, or Wire-shark to examine the requests and responses that the extension makes. Make sure that you understand what content the extension is requesting. Examine the traffic to be sure that the extension is not reading data or code that is not directly related to the purpose of the extension.

Changing the Identity Store

Infrastructure or business changes may require you to change the identity store on Tableau Server. There are two kinds of identity stores: local and external. When you installed Tableau Server you configured either a local identity store or an external identity store.

When you configure Tableau Server with a local identity store, all user and group information is stored and managed in the Tableau Server repository. In the local identity store scenario, there is no external source for users and groups.

When you configure Tableau Server with an external store, all user and group information is stored and managed by an external directory service. Tableau Server must synchronize with the external identity store so that local copies of the users and groups exist in the Tableau Server repository, but the external identity store is the master source for all user and group data. Examples of external identity stores are OpenLDAP and Active Directory.

For more information about the Tableau identity store, see Identity Store.

You can change from local store to an external store, or you can change from an external store to a local store. In either case, to change the identity store type, you complete these steps:

1. Uninstall (including manual deletion of directories) and then reinstall of Tableau Server. The procedure for full uninstall and clean install are at the end of this topic.
2. Restore content and permissions.
Warning

Changing the installation type on Tableau Server can be a complicated and time-consuming process. To avoid data loss or orphaning of content or users, you'll need to plan this process carefully. In all cases, user filters applied to workbooks and data sources will need to be updated manually after the change.

Most importantly, determine how you will transition content and permissions to the new identity store after you reinstall Tableau Server.

Methods for restoring content and permissions

The following list describes two methods for restoring content and permissions after you reinstall Tableau Server. Select the method that best fits with your environmental requirements.

- **Method 1: Use site export and import**—In this method, you start by exporting each site in your existing deployment. Then, you install the new server and configure it for the new identity store type. You then create new users in the default site on the new server. Finally, you import all the original sites. During the import stage, you can map the original identities to the new users that you created in the default site.

You must use the same version of Tableau Server for the export and import operations. Importing a site to a version of Tableau Server that is different from the exported site version is not supported.

Because this method exports all content and permissions at each site, it is the best method for organizations that require a high fidelity replica of the content and permissions after the identity store change is complete. Some organizations require an identity store change as the result of an authentication change. In these cases, a different user name syntax is a often a requirement in the new model. This method, which includes a process of mapping original user names to new names, provides flexibility for such scenarios.
Method 2: Fresh installation; users republish content—In this method, you install a new version of Tableau Server and select the new identity store type during setup. You also create new sites. You then create users and give them access, and they republish their workbooks and data sources. Unlike the other method, in this one, you do not reuse any of your existing Tableau Server infrastructure.

This method is most appropriate for smaller deployments with fairly autonomous and data savvy users. From an administrative perspective, this method is the simplest, since you’re not actively porting over content. However, because you rely entirely on users to republish content, this method may not be successful for large organizations or for those where centralized oversight of content is required.

User filters

User filters are domain-specific. Therefore, when the domain of Tableau Server changes or authentication type changes, filters no longer function as expected. Although the user filters are generated by Tableau Server, after they are set by the user, the filters are stored in the workbooks and data sources. Neither of these methods for changing the identity store modifies the contents of the workbooks or data sources.

As you plan the identity store change, you must also include a final task to correct user filtering in all workbooks and data sources with Tableau Desktop.

User names and the Tableau Identity store

If you are using Method 1, it's helpful to understand how Tableau Server stores user names in the Tableau identity store. Tableau stores all user identities in the repository, which coordinates content permissions and site membership with various services in Tableau Server. Generally, an identity store configured for Active Directory store user names in the format, domain\username. Some organizations use a UPN (jsmith@domain.lan).

On the other hand, organizations that configure Tableau Server with local identity store usually create standard, truncated user names, such as jsmith.
In all cases, these user names are literal strings that must be unique in the Tableau identity store. If you are changing from one identity store type to another, then your target authentication, SSO, or user provisioning solution may require a specific user name format.

Therefore, to maintain all permissions, content, and user viability, one of the following must be true after you change the identity store type:

- The new user names must match the original user names, or
- The original user names must be updated to match a new format.

If an authentication change is driving the identity store change, then the target authentication scheme will likely impose a user name syntax that is different than your original user names. Method 1 includes a process where you can map original user names to new user names.

