Tanium Client Management User Guide

2026H2 Semiannual Release

Version 2.8

November 19, 2026



The information in this document is subject to change without notice. Further, the information provided in this document is provided "as is" and is believed to be accurate, but is presented without any warranty of any kind, express or implied, except as provided in Tanium's customer sales terms and conditions. Unless so otherwise provided, Tanium assumes no liability whatsoever, and in no event shall Tanium or its suppliers be liable for any indirect, special, consequential, or incidental damages, including without limitation, lost profits or loss or damage to data arising out of the use or inability to use this document, even if Tanium Inc. has been advised of the possibility of such damages.

Any IP addresses used in this document are not intended to be actual addresses. Any examples, command display output, network topology diagrams, and other figures included in this document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Please visit https://help.tanium.com for the most current Tanium product documentation.

This documentation may provide access to or information about content, products (including hardware and software), and servicesprovided by third parties ("Third Party Items"). With respect to such Third Party Items, Tanium Inc. and its affiliates (i) are not responsible for such items, and expressly disclaim all warranties and liability of any kind related to such Third Party Items and (ii) will not be responsible for any loss, costs, or damages incurred due to your access to or use of such Third Party Items unless expressly set forth otherwise in an applicable agreement between you and Tanium.

Further, this documentation does not require or contemplate the use of or combination with Tanium products with any particular Third Party Items and neither Tanium nor its affiliates shall have any responsibility for any infringement of intellectual property rights caused by any such combination. You, and not Tanium, are responsible for determining that any combination of Third Party Items with Tanium products is appropriate and will not cause infringement of any third party intellectual property rights.

Tanium is committed to the highest accessibility standards for our products. To date, Tanium has focused on compliance with U.S.Federal regulations - specifically Section 508 of the Rehabilitation Act of 1998. Tanium has conducted 3rd party accessibility assessments over the course of product development for many years. We certify against the WCAG 2.2 / VPAT 2.5 standards for all major product modules. Tanium performs ongoing reassessments as appropriate, given the scope and type of changes to the UI and product features from release to release. In the most recent testing, the Tanium Console UI achieved supports or partially supports for all applicable WCAG 2.2 criteria. Tanium can make available any VPAT reports on a module-by-module basis as part of a larger solution planning process for any customer or prospect.

As new products and features are continuously delivered, Tanium will conduct testing to identify potential gaps in compliance with accessibility guidelines. Tanium is committed to making commercially reasonable efforts to address any gaps as quickly as is feasible, given the severity of the issue and scope of the changes. Tanium factors these objectives into the ongoing delivery schedule of features and releases with our existing resources.

Tanium welcomes customer input on making solutions accessible based on your Tanium modules and assistive technology requirements. Accessibility requirements are important to the Tanium customer community and we are

©2026 Tanium Inc. All Rights Reserved

committed to prioritizing these compliance efforts as part of our overall product roadmap. Tanium maintains transparency on our progress and milestones and welcomes any further questions or discussion around this work. Contact your sales representative, Tanium Support atsupport@tanium.com, or email accessibility@tanium.com to make further inquiries.

Tanium is a trademark of Tanium, Inc. in the U.S. and other countries. Third-party trademarks mentioned are the property of the irrespective owners.

Kubernetes®, K8s®, and the Kubernetes logo are registered trademarks of The Linux Foundation®.

Android, ChromeOS, and Google are trademarks of Google LLC.

iOS, iPad, iPadOS, iPhone, Mac, and macOS are trademarks of Apple Inc., and registered in the U.S. and other countries and regions.

Patents: https://www.tanium.com/patents

Tanium Open Source Disclosure : https://tanium.github.io/opensource/

© 2026 Tanium Inc. All rights reserved.

Table of contents

Overview 17
- Tanium Client 17
- Tanium Client Management service 18
  - Interoperability with other Tanium products 20

Tanium Client concepts 22
- Registration 22
- Client peering 23
  - Forward and backward leaders 23
  - Forward and backward reflection 24
  - LAN and WAN connections 24
  - Tanium Client version compatibility for peering 25
  - Satellites 26
- File distribution 26
  - File distribution among peers 26
  - Chunk caching 27
- TLS 27
- Client extensions and endpoint tools for Tanium solutions 27

Requirements 29
- Client version and operating system requirements 29
  - Supported Tanium Client versions 31
  - Supported operating systems 32
- Endpoint OS support in Tanium solutions 41
- Hardware requirements 45
- Module and service requirements 47
- Requirements for satellites used for Tanium Client deployment in Client Management 51
  - Operating systems supported for satellites used in Client deployment 51
  - Hardware requirements for satellites used in Client deployment 52
- Tanium Client Management dependencies 53

©2026 Tanium Inc. All Rights Reserved

Core platform dependencies 53
Solution dependencies 53
Tanium recommended installation 54
Import specific solutions 54
Required dependencies 54
Feature-specific dependencies 55
Client extensions and endpoint tools 55
Tanium™ Module Server 56
Compatibility among components in a Tanium release 56
Tanium™ Semiannual Release 2026H2 56
Maintenance releases 57
Upgrade process 57
Upgrading the Tanium Endpoint Configuration Toolset and Tanium Client 58
Endpoint accounts 59
Tanium Client service account 59
Account permissions for Client Management 59
Windows endpoints 60
Non-Windows endpoints 60
Trusted root certificate requirements on Windows endpoints 61
Network connectivity, ports, and firewalls 63
TCP/IP requirements for Tanium Client 63
Connectivity and TCP/IP requirements for Client Management 63
Port requirements for Tanium Client and Client Management 63
Packet inspection 70
Host system security exclusions 71
Security exclusions for Tanium Client 71
Security exclusions for Client Management 74
Internet URL required for Client Management 92
User role requirements for Client Management 93

Installing Client Management 104
Before you begin 104
Import Client Management with default settings 104
Import Client Management with custom settings 105
Manage solution dependencies 106

©2026 Tanium Inc. All Rights Reserved

Verify Client Management version 106
Upgrade Client Management 106
Migrating Client deployments from Client Management versions earlier than 2.1 106
Cloning Client deployments migrated from versions earlier than 2.1 107

Configuring Client Management 109
Install and configure Tanium Endpoint Configuration 109
Manage solution configurations with Tanium Endpoint Configuration 109
Configure the Client Management action group 111
Set up Client Management users 111
Configure the default Server names and Server port for Tanium Client deployments 114
Manage versions of the Tanium Client available for legacy deployments 115
Manage versions of the Tanium Client available in an air-gapped environment 116

Planning Client deployments 118
Assess the environment where you are deploying the Tanium Client 120
Determine deployment methods and pilot the deployment 121
Deploy to an initial set of endpoints 122
Onboard new computers 123
Maintain continuous hygiene 123

Deploying the Tanium Client 125
Deploying using Client Management 125
Plan deployment targeting 126
(Optional) Prepare a satellite for use with automatic deployment 128
Prepare for deployment to Linux, macOS, Solaris, or AIX endpoints 129
Prepare for deployment to Windows endpoints 134
Manage Client deployments 136
(Optional) Create a Client deployment template 137
(Optional) Designate a template as the default 137
(Optional) Download a tanium-init.dat file for alternative deployment 138
Deploy Clients 138
General Client deployment settings 143
Deployment process 149
View the deployment status and endpoint installation logs 150
Reissue a deployment 151
Manage scheduled or recurring deployments 151

©2026 Tanium Inc. All Rights Reserved

Stop or Delete a scheduled or recurring deployment 151
Edit a scheduled or recurring deployment 152
Manage endpoint credentials 152
Add a Windows credential set 153
Add a non-Windows credential set 153
Edit or delete existing credential sets 153
Deploying using an installer or package file 153
Download installation packages for the Tanium Client 154
Deploy to Windows 155
Prepare for installation 156
Install the Tanium Client on Windows using the installation wizard 158
Install the Tanium Client on Windows using the command line 159
Tanium Client command-line installation reference 161
Deploy to macOS 165
Prepare for installation 166
Install the Tanium Client on macOS using the installation wizard 169
Install the Tanium Client on macOS using the command line 171
Deploy to Linux 173
Prepare for installation 174
Tanium Client package files for Linux 175
Install the Tanium Client on Linux using the command line 178
Deploy to Solaris 181
Prepare for installation 182
Install the Tanium Client on Solaris using the command line 184
Perform unattended Tanium Client installation 187
Configure the Tanium Client on Solaris 188
Deploy to AIX 188
Prepare for installation 189
Install the Tanium Client on AIX using the command line 191
Preparing OS images 194
Information about registration and ComputerID (all operating systems) 194
Windows 194
macOS 197
Linux 200
Solaris 203

©2026 Tanium Inc. All Rights Reserved

AIX 206
VDI 209
Using the Microsoft Azure VM extension 215
Requirements for the Tanium Client VM extension 215
Operating system support in Microsoft Azure 215
Network connectivity 216
Installation methods for the Tanium Client VM extension 216
Manually install the extension using the Azure Portal, Azure CLI, or Azure PowerShell 217
Configure an Azure Resource Manager template 217
Configure Azure Policies 219
Resource properties for the Tanium Client VM extension 224
Tanium Client VM extension properties 224
Convert the tanium-init.dat file to base64 227
Convert to base64 To copy into the template or policy JSON 227
Use a parameter in the template or policy JSON to import the file directly 227
Troubleshooting the Tanium Client VM extension 228
Verify the Tanium Client installation 228

Connecting to the Tanium Core Platform 230
Settings for connections to Tanium Core Platform Servers 230
ServerNameList 230
ServerName 231
LastGoodServerName 232
ServerPort 232
Content for configuring connections to Tanium Core Platform Servers 233
Configure Clients to connect with multiple Tanium Servers 234
Connect through an HTTPS forward proxy server 238
Before you begin 240
Configure proxy connections during Client deployment 241
Configure specific proxy servers during Client deployment 241
Configure proxy connections during Client deployment with a PAC file (Windows endpoints only) 242
Configure automatic proxy detection during Client deployment (Windows endpoints only) 243
Configure proxy connections after Client deployment 244

©2026 Tanium Inc. All Rights Reserved

Configuring peering 247
Overview of Tanium Client peering settings 247
Address mask and prefix settings 250
Configure separated subnets 252
Configure separated subnets that are the same for Tanium Servers and Zone Servers 253
Add subnets 253
Edit subnets 254
Configure separated subnets that are specific to Zone Servers 254
Windows infrastructure 254
Tanium Appliance infrastructure 255
Configure isolated subnets 255
Configure isolated subnets that are the same for Tanium Servers and Zone Servers 257
Add subnets 257
Edit subnets 257
Configure isolated subnets that are specific to Zone Servers 258
Isolate all Clients connected to any Zone Server 258
Isolate all Clients connected to a particular Zone Server 258
Isolate Clients on specific subnets with Windows infrastructure 259
Isolate Clients on specific subnets with Tanium Appliance infrastructure 259
Configure intentional subnets 260
Overview of intentional subnets 260
Before you begin 261
Define intentional subnets using Sites 263
Add subnets 263
Edit subnets 264
Define intentional subnets using the PeerNeighborhood Client setting 264
Verify intentional subnets 264
Verify or remediate Tanium Client peering and leader connections 264
View the status of Tanium Client registration and communication 265
Client Status columns and connection states 266
Export Tanium Client status details 270
Copy Tanium Client status details 270
Deploy actions to remediate Client registration or connectivity issues 271
Use questions to review peering settings 271
Examine the Tanium Client configuration 272

©2026 Tanium Inc. All Rights Reserved

Customize listening ports 274
Configure a custom listening port 275
Randomize listening ports 275

Monitoring, managing, and maintaining Tanium Clients 278
Monitoring Tanium Clients 278
View the status of Tanium Client registration and communication 279
Client Status columns and connection states 279
Export Tanium Client status details 283
Copy Tanium Client status details 284
Monitor the Client health overview in Client Management 284
Access detailed Client health and troubleshooting information on an endpoint 287
Managing Tanium Clients 288
Use built-in saved questions, sensors, and packages 289
(Non-Windows only) Manage custom tags in the CustomTags.txt file 291
Add tags to the CustomTags.txt file 291
Example: Use custom tags to create a computer group 292
Manage the client on Windows 293
Manage the Tanium Client service on Windows 293
Manage tamper protection 294
Configure the anti-tamper recovery password 297
Redeploy settings configurations to update the anti-tamper recovery password on endpoints 298
Disable the anti-tamper feature on an offline endpoint 298
Determine whether anti-tamper is enabled on endpoints 299
Manage Client Service Hardening features 300
Install the Client Service Hardening content pack 300
Access the Client Service Hardening dashboards 301
Limit permission to start and stop Tanium Client services to the SYSTEM account 301
Limit permission to view or modify files in the Tanium Client directory to the SYSTEM account 301
Hide the Tanium Client from the Windows Add/Remove Programs list 302
Unharden the Tanium Client on Windows 302
Use Packages to unharden the Tanium Client 302
Unharden Tanium Client that is not reporting to the Tanium Server 303
Encrypt the Client state and sensor queries stored on the Client 304

©2026 Tanium Inc. All Rights Reserved

Manage the client on macOS 305
Manage macOS firewall rules 305
Manage pop-ups for Tanium Client upgrades 306
Configure an MDM policy or profile for multiple endpoints 307
Configure a firewall rule on a single endpoint 307
Configure the System Settings on a single endpoint 307
Manage the Tanium Client service on macOS 308
Manage the client on Linux 308
Manage Linux firewall rules 308
Amazon Linux 309
Debian 309
CentOS, AlmaLinux, Rocky Linux, Oracle Linux, Red Hat Linux 309
Version 7.x or later 309
Versions 5.x and 6.x 310
OpenSUSE and SLES 311
Version 15.x 311
Version 11.x and 12.X 312
Ubuntu 313
Manage the Tanium Client service on Linux 313
Move an existing installation of the Tanium Client on Linux 314
Manage the client on Solaris 315
Manage the Tanium Client service on Solaris 315
Move an existing installation of the Tanium Client on Solaris 316
Manage the client on AIX 316
Manage the Tanium Client service on AIX 317
Move an existing installation of the Tanium Client on AIX 317
Managing Client settings and Index configurations 318
Review Client settings 318
Client Health view 318
Summary view 319
Detail view 319
Tanium Client Explicit Setting Sensor 319
Command line interface (CLI) 320
Modify Client settings 320
Settings configurations in Client Management 320

©2026 Tanium Inc. All Rights Reserved

Packages ... 320
Command line interface (CLI) ... 323
Deployment with Client Management ... 323
Modify default Client settings in Tanium Console ... 323
Managing Client settings in Client Management ... 324
Create and deploy a Client settings configuration ... 324
Prioritize Client settings configurations ... 327
Managing Index configurations in Client Management ... 327
Create Index exclusions ... 328
(Optional) Import or export Index exclusions ... 329
Export Index exclusions ... 329
Import Index exclusions ... 329
Create an Index configuration ... 329
Prioritize Index configurations ... 331
Maintaining Tanium Clients ... 331
Configure automated maintenance ... 332
Audit and remediate disconnected Tanium Clients ... 332
Perform weekly maintenance ... 333
Check the endpoint leader percentage ... 333
Check the endpoint count ... 334
Review and update tags ... 335
Review and update enhanced tags ... 335
Review and update custom tags ... 335
Perform monthly maintenance ... 335
Review and remediate Tanium Client health and Client Extension issues ... 336
Review and adjust the distribution of Tanium Client registration traffic ... 336
Review and update Tanium Client logging levels ... 337
Review and update Tanium Client settings ... 338
Review and upgrade Tanium Client versions ... 339
Review and update Tanium Client subnets ... 340
Review and update isolated subnets ... 340
Review and update separated subnets ... 341
Review and update intentional subnets ... 341
Upgrading Tanium Clients ... 342
Best practices ... 343

©2026 Tanium Inc. All Rights Reserved

Before you begin 345
Assess the impact of upgrading on your environment 346
Enable Tanium Client upgrades in change management 346
Upgrade Tanium Clients using Client Management 346
Create a Client upgrade 347
Upgrade Tanium Clients using a package 349
Verify the upgrade 349
Disable the legacy Tanium Protocol used only for 7.2 and earlier clients 350
Uninstalling Tanium Clients 351
Uninstall the Tanium Client on Windows 351
Use a Tanium package to deploy an uninstallation program 351
Use Add/Remove Programs 352
Uninstallation program 352
Uninstall the Tanium Client on macOS 352
Uninstall without using a script 352
Uninstall using a script 353
Uninstall the Tanium Client on Linux 354
Uninstall the Tanium Client on Solaris 355
Uninstall the Tanium Client on AIX 355

Troubleshooting 356
Basic tips 356
Review the Tanium Client installation log to troubleshoot installation on Windows 357
Troubleshoot issues with connection and registration 357
Check the Client status 358
Perform a test registration of the Tanium Client from the endpoint 358
Verify that the Tanium Client service and process are running on an endpoint 359
Verify port accessibility and security exclusions 360
Verify server connection settings 360
Test DNS resolution 361
Test network connectivity and port accessibility 361
Collect troubleshooting information from endpoints 362
Access individual endpoint logs in Client Management 363
Review Tanium Client logs to troubleshoot connections and other Client issues 364
Network Configuration errors reported in the log 365

©2026 Tanium Inc. All Rights Reserved

Cache-related errors reported in the log 365
Logging levels 365
Review action logs and associated files to troubleshoot actions and packages 366
Action_<ID> directories 367
Access action logs in Client Management 367
Action log contents 368
Action log and package cleanup 369
Review action history logs to troubleshoot or audit actions 369
Review sensor history logs to troubleshoot or audit sensor activity 370
Create a custom log for a Tanium Client 371
CLI command options for custom logs 372
Review or reset the public key to troubleshoot connection issues 373
Review and manage sensor quarantines to troubleshoot sensors 377
Overview of sensor quarantines 377
View quarantined sensors 379
Remove all sensors from quarantine 379
Remove a single sensor from quarantine 380
Enable or disable enforcement of quarantined sensors 380
Identify and resolve issues with Client Extensions 381
Review the Extensions log for an endpoint 384
Remove Client Management tools from endpoints 385
Troubleshoot Client Management 387
Collect logs 387
View and configure logs 387
Adjust log level 387
Adjust log retention 387
View Client deployment logs 387
Troubleshoot deployment issues 388
Issue: Endpoint Installation Status = ERROR_CONNECTION_FAIL with SSH connection log message 389
Issue: Endpoint Installation Status = ERROR_INSTALL_FAIL with certificate log message 390
Issue: Satellite-based deployment fails with satellite connection log message 390
Uninstall Client Management 391
Get support for the Tanium Client 391

©2026 Tanium Inc. All Rights Reserved

Contact Tanium Support 392

Reference: Client settings and CLI 393
Tanium Client settings reference 393
Tuning Tanium Client settings for VDI endpoints and other endpoints with limited resources 407
Peering settings reference 411
Tanium Client command line interface (CLI) 413
CLI on Windows endpoints 413
Example 1: Set and confirm Server names 413
Example 2: Set and confirm log verbosity level 413
Example 3: Require TLS 414
CLI on non-Windows endpoints 414

Reference: Endpoint security exclusions 416
Tanium Client folders 417
Tanium Client system processes 417
Tanium binary file signers 419
Solution-specific exclusions 420
Asset endpoint exclusions 420
Benchmark endpoint exclusions 423
Certificate Manager endpoint exclusions 423
Client Management endpoint exclusions 425
Client Management server exclusions 437
Comply endpoint exclusions 439
Deploy endpoint exclusions 441
Direct Connect endpoint exclusions 447
Discover endpoint exclusions 448
End-User Notifications endpoint exclusions 451
Enforce endpoint exclusions 452
Engage endpoint exclusions 455
Impact endpoint exclusions 455
Integrity Monitor endpoint exclusions 456
Investigate endpoint exclusions 461
Patch endpoint exclusions 463
Performance endpoint exclusions 467
Provision endpoint exclusions 471

©2026 Tanium Inc. All Rights Reserved

Reveal endpoint exclusions 472
Screen Sharing endpoint exclusions 474
Threat Response endpoint exclusions 475
Solutions that require no additional security exclusions 484

Reference: Client extensions and endpoint tools used for Tanium solutions 486

Reference: Default installation directory for the Tanium Client 490

Reference: Registry key paths for the Tanium Client 491

Reference: Commands used during deployment with Client Management 492

Tanium Client Export Commodity Classification 493

©2026 Tanium Inc. All Rights Reserved

Tanium Client Overview

The Tanium™ Client is a service installed on endpoint computers that discovers and reports data from those endpoints. Deploy the Tanium Client using the Tanium Client Management shared service, an installation wizard (Windows and macOS endpoints only), or the Client command-line interface. You can monitor Client health using Client Management.

Note: If you plan to deploy the Tanium Client using third-party software distribution tools, this guide provides useful information but does not describe tool-specific procedures. Some tools that you can use are System Center Configuration Manager (SCCM), Altiris, LANDESK, Puppet, and Casper. For more information about using a third-party tool with Tanium installers, see the documentation for that tool.

For an illustrated example of a Tanium Client deployment, see Network connectivity, ports, and firewalls on page 63.

Tanium Client

In response to your questions in Tanium™ Interact, the Tanium Client discovers both static and dynamic real-time data pertaining to the endpoint and reports within seconds. This data can include the following information:

- Hardware and software inventory
- Software configuration
- Local or domain user details
- Installed applications or services, startup programs, and running processes
- Existence of Windows registry keys and values
- Windows Management Instrumentation (WMI) data elements

©2026 Tanium Inc. All Rights Reserved

- File system details, including identification of files by hash or contents
- Event log results
- Network configuration settings and state

With similar speed, you can use the Tanium Client to execute commands, actions, scripts, or other executable programs, as if an authorized administrator were taking actions from the command line on the target endpoint. For example, you can send the Tanium Client an instruction to take the following actions:

- Install or uninstall applications or services
- Update or patch installed applications, services, hardware drivers, or firmware
- Manage installed applications or services
- Add, remove, or modify the Windows Registry settings or other configuration stores
- Add, remove, or modify files or the contents of files
- Start or stop services

These powerful features enable large, geographically distributed organizations to identify and respond to a zero-day exploit, security breach, or application outage in seconds or minutes rather than days and weeks.

For information about how the Tanium Client registers with the Tanium™ Server or Tanium™ Zone Server, peers with other Tanium Clients, and distributes files, see Tanium Client concepts on page 22.

Tanium Client Management service

The Tanium Client Management service provides tools to help deploy and manage the Tanium Client in your environment. With Client Management, you can rapidly deploy the Tanium Client to targeted sets of endpoints, and you can upgrade or reinstall existing Clients as needed. You can also continuously monitor the health of all installed Clients to help quickly identify, diagnose, and resolve issues with Clients.

©2026 Tanium Inc. All Rights Reserved

Client deployment

Deploy the Tanium Client on page 125 to targeted sets of Windows, Linux, macOS, Solaris, or AIX endpoints.

Before you begin the deployment process, determine the set of endpoints that you are going to target on page 118. You can target by single IP, computer name, IP or CIDR range, or label that you define in Tanium™ Discover.

Create a Client deployment in Client Management with the desired settings and targets, and the credentials needed for the targeted endpoints. You can also create Client deployment templates to easily create multiple deployments with similar settings. When you run the deployment, the Tanium Module Server installs the Tanium Client on the targeted endpoints.

If there are endpoints where you want to deploy the Tanium Client manually, you can configure a Client deployment template, and then download a tanium-init.dat file on page 138 for use in manual deployment.

Client health monitoring

After Clients are installed, you can use Client Management to continuously monitor Client health on page 278. Quickly identify outliers and issues by viewing aggregated information for Clients on supported operating systems. Diagnose specific issues with Windows, Linux, and macOS Clients by directly connecting and exploring individualized Client health information.

Client settings management

Use the Client Management service to create Client settings configurations on page 324 that apply Client settings (such as logging level and cache size) to different groups of Clients.

Client upgrade

Client Management handles upgrades to the Tanium Client on endpoints that have earlier versions installed. A Client upgrade targets specific computer groups and upgrades any endpoints in those groups to the specified version as the endpoints become available. You can create a one-time upgrade to upgrade Clients within a specified window of time, or you can create an ongoing upgrade to keep Clients upgraded to the latest version of the Tanium Client or to upgrade Clients that are later added to the targeted group to a selected version.

©2026 Tanium Inc. All Rights Reserved

Best Practice: Enable Client upgrades in the change management feature in Endpoint Configuration to streamline Client upgrades and to more easily maintain a supported configuration. This feature upgrades the Tanium Client to a supported version each time it upgrades the endpoint toolset on an endpoint. For more information, see Endpoint Configuration: Managing Tanium Client and endpoint tool upgrade rollouts.

Interoperability with other Tanium products

Tanium™ Discover

You can apply labels to the unmanaged interfaces that are identified with Discover and then target endpoints using those labels on page 125. You can also configure a deployment to re-run automatically when a selected Discover label is updated.

Tanium™ Index

You can manage Index exclusions and blockout windows on page 327 in Client Management.

Tanium™ Trends

Client Management features Trends boards that provide data visualization of Client Management concepts, including successful and failed deployments, and the versions of the Tanium Client that were deployed. The following panels are in the Tanium Client Management board:

- Tanium Client versions deployed
- Tanium Client versions deployed - latest
- Successful installations
- Deployment failures

Note: The **Successful installations** and **Deployment failures** panels apply only to deployments using Client Management.

For more information about how to import the Trends boards that Client Management provides, see

©2026 Tanium Inc. All Rights Reserved

Importing the initial gallery.

©2026 Tanium Inc. All Rights Reserved

Tanium Client concepts

Registration

When you first deploy the Tanium Client to an endpoint, the Client initiates a connection to the Tanium Server or Tanium Zone Server that is assigned to it in the initial configuration. During *initial registration*, the Tanium Client establishes a unique ID, and the Server sends it the latest Client settings, a list of nearby peers, and the latest definitions for sensors, questions, and scheduled actions. Typically, the initial registration status is configured to reset at randomized intervals of two to six hours, forcing the Tanium Client to re-initialize registration. Repeating the initial registration ensures that the Server applies the latest settings and the Clients select optimal peers.

The Tanium Client also re-registers with the Server through a *normal registration*, which occurs at a randomized interval every few minutes. During a normal registration, the Tanium Client reports its current state of questions, actions, and settings to the Server. In response, the Server sends new questions, actions, or settings to apply. In environments with numerous endpoints, normal registrations are the primary way that Tanium Clients receive new questions, actions, and settings.

Note: In order to register with the Tanium Server, the Tanium Client must have been initialized with the tanium-init.dat file for the Tanium environment.

Important:

Be careful not to allow the tanium-init.dat file to be distributed or stored outside of your organization, such as in a publicly accessible source code repository or any other location accessible from the public internet. Limit the distribution to specific use in the deployment of Tanium Clients.

Though this file does not contain private keys and cannot be used to provide control over a Tanium environment, a user with malicious intent could use it to connect an unapproved Client and use this unauthorized access to learn how your organization is using Tanium.

©2026 Tanium Inc. All Rights Reserved

Client peering

In an enterprise network, Tanium Clients establish peer relationships with each other in a *linear chain*. Peer connections are continuous, long-lived connections that the Clients use to exchange Tanium messages and files. During registration, the Server sends the Tanium Client a *peer list* of other Tanium Clients with which it can try to establish a peer connection. The Tanium Client uses the list to determine which peers are the most optimal neighbors within the linear chain.

Tip: To customize Client peering settings to suit your deployment, see Configuring Tanium Client peering on page 247.

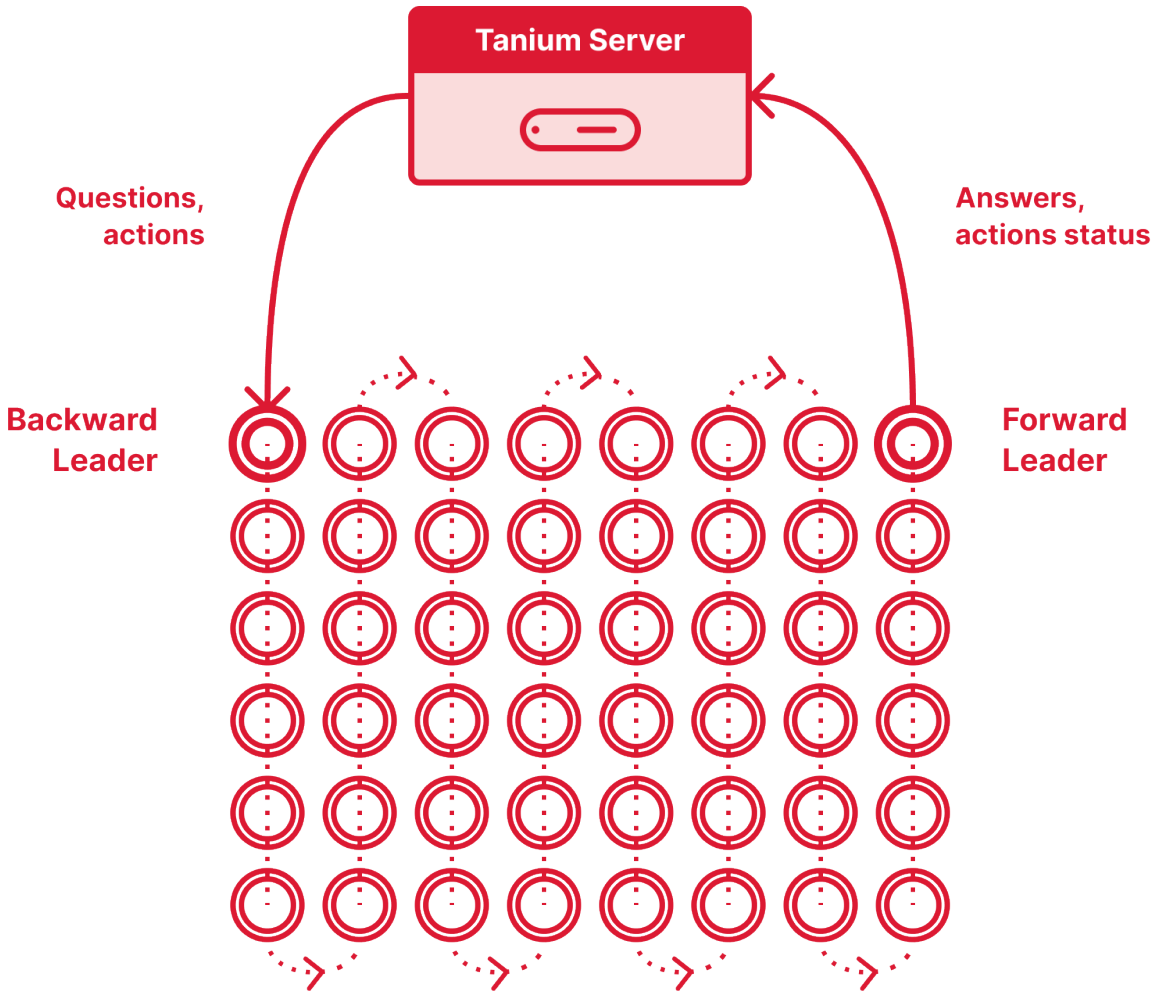
Forward and backward leaders

By design, one *forward leader* and one *backward leader* terminate opposite ends of the linear chain. Other than at registration, only leaders establish direct connections with the Tanium Server or Zone Server. The Server passes questions and scheduled actions to the backward leader, which passes them to its forward peer, which in turn passes them to its forward peer, and so on, until they reach the forward leader. The forward leader returns the question answers and the scheduled action statuses to the Server.

Note: Tanium Clients establish outgoing connections to backward peers for file distribution (see File distribution on page 26).

Figure 1. Tanium Client linear chain

©2026 Tanium Inc. All Rights Reserved



Forward and backward reflection

Tanium peer communication is designed to accommodate new Clients that come online, to route around Clients that are removed or stop communicating effectively, and to *reflect* around network-level blockages, such as firewall blocking. *Forward reflection* occurs if a Tanium Client cannot establish an outgoing connection to a forward peer in its peer list: the Client establishes its forward connection to the Server instead and becomes a forward leader. Similarly, *backward reflection* occurs if a Tanium Client cannot establish an outgoing connection to a backward peer: the Client establishes a backward connection to the Server and becomes a backward leader.

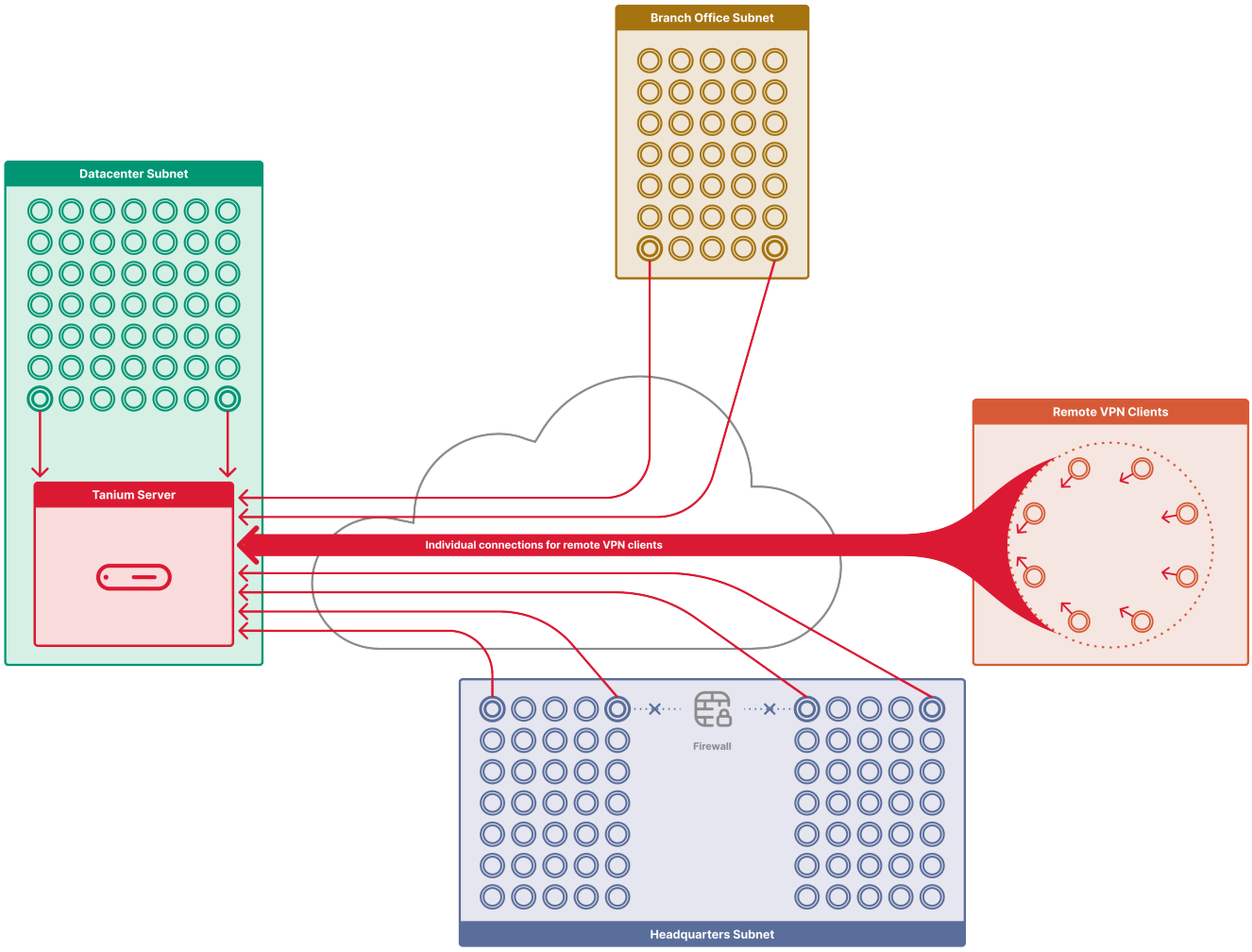
LAN and WAN connections

Client peering results in a profound reduction in connections and bandwidth over WAN links. The following figure illustrates the proportions of the savings in a large enterprise network that has

©2026 Tanium Inc. All Rights Reserved

subnets in a data center, headquarters, and branch office, as well as VPN connections from remote workers. Other than during registration, only the remote VPN clients and leaders, depicted in bright red, connect to the Server over the WAN (the internet, in this example). The remaining Clients, depicted in darker red, share data over peer connections on the LAN for each subnet.

Figure 2. Client peering in an enterprise network



Tanium Client version compatibility for peering

Tanium Clients peer only with other Clients that share the same minor version (the second component of the version number). For example, a Tanium Client running version 7.b.x peers with other 7.b.x Clients, but not with 7.a.x or 7.c.x Clients.

This version boundary means that while upgrading Clients in stages, endpoints on different minor versions cannot peer with one another. As a result, the proportion of endpoints that become forward or backward leaders can temporarily increase, leading to more direct connections to the Tanium Server and higher WAN bandwidth consumption.

©2026 Tanium Inc. All Rights Reserved

Best Practice:

To reduce peering disruption during upgrades, plan to complete upgrades quickly within each subnet, and avoid leaving mixed minor versions in the same subnet for an extended period. For upgrade planning guidance, see Best practices on page 343.

Satellites

Satellites are Tanium Clients that you designate to run secure workloads on endpoints that the Tanium Module ServerTanium Cloud cannot directly reach. Satellites enable Tanium solutions to perform operations on those endpoints, such as non-line-of-sight scans for Tanium Discover or remote authenticated scans for Tanium Comply.

The Module Server might need to send sensitive, encrypted data (such as credentials) to a satellite when running a workload. Therefore, you must verify each Tanium Client that you designate as a satellite to prevent spoofing attacks. The Server never sends such sensitive data through the Client linear chain and the satellite does not store that data on disk.

Designating and using satellites requires Direct Connect version 2.1 or later.

For more information about managing satellites, see Managing satellites.

File distribution

The Tanium Server distributes files (through a Zone Server, if one is deployed) to managed endpoints when you deploy actions that use those files. For example, if you deploy an action to upgrade Windows, the Tanium Server distributes a package that includes the Windows patch file. Tanium Clients running on the endpoints optimize the file distribution process through peering and caching.

File distribution among peers

Peering reduces the number of files that the Tanium Server distributes over WAN links. Instead of sending files to all managed endpoints, the Tanium Server sends files only to the backward leader of each linear chain. Each backward leader then relays the files over a high-speed LAN connection from one forward peer to another until they reach the forward leader.

©2026 Tanium Inc. All Rights Reserved

Chunk caching

Caching enables Clients to redistribute files in multiple small pieces known as *chunks*. Each Client maintains a local cache of the file chunks that the Tanium Server previously distributed to the linear chain. When the same files are requested later (for example, when an action runs again), Clients can use the cached chunks, instead of requesting that the Tanium Server redistribute the files again.

TLS

Tanium Core Platform uses Transport Layer Security (TLS) for encrypted communication in connections from Tanium Clients to the Tanium Server or Zone Server by default. For more information, see the Securing Tanium Server, Zone Server, and Tanium Client access or Securing Tanium Server, Zone Server, and Tanium Client access.

Client extensions and endpoint tools for Tanium solutions

In addition to the Tanium Client binary, Tanium installs Client Extensions and other tools on endpoints to perform tasks that are common to certain Tanium solutions. Endpoint Configuration installs these tools as they are needed by those solutions. For information about managing installed endpoint tools, see Managing endpoint tools.

Tools are bundled together in a versioned toolset that contains a specific version of each tool. The Endpoint Configuration Toolset Solution provides upgrades to the toolset, and it imports upgraded versions of the entire toolset as available. You can use the change management feature of Endpoint Configuration to perform a staged rollout of each toolset that accommodates the software upgrade strategy for your organization. For more information, see Managing endpoint tool upgrade rollouts.

Each Client Extension and tool has required security exclusions to allow the Tanium processes to run without interference. For more information, see Reference: Endpoint security exclusions on page 416 and for Windows-based Tanium Core Platform deployments, Tanium Core Platform Server security exclusions, or the requirements section of each solution user guide in the Tanium Resource Center.

Client extensions can run in separate processes, or together in a single process, depending on whether *Client Extension shared process mode* is enabled. For more information, see Manage Client Extension shared process mode.

The Tanium Client applies a CPU throttle (5% of total CPU capacity) to limit the aggregate CPU usage

©2026 Tanium Inc. All Rights Reserved

of all Client Extensions on an endpoint, regardless of whether Client Extension shared process mode is enabled. When a single extension is active, it can use up to the full 5% allocation; when multiple extensions are active simultaneously, they share the available CPU within that limit. Long-running work such as indexing might run faster when no other extensions are competing for CPU.

Note:

- After a Client Extension restart, the Client allows approximately 30 seconds before applying the throttle. Brief CPU peaks during this window are expected and allowed.
- The Client Recorder Extension is exempt from the CPU throttle to ensure reliable event recording. For more information, see Client Recorder Extension requirements.

The Tanium Client uses code signatures to verify the integrity of each Client Extension prior to loading the extension on the endpoint.

To troubleshoot issues with endpoint tools, see Identify and resolve issues with endpoint tools or Client Extensions.

For a list of Client Extensions and endpoint tools used for each solution, see Reference: Client extensions and endpoint tools used for Tanium solutions on page 486.

©2026 Tanium Inc. All Rights Reserved

Tanium Client and Client Management requirements

Review the requirements before deploying the Tanium Client to endpoints. Additionally, review the specific requirements for the Tanium Client Management shared service before installing it and using it to deploy Clients, monitor Client health, manage Client settings, or upgrade Clients.

Client version and operating system requirements

The Supported operating systems on page 32 table lists the supported operating systems on endpoint host systems where you install the Tanium Client.

Hardware resource requirements vary based on the actions that you deploy to the endpoints. For baseline RAM and disk space requirements, see Hardware requirements on page 45.

Some Tanium modules and shared services have additional requirements for the Tanium Client and endpoint hosts. The Solution-specific requirements for the Tanium Client and endpoints on page 47 table provides links to the user guide sections that list these requirements.

©2026 Tanium Inc. All Rights Reserved

Best Practice:

- Each version of the endpoint toolset that is deployed through Endpoint Configuration includes a specific version of the Tanium Client, which Tanium recommends that you install with the toolset. It is a best practice to upgrade the Tanium Client on endpoints using the change management feature. To do so, you must enable Tanium Client upgrades in the upgrade ring configuration. For more information about the endpoint toolset and managing Tanium Client upgrades with toolset deployment, see Tanium Endpoint Configuration User Guide: Managing Tanium Client and endpoint tool upgrade rollouts. If you do not enable this setting, you can upgrade to the required version of the Tanium Client on endpoints using Client Management or other means. For more information, see Upgrading Tanium Clients on page 342.

- Do not install the Tanium Client on the same host as a Tanium Core Platform Server. Managing Tanium Core Platform Servers as endpoints requires significantly more complex access restrictions in Tanium. Tanium users with management rights over Tanium Core Platform Servers might be able to circumvent access restrictions within Tanium or inadvertently deploy actions that interfere with Tanium functionality. If you choose to install the Client on Tanium Core Platform Server machines, you must carefully restrict access to computer groups that include Tanium Core Platform Servers, such as `All Computers`, `All Servers`, and `All Windows`. You cannot use Tanium Client Management to install the Client on the Tanium Module Server.

©2026 Tanium Inc. All Rights Reserved

Important:

- Client Management supports upgrading version 7.2 Tanium Clients on any OS where a later version of Tanium Client is supported. However, you cannot upgrade Tanium Client 7.2 directly to version 7.6 or later. To upgrade an endpoint with version 7.2 installed to version 7.6 or later, you must either perform a reinstallation of the Tanium Client that includes wiping Client data on page 138, or perform an intermediate upgrade on page 342 to version 7.4, after which you can upgrade to the latest version. Perform this upgrade before upgrading Tanium Core Platform to the 2025H1 or later semiannual release.
- Tanium Core Platform servers are backward-compatible with earlier versions of Tanium Clients; any of the listed Tanium Client versions can connect to the latest maintenance release of Tanium Core Platform 7.9.3. However, you cannot connect a Tanium Client with a later version to a Tanium Server or Zone Server with an earlier version. For example, if you are running Tanium Core Platform 7.9.3.1234, you cannot install a Tanium Client version later than 7.9.3.1234 on endpoints. If a later Tanium Client version becomes available, you cannot upgrade the Tanium Client on endpoints to that later version before you upgrade Tanium Core Platform.

Note:

You cannot install the Tanium Client on a Tanium Appliance.

Supported Tanium Client versions

The following versions of Tanium Client are supported with the 2026H2 semiannual release. Certain operating systems require a specific minimum version. For information about each supported operating system, see Supported operating systems on page 32.

©2026 Tanium Inc. All Rights Reserved

The following versions of the Tanium Client can connect to Tanium Core Platform and are receiving maintenance updates:

- 7.9.3
- 7.8.4
- 7.8.2
- 7.7.3

Supported operating systems

The following tables list supported operating systems and versions for endpoints connected to an on-premises Tanium installation:

- Table 1. Supported Windows versions for Tanium Client hosts on page 33
- Table 2. Supported macOS versions for Tanium Client hosts on page 34
- Table 3. Supported Linux distributions and versions for Tanium Client hosts on page 36
- Table 4. Supported AIX versions for Tanium Client hosts on page 41
- Table 5. Supported Solaris versions for Tanium Client hosts on page 41

Certain OS versions have a subset of supported Tanium Client versions, which is indicated in the notes where applicable. For a full list of supported Tanium Client versions, see Supported Tanium Client versions on page 31. The Client Management service supports all listed OS versions.

©2026 Tanium Inc. All Rights Reserved

Tip: You can manage some devices that do not support the Tanium Client, such as iPhones, iPads, and operational technology (OT) devices, using Tanium Endpoint Management for Mobile and Tanium Endpoint Management for Operational Technology.

Supported Windows versions for Tanium Client hosts

OS Version	Available Executables	Notes
Windows Server 2025 Windows Server 2022 Windows Server 2019 Windows Server 2016 Windows Server 2012, 2012 R2 Windows Server	x86	• Standard, Enterprise, and Datacenter editions are supported, with or without the Server Core option enabled. The Nano Server option is not supported. • Updates to certain Windows features or additional configuration might be necessary on some Windows endpoints. For more information, see Prepare for deployment to Windows endpoints on page 134 (for deployment with Client Management) or Prepare for installation on page 156 (for deployment using the installer). • Windows endpoints require certain trusted root certificates to be installed to verify the integrity of the Tanium Client binaries. Windows Update installs the required certificates by default as part of the Microsoft Root Certificate Program, but you might have to install specific certificates on endpoints that are in an air-gapped environment or that are otherwise blocked from regularly updating trusted certificates. For more information, including the specific required certificates, see Trusted root certificate requirements on Windows endpoints on page 61.

©2026 Tanium Inc. All Rights Reserved

OS Version	Available Executables	Notes
2008 R2		
Windows 11 Windows 10 Windows 8 Windows 7 (SP1)	x86	• All editions of the listed Windows versions are supported. • Tanium Client supports running the x86 binary on Windows 11 endpoints with Arm processors. Windows RT is not supported. Some solutions have specific limitations for Windows 11 endpoints with Arm processors. For more information, see the and for each solution. • Updates to certain Windows features or additional configuration might be necessary on some Windows endpoints. For more information, see Prepare for deployment to Windows endpoints on page 134 (for deployment with Client Management) or Prepare for installation on page 156 (for deployment using the installer). • Windows endpoints require certain trusted root certificates to be installed to verify the integrity of the Tanium Client binaries. Windows Update installs the required certificates by default as part of the Microsoft Root Certificate Program, but you might have to install specific certificates on endpoints that are in an air-gapped environment or that are otherwise blocked from regularly updating trusted certificates. For more information, including the specific required certificates, see Trusted root certificate requirements on Windows endpoints on page 61.

Supported macOS versions for Tanium Client hosts

OS Version	Available Executables	Notes
macOS 27 Golden Gate macOS 26 Tahoe	Universal x86-64	• Tanium recommends the universal binary on all Mac computers running macOS 11 or later, and replacing the x86-64 binary if it is already installed. The universal binary is supported and runs natively on both Intel-based Mac computers running macOS 11 or later and Apple "M" series-based Mac computers. However, you cannot upgrade an existing installation of the x86-64 version of the Tanium Client directly to the Universal version. You must first uninstall the existing Tanium Client on page 352 or perform a reinstallation that includes wiping data with Tanium Client Management on page 138. If you upgrade the x86-64 Client in Client Management on page 346 or allow the change management feature in Endpoint Configuration to upgrade the Client, it installs a newer version of the x86-64 Client.

©2026 Tanium Inc. All Rights Reserved

OS Version	Available Executables	Notes
macOS 15 Sequoia macOS 14 Sonoma macOS 13 Ventura macOS 12 Monterey macOS 11 Big Sur		• If you are using any solutions that use the Tanium™ Client Recorder Extension, you must install the universal binary for full functionality of the extension. • For full support of Tanium Client, you must perform additional configuration in your macOS mobile device management (MDM) solution. For more information, see Prepare for deployment to Linux, macOS, Solaris, or AIX endpoints on page 129 (for deployment with Client Management) or Prepare for installation on page 166 (for deployment using the installer). • The Tanium Core Platform requires Tanium™ Default Content 7.1.7 or later to manage endpoints that run macOS 10.14 Mojave or later.
macOS 10.15 Catalina macOS 10.14 Mojave macOS	x86-64	• (macOS 10.14 or later) For full support of Tanium Client, you must perform additional configuration in your macOS mobile device management (MDM) solution. For more information, see Prepare for deployment to Linux, macOS, Solaris, or AIX endpoints on page 129 (for deployment with Client Management) or Prepare for installation on page 166 (for deployment using the installer). • (macOS 10.14 or later) The Tanium Core Platform requires Tanium™ Default Content 7.1.7 or later to manage endpoints that run macOS 10.14 Mojave or later.

©2026 Tanium Inc. All Rights Reserved

OS Version	Available Executables	Notes
10.13 High Sierra		

Supported Linux distributions and versions for Tanium Client hosts

OS Version	Available Executables	Notes
Amazon Linux 2023	x86-64 ARM64	• Support for ARM64 architecture for each solution requires a specific minimum version of that solution. For more information, see .
Amazon Linux 2 LTS	x86-64 ARM64	• Support for ARM64 architecture for each solution requires a specific minimum version of that solution. For more information, see .
Amazon Linux 1 AMI (2018.03)	x86-64	
Debian 13.x	x86-64 ARM64	• Minimum Tanium Client version: 7.7.3.8248 • Minimum build for 7.8 Tanium Clients: 7.8.2.1111
Debian 12.x	x86-64 ARM64	
Debian 11.x	x86-64	

©2026 Tanium Inc. All Rights Reserved

OS Version	Available Executables	Notes
Debian 10.x	x86-64	
Debian 9.x, 8.x	x86 x86-64	
Red Hat Enterprise Linux (RHEL) 10.x AlmaLinux 10.x Rocky Linux 10.x Oracle Linux 10.x	x86-64 ARM64	• Minimum Tanium Client version: 7.7.3.8207 • Support for ARM64 architecture for each solution requires a specific minimum version of that solution. For more information, see . • CentOS Stream and Fedora are separate upstream distributions and are not supported. • Oracle Linux 10 uses the same installer package as RHEL 10. For more information, see Deploy the Tanium Client to Linux endpoints using package files on page 173.
Red Hat Enterprise Linux (RHEL) 9.x AlmaLinux 9.x Rocky Linux 9.x Oracle Linux 9.x	x86-64 ARM64	• Support for ARM64 architecture for each solution requires a specific minimum version of that solution. For more information, see . • CentOS Stream and Fedora are separate upstream distributions and are not supported. • For Oracle Linux, a separate installer package is available. For more information, see Deploy the Tanium Client to Linux endpoints using package files on page 173.
Red Hat Enterprise	x86-64	• Support for ARM64 architecture for each solution requires a specific minimum version of that solution. For more information, see .

©2026 Tanium Inc. All Rights Reserved

OS Version	Available Executables	Notes
Linux (RHEL) 8.x CentOS 8.x AlmaLinux 8.x Rocky Linux 8.x Oracle Linux 8.x	ARM64	• CentOS Stream and Fedora are separate upstream distributions and are not supported. • For Oracle Linux, a separate installer package is available. For more information, see Deploy the Tanium Client to Linux endpoints using package files on page 173.
Red Hat Enterprise Linux (RHEL) 7.x CentOS 7.x Oracle Linux 7.x	x86-64	• Fedora is a separate upstream distribution and is not supported. • For Oracle Linux, a separate installer package is available. For more information, see Deploy the Tanium Client to Linux endpoints using package files on page 173.
Red Hat Enterprise Linux (RHEL) 6.x CentOS 6.x Oracle Linux 6.x	x86 x86-64	• TSDB-CX, which is a Client Extension on page 27 installed by Tanium™ Client Management, requires a newer version of glibc and cannot be installed on this OS. Client Management is supported and functions as normal, but some monitoring and data collection features that are used for troubleshooting are not available. • Fedora is a separate upstream distribution and is not supported. • For Oracle Linux, a separate installer package is available. For more information, see Deploy the Tanium Client to Linux endpoints using package files on page 173.
Red Hat Enterprise Linux (RHEL) 5.x CentOS 5.x	x86 x86-64	• (CentOS 5.x) CentOS 5.x endpoints are included in summary Client health information in Client Management, but you cannot use Direct Connect to access detailed Client health information. • TSDB-CX, which is a Client Extension on page 27 installed by Tanium™ Client Management, requires a newer version of glibc and cannot be installed on this OS. Client Management is supported and functions as normal, but some monitoring and data collection features that are

©2026 Tanium Inc. All Rights Reserved

OS Version	Available Executables	Notes
Oracle Linux 5.x		used for troubleshooting are not available. • Fedora is a separate upstream distribution and is not supported. • For Oracle Linux, a separate installer package is available. For more information, see Deploy the Tanium Client to Linux endpoints using package files on page 173.
SUSE Linux Enterprise Server (SLES) 16.x openSUSE 16.x	x86-64	
SUSE Linux Enterprise Server (SLES) 15.x openSUSE 15.x	x86-64	
SUSE Linux Enterprise Server (SLES) 12.x openSUSE 12.x	x86-64	
Ubuntu 26.04.x	x86-64	• Minimum Tanium Client version: 7.7.3.8268

©2026 Tanium Inc. All Rights Reserved

OS Version	Available Executables	Notes
LTS	ARM64	• Minimum build for 7.8 Tanium Clients: 7.8.2.1171 • Only long-term support (LTS) releases of Ubuntu are supported.
Ubuntu 24.04.x LTS	x86-64 ARM64	• Minimum Tanium Client version: 7.6.2.1218 • Only long-term support (LTS) releases of Ubuntu are supported.
Ubuntu 22.04.x LTS	x86-64 ARM64	• Only long-term support (LTS) releases of Ubuntu are supported.
Ubuntu 20.04.x LTS	x86-64	• Only long-term support (LTS) releases of Ubuntu are supported.
Ubuntu 18.04.x LTS	x86-64	• Only long-term support (LTS) releases of Ubuntu are supported.
Ubuntu 16.04.x LTS	x86-64	• Only long-term support (LTS) releases of Ubuntu are supported.
Ubuntu 14.04.x LTS	x86-64	• Only long-term support (LTS) releases of Ubuntu are supported.

©2026 Tanium Inc. All Rights Reserved

Supported AIX versions for Tanium Client hosts

OS Version	Available Executables	Notes
IBM AIX 7.1 TL4 or later	POWER	• The Tanium Client for AIX requires a POWER7 or later CPU and a 64-bit operating system. • Installation of certain runtime libraries might be necessary on some AIX endpoints. For more information, see Prepare for deployment to Linux, macOS, Solaris, or AIX endpoints on page 129 (for deployment with Client Management) or Prepare for installation on page 189 (for installation using a package file). • Summary Client health information in Client Management includes AIX endpoints, but you cannot use Direct Connect to access detailed Client health information.

Supported Solaris versions for Tanium Client hosts

OS Version	Available Executables	Notes
Oracle Solaris 11.x Oracle Solaris 10 U11 or higher	SPARC x86	• Installation of certain utilities and packages might be necessary on some Solaris endpoints. For more information, see Prepare for deployment to Linux, macOS, Solaris, or AIX endpoints on page 129 (for deployment with Client Management) or Prepare for installation on page 182 (for installation using a package file). • Summary Client health information in Client Management includes Solaris endpoints, but you cannot use Direct Connect to access detailed Client health information.

Endpoint OS support in Tanium solutions

The table Table 6. Tanium Client OS product support on page 43 indicates the operating systems (OSs) that Tanium modules and shared services support for performing operations on managed endpoints (Tanium Client host systems). To see detailed information about

©2026 Tanium Inc. All Rights Reserved

Tanium Client support for a particular module or service, click the link in the **Product** column to go to the corresponding user guide. The table uses the following icons:

- : Full support
- : Partial support (click the **Product** link or Contact Tanium Support on page 392 for details)
- : No support

Note:

- Client OS support does not apply to the following Tanium modules and shared services because they are server-side solutions: API Gateway, Connect, Console, Criticality, Directory Query, Feed, Health Check, Interact, Reporting, Reputation, and Trends.
- Because container-based endpoints are not traditional endpoints that run packages or tooling, they support only basic monitoring and do not support most Tanium solution functionality. For more information, see the Tanium Cloud Workloads User Guide.

Important: Tanium's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at Tanium's sole discretion. Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision. Information about potential future products may not be incorporated into any contract. The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

©2026 Tanium Inc. All Rights Reserved

Tanium Client OS product support

Product	Windows	macOS	Linux	Solaris and AIX
Tanium Client	✓	✓	✓	✓
Asset	✓	✓	✓	~
Software Bill of Materials (SBOM) add-in for Asset	✓	✓	✓	✗
Benchmark	✓	✓	~	✗
Certificate Manager	✓	~	✓	✗
Client Management	~	✓	✓	✓
Comply	✓	✓	✓	~
Deploy	✓	✓	✓	✗
Direct Connect	~	✓	✓	✗
Screen Sharing add-in for Direct Connect	✓	~	✗	✗
Discover	✓	✓	✓	~

©2026 Tanium Inc. All Rights Reserved

Product	Windows	macOS	Linux	Solaris and AIX
Endpoint Configuration	✓	✓	✓	✓
End-User Notifications	✓	~	✗	✗
Enforce	✓	✓	~	✗
Engage	✓	✓	✗	✗
Impact	✓	✗	✗	✗
Integrity Monitor	✓	✗	✓	~
Investigate	✓	✓	✓	✗
Jump Gate	✓	✓	✓	✗
Patch	✓	✓	~	✗
Performance	✓	✓	✓	✗
Provision	✓	~	~	✗
Reveal	✓	✓	✓	✗

©2026 Tanium Inc. All Rights Reserved

Product	Windows	macOS	Linux	Solaris and AIX
Threat Response	✓	✓	✓	✗
Zero Trust	✓	✓	✓	✗

Hardware requirements

The following minimums are recommended to install and run the Tanium Client on endpoints:

- CPU cores: 2
- RAM: 2 GB
- Available disk space: 1 GB

On an endpoint that does not use functionality from Tanium modules and uses the Tanium Client only for basic visibility and endpoint information, the Tanium Client can function with a single-core CPU. However, overall performance of the endpoint might be reduced.

Best Practice: Virtual desktop infrastructure (VDI) environments: For better performance, provide at least two CPU cores for each VDI instance, even if CPU cores are overprovisioned.

The listed hardware requirements are the minimums for an endpoint with a minimal workload aside from Tanium Client processes. Installed modules or services might require additional RAM and disk space, depending on your usage. Other applications that run on an endpoint require additional CPU, RAM, and disk resources. Contact Tanium support on page 392 for guidance on specific configurations.

©2026 Tanium Inc. All Rights Reserved

The modules that are listed in the following table have specific additional hardware requirements. Requirements for RAM refer to the minimum installed RAM that the Client and *all* installed modules and services require. Requirements for disk space refer to the *additional* available disk space that *each* listed module requires. (For complete endpoint requirements for each listed modules, follow the links in the table. For links to endpoint requirements for all solutions, see the Solution-specific requirements for the Tanium Client and endpoints on page 47 table.)

Additional hardware requirements for specific modules

Product	Additional available disk space	Minimum RAM required
Tanium™ Comply	2 GB [1]	2 GB [2]
Tanium™ Deploy	2 GB [3]	2 GB [2]
Tanium™ Integrity Monitor	1 GB (3 GB recommended) [1,4]	4 GB
Tanium™ Patch	5 GB [3]	2 GB [2,5]
Tanium™ Performance	100 MB plus the amount specified in the **Database maximum size** parameter (1 GB by default) [6]	2 GB [2]
Tanium™ Reveal	2 GB [1,7]	2 GB [2]
Tanium™ Software Bill of Materials (SBOM) add-in for Tanium™ Asset	Only the additional space required for Tanium™ Index [1]	2 GB [2]
Tanium™ Threat Response	3 GB [1,4]	4 GB

©2026 Tanium Inc. All Rights Reserved

Product	Additional available disk space	Minimum RAM required

[1] This solution or add-in uses the Tanium™ Client Index Extension, which requires disk space in addition to what is listed for the solution. (Comply uses Index only if you use SBOM scanning.) A minimum of 1 GB of additional disk space is required for Index when it is initially installed, but the total size of the Index database depends on the file system on the endpoint. A general guideline is that the database uses approximately 1 MB for each 1 GB of files on disk. All solutions that use Index share the Index database and the disk space used by the database.

[2] This solution does not have a specific RAM requirement above the baseline 2 GB of RAM that the Tanium Client requires.

[3] The listed disk space represents the minimum space required for Client cache and scan metadata, but it does not include the size of software packages and patches. Deploy and Patch temporarily consume more than this cache space during deployment, depending on the size of software packages and patches you deploy. If both Deploy and Patch are installed, both solutions together require 5 GB minimum disk space for Client cache and scan metadata.

[4] This solution uses the Tanium™ Client Recorder Extension, which might require disk space in addition to what is listed for the solution. Specific disk space requirements for Recorder depend on the number of events recorded on the endpoint.

[5] The utilities that Patch uses for scanning use increased RAM for up to several minutes during endpoint scans. If an endpoint must also run other processes that use significant RAM during Patch scans, it might require more RAM than the minimum 2 GB.

[6] The Performance database collects approximately 45 MB per day for busy servers and 25-35 MB per day for workstations.

[7] The listed disk space is a base estimate for the Index database when Quick Search is disabled (the default). Enabling Quick Search can significantly increase disk usage, depending on the number of targeted files and how unique their text content is. Index exclusions also affect the size. Validate actual disk usage on representative test endpoints before you enable Quick Search broadly. Reveal 2.0 and later uses only the Tanium™ Client Index Extension and does not require the Tanium™ Client Recorder Extension.

Module and service requirements

Click the links in the following table to see the minimum Tanium Client version (Tanium dependencies) and Client endpoint requirements

©2026 Tanium Inc. All Rights Reserved

for each Tanium module and shared service.

Solution-specific requirements for the Tanium Client and endpoints

Product	Tanium Dependencies	Server Requirements	Endpoint Requirements
Tanium™ Asset	Core platform dependencies	Tanium Module Server	Endpoints
Tanium™ Software Bill of Materials (SBOM) add-in for Asset	Core platform dependencies	No additional requirements	Endpoints
Tanium™ Automate	No additional requirements	No additional requirements	N/A
Tanium™ Benchmark	Core platform dependencies	Tanium Module Server	Endpoints
Tanium™ Certificate Manager	Core platform dependencies	No additional requirements	Endpoints
Tanium™ Client Management	Core platform dependencies	• Tanium Module Server • Compatibility among components in a Tanium release	The following sections: • The table Supported OS versions for Tanium Client hosts • Port requirements for Client Management • Security exclusions for Client Management
Tanium™ Cloud Workloads	Core platform dependencies	No additional requirements	N/A
Tanium™ Comply	Core platform dependencies	No additional requirements	Endpoints
Tanium™ Connect	Core platform	Tanium Module Server	N/A

©2026 Tanium Inc. All Rights Reserved

Product	Tanium Dependencies	Server Requirements	Endpoint Requirements
	dependencies		
Tanium™ Console	Core platform dependencies	Core Platform resources	N/A
Tanium™ Criticality	Core platform dependencies	Tanium Module Server	N/A
Tanium™ Deploy	Core platform dependencies	Tanium Server and Module Server	Endpoints
Tanium™ Direct Connect	Core platform dependencies	• Tanium Module Server • Zone proxy server requirements	Endpoints
Tanium™ Screen Sharing add-in for Direct Connect	No additional requirements	No additional requirements	Endpoints
Tanium™ Directory Query	Core platform dependencies	No additional requirements	N/A
Tanium™ Discover	Core platform dependencies	Tanium Module Server	Endpoints
Tanium™ Endpoint Configuration	Core platform dependencies	Tanium Module Server	Endpoints
Tanium™ End-User Notifications	Core platform dependencies	Tanium Module Server	Endpoints
Tanium™ Enforce	Core platform dependencies	Tanium Module Server	Endpoints

©2026 Tanium Inc. All Rights Reserved

Product	Tanium Dependencies	Server Requirements	Endpoint Requirements
Tanium™ Engage	Core platform dependencies	Tanium Module Server	Endpoints
Tanium™ Gateway	Core platform dependencies	Tanium Module Server	N/A
Tanium™ Guide	Core platform dependencies	Tanium Module Server	N/A
Tanium™ Health Check	Core platform dependencies	Tanium Module Server	N/A
Tanium™ Impact	Core platform dependencies	Tanium Module Server	Endpoints
Tanium™ Integrations Gallery	Core platform dependencies	No additional requirements	N/A
Tanium™ Integrity Monitor	Core platform dependencies	No additional requirements	Endpoints
Tanium™ Interact	Core platform dependencies	No additional requirements	Endpoints
Tanium™ Investigate	Core platform dependencies	Tanium Module Server	Endpoints
Tanium™ Jump Gate	Core platform dependencies	No additional requirements	Endpoints
Tanium™ Patch	Core platform dependencies	Tanium Server and Module Server computer resources	Endpoints
Tanium™ Performance	Core platform dependencies	No additional requirements	Endpoints

©2026 Tanium Inc. All Rights Reserved

Product	Tanium Dependencies	Server Requirements	Endpoint Requirements
Tanium™ Provision	Core platform dependencies	Tanium Module Server	Endpoints
Tanium™ Reporting	Core platform dependencies	Tanium Module Server	N/A
Tanium™ Reputation	Core platform dependencies	Tanium Module Server	N/A
Tanium™ Reveal	Core platform dependencies	Tanium Module Server	Endpoints
Tanium™ Threat Response	Core platform dependencies	Tanium Module Server	Endpoints
Tanium™ Trends	Core platform dependencies	Tanium Module Server	N/A
Tanium™ Zero Trust	Core platform dependencies	No additional requirements	Endpoints

Requirements for satellites used for Tanium Client deployment in Client Management

Operating systems supported for satellites used in Client deployment

Only the following operating systems are supported for a satellite used for Tanium Client deployment. For other OS requirements for Tanium Client, see the table Supported operating systems on page 32.

- Windows

©2026 Tanium Inc. All Rights Reserved

    - Windows Server 2012 R2 or later
    - Windows 7 or later
- Linux
    - AlmaLinux 8.x or later
    - CentOS 7.x, 8.x
    - Debian 10.x or later
    - Oracle Linux 7.x or later
    - Red Hat Enterprise Linux 7.x or later
    - Rocky Linux 8.x or later
    - Ubuntu 20.04 or later



Important: If FIPS mode is enabled on a Linux satellite, you cannot use that satellite to deploy the Tanium Client to Windows endpoints.

Hardware requirements for satellites used in Client deployment

The following hardware specifications are the recommended minimum for a satellite used for Tanium Client deployment:

- CPU architecture: x64 or x86
- CPU cores: 4

©2026 Tanium Inc. All Rights Reserved

- RAM: 8 GB
- Disk space (in addition to space required for the Tanium Client and any modules in use): 500 MB
- Network bandwidth: 10 Mbps between the Module Server and the satellite, and between the satellite and targeted endpoints

Tanium Client Management dependencies

Core platform dependencies

Make sure that your environment meets the following requirements:

- Tanium license that includes Client Management. For more information about how to get Client Management, see Tanium Solutions & Bundles.
- Tanium Core Platform servers
- Tanium Client: Downloading Client installers from Client Management does not require a pre-existing installation of Tanium Client. Using Client profile and Client health features, including using Direct Connect to access detailed Client health information, requires any supported version of Tanium Client (see Supported operating systems on page 32).

Solution dependencies

Other Tanium solutions are required for specific Client Management features to work. The installation method that you select determines if the Tanium Server automatically imports dependencies or if you must manually import them.

©2026 Tanium Inc. All Rights Reserved

Note: Some Client Management dependencies have their own dependencies, which you can see by clicking the links in the lists of Required dependencies on page 54 and Feature-specific dependencies on page 55. Note that the links open the user guides for the latest version of each solution, not necessarily the minimum version that Client Management requires.

Important: For solutions to perform configuration changes or tool deployment through Endpoint Configuration on endpoints with action locks turned on, you must enable the **Manifest Package Ignore Action Lock** and **Deploy Client Configuration and Support Package Ignore Action Lock** settings. To access these settings, from the Endpoint Configuration **Overview** page, click Settings and select **Global**. For more information about action locks, see Managing action locks.

TANIUM RECOMMENDED INSTALLATION

If you select **Tanium Recommended Installation** when you import Client Management, the Tanium Server automatically imports all your licensed solutions at the same time. For more information, see Import all modules and services.

IMPORT SPECIFIC SOLUTIONS

If you select only Client Management to import, the Tanium Server automatically imports the latest available versions of any required dependencies that are missing. If some required dependencies are already imported but their versions are earlier than the minimum required for Client Management, the Server automatically updates those dependencies to the latest available versions.

REQUIRED DEPENDENCIES

Client Management has the following required dependencies:

©2026 Tanium Inc. All Rights Reserved

- Tanium™ Direct Connect
- Tanium™ Endpoint Configuration
- Tanium™ RDB
- Tanium™ Reporting
- Tanium™ Secrets
- Tanium™ Trends

FEATURE-SPECIFIC DEPENDENCIES

Client Management has the following feature-specific dependency:

- Tanium Discover is required to target endpoints based on Discover tags.

Client extensions and endpoint tools

Tanium Endpoint Configuration installs Client Extensions and other tools for endpoints. Client extensions perform tasks that are common to certain Tanium solutions. Each Client Extension and tool might have recommended security exclusions to allow them to run without interference. For a list of all Client Extensions and tools, see Reference: Client extensions used for Tanium solutions.

Note: The change management feature of Endpoint Configuration might affect the version of each endpoint tool installed on endpoints.

©2026 Tanium Inc. All Rights Reserved

Tanium™ Module Server

Client Management is installed and runs as a service on the Module Server host computer. The impact on the Module Server is minimal and depends on usage.

For information about Module Server sizing in a Windows deployment, see Host system sizing guidelines.

Compatibility among components in a Tanium release

Tanium™ Semiannual Release 2026H2

Tanium™ Semiannual Release 2026H2 includes new versions of the following components:

- Tanium Operating System (TanOS): The operating system that runs on each Appliance
- Tanium Core Platform: The software that runs on Tanium Core Platform Servers, including the Tanium Server, Tanium Module Server, Tanium Zone Server, and Tanium Zone Server Hub
- Tanium solutions: The solutions that you have licensed to provide specific functionality in your Tanium environment, including modules, shared services, and content-only solutions
- Tanium Client: The service that runs on endpoints to discover and report data in the Tanium environment
- Tanium™ Endpoint Configuration Toolset: A collection of tools, such as Tanium™ Client Extensions, that are deployed to endpoints to enable functionality for Tanium solutions

For version and support information, see 2026H2 release notes.

For more information about Tanium releases, see Tanium releases.

©2026 Tanium Inc. All Rights Reserved

Maintenance releases

Maintenance releases provide security and bug fixes for currently supported semiannual releases. These upgrades are typically released monthly, and the support window remains based on the semiannual release. The maintenance release provides new versions only for the components that have fixes since the last update and might or might not contain upgrades for

Tanium Core Platform, Tanium solutions, Tanium Client, and the Tanium Endpoint Configuration Toolset.

You can skip any maintenance release updates that become available after a semiannual release. When you install the latest maintenance release update, it includes all the updates from any previous maintenance release update.



Best Practice: Install each maintenance release update when it becomes available to ensure your Tanium deployment has all the latest security and bug fixes.

Upgrade process

Upgrading TanOS, Tanium Core Platform, and Tanium solutions

You must use the versions of TanOS, Tanium Core Platform, and Tanium solutions that are provided in a semiannual release together, or the later versions of each component that are provided in maintenance releases that upgrade the semiannual release. When upgrading to a new semiannual release, you must upgrade these components at the same time, beginning with TanOS in a Tanium Appliance deployment, or Tanium Core Platform in a Windows deployment. For specific upgrade steps, see Upgrade TanOS on Tanium Appliance (Tanium Appliance deployments) or Upgrading Tanium Core Platform Servers in a Windows deployment (Windows deployments).

©2026 Tanium Inc. All Rights Reserved

Important:

- After you start the upgrade process for a new semiannual release, you cannot access Tanium solutions until you finish upgrading both the platform and solutions. Make sure to plan a maintenance window with enough time to complete all upgrades.
- As a best practice, upgrade to the latest maintenance release available for semiannual release 2026H2. Do not upgrade to a maintenance release that has an earlier release date than the currently installed maintenance release. For example, if you have a maintenance release from February 1 currently installed, install a maintenance release of the 2026H2 semiannual release from February 1 or later.

Note: If you are installing a maintenance release that does not include a TanOS upgrade in a Tanium Appliance deployment, begin the upgrade process with Tanium Core Platform. For more information, see Upgrade Tanium Core Platform in an Appliance deployment.

UPGRADING THE TANIUM ENDPOINT CONFIGURATION TOOLSET AND TANIUM CLIENT

You deploy the Tanium Endpoint Configuration Toolset and, optionally, the Tanium Client to endpoints using the change management feature of Tanium Endpoint Configuration. For more information, see Managing endpoint tool upgrade rollouts. If you do not enable Client upgrades in the change management feature, or if you need to upgrade the Tanium Client in upgrade rings for which Client upgrades are not yet enabled, you must upgrade the Tanium Client on endpoints using Client Management or other means to maintain a supported configuration. For more information, see Upgrading Tanium Clients. Tanium Semiannual Release 2026H2 supports all Tanium Client versions that the Tanium Core Platform supports. Each semiannual release supports the current endpoint configuration toolset and the two previous toolset releases.

©2026 Tanium Inc. All Rights Reserved

Best Practice:

To ensure that all the features and fixes are available to endpoints, upgrade the Tanium Client to the version provided in the release, and deploy the Endpoint Configuration Toolset to all endpoints as soon as possible.

Note:

You cannot install the Tanium Client on a Tanium Appliance.

Endpoint accounts

Tanium Client service account

On Windows, the Tanium Client is installed as a service that must run in the security context of the Local System account.

On AIX, Linux, macOS, and Solaris, the Tanium Client is installed as a system service, which must run with a User ID (UID) of 0.

Account permissions for Client Management

During Client installation using Client Management, you must have an account configured with the appropriate permissions on each endpoint. You add credentials for these accounts during the deployment process (see Deploying the Tanium Client using Client Management on page 125Manage endpoint credentials on page 152). These accounts and permissions are necessary only during deployment, and they can be removed or changed after you successfully deploy Clients.

©2026 Tanium Inc. All Rights Reserved

Best Practice: To protect credentials that are used for Client deployment, use one of the following methods:

- Use a temporary account that is removed after deployment.
- Disable or change the password for the account after Client deployment is complete.

WINDOWS ENDPOINTS

On each Windows endpoint, you must have an account with Local Administrator rights or a local or domain account configured that has the following abilities:

- Remotely connect to the endpoint and authenticate with SMB
- Create folders within the installation directory for 32-bit applications, and, if applicable, the custom location where the Tanium Client will be installed (by default, C:\Program Files (x86)\ for 64-bit versions of Windows, or C:\Program Files\ for 32-bit versions of Windows)

  Note: A custom installation directory must be located on drive C for deployment with Client Management. To install Tanium Client on a different drive, you must use an alternative deployment method. For more information, see Deploying the Tanium Client using an installer or package file on page 153.

- Write and execute files in the Tanium installation directory (by default, C:\Program Files (x86)\Tanium\ for 64-bit versions of Windows, or C:\Program Files\Tanium\ for 32-bit versions of Windows)

NON-WINDOWS ENDPOINTS

©2026 Tanium Inc. All Rights Reserved

On each non-Windows endpoint, you must have an account configured that can remotely connect to the endpoint and authenticate with SSH. You must use *one* of the following options to configure a user with elevated privileges to perform installation:

- The root user
- A user that is listed in the sudoers file on each endpoint to allow the account you are using for installation to use sudo

> **Note:**
>
> - A non-root user must have a password, even when using key-based authentication.
> - If you restrict user commands in the sudoers file, you must allow the commands used by Client Management on page 492 during deployment.

Specific distributions or your specific environment might have specific authentication requirements.

> **Note: Amazon Linux:** Amazon Linux requires key-based authentication. On the endpoint, be sure to enable SSH key-based authentication and enable `NOPASSWD` in the sudoers file for the admin user account. Add this user name and password to the credentials list. This configuration ensures that the key, and not a password, is used to elevate the admin permissions of the user so that the user can install the Tanium Client and start the service.

Trusted root certificate requirements on Windows endpoints

Windows endpoints require certain trusted root certificates to be installed to verify the integrity of the Tanium Client binaries. Windows Update installs the required certificates by default as part of the Microsoft Root Certificate Program, but you might have to install specific

©2026 Tanium Inc. All Rights Reserved

certificates on endpoints that are in an air-gapped environment or that are otherwise blocked from regularly updating trusted certificates. For more information about the Microsoft Root Certificate Program and updating trusted certificates, see Windows Server documentation: Certificates and trust in Windows.

Best Practice: Regularly update trusted root certificates using Windows Update.

For the most recent versions of Tanium Client, the following root certificates are required to verify the integrity of the Tanium Client binaries:

Required trusted root certificates

Certificate Name	SHA1 Fingerprint
DigiCert Assured ID Root CA	`05:63:B8:63:0D:62:D7:5A:BB:C8:AB:1E:4B:DF:B5:A8:99:B2:4D:43`
DigiCert High Assurance EV Root CA	`5F:B7:EE:06:33:E2:59:DB:AD:0C:4C:9A:E6:D3:8F:1A:61:C7:DC:25`
DigiCert SHA2 Assured ID CA	`E1:2D:2E:8D:47:B6:4F:46:9F:51:88:02:DF:BD:99:C0:D8:6D:3C:6A`
DigiCert SHA2 Assured ID Code Signing CA	`92:C1:58:8E:85:AF:22:01:CE:79:15:E8:53:8B:49:2F:60:5B:80:C6`
DigiCert Trusted Root G4	`A9:9D:5B:79:E9:F1:CD:A5:9C:DA:B6:37:31:69:D5:35:3F:58:74:C6`
DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1	`7B:0F:36:0B:77:5F:76:C9:4A:12:CA:48:44:5A:A2:D2:A8:75:70:1C`

For certificate downloads, see DigiCert: DigiCert Trusted Root Authority Certificates. For information about manually installing certificates, see Microsoft Windows documentation: Importing Certificates.

©2026 Tanium Inc. All Rights Reserved

Network connectivity, ports, and firewalls

TCP/IP requirements for Tanium Client

Tanium Core Platform components use TCP/IP to communicate over IPv4 networks and IPv6 networks. Contact Tanium Support on page 392 if you need IPv6 support in Tanium Core Platform. Work with your network administrator to ensure that the Tanium components have IP addresses and can use the Domain Name System (DNS) to resolve host names.

Connectivity and TCP/IP requirements for Client Management

To automatically deploy the Tanium Client using Client Management, the Tanium Module Server must have a connection to endpoints, or at least one endpoint that is connected to the network must also have a connection to Tanium Cloud. This endpoint is used as a satellite. Additionally, both the Tanium Server and endpoints must have IPv4 addresses; IPv6 addresses are not supported in Client Management. If you plan to deploy the Tanium Client to endpoints where no endpoint can connect to the Module Server, or if you plan to deploy the Tanium Client where only IPv6 addresses are available, you can download and manually deploy an installation bundle. For more information, see (Optional) Download a tanium-init.dat file for alternative deployment on page 138.

Port requirements for Tanium Client and Client Management

The following ports are the defaults that are required for Tanium Client communication, and those that are required for Client Management communication.

©2026 Tanium Inc. All Rights Reserved

Default port requirements for

Source	Destination	Port	Protocol	Purpose
Tanium Client	Peer Clients	17472	TCP	Used for communication between the Tanium Client and peer Clients [1,2]
Peer Clients	Tanium Client	17472	TCP	Used for communication between the Tanium Client and peer Clients [1,2]
Tanium Client	Tanium Server	17472	TCP	Used for communication between the Tanium Client and the Tanium Server [2,4]
Tanium Client	Zone Server [3]	17472	TCP	Used for communication between the Tanium Client and the Zone Server [2,4]
Tanium Client	Tanium Client (loopback)	17473	TCP	Used for the Tanium Client API **Note:** This port is used with the loopback interface and usually does not require a firewall rule.
Tanium Client	Zone Server [3]	17486	TCP	Outbound communication from the Tanium Client and inbound communication to the Zone Server for direct endpoint connections using Direct Connect. For additional Direct Connect port requirements, see Direct Connect ports . [4]

©2026 Tanium Inc. All Rights Reserved

Source	Destination	Port	Protocol	Purpose
Endpoints in a Microsoft Azure environment where you install the Tanium Client VM extension	content.tanium.com	443	TCP (HTTPS)	Used for the endpoint to download the Tanium Client for installation. For more information, see Deploy the Tanium Client in Microsoft Azure environments using the Tanium Client VM extension .
Endpoints that access Tanium Account	*.cloud.tanium.com	443	TCP (HTTPS)	Used for browser access to Tanium Account

[1] You can change the port that Clients use for peer communication. Additionally, endpoints in isolated subnets or that otherwise do not have valid peers do not open the listening port and do not require firewall rules to allow incoming traffic on this port. For more information, see Customize listening ports and Configure isolated subnets .

[2] You must disable any form of packet or certificate inspection for Tanium Protocol traffic. For more information, see Packet inspection on page 70 .

[3] This destination is required only when you use a Zone Server.

[4] Tanium Core Platform Servers can use custom ports for communication with Tanium Client. For more information, see Configuring connections to the Tanium Core Platform .

Port requirements for Client Management

Source	Destination	Port	Protocol	Purpose
Module Server or satellite endpoint	Endpoints targeted for Tanium Client installation (non-Windows)	22	TCP	Used for SSH communication from the Module Server or satellite endpoint to the target endpoint during Client installation [1]

©2026 Tanium Inc. All Rights Reserved

Source	Destination	Port	Protocol	Purpose
Module Server or satellite endpoint	Endpoints targeted for Tanium Client installation (Windows)	135	TCP	Used for initiating WMI communication from the Module Server or satellite endpoint to the target endpoint during Client installation
		445	TCP	Used for SMB communication from the Module Server or satellite endpoint to the target endpoint during Client installation. If port `445` is inaccessible, the Module Server or satellite endpoint attempts a connection on port `139`. [2]
		49152–65535	TCP	Randomly allocated dynamic ports used for WMI communication after it is initiated on port `135`. If a different dynamic port range is configured for RPC communication, that port range must be allowed by the firewall.
Tanium Client (internal)	Module Server	17475	TCP	Used for direct connection to endpoints for detailed Client health information
Tanium Client (external)	Zone Server [3]	17486	TCP	Used for direct connection to endpoints for detailed Client health information. The default port number is `17486`. If needed, you can specify a different port number when you configure the Zone Proxy.
Module Server	Zone Server [3]	17487, 17488	TCP	Used by Direct Connect for communication between the Module Server and Zone Server. For more information, see Direct Connect ports.
Tanium Server	Module Server	17477	TCP	Used by Direct Connect for communication between the Tanium Server and Module Server. For more information, see Direct Connect ports.

[1] You can specify a custom SSH port in each deployment.

[2] This communication defaults to Server Message Block version 3 (SMBv3) for Module Server deployments in a Tanium Appliance deployment. It also defaults to SMBv3 when it is

©2026 Tanium Inc. All Rights Reserved

Source	Destination	Port	Protocol	Purpose
available on a Windows-based Module Server or a satellite endpoint. Client Management is also compatible with SMBv2 and SMBv1 and automatically uses the latest available version on the Module Server or satellite endpoint.				
[3] These ports are required only when you use a Zone Server.				



Best Practice: Configure firewall policies to open ports for Tanium traffic with TCP-based rules instead of application identity-based rules. For example, on a Palo Alto Networks firewall, configure the rules with service objects or service groups instead of application objects or application groups.



Note: Some Tanium modules and shared services have additional port requirements for the Tanium Client. For more information, see Network connectivity and firewall or Ports and firewalls.

Work with your network security administrator to ensure that firewalls and security applications do not block the port that the Tanium Client uses for communication with the Tanium Server or Zone Server and with peer Clients (default is port 17472). You can change the port that Clients use to communicate with the Server by configuring the ServerPort on page 232 setting. You can also change the port that Clients use for peer communication by configuring the **ListenPort** or **EnableRandomListeningPort** setting. For more information, see Customize listening ports on page 274. If you do not configure either of these settings, Clients default to using **ServerPort** for peer communication.

The default Client peering settings ensure that Clients form linear chains only within the boundaries of local area networks (LANs). Therefore, firewalls must allow bi-directional TCP communication on the listening port between Clients that are in the same LAN, but not necessarily between all Clients across your enterprise wide area network (WAN). For more information about network port requirements in Tanium, see Network connectivity and firewall or Ports and firewalls. For more information about Client peering settings, see

©2026 Tanium Inc. All Rights Reserved

Configuring Tanium Client peering on page 247.

©2026 Tanium Inc. All Rights Reserved

Note:

- **Windows:** If you use service-specific rules on a host-based firewall on endpoints running the Tanium Client, these rules must apply to the **Tanium Client** service.
- **macOS:** The Tanium Client service is signed to automatically allow communication through the default macOS firewall. However, the Client installation process does not modify any host-based firewall that is in use. For more information about managing macOS firewalls, see Manage macOS firewall rules on page 305.

  On endpoints that run macOS 10.14 (Mojave) or later, you might have to configure a firewall rule to prevent end users from seeing a pop-up for allowing connections during a Tanium Client upgrade. For more information, see Manage pop-ups for Tanium Client upgrades on page 306.
- **Linux:** For more information about managing Linux firewalls, see Manage Linux firewall rules on page 308.
- The Tanium Server and Zone Server also use port 17472 by default. Therefore, if you install the Client on the same host as the Server in a Windows deployment, the listening port for client-to-client communication automatically increments by one on that host to prevent port conflicts, so the default is 17473. This installation is not a best practice. For more information, see Compatibility among components in a Tanium release on page 56.
- If you configure the Tanium Client to randomly select a new listening port at intervals, you must configure endpoint firewalls to allow incoming connections on any port that the Tanium Client process requests. For more information, see Randomize listening ports on page 275.
- The port number for the Client API is one higher than the client-Client listening port, which means that, by default, the API port is 17473. However, if the listening port changes, the API port also changes. For example, if you set **ListenPort** to 17473, the Client API port becomes 17474. Because the API is on the loopback interface (localhost), the API port usually

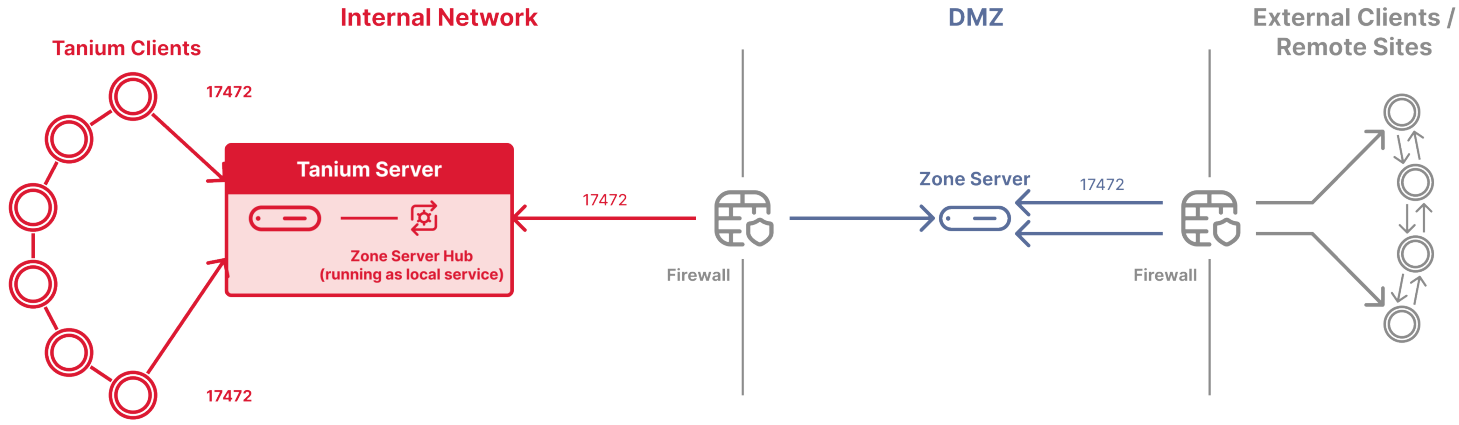
©2026 Tanium Inc. All Rights Reserved

does not require a firewall rule for allowing traffic.

For additional information about preparing endpoints for remote installation using Client Management, see Prepare for deployment to Linux, macOS, Solaris, or AIX endpoints on page 129Deploying the Tanium Client using Client Management on page 125 and Deploying the Tanium Client using Client Management on page 125Prepare for deployment to Windows endpoints on page 134.

The following figure illustrates a deployment with external and internal Tanium Clients. In this example, the external Clients are in virtual private networks (VPNs) and therefore do not peer with each other (see Configuring Tanium Client peering on page 247). Each external Client has a leader connection to the Tanium Zone Server. The internal Clients peer with each other in linear chains, and each chain connects to the Tanium Server through a backward and forward leader.

Figure 3. Tanium Client connectivity



Packet inspection

Communication between the Tanium Client and Tanium Core Platform Servers and between peer Clients uses the proprietary Tanium™

©2026 Tanium Inc. All Rights Reserved

Protocol and is encrypted with TLS 1.3 when using Tanium Core Platform 7.6.2 or later with Tanium Client 7.6.2 or later, or TLS 1.2 when using earlier versions. You must disable any form of deep packet inspection, SSL/TLS decryption, or certificate inspection on firewalls, proxy servers, or any other network devices through which Tanium Protocol traffic passes, or you must configure exceptions or bypasses for Tanium Protocol traffic on such devices. Decryption or inspection of Tanium Protocol traffic can corrupt packets and interrupt Tanium functionality.

Host system security exclusions

If antivirus (AV) or other security software is in use in the environment to monitor and block unknown host system processes, Tanium requires that a security administrator create exclusions to allow the Tanium processes to run without interference. This software can include security applications that are included with an endpoint operating system, such as fapolicyd on some Linux distributions, or Microsoft Defender on Windows. The configuration of these exclusions varies depending on the security software.

For more information about security exclusions to define across Tanium, see Reference: Endpoint security exclusions. For Windows-based Tanium Core Platform deployments, see Tanium Core Platform Server security exclusions.

Security exclusions for Tanium Client

You might need to exclude the Tanium Client installation directories from real-time inspection on some AV or other host-based security software. Typically, you also configure a policy to ignore the input and output of Tanium binaries. How you configure these exclusions varies based on your security software.

The following tools and files have specific requirements for the Tanium Client:

- Microsoft Group Policy Objects (GPO) or other central management tools for managing host firewalls: Tanium recommends creating rules to allow inbound and outbound TCP traffic across the port that the Client uses for Tanium traffic (default 17472) and port 17486 on any managed endpoints. For more information, see Network connectivity, ports, and firewalls on page 63.

©2026 Tanium Inc. All Rights Reserved

- Windows Update offline scan file (Wsusscn2.cab): The Tanium Client uses Wsusscn2.cab to assess endpoints for installed or missing operating system and application security patches. If your endpoint security solutions scan archive files, see the Microsoft KB for information on configuring those tools to interact appropriately with the Wsusscn2.cab file.
- McAfee Host Intrusion Detection (in older versions of McAfee security software): Tanium recommends marking the Tanium Client as both **Trusted for Firewall** and Trusted for IPS.

Note: Some Tanium modules and shared services have their own security exclusions for the Tanium Client. For more information, see Solution endpoint exclusions on page 420.

The following table lists Tanium Client directories that Tanium requires AV software or other host-based security applications exclude from on-access or real-time scans. Include subdirectories of these locations when you create the exception rules. The listed directory paths are the defaults. If you changed the directory locations to non-default paths, create rules that are based on the actual locations.

Security exclusions for Tanium Client folders Download as CSV

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows x86		Folder	C:\Program Files\Tanium\Tanium Client
Windows x64		Folder	C:\Program Files (x86)\Tanium\Tanium Client
macOS		Folder	/Library/Tanium/TaniumClient
Linux, Solaris, AIX		Folder	/opt/Tanium/TaniumClient

Tanium requires that security applications allow (not block, quarantine, or otherwise process) the following system processes. The

©2026 Tanium Inc. All Rights Reserved

<Tanium Client> variable indicates the Tanium Client installation directory on page 490, which is configurable during Client installation.