It's possible that the original user name format will work with the new authentication type. For example, if you used UPN names in a local identity store deployment, you might be able to use the same user names in an Active Directory deployment. You could also use the `domain\username` format for local identity store, as long as users continue to use that format to sign in to Tableau Server.

If you are changing from local identity store to an external Active Directory store, review the topic, User Management in Active Directory Deployments, as part of your planning process.

**Method 1: Use site export and import**

You must use the same version of Tableau Server for the export and import operations.

1. Export all sites on your server. See Export or Import a Site.
2. Back up, remove, and then reinstall.
3. Create new users on Tableau Server. You should have a new user that corresponds to each user on the original server.
4. Import the sites that you exported in Step 1. See Export or Import a Site. During import, you will be prompted to map the new users to the original users.
Method 2: Fresh installation—users republish content

Even if you do not plan to port content as part of your identity store change, we recommend that you back up the server.

1. Back up, remove, and then reinstall.
2. Create users, sites, and groups.
3. Inform your users of the new Tableau Server, provide them with credentials, and allow them to republish their content.

Back up, remove, and then reinstall

Both methods include the following steps:

1. Back up Tableau Server
2. Remove Tableau Server.
3. Reinstall Tableau Server with the new identity store type.

Step 1: Back up Tableau Server

As a best practice, you should back up the server before proceeding.

Follow the procedure, Create a backup using the TSM command line interface (CLI). Run the `backup` command with the `-d` option. The `-d` option adds the datestamp.

When you are finished, copy the backup file (.tsbak) to a safe location that is not a part of your Tableau Server installation.

Step 2: Remove Tableau Server

You must completely remove Tableau Server from the computer. See Remove Tableau Server from Your Computer.

Step 3: Reinstall Tableau Server with new authentication type

1. Go to the Tableau Customer Portal, sign in with your Tableau user name and password, and then download Tableau Server.
2. Install Tableau Server. See Install and Configure Tableau Server more information. During installation, you will select the new identity store type. See Configure Initial Node Settings.

LDAP Configuration Reference

This topic provides a description of all LDAP-related configuration options. The option name that you specify is dependent on the tool that you use to configure LDAP:

- **configEntities**: Options are set with a JSON file as described in identityStore Entity. Values that you enter as configEntites are validated before they are saved.

- **tsm CLI**: Options are set with the tsm command line tool as described in tsm user-identity-store. Values that you enter with tsm CLI are validated before they are saved.

- **configKey**: Options are set by running tsm configuration set Options. Alternatively, they may be included in a JSON configuration file as described in Configuration File Example. When you set an option with a configKey, the value that you enter is copied straight to the underlying .yaml configuration file. Tableau Server does not validate the value. For this reason, we recommend using configKeys only when no option exists to set the configuration with configEntites, tsm CLI, or the TSM Web UI.

If you are configuring Tableau Server to use Active Directory, we recommend using the TSM Web UI for installation. The TSM Web UI is optimized to configure Tableau Server for Active Directory with the minimum necessary input. See Configure Initial Node Settings.

Consider using the Tableau Identity Store Configuration Tool to generate your LDAP json configuration file. The Tableau Identity Store Configuration Tool will also generate a list of key/value pairs that you can set by running tsm configuration set Options. The tool itself is not supported by Tableau. However, using a JSON file created by the tool instead of creating a file manually does not change the supported status of your server.

<table>
<thead>
<tr>
<th>configEntities</th>
<th>tsm CLI</th>
<th>configKey</th>
<th>Scenario</th>
<th>Notes</th>
</tr>
</thead>
</table>

Tableau Software

Version: 2019.1

1499
### Options are case sensitive

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>N/A</td>
<td><code>wgserv-er.authenticate</code> Where you want to store user identity information. Values: <code>local</code> or <code>activedirectory</code>. If you want to connect to any LDAP server, enter <code>activedirectory</code>.</td>
</tr>
<tr>
<td>sslPort</td>
<td>N/A</td>
<td><code>wgserv-er.domain.ssl_port</code> Use this option to specify the secure port of the LDAP server. We recommend secure LDAP for simple bind. LDAPS is usually port 636.</td>
</tr>
<tr>
<td>port</td>
<td>N/A</td>
<td><code>wgserv-er.domain.port</code> Use this option to specify the non-secure port of the LDAP server. Plain-text is usually 389.</td>
</tr>
<tr>
<td>domain</td>
<td>domain</td>
<td><code>wgserv-er.domain.default</code> In Windows Active Directory environments, specify the domain where Tableau Server is installed, for example, &quot;example.lan&quot;. In LDAP directories, specify the root domain name in the same format. For example, if your root is &quot;dc=my,dc=root&quot;, specify</td>
</tr>
</tbody>
</table>
If your root does not use a `dc` component, see the root `configEntity` option below.