Security exclusions for Tanium Client processes Download as CSV

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows		Process	< *Tanium Client* >\TaniumClient.exe
		Process	< *Tanium Client* >\TaniumCX.exe
	Windows endpoints running Tanium Client 7.9.3	Process	< *Tanium Client* >\TaniumScriptRunner32.exe
		Process	< *Tanium Client* >\Tools\StdUtils\7za.exe
		Process	< *Tanium Client* >\Tools\StdUtils\runasuser.exe
		Process	< *Tanium Client* >\Tools\StdUtils\runasuser64.exe
		Process	< *Tanium Client* >\Tools\StdUtils\TaniumExecWrapper.exe
		Process	< *Tanium Client* >\Tools\StdUtils\TaniumFileInfo.exe
		Process	< *Tanium Client* >\Tools\StdUtils\TPowerShell.exe
macOS, Linux, Solaris, AIX		Process	< *Tanium Client* >/TaniumClient
		Process	< *Tanium Client* >/taniumclient

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	< *Tanium Client* >/TaniumCX
	macOS endpoints running the universal Tanium Client binary only	Process	< *Tanium Client* >/TaniumCX.app/Contents/MacOS/TaniumCX
		Process	< *Tanium Client* >/Tools/StdUtils/TaniumExecWrapper
		Process	< *Tanium Client* >/Tools/StdUtils/distribute-tools.sh

Security exclusions for Client Management

For the Client Management solution, Tanium requires the following exclusions.

The <*Tanium Client*> variable refers to the Tanium Client installation directory on page 490, which is configurable during Client installation.

The *<Module Server>* variable refers to the Tanium Module Server installation directory.

©2026 Tanium Inc. All Rights Reserved

Client Management security exclusions for Tanium Core Platform Servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	*<Module Server>* \services\client-management-service\node.exe
		Process	*<Module Server>* \services\client-profile-service\TaniumClientProfileService.exe
	When Direct Connect is installed	Process	*<Module Server>* \services\direct-connect-service\TaniumDirectConnectService.exe
	When Discover is installed	Process	*<Module Server>* \services\discover-service\node.exe
	When Discover is installed	Process	*<Module Server>* \plugins\content\discover-proxy\proxyplugin.exe
		Process	*<Module Server>* \services\endpoint-configuration-service\TaniumEndpointConfigService.exe
		Process	*<Module Server>* \services\twsm-v1\twsm.exe
Zone Server	When Direct Connect is installed	Process	<Tanium Installation Directory>\Tanium Direct Connect Zone Proxy\node.exe
	When Direct Connect is	Process	<Tanium Installation Directory>\Tanium Direct Connect Zone Proxy\twsm.exe

©2026 Tanium Inc. All Rights Reserved

Target Device	Notes	Exclusion Type	Exclusion
	installed		

Client Management security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows	During Client installation; x64 endpoints	Process	C:\Program Files (x86)\Tanium\TaniumClientBootstrap.exe
	During Client installation; x64 endpoints	Process	C:\Program Files (x86)\Tanium\SetupClient.exe
	During Client upgrade; x64 endpoints	Process	C:\Program Files (x86)\Tanium\TaniumClientUpgrade\SetupClient.exe
	During Client installation; x86 endpoints	Process	C:\Program Files\Tanium\TaniumClientBootstrap.exe
	During Client	Process	C:\Program Files\Tanium\SetupClient.exe

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	installation; x86 endpoints		
	During Client upgrade; x86 endpoints	Process	C:\Program Files\Tanium\TaniumClientUpgrade\SetupClient.exe
	During Client installation	Process	*<Tanium Client>* \SetupClient.exe
		File	*<Tanium Client>* \TaniumClientExtensions.dll
		File	*<Tanium Client>* \TaniumClientExtensions.dll.sig
		Process	*<Tanium Client>* \TaniumCX.exe
	Satellites used for Client deployment; installed on a satellite the first time you start a Client deployment that uses that	File	*<Tanium Client>* \extensions\TaniumClientDeploy.dll

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	satellite		
	Satellites used for Client deployment; installed on a satellite the first time you start a Client deployment that uses that satellite	File	*<Tanium Client>* \extensions\TaniumClientDeploy.dll.sig
	When Direct Connect is installed	File	*<Tanium Client>* \extensions\TaniumDEC.dll
	When Direct Connect is installed	File	*<Tanium Client>* \extensions\TaniumDEC.dll.sig
	When Discover is installed; satellite profiles only	File	*<Tanium Client>* \extensions\TaniumDiscover.dll

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	When Discover is installed; satellite profiles only	File	*<Tanium Client>* \extensions\TaniumDiscover.dll.sig
	When Discover is installed; satellite profiles only	File	*<Tanium Client>* \extensions\TaniumExtras.dll
	When Discover is installed; satellite profiles only	File	*<Tanium Client>* \extensions\TaniumExtras.dll.sig
		File	*<Tanium Client>* \extensions\TaniumTSDB.dll
		File	*<Tanium Client>* \extensions\TaniumTSDB.dll.sig
	When Discover is installed; (Distributed level 3, distributed level 4, and	Folder	C:\Program Files\Npcap

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	satellite profiles only)		
	When Discover is installed; (Distributed level 3, distributed level 4, and satellite profiles only)	Process	<*Tanium Client*> \Tools\Discover\nmap\nmap.exe
	x86 endpoints	Process	<*Tanium Client*> \tools\driver\TaniumDriverCtl.exe
	x64 endpoints	Process	<*Tanium Client*> \tools\driver\TaniumDriverCtl64.exe
	x86 endpoints	Process	<*Tanium Client*> \tools\driver\TaniumDriverSvc.exe
	x64 endpoints	Process	<*Tanium Client*> \tools\driver\TaniumDriverSvc64.exe
		Process	<*Tanium Client*> \tools\driver\service\TaniumDriverSvc.exe
		File	<*Tanium Client*> \tools\driver\TaniumProcessMonitor.dll
		File	<*Tanium Client*> \tools\driver\TaniumProcessMonitor64.dll

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
macOS	During Client installation using the universal binary; * represents the Tanium Client version, which can be substituted where wildcards are not allowed.	File	*<Tanium Client>* /TaniumClient-*-universal.pkg
	During Client installation using the x64 binary; * represents the Tanium Client version, which can be substituted where	File	*<Tanium Client>* /TaniumClient-*-x64.pkg

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	wildcards are not allowed.		
	During upgrade of a Client using the universal binary; * represents the Tanium Client version, which can be substituted where wildcards are not allowed.	File	*<Tanium Client>* /Downloads/TaniumClient-*-universal.pkg
	During upgrade of a Client using the x64 binary; * represents the Tanium Client version,	File	*<Tanium Client>* /Downloads/TaniumClient-*-x64.pkg

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	which can be substituted where wildcards are not allowed.		
		File	*<Tanium Client>* /libTaniumClientExtensions.dylib
		File	*<Tanium Client>* /libTaniumClientExtensions.dylib.sig
		Process	*<Tanium Client>* /TaniumCX
	Endpoints running the universal Tanium Client binary	Process	*<Tanium Client>* /TaniumCX.app/Contents/MacOS/TaniumCX
	When Direct Connect is installed	File	*<Tanium Client>* /extensions/libTaniumDEC.dylib
	When Direct Connect is installed	File	*<Tanium Client>* /extensions/libTaniumDEC.dylib.sig

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	When Discover is installed (Distributed level 3, distributed level 4, and satellite profiles only)	Process	*<Tanium Client>* /Tools/Discover/nmap/nmap
	When Discover is installed (Satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumDEC.dylib
	When Discover is installed (Satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumDEC.dylib.sig
	When Discover is installed (Satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumDiscover.dylib
	When Discover	File	*<Tanium Client>* /extensions/libTaniumDiscover.dylib.sig

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	is installed (Satellite profiles only)		
	When Discover is installed (Satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumExtras.dylib
	When Discover is installed (Satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumExtras.dylib.sig
		File	*<Tanium Client>* /extensions/libTaniumTSDB.dylib
		File	*<Tanium Client>* /extensions/libTaniumTSDB.dylib.sig
Linux	During Client installation; <Installation-package-file> represents the .rpm or .deb file for the	File	*<Tanium Client>* /<Installation-package-file>

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	target Linux distribution. For more information see Tanium Client package files for Linux Tanium Client package files for Linux on page 175 .		
	During Client upgrade; <Installation-package-file> represents the .rpm or .deb file for the target Linux distribution. For more information, see Tanium	File	*<Tanium Client>* /downloads/<Installation-package-file>

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	Client package files for Linux Tanium Client package files for Linux on page 175 .		
		File	*<Tanium Client>* /libTaniumClientExtensions.so
		File	*<Tanium Client>* /libTaniumClientExtensions.so.sig
		Process	*<Tanium Client>* /TaniumCX
	Satellites used for Client deployment; installed on a satellite the first time you start a Client deployment that uses that satellite	File	*<Tanium Client>* /extensions/libTaniumClientDeploy.so
	Satellites used	File	*<Tanium Client>* /extensions/libTaniumClientDeploy.so.sig

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	for Client deployment; installed on a satellite the first time you start a Client deployment that uses that satellite		
	When Direct Connect is installed	File	*<Tanium Client>* /extensions/libTaniumDEC.so
	When Direct Connect is installed	File	*<Tanium Client>* /extensions/libTaniumDEC.so.sig
	When Discover is installed; (Distributed level 3, distributed level 4, and satellite	Folder	*<Tanium Client>* /Tools/Discover/nmap/nmap

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	profiles only)		
	When Discover is installed (Satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumDiscover.so
	When Discover is installed (Satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumDiscover.so.sig
	When Discover is installed (Satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumExtras.so
	When Discover is installed (Satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumExtras.so.sig
		File	*<Tanium Client>* /extensions/libTaniumTSDB.so
		File	*<Tanium Client>* /extensions/libTaniumTSDB.so.sig

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
Solaris	During Client installation on x86 endpoints; * represents the Tanium Client version, which can be substituted where wildcards are not allowed.	File	*<Tanium Client>* /TaniumClient-*-SunOS-5.10.i386.pkg.tar.gz
	During Client installation on SPARC endpoints; * represents the Tanium Client version, which can be substituted where wildcards are not allowed.	File	*<Tanium Client>* /TaniumClient-*-SunOS-5.10.sparc.pkg.tar.gz

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	During Client upgrade on x86 endpoints; * represents the Tanium Client version, which can be substituted where wildcards are not allowed.	File	*<Tanium Client>* /downloads/TaniumClient-*-SunOS-5.10.i386.pkg.tar.gz
	During Client upgrade on SPARC endpoints; * represents the Tanium Client version, which can be substituted where wildcards are not allowed.	File	*<Tanium Client>* /downloads/TaniumClient-*-SunOS-5.10.sparc.pkg.tar.gz

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
AIX	During Client installation; * represents the Tanium Client version, which can be substituted where wildcards are not allowed.	File	*<Tanium Client>* /TaniumClient-*-powerpc.pkg
	During Client upgrade; * represents the Tanium Client version, which can be substituted where wildcards are not allowed.	File	*<Tanium Client>* /downloads/TaniumClient-*-powerpc.pkg

INTERNET URL REQUIRED FOR CLIENT MANAGEMENT

©2026 Tanium Inc. All Rights Reserved

The Module Server must be able to connect to https://content.tanium.com to allow Client Management to import the files needed to deploy the Tanium Client.

User role requirements for Client Management

Predefined roles grant the following permissions, which are required to use Client Management functionality:

- solution permissions on page 94
- administration, platform content, and global permissions on page 99: The solution permissions automatically provide some of these permissions.

To review a summary of the predefined roles, see Set up Client Management users on page 111.



Note: Do not assign the **Client Management Service Account** and **Client Management Service Account - All Content Sets** roles to users. These roles are for internal purposes only.

Some Client Management solution permissions provide permissions that are associated with other solutions. Furthermore, all the platform content permissions and some solution permissions apply to content sets that might contain content for other solutions in addition to Client Management. If you create custom roles for Client Management users, be sure to assign all the solution permissions and content set permissions that are required for Client Management functionality. If you are not sure which permissions are required for a custom role, view the permissions of the predefined roles. For more information, see the following sections of the Tanium Console User Guide:

- RBAC overview (provides an overview of roles, permissions, and content sets)
- Provided role permissions
- View effective role permissions

©2026 Tanium Inc. All Rights Reserved

- Configure a custom role

Note: To install Client Management, you must be assigned the Administrator reserved role.

Client Management solution permissions

Permission	Client Management Administrator [1] [2]	Client Management User [1] [2]	Client Management Read-Only User [1] [2]	Client Management Downloader [1]	Client Management Operator [1]	Client Management Upgrade Operator [1]	Client Management Endpoint Configuration Approver [1]
Client-Management API Access the Client Management API	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✗
Client-Management Client Version Access and manage the versions of the Tanium Client used in deployments and upgrades	✓ READ WRITE	✓ READ	✓ READ	✗	✓ READ WRITE	✗	✗
Client-Management	✓	✓	✓	✗	✓	✗	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Client Management Administrator [1] [2]	Client Management User [1] [2]	Client Management Read-Only User [1] [2]	Client Management Downloader [1]	Client Management Operator [1]	Client Management Upgrade Operator [1]	Client Management Endpoint Configuration Approver [1]
Credential Access the credentials list (cannot view associated passwords or key data)	READ WRITE	READ	READ		READ WRITE		
Client-Management Deployment [6] Access data in Client deployments	✓ READ WRITE EXECUTE	✓ READ	✓ READ	✗	✓ READ WRITE EXECUTE	✗	✗
Client-Management Direct Connect to an endpoint using Direct Connect and read data from that endpoint	✓ CONNECT	✗	✗	✗	✓ CONNECT	✗	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Client Management Administrator [1] [2]	Client Management User [1] [2]	Client Management Read-Only User [1] [2]	Client Management Downloader [1]	Client Management Operator [1]	Client Management Upgrade Operator [1]	Client Management Endpoint Configuration Approver [1]
Client-Management Discover API Access the Client Management Discover API	✓ EXECUTE	✗	✗	✗	✓ EXECUTE	✗	✗
Client-Management Endpoint Configuration / Client Management Endpoint Configuration Approve Endpoint Configuration items for Client Management	✗	✗	✗	✗	✗	✗	✓ APPROVE
Client-Management Index Configuration Manage Client Index configurations	✓ READ WRITE DEPLOY	✓ READ	✓ READ	✗	✓ READ WRITE DEPLOY	✗	✗
Client-Management Profile Support	✓	✗	✗	✗	✗	✗	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Client Management Administrator [1] [2]	Client Management User [1] [2]	Client Management Read-Only User [1] [2]	Client Management Downloader [1]	Client Management Operator [1]	Client Management Upgrade Operator [1]	Client Management Endpoint Configuration Approver [1]
Bundle Access the Client Management support bundle	READ						
Client-Management Settings Configuration Manage Client settings configurations	✓ READ WRITE DEPLOY	✓ READ	✓ READ	✗	✓ READ WRITE DEPLOY	✗	✗
Client-Management Trends Supply data to Trends and view charts from Trends in Client Management	✓ READ WRITE	✓ READ	✓ READ	✗	✓ READ WRITE	✗	✗
Client-Management Upgrade Manage and run Client upgrades	✓ READ	✓ READ	✓ READ	✗	✓ READ	✓ READ	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Client Management Administrator [1] [2]	Client Management User [1] [2]	Client Management Read-Only User [1] [2]	Client Management Downloader [1]	Client Management Operator [1]	Client Management Upgrade Operator [1]	Client Management Endpoint Configuration Approver [1]
	WRITE				WRITE	WRITE	
Client-Management View View Client health charts	✓ HEALTH	✓ HEALTH	✓ HEALTH	✗	✓ HEALTH	✓ HEALTH	✗
Client-Management Download installation packages for the Tanium Client when using Client Management in Tanium Cloud	✓ DOWNLOAD	✗	✗	✓ DOWNLOAD	✓ DOWNLOAD	✗	✗
Clientmanagement View the Client Management workbench	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW	✗

[1] To view the content sets to which the platform content permissions apply, see View effective role permissions .

©2026 Tanium Inc. All Rights Reserved

Permission	Client Management Administrator [1] ,[2]	Client Management User [1] ,[2]	Client Management Read-Only User [1] ,[2]	Client Management Downloader [1]	Client Management Operator [1]	Client Management Upgrade Operator [1]	Client Management Endpoint Configuration Approver [1]

[2] To create or view a Client deployment that uses a Tanium Discover label for targeting, a user must also have the **Discover Location Permissions WRITE** and **Discover Asset READ** permissions. The default Client Management roles do not have these permissions assigned. For more information about targeting Client deployments, see Deploy Clients on page 138. For more information about Discover permissions, see User role requirements.

Client Management Administration and Platform content user role permissions

Permission	Role Type	Client Management Administrator	Client Management User	Client Management Read-Only User	Client Management Downloader	Client Management Operator	Client Management Upgrade Operator	Client Management Endpoint Configuration Approver
Action Group	Administration	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ	✗
Computer Group	Administration	✓ READ	✓ READ	✓ READ	✗	✓ READ	✓ READ	✗
User Group	Administration	✓ READ	✓ READ	✓ READ	✗	✓ READ	✓ READ	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Role Type	Client Management Administrator	Client Management User	Client Management Read-Only User	Client Management Downloader	Client Management Operator	Client Management Upgrade Operator	Client Management Endpoint Configuration Approver
Endpoint Configuration	Platform Content	✓ READ WRITE	✓ READ	✓ READ	✗	✓ READ WRITE	✗	✓ APPROVE DISMISS REJECT SHOW READ
Endpoint Configuration API	Platform Content	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✗	✓ EXECUTE	✗	✓ EXECUTE
Endpoint Configuration Module	Platform Content	✓ USE	✗	✗	✗	✓ USE	✗	✗
Endpoint Configuration Support Bundle	Platform Content	✓ READ	✗	✗	✗	✓ READ	✗	✗
Action	Platform Content	✓	✓	✓	✗	✓	✓	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Role Type	Client Management Administrator	Client Management User	Client Management Read-Only User	Client Management Downloader	Client Management Operator	Client Management Upgrade Operator	Client Management Endpoint Configuration Approver
		READ WRITE	READ	READ		READ WRITE	READ WRITE	
Own Action	Platform Content	✓ READ	✓ READ	✓ READ	✗	✓ READ	✓ READ	✗
Package	Platform Content	✓ READ	✓ READ	✓ READ	✗	✓ READ	✓ READ	✗
Plugin	Platform Content	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✗
Sensor	Platform Content	✓ READ	✗	✗	✓ READ	✓ READ	✓ READ	✗
Trends API Board	Platform Content	✓ READ WRITE	✓ READ	✓ READ	✗	✓ READ WRITE	✗	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Role Type	Client Management Administrator	Client Management User	Client Management Read-Only User	Client Management Downloader	Client Management Operator	Client Management Upgrade Operator	Client Management Endpoint Configuration Approver
Trends API Source	Platform Content	✓ READ WRITE	✓ READ	✓ READ	✗	✓ READ WRITE	✗	✗
Trends Data	Platform Content	✓ READ	✓ READ	✓ READ	✗	✓ READ	✗	✗
Trends View Recent	Platform Content	✓ RESULTS	✓ RESULTS	✓ RESULTS	✗	✓ RESULTS	✗	✗

To view the content sets to which the platform content permissions apply, see View effective role permissions .

©2026 Tanium Inc. All Rights Reserved

Tip:

To configure a user who can only view Client health information and connect to endpoints to access detailed Client health and troubleshooting information, assign the following roles:

- **Direct Connect User**
- A custom role with the following permissions:
  - **Clientmanagement Show**
  - **Client-Management Direct Connect**
  - **Client-Management View Health**

For information about creating a custom role, see Configure a custom role, and for information about assigning user roles, see Manage role assignments for a user.

For more information and descriptions of content sets and permissions, see Managing roles.

©2026 Tanium Inc. All Rights Reserved

Installing Client Management

Use the **Solutions** page to install Client Management and choose either automatic or manual configuration:

- Automatic configuration with default settings: Client Management is installed with any required dependencies and other selected products. After installation, the Tanium Server automatically configures the recommended default settings. This option is the best practice for most deployments. For more information about the automatic configuration for Client Management, see Import Client Management with default settings on page 104.
- Manual configuration with custom settings: After installing Client Management, you must manually configure required settings. Select this option only if Client Management requires settings that differ from the recommended default settings. For more information, see Import Client Management with custom settings on page 105.

Before you begin

- Read the .
- Review the Tanium Client and Client Management requirements on page 29.
- Assign the correct roles to users for Client Management. Review the User role requirements for Client Management on page 93.
    - To import the Client Management solution, you must be assigned the Administrator reserved role.
    - To configure the Client Management action group, you must be assigned the Administrator reserved role, Content Administrator reserved role, or a role that has the **Action Group** write permission.

Import Client Management with default settings

You can set the Client Management action group to target the **No Computers** filter group by enabling

©2026 Tanium Inc. All Rights Reserved

restricted targeting before importing Client Management. This option enables you to control Client Management tools deployment through scheduled actions that are created during the import and that target the Client Management tools action group. For example, you might want to test Client Management tools on a subset of endpoints before deploying the Client Management tools to all endpoints. In this case, you can manually deploy the Client Management tools to an action group that you configured to target only the subset. To configure an action group, see Targeting actions through action groups. To enable or disable restricted targeting, see Tools deployment and restricted targeting.

When you import Client Management with automatic configuration, the following default setting is configured:

Setting	Default Value
Action group	• Restricted targeting disabled (default): `All Computers` computer group • Restricted targeting enabled: `No Computers` computer group **Best Practice:** If you import Client Management with restricted targeting disabled, leave the Client Management action group set to the default of `All Computers`. If you use restricted targeting to set the Client Management action group to target the **No Computers** filter group, set the action group to target the computer group `All Computers`.
Client upgrade	If you imported Client Management on Tanium Core Platform 7.6 or later, a Client upgrade named `TCM CMI x.y Client Upgrade` is created to automatically upgrade all endpoints in the `All Computers` computer group to the latest version of the Tanium Client. You can modify this Client upgrade as desired. For more information, see Upgrade Tanium Clients using Client Management.

To import Client Management and configure default settings, see Import all modules and services. After the import, verify that the correct version is installed. For more information, see Verify Client Management version on page 106.

Import Client Management with custom settings

To import Client Management without automatically configuring default settings, be sure to clear the selection for **Apply All Tanium recommended configurations** while performing the steps in Managing Tanium solutions. After the import, verify that the correct version is installed. For more information, see Verify Client Management version on page 106.

©2026 Tanium Inc. All Rights Reserved

To configure the Client Management action group, see Configure the Client Management action group on page 111.

Manage solution dependencies

When you start the Client Management workbench for the first time, the Tanium Server checks whether all the Tanium modules and shared services (solutions) that are required for Client Management are installed at the required versions. The Client Management workbench cannot load unless all required dependencies are installed. If you selected **Tanium Recommended Installation** when you imported Client Management , the Tanium Server automatically imported all your licensed solutions at the same time. Otherwise, if you manually imported Client Management and did not import all its dependencies, Tanium Console displays a banner that lists the dependencies and the required versions.

1. Install the dependencies as described in Import or update specific solutions.
2. Open the **Client Management Overview** page. From the Main menu, go to **Shared Services** > **Client Management**. Verify that the Console no longer displays a banner to list missing dependencies.

Verify Client Management version

After you import or upgrade Client Management, verify that the correct version is installed.

1. Refresh your browser.
2. From the Main menu, go to **Shared Services** > **Client Management**.
3. To display version information, click Info .

Upgrade Client Management

For information upgrading Client Management, see Import or update specific solutions. After the upgrade, verify that the correct version is installed. For more information, see Verify Client Management version on page 106.

Migrating Client deployments from Client Management versions earlier than 2.1

Client deployments are structured differently from earlier versions in Client Management 2.1 and

©2026 Tanium Inc. All Rights Reserved

later. In versions earlier than 2.1, you created Client Configurations to define the general settings for the deployed Client and then applied those configurations to deployments that targeted specific endpoints. In version 2.1 and later, you configure all settings in a Client deployment, and you can optionally create Client deployment templates to specify general settings to be used across multiple deployments. For more information, see Manage Client deployments on page 136.

Because of these differences, when you upgrade from version 1.10–1.12 to version 2.1, the upgrade automatically migrates Client Configurations as follows:

- Client credentials: The upgrade migrates all credential sets with no changes.
- Legacy Client Configurations assigned to at least one legacy Client deployment: The upgrade creates a Client deployment that uses settings from the Client Configuration and the most recently run deployment that used that Client Configuration, including the credentials assigned to that deployment. You cannot reissue this deployment; you must instead clone it to a new deployment. For more information, see Migrating Client deployments from Client Management versions earlier than 2.1 on page 106.
- Legacy Client Configurations not assigned to any Client deployment: The upgrade creates a Client deployment template with the settings from the legacy Client Configuration. You can create Client deployments using this template. For more information, see Manage Client deployments on page 136.

Important: If you are using a version 1.9 or earlier, an upgrade directly to version 2.1 or later will not automatically migrate Client deployments and credentials. To preserve these items, upgrade to version 1.12 as an intermediate step before upgrading further.

CLONING CLIENT DEPLOYMENTS MIGRATED FROM VERSIONS EARLIER THAN 2.1

About this task

You cannot reissue a deployment that you created before you upgraded to Client Management 2.1 or later. If you want to continue to use such a deployment, you must clone it to a new deployment. The cloned deployment includes all settings migrated from the original deployment except for **Name** and **Description**.

1. From the Main menu, go to **Shared Services >** Client Management.

©2026 Tanium Inc. All Rights Reserved

2. From the **Client Management** menu, go to **Client Deployments**.
3. Click the name of a deployment that was migrated from an earlier version, and then click **Clone**.
4. Enter a **Name** and optionally a **Description** for the deployment.
5. Adjust settings as needed, and run the new deployment or save the settings as a new template. For more information, see Deploy Clients on page 138.

©2026 Tanium Inc. All Rights Reserved

Configuring Client Management

If you did not install Client Management with the **Apply All Tanium recommended configurations** option, you must enable and configure certain features. Additionally, you must add Client installation files if you are using an air-gapped environment.

Install and configure Tanium Endpoint Configuration

Manage solution configurations with Tanium Endpoint Configuration

Tanium Endpoint Configuration delivers configuration information and required tools for Tanium Solutions to endpoints. Endpoint Configuration consolidates the configuration actions that traditionally accompany additional Tanium functionality and eliminates the potential for timing errors that occur between when a solution configuration is made and the time that configuration reaches an endpoint. Managing configuration in this way greatly reduces the time to install, configure, and use Tanium functionality, and improves the flexibility to target specific configurations to groups of endpoints.

Endpoint tools are bundled together in a versioned toolset. Each toolset contains a specific version of each tool. The Endpoint Configuration Toolset Solution provides upgrades to the toolset, and it imports upgraded versions of the entire toolset as needed by upgraded or newly installed solutions.

©2026 Tanium Inc. All Rights Reserved

Important:

When you upgrade Client Management, the change management feature enables you to perform a staged rollout of the endpoint tools associated with the new version of Client Management. Client Management remains compatible with earlier versions of the endpoint tools and so continues to function with endpoints in rings that have not yet received the latest tools. However, any functionality added in the upgrade of Client Management might not be available on these endpoints until they receive the upgraded tools.

In some cases, multiple solutions install the same endpoint tool, but upgraded endpoint tools remain compatible with all associated solutions. For example, both Tanium™ Threat Response and Tanium™ Reveal install and use index-cx. When you upgrade Threat Response, it might install version x.6.yyyy of index-cx, superseding version x.5.zzzz that Reveal previously installed. The index-cx upgrade from Threat Response does not affect the Index-related functionality of Reveal on the upgraded endpoints. For more information about the change management feature, see Tanium Endpoint Configuration User Guide: Managing endpoint tool upgrade rollouts.

Note: For information about how to install Endpoint Configuration, see Installing Endpoint Configuration.

Optionally, you can use Endpoint Configuration to require approval of configuration changes. When configuration approvals are enabled, Endpoint Configuration does not deploy a configuration change to endpoints until a user with approval permission approves the change. For information about the roles and permissions that are required to approve configuration changes for Client Management, see User role requirements. For more information about how to enable and use configuration approvals in Endpoint Configuration, see Managing approvals.

Important: For solutions to perform configuration changes or tool deployment through Endpoint Configuration on endpoints with action locks turned on, you must enable the **Manifest Package Ignore Action Lock** and **Deploy Client Configuration and Support Package Ignore Action Lock** settings. To access these settings, from the Endpoint Configuration **Overview** page, click Settings  and select **Global**. For more information about action locks, see Managing action locks.

©2026 Tanium Inc. All Rights Reserved

For more information about Endpoint Configuration, see Tanium Endpoint Configuration User Guide.

Configure the Client Management action group

About this task

If you imported Client Management without the **Apply All Tanium recommended configurations** option or with Restricted Targeting enabled, the Client Management action group targets `No Computers` by default. To enable Client Management functionality after importing without the **Apply All Tanium recommended configurations** option or with Restricted Targeting enabled, set the Client Management action group to target the computer group `All Computers`.

1. From the Main menu, go to **Administration** > **Actions** > **Action Groups**.
2. Click Tanium Client Management.
3. Clear the selection for **No Computers**.
4. Select **All Computers** and click **Save**.

Set up Client Management users

You can use the following set of predefined user roles to set up Client Management users.

To review specific permissions for each role, see User role requirements for Client Management on page 93.

Important: On installation, Client Management creates a Client Management user to automatically manage the Client Management service account. Do not edit or delete the Client Management user.

For more information about assigning user roles, see Manage role assignments for a user.

©2026 Tanium Inc. All Rights Reserved

Tip: To provide just-in-time access or scalable standing access to Client Management functionality, you can use SCIM provisioning combined with Tanium user groups. This approach lets you manage user access at scale or ad hoc through your identity provider, without creating users individually in Tanium. For more information, see Provision users into Tanium user groups with SCIM.

Client Management Administrator

Assign the **Client Management Administrator** role to users who manage all configuration in Client Management, configure Client deployments, and investigate issues with specific Clients.

This role can perform the following tasks:

- View, create, edit, and delete Client deployment templates, Client credentials, and Client deployments

  Note: No user can view passwords in existing credentials.

- View, create, and delete Client deployments
- View summarized Client health information
- Directly connect to endpoints to view detailed Client health information

Client Management User

Assign the **Client Management User** role to users who execute Client deployments.

This role can perform the following tasks:

- View Client deployment templates, Client credentials, and Client deployments

  Note: No user can view passwords in existing credentials.

- View and execute Client deployments
- View summarized Client health information

©2026 Tanium Inc. All Rights Reserved

Client Management Read-Only User

Assign the **Client Management Read-Only User** role to users who can review details of Client deployments.

This role can view Client deployment templates, Client credentials, and Client deployments.

Client Management Downloader

Assign the **Client Management Downloader** role to users who download installation packages for the Tanium Client.

Client Management Operator

Assign the **Client Management Operator** role to users who download installation packages for the Tanium Client or investigate issues with specific Clients.

This role can perform the following tasks:

- Download installation packages for the Tanium Client.
- Directly connect to endpoints to view detailed Client health information.

Client Management Upgrade Operator

Assign the **Client Management Upgrade Operator** role to users who manage upgrades of the Tanium Client on endpoints.

This role can perform the following tasks:

- Upgrade the Tanium Client on endpoints.
- manage versions of the Tanium Client that are available for upgrades.

Client Management Endpoint Configuration Approver

Assign the **Client Management Endpoint Configuration Approver** role to a user who approves or rejects Client Management configuration items in Endpoint Configuration.



Note: Do not assign the **Client Management Service Account** and **Client Management Service Account - All Content Sets** roles to users. These roles are for internal purposes only.

©2026 Tanium Inc. All Rights Reserved

Tip:

To configure a user who can only view Client health information and connect to endpoints to access detailed Client health and troubleshooting information, assign the following roles:

- **Direct Connect User**
- A custom role with the following permissions:
  - **Clientmanagement Show**
  - **Client-Management Direct Connect**
  - **Client-Management View Health**

For information about creating a custom role, see Configure a custom role, and for information about assigning user roles, see Manage role assignments for a user.

Configure the default Server names and Server port for Tanium Client deployments

About this task

You can configure default Server name or names and Server port that populate the **Server Names** and **Server Port** settings when you create a new deployment in Client Management. You can change these values when you create a deployment. For more information, see Manage Client deployments on page 136.

1. From the Main menu, go to **Shared Services >** Client Management.
2. From the Client Management **Overview** page, click Settings.
3. For **Server Names**, enter the fully qualified domain names (FQDNs) or IP addresses of the Tanium Servers. In a deployment with Zone Servers, add their FQDNs or IP addresses. Using internally defined FQDNs or aliases is strongly recommended. Use a comma to separate the entry for each Server. If you include a port for a listed Server by appending `:<port_number>` to the Server address, it overrides the port specified for the **Server Port** setting.

©2026 Tanium Inc. All Rights Reserved

4. For **Server Port**, enter the port that the Tanium Client uses for communication with the Tanium Server and with peers. The default port is 17472.

Manage versions of the Tanium Client available for legacy deployments

About this task

The Tanium Server must download and cache the installers for each version of the Tanium Client that you want to use in Client deployments or upgrades. The server caches the latest version by default. When you synchronize the manifest and a new version is available, the Server automatically caches the new version, but it does not remove the previously cached version. To temporarily support legacy deployments, you can manually cache other specific versions that you want to use in Client deployments or upgrades.



Important:

- Each version of the endpoint toolset includes a specific version of the Tanium Client, which must be installed with the toolset to maintain a supported configuration. Endpoints with versions of the Tanium Client older than the associated toolset are unsupported. Caching and deployment of previous versions of the Tanium Client is provided for temporary support of legacy deployments.
- If you plan to upgrade endpoints that currently have Tanium Client 7.2 installed, cache the packages for a 7.4 version, such as version 7.4.10.1086, to perform the intermediate upgrade that is necessary before you upgrade to version 7.6 or later. Perform this upgrade before upgrading Tanium Core Platform to the 2025H1 semiannual release. For more information, see Upgrading Tanium Clients on page 342.

©2026 Tanium Inc. All Rights Reserved

Best Practice: Keep the Tanium Client up to date with the toolset on endpoints using the change management feature in Endpoint Configuration. To do so, you must enable Tanium Client upgrades in the upgrade ring configuration. For information about enabling this setting and managing upgrade rings and toolset promotions, see Managing Tanium Client and endpoint tool upgrade rollouts.

1. From the Main menu, go to **Shared Services >** Client Management.
2. Go to **Client Versions**.
3. (Optional) To download the latest manifest for Tanium Client installers from content.tanium.com, click **Synchronize Manifest**.
4. Beside each version that you want to cache for Client upgrades, click Cache Packages.

   Tip: To remove the cached packages for a version that is no longer needed and free up storage space, click Clear Package Cache beside that version. That version is not available for Client upgrades until you cache it again. You cannot remove the cached packages for a version that is selected in an existing Client upgrade.

Manage versions of the Tanium Client available in an air-gapped environment

About this task

If you cannot enable communication between your Tanium Module Server and content.tanium.com, you must manually import previous versions of the Tanium Client instead of caching versions from the online manifest. The latest version of the Tanium Client is provided in each air gap update; these steps are necessary only for temporary support of legacy deployments.

1. Contact Tanium Support on page 392 to obtain a ZIP file with the installation packages.
2. From the Main menu, go to **Shared Services** > **Client Management**.
3. Click **Upload Tanium Client**, click **Select Client ZIP file**, select the file, and click **Upload**.

©2026 Tanium Inc. All Rights Reserved

Tip: To delete an imported version, click Delete Version  beside that version. That version is not available for Client upgrades until you reimport it. You cannot delete a version that is selected in an existing Client upgrade.

©2026 Tanium Inc. All Rights Reserved

Deploying the Tanium Client

Deploying the Tanium Client to enterprise computers and integrating the deployment into standard IT processes involves multiple phases, as illustrated in the following figure. Each phase involves various considerations, tools, and options.

Figure 4. Tanium Client deployment phases

©2026 Tanium Inc. All Rights Reserved



The information on this page helps you carefully plan the deployment; review the following best practices for each phase.

Additionally, the subsequent topics in this section cover the methods and steps to deploy Tanium Client.

©2026 Tanium Inc. All Rights Reserved

Assess the environment where you are deploying the Tanium Client

When planning the deployment of the Tanium Client, assess the following factors to help determine the Client settings to use during deployment.

- IPv4 or IPv6 protocol: The network protocol that you use determines the addresses that you use for Tanium Servers or Zone Servers, the Client peering settings you use, and the deployment methods available. For more information about TCP/IP requirements, see Network connectivity, ports, and firewalls on page 63.

- Tanium infrastructure: Whether your Tanium environment uses a single Tanium Server or an active-active cluster, and whether it uses Zone Servers determines the Server addresses you specify during deployment. For more information about Tanium Core Platform Servers, see Tanium Tanium Core Platform for Windows Deployments User Guide and Tanium Appliance User Guide.

- Proxy servers: If endpoints must connect to a Tanium Server or Zone Server through a proxy server, you must configure the appropriate Client settings For more information, see Connect through an HTTPS forward proxy server on page 238.

  Best Practice: Configure proxy server settings during Client deployment.

- Subnets and WAN connections: If the network includes wide area network (WAN) connections between peers on the same subnet defined by the default /24 address mask, or it there are other factors that would slow connections between such peers, you might need to use Tanium Client peering settings to adjust the boundaries of the linear chains in which Tanium Clients form peer relationships. For more information about how Tanium Client peering works, see Client peering on page 23.

  Best Practice: Use the default Client peering settings when all endpoints on a subnet defined by the default /24 address mask share a high-speed local connection. Contact Tanium Support on page 392 for guidance in adjusting Client peering settings.

- Endpoint resources: If you are deploying the Tanium Client to endpoints with limited resources, virtualized servers, or virtual desktop infrastructure (VDI) instances, you might

©2026 Tanium Inc. All Rights Reserved

need to adjust certain Client settings, such as disabling logging and increasing the "distribute over time" value for actions. For more information, see Tuning Tanium Client settings for VDI endpoints and other endpoints with limited resources on page 407 and Preparing the Tanium Client on a virtual desktop infrastructure (VDI) instance on page 209.

Tip: To help simplify future management of VDI endpoints, consider creating computer groups with custom tag-based membership and applying corresponding custom tags to VDI endpoints. For more information, see Manage custom tags for computer groups.

- Licensing in VDI environments: The Tanium Server allocates a license for each unique Tanium Client for 30 days after that Client last registers with the Tanium Server or Tanium Zone Server. Each VDI instance that is created or reimaged counts as a licensed endpoint for at least 30 days, and each VDI instance that is deleted continues to consume a license for 30 days after it last registers.

  Use the following formula to calculate the number of licenses required to support your Tanium deployment.

  ### Formula for calculating Tanium Client licenses in VDI environments

Devices and VDI Instances	Estimated Count
Physical endpoints and persistent VDI instances	+
VDI instances that are created or reimaged over a 30-day period	+
Physical endpoints that are added or reimaged over a 30-day period	+
Total required licenses	=

  For assistance with licensing, contact Tanium Support on page 392.

For more information about configuring the Tanium Client for connections to the Tanium Core Platform and to peer Clients, see Configuring connections to the Tanium Core Platform on page 230 and Configuring Tanium Client peering on page 247.

Determine deployment methods and pilot the deployment

©2026 Tanium Inc. All Rights Reserved

The available deployment mechanisms are:

- **Tanium Client Management service:** You can deploy any version of the Tanium Client to any number of endpoints in a single operation. For more information, see the Deploying the Tanium Client using Client Management on page 125.
- **Existing application package deployment tools:** You can use standard third-party tools, such as System Center Configuration Manager (SCCM), Altiris, LANDESK, Puppet, and Casper. You can also use custom scripts that run the appropriate installation commands. For more information about the installer files and Client settings that are required to deploy the Client, see Deploying the Tanium Client using an installer or package file on page 153.
- **Manual installation:** For a small number of pilot endpoints, you can copy the installer or package file to the endpoint and run it manually. For more information about the installer files and Client settings that are required to deploy the Client, see Deploying the Tanium Client using an installer or package file on page 153.

Pilots usually target fewer than 5,000 endpoints. During your pilot, test deploying the Tanium Client with the standard software package deployment tool of your organization, or use Client Management if you have direct network access to the pilot endpoints and an account with the necessary permissions on each endpoint or at least one endpoint that is connected to the network has a connection to the Module ServerTanium Cloud. For more information about the requirements to deploy Clients with Client Management, see Tanium Client and Client Management requirements on page 29.



Note: This guide does not describe third-party tool-specific procedures for deploying the Tanium Client. For more information about using a third-party tool with Tanium installers, see the documentation for that tool.

Tip: To monitor containers on endpoints, use Tanium Cloud Workloads. For more information, see the Tanium Cloud Workloads User Guide.

Deploy to an initial set of endpoints

©2026 Tanium Inc. All Rights Reserved

After the pilot, an initial deployment into an enterprise might target 500,000 endpoints or more, and the deployment might reach across data center, headquarter, and branch locations.

Best Practice: For the initial rollout, use either Client Management or the standard application package deployment tools with which your IT organization and end users are already familiar.

Onboard new computers

Plan to integrate the Tanium Client installation into standard build processes for new computers, such as Microsoft Deployment Toolkit task sequences. You can optionally install the Client within operating system-specific images to adhere to organizational policies for provisioning new computers or virtual desktop infrastructure (VDI) instances. For more information, see Preparing the Tanium Client on OS images on page 194. When a new computer boots for the first time, the Tanium Client starts and registers with the Tanium Server.

Tip:

- For bare-metal provisioning of Windows or Linux endpoints, you can use Tanium™ Provision. For more information, see Tanium Provision User Guide.
- For deploying the Tanium Client on Microsoft Azure VMs and VM Scale Sets, you can use the Tanium Client Azure virtual machine (VM) extensions. For more information, see Deploy the Tanium Client in Microsoft Azure environments using the Tanium™ Client VM extension on page 215.

Maintain continuous hygiene

After the initial rollout, establish policies and procedures to enforce the use of the Tanium Client on endpoints in an enterprise network. Many organizations use Active Directory (AD) computer startup scripts to ensure that the Tanium Client is installed and that the Tanium Client service is started. Contact Tanium Support on page 392 for details.

Use Tanium™ Discover to scan for previously unmanaged or even unknown endpoints. For more

©2026 Tanium Inc. All Rights Reserved

information, see the Tanium Discover User Guide.

You can use Client Management to continuously monitor the health of installed Clients. Quickly identify outliers and issues by viewing aggregated information for Clients on supported operating systems. Diagnose specific issues with Windows, Linux, and macOS Clients by directly connecting and exploring individualized Client health information. For more information, see Monitor the Client health overview in Client Management on page 284.

Manage the rollout of endpoint tooling, including upgrades to the Tanium Client, using the change management feature in Tanium Endpoint Configuration. For more information, see Endpoint Configuration: Managing Tanium Client and endpoint tool upgrade rollouts.

For an overview of Tanium Client maintenance tasks, see Maintaining Tanium Clients on page 331.

©2026 Tanium Inc. All Rights Reserved

Deploying the Tanium Client

The subsequent topics in this section describe the methods that you can use to deploy the Tanium Client to endpoints and how to verify the installation.

- Deploying using Client Management on page 125
- Deploying using an installer or package file on page 153
- Preparing OS images on page 194
- Using the Microsoft Azure VM extension on page 215
- Verify the Tanium Client installation on page 228

Deploying the Tanium Client using Client Management

Use Client Management to deploy the Tanium Client to any number of endpoints in a single operation. You can optionally use a satellite endpoint to deploy the Tanium Client to endpoints that do not have a direct connection to the Module Server.



Important: If you are using a Tanium Appliance-based deployment with FIPS mode enabled, you must use a satellite for deployment. For more information about FIPS mode, see Enable FIPS 140-3 mode.

To begin, plan and prepare the set of targeted endpoints. If you are using a satellite for deployment, use a third-party deployment tool or manual installation to deploy the Tanium Client to an endpoint that will be configured as the satellite and then configure that endpoint as a satellite. Optionally, if you plan to create multiple deployments with similar settings, create a deployment template. Create a Client deployment with the desired settings and targets, and the credentials needed for the targeted endpoints.

©2026 Tanium Inc. All Rights Reserved

Tip:

- When you use Client Management to deploy the Tanium Client to endpoints, Client Management also installs Client Management tools on the endpoints to provide Client health information. For more information, see Monitor the Client health overview in Client Management on page 284 and Access detailed Client health and troubleshooting information on an endpoint on page 287.
- For information about troubleshooting deployment with Client Management, see Troubleshoot deployment issues on page 388.
- You can also obtain installation packages and install the Client on endpoints using an alternative method. For more information, see Deploying the Tanium Client using an installer or package file on page 153.
- If you use an operating system (OS) image to deploy an OS to new endpoints, you can use Client Management to install the Tanium Client on the template image (as described in this section) and perform additional steps to prepare the Tanium Client for deployment through the image. For the procedures to prepare OS images that include the Tanium Client, see Preparing the Tanium Client on OS images on page 194.

Plan deployment targeting

You can target deployment of the Tanium Client using any of the following methods:

- A single IP address or a list of individual IP addresses
- A single fully qualified domain names (FQDN) or host name, or a list of FQDNs or host names
- A range of IP addresses
- A CIDR range
- A Discover label

©2026 Tanium Inc. All Rights Reserved

Note: In a single deployment, you can target at most 65,536 endpoints, which is the number of endpoints in a /16 subnet.

Both the Tanium Server and endpoints must have IPv4 addresses; IPv6 addresses are not supported in Client ManagementTanium Cloud.

The Tanium Module Server or at least one endpoint in the network must have a connection to targeted endpoints to automatically deploy the Tanium Client using Client Management. If you deploy the Tanium Client to endpoints that cannot be reached directly from the Tanium Module Server, such as those connected to a Zone Server, you can use one of the following deployment methods:

- Deploy the Tanium Client to an endpoint in the network using an installer or package file on page 153, or if at least one endpoint in the network has a connection to the Module Server, you can use a Module Server deployment as described in this topic. Designate that endpoint as a satellite, and configure a satellite deployment. Client Management uses the satellite to automatically deploy the Tanium Client to targeted endpoints.
- Create a deployment template on page 137, download the tanium-init.dat file on page 138, and deploy the Client using an installer or package file on page 153. This method is required if only IPv6 addresses are available.

A host name or fully qualified domain name listed in a deployment must resolve correctly from the Module Server or from a satellite used for the deployment.

If you want to deploy to unmanaged interfaces as they are identified in Discover, you can create a label and use the label as a deployment target. For example, you might create a `New Computers` label with the condition: `First Seen in the last 30 minutes AND Computer Id = "0"`. For more information about creating labels in Discover, see Labels.

©2026 Tanium Inc. All Rights Reserved

Note:

Discover labels must have the following settings to be used with Client Management:

- **Type**: Automatic
- **Activity**: Retain
- **Retain Activity**: Label

By default, a deployment installs the Tanium Client only on unmanaged endpoints and ignores any endpoints where the Client is already installed. However, you can also configure the deployment to reinstall the Client. For more information, see Manage Client deployments on page 136.

(Optional) Prepare a satellite for use with automatic deployment

About this task

You can optionally use a Tanium Client as a satellite for automatic deployment with Client Management. Using a satellite lets you deploy the Tanium Client to endpoints that do not have a direct connection to the Module Server.

Important: If you are using a Tanium Appliance-based deployment with FIPS mode enabled, you must use a satellite for deployment. For more information about FIPS mode, see Enable FIPS 140-3 mode.

An endpoint that you use as a satellite to deploy the Tanium Client must meet certain requirements. For more information, see Requirements for satellites used for Tanium Client deployment in Client Management on page 51.

Important: If FIPS mode is enabled on a Linux satellite, you cannot use that satellite to deploy the Tanium Client to Windows endpoints.

©2026 Tanium Inc. All Rights Reserved

Note: Credentials that are used for Tanium Client installation remain encrypted when they are sent to the satellite. Credentials are never sent using the linear chain, nor are they stored on-disk on the satellite.

1. Use an installer or package file to deploy the Tanium Client to the endpoint that you plan to designate as a satellite. For more information, see Deploying the Tanium Client using an installer or package file on page 153.
   Use a Module Server deployment or an installer or package file to deploy the Tanium Client to the endpoint that you plan to designate as a satellite.

   - For a Module Server deployment, continue with the steps in the following sections. Target the satellite endpoint specifically, and select **Module Server** for the **Deployment method**.
   - For deployment with an installer or package file, see Deploying the Tanium Client using an installer or package file on page 153.

2. Create a satellite in Tanium Direct Connect. For more information, see Managing satellites.
3. (Linux satellites) To enable deployment from a Linux satellite to Windows endpoints, you must install the Samba SMB Client and tools on the satellite. For more information, see the Samba website. Use the appropriate installation method for the specific Linux distribution. For example:
   - AlmaLinux, CentOS, Oracle Linux, Red Hat Enterprise Linux, or Rocky Linux:

     ```
     yum install samba-client samba-common-tools
     ```

   - Debian or Ubuntu:

     ```
     apt install smbclient samba-common-bin
     ```

Prepare for deployment to Linux, macOS, Solaris, or AIX endpoints

1. Ensure that the endpoint meets the basic requirements on page 29 for the Tanium Client.
2. Configure password-based or SSH key-based authentication based on the authentication requirements on the endpoints.
   On each non-Windows endpoint, you must have an account configured that can remotely connect to the endpoint and authenticate with SSH. You must use *one* of the following options to configure a user with elevated privileges to perform installation:

©2026 Tanium Inc. All Rights Reserved

- The root user
- A user that is listed in the sudoers file on each endpoint to allow the account you are using for installation to use sudo

> **Note:**
> - A non-root user must have a password, even when using key-based authentication.
> - If you restrict user commands in the sudoers file, you must allow the commands used by Client Management on page 492 during deployment.

Specific distributions or your specific environment might have specific authentication requirements.

> **Note: Amazon Linux:** Amazon Linux requires key-based authentication. On the endpoint, be sure to enable SSH key-based authentication and enable `NOPASSWD` in the sudoers file for the admin user account. Add this user name and password to the credentials list. This configuration ensures that the key, and not a password, is used to elevate the admin permissions of the user so that the user can install the Tanium Client and start the service.

> **Best Practice:** To protect credentials that are used for Client deployment, use one of the following methods:
> - Use a temporary account that is removed after deployment.
> - Disable or change the password for the account after Client deployment is complete.

3. Allow traffic from the Module Server or satellite endpoint to the endpoints on which you want to deploy the Tanium Client on TCP port 22 (SSH port, configurable), and allow SFTP access. For more information, see Port requirements for Tanium Client and Client Management on page 63.
4. Configure any host-based firewalls or other security tools on endpoints that might interfere with a remote installation that is initiated through SSH, and ensure that host and network

©2026 Tanium Inc. All Rights Reserved

firewalls are configured to allow inbound and outbound TCP traffic on the ports that the Tanium Client uses.. For more information, see Manage macOS firewall rules on page 305, Manage Linux firewall rules on page 308, and Port requirements for Tanium Client and Client Management on page 63.

5. (macOS 10.14 or later only) Create a mobile device management (MDM) profile that provides the necessary permissions for the following Tanium applications.

   Important:
   This step is critical for full support of Tanium Client functionality on macOS 10.14 or later.

Application	Location	Required Permissions	Apple Events
Tanium Client	/Library/Tanium/TaniumClient/TaniumClient	All System Files, Admin System Files, Post Events	System Events, SystemUIServer, Finder
Tanium Client Extensions [1]	/Library/Tanium/TaniumClient/TaniumCX	All System Files, Admin System Files, Post Events	System Events, SystemUIServer, Finder
	/Library/Tanium/TaniumClient/TaniumCX.app	All System Files, Admin System Files, Post Events	System Events, SystemUIServer, Finder
Tanium End-User Notifications	End-User Notifications 1.18.57 or later: /Library/Tanium/EndUserNotifications/bin/Launcher.app Earlier versions: /Library/Tanium/EndUserNotifications/bin/end-user-notifications.app	Post Events	System Events, SystemUIServer, Finder

[1] On endpoints running the universal Tanium Client binary, you must specify both of the locations listed for Tanium Client Extensions. On endpoints running the x86-64 Tanium Client binary, you do not need to specify /Library/Tanium/TaniumClient/TaniumCX.app . Tanium recommends the universal binary for all Mac computers running macOS 11 or later. For more information, see Client version and operating system requirements on page 29 .

An MDM administrator must create a PPPC custom payload that specifies the necessary permissions for each application. The PPPC custom payload must be delivered using a User-

©2026 Tanium Inc. All Rights Reserved

Approved MDM (UAMDM) payload in a device profile.

The team identifier for Tanium applications is TZTPM3VTUU.

Important: If you previously created a PPPC custom payload for a version of the Tanium Client earlier than 7.2.314.3608, you must update the code signing requirement for newer versions of the Tanium Client.

For more information about MDM on macOS, see Apple Platform Deployment.

6. (Solaris 11.4 only) Install the legacy **pkgadd** utilities:
    a. Access the endpoint CLI.
    b. Find the **pkgadd** IPS package name:

```
pkg search pkgadd
```

```
INDEX       ACTION VALUE       PACKAGE
basename    file                    usr/sbin/pkgadd pkg:/package/
svr4@11.4-11.4.6.0.1.4.0
```

    c. Install the **pkgadd** utilities:

```
pkg install pkg:/package/svr4@11.4-11.4.6.0.1.4.0
```

7. (Solaris 10 or 11.0–11.3 only) Install the **SUNWgccruntime** package if it is not yet installed.

Note: Although this package is part of a default Solaris installation, some organizations omit it in their standard image.

    a. Determine whether the package is installed:

```
pkginfo -l SUNWgccruntime
```

The following example output indicates the package is installed:

```
PKGINST:  SUNWgccruntime
NAME:  GCC Runtime libraries
CATEGORY:  system
ARCH:  sparc
VERSION:  11.11.0,REV=2010.05.25.01.00
BASEDIR:  /
```

©2026 Tanium Inc. All Rights Reserved

```
VENDOR:  Oracle Corporation
DESC:  GCC Runtime - Shared libraries used by gcc and other gnu components
INSTDATE:  Dec 01 2015 11:43
HOTLINE:  Please contact your local service provider
STATUS:  completely installed
```

b. If the **SUNWgccruntime** package is not yet installed, run one of the following commands:
   - Solaris 10 or 11.0–11.3 (without using Image Packing System [IPS]):

     ```
     # pkgadd -d /path/to/SUNWGccruntime.pkg SUNWgccruntime
     ```

   - Solaris 11.0–11.3 using IPS:

     ```
     # pkg install SUNWgccruntime
     ```

8. (AIX only) If they are not yet installed, install the IBM XL C++ runtime libraries file set (xlC.rte), version 16.1.0.0 or later, and the IBM LLVM runtime libraries file set (libc++.rte).
   Install the file sets as follows:

   a. Access the operating system CLI on the endpoint.
   b. Run the following commands to determine the versions of the currently installed xlC.rte bundle and the libc++.rte bundle:

      ```
      lslpp -l xlC\.*
      lslpp -l libc++\.*
      ```

      If the appropriate version of each bundle is already installed, skip to Install the Tanium Client on AIX using the command line on page 191. Otherwise, complete the remaining steps for each bundle that needs to be installed or updated.

   c. Obtain the appropriate xlC.rte and libc++.rte bundles for your system from IBM Fix Central.
   d. Download each bundle to your endpoint.
   e. Extract, unzip, or untar each bundle to the /usr/sys/inst.images directory.
   f. Install the bundles:

      ```
      sudo installp -aXYgd /usr/sys/inst.images -e /tmp/install.log all
      ```

   g. Review the installation log /tmp/install.log for any errors.

©2026 Tanium Inc. All Rights Reserved

9. If you use the root account to install, make sure the sshd_config allows root login.
10. Verify that you can log in to the remote system with SSH, using the same credentials that you will use for the Tanium Client deployment.

Prepare for deployment to Windows endpoints

1. Ensure that the endpoint meets the basic requirements on page 29 for the Tanium Client.
2. Perform any necessary configuration or updates for Windows features:
    - Ensure that VBScript execution using Windows Script Host (WSH) is unrestricted. VBScript execution using WSH is required for installation and operation of the Tanium Client.
    - Ensure that Windows Management Instrumentation (WMI) queries and PowerShell are unrestricted. Some Tanium content requires unrestricted access to these features. If you restrict either of these features, Tanium functionality is limited.
    - (Windows Server 2008 R2 or Windows 7 only) Update PowerShell to version 3.0 or later. PowerShell 3.0 or later is required for PowerShell-based sensors to work on Windows endpoints.
    - Ensure that all PowerShell-based content provided by Tanium is allowed to run in `FullLanguage` mode. Forcing all PowerShell instances to run in a different mode (such as configuring the `__PSLockdownPolicy` environment variable to specify `ConstrainedLanguage` mode) is not supported.
    - Ensure that if the **Turn on Script Execution** Group Policy setting is configured, it is not disabled, nor enabled with the **Allow only signed scripts** execution policy setting configured. For PowerShell-based content to run properly, this Group Policy setting must be either omitted, or if configured, enabled and configured with the **Allow all scripts** or **Allow local scripts and remote signed scripts** execution policy setting.
3. Configure local or domain accounts with the necessary permissions.
   On each Windows endpoint, you must have an account with Local Administrator rights or a local or domain account configured that has the following abilities:
    - Remotely connect to the endpoint and authenticate with SMB

©2026 Tanium Inc. All Rights Reserved

- Create folders within the installation directory for 32-bit applications, and, if applicable, the custom location where the Tanium Client will be installed (by default, C:\Program Files (x86)\ for 64-bit versions of Windows, or C:\Program Files\ for 32-bit versions of Windows)

  Note: A custom installation directory must be located on drive C for deployment with Client Management. To install Tanium Client on a different drive, you must use an alternative deployment method. For more information, see Deploying the Tanium Client using an installer or package file on page 153.

- Write and execute files in the Tanium installation directory (by default, C:\Program Files (x86)\Tanium\ for 64-bit versions of Windows, or C:\Program Files\Tanium\ for 32-bit versions of Windows)

Best Practice: To protect credentials that are used for Client deployment, use one of the following methods:

- Use a temporary account that is removed after deployment.
- Disable or change the password for the account after Client deployment is complete.

4. Enable Windows file-and-print sharing and administrative shares on the target endpoint, and make sure the Windows Management Instrumentation (WMI) service is enabled and started.

   Tip: Enabling these settings and services is required only for installation. You can disable sharing and WMI as needed after the installation.

5. Configure any host-based firewalls or other security tools on the endpoint that might interfere with WMI, which uses port 135, or file sharing, which uses port 445. Additionally, ensure that host and network firewalls are configured to allow inbound and outbound TCP traffic on the ports that the Tanium Client uses. For more information, see Port requirements for Tanium Client and Client Management on page 63.

6. Allow TCP traffic on ports 135 and 445 from the Module Server or satellite endpoint to endpoints on which you want to deploy the Tanium Client. For more information, see Port requirements for Tanium Client and Client Management on page 63.

©2026 Tanium Inc. All Rights Reserved

7. If both of the following conditions are met, User Account Control (UAC) remote restrictions prevent access to administrative shares and remote installations:
    - The endpoint is not joined to a domain.
    - You use a non-default Administrator account, or you use the default local Administrator account with the **Admin Approval Mode for the Built-in Administrator account** policy setting enabled.

    Because these administrative tasks are necessary for deployment of the Tanium Client using Client Management, you must disable UAC remote restrictions under these conditions to allow deployment. To disable UAC remote restrictions, add the following value to the Windows registry and restart the machine:

    ```
    Subkey: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System
    Data type: REG_DWORD
    Value name: LocalAccountTokenFilterPolicy
    Value data: 1
    ```

    Important: Administrative shares are not available in Home editions of Windows operating systems.

    Best Practice: After you deploy the Tanium Client, remove the `LocalAccountTokenFilterPolicy` registry value or set it to `0` to restore UAC remote restrictions. These restrictions help prevent malicious users from accessing the endpoint remotely with administrative rights.

8. Verify that you can execute the `wmic` and `net use` commands remotely on a targeted endpoint with the same administrator credentials that you will use for the Tanium Client deployment. For example:
    - Port 135: `wmic /node:"endpoint_fqdn_or_ip_address" /user:"admin_user_name_on_endpoint" useraccount list brief`
    - Port 445: `net use p: \\endpoint_fqdn_or_ip_address\C$ admin_password_on_endpoint /user:admin_user_name_on_endpoint`

Manage Client deployments

©2026 Tanium Inc. All Rights Reserved

You configure a Client deployment to deploy the Tanium Client to a group of endpoints identified by computer names, IP addresses, a CIDR range, or a Discover label. As appropriate for your deployment workflow, you can create a Client deployment from scratch, or you can create a Client deployment template to quickly configure future deployments.

(OPTIONAL) CREATE A CLIENT DEPLOYMENT TEMPLATE

About this task

Create a Client deployment template to quickly configure future deployments.

Tip: You can also save a newly configured Client deployment as a template for future use. For more information, see Deploy Clients on page 138.

1. From the Main menu, go to **Shared Services >** Client Management.
2. Go to **Client Installations** > **Client Deployment Templates**, and then click **Create Client Deployment Template**.
3. Enter a **Name** and optionally a **Description** for the template.
4. Configure Client deployment settings as detailed in General Client deployment settings on page 143.
5. Click **Save**.

(OPTIONAL) DESIGNATE A TEMPLATE AS THE DEFAULT

About this task

Designate a template as the default to automatically populate newly created Client deployments with the settings from the template.

1. From the Main menu, go to **Shared Services >** Client Management.
2. Go to **Client Installations** > **Client Deployment Templates**.
3. In the row for a template, click Actions and select **Set as Default**.
   To remove a default template and return to the built-in default settings for newly created

©2026 Tanium Inc. All Rights Reserved

Client deployments, click Actions ⋮ in the row for the default template and select **Remove as Default**.

(OPTIONAL) DOWNLOAD A TANIUM-INIT.DAT FILE FOR ALTERNATIVE DEPLOYMENT

About this task

For endpoints where you want to use manual deployment, you can download the tanium-init.dat that contains the **ServerNameList** setting configured in a Client deployment template. It also includes **ServerPort**, **LogLevel**, and any other Client settings and tags that you added to the Client deployment template, which the installer for Tanium Client automatically applies during installation. Using this file reduces the manual configuration steps when you deploy the Tanium Client outside of Client Management.

1. From the Main menu, go to **Shared Services >** Client Management.
2. Go to **Client Installations** > **Client Deployment Templates**.
3. In the row for a template, click Actions ⋮ and select **Download tanium-init.dat**.
4. Deploy Tanium Client using the appropriate installer or package file and the tanium-init.dat file you downloaded. For more information, see Deploying the Tanium Client using an installer or package file on page 153.

DEPLOY CLIENTS

About this task

Create a Client deployment from scratch or from a template to target endpoints and deploy the Tanium Client. You can create a one-time or a recurring deployment, and you can start it immediately or schedule it for a later time.

1. From the Main menu, go to **Shared Services >** Client Management.
2. Go to **Client Installations** > **Client Deployments**, and then click **Create Client Deployment**.

©2026 Tanium Inc. All Rights Reserved

> **Tip:** You can also clone an existing deployment. On the **Client Deployments** page, click the name of a deployment, and then click **Clone**. A cloned deployment includes all settings from the original deployment except for **Name** and **Description**; make sure to change settings as needed.

3. (Optional)To create the deployment from an existing Client deployment template, click **Apply Deployment Template** and select a template.

   > **Note:** If a template is designated as the default on page 137, the settings from that template are already applied.

4. Enter a **Name** and optionally a **Description** for the deployment.

5. Configure the Client deployment settings.
   - Configure the **Deployment Details**:

     > **Tip:** Click Edit  in a section that is not open for editing if you need to make changes.

Section	Setting	Description
Deployment Schedule	Deployment Type	Select **One-Time** for a deployment that you want to run once, or **Recurring** for a deployment that you want to automatically repeat. **Tip:** A recurring deployment appears on the **Scheduled Client Deployments** page and automatically creates individual one-time deployments according to the configured schedule. The individually created one-time deployments appear on the **Client Deployments** page.
	Recurrence Interval	Recurring deployments only: Specify the interval between each recurrence of the deployment.
	Deployment Time Zone	Select the time zone that applies for the deployment. This time zone applies to the **Start Time** and **End Time** if they are set for the deployment.
	Start Time	To start the deployment immediately, clear the selection for **Specify Start**

©2026 Tanium Inc. All Rights Reserved

Section	Setting	Description
		Time . To schedule the deployment to start at a later time, select **Specify Start Time** and configure a time. **Note:** The start time must be within 31 days. **Tip:** A scheduled one-time deployment appears on the **Scheduled Client Deployments** page and automatically creates an individual one-time deployment at the configured start time. Recurring deployments also appear there and automatically create individual one-time deployments according to the configured schedule. If you do not configure a start time for a recurring deployment, it is still classified as a scheduled deployment, and it uses the time at which you create the deployment as the start time. The individually created one-time deployments appear on the **Client Deployments** page.
	End Time	Recurring deployments only: To repeat the deployment indefinitely, clear the selection for **Specify End Time** . To stop repeating the deployment after a specific time, select **Specify End Time** and configure a time. **Note:** The end time must be within one year.
Endpoints to target	Targeting Method	Select a targeting method, and enter a list of IP addresses, a list of FQDNs or host names, an IP or CIDR range, or a Discover label. For information about configuring Discover labels, see Labels . **Note:** Discover labels must have the following settings to be used with Client Management: • **Type**: Automatic • **Activity**: Retain • **Retain Activity**: Label

©2026 Tanium Inc. All Rights Reserved

Section	Setting	Description
		To define an additional target for the deployment, click **Add Target** . To remove a target, click Delete .
Endpoint credentials	Credentials to Authenticate with Targeted Endpoints	Add credential sets to try for the targeted endpoints. Each credential set is saved as a separate item that you can update at a later time as necessary. • If you are targeting Windows endpoints, configure each Windows credential combination to be tried during the deployment. a. Click **+ Windows Credential Set**. b. Enter a **Name** for the credential set. c. Enter the **Username** and, as necessary, the **Domain** and **Password** for the account. d. Click **Save**. • If you are targeting non-Windows endpoints, configure each non-Windows credential combination to be tried during the deployment. a. Click **+ Non-Windows Credential Set**. b. Enter a **Name** for the credential set. c. Enter the **Username** and, as necessary, the **Domain**, **Password**, **SSH Key**, and **Keyphrase** for the account. **Note:** If you are using an SSH key, the private key is required in PEM format. Copy the contents of the PEM-formatted private key, paste the contents in the **SSH Key** field, and enter the passphrase in the **Keyphrase** field. When you use an SSH key for authentication, a user name is required, and a password is optional. However, endpoints typically still require a password for non-root users, unless the specified user is configured to use `sudo` without a password. d. Click **Save**.

©2026 Tanium Inc. All Rights Reserved

Section	Setting	Description
		Tip: For specific requirements for authentication and permissions, see Account permissions for Client Management on page 59.
Deployment method	Deployment Method	Select **Satellite** or **Tanium Module Server**. If you select **Satellite**, select the satellite you configured to use for deploying the Tanium Client. If you need to configure a satellite, see (Optional) Prepare a satellite for use with automatic deployment on page 128. **Note:** You can select still a supported satellite if its last known status is offline. In this case, the deployment will still try to connect, but the satellite must be back online for the deployment to proceed. **Important:** If FIPS mode is enabled on a Linux satellite, you cannot use that satellite to deploy the Tanium Client to Windows endpoints. **Important:** If you are using a Tanium Appliance-based deployment with FIPS mode enabled, you must use a satellite for deployment. For more information about FIPS mode, see Enable FIPS 140-3 mode.

- Complete the **Deployment Configuration** as detailed in General Client deployment settings on page 143. If you started from a template, edit these settings only as necessary.

6. (Optional) To save the deployment settings as a Client deployment template from which you can easily create similar deployments, click **Save Settings as New Template**. Enter a **Template Name**, and click **Save**.
7. Review the **Deployment Summary**. To deploy the Client to the targeted endpoints, click **Deploy**.

©2026 Tanium Inc. All Rights Reserved

Note:

- Immediate, one-time deployments: You can delete deployments, but you cannot edit a Client deployment after you click **Deploy**. If you want to use similar settings in multiple deployments, you can save the settings as a template. If a deployment has incorrect settings, you can stop it if it is still in progress, clone it, make corrections to the new deployment, and then optionally delete the old deployment.
- Scheduled or recurring deployments: Scheduled or recurring deployments automatically create individual one-time deployments at the scheduled time and, if applicable, according to the recurrence schedule. You can edit a one-time scheduled deployment that has not occurred yet or a recurring deployment that is ongoing, which will update the settings for the future one-time deployments that it creates. You cannot edit the automatically created one-time deployments, but you can stop them if they are still in in progress.

After a deployment is complete, wait a few minutes for the Tanium Client to register with the Tanium Server or Zone Server, and then verify that the Client installed correctly and is communicating properly. For more information, see Verify the Tanium Client installation on page 228.

GENERAL CLIENT DEPLOYMENT SETTINGS

The following settings are often configured the same for multiple deployments. You can optionally configure these settings in a Client deployment template.

Section	Setting	Description
Content to deploy	Client Version	Select the version of the Tanium Client to install.

©2026 Tanium Inc. All Rights Reserved

Section	Setting	Description
		Important: Each version of the endpoint toolset includes a specific version of the Tanium Client, which must be installed with the toolset to maintain a supported configuration. Endpoints with versions of the Tanium Client older than the associated toolset are unsupported. Deployment of previous versions of the Tanium Client is provided for temporary support of legacy deployments. For more information, see Managing Tanium Client and endpoint tool upgrade rollouts . **Tip:** To manage the Client versions that are available for this setting, see Manage versions of the Tanium Client available for legacy deployments on page 115 .
Method settings	SSH Ports	Enter the SSH port to use for deployment to non-Windows endpoints. The default port is 22. **Important:** Make sure that any firewalls or security applications do not block the specified port.
	Retry Delay	Enter the delay between connection retries to a single endpoint during the deployment. The value for this setting must be between 5 seconds and 15 minutes.
	Retry Limit	Enter the maximum number of attempts to make a connection to a single endpoint during the deployment. The maximum value for this setting is 30.
	Installation Limit	Enter the maximum number of concurrent installations during the deployment. The maximum value for this setting is 300.
	File Transfer Timeout	Enter the time-out for file transfers during the deployment. The maximum value for this setting is 60 minutes.
	Installation Validation Retry Limit	Enter the maximum number of attempts to check the health of a newly installed Tanium Client to validate the installation. The value for this setting must be between 3 and 75.
	Verbose Logging	If you need to troubleshoot Client installation issues, select **Enable verbose logging for Client installations on targeted endpoints** .

©2026 Tanium Inc. All Rights Reserved

Section	Setting	Description
		Tip: To view the installation log, see View the deployment status and endpoint installation logs on page 150 .
	Skip Certificate Verification	Skip verification of the required trusted root certificates on endpoints prior to installation of the Tanium Client. **Important:** Endpoints cannot verify the Tanium Client installer signature when this option is selected. **Best Practice:** Do not enable this setting unless you have a critical need to deploy the Tanium Client to endpoints that do not yet have the required trusted root certificates. If you enable this setting for that purpose, install the required certificates as soon as possible.
Installation options	Installation Directory on Windows	(Optional) Enter a custom installation directory for Windows endpoints. Leave blank to use the default installation directory on page 490 . **Important:** • You must specify an installation directory on a local fixed drive on each endpoint. A volume mounted in a directory on another volume is not supported. • The installation directory must be located on drive C for deployment with Client Management. To install Tanium Client on a different drive, you must use an alternative deployment method. For more information, see Deploying the Tanium Client using an installer or package file on page 153.
	Installation Directory on non-Windows	(Optional) Enter a custom installation directory for non-Windows endpoints. Leave blank to use the default installation directory on page 490 .

©2026 Tanium Inc. All Rights Reserved

Section	Setting	Description
		Important: • The installation directory must be located on a local fixed drive on each endpoint. • (macOS endpoints) You cannot customize the installation directory on macOS. The fixed installation directory for macOS is /Library/Tanium/TaniumClient.
	Space Required (Windows)	(Optional) Enter the disk space that should be available on a targeted Windows endpoint for the Client to be installed. **Note:** The default of 3000 MB is sufficient for the Tanium Client itself, but the total space required depends on the modules that you use with each endpoint. For more information, see Hardware requirements on page 45 .
	Space Required (non-Windows)	(Optional) Enter the disk space that should be available on a targeted non-Windows endpoint for the Client to be installed. **Note:** The default of 3000 MB is sufficient for the Tanium Client itself, but the total space required depends on the modules that you use with each endpoint. For more information, see Hardware requirements on page 45 .
	Endpoints without the Tanium Client	To install the Client on unmanaged endpoints, select **Install Tanium Client** . **Tip:** This setting is enabled in a typical deployment. You might disable this setting if you are creating a deployment to specifically to reinstall the Tanium Client on endpoints that are already managed.
	Endpoints with an Installed Tanium Client	Select one of the following options: • **No action to endpoint:** Ignore endpoints where the Client is already installed. Select this option for a typical deployment to unmanaged endpoints. • **Install if newer Tanium Client version:** Install the version that you specified in the selected Client Configuration only on endpoints where an earlier version is currently installed.

©2026 Tanium Inc. All Rights Reserved

Section	Setting	Description
		Best Practice: For general management of upgrades to existing Clients, use the change management feature in Endpoint Configuration. To do so, you must enable Tanium Client upgrades in the upgrade ring configuration. For information about enabling this setting and managing upgrade rings and toolset promotions, see Managing Tanium Client and endpoint tool upgrade rollouts. If you do not use this feature, or if you need to upgrade the Tanium Client in upgrade rings for which Client upgrades are not yet enabled, use upgrade deployments that target computer groups to upgrade existing Tanium Clients. For more information, see Upgrade Tanium Clients using Client Management on page 346. • **Reinstall Tanium Client:** Reinstall existing Clients. Use this option to repair disabled or corrupt Clients. This selection provides additional options: **Clear Existing Data** and **Overwrite Connected Clients**. If neither of these options is selected, Client Management reinstalls Clients only on endpoints where the Client is not communicating properly with the Tanium Server and where the currently installed version is earlier than or the same as the version that you configure in a Client Configuration. Any data that the Client has collected remains on the Client. Select **Clear Existing Data** to wipe all Client data. If you select this option, the version that you deploy replaces *any* existing version, since the deployment first removes any version of the Client found on the endpoint. Select **Overwrite Connected Clients** to reinstall Clients that are still communicating with the Server. **Note:** macOS: If you are installing the universal version of the macOS client on an endpoint where the x86-64 version of the Client is installed, you must select **Clear Existing Data**. **Important:** Windows: If anti-tamper is enabled on a Windows endpoint, reinstallation through Client Management is not possible on that endpoint. You must disable anti-tamper on the endpoint before reinstalling the Tanium Client. For more information, see Manage tamper protection on page 294.
Client options	Server Names	Fully qualified domain names (FQDNs) or IP addresses of the Tanium Servers. In a deployment with Zone Servers, add their FQDNs or IP addresses. Use a comma to separate the entry for each Server. If you include a port for a listed Server by appending `: <port_number>` to the Server address, it

©2026 Tanium Inc. All Rights Reserved

Section	Setting	Description
		overrides the port specified for the **Server Port** setting. You can configure the default value for this setting. For more information, see Configure the default Server names and Server port for Tanium Client deployments on page 114.  **Best Practice:** Specify FQDNs for the **Server Names** setting.
	Server Port	The port that the Tanium Client uses for communication with the Tanium Server and with peers. You can configure the default value for this setting. For more information, see Configure the default Server names and Server port for Tanium Client deployments on page 114.
	Proxy	If deployed Clients must connect through a proxy server, select one of the following options: • **PAC file** (Windows endpoints only): Use a PAC file to configure the proxy on endpoints. Selecting this option automatically adds the **ProxyAutoConfigAddress** Client setting. Configure the URL of the PAC file for the value. • **Proxy server**: Use specific addresses to connect endpoints through a proxy server. Selecting this option automatically adds the **ProxyServers** Client setting. Configure the addresses of proxy servers for the value. Alternatively, to detect the proxy configuration in the registry on Windows endpoints, include the **ProxyAutoDetect** setting as a key with a value of `1` in **Client Settings**. For more information about using a proxy server, see Connect through an HTTPS forward proxy server on page 238.
	Log Level	(Optional) Enter a log level for the Tanium Client on targeted endpoints. The following values are best practices for specific scenarios: • `1` (default): Use this value during normal operation. • `41`: Use this value during troubleshooting. • `91` or higher: Use this value for full logging, for short periods of time only.  **Note:** A value of `0` disables logging. As a best practice, do not disable logging.  **Note:** This value does not affect the verbosity of the Client installation log during deployment. For troubleshooting Client installations, enable the Verbose Logging on page 144 setting.

©2026 Tanium Inc. All Rights Reserved

Section	Setting	Description
	Client Settings	(Optional) To change a default Client setting, click **Add Client Setting**, and then enter a **Key** and **Value**. For information about specific Client settings, see Tanium Client settings reference on page 393. **Note:** • If you selected **PAC file** for the **Proxy** setting, do not delete the **ProxyAutoConfigAddress** Client setting. If you selected **Proxy server** for the **Proxy** setting, do not delete the **ProxyServers** Client setting. • If you are deploying the Tanium Client to virtual desktop infrastructure (VDI) instances or other endpoints with limited resources, you might need to adjust certain Client settings to help to reduce resource usage. For more information, see Tuning Tanium Client settings for VDI endpoints and other endpoints with limited resources on page 407.
	Custom Tags	(Optional) To add a custom tag to the Client during deployment, click **Add Custom Tag** and enter a tag name. The `InstalledByTCM` tag is included by default so that you can later easily target Clients that were installed using Client Management. **Note:** Do not include spaces in a tag name.

DEPLOYMENT PROCESS

When you start a deployment, Tanium takes the following actions to install the Tanium Client:

1. Pings the targeted endpoints to verify they are online.
2. Detects the operating system of the endpoints that respond to the ping.
3. Tries the credentials that are associated with the deployment to log into the endpoint for installation.
4. Checks for the space required on the endpoint as specified in the deployment configuration.
5. Copies the Tanium public key file for the Tanium Server to the endpoint.

©2026 Tanium Inc. All Rights Reserved

6. Installs Tanium Client on the endpoint. The version and installation location are defined in the deployment configuration.

7. Displays the deployment status.

VIEW THE DEPLOYMENT STATUS AND ENDPOINT INSTALLATION LOGS

About this task

You can view the status of the deployment on each targeted endpoint while the deployment is running or the final results after the deployment completes. For a recurring deployment, this status applies to each automatically created one-time deployment.

1. From the Main menu, go to **Shared Services >** Client Management.
2. Go to **Client Installations** > **Client Deployments**, and then click the name of the deployment you want to view.

   Tip: This page contains one-time deployments you created to run immediately, as well as the one-time deployments that Client Management creates automatically for a scheduled deployment and for each occurrence of a recurring deployment.

3. In the **Endpoint details** section view the list of targeted endpoints with status information. Each successful deployment reports a status of `COMPLETE` in the **Installation Status** column. Use the **Filter items** box to find specific endpoints, or sort the table by the desired column to help find endpoints with a particular installation status or result.
4. (Optional) To view the installation log for an endpoint, click Endpoint Details in the row for the endpoint.

   Tip: To help troubleshoot installation issues, you can increase the verbosity of the installation log. Enable the Verbose Logging on page 144 setting, and then reissue the deployment on page 151.

   After the deployment is complete, wait a few minutes for the Tanium Client to register with the Tanium Server or Zone Server, and then verify that the Client installed correctly and is communicating properly. For more information, see Verify the Tanium Client installation on page 228.

©2026 Tanium Inc. All Rights Reserved

REISSUE A DEPLOYMENT

About this task

You can reissue a deployment when necessary. For example, you might reissue a deployment in which some endpoints were offline during the initial deployment, or you might regularly reissue a deployment that targets a Discover label that identifies new unmanaged endpoints or disconnected Clients on page 332.

> **Note:** You cannot reissue a deployment that you created before you upgraded to Client Management 2.1 or later. You must clone the migrated deployment to a new deployment or template. For more information, see Cloning Client deployments migrated from versions earlier than 2.1 on page 107.

1. From the Main menu, go to **Shared Services >** Client Management.
2. Go to **Client Installations** > **Client Deployments**, and then click the name of the deployment you want to reissue.
3. Click **Reissue**.

MANAGE SCHEDULED OR RECURRING DEPLOYMENTS

To review scheduled deployments or recurring deployments, from the Client Management menu, click **Client Installations** > **Scheduled Client Deployments**.

This list includes both one-time deployments with a scheduled start time and recurring deployments.

Stop or Delete a scheduled or recurring deployment

1. On the **Scheduled Client Deployments** page, click the name of the scheduled deployment you want to stop.
2. On the page for the scheduled deployment, click **Stop**.
3. (Optional) To delete the scheduled deployment, click Delete .

©2026 Tanium Inc. All Rights Reserved

Edit a scheduled or recurring deployment

1. On the **Scheduled Client Deployments** page, click the name of the scheduled deployment you want to edit.
2. On the page for the deployment, click Edit for the section that contains the setting you want to edit, and update the setting. For more information, see Deploy Clients on page 138 and General Client deployment settings on page 143.
3. Review the **Deployment Summary**. To resume the scheduled deployment with updated settings, click **Deploy**.

   Note: Scheduled or recurring deployments automatically create individual one-time deployments at the scheduled time and, if applicable, according to the recurrence schedule. When you edit a one-time scheduled deployment that has not occurred yet or a recurring deployment that is ongoing, it updates the settings for the future one-time deployments that it creates. You cannot edit the automatically created one-time deployments, but you can stop them if they are still in in progress.

MANAGE ENDPOINT CREDENTIALS

You can edit or remove credential sets that you created while configuring Client deployments, or you can separately create new credential sets that you can use in deployments.

Tip: For specific requirements for authentication and permissions, see Account permissions for Client Management on page 59.

Best Practice: To protect credentials that are used for Client deployment, use one of the following methods:

- Use a temporary account that is removed after deployment.
- Disable or change the password for the account after Client deployment is complete.

©2026 Tanium Inc. All Rights Reserved

Add a Windows credential set

1. Click **Create** > **Create Windows Credential Set**.
2. Enter a **Name** for the credential set.
3. Enter the **Username** and, as necessary, the **Domain** and **Password** for the account.
4. Click **Save**, and then select the newly created credential set from the list.

Add a non-Windows credential set

1. Click **Create** > **Create Non-Windows Credential Set**.
2. Enter a **Name** for the credential set.
3. Enter the **Username** and, as necessary, the **Domain**, **Password**, **SSH Key**, and **Keyphrase** for the account.

   > **Note:** If you are using an SSH key, the private key must be in PEM format. Copy the contents of the PEM-formatted private key, paste the contents in the **SSH Key** field, and enter the passphrase in the **Keyphrase** field. When you use an SSH key for authentication for a non-root user, a password is still required. When you use an SSH key for authentication for the root user, a password is optional, depending on whether it is required on endpoints.

4. Click **Save**, and then select the newly created credential set from the list.

Edit or delete existing credential sets

To edit a credential set, click Edit in the row for the credential set.

To delete a credential set, click Delete in the row for the credential set.

Deploying the Tanium Client using an installer or package file

If you are deploying the Tanium Client to endpoints that cannot be reached directly from the Tanium Module Server, such as those connected to a Zone Server, or if your organization has a preferred standard software package deployment tool, you can use an installer or package file to deploy the Tanium Client.

©2026 Tanium Inc. All Rights Reserved

Best Practice: Use Client Management to create a Client deployment template and then download the tanium-init.dat file for use in alternative deployment. The tanium-init.dat file that is contained in this bundle includes the **ServerNameList**, **ServerPort**, **Log Level**, and any other Client settings and tags from the Client Configuration. For the procedure, see (Optional) Create a Client deployment template on page 137 and (Optional) Download a tanium-init.dat file for alternative deployment on page 138.

Note: You can also deploy the Tanium Client using the Client Management service. For more information, see Deploying the Tanium Client using Client Management on page 125.

Note: If you are deploying the Tanium Client to virtual desktop infrastructure (VDI) instances or other endpoints with limited resources, you might need to adjust certain Client settings to help to reduce resource usage. For more information, see Tuning Tanium Client settings for VDI endpoints and other endpoints with limited resources on page 407.

Tip: If you use an operating system (OS) image to deploy an OS to new endpoints, you can install the Tanium Client on the template image (as described in this section) and perform additional steps to prepare the Tanium Client for deployment through the image. For the procedures to prepare OS images that include the Tanium Client, see Preparing the Tanium Client on OS images on page 194.

The subsequent topics in this section detail using a package to install the Tanium Client on each operating system.

- Deploy to Windows on page 155
- Deploy to macOS on page 165
- Deploy to Linux on page 173
- Deploy to Solaris on page 181
- Deploy to AIX on page 188

Download installation packages for the Tanium Client

About this task

©2026 Tanium Inc. All Rights Reserved

Download Tanium Client installation packages for each operating system from the Tanium **Client Management Overview** page:

1. From the Main menu, go to **Shared Services** > **Client Management**.
2. In the **Deploy the Tanium Client** section of the Tanium **Client Management Overview** page, click **Download Installers**, and select an installation package to download.

   Tip: The available installers are based on the available Tanium Client versions you have configured. If you have recently updated the available Tanium Client versions on page 115 and the installers have not yet automatically updated, you can click **Refresh Installers** to initiate the update.

Deploy the Tanium Client to Windows endpoints using the installer

You can use the installation wizard on page 158, Client command-line interface (CLI) on page 159, or third-party software distribution tools, such as System Center Configuration Manager (SCCM), to deploy the Tanium Client to Windows endpoints. For more information about using a third-party tool with Tanium installers, see the documentation for that tool.

Tip: If you encounter issues when deploying the Tanium Client, examine the Tanium Client installation log on page 357.

All these deployment methods use the Tanium Client installer SetupClient.exe, which makes the following changes to the target endpoints:

- Creates the Tanium Client installation directories on page 490 for the Client application files and related content files.
- Creates the Tanium Client Windows registry on page 491 key along with an initial set of registry values.
- Adds the Tanium Client program to the Windows **Add/Remove Programs** list.
- Creates the Tanium Client service with a **Startup Type** set to **Automatic**.

©2026 Tanium Inc. All Rights Reserved

For information about managing the Tanium Client service or uninstalling the Tanium Client after deployment, see Manage the Tanium Client on Windows on page 293.

Related information

- Manage the Tanium Client on Windows on page 293
- Preparing the Tanium Client on a Windows OS image on page 194
- Uninstall the Tanium Client on Windows on page 351
- Client version and operating system requirements on page 29
- Managing Client settings and Index configurations on page 318
- Tanium Client settings reference on page 393

PREPARE FOR INSTALLATION

1. Ensure that the endpoint meets the basic requirements on page 29 for the Tanium Client on Windows.
2. Perform any necessary configuration or updates for Windows features:
    - Ensure that VBScript execution using Windows Script Host (WSH) is unrestricted. VBScript execution using WSH is required for installation and operation of the Tanium Client.
    - Ensure that Windows Management Instrumentation (WMI) queries and PowerShell are unrestricted. Some Tanium content requires unrestricted access to these features. If you restrict either of these features, Tanium functionality is limited.
    - (Windows Server 2008 R2 or Windows 7 only) Update PowerShell to version 3.0 or later. PowerShell 3.0 or later is required for PowerShell-based sensors to work on Windows endpoints.
    - Ensure that all PowerShell-based content provided by Tanium is allowed to run in `FullLanguage` mode. Forcing all PowerShell instances to run in a different mode (such as configuring the `__PSLockdownPolicy` environment variable to specify `ConstrainedLanguage` mode) is not supported.
    - Ensure that if the **Turn on Script Execution** Group Policy setting is configured, it is not disabled, nor enabled with the **Allow only signed scripts** execution policy setting configured. For PowerShell-based content to run properly, this Group Policy setting must be either omitted, or if configured, enabled and configured with the **Allow all scripts** or **Allow local scripts and remote signed scripts** execution policy

©2026 Tanium Inc. All Rights Reserved

setting.

3. Ensure that host and network firewalls are configured to allow inbound and outbound TCP traffic on the ports that the Tanium Client uses. For more information, see Network connectivity, ports, and firewalls on page 63.

4. Sign in to the target endpoint with a local user or domain account that has administrative permissions.

5. Use the Tanium Client Management service to download the Client installer bundle to the Windows endpoint. From the Client Management **Overview** page, click **Download Installers > Download Windows Package**.
   The bundle (windows-client-bundle.zip) contains the following files:

   - install.bat
   - SetupClient.exe

6. Download the tanium-init.dat file from a Client Deployment Template in the Tanium Client Management service:
   a. From the Main menu, go to **Shared Services >** Client Management.
   b. Go to **Client Installations > Client Deployment Templates**.
   c. In the row for a template, click Actions and select **Download tanium-init.dat**.
   d. Deploy Tanium Client using the appropriate installer or package file and the tanium-init.dat file you downloaded. For more information, see Deploying the Tanium Client using an installer or package file on page 153.

Tip: You must create a Client Deployment Template in Client Management before performing this step. For more information, see (Optional) Create a Client deployment template on page 137.

Best Practice: Download the tanium-init.dat file for a Client Deployment Template in Client Management. Though you can also download tanium-init.dat through Tanium Console without creating a Client Deployment Template (see Download infrastructure configuration files (keys)), the installation process requires fewer manual configuration steps if you use these steps.

©2026 Tanium Inc. All Rights Reserved

Important:
Be careful not to allow the tanium-init.dat file to be distributed or stored outside of your organization, such as in a publicly accessible source code repository or any other location accessible from the public internet. Limit the distribution to specific use in the deployment of Tanium Clients.

Though this file does not contain private keys and cannot be used to provide control over a Tanium environment, a user with malicious intent could use it to connect an unapproved Client and use this unauthorized access to learn how your organization is using Tanium.

7. Extract the files from the bundle, and copy SetupClient.exe, tanium-init.dat, and, optionally, install.bat to a temporary directory on the endpoint. Make sure to keep the tanium-init.dat file in the same directory as SetupClient.exe.

INSTALL THE TANIUM CLIENT ON WINDOWS USING THE INSTALLATION WIZARD

1. Sign in to the Windows endpoint with a local user or domain account that has administrative permissions.
2. Right-click SetupClient.exe and select **Run as administrator** to start the wizard.
3. Respond to the wizard prompts.
   The values that you enter depend on the source of the installation files. If you used Client Management to download tanium-init.dat and the file is in the same directory as SetupClient.exe, the wizard prompts you to accept the license agreement and select an installation directory, and then automatically configures the remaining settings, including Client settings configured in the Client Deployment Template. Otherwise, you must manually specify the **Initialization File** (tanium-init.dat) and other settings.

Tip: To configure custom values instead of default values, move tanium-init.dat to a different directory than SetupClient.exe before starting the wizard. The wizard then prompts you to specify the settings.

Note: You must specify an installation directory on a local fixed drive on each endpoint. A volume mounted in a directory on another volume is not supported.

©2026 Tanium Inc. All Rights Reserved

(Optional) Use the CLI on Windows endpoints on page 413 to configure additional Tanium Client settings on page 393 that you did not set through the installation wizard. For information about configuring additional settings at a later time, see Modify Client settings on page 320.

4. Wait a few minutes for the Tanium Client to register with the Tanium Server or Zone Server, and then verify that the Client installed correctly and is communicating properly. For more information, see Verify the Tanium Client installation on page 228.

INSTALL THE TANIUM CLIENT ON WINDOWS USING THE COMMAND LINE

About this task

You can use the endpoint command-line interface (CLI) to install the Tanium Client. For more information about using the CLI, see CLI on Windows endpoints on page 413.

Tip:

The install.bat file provides an example of a script that installs the Tanium Client silently. By default, the script checks for administrative access and runs a silent express installation. You can modify this script with other arguments that are necessary for your environment. You can then use the modified script for automated deployment of the Tanium Client.

If User Account Control (UAC) is enabled and you are using an account other than the default Administrator account, you must run the install.bat script as an Administrator to prevent a UAC prompt when the script runs the Tanium Client installer.

1. Sign in to the Windows endpoint with a local user or domain account that has administrative permissions.
2. Access the endpoint command prompt.

   Note: If User Account Control (UAC) is enabled and you are using an account other than the default Administrator account, open the command prompt as an Administrator to prevent a UAC prompt when you run the Tanium Client installer.

©2026 Tanium Inc. All Rights Reserved

3. Navigate to the directory where the Tanium Client installer resides.
4. Use the following command to run the Tanium Client installer.

   ```
   SetupClient.exe
   /ServerAddress={<FQDN|IPaddress>}[,{<FQDN|IPaddress>},...]
   [/ServerPort=<PortNumber>] [/LogVerbosityLevel=<LogLevel>]
   [/KeyPath=<FullPath>\[tanium-init.dat|tanium.pub]
   [/ReportingTLSMode=[0|1|2]] [/ProxyAutoConfigAddress=<URL/
   filename.pac>] [/ProxyServers=<FQDN|IPaddress:PortNumber>] [/S]
   [/D=<DirectoryPath>]
   ```

   Table 19. Tanium Client command-line installation syntax on page 161 describes the arguments for the SetupClient.exe command.

   Before running the installer, determine which installation type to use based on whether the Tanium Client requires default or custom settings:

   - Express: The installer uses settings configured in the tanium-init.dat file or otherwise the default values, except for ServerNameList on page 230and requires only the following arguments:
     - `/ServerAddress` sets the **ServerNameList** and is required only if tanium-init.dat does not specify **ServerNameList**. By default, the tanium-init.dat that you download through Client Management specifies **ServerNameList**, while the tanium-init.dat that you download through Tanium Console does not.
     - `/KeyPath` specifies the full path of the tanium-init.dat file and is required only if the file is not in the same directory as SetupClient.exe.
     - `/S` specifies silent installation and is required for express installation of any Tanium Client version.
   - Custom: Specify the arguments from Table 19. Tanium Client command-line installation syntax on page 161 for settings that require custom values instead of settings configured in the tanium-init.dat file or default values. If you omit the `/S` argument, the Tanium Client installation wizard on page 158 opens and prompts you to configure the settings.

©2026 Tanium Inc. All Rights Reserved

Table 20. Tanium Client command-line installation examples on page 165 shows examples of how to use the CLI for express and custom installations.