| username       | ldap-username | wgserv-er.domain.username | A-D, L-D-A-P | The user name that you want to use to connect to the directory service. The account that you specify must have permission to query the directory service. For Active Directory, enter the user name, for example, `j smith`. For LDAP servers, enter the distinguished name (DN) of the user that you want to use to connect. For example, "cn=*


| password       | ldap-password | wgserv-er.domain.password | A-D, L-D-A-P | The password of the user account that you will use to connect to the LDAP server. tsm CLI: Uses `tsm user-identity-store set-connection [options]` command.
<table>
<thead>
<tr>
<th><strong>directoryServiceType</strong></th>
<th>N/A</th>
<th>wgserv-er.-domain.directoryservice.type</th>
<th>A-D, L-D-A-P</th>
<th>The type of LDAP directory service that you want to connect to. Values: active directory or openldap.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>kerberosPrincipal</code></td>
<td>kerbprincipal</td>
<td>wgserv-er.-domain.ldap.principal</td>
<td>A-D, L-D-A-P</td>
<td>The service principal name for Tableau Server on the host machine. The keytab must have permission for this principal. Do not use the existing system keytab at /etc/krb5.keytab. Rather, we recommend that you register a new service principal. To see principals in a given keytab, run the <code>klist -k</code> command. See Understanding Keytab Requirements. tsm CLI: Uses tsm user-identity-store set-connection [options] command.</td>
</tr>
<tr>
<td><code>hostname</code></td>
<td>hostname</td>
<td>wgserv-er.-domain.ldap.hostname</td>
<td>A-D, L-D-A-P</td>
<td>The hostname of the LDAP server. You can enter a hostname or an IP address for this value. The host that you specify here will be used for user/group queries on the primary domain. In the case where user/group queries are in other domains, Tableau Server will query DNS to identify the appropriate domain controller. tsm CLI: Uses tsm user-identity-store set-connection [options] command.</td>
</tr>
<tr>
<td>Option</td>
<td>Default</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mem-retrievalPageSize</td>
<td>N/A</td>
<td>This option determines the maximum number of results returned by an LDAP query.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example, consider a scenario where Tableau Server is importing an LDAP group that contains 50,000 users. Attempting to import such a large number of users in a single operation is not a best practice. When this option is set to 1500, Tableau Server imports the first 1500 users in the first response. After those users are processed, Tableau Server requests the next 1500 users from the LDAP server, and so forth. We recommend that you modify this option only to accommodate the requirements of your LDAP server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>wgserv-domain.ldap.connectionpool.enabled</td>
<td>N/A</td>
<td>When this option is set to true, Tableau Server will attempt to reuse the same connection when sending queries to the LDAP server. This behavior decreases the overhead of having to re-authenticate with the LDAP server on each new request. Connection pooling only works with simple bind and TSL/SSL bind connections. Connection pooling is not supported for GSSAPI bind connections.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
<td>Required Databases</td>
<td>Notes</td>
<td></td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------</td>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>kerberosConfig</td>
<td>The path to the Kerberos configuration file on the local computer. If you are installing into Active Directory, we don't recommend using the existing Kerberos configuration file or keytab file that may already be on the domain-joined computer. See Identity Store tsm CLI: Uses tsm user-identity-store set-connection [options] command.</td>
<td>A-D, L-DA-P</td>
<td></td>
<td></td>
</tr>
<tr>
<td>kerberosKeytab</td>
<td>The path to the Kerberos keytab file on the local computer. It is recommended that you create a keytab file with keys specifically for Tableau Server service and that you do not share the keytab file with other applications on the computer. For example, on Linux, you might place the keytab file in the /var/opt/tableau/keytab directory. tsm CLI: Uses tsm user-identity-store set-connection [options] command.</td>
<td>A-D, L-DA-P</td>
<td></td>
<td></td>
</tr>
<tr>
<td>nickname</td>
<td>The nickname of the domain. This is also referred to as the NetBIOS name in Windows/Active Directory environments. The nickname option is required for all LDAP entities. If your organization does not require a nickname/NetBIOS, then pass a blank key,</td>
<td>A-D</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Setting</td>
<td>Value</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>-------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>N/A</td>
<td>For example: &quot;&quot;. If you do not use a dc component in the LDAP root or you want to specify a more complex root you need to set the LDAP root. Use the &quot;o=my,u=root&quot; format. For example, for the domain, example.lan, the root would be &quot;o=example,u=lan&quot;.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>server-SideSort-ing</td>
<td>N/A</td>
<td>Whether the LDAP server is configured for server-side sorting of query results. If your LDAP server supports server-side sorting, set this option to true. If you are unsure whether your LDAP server supports this, enter false, as misconfiguration may cause errors.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rangeRetrieval</td>
<td>N/A</td>
<td>Whether the LDAP server is configured to return a range of query results for a request. This means that groups with many users will be requested in small sets instead of all at once. LDAP servers that support range retrieval will perform better for large queries. If your LDAP server supports range retrieval, set this option to true. If you are unsure whether your LDAP server supports range retrieval, enter false, as misconfiguration may cause errors.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bind</td>
<td>N/A</td>
<td>The way that you want to secure communication to the directory service. Enter simple for LDAP unless you are</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>connecting to an LDAP server with Ker-</td>
<td>Connecting to an LDAP server with Kerberos. For Kerberos, enter gssapi.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>bers.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>wgserv-er.-domain.ldap.domain_custom_</td>
<td>Allows you to map child domains and their LDAP ports. Domain and port are</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ports</td>
<td>separated by a colon (:) and each domain:port pair is separated by a comma</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(,) using this format: FQDN1:-port,FQDN2:port</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: tsm configuration set -k wgserv-er.domain.ldap.domain_custom_</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dis-tin-guishedNameAttribute</td>
<td>The attribute that stores the distinguished names of users. This attribute</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>is optional, but it greatly improves the performance of LDAP queries.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>groupBaseDn</td>
<td>Use this option to specify an alternative root for groups. For example, if</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>all of your group are stored in the base organization called &quot;groups,&quot; then</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>enter &quot;o=groups&quot;.&quot;</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| N/A | classes-names | wgserv-er.-domain.ldap.group.classnames | By default Tableau Server looks for LDAP group object classes containing the string “group”. If your LDAP group objects do not fit the default class name, override the default by setting this value. You can provide multiple classnames separated by commas.