> **Note:**
>
> - Command-line arguments for the installer are case-sensitive. Make sure to use capital letters for the `/S` or `/D` arguments.
> - To configure settings other than those that Table 19. Tanium Client command-line installation syntax on page 161 describes, see Modify Client settings on page 320.

5. Wait a few minutes for the Tanium Client to register with the Tanium Server or Zone Server, and then verify that the Client installed correctly and is communicating properly. For more information, see Verify the Tanium Client installation on page 228.

TANIUM CLIENT COMMAND-LINE INSTALLATION REFERENCE

Tanium Client command-line installation syntax

Argument	Guidance
/ServerAddress	Fully qualified domain names (FQDNs) or IP addresses of the Tanium Servers. In a deployment with Zone Servers, add their FQDNs or IP addresses. Use a comma to separate the entry for each server. If you specify one value for this option, it populates the ServerName on page 231 registry entry. If you specify multiple values, they populate the **ServerNameList** registry entry. Omit `/ServerAddress` during the initial installation if the tanium-init.dat file specifies the **ServerNameList** (see the Client installation types on page 159). If tanium-init.dat does not specify the **ServerNameList** , you must include `/ServerAddress` during installation. You can omit this argument when reinstalling or upgrading any version of the Client. **Note:** If the tanium-init.dat file includes the **ServerNameList** setting, the installer ignores this argument and applies the **ServerNameList** from the tanium-init.dat file. By default, the tanium-init.dat that you download through Client Management specifies **ServerNameList** , while the tanium-init.dat that you download through Tanium Console does not.

©2026 Tanium Inc. All Rights Reserved

Argument	Guidance
	Best Practice: If the tanium-init.dat file does not include the **ServerNameList**, specify FQDNs for this argument. **Tip:** You can optionally set the port that the Tanium Client uses to communicate with Servers by appending `:<port_number>` to the Server IP addresses or FQDNs (for example, `ts1.local.com:443,ts2.local.com:443,zs1.example.com:443`). The **ServerNameList** port values override the **ServerPort** setting for the Tanium Client (default is 17472).
/ServerPort	The port that the Tanium Client uses for communication with the Tanium Server and with peers. You can omit this argument if the tanium-init.dat file came from a Client Management Client deployment template. If you omit this argument and the tanium-init.dat file does not supply this setting, the Tanium Client uses the default port, 17472. For more information, see ServerPort on page 232.
/LogVerbosityLevel	The level of logging on the endpoint. You can omit this argument if the tanium-init.dat file came from a Client Management Client deployment template. If you omit this argument and the tanium-init.dat file does not supply this setting, the Tanium Client uses the default value of 1. The following values are best practices for specific scenarios: • `1` (default): Use this value during normal operation. • `41`: Use this value during troubleshooting. • `91` or higher: Use this value for full logging, for short periods of time only. **Note:** A value of `0` disables logging. As a best practice, do not disable logging.
/KeyPath	The full path and file name that the Tanium Client installer program uses to locate the tanium-init.dat file and copy it to the Tanium Client installation directory on page 490. Typically, the tanium-init.dat file included with the installation package is located in the same directory as the installer and you omit this argument. Only include this argument in a specific case where you cannot provide the tanium-init.dat file in the same directory as the installer. No quotation marks are necessary, except to enclose path or file names with spaces. The `KeyPath` argument requires a fully qualified path name when the installer runs directly from a command prompt. However, in a batch file, you can use the batch file command variable `%~dp0` to expand a

©2026 Tanium Inc. All Rights Reserved

Argument	Guidance
	relative path before passing the `KeyPath` value to SetupClient.exe . For example: `/KeyPath=%~dp0 <My\Relative\Path> \tanium-init.dat` If you omit the `KeyPath` argument for silent installations (`/S` argument), the tanium-init.dat file must be in the same directory as SetupClient.exe .
/S	Run the installation command *silently* , which means the Tanium Client installation wizard does not open and prompt you to configure settings. If you include this argument without specifying the `/KeyPath` argument, tanium-init.dat must be in the same directory as SetupClient.exe . For examples of how to run silent installations, see Table 20. Tanium Client command-line installation examples on page 165 . **Note:** Make sure to use a capital letter for this argument.
/D	Sets the destination path for the Tanium Client installation directory. No quotation marks are necessary to enclose path names with spaces. Because environment variables are expanded, the argument value can include path variables, such as `%programfiles%` . **Important:** • Because the value of this argument can include spaces, it must be the last argument on the command line if you include it. This includes appearing after the `/S` argument if you also include that argument. • You must specify an installation directory on a local fixed drive on each endpoint. A volume mounted in a directory on another volume is not supported. If you omit this argument, the installer uses a default directory based on whether the endpoint is running a 64-bit or 32-bit version of Windows: • 64-bit versions of Windows: \Program Files (x86)\Tanium\Tanium Client • 32-bit versions of Windows: \Program Files\Tanium\Tanium Client For an example commmand that includes the `/D` argument, see Table 20. Tanium Client command-line installation examples on page 165 .

©2026 Tanium Inc. All Rights Reserved

Argument	Guidance
	Note: • Make sure to use a capital letter for this argument. • If you are using the command line to reinstall or upgrade an existing Tanium Client, you cannot change the installation directory. The installer ignores this argument and automatically reinstalls or upgrades the Tanium Client in the existing directory, whether it is the default directory or a custom directory.
/ProxyAutoConfigAddress	Include this setting if the Tanium Client connects to the Tanium Server or Zone Server through a Hypertext Transfer Protocol Secure (HTTPS) proxy server. The setting specifies the URL and file name of a proxy auto configuration (PAC) file that the Client can access. Specify the value in the format `http[s]://<URL>/<file name>.pac`. The Client downloads the file from the URL that you specify and runs a script that the file contains to select the correct proxy for connecting to a particular server. If no proxy is available, the Client ignores the setting and connects directly to the Tanium Server or Zone Server. For more information, see Configure proxy connections during Client deployment with a PAC file (Windows endpoints only) on page 242.
/ProxyServers	Include this setting if the Tanium Client connects to the Tanium Server or Zone Server through an HTTPS proxy server but cannot access a PAC file. The setting specifies the IP address or FQDN, and port number, of the HTTPS proxy server. You can specify multiple proxies as a comma-separated list in the format `"<proxy1>:<port>,...,<proxyN>:<port>"`. The Client tries to connect to the proxies in the order that you list them. After any single connection succeeds, the Client stops trying to connect with more proxies. If no proxy is available, the Client ignores the setting and connects directly to the Tanium Server or Zone Server. For more information, see Configure specific proxy servers during Client deployment on page 241.
/ProxyAutoDetect	Include this setting if the Tanium Client connects to the Tanium Server or Zone Server through an HTTPS proxy server and you want to detect the locally configured proxy settings on the endpoint. Specify the value `1` to enable this detection. For more information, see Configure proxy connections during Client deployment with a PAC file (Windows endpoints only) on page 242.

The following are examples of using the CLI command to install the Tanium Client.

©2026 Tanium Inc. All Rights Reserved

Note: Omit the `/ServerAddress`, `/ServerPort`, and `/LogVerbosityLevel` arguments if the tanium-init.dat file came from a Client Management Client Deployment Template. For more information, see the Install the Tanium Client on Windows using the command line on page 159.

Tanium Client command-line installation examples

Example	Description

Silent express installation	In an express installation, SetupClient.exe installs and configures the Tanium Client with default values for all the arguments, except `/ServerAddress` when it is not specified by tanium-init.dat. Before starting, make sure that the Tanium initialization file tanium-init.dat is in the same directory as SetupClient.exe.
	`SetupClient.exe /ServerAddress=ts1.example.com /S`
	`SetupClient.exe /ServerAddress=192.168.1.10 /S`
	In a deployment with Zone Servers or multiple Tanium Servers, specify each Server in `/ServerAddress`:
	`SetupClient.exe /ServerAddress= ts1.example.com,ts2.example.com,zs1.example.com /S`

Silent custom installation	The following example specifies non-default values in a silent installation:
	`SetupClient.exe /ServerAddress=ts1.example.com ^ /ServerPort=63422 /LogVerbosityLevel=1 /S`
	To use a custom installation directory, add the `/D` parameter. Note that it must be the last argument in the command, even when you include `/S`.
	`SetupClient.exe /ServerAddress=ts1.example.com ^ /ServerPort=63422 /LogVerbosityLevel=1 /S ^ /D=C:\Custom Installation Directory\Tanium\Tanium Client`

Batch file format	When you run a batch file, the Windows command interpreter expands the variable `%~dp0` to the full drive and path name of the batch file working directory. The following example of a batch file instruction performs a silent installation: `"%~dp0SetupClient.exe" /ServerAddress=ts1.example.com ^ /ServerPort=28583 /S`

Deploy the Tanium Client to macOS endpoints using the installer

On macOS endpoints, the Tanium Client is installed as a system service. The Client files are installed in the /Library/Tanium/TaniumClient directory.

©2026 Tanium Inc. All Rights Reserved

You can use the installation wizard on page 169 or CLI on page 171 to deploy the Tanium Client to macOS endpoints. You must perform the installation as a user with an administrator account.

Note: You cannot install the universal version of the macOS Tanium Client on an endpoint where the x86-64 version is already installed. You must first uninstall the existing Tanium Client on page 352.

For information about managing the Tanium Client service, managing firewall rules or pop-ups, or uninstalling the Tanium Client after deployment, see Manage the Tanium Client on macOS on page 305.

Related information

- Manage the Tanium Client on macOS on page 305
- Preparing the Tanium Client on a macOS image on page 197
- Uninstall the Tanium Client on macOS on page 352
- Client version and operating system requirements on page 29
- Managing Client settings and Index configurations on page 318
- Tanium Client settings reference on page 393

PREPARE FOR INSTALLATION

1. Ensure that the endpoint meets the basic requirements on page 29 for the Tanium Client on macOS.
2. Ensure that host and network firewalls are configured to allow inbound and outbound TCP traffic on the ports that the Tanium Client uses. For more information, see Manage macOS firewall rules on page 305 and Network connectivity, ports, and firewalls on page 63.
3. (macOS 10.14 or later only) Create a mobile device management (MDM) profile that provides the necessary permissions for the following Tanium applications.

   Important:
   This step is critical for full support of Tanium Client functionality on macOS 10.14 or later.

Application	Location	Required Permissions	Apple Events
Tanium Client	/Library/Tanium/TaniumClient/	All System Files, Admin	System Events,

©2026 Tanium Inc. All Rights Reserved

Application	Location	Required Permissions	Apple Events
	TaniumClient	System Files, Post Events	SystemUIServer, Finder
Tanium Client Extensions [1]	/Library/Tanium/TaniumClient/TaniumCX	All System Files, Admin System Files, Post Events	System Events, SystemUIServer, Finder
	/Library/Tanium/TaniumClient/TaniumCX.app	All System Files, Admin System Files, Post Events	System Events, SystemUIServer, Finder
Tanium End-User Notifications	End-User Notifications 1.18.57 or later: /Library/Tanium/EndUserNotifications/bin/Launcher.app Earlier versions: /Library/Tanium/EndUserNotifications/bin/end-user-notifications.app	Post Events	System Events, SystemUIServer, Finder

[1] On endpoints running the universal Tanium Client binary, you must specify both of the locations listed for Tanium Client Extensions. On endpoints running the x86-64 Tanium Client binary, you do not need to specify /Library/Tanium/TaniumClient/TaniumCX.app . Tanium recommends the universal binary for all Mac computers running macOS 11 or later. For more information, see Client version and operating system requirements on page 29 .

An MDM administrator must create a PPPC custom payload that specifies the necessary permissions for each application. The PPPC custom payload must be delivered using a User-Approved MDM (UAMDM) payload in a device profile.

The team identifier for Tanium applications is TZTPM3VTUU.

Important: If you previously created a PPPC custom payload for a version of the Tanium Client earlier than 7.2.314.3608, you must update the code signing requirement for newer versions of the Tanium Client.

For more information about MDM on macOS, see Apple Platform Deployment.

4. Sign in to the target endpoint.
5. Use the Tanium Client Management service to download the Client installer bundle to the

©2026 Tanium Inc. All Rights Reserved

macOS endpoint. From the Client Management **Overview** page, click **Download Installers** > **Download macOS Package**.

The bundle (mac-client-bundle.zip) contains the following files:

- install.sh
- TaniumClient-<*version*>-universal.pkg
- TaniumClient-<*version*>-x64.pkg

6. Download the tanium-init.dat file from a Client Deployment Template in the Tanium Client Management service:
   a. From the Main menu, go to **Shared Services >** Client Management.
   b. Go to **Client Installations** > **Client Deployment Templates**.
   c. In the row for a template, click Actions and select **Download tanium-init.dat**.
   d. Deploy Tanium Client using the appropriate installer or package file and the tanium-init.dat file you downloaded. For more information, see Deploying the Tanium Client using an installer or package file on page 153.

Tip: You must create a Client Deployment Template in Client Management before performing this step. For more information, see (Optional) Create a Client deployment template on page 137.



Best Practice: Download the tanium-init.dat file for a Client Deployment Template in Client Management. Though you can also download tanium-init.dat through Tanium Console without creating a Client Deployment Template (see Download infrastructure configuration files (keys)), the installation process requires fewer manual configuration steps if you use these steps.

©2026 Tanium Inc. All Rights Reserved

Important:
Be careful not to allow the tanium-init.dat file to be distributed or stored outside of your organization, such as in a publicly accessible source code repository or any other location accessible from the public internet. Limit the distribution to specific use in the deployment of Tanium Clients.

Though this file does not contain private keys and cannot be used to provide control over a Tanium environment, a user with malicious intent could use it to connect an unapproved Client and use this unauthorized access to learn how your organization is using Tanium.

7. Extract the files from the bundle, and copy the package files, tanium-init.dat, and, optionally, install.sh to a temporary directory on the endpoint. Make sure to keep the tanium-init.dat file in the same directory as the package files.

INSTALL THE TANIUM CLIENT ON MACOS USING THE INSTALLATION WIZARD

1. Sign in locally to the macOS endpoint as a user with an administrator account.
2. Double-click TaniumClient-<*version*>-universal.pkg or TaniumClient-<*version*>-x64.pkg to start the installation wizard.

   Best Practice: Tanium recommends the universal binary for all Mac computers running macOS 11 or later. The universal binary is supported and runs natively on both Intel-based Mac computers running macOS 11 or later and Apple "M" series-based Mac computers.

   Note: If you are using any solutions that use the Tanium™ Client Recorder Extension, you must install the universal binary for full functionality of the extension.

3. Respond to the wizard prompts. Specify the **User Name** and **Password** of a local administrator when the wizard prompts you for credentials.
4. (For tanium-init.dat files that do not include Client settings) Use the CLI (see CLI on non-Windows endpoints on page 414) to configure the following basic Tanium Client settings.

ServerName on page 231 or ServerNameList	In a deployment with a standalone Tanium Server, set the `ServerName` to the Server FQDN or IP address. In a deployment with Tanium Zone Servers or multiple Tanium Servers, configure `ServerNameList` with the FQDN or IP address of each Server, separated with a comma.

©2026 Tanium Inc. All Rights Reserved

on page 230	**Important:** If the tanium-init.dat file specifies `ServerNameList`, you do not need to configure `ServerName` or `ServerNameList`; any setting that you specify here is added to the `ServerNameList` specified in tanium-init.dat. By default, the tanium-init.dat that you download through the Client Management service specifies `ServerNameList`, while the tanium-init.dat that you download through Tanium Console does not. You can use the `TaniumClient pki show <path_to_tanium-init.dat>` command on an endpoint where Tanium Client is already installed to view the `ServerNameList` that the tanium-init.dat file specifies. **Best Practice:** If the tanium-init.dat file does not include the **ServerNameList**, specify FQDNs for this setting. **Tip:** You can optionally set the port that the Tanium Client uses to communicate with Servers by appending `:<port_number>` to the Server IP addresses or FQDNs (for example, `ts1.local.com:443,ts2.local.com:443,zs1.example.com:443`). The **ServerNameList** port values override the **ServerPort** setting for the Tanium Client (default is 17472).
ServerPort	The port that the Tanium Client uses for communication with the Tanium Server and with peers. The default port is 17472. For more information, see ServerPort on page 232.
LogVerbosityLevel	The level of logging on the endpoint. The following values are best practices for specific scenarios: • `1` (default): Use this value during normal operation. • `41`: Use this value during troubleshooting. • `91` or higher: Use this value for full logging, for short periods of time only. **Note:** A value of `0` disables logging. As a best practice, do not disable logging.

Note: For information about configuring additional settings, see Modify Client settings on page 320 and Tanium Client settings reference on page 393.

The following example commands are for a deployment with multiple Tanium Servers and Zone Servers:

©2026 Tanium Inc. All Rights Reserved

```
sudo /Library/Tanium/TaniumClient/TaniumClient config set ServerNameList \
ts1.example.com,ts2.example.com,zs1.example.com,zs2.example.com
sudo /Library/Tanium/TaniumClient/TaniumClient config set LogVerbosityLevel 1
```

5. Use the following command to copy tanium-init.dat from the temporary directory to the Tanium Client installation directory:

```
sudo cp <extracted installer bundle directory>/tanium-init.dat /Library/Tanium/
TaniumClient
```

6. Wait a few minutes for the Tanium Client to register with the Tanium Server or Zone Server, and then verify that the Client installed correctly and is communicating properly. For more information, see Verify the Tanium Client installation on page 228.

INSTALL THE TANIUM CLIENT ON MACOS USING THE COMMAND LINE

About this task

To install the Tanium Client, you must have root or sudo permissions to run the installer command. For more information about using the CLI, see CLI on non-Windows endpoints on page 414.

Tip: The install.sh file provides an example of a script that performs an installation of the Tanium Client. By default, the script checks for a supported version of macOS, installs the appropriate Tanium Client package, and copies the tanium-init.dat file. You can modify this script with CLI commands that configure the Tanium Client settings that are necessary for your environment. You can then use the modified script for automated deployment of the Tanium Client. To run the install.sh script, you must have root or sudo permissions.

1. Sign in locally to the macOS endpoint as a user with an administrator account.
2. Open **Terminal**.
3. Run the following command in the directory into which you copied TaniumClient-*<version>*-universal.pkg or TaniumClient-*<version>*-x64.pkg to install the Client :

```
sudo installer -pkg TaniumClient-<version>-binary.pkg -target /
installer: Package name is TaniumClient
```

©2026 Tanium Inc. All Rights Reserved

```
installer: Installing at base path /
installer: The install was successful.
```

Note: Tanium recommends the universal binary for all Mac computers running macOS 11 or later. The universal binary is supported and runs natively on both Intel-based Mac computers running macOS 11 or later and Apple "M" series-based Mac computers.

4. (For tanium-init.dat files that do not include Client settings) Use the CLI (see CLI on non-Windows endpoints on page 414) to configure the following basic Tanium Client settings.

ServerName on page 231 or ServerNameList on page 230	In a deployment with a standalone Tanium Server, set the `ServerName` to the Server FQDN or IP address. In a deployment with Tanium Zone Servers or multiple Tanium Servers, configure `ServerNameList` with the FQDN or IP address of each Server, separated with a comma. **Important:** If the tanium-init.dat file specifies `ServerNameList`, you do not need to configure `ServerName` or `ServerNameList`; any setting that you specify here is added to the `ServerNameList` specified in tanium-init.dat. By default, the tanium-init.dat that you download through the Client Management service specifies `ServerNameList`, while the tanium-init.dat that you download through Tanium Console does not. You can use the `TaniumClient pki show <path_to_tanium-init.dat>` command on an endpoint where Tanium Client is already installed to view the `ServerNameList` that the tanium-init.dat file specifies. **Best Practice:** If the tanium-init.dat file does not include the **ServerNameList**, specify FQDNs for this setting. **Tip:** You can optionally set the port that the Tanium Client uses to communicate with Servers by appending `:<port_number>` to the Server IP addresses or FQDNs (for example, `ts1.local.com:443,ts2.local.com:443,zs1.example.com:443`). The **ServerNameList** port values override the **ServerPort** setting for the Tanium Client (default is 17472).
ServerPort	The port that the Tanium Client uses for communication with the Tanium Server and with peers. The default port is 17472. For more information, see ServerPort on page 232.
LogVerbosityLevel	The level of logging on the endpoint. The following values are best practices for specific scenarios:

©2026 Tanium Inc. All Rights Reserved

- `1` (default): Use this value during normal operation.
- `41`: Use this value during troubleshooting.
- `91` or higher: Use this value for full logging, for short periods of time only.

Note:

A value of `0` disables logging. As a best practice, do not disable logging.

Note: For information about configuring additional settings, see Modify Client settings on page 320 and Tanium Client settings reference on page 393.

The following example commands are for a deployment with multiple Tanium Servers and Zone Servers:

```
sudo /Library/Tanium/TaniumClient/TaniumClient config set ServerNameList \
ts1.example.com,ts2.example.com,zs1.example.com,zs2.example.com
sudo /Library/Tanium/TaniumClient/TaniumClient config set LogVerbosityLevel 1
```

5. Use the following command to copy tanium-init.dat to the Tanium Client installation directory:

```
sudo cp tanium-init.dat /Library/Tanium/TaniumClient
```

6. Wait a few minutes for the Tanium Client to register with the Tanium Server or Zone Server, and then verify that the Client installed correctly and is communicating properly. For more information, see Verify the Tanium Client installation on page 228.

Deploy the Tanium Client to Linux endpoints using package files

On Linux endpoints, the Tanium Client is installed as a system service. The default installation directory for Tanium Client files is /opt/Tanium/TaniumClient.

Tip: If your environment requires a different installation location for applications, you can create a symbolic link during installation.

For information about managing the Tanium Client service, managing firewall rules, or uninstalling

©2026 Tanium Inc. All Rights Reserved

the Tanium Client after deployment, see Manage the Tanium Client on Linux on page 308.

Related information

- Manage the Tanium Client on Linux on page 308
- Preparing the Tanium Client on a Linux OS image on page 200
- Uninstall the Tanium Client on Linux on page 354
- Client version and operating system requirements on page 29
- Managing Client settings and Index configurations on page 318
- Tanium Client settings reference on page 393

PREPARE FOR INSTALLATION

1. Ensure that the endpoint meets the basic requirements on page 29 for the Tanium Client on Linux.
2. Ensure that host and network firewalls are configured to allow inbound and outbound TCP traffic on the ports that the Tanium Client uses. For more information, see Manage Linux firewall rules on page 308 and Network connectivity, ports, and firewalls on page 63.
3. Sign in to the target endpoint using an account that has administrative privileges, or that is listed in the sudoers file to allow the account you are using to use sudo.
4. Use the Tanium Client Management service to download the Client installer bundle to the Linux endpoint. From the Client Management **Overview** page, click **Download Installers** > **Download Linux Package**.
   The bundle (linux-client-bundle.zip) contains the following files:
   - install.sh
   - Installer package files for each Linux distribution (such as TaniumClient-7.9.3.xxxx-1.oel8.x86_64.rpm; see Tanium Client package files for Linux on page 175)
5. Download the tanium-init.dat file from a Client Deployment Template in the Tanium Client Management service:
   a. From the Main menu, go to **Shared Services >** Client Management.
   b. Go to **Client Installations** > **Client Deployment Templates**.
   c. In the row for a template, click Actions and select **Download tanium-init.dat**.
   d. Deploy Tanium Client using the appropriate installer or package file and the tanium-

©2026 Tanium Inc. All Rights Reserved

init.dat file you downloaded. For more information, see Deploying the Tanium Client using an installer or package file on page 153.

Tip: You must create a Client Deployment Template in Client Management before performing this step. For more information, see (Optional) Create a Client deployment template on page 137.

Best Practice: Download the tanium-init.dat file for a Client Deployment Template in Client Management. Though you can also download tanium-init.dat through Tanium Console without creating a Client Deployment Template (see Download infrastructure configuration files (keys)), the installation process requires fewer manual configuration steps if you use these steps.

Important:
Be careful not to allow the tanium-init.dat file to be distributed or stored outside of your organization, such as in a publicly accessible source code repository or any other location accessible from the public internet. Limit the distribution to specific use in the deployment of Tanium Clients.

Though this file does not contain private keys and cannot be used to provide control over a Tanium environment, a user with malicious intent could use it to connect an unapproved Client and use this unauthorized access to learn how your organization is using Tanium.

6. Extract the files from the bundle, and copy the appropriate package file, tanium-init.dat, and, optionally, install.sh to a temporary directory on the endpoint. Make sure to keep the tanium-init.dat file in the same directory as the package file.

TANIUM CLIENT PACKAGE FILES FOR LINUX

The Linux installer bundle that you download through Tanium Client Management contains package installer files for every Linux distribution. Contact Tanium Support on page 392 for other means to obtain the package file for your Linux distribution.

©2026 Tanium Inc. All Rights Reserved

Note:

- To verify the digital signature on RPM package files, use the Tanium public key for Linux RPM files.
- For the versions of the Tanium Client that are available for each Linux distribution, see Supported operating systems on page 32.

Tanium Client package files for Linux

Linux Distribution	Latest Installation Package Files
Amazon Linux 2023	TaniumClient- *<client_version>* -1.amzn2023.0.20230503.x86_64.rpm TaniumClient- *<client_version>* -1.amzn2023.0.20230503.aarch64.rpm
Amazon Linux 2 LTS	TaniumClient- *<client_version>* -1.amzn2.x86_64.rpm TaniumClient- *<client_version>* -1.amzn2.aarch64.rpm
Amazon Linux AMI 2018.3	TaniumClient- *<client_version>* -1.amzn2018.03.x86_64.rpm
Amazon Linux AMI 2016.09	TaniumClient- *<client_version>* -1.amzn2016.09.x86_64.rpm
Debian 13.x	taniumclient- *<client_version>* -debian13_amd64.deb taniumclient- *<client_version>* -debian13_arm64.deb
Debian 12.x	taniumclient- *<client_version>* -debian12_amd64.deb taniumclient- *<client_version>* -debian12_arm64.deb
Debian 11.x	taniumclient- *<client_version>* -debian11_amd64.deb
Debian 10.x	taniumclient- *<client_version>* -debian10_amd64.deb
Debian 9.x	taniumclient- *<client_version>* -debian9_i386.deb taniumclient- *<client_version>* -debian9_amd64.deb
Debian 8.x	taniumclient- *<client_version>* -debian8_i386.deb taniumclient- *<client_version>* -debian8_amd64.deb
Debian 7.x, 6.x	taniumclient- *<client_version>* -debian6_i386.deb

©2026 Tanium Inc. All Rights Reserved

Linux Distribution	Latest Installation Package Files
	taniumclient- *<client_version>* -debian6_amd64.deb
Oracle Linux 9.x	TaniumClient- *<client_version>* -1.oel9.x86_64.rpm TaniumClient- *<client_version>* -1.oel9.aarch64.rpm
Oracle Linux 8.x	TaniumClient- *<client_version>* -1.oel8.x86_64.rpm TaniumClient- *<client_version>* -1.oel8.aarch64.rpm
Oracle Linux 7.x	TaniumClient- *<client_version>* -1.oel7.x86_64.rpm
Oracle Linux 6.x	TaniumClient- *<client_version>* -1.oel6.i686.rpm TaniumClient- *<client_version>* -1.oel6.x86_64.rpm
Oracle Linux 5.x	TaniumClient- *<client_version>* -1.oel5.i386.rpm TaniumClient- *<client_version>* -1.oel5.x86_64.rpm
Red Hat / AlmaLinux / Rocky Linux / Oracle Linux 10.x	TaniumClient- *<client_version>* -1.rhe10.x86_64.rpm TaniumClient- *<client_version>* -1.rhe10.aarch64.rpm
Red Hat / AlmaLinux / Rocky Linux 9.x	TaniumClient- *<client_version>* -1.rhe9.x86_64.rpm TaniumClient- *<client_version>* -1.rhe9.aarch64.rpm
Red Hat / CentOS / AlmaLinux / Rocky Linux 8.x	TaniumClient- *<client_version>* -1.rhe8.x86_64.rpm TaniumClient- *<client_version>* -1.rhe8.aarch64.rpm
Red Hat / CentOS 7.x	TaniumClient- *<client_version>* -1.rhe7.x86_64.rpm
Red Hat / CentOS 6.x	TaniumClient- *<client_version>* -1.rhe6.i686.rpm TaniumClient- *<client_version>* -1.rhe6.x86_64.rpm
Red Hat / CentOS 5.x	TaniumClient- *<client_version>* -1.rhe5.i386.rpm TaniumClient- *<client_version>* -1.rhe5.x86_64.rpm
SUSE Linux Enterprise Server (SLES) / OpenSUSE 16.x	TaniumClient- *<client_version>* -1.sle16.x86_64.rpm
SUSE Linux Enterprise Server (SLES) / OpenSUSE 15.x	TaniumClient- *<client_version>* -1.sle15.i586.rpm TaniumClient- *<client_version>* -1.sle15.x86_64.rpm

©2026 Tanium Inc. All Rights Reserved

Linux Distribution	Latest Installation Package Files
SUSE Linux Enterprise Server (SLES) / OpenSUSE 12.x	TaniumClient- *<client_version>* -1.sle12.i586.rpm TaniumClient- *<client_version>* -1.sle12.x86_64.rpm
SUSE Linux Enterprise Server (SLES) / OpenSUSE 11.x	TaniumClient- *<client_version>* -1.sle11.i586.rpm TaniumClient- *<client_version>* -1.sle11.x86_64.rpm
Ubuntu 26.04 LTS	taniumclient_ *<client_version>* -ubuntu26_amd64.deb taniumclient_ *<client_version>* -ubuntu26_arm64.deb
Ubuntu 24.04 LTS	taniumclient_ *<client_version>* -ubuntu24_amd64.deb taniumclient_ *<client_version>* -ubuntu24_arm64.deb
Ubuntu 22.04 LTS	taniumclient_ *<client_version>* -ubuntu22_amd64.deb taniumclient_ *<client_version>* -ubuntu22_arm64.deb
Ubuntu 20.04 LTS	taniumclient_ *<client_version>* -ubuntu20_amd64.deb
Ubuntu 18.04 LTS	taniumclient_ *<client_version>* -ubuntu18_amd64.deb
Ubuntu 16.04 LTS	taniumclient_ *<client_version>* -ubuntu16_amd64.deb
Ubuntu 14.04 LTS	taniumclient_ *<client_version>* -ubuntu14_amd64.deb

INSTALL THE TANIUM CLIENT ON LINUX USING THE COMMAND LINE

About this task

Use the endpoint CLI to install the Tanium Client. For more information about using the CLI, see CLI on non-Windows endpoints on page 414.

©2026 Tanium Inc. All Rights Reserved

Tip: The install.sh file provides an example of a script that performs an installation of the Tanium Client. By default, the script determines the distribution and version of Linux, installs the appropriate Tanium Client package, and copies the tanium-init.dat file. You can modify this script with CLI commands that configure the Tanium Client settings that are necessary for your environment. You can then use the modified script for automated deployment of the Tanium Client. To run the install.sh script, you must have root or sudo permissions.

1. (Optional) To use a directory other than the default on page 490 for the Client installation, create a symbolic link. For example, to use the directory /appbin/Tanium, run the following command:

   ```
   ln -s /appbin/Tanium /opt/Tanium
   ```

   Important: You must install the Tanium Client on a local fixed drive.

2. Run the appropriate installation command to install the package and generate a default configuration file.
   The RPM installers for Redhat and SUSE have command syntax similar to the following example:

   ```
   sudo rpm -Uvh TaniumClient-7.9.3.xxxx-1.oel6.x86_64.rpm
   ```

   The Debian installers for Debian and Ubuntu have command syntax similar to the following example:

   ```
   sudo dpkg -i taniumclient_7.9.3.xxxx-debian6_amd64.deb
   ```

3. Copy tanium-init.dat to the installation directory on page 490. For example:

   ```
   cp tanium-init.dat /opt/Tanium/TaniumClient
   ```

4. (For tanium-init.dat files that do not include Client settings) Use the CLI (see CLI on non-Windows endpoints on page 414) to configure the following basic Tanium Client settings.

ServerName on	In a deployment with a standalone Tanium Server, set the `ServerName` to the Server FQDN or

©2026 Tanium Inc. All Rights Reserved

page 231 or ServerNameList on page 230	IP address. In a deployment with Tanium Zone Servers or multiple Tanium Servers, configure `ServerNameList` with the FQDN or IP address of each Server, separated with a comma. **Important:** If the tanium-init.dat file specifies `ServerNameList`, you do not need to configure `ServerName` or `ServerNameList`; any setting that you specify here is added to the `ServerNameList` specified in tanium-init.dat. By default, the tanium-init.dat that you download through the Client Management service specifies `ServerNameList`, while the tanium-init.dat that you download through Tanium Console does not. You can use the `TaniumClient pki show <path_to_tanium-init.dat>` command on an endpoint where Tanium Client is already installed to view the `ServerNameList` that the tanium-init.dat file specifies. **Best Practice:** If the tanium-init.dat file does not include the **ServerNameList**, specify FQDNs for this setting. **Tip:** You can optionally set the port that the Tanium Client uses to communicate with Servers by appending `:<port_number>` to the Server IP addresses or FQDNs (for example, `ts1.local.com:443,ts2.local.com:443,zs1.example.com:443`). The **ServerNameList** port values override the **ServerPort** setting for the Tanium Client (default is 17472).
ServerPort	The port that the Tanium Client uses for communication with the Tanium Server and with peers. The default port is 17472. For more information, see ServerPort on page 232.
LogVerbosityLevel	The level of logging on the endpoint. The following values are best practices for specific scenarios: • `1` (default): Use this value during normal operation. • `41`: Use this value during troubleshooting. • `91` or higher: Use this value for full logging, for short periods of time only. **Note:** A value of `0` disables logging. As a best practice, do not disable logging.

Note: For information about configuring additional settings, see Modify Client settings on page 320 and Tanium Client settings reference on page 393.

©2026 Tanium Inc. All Rights Reserved

The following example commands are for a deployment with multiple Tanium Servers and Zone Servers:

```
cd <Tanium Client installation directory>
sudo ./TaniumClient config set ServerNameList \
ts1.example.com,ts2.example.com,zs1.example.com,zs2.example.com
sudo ./TaniumClient config set LogVerbosityLevel 1
```

5. Start the Tanium Client service. For more information, see Manage the Tanium Client service on Linux on page 313.
6. Wait a few minutes for the Tanium Client to register with the Tanium Server or Zone Server, and then verify that the Client installed correctly and is communicating properly. For more information, see Verify the Tanium Client installation on page 228.

Deploy the Tanium Client to Solaris endpoints using a package file

On Solaris endpoints, the Tanium Client is installed as a system service. The Tanium Client files are installed by default in the /opt/Tanium/TaniumClient directory.

Tip: If your environment requires a different installation location for applications, you can create a symbolic link during installation.

The following procedures describe how to use the endpoint CLI to install the Tanium Client. For more information about using the CLI, see CLI on non-Windows endpoints on page 414.

For information about managing the Tanium Client service or uninstalling the Tanium Client after deployment, see Manage the Tanium Client on Solaris on page 315.

Related information

- Manage the Tanium Client on Solaris on page 315
- Preparing the Tanium Client on a Solaris OS image on page 203
- Uninstall the Tanium Client on Solaris on page 355
- Client version and operating system requirements on page 29
- Managing Client settings and Index configurations on page 318
- Tanium Client settings reference on page 393

©2026 Tanium Inc. All Rights Reserved

PREPARE FOR INSTALLATION

1. Ensure that the endpoint meets the basic requirements on page 29 for the Tanium Client on Solaris.
2. Ensure that host and network firewalls are configured to allow inbound and outbound TCP traffic on the ports that the Tanium Client uses. For more information, see Network connectivity, ports, and firewalls on page 63.
3. (Solaris 11.4 only) Install the legacy **pkgadd** utilities:
    a. Access the endpoint CLI.
    b. Find the **pkgadd** IPS package name:

    ```
    pkg search pkgadd
    ```

    ```
    INDEX       ACTION VALUE       PACKAGE
    basename    file                    usr/sbin/pkgadd pkg:/package/
    svr4@11.4-11.4.6.0.1.4.0
    ```

    c. Install the **pkgadd** utilities:

    ```
    pkg install pkg:/package/svr4@11.4-11.4.6.0.1.4.0
    ```

4. (Solaris 10 or 11.0–11.3 only) Install the **SUNWgccruntime** package if it is not yet installed.

    Note: Although this package is part of a default Solaris installation, some organizations omit it in their standard image.

    a. Determine whether the package is installed:

    ```
    pkginfo -l SUNWgccruntime
    ```

    The following example output indicates the package is installed:

    ```
    PKGINST:  SUNWgccruntime
    NAME:  GCC Runtime libraries
    CATEGORY:  system
    ARCH:  sparc
    VERSION:  11.11.0,REV=2010.05.25.01.00
    BASEDIR:  /
    VENDOR:  Oracle Corporation
    DESC:  GCC Runtime - Shared libraries used by gcc and other gnu components
    ```

©2026 Tanium Inc. All Rights Reserved

```
INSTDATE:  Dec 01 2015 11:43
HOTLINE:  Please contact your local service provider
STATUS:  completely installed
```

b. If the **SUNWgccruntime** package is not yet installed, run one of the following commands:

- Solaris 10 or 11.0–11.3 (without using Image Packing System [IPS]):

```
# pkgadd -d /path/to/SUNWGccruntime.pkg SUNWgccruntime
```

- Solaris 11.0–11.3 using IPS:

```
# pkg install SUNWgccruntime
```

5. Sign in to the target endpoint.
6. Use the Tanium Client Management service to download the Client installer bundle to the Solaris endpoint. From the Client Management **Overview** page, click **Download Installers** > **Download Solaris Package**.
   The bundle (solaris-client-bundle.zip) contains the following files:
   - install.sh
   - TaniumClient-<*version*>-SunOS-5.10.i386.pkg.tar.gz
   - TaniumClient-<*version*>-SunOS-5.10.sparc.pkg.tar.gz
7. Download the tanium-init.dat file from a Client Deployment Template in the Tanium Client Management service:
   a. From the Main menu, go to **Shared Services >** Client Management.
   b. Go to **Client Installations** > **Client Deployment Templates**.
   c. In the row for a template, click Actions and select **Download tanium-init.dat**.
   d. Deploy Tanium Client using the appropriate installer or package file and the tanium-init.dat file you downloaded. For more information, see Deploying the Tanium Client using an installer or package file on page 153.

©2026 Tanium Inc. All Rights Reserved

Tip: You must create a Client Deployment Template in Client Management before performing this step. For more information, see (Optional) Create a Client deployment template on page 137.

Best Practice: Download the tanium-init.dat file for a Client Deployment Template in Client Management. Though you can also download tanium-init.dat through Tanium Console without creating a Client Deployment Template (see Download infrastructure configuration files (keys)), the installation process requires fewer manual configuration steps if you use these steps.

Important:
Be careful not to allow the tanium-init.dat file to be distributed or stored outside of your organization, such as in a publicly accessible source code repository or any other location accessible from the public internet. Limit the distribution to specific use in the deployment of Tanium Clients.

Though this file does not contain private keys and cannot be used to provide control over a Tanium environment, a user with malicious intent could use it to connect an unapproved Client and use this unauthorized access to learn how your organization is using Tanium.

8. Extract the files from the bundle, and copy the package files, tanium-init.dat, and, optionally, install.sh to a temporary directory on the endpoint. Make sure to keep the tanium-init.dat file in the same directory as the package files.

INSTALL THE TANIUM CLIENT ON SOLARIS USING THE COMMAND LINE

Before you begin

©2026 Tanium Inc. All Rights Reserved

Tip: The install.sh file provides an example of a script that performs an installation of the Tanium Client. By default, the script checks for a supported version of Solaris, installs the appropriate Tanium Client package, and copies the tanium-init.dat file. You can modify this script with CLI commands that configure the Tanium Client settings that are necessary for your environment. You can then use the modified script for automated deployment of the Tanium Client. To run the install.sh script, you must have root or sudo permissions.

1. (Optional) To use a directory other than the default on page 490 for the Client installation, create a symbolic link, and set the `PKG_NONABI_SYMLINKS` environment variable to `true`. For example, to use the directory /appbin/Tanium, run the following commands:

```
ln -s /appbin/Tanium /opt/Tanium
PKG_NONABI_SYMLINKS=true
export PKG_NONABI_SYMLINKS
```

Important: You must install the Tanium Client on a local fixed drive.

2. Run the following command from the temporary directory to install the package and generate a default configuration file:

```
sudo pkgadd -d ./TaniumClient-<client_version>-SunOS-5.10-<platform>.pkg TaniumClient
```

Note: If you are signed into the Global Zone and want to install only in the current zone, specify the `-G` flag. If you have questions, consult your system administrator for proper zone behavior.

3. (For tanium-init.dat files that do not include Client settings) Use the CLI (see CLI on non-Windows endpoints on page 414) to configure the following basic Tanium Client settings.

Note: The `Resolver` Client setting is not included in the tanium-init.dat file by default. You must either create a separate Client Configuration for Solaris that includes the custom Client setting `Resolver=nslookup` or manually set `Resolver=nslookup` using the CLI.

ServerName on page 231 or ServerNameList	In a deployment with a standalone Tanium Server, set the `ServerName` to the Server FQDN or IP address. In a deployment with Tanium Zone Servers or multiple Tanium Servers, configure `ServerNameList` with the FQDN or IP address of each Server, separated with a comma.

©2026 Tanium Inc. All Rights Reserved

[on page 230](#)	**Important:** If the tanium-init.dat file specifies `ServerNameList`, you do not need to configure `ServerName` or `ServerNameList`; any setting that you specify here is added to the `ServerNameList` specified in tanium-init.dat. By default, the tanium-init.dat that you download through the Client Management service specifies `ServerNameList`, while the tanium-init.dat that you download through Tanium Console does not. You can use the `TaniumClient pki show <path_to_tanium-init.dat>` command on an endpoint where Tanium Client is already installed to view the `ServerNameList` that the tanium-init.dat file specifies. **Best Practice:** If the tanium-init.dat file does not include the **ServerNameList**, specify FQDNs for this setting. **Tip:** You can optionally set the port that the Tanium Client uses to communicate with Servers by appending `:<port_number>` to the Server IP addresses or FQDNs (for example, `ts1.local.com:443,ts2.local.com:443,zs1.example.com:443`). The **ServerNameList** port values override the **ServerPort** setting for the Tanium Client (default is 17472).
ServerPort	The port that the Tanium Client uses for communication with the Tanium Server and with peers. The default port is 17472. For more information, see [ServerPort on page 232](#).
LogVerbosityLevel	The level of logging on the endpoint. The following values are best practices for specific scenarios: • `1` (default): Use this value during normal operation. • `41`: Use this value during troubleshooting. • `91` or higher: Use this value for full logging, for short periods of time only. **Note:** A value of `0` disables logging. As a best practice, do not disable logging.
Resolver	Add the `Resolver=nslookup` setting to enable host name resolution.

Note: For information about configuring additional settings, see [Modify Client settings on page 320](#) and [Tanium Client settings reference on page 393](#).

The following example commands are for a deployment with multiple Tanium Servers and

©2026 Tanium Inc. All Rights Reserved

Zone Servers:

```
cd <Tanium Client installation directory>
sudo ./TaniumClient config set ServerNameList \
ts1.example.com,ts2.example.com,zs1.example.com,zs2.example.com
sudo ./TaniumClient config set LogVerbosityLevel 1
sudo ./TaniumClient config set Resolver nslookup
```

4. Copy the tanium-init.dat file from the Tanium Server to the Tanium Client installation directory on the Solaris endpoint.
5. Run the following command to start the Tanium Client service:

```
svcadm enable taniumclient
```

6. Wait a few minutes for the Tanium Client to register with the Tanium Server or Zone Server, and then verify that the Client installed correctly and is communicating properly. For more information, see Verify the Tanium Client installation on page 228.

PERFORM UNATTENDED TANIUM CLIENT INSTALLATION

About this task

By default, the pkgadd utility performs a manual installation. The utility prompts for user intervention when it encounters operations that might be a security issue or conflict, such as running scripts with SUID, creating directories, or changing permissions. The utility provides a method to bypass these interventions and perform or abandon the installation. You accomplish this with a tanium.admin file, which contains operator identifiers and specifies what to do when the utility encounters security issues or conflicts.

1. Create the tanium.admin file with the following contents:

```
mail=
instance=overwrite
partial=nocheck
runlevel=nocheck
idepend=nocheck
rdepend=nocheck
space=nocheck
```

©2026 Tanium Inc. All Rights Reserved

```
setuid=nocheck
conflict=nocheck
action=nocheck
networktimeout=60
networkretries=3
authentication=quit
keystore=/var/sadm/security
proxy=
basedir=default
```

2. Run pkgadd with the `-a` option:

```
pkgadd -a tanium.admin -d ./TaniumClient-<client_version>-SunOS-5.10-<platform>.pkg
TaniumClient
```

CONFIGURE THE TANIUM CLIENT ON SOLARIS

About this task

The Tanium Client binary has statically linked libraries. All the libraries are in the standard default location (/lib) except libstdc++ and gcc. These two libraries are assumed to be in /usr/sfw/lib. If they are not, the Client does not start. If libstdc++ and gcc are not in /usr/sfw/lib, you must add the library search path to the Service Management Facility (SMF) taniumclient service:

1. Find the directory location of libgcc.* and libstdc++.*.
2. Run the following command to add the search path to the SMF service:
   `svccfg -s application/taniumclient setenv LD_LIBRARY_PATH /lib:/usr/lib:/usr/local/lib:/usr/sfw/lib`

Deploy the Tanium Client to AIX endpoints using a package file

On AIX endpoints, the Tanium Client is installed as a system service. The default installation directory for Tanium Client files is /opt/Tanium/TaniumClient.

©2026 Tanium Inc. All Rights Reserved

Tip: If your environment requires a different installation location for applications, you can create a symbolic link during installation.

The following procedures describe how to use the endpoint CLI to install the Tanium Client. For more information about using the CLI, see CLI on non-Windows endpoints on page 414.

For information about managing the Tanium Client service or uninstalling the Tanium Client after deployment, see Manage the Tanium Client on AIX on page 316.

Related information

- Manage the Tanium Client on AIX on page 316
- Preparing the Tanium Client on an AIX OS image on page 206
- Uninstall the Tanium Client on AIX on page 355
- Client version and operating system requirements on page 29
- Managing Client settings and Index configurations on page 318
- Tanium Client settings reference on page 393

PREPARE FOR INSTALLATION

1. Ensure that the endpoint meets the basic requirements on page 29 for the Tanium Client on AIX.
2. Ensure that host and network firewalls are configured to allow inbound and outbound TCP traffic on the ports that the Tanium Client uses. For more information, see Network connectivity, ports, and firewalls on page 63.
3. (AIX only) If they are not yet installed, install the IBM XL C++ runtime libraries file set (xlC.rte), version 16.1.0.0 or later, and the IBM LLVM runtime libraries file set (libc++.rte).
   Install the file sets as follows:

   a. Access the operating system CLI on the endpoint.
   b. Run the following commands to determine the versions of the currently installed xlC.rte bundle and the libc++.rte bundle:

   ```
   lslpp -l xlC\.*
   lslpp -l libc++\.*
   ```

   If the appropriate version of each bundle is already installed, skip to Install the Tanium Client on AIX using the command line on page 191. Otherwise, complete the

©2026 Tanium Inc. All Rights Reserved

remaining steps for each bundle that needs to be installed or updated.

c. Obtain the appropriate xlC.rte and libc++.rte bundles for your system from IBM Fix Central.
d. Download each bundle to your endpoint.
e. Extract, unzip, or untar each bundle to the /usr/sys/inst.images directory.
f. Install the bundles:

```
sudo installp -aXYgd /usr/sys/inst.images -e /tmp/install.log all
```

g. Review the installation log /tmp/install.log for any errors.

4. Sign in to the target endpoint.
5. Use the Tanium Client Management service to download the Client installer bundle to the AIX endpoint. From the Client Management **Overview** page, click **Download Installers** > **Download AIX Package**.
   The bundle (aix-client-bundle.zip) contains the following files:
   - install.sh
   - TaniumClient-<*version*>-powerpc.pkg
6. Download the tanium-init.dat file from a Client Deployment Template in the Tanium Client Management service:
   a. From the Main menu, go to **Shared Services >** Client Management.
   b. Go to **Client Installations** > **Client Deployment Templates**.
   c. In the row for a template, click Actions and select **Download tanium-init.dat**.
   d. Deploy Tanium Client using the appropriate installer or package file and the tanium-init.dat file you downloaded. For more information, see Deploying the Tanium Client using an installer or package file on page 153.

Tip: You must create a Client Deployment Template in Client Management before performing this step. For more information, see (Optional) Create a Client deployment template on page 137.

©2026 Tanium Inc. All Rights Reserved

Best Practice: Download the tanium-init.dat file for a Client Deployment Template in Client Management. Though you can also download tanium-init.dat through Tanium Console without creating a Client Deployment Template (see Download infrastructure configuration files (keys)), the installation process requires fewer manual configuration steps if you use these steps.

Important:
Be careful not to allow the tanium-init.dat file to be distributed or stored outside of your organization, such as in a publicly accessible source code repository or any other location accessible from the public internet. Limit the distribution to specific use in the deployment of Tanium Clients.

Though this file does not contain private keys and cannot be used to provide control over a Tanium environment, a user with malicious intent could use it to connect an unapproved Client and use this unauthorized access to learn how your organization is using Tanium.

7. Extract the files from the bundle, and copy the package file, tanium-init.dat, and, optionally, install.sh to a temporary directory on the endpoint. Make sure to keep the tanium-init.dat file in the same directory as the package file.

INSTALL THE TANIUM CLIENT ON AIX USING THE COMMAND LINE

Before you begin

Tip: The install.sh file provides an example of a script that performs an installation of the Tanium Client. By default, the script checks for a supported version of AIX, installs the appropriate Tanium Client package, and copies the tanium-init.dat file. You can modify this script with CLI commands that configure the Tanium Client settings that are necessary for your environment. You can then use the modified script for automated deployment of the Tanium Client. To run the install.sh script, you must have root or sudo permissions.

1. (Optional) To use a directory other than the default on page 490 for the Client installation, create a symbolic link. For example, to use the directory /appbin/Tanium, run the following command:

©2026 Tanium Inc. All Rights Reserved

```
ln -s /appbin/Tanium /opt/Tanium
```

Important: You must install the Tanium Client on a local fixed drive.

2. Run the following command from the temporary directory to install the package and generate a default configuration file:

```
sudo installp -agqXYd ./TaniumClient-<client_version>-powerpc.pkg TaniumClient
```

3. (For tanium-init.dat files that do not include Client settings) Use the CLI (see CLI on non-Windows endpoints on page 414) to configure the following basic Tanium Client settings.

Note: The `Resolver` Client setting is not included in the tanium-init.dat file by default. You must either create a separate Client Configuration for AIX that includes the custom Client setting `Resolver=nslookup` or manually set `Resolver=nslookup` using the CLI.

ServerName on page 231 or ServerNameList on page 230	In a deployment with a standalone Tanium Server, set the `ServerName` to the Server FQDN or IP address. In a deployment with Tanium Zone Servers or multiple Tanium Servers, configure `ServerNameList` with the FQDN or IP address of each Server, separated with a comma. **Important:** If the tanium-init.dat file specifies `ServerNameList`, you do not need to configure `ServerName` or `ServerNameList`; any setting that you specify here is added to the `ServerNameList` specified in tanium-init.dat. By default, the tanium-init.dat that you download through the Client Management service specifies `ServerNameList`, while the tanium-init.dat that you download through Tanium Console does not. You can use the `TaniumClient pki show <path_to_tanium-init.dat>` command on an endpoint where Tanium Client is already installed to view the `ServerNameList` that the tanium-init.dat file specifies. **Best Practice:** If the tanium-init.dat file does not include the **ServerNameList**, specify FQDNs for this setting.

©2026 Tanium Inc. All Rights Reserved

	Tip: You can optionally set the port that the Tanium Client uses to communicate with Servers by appending `:<port_number>` to the Server IP addresses or FQDNs (for example, `ts1.local.com:443,ts2.local.com:443,zs1.example.com:443`). The **ServerNameList** port values override the **ServerPort** setting for the Tanium Client (default is 17472).
ServerPort	The port that the Tanium Client uses for communication with the Tanium Server and with peers. The default port is 17472. For more information, see ServerPort on page 232.
LogVerbosityLevel	The level of logging on the endpoint. The following values are best practices for specific scenarios: • `1` (default): Use this value during normal operation. • `41`: Use this value during troubleshooting. • `91` or higher: Use this value for full logging, for short periods of time only. **Note:** A value of `0` disables logging. As a best practice, do not disable logging.
Resolver	The default hostname resolver for Tanium is getent. Because AIX generally does not have the getent command, add the `Resolver=nslookup` setting.

Note: For information about configuring additional settings, see Modify Client settings on page 320 and Tanium Client settings reference on page 393.

The following example commands are for a deployment with multiple Tanium Servers and Zone Servers:

```
cd <Tanium Client installation directory>
sudo ./TaniumClient config set ServerNameList \
ts1.example.com,ts2.example.com,zs1.example.com,zs2.example.com
sudo ./TaniumClient config set LogVerbosityLevel 1
sudo ./TaniumClient config set Resolver nslookup
```

4. Copy the tanium-init.dat file to the Tanium Client installation directory on the AIX endpoint.
5. Use the following command to start the Tanium Client service:

©2026 Tanium Inc. All Rights Reserved

```
startsrc -s taniumclient
```

6. Wait a few minutes for the Tanium Client to register with the Tanium Server or Zone Server, and then verify that the Client installed correctly and is communicating properly. For more information, see Verify the Tanium Client installation on page 228.

Preparing the Tanium Client on OS images

You can install the Tanium Client on an operating system (OS) image that you use as a template when provisioning an OS for new endpoints or virtual desktop infrastructure (VDI) instances.

The subsequent topics in this section describe best practices for preparing the Tanium Client on OS images.

- Windows on page 194
- macOS on page 197
- Linux on page 200
- Solaris on page 203
- AIX on page 206
- VDI on page 209

Information about registration and ComputerID (all operating systems)

When you start the OS image for the first time and the Tanium Client registers with the Tanium Server, the Server assigns a unique computer ID to the endpoint. The Tanium Server uses this computer ID to track and monitor each endpoint even if other identifiers change, such as the computer name, IP address, MAC address, or OS GUID. The Server detects and resolves duplicate IDs during registration to ensure each computer has a unique identifier, even if computers are cloned from an OS image that has a non-zero value for the computer ID.

Best Practice: To avoid the additional processing that is required to resolve duplicate IDs and the potential data infidelity during that processing, delete the Tanium Client ComputerID setting in the OS image. This removal is included in the image preparation steps in the subsequent sections for each OS.

Preparing the Tanium Client on a Windows OS image

©2026 Tanium Inc. All Rights Reserved

About this task

For complete details on Windows OS imaging, see Microsoft documentation.

Prepare the Tanium Client on a reference computer:

1. Install the Tanium Client. Review the endpoint requirements on page 33 and follow the steps in Deploy the Tanium Client to Windows endpoints using the installer on page 155. During the installation, make sure you do the following:
    - Configure the appropriate Server settings. For more information, see Configuring connections to the Tanium Core Platform on page 230.
    - Leave the **LogVerbosityLevel** setting at the default of `1`.
2. Open the Windows **Services** program, stop the **Tanium Client** service, and verify that its **Startup Type** is set to **Automatic**.
3. To avoid unnecessary processing to resolve conflicts or duplicates when deploying the image, use the CLI to delete the Tanium Client **ComputerID**, **RegistrationCount**, and **LastGoodServerName** settings:

    ```
    TaniumClient config remove ComputerID
    TaniumClient config remove RegistrationCount
    TaniumClient config remove LastGoodServerName
    ```

4. Use the CLI to configure any necessary Client settings that you did not configure during the initial installation. For more information, see CLI on Windows endpoints on page 413 and Tanium Client settings reference on page 393.
5. Delete the following files and directories in the Tanium Client installation directory on page 490:
    - pki.db
    - The Downloads directory, including all subdirectories and files
    - The Logs directory, including all subdirectories and files
    - The Backup directory, including all subdirectories and files
6. (Optional) For an image that you plan to use for a long period of time without updates, also delete all of the following files and directories within the Tanium Client installation directory on page 490 to ensure a fresh installation of up-to-date endpoint tools when you provision each endpoint:
    - TaniumClientExtensions.dll

©2026 Tanium Inc. All Rights Reserved

- TaniumClientExtensions.dll.sig
- The Extensions directory, including all subdirectories and files
- The Tools directory, including all subdirectories and files

Important: Do not delete the Tools directory without also deleting the Extensions directory and the listed files. Endpoint tools might not be reinstalled on endpoints that still have the listed files.

Note: Deleting all of these additional files and directories ensures a fresh installation of up-to-date endpoint tools when you provision each endpoint, but the endpoint requires more time and bandwidth to initialize the Tanium Client and deploy endpoint tools.

Tip: If you regularly update the image with Tanium Client upgrades and updated endpoint tools from your Tanium Client, it is not necessary to delete these additional directories and files. Newly provisioned endpoints that already have up-to-date endpoint tools require less time and bandwidth to initialize.

7. Obtain the latest tanium-init.dat file and add it to the Client.
   a. From the Main menu in Tanium Console, go to **Administration** > **Configuration** > **Infrastructure**.
   b. Click **Download**.
   c. Copy the downloaded file into the Tanium Client installation directory on page 490.

   Confirm that the date and time stamp of the file in the Tanium Client installation directory match the date and time stamp of that file on the Tanium Server (top-level installation directory).

©2026 Tanium Inc. All Rights Reserved

Note: If you are using Client Management, you can also obtain a version of tanium-init.dat that includes `ServerNameList` from the Client Configuration that is associated with the image you are preparing. When you use this version, the `ServerNameList` specified in tanium-init.dat overwrites the `ServerName` or `ServerNameList` that are specified in the Windows registry. For more information about managing Client Configurations in Client Management, see Managing Client settings and Index configurations on page 318. For more information about downloading a preconfigured version of tanium-init.dat, see (Optional) Download a tanium-init.dat file for alternative deployment on page 138.

Important:
Be careful not to allow the tanium-init.dat file to be distributed or stored outside of your organization, such as in a publicly accessible source code repository or any other location accessible from the public internet. Limit the distribution to specific use in the deployment of Tanium Clients.

Though this file does not contain private keys and cannot be used to provide control over a Tanium environment, a user with malicious intent could use it to connect an unapproved Client and use this unauthorized access to learn how your organization is using Tanium.

8. Shut down the computer and save the image.

Important: The Tanium Client service is configured to start automatically when the OS is started. If the reference computer is restarted before the reference image is captured, you might need to repeat these steps.

Related information

- Deploy the Tanium Client to Windows endpoints using the installer on page 155
- Manage the Tanium Client on Windows on page 293
- Uninstall the Tanium Client on Windows on page 351
- Client version and operating system requirements on page 29
- Managing Client settings and Index configurations on page 318
- Tanium Client settings reference on page 393

Preparing the Tanium Client on a macOS image

About this task

©2026 Tanium Inc. All Rights Reserved

For complete details on macOS imaging, see Apple documentation.

Prepare the Tanium Client on a reference computer:

1. Install the Tanium Client. Review the endpoint requirements on page 34 and follow the steps in Deploy the Tanium Client to macOS endpoints using the installer on page 165. During the installation, make sure you do the following:
    - Configure the appropriate Server settings. For more information, see Configuring connections to the Tanium Core Platform on page 230.
    - Leave the **LogVerbosityLevel** setting at the default of `1`.
2. Open **Terminal** and use the launchctl command to stop the Tanium Client daemon (sudo permissions are required):

    ```
    sudo launchctl unload /Library/LaunchDaemons/com.tanium.taniumclient.plist
    ```

3. To avoid unnecessary processing to resolve conflicts or duplicates when deploying the image, use the CLI to delete the Tanium Client **ComputerID**, **RegistrationCount**, and **LastGoodServerName** settings:

    ```
    sudo ./TaniumClient config remove ComputerID
    sudo ./TaniumClient config remove RegistrationCount
    sudo ./TaniumClient config remove LastGoodServerName
    ```

4. Use the CLI to configure any necessary Client settings that you did not configure during the initial installation. For more information, see CLI on non-Windows endpoints on page 414 and Tanium Client settings reference on page 393.
5. Delete the following files and directories in the Tanium Client installation directory on page 490:
    - pki.db
    - The Downloads directory, including all subdirectories and files
    - The Logs directory, including all subdirectories and files
    - The Backup directory, including all subdirectories and files
6. (Optional) For an image that you plan to use for a long period of time without updates, also delete all of the following files and directories within the Tanium Client installation directory on page 490 to ensure a fresh installation of up-to-date endpoint tools when you provision each endpoint:
    - libTaniumClientExtensions.dylib

©2026 Tanium Inc. All Rights Reserved

- libTaniumClientExtensions.dylib.sig
- The Extensions directory, including all subdirectories and files
- The Tools directory, including all subdirectories and files

Important: Do not delete the Tools directory without also deleting the Extensions directory and the listed files. Endpoint tools might not be reinstalled on endpoints that still have the listed files.

Note: Deleting all of these additional files and directories ensures a fresh installation of up-to-date endpoint tools when you provision each endpoint, but the endpoint requires more time and bandwidth to initialize the Tanium Client and deploy endpoint tools.

Tip: If you regularly update the image with Tanium Client upgrades and updated endpoint tools from your Tanium Client, it is not necessary to delete these additional directories and files. Newly provisioned endpoints that already have up-to-date endpoint tools require less time and bandwidth to initialize.

7. Obtain the latest tanium-init.dat file and add it to the Client.
   a. From the Main menu in Tanium Console, go to **Administration** > **Configuration** > **Infrastructure**.
   b. Click **Download**.
   c. Copy the downloaded file into the Tanium Client installation directory on page 490.

   Confirm that the date and time stamp of the file in the Tanium Client installation directory match the date and time stamp of that file on the Tanium Server (top-level installation directory).

©2026 Tanium Inc. All Rights Reserved

Note: If you are using Client Management, you can also obtain a version of tanium-init.dat that includes `ServerNameList` from the Client Configuration that is associated with the image you are preparing. When you use this version, the `ServerNameList` specified in tanium-init.dat overwrites the `ServerName` or `ServerNameList` that are specified in the Windows registry. For more information about managing Client Configurations in Client Management, see Managing Client settings and Index configurations on page 318. For more information about downloading a preconfigured version of tanium-init.dat, see (Optional) Download a tanium-init.dat file for alternative deployment on page 138.

Important:
Be careful not to allow the tanium-init.dat file to be distributed or stored outside of your organization, such as in a publicly accessible source code repository or any other location accessible from the public internet. Limit the distribution to specific use in the deployment of Tanium Clients.

Though this file does not contain private keys and cannot be used to provide control over a Tanium environment, a user with malicious intent could use it to connect an unapproved Client and use this unauthorized access to learn how your organization is using Tanium.

8. Shut down the computer and save the image.

Important: The Tanium Client service is configured to start automatically when the OS is started. If the reference computer is restarted before the reference image is captured, you might need to repeat these steps.

Related information

- Deploy the Tanium Client to macOS endpoints using the installer on page 165
- Manage the Tanium Client on macOS on page 305
- Uninstall the Tanium Client on macOS on page 352
- Client version and operating system requirements on page 29
- Managing Client settings and Index configurations on page 318
- Tanium Client settings reference on page 393

Preparing the Tanium Client on a Linux OS image

About this task

©2026 Tanium Inc. All Rights Reserved

Linux service commands vary by Linux distribution. This documentation provides examples but is not a reference for each Linux distribution. If you are not already familiar with installing and managing services on your target Linux distribution, review the documentation for the particular Linux operating system before starting.

Prepare the Tanium Client on a reference computer:

1. Install the Tanium Client. Review the endpoint requirements on page 36 and follow the steps in Deploy the Tanium Client to Linux endpoints using package files on page 173. Use the Tanium Client installation package file for your particular Linux distribution, as listed under Tanium Client package files for Linux on page 175. During the installation, make sure you do the following:
    - Configure the appropriate Server settings. For more information, see Configuring connections to the Tanium Core Platform on page 230.
    - Leave the **LogVerbosityLevel** setting at the default of `1`.
2. Stop the Tanium Client daemon by entering the service command for your Linux distribution. For more information, see Manage the Tanium Client service on Linux on page 313.
3. To avoid unnecessary processing to resolve conflicts or duplicates when deploying the image, use the CLI to delete the Tanium Client **ComputerID**, **RegistrationCount**, and **LastGoodServerName** settings:

    ```
    sudo ./TaniumClient config remove ComputerID
    sudo ./TaniumClient config remove RegistrationCount
    sudo ./TaniumClient config remove LastGoodServerName
    ```

4. Confirm that the Tanium Client daemon is in place in the system init directory. For example: /etc/init.d/TaniumClient or /etc/systemd/system/multi-user.target.wants/taniumclient.service. This ensures that the daemon is launched when the system is rebooted.
5. Use the CLI to configure any necessary Client settings that you did not configure during the initial installation. For more information, see CLI on non-Windows endpoints on page 414 and Tanium Client settings reference on page 393.
6. Delete the following files and directories in the Tanium Client installation directory on page 490:
    - pki.db
    - The Downloads directory, including all subdirectories and files
    - The Logs directory, including all subdirectories and files

©2026 Tanium Inc. All Rights Reserved

- The Backup directory, including all subdirectories and files

7. (Optional) For an image that you plan to use for a long period of time without updates, also delete all of the following files and directories within the Tanium Client installation directory on page 490 to ensure a fresh installation of up-to-date endpoint tools when you provision each endpoint:
   - libTaniumClientExtensions.so
   - libTaniumClientExtensions.so.sig
   - The Extensions directory, including all subdirectories and files
   - The Tools directory, including all subdirectories and files

   Important: Do not delete the Tools directory without also deleting the Extensions directory and the listed files. Endpoint tools might not be reinstalled on endpoints that still have the listed files.

   Note: Deleting all of these additional files and directories ensures a fresh installation of up-to-date endpoint tools when you provision each endpoint, but the endpoint requires more time and bandwidth to initialize the Tanium Client and deploy endpoint tools.

   Tip: If you regularly update the image with Tanium Client upgrades and updated endpoint tools from your Tanium Client, it is not necessary to delete these additional directories and files. Newly provisioned endpoints that already have up-to-date endpoint tools require less time and bandwidth to initialize.

8. Obtain the latest tanium-init.dat file and add it to the Client.
   a. From the Main menu in Tanium Console, go to **Administration** > **Configuration** > **Infrastructure**.
   b. Click **Download**.
   c. Copy the downloaded file into the Tanium Client installation directory on page 490.

   Confirm that the date and time stamp of the file in the Tanium Client installation directory match the date and time stamp of that file on the Tanium Server (top-level installation directory).

©2026 Tanium Inc. All Rights Reserved

Note: If you are using Client Management, you can also obtain a version of tanium-init.dat that includes `ServerNameList` from the Client Configuration that is associated with the image you are preparing. When you use this version, the `ServerNameList` specified in tanium-init.dat overwrites the `ServerName` or `ServerNameList` that are specified in the Windows registry. For more information about managing Client Configurations in Client Management, see Managing Client settings and Index configurations on page 318. For more information about downloading a preconfigured version of tanium-init.dat, see (Optional) Download a tanium-init.dat file for alternative deployment on page 138.

Important:
Be careful not to allow the tanium-init.dat file to be distributed or stored outside of your organization, such as in a publicly accessible source code repository or any other location accessible from the public internet. Limit the distribution to specific use in the deployment of Tanium Clients.

Though this file does not contain private keys and cannot be used to provide control over a Tanium environment, a user with malicious intent could use it to connect an unapproved Client and use this unauthorized access to learn how your organization is using Tanium.

9. Shut down the computer and save the image.

Important: The Tanium Client service is configured to start automatically when the OS is started. If the reference computer is restarted before the reference image is captured, you might need to repeat these steps.

Related information

- Deploy the Tanium Client to Linux endpoints using package files on page 173
- Manage the Tanium Client on Linux on page 308
- Uninstall the Tanium Client on Linux on page 354
- Client version and operating system requirements on page 29
- Managing Client settings and Index configurations on page 318
- Tanium Client settings reference on page 393

Preparing the Tanium Client on a Solaris OS image

About this task

©2026 Tanium Inc. All Rights Reserved

Prepare the Tanium Client on a reference computer:

1. Install the Tanium Client. Review the endpoint requirements on page 41 and follow the steps in Deploy the Tanium Client to Solaris endpoints using a package file on page 181. During the installation, make sure you do the following:
    - Configure the appropriate Server settings. For more information, see Configuring connections to the Tanium Core Platform on page 230.
    - Leave the **LogVerbosityLevel** setting at the default of `1`.
2. Stop the Tanium Client service by entering the following command:

    ```
    svcadm disable taniumclient
    ```

3. To avoid unnecessary processing to resolve conflicts or duplicates when deploying the image, use the CLI to delete the Tanium Client **ComputerID**, **RegistrationCount**, and **LastGoodServerName** settings:

    ```
    sudo ./TaniumClient config remove ComputerID
    sudo ./TaniumClient config remove RegistrationCount
    sudo ./TaniumClient config remove LastGoodServerName
    ```

4. Confirm that the Tanium Client daemon is in place in the system init directory (/etc/init.d/TaniumClient). This ensures that the daemon is launched when the system is rebooted.
5. Use the CLI to configure any necessary Client settings that you did not configure during the initial installation. For more information, see CLI on non-Windows endpoints on page 414 and Tanium Client settings reference on page 393.
6. Delete the following files and directories in the Tanium Client installation directory on page 490:
    - pki.db
    - The Downloads directory, including all subdirectories and files
    - The Logs directory, including all subdirectories and files
    - The Backup directory, including all subdirectories and files
7. (Optional) For an image that you plan to use for a long period of time without updates, also delete all of the following files and directories within the Tanium Client installation directory on page 490 to ensure a fresh installation of up-to-date endpoint tools when you provision each endpoint:
    - libTaniumClientExtensions.so

©2026 Tanium Inc. All Rights Reserved

- libTaniumClientExtensions.so.sig
- The Extensions directory, including all subdirectories and files
- The Tools directory, including all subdirectories and files

Important: Do not delete the Tools directory without also deleting the Extensions directory and the listed files. Endpoint tools might not be reinstalled on endpoints that still have the listed files.

Note: Deleting all of these additional files and directories ensures a fresh installation of up-to-date endpoint tools when you provision each endpoint, but the endpoint requires more time and bandwidth to initialize the Tanium Client and deploy endpoint tools.

Tip: If you regularly update the image with Tanium Client upgrades and updated endpoint tools from your Tanium Client, it is not necessary to delete these additional directories and files. Newly provisioned endpoints that already have up-to-date endpoint tools require less time and bandwidth to initialize.

8. Obtain the latest tanium-init.dat file and add it to the Client.
   a. From the Main menu in Tanium Console, go to **Administration** > **Configuration** > **Infrastructure**.
   b. Click **Download**.
   c. Copy the downloaded file into the Tanium Client installation directory on page 490.

   Confirm that the date and time stamp of the file in the Tanium Client installation directory match the date and time stamp of that file on the Tanium Server (top-level installation directory).

©2026 Tanium Inc. All Rights Reserved

Note: If you are using Client Management, you can also obtain a version of tanium-init.dat that includes `ServerNameList` from the Client Configuration that is associated with the image you are preparing. When you use this version, the `ServerNameList` specified in tanium-init.dat overwrites the `ServerName` or `ServerNameList` that are specified in the Windows registry. For more information about managing Client Configurations in Client Management, see Managing Client settings and Index configurations on page 318. For more information about downloading a preconfigured version of tanium-init.dat, see (Optional) Download a tanium-init.dat file for alternative deployment on page 138.

Important:
Be careful not to allow the tanium-init.dat file to be distributed or stored outside of your organization, such as in a publicly accessible source code repository or any other location accessible from the public internet. Limit the distribution to specific use in the deployment of Tanium Clients.

Though this file does not contain private keys and cannot be used to provide control over a Tanium environment, a user with malicious intent could use it to connect an unapproved Client and use this unauthorized access to learn how your organization is using Tanium.

9. Shut down the computer and save the image.

Important: The Tanium Client service is configured to start automatically when the OS is started. If the reference computer is restarted before the reference image is captured, you might need to repeat these steps.

Related information

- Deploy the Tanium Client to Solaris endpoints using a package file on page 181
- Manage the Tanium Client on Solaris on page 315
- Uninstall the Tanium Client on Solaris on page 355
- Client version and operating system requirements on page 29
- Managing Client settings and Index configurations on page 318
- Tanium Client settings reference on page 393

Preparing the Tanium Client on an AIX OS image

About this task

©2026 Tanium Inc. All Rights Reserved

Prepare the Tanium Client on a reference computer:

1. Install the Tanium Client. Review the endpoint requirements on page 41 and follow the steps in Deploy the Tanium Client to AIX endpoints using a package file on page 188. During the installation, make sure you do the following:
    - Configure the appropriate Server settings. For more information, see Configuring connections to the Tanium Core Platform on page 230.
    - Leave the **LogVerbosityLevel** setting at the default of `1`.
2. Stop the Tanium Client service by entering the following command:

    ```
    stopsrc -s taniumclient
    ```

3. To avoid unnecessary processing to resolve conflicts or duplicates when deploying the image, use the CLI to delete the Tanium Client **ComputerID**, **RegistrationCount**, and **LastGoodServerName** settings:

    ```
    sudo ./TaniumClient config remove ComputerID
    sudo ./TaniumClient config remove RegistrationCount
    sudo ./TaniumClient config remove LastGoodServerName
    ```

4. Confirm that the Tanium Client daemon is in place in the system init directory (/etc/inittab/TaniumClient). This ensures that the daemon is launched when the system is rebooted.
5. Use the CLI to configure any necessary Client settings that you did not configure during the initial installation. For more information, see CLI on non-Windows endpoints on page 414 and Tanium Client settings reference on page 393.
6. Delete the following files and directories in the Tanium Client installation directory on page 490:
    - pki.db
    - The Downloads directory, including all subdirectories and files
    - The Logs directory, including all subdirectories and files
    - The Backup directory, including all subdirectories and files
7. (Optional) For an image that you plan to use for a long period of time without updates, also delete all of the following files and directories within the Tanium Client installation directory on page 490 to ensure a fresh installation of up-to-date endpoint tools when you provision each endpoint:
    - libTaniumClientExtensions.so

©2026 Tanium Inc. All Rights Reserved

- libTaniumClientExtensions.so.sig
- The Extensions directory, including all subdirectories and files
- The Tools directory, including all subdirectories and files

Important: Do not delete the Tools directory without also deleting the Extensions directory and the listed files. Endpoint tools might not be reinstalled on endpoints that still have the listed files.

Note: Deleting all of these additional files and directories ensures a fresh installation of up-to-date endpoint tools when you provision each endpoint, but the endpoint requires more time and bandwidth to initialize the Tanium Client and deploy endpoint tools.

Tip: If you regularly update the image with Tanium Client upgrades and updated endpoint tools from your Tanium Client, it is not necessary to delete these additional directories and files. Newly provisioned endpoints that already have up-to-date endpoint tools require less time and bandwidth to initialize.

8. Obtain the latest tanium-init.dat file and add it to the Client.
   a. From the Main menu in Tanium Console, go to **Administration** > **Configuration** > **Infrastructure**.
   b. Click **Download**.
   c. Copy the downloaded file into the Tanium Client installation directory on page 490.

   Confirm that the date and time stamp of the file in the Tanium Client installation directory match the date and time stamp of that file on the Tanium Server (top-level installation directory).

©2026 Tanium Inc. All Rights Reserved

Note: If you are using Client Management, you can also obtain a version of tanium-init.dat that includes `ServerNameList` from the Client Configuration that is associated with the image you are preparing. When you use this version, the `ServerNameList` specified in tanium-init.dat overwrites the `ServerName` or `ServerNameList` that are specified in the Windows registry. For more information about managing Client Configurations in Client Management, see Managing Client settings and Index configurations on page 318. For more information about downloading a preconfigured version of tanium-init.dat, see (Optional) Download a tanium-init.dat file for alternative deployment on page 138.

Important:
Be careful not to allow the tanium-init.dat file to be distributed or stored outside of your organization, such as in a publicly accessible source code repository or any other location accessible from the public internet. Limit the distribution to specific use in the deployment of Tanium Clients.

Though this file does not contain private keys and cannot be used to provide control over a Tanium environment, a user with malicious intent could use it to connect an unapproved Client and use this unauthorized access to learn how your organization is using Tanium.

9. Shut down the computer and save the image.

Important: The Tanium Client service is configured to start automatically when the OS is started. If the reference computer is restarted before the reference image is captured, you might need to repeat these steps.

Related information

- Deploy the Tanium Client to AIX endpoints using a package file on page 188
- Manage the Tanium Client on AIX on page 316
- Uninstall the Tanium Client on AIX on page 355
- Client version and operating system requirements on page 29
- Managing Client settings and Index configurations on page 318
- Tanium Client settings reference on page 393

Preparing the Tanium Client on a virtual desktop infrastructure (VDI) instance

About this task

©2026 Tanium Inc. All Rights Reserved

For licensing and performance considerations that apply in VDI environments, see Assess the environment where you are deploying the Tanium Client on page 120.

Tip: To help simplify future management of VDI endpoints, consider creating computer groups with custom tag-based membership and applying corresponding custom tags to VDI endpoints. For more information, see Manage custom tags for computer groups.

Create a VDI golden image by preparing a reference endpoint:

1. Prepare the Tanium Client based on the OS of the intended endpoints:
   - Preparing the Tanium Client on a Windows OS image on page 194
   - Preparing the Tanium Client on a Linux OS image on page 200
   - Preparing the Tanium Client on a macOS image on page 197
   - Preparing the Tanium Client on a Solaris OS image on page 203
   - Preparing the Tanium Client on an AIX OS image on page 206

   Note: It is not necessary to delete the **ComputerID** setting during this step, since the Client will reregister with the Tanium Server or Tanium Zone Server during the following additional steps. You delete this setting in a later step.

2. Check the **ComputerID**, which should be a non-zero numeric value, to verify that the Client has registered with the Tanium Server or Tanium Zone Server. In the endpoint CLI, navigate to the Tanium Client installation directory on page 490, and run one of the following commands based on the OS:
   - Windows: `TaniumClient config get ComputerID`
   - Non-Windows: `sudo ./TaniumClient config get ComputerID`

3. Review the action history in Tanium Console to make sure that the Client runs any scheduled actions that affect the Client Configuration. For more information, see Manage actions that are completed or in progress.
   To run actions immediately instead of waiting for them to run according to a schedule, use one-time actions to deploy the associated packages to the endpoint that hosts the golden

©2026 Tanium Inc. All Rights Reserved

image. For more information, see Deploying actions.

4. From each solution in Tanium Console, deploy any endpoint tools that are required by the Tanium solutions that you plan to use with VDI instances. The tool deployment method varies for each solution.
   For example, if you are using Threat Response, create a profile that includes all components that you plan to use with VDI instances, and deploy that profile to the endpoint. The deployment includes any tools that the Threat Response profile requires, such as Tanium™ Index if you included an index configuration.

   For more information about how to deploy tools for a solution, review the User Guide for that solution.

5. Allow any processes that endpoint tools initiate to complete on the endpoint. To determine whether these processes have completed, ask a question from Tanium Console using a sensor that returns tool status for each solution or Client Extension.
   For example, if you are using a Threat Response profile with an index configuration, ask the question: `Get Client Extensions - Status from all machines with Computer Name contains <reference_computer_hostname>`. In the results, for the domain `threatresponse` and the key `initial_index_scan_complete`, make sure that the value is `true`.

©2026 Tanium Inc. All Rights Reserved

Note:

If you are using Index tools with a solution (such as Threat Response, Reveal, Integrity Monitor, or Asset), the following considerations apply:

- The default "distribute over time" value for the initial index scan is 24 hours, which means that the initial scan occurs at a random time within 24 hours after Index is deployed to the endpoint. Under typical circumstances, this delay helps to reduce resource use during initial deployment. To avoid the delay when creating an image, temporarily set the **CX.index.FirstScanDistributeOverTimeMinutes** setting to `0`. In the endpoint CLI, navigate to the Tanium Client installation directory on page 490, and run one of the following commands based on the OS:
  - Windows: `TaniumClient config set CX.index.FirstScanDistributeOverTimeMinutes 0`
  - Non-Windows: `sudo ./TaniumClient config set CX.index.FirstScanDistributeOverTimeMinutes 0`

  After the index scan has started but before saving the image, make sure to restore the original setting to reduce resource use when you create new endpoints from the image. Run one of the following commands based on the OS:
  - Windows: `TaniumClient config set CX.index.FirstScanDistributeOverTimeMinutes 1440`
  - Non-Windows: `sudo ./TaniumClient config set CX.index.FirstScanDistributeOverTimeMinutes 1440`
- Even when you start the initial index scan immediately, it might take significantly longer to complete than other processes. Make sure that the initial index scan completes before continuing.

For more information about how to determine tool status for a solution, review the User Guide for that solution.

6. Stop the Tanium Client service:

©2026 Tanium Inc. All Rights Reserved

- Manage the Tanium Client service on Windows on page 293
- Manage the Tanium Client service on macOS on page 308
- Manage the Tanium Client service on Linux on page 313
- Manage the Tanium Client service on Solaris on page 315
- Manage the Tanium Client service on AIX on page 317

7. Verify that the service has stopped and that it is configured to start automatically on the next reboot.
8. To avoid unnecessary processing to resolve conflicts or duplicates when you later deploy the image, use the CLI to delete the Tanium Client **ComputerID** setting:
   - Windows: `TaniumClient config remove ComputerID`
   - Non-Windows: `sudo ./TaniumClient config remove ComputerID`
9. Add or update the following settings through the CLI. These settings help to avoid the concentration of resource usage that otherwise might occur as a consequence of cloning and shared hardware. The CLI syntax depends on the endpoint OS:
   - Windows: `TaniumClient config set <setting>`
   - Non-Windows: `sudo ./TaniumClient config set <setting>`

Best practice Client settings for VDI instances

Client Setting	Default Value	Best Practice Value for VDI	Explanation
RandomSensorDelayInSeconds	0	5	By default, sensors run immediately. This setting delays the execution of any sensor by a random time up to 5 seconds, which reduces concurrent execution of sensors and packages.

©2026 Tanium Inc. All Rights Reserved

Client Setting	Default Value	Best Practice Value for VDI	Explanation
			Note: If poor performance occurs on VDI infrastructure, you can increase this value incrementally up to `20`.
MaxAgeMultiplier	1	2	Each sensor has a **Max Sensor Age** setting that determines how long the Client caches sensor results for subsequent questions that include the same sensor. This setting causes the Client to multiply the maximum age configured for each sensor by 2, which doubles the time results are cached for each sensor and reduces sensor executions.
MinDistributeOverTimeInSeconds	0	60	Each action has a **Distribute Over** setting that randomizes the distribution of that action over the specified time. By default, no minimum applies, and some actions might be configured for immediate distribution. This setting forces all actions to distribute over at least 1 minute.
SaveClientStateIntervalInSeconds	300	1800	By default, the Client state is written to disk every 5 minutes. This setting increases the time to 30 minutes to reduce disk writes.

Best Practice: To minimize disk writes, leave **LogVerbosityLevel** and **Logs.extensions.LogVerbosityLevel** set to their default values of `1` and `11` respectively. Do not disable logging.

10. Shut down the reference machine or block network access to the Tanium Server so that the Tanium Client on the reference machine does not register with the Server, and then save the image.

Next steps

©2026 Tanium Inc. All Rights Reserved

Note: The Tanium Client service is configured to start automatically when the OS is started. If the reference machine is restarted before the reference image is captured, you might need to repeat these steps.

Tip: For information about identifying and tuning Tanium Client settings for existing VDI endpoints, see Tuning Tanium Client settings for VDI endpoints and other endpoints with limited resources on page 407.

Deploy the Tanium Client in Microsoft Azure environments using the Tanium™ Client VM extension

Tanium provides Azure virtual machine (VM) extensions that can be installed to automatically deploy the Tanium Client on Microsoft Azure VMs and VM Scale Sets.

Tip: You can use alternative methods to deploy the Tanium Client to Azure VMs, such as the Tanium Client Management service on page 125. However, the Tanium Client VM extension provides a mechanism to easily enforce installation of the Tanium Client in Azure environments where users routinely create new VMs.

Requirements for the Tanium Client VM extension

OPERATING SYSTEM SUPPORT IN MICROSOFT AZURE

The Tanium Client supports both Windows and Linux VMs in Azure. Supported versions and Linux distributions are the same as for any endpoint; see Client version and operating system requirements on page 29. However, for Linux VMs in Azure, the Tanium Client VM extension is supported only on Linux distributions that are both endorsed by Microsoft and supported by the Tanium Client. For a list of Linux distributions that are endorsed by Microsoft, see Microsoft Azure Documentation: Endorsed Linux distributions on Azure.

Tanium provides separate Azure VM extensions for Windows and Linux VMs.

©2026 Tanium Inc. All Rights Reserved

NETWORK CONNECTIVITY

Each VM must be able to connect to https://content.tanium.com for the VM extension to import the files needed to deploy the Tanium Client.

Installation methods for the Tanium Client VM extension

When you install the Tanium Client VM extension on a VM, it automatically deploys the Tanium Client to the VM using the settings that you configure in the extension properties.

You can install the extension using the following methods:

- Manually install the extension on a VM using the Azure Portal, Azure CLI or Azure PowerShell.
- Configure the extension as a resource in an Azure Resource Manager (ARM) template. This method is useful if you deploy VMs from a controlled set of ARM templates.
- Configure the extension as a resource in an Azure Policy. This method is useful if multiple teams deploy VMs and use a variety of templates that are not closely controlled, and it can install the extension on existing VMs.

For more information about using Azure VM extensions, see Microsoft Azure Documentation: Azure virtual machine extensions and features.

Tip: This topic provides general guidance to use standard Microsoft Azure features to install the Tanium Client VM extension. If you are unfamiliar with these features, see Knowledge Article: Using an Azure Virtual Machine Extension to Install and Register a Tanium Client (sign-in required) for a detailed walkthrough.

Each of these methods requires you to supply a tanium-init.dat file for your environment. You can create a Tanium Client initialization profile in Tanium™ Integrations Gallery to create this file, and optionally copy the base64 version as needed during installation. For more information, see Create a Tanium Client initialization profile.

©2026 Tanium Inc. All Rights Reserved

Tip: You can include a custom tag that identifies endpoints where the Tanium Client was deployed by the Tanium Client VM extension, such as `InstalledByAzure`. For more information, see General Client deployment settings on page 143.

MANUALLY INSTALL THE EXTENSION USING THE AZURE PORTAL, AZURE CLI, OR AZURE POWERSHELL

You can manually install the Tanium Client VM extension on an existing VM resource using the following methods:

- **Azure Portal:** the **Extensions + Applications** menu
- **Azure CLI:** the `az vm extension set` command
- **Azure PowerShell:** the `Set-AzVMExtension` command

For more information about manually installing extensions, see the following Microsoft Azure documentation:

- Microsoft Azure Documentation: Virtual machine extensions and features for Linux
- Microsoft Azure Documentation: Virtual machine extensions and features for Windows.

For the properties to use to include the extension using Azure CLI or Azure PowerShell, see Resource properties for the Tanium Client VM extension on page 224. For the properties to configure the extension using any available method, see Tanium Client VM extension properties on page 224.

The following example demonstrates using the Azure CLI to manually install the Tanium Client VM extension on an existing Linux VM:

```
declare _base64_tanium_init_dat=$(base64 < "./tanium-init.dat")
az vm extension set --name TaniumClientLinux \
  --publisher Tanium.Client \
  --vm-name MyLinuxVM \
  --resource-group MyResourceGroup \
  --protected-settings
'{"TaniumInitDat":"'$_base64_tanium_init_dat'","TaniumServer":"MyTaniumServer"}
```

CONFIGURE AN AZURE RESOURCE MANAGER TEMPLATE

If you deploy VMs from a controlled set of ARM templates, you can add the Tanium Client VM extension to these templates to automatically deploy the Tanium Client on all newly deployed

©2026 Tanium Inc. All Rights Reserved

VMs. Include the Tanium Client VM extension in the `resources` of each ARM template and specify the properties as appropriate.

For information about creating VMs from ARM templates, see Microsoft Azure Documentation: How to create a Linux virtual machine with Azure Resource Manager templates and Microsoft Azure Documentation: Create a Windows virtual machine from a Resource Manager template.

For the properties to use in the template JSON, see Resource properties for the Tanium Client VM extension on page 224 and Tanium Client VM extension properties on page 224.

The following example provides sample JSON from the `resources` of an ARM template to deploy the Tanium Client on a Linux VM and configure a proxy server.

```
{
      "name": "[concat(parameters('vmName'),'/TaniumClientLinux')]",
      "type": "Microsoft.Compute/virtualMachines/extensions",
      "location": "[resourceGroup().location]",
      "dependsOn": [
        "[concat('Microsoft.Compute/virtualMachines/', parameters('vmName'))]"
      ],
      "apiVersion": "2015-06-15",
      "properties": {
        "publisher": "Tanium.Client",
        "type": "TaniumClientLinux",
        "typeHandlerVersion": "1.1",
        "autoUpgradeMinorVersion": true,
        "settings": {},
        "protectedSettings": {
          "TaniumInitDat":
"TG9yZW0gaXBzdW0gb2RvciBhbWV0LCBjb25zZWN0ZXR1ZXIgYWRpcGlzY2luZyBlbGl

0LiBNdXMgaW1wZXJkaWV0IGEgZGljdHVtIGxlY3R1cyBtb250ZXMgcGVuYXRpYnVzIGluY2VwdG9zIGFyY3Uu

IFNhcGllbiBmcmluZ2lsbGEgc2FwaWVuIHB1bHZpbmFyIHRlbXB1czsgbmVjIGlhY3VsaXMgbnVuYy4gRXQgd

GluY2lkdW50IG5hbSBkaWFtIG51bGxhbSBsYWNpbmlhIGVnZXQuIFF1aXMgYmliZW5kdW0gc29sbGljaXR1ZG

luIGNvbmd1ZSBtb3JiaSBsb2JvcnRpcyB2ZWxpdCBpbmNlcHRvcyBldWlzbW9kLiBMb3JlbSBlZ2VzdGFzIGh

pbWVuYWVvcyBjdXJzdXMgdml2YW11cyBhYyBwaGFzZWxsdXMgb3JuYXJlIG9kaW8uIERpY3R1bXN0IG1hdXJp

cyBlcmF0IGludGVyZHVtIHByaW1pcyBlZ2VzdGFzIGF0IGxlY3R1cy4KClNvbGxpY2l0dWRpbiBzZW0gaGVuZ

HJlcml0IGV1IG51bmMgcGVyIHNhZ2l0dGlzIHVsdHJpY2VzIGNvbnNlY3RldHVyPyBTb2Npb3NxdSBwdXJ1cy

BtYWduYSB2aXZlcnJhIGJsYW5kaXQgY2xhc3MgcHVsdmluYXIgcGFydHVyaWVudC4gTnVsbGFtIGZldWdpYXQ

gY29uc2VxdWF0IHNhZ2l0dGlzIHVybmEgcXVhbSBpcHN1bSBmYW1lcyBzZW5lY3R1cy4gU3VzcGVuZGlzc2Ug

cG9zdWVyZSBpcHN1bSBtb2xsaXMgbmVxdWUgbmF0b3F1ZSBjcmFzLiBDb25zZXF1YXQgdm9sdXRwYXQgdHJpc

3RpcXVlIGNvbnNlY3RldHVyIGVsaXQgZHVpIGhlbmRyZXJpdCBjdWJpbGlhLiBGYWNpbGlzaSBlcm9zIHBsYW

NlcmF0IGRpYW0gZmFjaWxpc2kgdWx0cmljZXMgdmVzdGlidWx1bSB1bGxhbWNvcnBlciBlcm9zLiBMaWd1bGE

ganVzdG8gbWF1cmlzIGlwc3VtIHBvcnR0aXRvciBiaWJlbmR1bSBhbWV0IGF1Z3VlLiBWYXJpdXMgbGFjaW5p
```

```
YSBtaSBlbGVpZmVuZCBwcm9pbiBzZW1wZXIgc29jaW9zcXUuCgpUZW1wb3IgbWF0dGlzIGNyYXMgYXVjdG9yH

F1YW0sIGV1IGFkLiBOZXR1cyBwaGFzZWxsdXMgaW5jZXB0b3MgYWxpcXVhbSBkaWFtIGNvbW1vZG8gbGFjaW5

pYSBmYWNpbGlzaS4gTmVxdWUgbWF0dGlzIHBlbGxlbnRlc3F1ZSBudW5jIHJpc3VzIGxpZ3VsYSBhdWN0b3Ig

cHJpbWlzIHVsdHJpY2VzLiBUb3JxdWVudCBzY2VsZXJpc3F1ZSB2b2x1dHBhdCBjb21tb2RvIG5pc2wgdmVsL
          iBJYWN1bGlzIG5vbiBjb25kaW1lbnR1bSBtb3JiaS4K",
          "TaniumServer": "mytaniumserver.mydomain",
          "TaniumProxyServers": "myproxyserver.mydomain:1234"
        }
      }
    }
```

Tip: You can also use parameters in Azure CLI or Azure PowerShell to provide properties, which can be useful for providing the tanium-init.dat file. For an example, see Use a parameter in the template or policy JSON to import the file directly on page 227.

CONFIGURE AZURE POLICIES

If multiple teams deploy VMs and use a variety of templates that are not closely controlled, you can add the Tanium Client VM extension to an Azure Policy to deploy the Tanium Client on both new and pre-existing VMs. Include the Tanium Client VM extension in the `resources` of a policy with the `effect` of `deployIfNotExists`, and specify the properties as appropriate. You can assign policies to management groups, subscriptions, resource groups, and resources.

Note: Tanium provides separate Azure VM extensions for Windows and Linux VMs, and you must configure separate policies for Windows and Linux VMs.