If your group names include commas, you must escape them with a backslash (\). For example, if you have a group name, groupOfNames, top, then enter "groupOfNames\, top".


| groupBaseFilter | base-filter | wgserv-er.-domain.ldap.group.baseFilter | The filter that you want to use for groups of users of Tableau Server. You might specify an object class attribute and an organization unit attribute. For example:

"(&(objectClass=groupOfNames)(ou=Group))"


| groupName | group-pna- | wgserv- | The attribute that corresponds to group

Tableau Server on Linux Administrator Guide
<table>
<thead>
<tr>
<th>me</th>
<th>er.-domain.ldap.-group.name</th>
<th>D-AP names on your LDAP server. tsm CLI: Uses tsm user-identity-store set-group-mappings [options] command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupEmail</td>
<td>wgserv-ver.-domain.ldap.group.email</td>
<td>L-D-A-P The attribute that corresponds to group email addresses on your LDAP server. tsm CLI: Uses tsm user-identity-store set-group-mappings [options] command.</td>
</tr>
<tr>
<td>groupDescription</td>
<td>wgserv-ver.-domain.ldap.group.description</td>
<td>L-D-A-P The attribute that corresponds to group descriptions on your LDAP server. tsm CLI: Uses tsm user-identity-store set-group-mappings [options] command.</td>
</tr>
<tr>
<td>member</td>
<td>wgserv-ver.-domain.ldap.group.member</td>
<td>L-D-A-P Specify the LDAP attribute that contains a list of distinguished names of users that are part of that group. tsm CLI: Uses tsm user-identity-store set-group-mappings [options] command.</td>
</tr>
<tr>
<td>N/A</td>
<td>wgserv-ver.-domain.ldap.group.memberURL</td>
<td>L-D-A-P Specify the name of the LDAP attribute that stores the LDAP query for dynamic groups.</td>
</tr>
</tbody>
</table>
| user-Basedn | wgserv-ver.- | L-D-A-P Use this option to specify an alternative root for users. For example, if all of
<table>
<thead>
<tr>
<th><strong>domain.ldap.user.baseDn</strong></th>
<th>A-P</th>
<th>your users are stored in the base organization called &quot;users,&quot; then enter &quot;o=users&quot;.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>N/A</strong></td>
<td>clas-sna-mes</td>
<td><strong>By default Tableau Server looks for LDAP user object classes containing the string “user” and “inetOrgPerson”.</strong> If your LDAP user objects do not use these default class names, override the default by setting this value. You can provide multiple classnames separated by commas. For example: &quot;user-class1, userclass2&quot;. If your names include commas, you must escape them with a backslash (). For example, if you have a name, Names, top, then enter &quot;Names, top&quot;. <strong>tsm CLI:</strong> Uses tsm user-identity-store set-user-mappings [options] command.</td>
</tr>
<tr>
<td><strong>user-BaseFilter</strong></td>
<td>base-filter</td>
<td><strong>The filter that you want to use for users of Tableau Server. You might specify an object class attribute and an organization unit attribute.</strong> For example: &quot;(&amp; (objectClass=s=inetOrgPerson) (ou=People))&quot;</td>
</tr>
<tr>
<td>User Field</td>
<td>LDAP Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Username</td>
<td>wgserv-er.-domain.ldap.user.username</td>
<td>The attribute that corresponds to user names on your LDAP server.</td>
</tr>
<tr>
<td>Display Name</td>