For information about creating and assigning Azure Policies, see Microsoft Azure Documentation: Azure Policy documentation.

For the properties to use in the policy JSON, see Resource properties for the Tanium Client VM extension on page 224 and Tanium Client VM extension properties on page 224.

The following examples provide sample Azure Policies that install the Tanium Client VM extension on VMs where it is not yet deployed.

```
{
      "if": {
```

©2026 Tanium Inc. All Rights Reserved

```
        "allOf": [
          {
            "field": "type",
            "equals": "Microsoft.Compute/virtualMachines"
          },
          {
            "field": "Microsoft.Compute/imagePublisher",
            "equals": "MicrosoftWindowsServer"
          },
          {
            "field": "Microsoft.Compute/imageOffer",
            "equals": "WindowsServer"
          },
          {
            "field": "Microsoft.Compute/imageSKU",
            "in": ["2016-Datacenter"]
          }
        ]
      },
      "then": {
        "effect": "deployIfNotExists",
        "details": {
          "type": "Microsoft.Compute/virtualMachines/extensions",
          "evaluationDelay": "AfterProvisioningSuccess",
          "existenceCondition": {
            "allOf": [
              {
                "field": "Microsoft.Compute/virtualMachines/extensions/type",
                "equals": "TaniumClientWindows"
              },
              {
                "field": "Microsoft.Compute/virtualMachines/extensions/publisher",
                "equals": "Tanium.Client"
              }
            ]
          },
          "roleDefinitionIds": [
            "/subscriptions/{subscriptionId}/providers/Microsoft.Authorization/
roleDefinitions/{builtinroleGUID}"
          ],
          "deployment": {
            "properties": {
              "mode": "incremental",
              "template": {
                "$schema": "http://schema.management.azure.com/schemas/2015-01-01/
deploymentTemplate.json#",
                "contentVersion": "1.0.0.0",
                "parameters": {
                  "vmName": {
                    "type": "string"
                  },
                  "location": {
                    "type": "string"
                  }
                }
                "resources": [
                  {
                    "name": "[concat(parameters('vmName'),'/TaniumClientWindows')]",
                    "type": "Microsoft.Compute/virtualMachines/extensions",
                    "location": "[parameters('location')]",
                    "dependsOn": [
                      "[concat('Microsoft.Compute/virtualMachines/', parameters('vmName'))]"
                    ],
                    "apiVersion": "2017-12-01",
```

```
                    "properties": {
                      "publisher": "Tanium.Client",
                      "type": "TaniumClientWindows",
                      "typeHandlerVersion": "1.1",
                      "autoUpgradeMinorVersion": true,
                      "settings": {},
                      "protectedSettings": {
                        "TaniumInitDat":
"TG9yZW0gaXBzdW0gb2RvciBhbWV0LCBjb25zZWN0ZXR1ZXIgYWRpcGlzY2luZyBlbGl

0LiBNdXMgaW1wZXJkaWV0IGEgZGljdHVtIGxlY3R1cyBtb250ZXMgcGVuYXRpYnVzIGluY2VwdG9zIGFyY3Uu

IFNhcGllbiBmcmluZ2lsbGEgc2FwaWVuIHB1bHZpbmFyIHRlbXB1czsgbmVjIGlhY3VsaXMgbnVuYy4gRXQgd

GluY2lkdW50IG5hbSBkaWFtIG51bGxhbSBsYWNpbmlhIGVnZXQuIFF1aXMgYmliZW5kW0gc29sbGljaXR1ZG

luIGNvbmd1ZSBtb3JiaSBsb2JvcnRpcyB2ZWxpdCBpbmNlcHRvcyBldWlzbW9kLiBMb3JlbSBlZ2VzdGFzIGh

pbWVuYWVvcyBjdXJzdXMgdml2YW11cyBhYyBwaGFzZWxsdXMgb3JuYXJlIG9kaW8uIERpY3R1bXN0IG1hdXJp

cyBlcmF0IGludGVyZHVtIHByaW1pcyBlZ2VzdGFzIGF0IGxlY3R1cy4KClNvbGxpY2l0dWRpbiBzZW0gaGVuZ

HJlcml0IGV1IG51bmMgcGVyIHNhZ2l0dGlzIHVsdHJpY2VzIGNvbnNlY3RldHVyPyBTb2Npb3NxdSBwdXJ1cy

BtYWduYSB2aXZlcnJhIGJsYW5kaXQgY2xhc3MgcHVsdmluYXIgcGFydHVyaWVudC4gTnVsbGFtIGZldWdpYXQ

gY29uc2VxdWF0IHNhZ2l0dGlzIHVybmEgcXVhbSBpcHN1bSBmYW1lcyBzZW5lY3R1cy4gU3VzcGVuZGlzc2Ug

cG9zdWVyZSBpcHN1bSBtb2xsaXMgbmVxdWUgbmF0b3F1ZSBjcmFzLiBDb25zZXF1YXQgdm9sdXRwYXQgdHJpc

3RpcXVlIGNvbnNlY3RldHVyIGVsaXQgZHVpIGhlbmRyZXJpdCBjdWJpbGlhLiBGYWNpbGlzaSBlcm9zIHBsYW

NlcmF0IGRpYW0gZmFjaWxpc2kgdWx0cmljZXMgdmVzdGlidWx1bSB1bGxhbWNvcnBlciBlcm9zLiBMaWd1bGE

ganVzdG8gbWF1cmlzIGlwc3VtIHBvcnR0aXRvciBiaWJlbmR1bSBhbWV0IGF1Z3VlLiBWYXJpdXMgbGFjaW5p

YSBtaSBlbGVpZmVuZCBwcm9pbiBzZW1wZXIgc29jaW9zcXUuCgpUZW1wb3IgbWF0dGlzIGNyYXMgYXVjdG9yH

F1YW0sIGV1IGFkLiBOZXR1cyBwaGFzZWxsdXMgaW5jZXB0b3MgYWxpcXVhbSBkaWFtIGNvbW1vZG8gbGFjaW5

pYSBmYWNpbGlzaS4gTmVxdWUgbWF0dGlzIHBlbGxlbnRlc3F1ZSBudW5jIHJpc3VzIGxpZ3VsYSBhdWN0b3Ig

cHJpbWlzIHVsdHJpY2VzLiBUb3JxdWVudCBzY2VsZXJpc3F1ZSB2b2x1dHBhdCBjb21tb2RvIG5pc2wgdmVsL
                        iBJYWN1bGlzIG5vbiBjb25kaW1lbnR1bSBtb3JiaS4K",
                        "TaniumServer": "mytaniumserver.mydomain",
                        "TaniumProxyServers": "myproxyserver.mydomain:1234"
                      }
                    }
                  }
                ]
              }
            }
          }
        }
      }
    }
```

```
{
      "if": {
        "allOf": [
          {
            "field": "type",
            "equals": "Microsoft.Compute/virtualMachines"
          },
```

©2026 Tanium Inc. All Rights Reserved

```
          {
            "field": "Microsoft.Compute/imagePublisher",
            "equals": "Canonical"
          },
          {
            "field": "Microsoft.Compute/imageOffer",
            "equals": "0001-com-ubuntu-server-jammy"
          },
          {
            "field": "Microsoft.Compute/imageSKU",
            "in": ["22_04-lts-gen2"]
          }
        ]
      },
      "then": {
        "effect": "deployIfNotExists",
        "details": {
          "type": "Microsoft.Compute/virtualMachines/extensions",
          "evaluationDelay": "AfterProvisioningSuccess",
          "existenceCondition": {
            "allOf": [
              {
                "field": "Microsoft.Compute/virtualMachines/extensions/type",
                "equals": "TaniumClientLinux"
              },
              {
                "field": "Microsoft.Compute/virtualMachines/extensions/publisher",
                "equals": "Tanium.Client"
              }
            ]
          },
          "roleDefinitionIds": [
            "/subscriptions/{subscriptionId}/providers/Microsoft.Authorization/
roleDefinitions/{builtinroleGUID}"
          ],
          "deployment": {
            "properties": {
              "mode": "incremental",
              "template": {
                "$schema": "http://schema.management.azure.com/schemas/2015-01-01/
deploymentTemplate.json#",
                "contentVersion": "1.0.0.0",
                "parameters": {
                  "vmName": {
                    "type": "string"
                  },
                  "location": {
                    "type": "string"
                  }
                }
                "resources": [
                  {
                    "name": "[concat(parameters('vmName'),'/TaniumClientLinux')]",
                    "type": "Microsoft.Compute/virtualMachines/extensions",
                    "location": "[parameters('location')]",
                    "dependsOn": [
                      "[concat('Microsoft.Compute/virtualMachines/', parameters('vmName'))]"
                    ],
                    "apiVersion": "2017-12-01",
                    "properties": {
                      "publisher": "Tanium.Client",
                      "type": "TaniumClientLinux",
                      "typeHandlerVersion": "1.1",
                      "autoUpgradeMinorVersion": true,
```

```
                    "settings": {},
                    "protectedSettings": {
                      "TaniumInitDat":
"TG9yZW0gaXBzdW0gb2RvciBhbWV0LCBjb25zZWN0ZXR1ZXIgYWRpcGlzY2luZyBlbGl

0LiBNdXMgaW1wZXJkaWV0IGEgZGljdHVtIGxlY3R1cyBtb250ZXMgcGVuYXRpYnVzIGluY2VwdG9zIGFyY3Uu

IFNhcGllbiBmcmluZ2lsbGEgc2FwaWVuIHB1bHZpbmFyIHRlbXB1czsgbmVjIGlhY3VsaXMgbnVuYy4gRXQgd

GluY2lkdW50IG5hbSBkaWFtIG51bGxhbSBsYWNpbmlhIGVnZXQuIFF1aXMgYmliZW5kdW0gc29sbGljaXR1ZG

luIGNvbmd1ZSBtb3JiaSBsb2JvcnRpcyB2ZWxpdCBpbmNlcHRvcyBldWlzbW9kLiBMb3JlbSBlZ2VzdGFzIGh

pbWVuYWVvcyBjdXJzdXMgdml2YW11cyBhYyBwaGFzZWxsdXMgb3JuYXJlIG9kaW8uIERpY3R1bXN0IG1hdXJp

cyBlcmF0IGludGVyZHVtIHByaW1pcyBlZ2VzdGFzIGF0IGxlY3R1cy4KClNvbGxpY2l0dWRpbiBzZW1wZXIgc

3RpcXVlIGNvbnNlY3RldHVyIGVsaXQgZHVpIGhlbmRyZXJpdCBjdWJpbGlhLiBGYWNpbGlzaSBlcm9zIHBsYW

NlcmF0IGRpYW0gZmFjaWxpc2kgdWx0cmljZXMgdmVzdGlidWx1bSB1bGxhbWNvcnBlciBlcm9zLiBMaWd1bGE

ganVzdG8gbWF1cmlzIGlwc3VtIHBvcnR0aXRvciBiaWJlbmR1bSBhbWV0IGF1Z3VlLiBWYXJpdXMgbGFjaW5p

YSBtaSBlbGVpZmVuZCBwcm9pbiBzZW1wZXIgc29jaW9zcXUuCgpUZW1wb3IgbWF0dGlzIGNyYXMgYXVjdG9yH

F1YW0sIGV1IGFkLiBOZXR1cyBwaGFzZWxsdXMgaW5jZXB0b3MgYWxpcXVhbSBkaWFtIGNvbW1vZG8gbGFjaW5

pYSBmYWNpbGlzaS4gTmVxdWUgbWF0dGlzIHBlbGxlbnRlc3F1ZSBudW5jIHJpc3VzIGxpZ3VsYSBhdWN0b3Ig

cHJpbWlzIHVsdHJpY2VzLiBUb3JxdWVudCBzY2VsZXJpc3F1ZSB2b2x1dHBhdCBjb21tb2RvIG5pc2wgdmVsL
                      iBJYWN1bGlzIG5vbiBjb25kaW1lbnR1bSBtb3JiaS4K",
                      "TaniumServer": "mytaniumserver.mydomain",
                      "TaniumProxyServers": "myproxyserver.mydomain:1234"
                    }
                  }
                }
              ]
            }
          }
        }
      }
    }
```


Tip: You can also use parameters in Azure CLI or Azure PowerShell to provide properties, which can be useful for providing the tanium-init.dat file. For an example, see Use a parameter in the template or policy JSON to import the file directly on page 227.

©2026 Tanium Inc. All Rights Reserved

Resource properties for the Tanium Client VM extension

The following table provides the properties of the Tanium Client VM extension to include in the `resources` of an ARM template on page 217 or an Azure Policy on page 219, or to install it using the `az vm extension set` command in Azure CLI on page 217 or the `Set-AzVMExtension` command in Azure PowerShell on page 217. Separate extensions are provided for Windows and Linux VMs.

Tanium Client VM extension resource properties

Azure VM extension JSON key	`az vm extension set` parameter in Azure CLI	`Set-AzVMExtension` parameter in Azure PowerShell	Value
`publisher`	`--publisher`	`-Publisher`	`Tanium.Client`
`type`	`--name`	`-Name`	• Windows VMs: `TaniumClientWindows` • Linux VMs: `TaniumClientLinux`
`typeHandlerVersion`	`--version`	`-TypeHandlerVersion`	Current version: 1.1

Tanium Client VM extension properties

Use the following settings to configure the deployment of the Tanium Client when you manually deploy on page 217 a virtual machine resource, create an ARM template on page 217, or create an Configure Azure Policies on page 219.

Tanium Client VM extension configuration properties

Setting in Azure Portal	JSON Key	Required	Description
Base 64 of tanium-init.dat	`TaniumInitDat`	Yes	Provides the contents of the tanium-init.dat file that you use to deploy the Tanium Client, encoded as base64. You can create a Tanium Client initialization profile in Tanium™ Integrations Gallery to create this file and optionally download the contents already

©2026 Tanium Inc. All Rights Reserved

Setting in Azure Portal	JSON Key	Required	Description
File			encoded as base64. For more information, see Create a Tanium Client initialization profile . **Tip:** For methods to convert a tanium-init.dat file to base64 (if you did not copy the base64 from Integrations Gallery), see Convert the tanium-init.dat file to base64 on page 227 .
Server Name	`TaniumServerName`	Yes	Specifies the FQDN or IP address of the Tanium Server or Zone Server FQDN or IP address with which the Client connects. If the tanium-init.dat file contains the **ServerNameList** setting, or if you specify a Server list for the VM, the first Server that the Tanium Client selects from the listed Servers overwrites this setting. For more information, see Configuring connections to the Tanium Core Platform on page 230 . **Best Practice:** If you are manually configuring this setting, specify an FQDN.
Server List	`TaniumServerList`	No	Specifies the Tanium Server and Zone Server FQDNs or IP addresses with which the Client can try to connect as a comma-separated list. This value is unnecessary if the tanium-init.dat file specifies Server names. For more information, see Configuring connections to the Tanium Core Platform on page 230 . **Best Practice:** Specify FQDNs for this setting.
Server Port	`TaniumServerPort`	No	Specifies the port to use for communication between Clients and between Clients and Tanium Cloud Tanium Core Platform Servers . The default is 17472. **Note:** If you configure the ListenPort setting, it overrides ServerPort for client-client communication. For more information, see Customize listening ports on page 274 .

©2026 Tanium Inc. All Rights Reserved

Setting in Azure Portal	JSON Key	Required	Description
Client Listen Port	`TaniumClientListenPort`	No	Specifies the port on which the Client listens for communications from peer Clients. The default is `17472`. **Note:** Changes to ListenPort automatically affect the Tanium Client API port, which is one port number higher. For example, if you set ListenPort to `17473`, the Client API port becomes `17474`. ListenPort overrides the ServerPort setting for client-client communication.
Proxy Servers	`TaniumProxyServers`	No	Specifies the IP address or FQDN, and port number, of an HTTPS forward proxy server through which the Tanium Client connects to the Tanium Server or Zone Server. You can specify multiple proxies as a comma-separated list in the format `"<proxy1>:<port>,...,<proxyN>:<port>"`. The Client tries to connect to the proxies in the order that you list them. After any single connection succeeds, the Client stops trying to connect with more proxies. If no proxy is available, the Client falls back to connecting directly with the Tanium Server or Zone Server. For more information, see Configure specific proxy servers during Client deployment on page 241.
Client Version	`TaniumClientVersion`	No	The version of the Tanium Client to install. If you omit this value, the latest version of the Tanium Client is installed. **Best Practice:** Omit this value and install the latest version of the Tanium Client.
Log Level	`TaniumClientLogLevel`	No	The logging level of the Tanium Client, specified as an integer. • `1` (default): Use this value during normal operation. • `41`: Use this value during troubleshooting. • `91` or higher: Use this value for full logging, for short periods of time only.

©2026 Tanium Inc. All Rights Reserved

Setting in Azure Portal	JSON Key	Required	Description
			Note: A value of `0` disables logging. As a best practice, do not disable logging.

CONVERT THE TANIUM-INIT.DAT FILE TO BASE64

If you did not copy the base64-encoded contents of the tanium-init.dat file from Integrations Gallery, use one of the following methods to supply the file in base64 format.

Convert to base64 To copy into the template or policy JSON

You can use one of the following commands to base64-encode the tanium-init.dat file:

- **Windows:** `powershell "[Convert]::ToBase64String([IO.File]::ReadAllBytes('<absolute-path-to-init-file>\tanium-init.dat'))"`
- **Non-Windows:** `base64 -i '<path-to-init-file>/tanium-init.dat'`

Use a parameter in the template or policy JSON to import the file directly

You can use a parameter in Azure CLI or Azure PowerShell to provide the `TaniumInitDat` property and identify the tanium-init.dat file in the Azure CLI script that uses the template or policy. The following example demonstrates using a parameter in AzureCLI to import the tanium-init.dat file.

Configure the parameter in the `parameters` section of the template and specify the parameter for the `TaniumInitDat` key:

```
"parameters: {
  "TaniumInitDat": {"type": "string"},
  ...
}
```

©2026 Tanium Inc. All Rights Reserved

```
"protectedSettings": {
  "TaniumInitDat": "[parameters('TaniumInitDat')]",
  ...
}
```

Then, specify the parameter in the Azure CLI script:

```
declare _base64_tanium_init_dat=$(base64 < "./tanium-init.dat")
```

```
az deployment group create \
  --name "my-vm" \
  --resource-group "my-rg" \
  --template-file "./templates/linux-template.json" \
  -p TaniumInitDat="${_base64_tanium_init_dat}"
```

Troubleshooting the Tanium Client VM extension

About this task

If you encounter an issue with the installation of the Tanium Client VM extension, check the following items:

1. Make sure the OS on the VM is both supported by the Tanium Client and endorsed by Microsoft. For more information, see Operating system support in Microsoft Azure on page 215.
2. If an ARM template or an Azure Policy fails to evaluate, review the template or policy for errors. For more information, see Microsoft Azure Documentation: Azure virtual machine extensions and features. If necessary, contact Microsoft Support. You can try installing the extension on an endpoint manually to make sure the extension itself is working with the VM. For more information, see Manually install the extension using the Azure Portal, Azure CLI, or Azure PowerShell on page 217.
3. If you corrected all issues in a template or policy and continue to experience installation issues, or if you cannot manually install the extension, contact Tanium Support on page 392 for assistance.

Verify the Tanium Client installation

About this task

©2026 Tanium Inc. All Rights Reserved

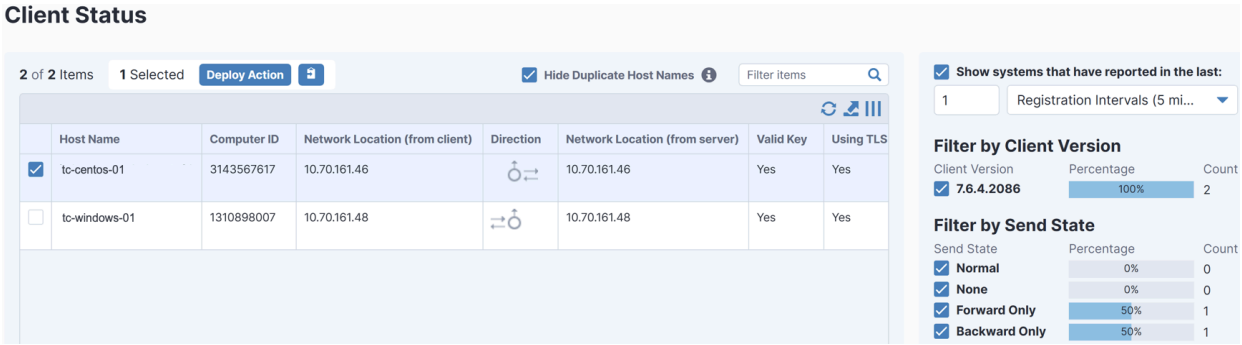
Note: Wait a few minutes after installation for the Tanium Client to register with the Tanium Server or Zone Server.

After you deploy the Tanium Client, perform the following steps to verify that the Client installed correctly and can communicate with the Tanium Server or Zone Server.

1. From Interact, ask a question to verify that the endpoints respond to the following query: `Get Computer Name and Operating System and Tanium Client Version and Tanium Server Name from all machines`
2. Review the **Question Results** grid to verify that all endpoints where you deployed Tanium Client software are reporting.
3. (Optional) From the Main menu, go to **Administration** > **Configuration** > **Client Status** , and review recent Client registration details.

   Tip: To find a specific Tanium Client, enter a text string in the **Filter items** field above the grid to filter it by **Host Name** or **Network Location** (IP address).

Figure 5. Client Status page



©2026 Tanium Inc. All Rights Reserved

Configuring connections to the Tanium Core Platform

After you install the Tanium Client on an endpoint, the Client initiates a connection to the Tanium Server or Zone Server that is configured in the initial settings. After installation, you can change the connection settings as necessary through sensors and packages that Tanium provides. You can configure a direct connection to the Server or establish a Transport Layer Security (TLS) tunnel through a Hypertext Transfer Protocol Secure (HTTPS) proxy server.

Settings for connections to Tanium Core Platform Servers

The following settings, which govern connections from Tanium Clients to the Tanium Server or Zone Server, are stored on the Client endpoints.

Tip: For information about methods to configure Client settings, see Modify Client settings on page 320. For information about content that you can use to manage these specific settings, see Content for configuring connections to Tanium Core Platform Servers on page 233.

Note: For the settings that connect Tanium Clients through HTTPS proxy servers, see Connect through an HTTPS forward proxy server on page 238.

ServerNameList

The Tanium Client connects to only one Tanium Server or Zone Server at a time. However, to avoid a single point of failure, you can configure the **ServerNameList** setting with a list of servers to which the Client can attempt a connection. You specify the Servers as a comma-separated list of FQDNs or IP addresses.

©2026 Tanium Inc. All Rights Reserved

Important: The Tanium Server and Zone Server names in the **ServerNameList** setting must be fully qualified domain names (FQDNs) or IP addresses that Clients can access from their network location. The Server FQDNs might vary among sets of Clients in different locations and might vary from the FQDNs that you configure locally on the Servers. Consult a network administrator for the Server FQDNs that you must configure on Clients.

Best Practice: Specify FQDNs for this setting.

When **ServerNameList** has multiple entries, the Tanium Client must select one each time the Client process restarts or the Client resets. The Client randomly selects a Server from **ServerNameList** without regard to the order in which the servers are listed. However, the Client maintains a count of failed connection attempts, and gives preference to the server with the least failed connections.

The Tanium Client overwrites the value of the **ServerName** setting with the server that it selects from **ServerNameList**. The Client then uses that value when requesting a connection to the Tanium Server or Zone Server.

Tip: You can optionally set the port that the Tanium Client uses to communicate with Servers by appending `:<port_number>` to the Server IP addresses or FQDNs (for example, `ts1.local.com:443,ts2.local.com:443,zs1.example.com:443`). The **ServerNameList** port values override the **ServerPort** setting for the Tanium Client (default is 17472).

ServerName

ServerName specifies the FQDN or IP address of the Tanium Server or Zone Server with which the Tanium Client attempts to connect. Configure **ServerName** only if you do not configure the **ServerNameList** setting. If **ServerNameList** is configured, the Tanium Client overwrites the **ServerName** value with the server that it selects from **ServerNameList**.

©2026 Tanium Inc. All Rights Reserved

Important: The Tanium Server or Zone Server name in the **ServerName** setting must be a fully qualified domain name (FQDN) or IP address that Clients can access from their network location. The Server FQDN might vary among sets of Clients in different locations and might vary from the FQDN that you configure locally on the Server. Consult a network administrator for the Server FQDN that you must configure on Clients.

Best Practice: If you are manually configuring this setting, specify an FQDN.

Tip: You can optionally set the port that the Tanium Client uses to communicate with Servers by appending `:<port_number>` to the Server IP addresses or FQDNs (for example, `ts1.local.com:443,ts2.local.com:443,zs1.example.com:443`). The **ServerNameList** port values override the **ServerPort** setting for the Tanium Client (default is 17472).

LastGoodServerName

LastGoodServerName stores the name of the Tanium Server or Zone Server to which the Tanium Client last successfully connected. If the Client cannot reach the Server in **ServerName** or any server in **ServerNameList**, the Client attempts to connect to the server that **LastGoodServerName** specifies. Do not set **LastGoodServerName**; the Client defines it automatically.

ServerPort

ServerPort specifies the port that the Tanium Client uses for communication with the Server and with peer Clients. The default is 17472, but you can configure a custom port. The Client automatically uses **ServerPort** for connections to the Tanium Servers and Zone Servers that are specified in the **ServerNameList** and **ServerName** settings. Specifying the port within those settings is not required. However, if **ServerName** or **ServerNameList** does specify a port, it overrides **ServerPort**.

©2026 Tanium Inc. All Rights Reserved

Tip:

If you configure the **ListenPort** setting, it overrides **ServerPort** for communication with peer Clients. You can also randomize the port for client-client communication. For more information, see Customize listening ports on page 274

Content for configuring connections to Tanium Core Platform Servers

The Tanium Default Content pack includes sensors and packages to manage the **ServerNameList** and **ServerName** settings on the endpoints that host the Tanium Client.

Tip: For information about other methods to configure Client settings, see Modify Client settings on page 320.

Default content related to ServerNameList, ServerName, and ServerPort

Content	Object Name	Usage
Sensors	Tanium Server Name	Returns the current value of **ServerName** from the Tanium Client. For a Client on which **ServerNameList** is configured, you can use the sensor to identify the Tanium Server or Zone Server with which the Client currently connects. For example: `Get Computer Name and Tanium Server Name from all machines`
	Tanium Server Name List	Returns the current value of **ServerNameList** from the Tanium Client. For example: `Get Computer Name and Tanium Server Name List from all machines`
	Tanium Client Explicit Setting	Returns the current value of any Tanium Client setting that you specify. For example: `Get Computer Name and Tanium Client Explicit Setting[ServerPort] from all machines` For the complete list of Client settings that you can specify with this sensor, see Tanium Client settings reference on page 393 .

©2026 Tanium Inc. All Rights Reserved

Content	Object Name	Usage
Packages	Set Tanium Server Name	Sets the **ServerName** value on Windows endpoints
	Set Tanium Server Name [Non-Windows]	Sets the **ServerName** value on non-Windows endpoints
	Set Tanium Server Name List	Sets the **ServerNameList** value on Windows endpoints
	Set Tanium Server Name List [Non-Windows]	Sets the **ServerNameList** value on non-Windows endpoints

Configure Clients to connect with multiple Tanium Servers

About this task

The following procedure provides an example of how to use the objects listed in the Table 25. Default content related to ServerNameList, ServerName, and ServerPort on page 233 table to set the **ServerNameList** on managed endpoints in a scenario where a second Tanium Server is added to the deployment after the Tanium Client is deployed. In a deployment with both Windows and non-Windows endpoints, repeat the steps for both types of endpoints.



Note: For an example of how to set the **ServerNameList** on Tanium Clients that register with a Zone Server, see Configure Tanium Clients to register with the Zone Server.

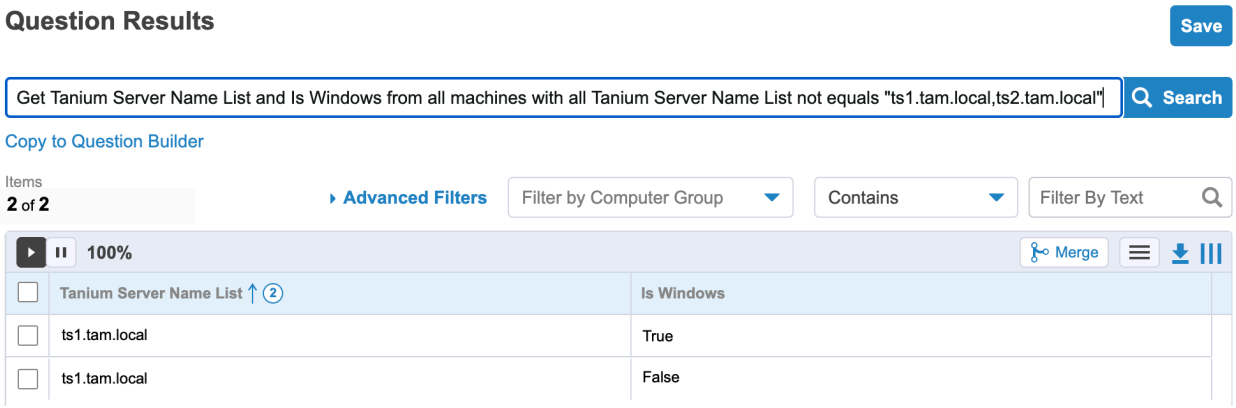
1. Delete any existing scheduled actions that configure **ServerNameList** or **ServerName** to prevent conflicts with the new actions that you create for those settings.
2. Use Tanium Interact to ask a question that identifies the Tanium Clients that require an updated **ServerNameList**.
   The following example identifies Tanium Clients that do not include both Tanium Servers (`ts1.tam.local` and `ts2.tam.local`, in this example):

   ```
   Get Tanium Server Name List and Is Windows from all machines
   ```

©2026 Tanium Inc. All Rights Reserved

```
with all Tanium Server Name List not equals
"ts1.tam.local,ts2.tam.local"
```

Figure 6. Question results identifying Tanium Clients with an outdated ServerNameList



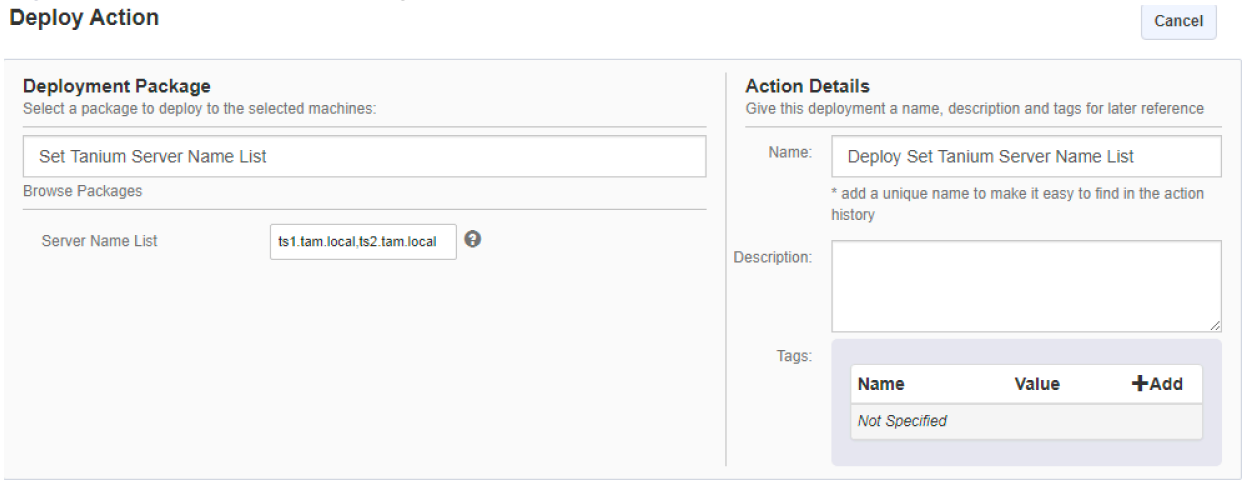
3. In the **Question Results** grid, select a group of either Windows or non-Windows endpoints that need an updated **Tanium Server Name List** value and click **Deploy Action**.

> **Note:** Windows endpoints and non-Windows endpoints require different packages. If you are updating both Windows and non-Windows endpoints, complete this procedure separately for each group.

4. Specify one of the following as the **Deployment Package**:
   - **Set Tanium Server Name List** for Windows endpoints
   - **Set Tanium Server Name List [Non-Windows]** for non-Windows endpoints

5. Enter the FQDNs or IP addresses of both Tanium Servers in the **Server Name List** field.

Figure 7. Deploy action package with updated Server Name List values

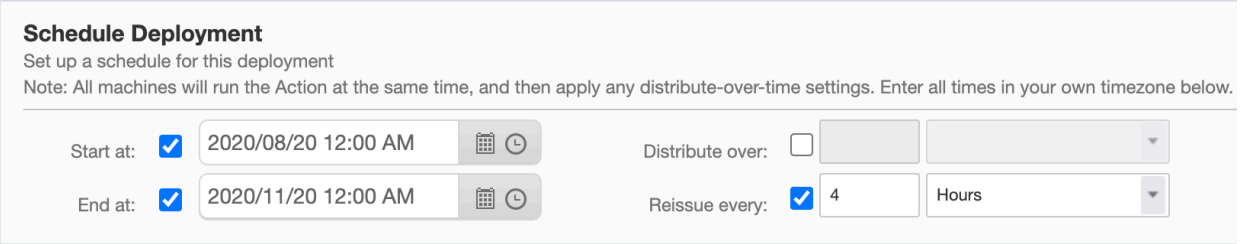


6. Set a schedule for the action.

©2026 Tanium Inc. All Rights Reserved

Best Practice: Set a reissue interval if some target endpoints might be offline when you initially deploy the action.

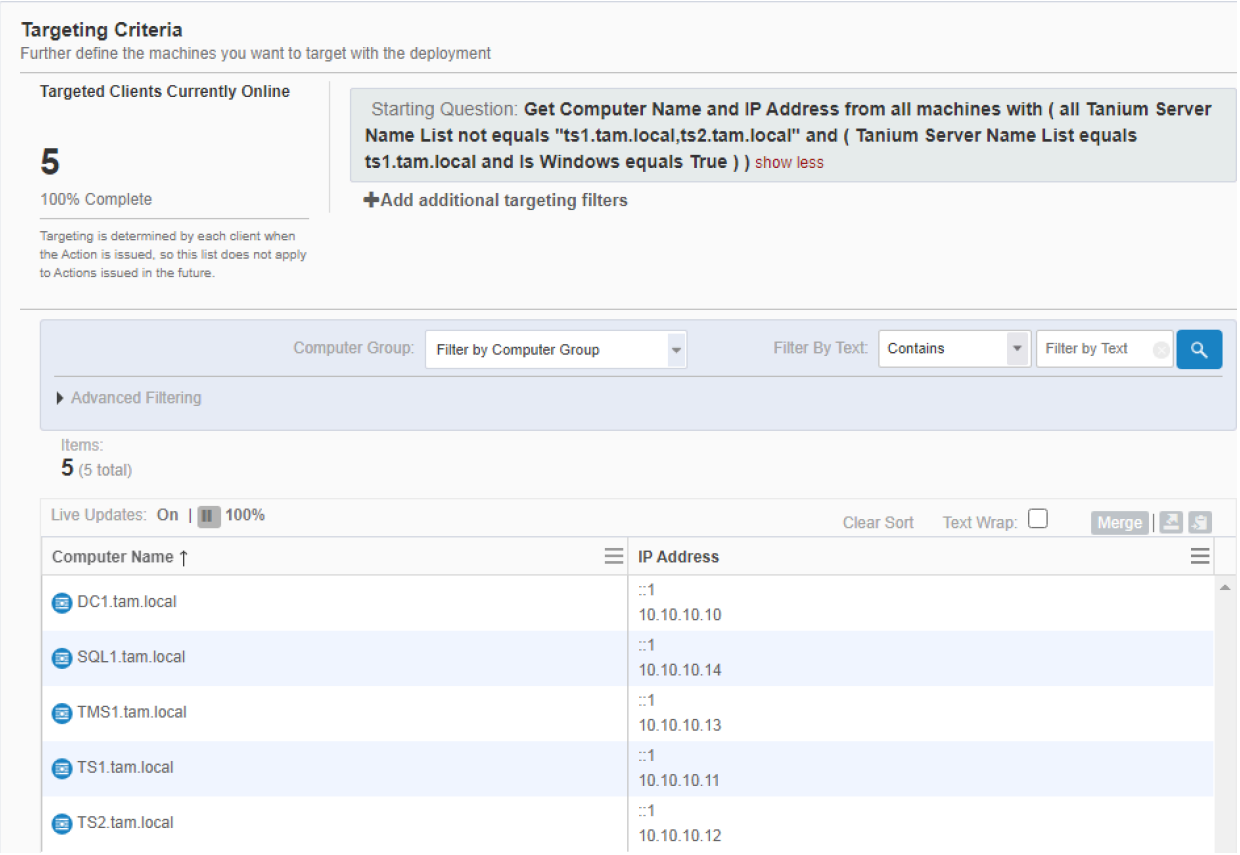
Figure 8. Action schedule settings



7. In the **Targeting Criteria** section, ensure the settings target Windows endpoints or non-Windows endpoints based on the package that you selected.

8. Click **Show preview to continue** and verify that the targeting is correct.

Figure 9. Action targeting preview

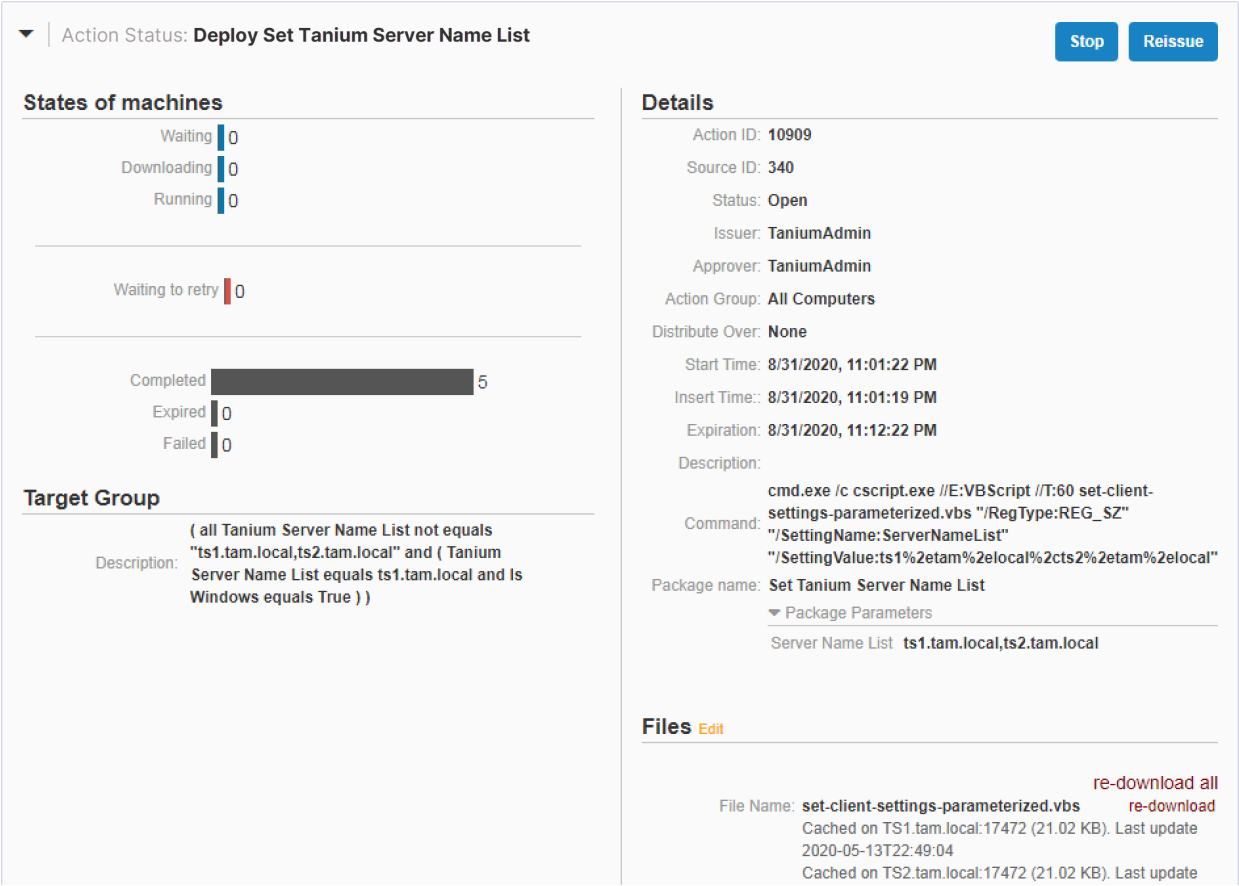


9. Click **Deploy Action** and review the action status to verify that the action completes without errors.

   For more information about the action status, see View action status.

Figure 10. Action status for the ServerNameList deployment

©2026 Tanium Inc. All Rights Reserved

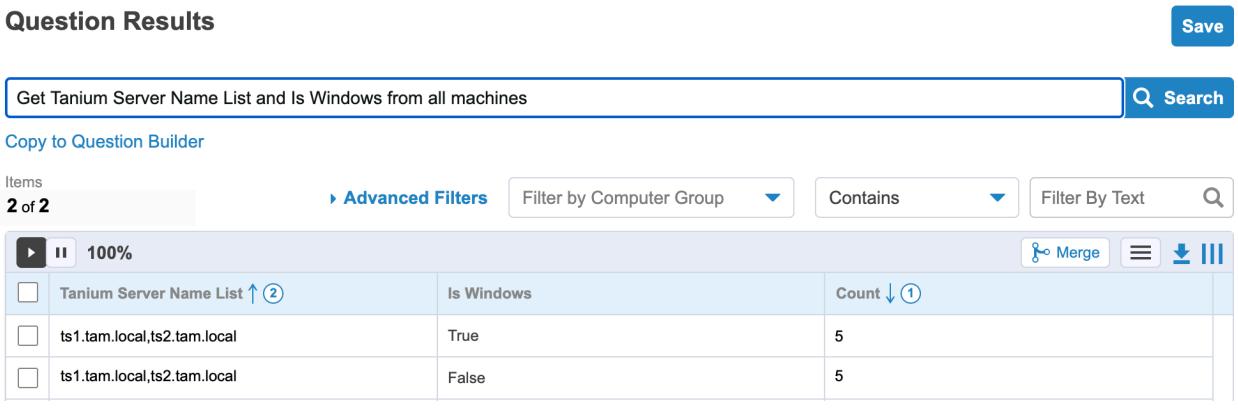


10. Use Tanium Interact to ask a question that returns the **ServerNameList** values from Tanium Clients.

```
Get Tanium Server Name List and Is Windows from all machines
```

11. Review the **Question Results** grid to verify that the **Tanium Server Name List** value includes both Tanium Servers.

Figure 11. Question results confirming updated ServerNameList values



©2026 Tanium Inc. All Rights Reserved

Note: You might have to wait a few minutes for the results to show the new values.

Ensure that live updates  are enabled for the results grid.

Connect through an HTTPS forward proxy server

If the network policies of your organization prohibit endpoints from connecting through the Internet directly to a Tanium Server or Zone Server, you can configure Tanium Client to establish a TLS tunnel through an HTTPS forward proxy server. For example, an organization might require a proxy for Tanium Clients in remote branch office networks. You might also require a proxy if the Tanium Server functions as a managed security service provider (MSSP) in an isolated network where routing changes are not possible. To prevent a single proxy failure from interrupting Client connections, you can configure Clients to send connection requests to multiple proxies. For more information about using TLS communication, see Securing Tanium Server, Zone Server, and Tanium Client access or Securing Tanium Server, Zone Server, and Tanium Client access.

Important:

To use a proxy server with Tanium Clients, your environment must meet the following requirements:

- The proxy server must use the HTTP CONNECT method for TLS tunneling.
- The proxy server must not require authentication.
- The proxy server must not perform SSL/TLS inspection. You cannot use network devices such as firewalls to decrypt and inspect Tanium Protocol traffic between Tanium Clients and the Tanium Server or between peer Tanium Clients.

Use one of the following proxy configuration types:

- Manually specify proxy servers: Use the **ProxyServers** setting to explicitly specify the proxy IP addresses or FQDNs and ports. If you specify multiple proxies, the Client tries to connect to the proxies in the order that **ProxyServers** lists them. After any single connection succeeds, the Client stops trying to connect with more proxies. You must use this method for all non-Windows endpoints.

©2026 Tanium Inc. All Rights Reserved

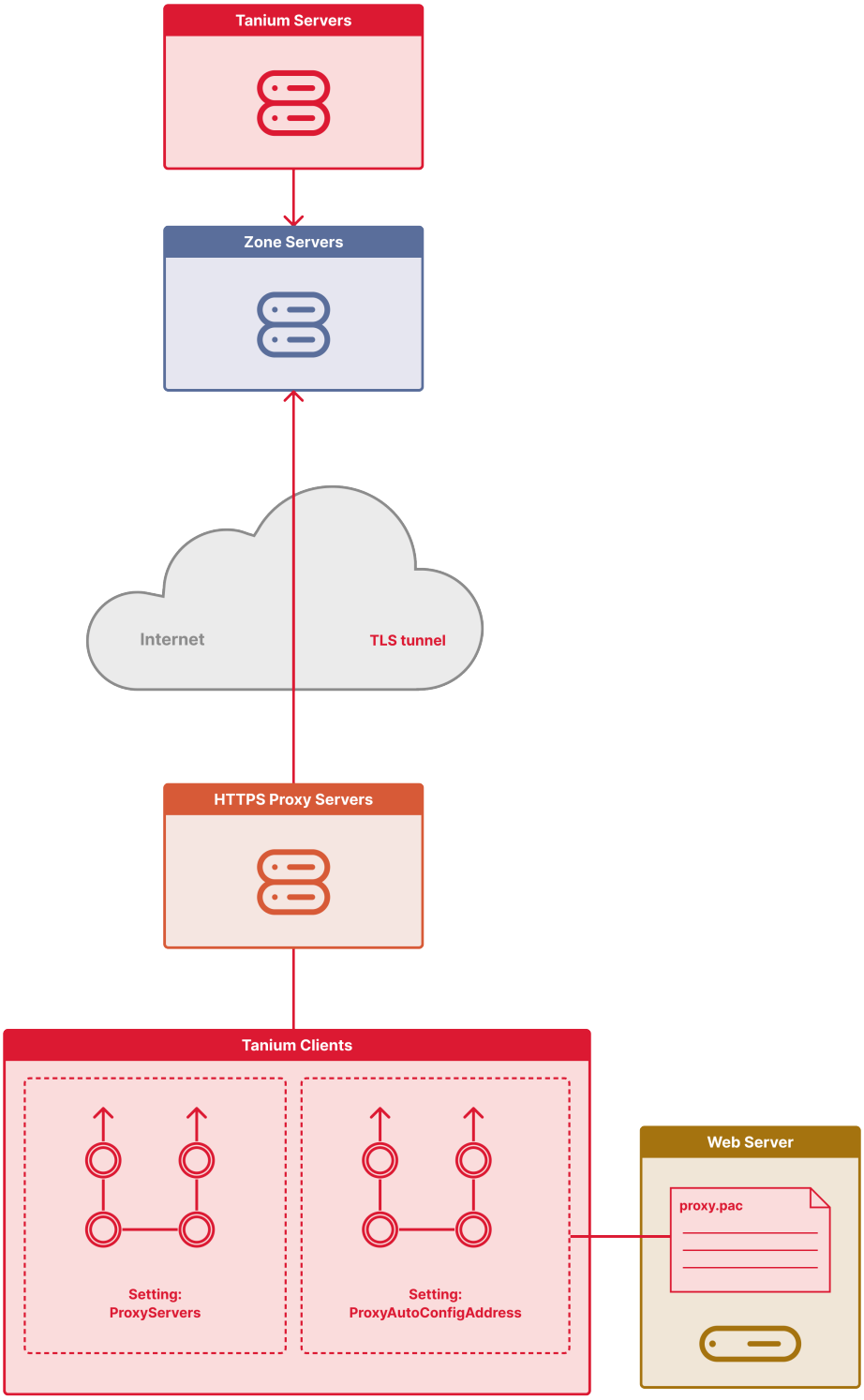
- Specify a PAC file (Windows endpoints only): Use the **ProxyAutoConfigAddress** setting to specify a proxy auto configuration (PAC) file. A PAC file defines how web browsers connect to specific hosts—directly or through specific proxy servers—and defines how the browsers select the correct proxy for each URL. The endpoint downloads the file from the URL that you specify and runs a script that the file contains to select the correct proxy for connecting to a particular Tanium Server or Zone Server.
- Automatically detect local proxy settings (Windows endpoints only): Use the **ProxyAutoDetect** setting to detect the proxy configuration in the Windows registry.