<td>wgserv-er.-domain.ldap.user.displayname</td>
<td>The attribute that corresponds to user display names on your LDAP server.</td>
</tr>
<tr>
<td>Email</td>
<td>wgserv-er.-domain.ldap.user.email</td>
<td>The attribute that corresponds to user email addresses on your LDAP server.</td>
</tr>
<tr>
<td>Certificate</td>
<td>wgserv-er.-domain.ldap.user.usercertificate</td>
<td>The attribute that corresponds to user certificates on your LDAP server.</td>
</tr>
<tr>
<td>Thumbnail</td>
<td>wgserv-er.-domain.ldap.user.thumbnail</td>
<td>The attribute that corresponds to user thumbnail images on your LDAP server.</td>
</tr>
</tbody>
</table>
### Tableau Server on Linux Administrator Guide

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>user-JpegPhoto</strong></td>
<td>The attribute that corresponds to user profile images on your LDAP server.</td>
</tr>
<tr>
<td><strong>memberOf</strong></td>
<td>Group that the user is a member of.</td>
</tr>
<tr>
<td><strong>groupClassNames</strong></td>
<td>By default Tableau Server looks for LDAP group object classes containing the string “group”. If your LDAP group objects do not fit the default class name, override the default by setting this value. For configEntity: This option takes a list of strings, which requires passing each class in quotes, separated by a comma (no space) and within brackets. For example: <code>[&quot;basegroup&quot;, &quot;other-group&quot;]</code>. For configKey: Enter each class, separated by a comma (no space) and within double quotes. For example:</td>
</tr>
</tbody>
</table>

---


By default Tableau Server looks for LDAP user object classes containing the string “user” and “inetOrgPerson”. If your LDAP user objects do not use these default class names, override the default by setting this value.

For configEntity: This option takes a list of strings, which requires passing each class in quotes, separated by a comma (no space) and within brackets. For example: ["user-class1",userclass2"].

For configKey: Enter each class, separated by a comma (no space) and within double quotes. For example: "userclass1,userclass2".

Calculated configKeys

The following Kerberos-related configKeys are calculated and set according to multiple environmental inputs. As such, they must be set by CLI or configEntries. Do not attempt to set these configKeys manually.

<table>
<thead>
<tr>
<th>Calculated configKey</th>
<th>To use the TSM CLI:</th>
<th>To use configEntity json:</th>
</tr>
</thead>
<tbody>
<tr>
<td>wgserv-domain.ldap.kerberos.conf, cfs.ldap.kerberos.conf</td>
<td>Set the Kerberos configuration file location with the kerberosConfig option of</td>
<td>Set the Kerberos configuration file location with the kerberosConfig configEntity option.</td>
</tr>
</tbody>
</table>

| wgserver.domain.ldap.kerberos.keytab, cfs.ldap.kerberos.keytab | Set the Kerberos keytab file location with the **kerb-keytab** option of tsm user-identity-store set-connection [options] command. | Set the Kerberos keytab file location with the **kerberosKeytab configEntity** option. |

### Unsupported configKeys

Some unsupported configKeys are present in underlying YAML configuration files. The following keys are not intended for standard deployments. Do not configure these keys:

- `wgserver.domain.ldap.kerberos.login`
- `wgserver.domain.ldap.guid`
- `wgserver.domain.fqdn`