Note:

- Configure only one of the settings on any single endpoint. If you configure **ProxyAutoDetect**, the Tanium Client ignores the other two settings. If you configure **ProxyAutoConfigAddress** and **ProxyServers** together, the Tanium Client ignores the **ProxyServers** setting.
- If the specified setting results in no proxy configuration, or if no specified proxy servers are available, the Tanium Client attempts to connect directly to the Tanium Server or Zone Server.
- Tanium Clients can traverse a proxy only when connecting to a Server. Connections between Clients must be direct.

Figure 12. Connecting through an HTTPS proxy server to Tanium Core Platform Servers

©2026 Tanium Inc. All Rights Reserved



Before you begin

About this task

Work with your network administration team to perform the following tasks before connecting

©2026 Tanium Inc. All Rights Reserved

Tanium Clients to a proxy server:

1. Configure the proxy server to allow the port that the Client uses for Tanium traffic (default 17472), regardless of any security restrictions that are configured on the Server. For more information, see Network connectivity, ports, and firewalls on page 63.
2. (Windows endpoints only) If Tanium Clients must establish proxy connections through a PAC file, create the file and copy it to a web server that the Clients can access.

Next steps

Note: Tanium Clients that can connect only through a proxy connection do not connect directly to Tanium Core Platform Servers. Because the Tanium Client Management service requires a direct connection from the Tanium Module Server to Clients, you cannot use Client Management to deploy Clients that cannot connect without a proxy connection. However, you can use Client Management to create a Client deployment template, and then download a tanium-init.dat file for use in another deployment method. For more information, see Manage Client deployments on page 136.

Best Practice: Configure proxy server settings during Client deployment.

Configure proxy connections during Client deployment

Use only one of the following methods to configure proxy connections on any given endpoint.

CONFIGURE SPECIFIC PROXY SERVERS DURING CLIENT DEPLOYMENT

On non-Windows endpoints, or on Windows endpoints that cannot access a PAC file, configure the Tanium Client to connect to a proxy server by specifying the proxy IP address or FQDN and the proxy port in the **ProxyServers** setting. If you specify multiple proxies, the Client tries to connect to the proxies in the order that **ProxyServers** lists them. After any single connection succeeds, the Client stops trying to connect with more proxies.

©2026 Tanium Inc. All Rights Reserved

Methods to set proxy server addresses during deployment

Installation method	OS	Method to set ProxyServers
Client Management	Any	In the Client deployment, select **Proxy server** for the **Proxy** setting, which automatically adds the **ProxyServers** Client setting. Enter the addresses of proxy servers. For more information, see Manage Client deployments on page 136 .

Command-line interface (CLI)	Windows	Specify the setting as one of the parameters of a silent installation:
		`SetupClient.exe ^`
		`/ProxyServers= <FQDN|IPaddress:PortNumber> /S`

	Non-Windows	Run the following CLI command to configure **ProxyServers** during the step to configure Tanium Client settings:
		`./TaniumClient config set-string ProxyServers \`
		`" <proxy1 FQDN|IP address> : <port> ,..., <proxyN FQDN|IP address> : <port> "`
		For example: `./TaniumClient config set-string ProxyServers`
		`myproxy.mydomain.com:17472,myproxy2.mydomain.com:17472`

Installation wizard	Windows	Run the following CLI command to configure **ProxyServers** after completing the wizard:
		`TaniumClient config set-string ProxyServers ^`
		`" <proxy1 FQDN|IP address> : <port> ,..., <proxyN FQDN|IP address> : <port> "`
		For example: `TaniumClient config set-string ProxyServers`
		`myproxy.mydomain.com:17472,myproxy2.mydomain.com:17472`

	macOS	Run the following CLI command to configure **ProxyServers** after completing the wizard:
		`./TaniumClient config set-string ProxyServers \`
		`" <proxy1 FQDN|IP address> : <port> ,..., <proxyN FQDN|IP address> : <port> "`
		For example: `./TaniumClient config set-string ProxyServers`
		`myproxy.mydomain.com:17472,myproxy2.mydomain.com:17472`

CONFIGURE PROXY CONNECTIONS DURING CLIENT DEPLOYMENT WITH A PAC FILE (WINDOWS ENDPOINTS ONLY)

For Tanium Clients on Windows endpoints, you can configure proxy connections using a PAC file if one is available.

Configure Tanium Clients to use a PAC file by setting **ProxyAutoConfigAddress** during Client

©2026 Tanium Inc. All Rights Reserved

installation. SeeDeploying the Tanium Client using Client Management on page 125 orDeploy the Tanium Client to Windows endpoints using the installer on page 155 for the steps to install the Client.

Methods to set a PAC file URL during deployment

Installation method	Method to set ProxyAutoConfigAddress
Client Management on page 125	In the Client deployment, select **PAC file** for the **Proxy** setting, which automatically adds the **ProxyAutoConfigAddress** Client setting. Enter the URL of the PAC file. For more information, see Manage Client deployments on page 136 .
Command-line interface (CLI) on page 159	Specify the setting as one of the parameters of a silent installation: `SetupClient.exe /ProxyAutoConfigAddress=http[s]:// <PAC file host URL> / <PAC file name> /S` **Note:** You might also have to specify the `/ServerAddress= <Tanium Server FQDNs|IPs>` parameter depending on the Client version and whether a tanium-init.dat file with the appropriate Server list is available. For more information, see Install the Tanium Client on Windows using the command line on page 159 .

installation wizard on page 158	Run the following CLI command to configure **ProxyAutoConfigAddress** after completing the wizard:
	`TaniumClient config set-string ProxyAutoConfigAddress ^`
	`"http[s]:// <PAC file host URL> / <PAC file name> .pac"`

CONFIGURE AUTOMATIC PROXY DETECTION DURING CLIENT DEPLOYMENT (WINDOWS ENDPOINTS ONLY)

For Tanium Clients on Windows endpoints, you can configure the Tanium Client to use the local proxy configuration in the Windows registry if it is available.

Configure Tanium Clients to automatically detect the proxy configuration in this manner using the **ProxyAutoDetect** setting during Client installation. SeeDeploying the Tanium Client using Client Management on page 125 orDeploy the Tanium Client to Windows endpoints using the installer on page 155 for the steps to install the Client.

©2026 Tanium Inc. All Rights Reserved

Methods to set automatic proxy detection during deployment

Installation method	Method to set ProxyAutoDetect
Client Management on page 125	Include the **ProxyAutoDetect** setting as a key with a value of `1` in Client settings. For more information, see Manage Client deployments on page 136 .
Command-line interface (CLI) on page 159	Specify the setting as one of the parameters of a silent installation: `SetupClient.exe /ProxyAutoDetect=1 /S` **Note:** You might also have to specify the `/ServerAddress= <Tanium Server FQDNs|IPs>` parameter depending on the Client version and whether a tanium-init.dat file with the appropriate Server list is available. For more information, see Install the Tanium Client on Windows using the command line on page 159 .
installation wizard on page 158	Run the following CLI command to configure **ProxyAutoConfigAddress** after completing the wizard: `TaniumClient config set-number ProxyAutoDetect 1`

Configure proxy connections after Client deployment

About this task

You can configure Tanium Clients to establish proxy connections after the initial Client deployment, or change the proxy setting on Clients that already connect to a proxy. In a deployment with both Windows and non-Windows endpoints, repeat the steps for both types of endpoints.

1. Go to the Tanium **Home** page and ask the following question to identify the proxy configurations currently in use by Tanium Clients, if any:
   `Get Tanium Client Explicit Setting[ProxyAutoConfigAddress] and Tanium Client Explicit Setting[ProxyServers] and Tanium Client Explicit Setting[ProxyAutoDetect] and Is Windows from all machines`

2. Drill down as necessary, select the results for either Windows or non-Windows endpoints that require new or updated proxy connections, and click **Deploy Action**.

©2026 Tanium Inc. All Rights Reserved

> **Note:** Windows endpoints and non-Windows endpoints require different packages. If you are updating both Windows and non-Windows endpoints, complete this procedure separately for each group.

3. Configure the package settings:
   - **Deployment Package**: Select **Modify Tanium Client Setting** for Windows endpoints or **Modify Tanium Client Setting [Non-Windows]** for other endpoints.
   - **RegType** (Windows only): Select **REG_SZ**.
   - **Type** (non-Windows only): Select **STRING**.
   - Enter one of the following pairs of **ValueName** and **ValueData** as appropriate:

     #### Tanium Client proxy connection settings

ValueName	ValueData
`ProxyServers`	A comma-separated list of proxy IP addresses or FQDNs and proxy ports in the format `<proxy1 FQDN|IP address> : <port> ,..., <proxyN FQDN|IP address> : <port>` For example: `myproxy.mydomain.com:17472,myproxy2.mydomain.com:17472`
`ProxyAutoConfigAddress` (Windows endpoint only)	A PAC file URL and file name in the format `http[s]:// <PAC file URL> / <PAC file name> .pac`
`ProxyAutoDetect` (Windows endpoints only)	`1` to enable automatic proxy detection, or `0` to disable **Note:** It is necessary to configure `0` for this setting on an endpoint only if you have previously created the setting to enable it.

4. (Optional) In the **Schedule Deployment** section, set a schedule for the action.

   > **Best Practice:** Set a reissue interval if some target endpoints might be offline when you initially deploy the action.

5. In the **Targeting Criteria** section, ensure that the settings target only the endpoints that:
   - Require the updated proxy setting

©2026 Tanium Inc. All Rights Reserved

- Run the operating system that matches the selected package (Windows or non-Windows)

6. Click **Show preview to continue** and verify that the targeting is correct.
7. Click **Deploy Action** and review the action status to verify that the action completes without errors.

   Important: Clients do not apply the updated setting until you manually restart them or wait for the automatic Client reset, which typically occurs at a random interval in the range of two to six hours.

8. (Optional) Restart the Tanium Client service on each endpoint to apply the updated proxy setting immediately:
   - Manage the Tanium Client service on Windows on page 293
   - Manage the Tanium Client service on macOS on page 308
   - Manage the Tanium Client service on Linux on page 313
   - Manage the Tanium Client service on Solaris on page 315
   - Manage the Tanium Client service on AIX on page 317
9. To verify that Clients have the correct configuration, ask one of the following questions according to the setting you modified.
   - `Get Tanium Client Explicit Setting[ProxyServers] and Is Windows from all machines`
   - `Get Tanium Client Explicit Setting[ProxyAutoConfigAddress] from all machines`
   - `Get Tanium Client Explicit Setting[ProxyAutoDetect] from all machines`

©2026 Tanium Inc. All Rights Reserved

Configuring Tanium Client peering

Overview of Tanium Client peering settings

Peering settings define the subnet boundaries of the linear chains in which Tanium Clients form peer relationships. Peering settings are designed to optimize network resources that are required to manage endpoints by ensuring that most data transmission is distributed among the low-latency, high-bandwidth links of local area networks (LANs). Using mostly LAN links dramatically reduces resource use over the wide area network (WAN).

For more information about how Tanium Client peering works and related concepts, see Client peering on page 23.

You can configure a custom listening port for communication between Tanium Clients, or you can configure the Tanium Client to periodically select a new listening port at random, instead of using a fixed port for communications from peers. For more information, see Customize listening ports on page 274.

©2026 Tanium Inc. All Rights Reserved

Best Practice:

Use the default Client peering settings to optimize network resources when all endpoints on a subnet defined by the default /24 address mask share a high-speed local connection, or when you do not have much information about the enterprise network. Work with network administrators and Tanium Support on page 392 to use the following settings and configurations to further optimize peer communication based on the characteristics of your network. Separate settings and configurations apply to Clients that connect directly to the Tanium Server and to Clients that connect to a Tanium Zone Server.

- Address Mask: The default address mask (IPv4) and address prefix (IPv6) settings are designed to prevent Tanium Client peering across WANs. For more information, see Address mask and prefix settings on page 250.
- Separated subnets: Specify more granular exceptions to the boundaries that the address mask or prefix setting defines. For example, within a subnet that the address mask or prefix setting defines, you might have a smaller subnet that crosses WAN links. In this case, you can define separated subnets within that smaller subnet so that its Clients do not peer across the WAN links. For more information, see Configure separated subnets on page 252.
- Isolated subnets: Specify the addresses of subnets and endpoints for which you want to disable Tanium Client peering. You can configure isolated subnets that are standalone subnets or that comprise smaller linear chains within the chain that the address mask or prefix setting defines (see the figure Figure 13. Tanium Client peering on page 250). For more information, see Configure isolated subnets on page 255.
- Intentional subnets: Specify multiple public IP addresses that belong to a single site to allow peering among Clients that are behind network address translation (NAT) and that have different public IP addresses within that site.

When a Tanium Client registers through the Tanium Server or Zone Server, the Server evaluates peering settings and configurations and applies the most restrictive rule to determine the subnet for that Client. For example, if the default address mask defines a /24 subnet, and a separated subnets configuration defines a /26 subnet, the Server applies the peering boundaries of the separated subnet to a Client that has an IP address within the bounds of both.

©2026 Tanium Inc. All Rights Reserved

Tanium Servers write subnet configurations to the Tanium database and automatically synchronize them in an active-active deployment. The subnet configurations in the database are also synchronized among Tanium Zone Servers. In most environments, the separated and isolated subnets configurations are the same for all Zone Servers and Tanium Servers. In complex environments with overlapping subnets, you might have to segregate subnets differently for Zone Servers. In such cases, you can add SeparatedSubnets.txt and IsolatedSubnets.txt files to the Zone Servers to override the synchronized database configurations. Intentional subnets configurations are always synchronized across all Zone Servers and Tanium Servers.

Note: Contact Tanium Support on page 392 if you need IPv6 support in Tanium Core Platform. Each Tanium Client can register with the Tanium Server as an IPv4 Client or IPv6 Client, but not both. Also, a Tanium deployment can include both IPv4 and IPv6 linear chains, but each chain contains Clients for only one IP version; IPv4 Clients can never peer with IPv6 Clients.

The figure Figure 13. Tanium Client peering on page 250 illustrates an IPv4 deployment where internal Tanium Clients connect with Tanium Servers in an active-active deployment and external Clients connect with the Zone Server.

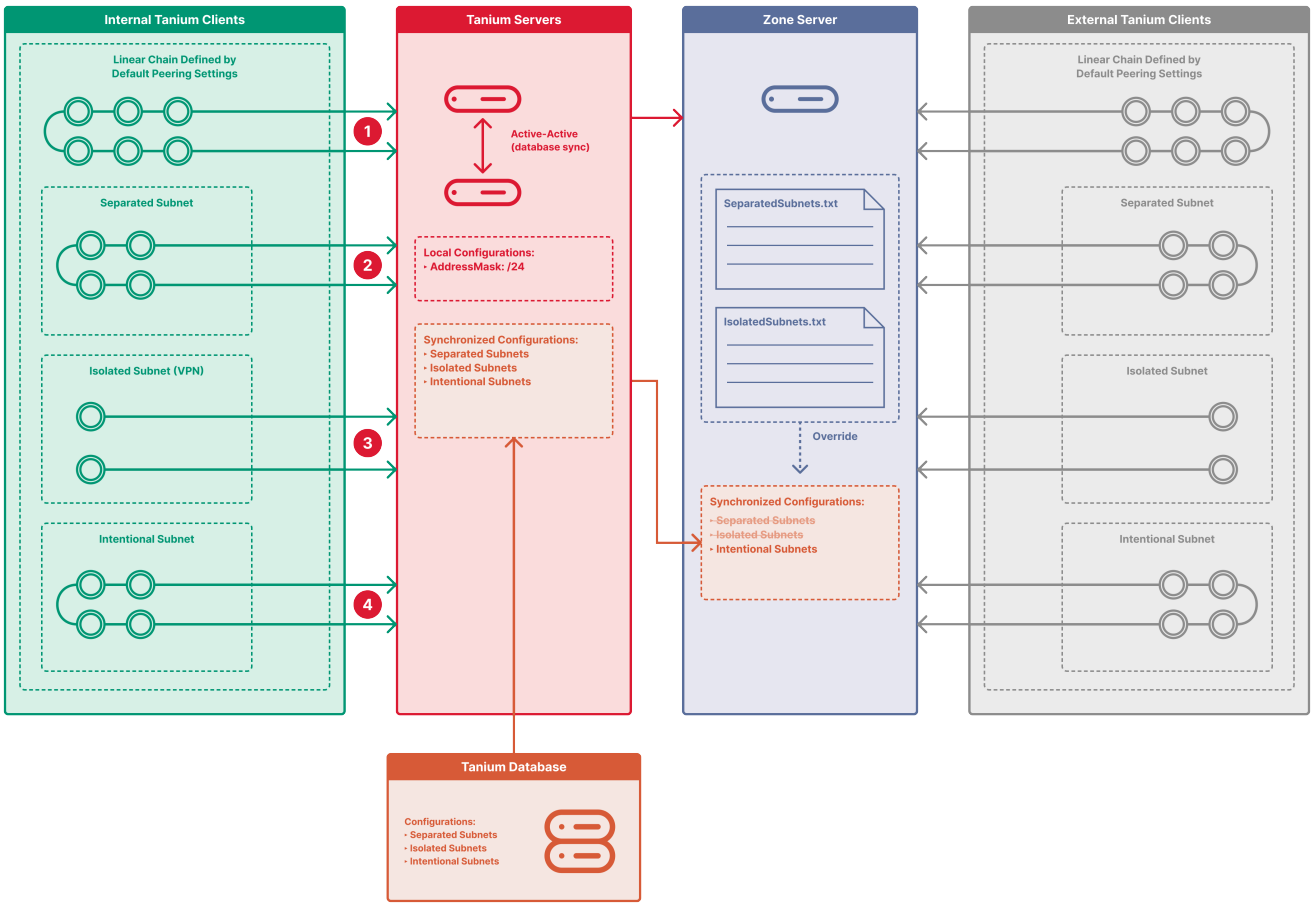
1	AddressMask and zs_address_mask When each Tanium Client registers, the Tanium Server or Zone Server sends the Client a *neighborhood list*. This is a list of adjacent Clients that are optimal for peering and that are within the boundaries that the **AddressMask** or **zs_address_mask** setting defines. In this example, both settings apply the default /24 address mask as the linear chain boundaries. **Note:** In the figure Figure 13. Tanium Client peering on page 250, the Zone Server uses the **zs_address_mask** that it receives from a Tanium Server. If necessary, you can override the setting by configuring the **AddressMask** locally on the Zone Server.
2	Separated subnets configuration Upon evaluating the separated subnets configuration, the Tanium Servers and Zone Server apply exceptions that define smaller linear chains that are contained within the **AddressMask** or **zs_address_mask** chains.
3	Isolated subnets configuration The Tanium Servers and Zone Server evaluate the isolated subnets configuration to define linear chains for subnets in which the Clients do not peer with each other.

©2026 Tanium Inc. All Rights Reserved

4	Intentional subnets configuration The Tanium Servers and Zone Server evaluate the intentional subnets configuration to determine Clients that can peer with each other even when they are behind network address translation (NAT) and have different public IP addresses.

Note: The following figure shows the Tanium database on a dedicated host. However, in a Tanium Appliance deployment, the database is on the same host as the Tanium Servers.

Figure 13. Tanium Client peering



Address mask and prefix settings

Contact Tanium Support on page 392 to help determine the appropriate values for the following Tanium Client peering settings.

©2026 Tanium Inc. All Rights Reserved

AddressMask

In IPv4 subnets where Tanium Clients register directly with the Tanium Server, **AddressMask** governs the network proximity of Client peers to prevent suboptimal peer connections (such as connections across WANs). The Tanium Server installation automatically adds the setting (**Administration** > **Configuration** > **Settings** > **Advanced Settings**) with a default value that limits peering to neighbors that share the same 24-bit address mask. For example, a Tanium Client in subnet 192.168.0.0/24 can peer with other Tanium Clients in 192.168.0.0/24 but not those in 192.168.1.0/24. When each Tanium Client registers with the Tanium Server, the Server sends the Client a list of neighbors with which it can attempt to peer. This neighborhood list adheres to the **AddressMask** boundary.

The following table lists typical values for this setting:

Tanium Client AddressMask peering setting values by CIDR

CIDR	Value for AddressMask Setting
/8	255
/16	65535
/24	16777215
/32	4294967295 [1]

[1] This value disables Client peering. You can use this value for the **zs_address_mask** setting or the **AddressMask** setting on Zone Servers to isolate Clients that register with Zone Servers. For Tanium Clients that register directly with the Tanium Server, configure isolated subnets instead. For more information, see Configure isolated subnets on page 255 .

zs_address_mask

In IPv4 subnets where Tanium Clients register with a Zone Server, **zs_address_mask** governs the network proximity of Client peers to prevent suboptimal peer connections. The Zone Server receives the setting from the Tanium Server (**Administration** > **Configuration** > **Settings** > **Advanced Settings**) with a default value that limits peering to neighbors that share the same 24-bit address mask. If necessary, you can override the platform setting by configuring **AddressMask** locally on each Zone Server. When each Tanium Client registers with the Zone Server, the Server sends the Client a neighborhood list that adheres to the **zs_address_mask** (or local **AddressMask**) boundary.

©2026 Tanium Inc. All Rights Reserved

This setting uses the same values as the **AddressMask** setting.

AddressPrefixIPv6

In IPv6 subnets where Tanium Clients register directly with the Tanium Server, **AddressPrefixIPv6** governs the network proximity of Client peers to prevent suboptimal peer connections. By default, this setting is not visible until you manually configure it (**Administration** > **Configuration** > **Settings** > **Advanced Settings**). The default value is 0, which specifies no peering. When each Tanium Client registers with the Tanium Server, the Server sends the Client a neighborhood list that adheres to the **AddressPrefixIPv6** boundary. Contact Tanium Support on page 392 to determine the optimum value for peering in IPv6 networks.

zs_address_prefix_ipv6

In IPv6 subnets where Tanium Clients register with a Zone Server, **zs_address_prefix_ipv6** governs the network proximity of Client peers to prevent suboptimal peer connections. The Zone Server receives the setting from the Tanium Server (**Administration** > **Configuration** > **Settings** > **Advanced Settings**). The default value is 0, which specifies no peering. If necessary, you can override the platform setting by configuring **AddressPrefixIPv6** locally on each Zone Server. When each Tanium Client registers with the Zone Server, the Server sends the Client a neighborhood list that adheres to the **zs_address_prefix_ipv6** (or local **AddressPrefixIPv6**) boundary. Contact Tanium Support on page 392 to determine the optimum value for peering in IPv6 networks.

Configure separated subnets

About this task

Tanium Clients in a *separated subnet* can peer only with other Clients that are within that subnet. Configure separated subnets to specify more granular exceptions for Client peering than the subnet boundaries that the address mask or prefix settings define (see Address mask and prefix settings). Clients use the separated subnets configuration for peering based on whether they connect to the Tanium Server or Zone Server. Each Server uses the configuration to manage the peer lists for Clients that register through it.

After you configure separated subnets, you do not have to restart the Tanium Servers or Zone Servers. Tanium Clients might take up to two to six hours (the randomized Client-reset interval) to finish applying all the changes associated with the new configuration. To verify that the separated subnets work as expected after the Clients register, see Verify or remediate Tanium Client peering and

©2026 Tanium Inc. All Rights Reserved

leader connections.

The figure Tanium Client peering on page 247 shows an example deployment with separated subnets.

Best Practice: In most environments, the separated subnets configuration is the same for all Zone Servers and Tanium Servers, and the best practice is to keep the configuration synchronized across Servers to avoid confusion. In complex environments with overlapping subnets, you might have to segregate subnets differently for Zone Servers. In such cases, you can modify SeparatedSubnets.txt on each Zone Server that requires a unique configuration.

Note: A user role with the **Read Separated Subnets** permission is required to view the separated subnets configuration. The **Write Separated Subnets** permission is required to create, modify, or delete the separated subnets configuration. The Administrator reserved role has these permissions.

Tanium Core Platform 7.3 or later supports IPv6 subnets, such as: `2001:db8::/32`. Contact Tanium Support on page 391 for details.

Configure separated subnets that are the same for Tanium Servers and Zone Servers

ADD SUBNETS

1. From the Main menu, go to **Administration** > **Configuration** > **Subnets**.
2. In the **Separated Subnets** section, click **New Subnets**.
3. Enter each subnet in CIDR format using separate lines or commas as delimiters. Use the semicolon `;` or hash `#` character before any optional comments, as shown in the following example. You cannot use a comma `,` within the comment text because that character is reserved as a subnet delimiter.

```
192.168.0.0/26 #This is a data center subnet.
192.168.2.0/26 ;This is a branch office subnet.
2001:db8::/32
```

©2026 Tanium Inc. All Rights Reserved

Tip: If your deployment includes Zone Servers that require different separated subnets than the Tanium Servers, copy entries from the text field to the clipboard to use when you configure separated subnets that are specific to Zone Servers.

4. Click **Save**.

EDIT SUBNETS

1. From the Main menu, go to **Administration** > **Configuration** > **Subnets**.
2. Select one of the **Separated Subnets** and click **Edit**.
3. Edit the subnet (**CIDR**) and **Comment**, and click **Save**.

Configure separated subnets that are specific to Zone Servers

About this task

If a deployment includes Zone Servers that require different separated subnets than the Tanium Servers, perform the following steps based on your Tanium infrastructure to add a custom separated subnets configuration to each Zone Server. Because Zone Servers do not synchronize custom subnet configurations, each Zone Server can have a unique configuration.

WINDOWS INFRASTRUCTURE

1. Create a plain text file named SeparatedSubnets.txt.
2. Enter the subnets and optional comments that you entered for the Tanium Server into SeparatedSubnets.txt. Use the formatting described in Add subnets.
3. Move SeparatedSubnets.txt to the installation directory of each Zone Server (the default installation directory is \Program Files (x86)\Tanium\Tanium Zone Server). If necessary, you can modify the file contents for each Zone Server that requires a unique configuration.

Next steps

©2026 Tanium Inc. All Rights Reserved

Note: If you remove SeparatedSubnets.txt from the Zone Server, it reverts to using the separated subnets that are configured on the Tanium Servers.

TANIUM APPLIANCE INFRASTRUCTURE

1. On the Zone Server Appliance, sign in to the TanOS console as a user with the `tanadmin` role.
2. From the **tanadmin menu**, enter `2-2` (Tanium Operations > Configuration Settings).
3. Enter `12` to edit the SeparatedSubnets.txt file.

```
>>> Tanium TanOS -> Tools -> Edit Files -> SeparatedSubnets.txt <<<

          #: Line Content

          1: 192.168.1.0/24

          A: Add a line

          R: Return to previous menu

-------------------------------------------------------
```

4. Use the menu to specify subnets in CIDR format.

Configure isolated subnets

About this task

Configure *isolated subnets* to disable Client peering for a specified list of subnet and endpoint IP addresses. If the IP address of a Tanium Client is in an isolated subnet, the Tanium Server or Zone Server sends that Client an empty peer list to prevent the Client from participating in peering. Each Server uses the configuration to manage the peer list for Tanium Clients that register through it.

After you configure isolated subnets, you do not have to restart the Tanium Servers or Zone Servers. Tanium Clients might take up to two to six hours (the randomized Client-reset interval) to finish applying all the changes associated with the new configuration. To verify that the isolated subnets

©2026 Tanium Inc. All Rights Reserved

work as expected after the Clients register, see Verify or remediate Tanium Client peering and leader connections.

The figure Tanium Client peering on page 247 shows an example deployment with isolated subnets.

Important: Configure isolated subnets for Tanium Clients that are in VPNs. VPN Clients have local IP addresses in a special VPN address block, but their host endpoints are actually not close to each other. VPN Clients would use WAN links for peering and latency would be significantly greater than for Client-to-server connections.

Best Practice:

- Configure isolated subnets for virtual desktop infrastructure (VDI) instances in a high-density environment with shared storage or for any other virtual endpoints where concurrent disk I/O operations must be limited. Endpoints cache file chunks to share distributed files with peers, which requires multiple endpoints in the linear chain to concurrently read and write file chunks. Isolating an endpoint reduces the concurrent disk I/O that normally occurs when this cache is used to share files with peers. For more information, see Tanium Client Management User Guide: File distribution.
- You might find it convenient to use isolated subnets to disable peering in other cases, such as for testing or debugging peering when you have to troubleshoot network issues. Note that disabling peering causes Tanium Clients to consume more network resources in terms of bandwidth and Client-server connections over the WAN. For troubleshooting cases, after you resolve the network issues, the best practice is to remove the Clients from the isolated subnets configuration so that they resume peering.
- In most environments, the isolated subnets configuration is the same for all Zone Servers and Tanium Servers, and the best practice is to keep the configuration synchronized across Servers to avoid confusion. In complex environments with overlapping subnets, you might have to segregate subnets differently for Zone Servers. In such cases, you can modify the subnets configuration on each Zone Server that requires a unique configuration.

©2026 Tanium Inc. All Rights Reserved

Note: A user role with the **Read Isolated Subnets** permission is required to view the isolated subnets configuration. The **Write Isolated Subnets** permission is required to create, modify, or delete the isolated subnets configuration. The Administrator reserved role has these permissions.

Tanium Core Platform 7.3 or later supports IPv6 subnets, such as: `2001:db8::/32`. Contact Tanium Support on page 391 for details.

Configure isolated subnets that are the same for Tanium Servers and Zone Servers

ADD SUBNETS

1. From the Main menu, go to **Administration** > **Configuration** > **Subnets**.
2. In the **Isolated Subnets** section, click **New Subnets**.
3. Enter each subnet in CIDR format using separate lines or commas as delimiters. Use the semicolon `;` or hash `#` character before any optional comments, as shown in the following example. You cannot use a comma `,` within the comment text because that character is reserved as a subnet delimiter.

```
192.168.0.0/26 #This is a data center subnet.
192.168.2.0/26 ;This is a branch office subnet.
2001:db8::/32
```

Tip: If your deployment includes Zone Servers that require different isolated subnets than the Tanium Servers, copy entries from the text field to the clipboard to use when you configure isolated subnets that are specific to Zone Servers.

4. Click **Save**.

EDIT SUBNETS

1. From the Main menu, go to **Administration** > **Configuration** > **Subnets**.
2. Select one of the **Isolated Subnets** and click **Edit**.
3. Edit the subnet (**CIDR**) and **Comment**, and click **Save**.

©2026 Tanium Inc. All Rights Reserved

Configure isolated subnets that are specific to Zone Servers

About this task

If a deployment includes Zone Servers that require different isolated subnets than the Tanium Servers, perform one of the following procedures based on your Tanium infrastructure and whether you want to isolate all Clients or Clients on specific subnets. Because Zone Servers do not synchronize custom subnet configurations, each Server can have a unique configuration.

> **Note:** The Zone Server applies the most restrictive rule to determine the subnet for a Client. If you configure the **zs_address_mask** or **AddressMask** setting to isolate Clients, that setting overrides any subnet-based isolation that is configured in an IsolatedSubnets.txt file.

ISOLATE ALL CLIENTS CONNECTED TO ANY ZONE SERVER

About this task

Set the **zs_address_mask** platform setting on the Tanium Server (**Administration** > **Configuration** > **Settings** > **Advanced Settings**) to `4294967295`, which specifies /32 subnet boundaries (single hosts) for all Zone Servers.

For more information, see Tanium Client Management User Guide: Address mask and prefix settings.

ISOLATE ALL CLIENTS CONNECTED TO A PARTICULAR ZONE SERVER

1. Sign in to the Zone Server host as an administrator user.
2. Access the CLI.
   For more information, see:
   - Reference: Tanium Core Platform command-line interface (Tanium Appliance deployments)
   - Reference: Command-line interface (Windows deployments)
3. Navigate to the Zone Server installation folder:

```
&gt;cd<Tanium Zone Server>
```

©2026 Tanium Inc. All Rights Reserved

4. Configure the **AddressMask** local setting to specify /32 subnet boundaries (single hosts):

```
&gt;TaniumZoneServer config set AddressMask 4294967295
```

For more information, see Tanium Client Management User Guide: Address mask and prefix settings.

ISOLATE CLIENTS ON SPECIFIC SUBNETS WITH WINDOWS INFRASTRUCTURE

1. Create a plain text file named IsolatedSubnets.txt.
2. Enter the subnets and optional comments that you entered for the Tanium Server into IsolatedSubnets.txt. Use the formatting described in Add subnets.
3. Move IsolatedSubnets.txt to the installation directory of each Zone Server (the default installation directory is \Program Files (x86)\Tanium\Tanium Zone Server). If necessary, you can modify the file contents for each Zone Server that requires a unique configuration.

Next steps

Note: If you remove IsolatedSubnets.txt from the Zone Server, it reverts to using the isolated subnets that are configured on the Tanium Servers.

ISOLATE CLIENTS ON SPECIFIC SUBNETS WITH TANIUM APPLIANCE INFRASTRUCTURE

1. On the Zone Server Appliance, sign in to the TanOS console as a user with the `tanadmin` role.
2. From the **tanadmin menu**, enter `2`-`2` (Tanium Operations > Configuration Settings).
3. Enter `11` to edit the IsolatedSubnets.txt file.

```
>>> Tanium TanOS -> Tools -> Edit Files -> IsolatedSubnets.txt <<<

          #: Line Content

          1: 192.168.1.0/24

          A: Add a line
```

©2026 Tanium Inc. All Rights Reserved

```
        R: Return to previous menu

--------------------------------------------------
```

4. Use the menu to specify subnets in CIDR format.

Configure intentional subnets

Overview of intentional subnets

In a network configuration that uses network address translation (NAT), the local IP addresses of Tanium Clients in the same local area network (subnet) might be mapped to different NAT IP addresses for communication with the Tanium Server or Tanium Zone Server. The default Tanium peering settings allow Clients in that subnet to peer with each other only if they share the same NAT IP address. If Clients in the same subnet are assigned to different NAT IP addresses, they can peer with each other only if you assign them to an *intentional subnet* that specifies the full range of NAT IP addresses for that subnet. Without an intentional subnet, each Client with a different NAT IP address establishes a leader connection to the Server. Network traffic is higher in a deployment with more leader connections, especially when Clients download package files for running actions. Therefore, configuring intentional subnets can increase peering and reduce traffic, particularly in deployments where many Clients use NAT when connecting to the Server over the Internet.

The figure Tanium Client peering on page 247 shows an example deployment with intentional subnets.

Note: A user role with the **Read Intentional Subnets** permission is required to view the intentional subnets configuration. The **Write Intentional Subnets** permission is required to create, modify, or delete the intentional subnets configuration. The Administrator reserved role has these permissions.

You can configure IPv6 subnets, such as `2001:db8::/32`. Contact Tanium Support on page 391 for details.

The following table shows examples of Tanium Clients that do or do not require intentional subnets to enable peering. The example IP addresses are listed as they would appear on the **Administration**

©2026 Tanium Inc. All Rights Reserved

> **Configuration** > **Client Status** page, where the **Network Location (from Client)** column shows the pre-NAT IP addresses and the **Network Location (from Server)** column shows the NAT IP addresses. In this example, the **AddressMask** platform setting specifies a /24 address mask, which is the default peering range (see Overview of Tanium Client peering settings on page 247).

Example of Tanium Client peering requirements

Tanium Client	Network Location (from Client)	Network Location (from Server)	Intentional subnet required for peering?
TC-UK-1	31.0.0.11	31.0.0.11	No: The Clients do not use NAT. Therefore, even though their IP addresses differ, they can peer because they are in the same subnet within the default peering range (**AddressMask** = `/24`).
TC-UK-2	31.0.0.12	31.0.0.12	
TC-US-1	172.16.0.11	14.0.0.11	No: The Clients can peer because they use the same NAT address.
TC-US-2	172.16.0.12	14.0.0.11	
TC-HQ-1	10.0.0.11	98.0.0.1	Yes: The Clients are in the same subnet within the default peering range, but the **AddressMask** setting does not apply because their NAT IP addresses differ. Without an intentional subnet, the Tanium Server interprets the different NAT IP addresses as an indication that the Clients are in different subnets and therefore prevents peering.
TC-HQ-2	10.0.0.12	98.0.0.2	

Before you begin

About this task

You can define intentional subnets using either of the following methods:

- Intentional subnet sites: In Tanium Console, you can specify a **Site** name for an *intentional subnet site* and the subnets that belong to that **Site**. Clients in the subnets that belong to a single site can peer with one another.
- PeerNeighborhood Client setting: You can configure the same *neighborhood name* for the **PeerNeighborhood** setting on each Client that can peer. You can use this setting to define intentional subnets in the following scenarios:

©2026 Tanium Inc. All Rights Reserved

- You want to allow Clients that have a wide variety of NAT IP addresses to peer, and the variety of IP addresses makes subnets difficult to define, or subnets overlap among sites that need to remain isolated.
- You want to deploy Clients that are always allowed to peer, regardless of NAT IP addresses, such as virtual machines in a cloud environment.
- You want to manually allow specific Clients to peer.

To determine the appropriate method to define intentional subnets, and the appropriate **Site** names and subnet CIDR values or **PeerNeighborhood** names:

1. From the Main menu, go to **Administration** > **Configuration** > **Client Status** and identify endpoints that are in the same subnet [based on their **Network Location (from Client)**] but are not peering because their NAT IP addresses [**Network Location (from Server**)] differ.

   Note: The Tanium Server considers pre-NAT IP addresses to be in the same subnet based on the **AddressMask** (IPv4) or **AddressPrefixIPv6** setting.

2. Choose appropriate **Site** or **PeerNeighborhood** names for the endpoints that you identified. For example, you might have a `HeadQuarters` site for endpoints in the headquarters subnet and a `NAM` site for endpoints in a North America branch office subnet.

3. Inventory the NAT IP addresses of each site to determine the appropriate method to define the intentional subnets and, if applicable, the CIDR values to enter.
   - If the subnets are reasonable to define and do not overlap among sites that need to remain isolated, use the NAT IP addresses to determine the appropriate subnets in intentional subnet sites.

     The best practice is to enter the smallest subnet ranges possible that include the identified endpoints while allowing for potential changes to their NAT IP addresses. As an example, for the Clients TC-HQ-1 (98.0.0.1) and TC-HQ-2 (98.0.0.2) in the table Example of Tanium Client peering requirements, you might configure a **Site** named `HeadQuarters` with one of the following subnets, which are listed in descending order in terms of the size of their IP address range:

     - 98.0.0.0/24: Peering is allowed for all Tanium Clients with NAT IP addresses in the range 98.0.0.0 to 98.0.0.255. If TC-HQ-1 and TC-HQ-2 are assigned to new NAT IP addresses within that range, they can still peer.

©2026 Tanium Inc. All Rights Reserved

- 98.0.0.0/30: Peering is allowed for all Tanium Clients with NAT IP addresses in the range 98.0.0.0 to 98.0.0.3. If the NAT IP address of TC-HQ-1 changes to 98.0.0.3 and TC-HQ-2 stays at 98.0.0.2, they can still peer. However, if TC-HQ-1 changes to 98.0.0.4, it cannot peer with TC-HQ-2.
- 98.0.0.1/32 and 98.0.0.2/32: Peering is allowed only for Tanium Clients with NAT IP addresses 98.0.0.1 and 98.0.0.2. TC-HQ-1 and TC-HQ-2 cannot peer if their NAT IP addresses change.

After you determine the appropriate subnet ranges, follow the steps in Define intentional subnets using Sites.

- If the IP addresses are too varied to define reasonable subnets, or if subnets overlap among sites that need to remain isolated, see Define intentional subnets using the PeerNeighborhood Client setting.

4. Consider whether newly deployed Clients in certain networks might have different NAT IP addresses but are allowed to peer. If so, see Define intentional subnets using the PeerNeighborhood Client setting.

> **Note:** After you configure intentional subnets, Tanium Clients might take up to two to six hours (the randomized Client-reset interval) to finish applying all the changes associated with the new configuration.
> Intentional subnet configurations are always synchronized across all Zone Servers and Tanium Servers.

Define intentional subnets using Sites

The Tanium Server can identify an intentional subnet by a **Site** name that you specify and allow peering among all Tanium Clients that are in the subnets you add to that **Site**.

ADD SUBNETS

1. From the Main menu, go to **Administration** > **Configuration** > **Subnets**.
2. In the **Intentional Subnets** section, click **New Subnets**.
3. Enter a name to identify the **Site** that comprises the intentional subnets.

©2026 Tanium Inc. All Rights Reserved

4. (Optional) Enter a comment to help other users understand the function of the subnet in your organization.
5. In the **New subnet CIDRs** field, enter each subnet in CIDR format (`a.b.c.d/x`) using separate lines or commas as delimiters.
6. Click **Save**.

EDIT SUBNETS

1. From the Main menu, go to **Administration** > **Configuration** > **Subnets**.
2. Select one of the **Intentional Subnets** and click **Edit**.
3. Edit the subnet (**CIDR**) and **Comment**, and click **Save**.

Define intentional subnets using the PeerNeighborhood Client setting

Use the **PeerNeighborhood** Client setting to designate certain Clients that are allowed to peer with one another. You can apply the setting during or after Client deployment. The Tanium Server allows these Clients to peer, regardless of the NAT IP of each Client.

Set the same **PeerNeighborhood** name for all Clients in each site that are allowed to peer. For example, if you have lab sites "Lab East" and "Lab West," you can set the **PeerNeighborhood** Client setting for all Clients in each site to `Lab-East` and `Lab-West` respectively.

For methods to modify the **PeerNeighborhood** Client setting, see Tanium Client Management User Guide: Modify Client settings.

Verify intentional subnets

After you configure intentional subnets, wait for the next Client-reset interval before verifying that the subnets work as expected. For more information, see Verify or remediate Tanium Client peering and leader connections. In the **Administration** > **Configuration** > **Client Status** page, the **Network Location (from Client)** column shows the pre-NAT IP addresses and the **Network Location (from Server)** column shows the NAT IP addresses.

Verify or remediate Tanium Client peering and leader connections

©2026 Tanium Inc. All Rights Reserved

The **Client Status** page shows information about the state of Tanium Client registration and connectivity, and enables you to deploy actions to remediate issues.

> **Note:**
>
> **Client Status read** permission is required to see the **Client Status** page. The **Administrator** reserved role has this permission.
>
> The **Client Status** page shows information for all Clients that meet the specified filter criteria, regardless of whether those Clients are in computer groups that are assigned to your user account or persona. However, computer group assignments still determine to which Clients you can deploy actions.
>
> The **Client Status** page does not show information for endpoints managed using entity providers. For more information, see Entity providers.

View the status of Tanium Client registration and communication

1. From the Main menu, go to **Administration** > **Configuration** > **Client Status**.
2. (Optional) Edit the default filter settings to view details only for specific Clients. You can also enter text in the **Filter items** field to filter the grid by host name, computer ID, network location, send/receive state, status, or version.
3. (Optional) Select **Hide Duplicate Host Names** (it is selected by default) to show only one row for each **Host Name**, containing only the information from the last time the Client registered. If you clear the checkbox, the grid shows a separate row for each registration in which the Tanium Server assigned a different Computer ID on page 280 to the host.

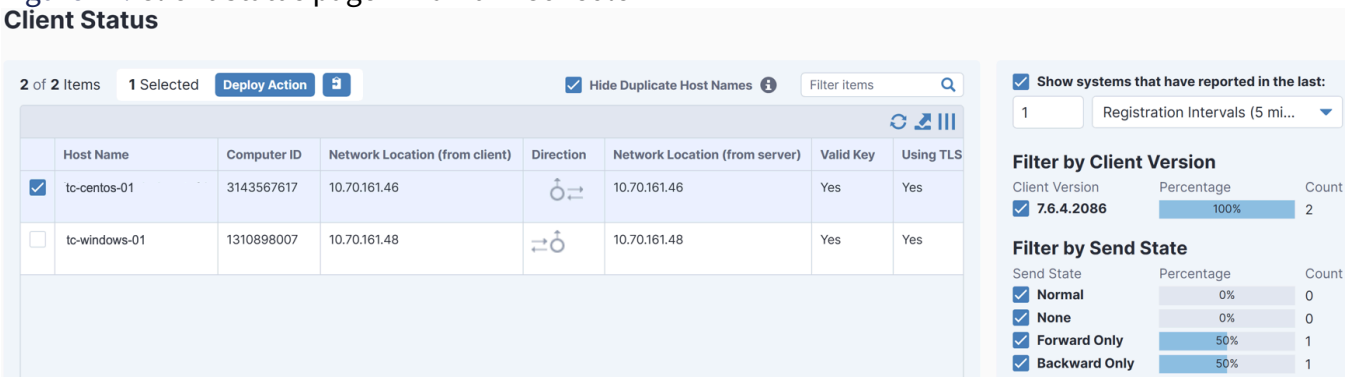
   > **Note:** In the **<#> of <#> Items** count, the first number shows the number of grid rows, which changes based on the filters that you specify. The second number shows the unfiltered number of registered Clients, which changes based on whether you select **Hide Duplicate Host Names**.

©2026 Tanium Inc. All Rights Reserved

Tip: To check if the count of managed endpoints is within the limit of your Tanium license, select **Hide Duplicate Host Names** and set the filter **Show systems that have reported in the last** to `30 Days`. To see the most accurate count for purposes other than license usage, go to the Tanium **Home** page, **Environment Status** section, and check the **Total Endpoints**. For more information, see View environment status.

Client Status columns and connection states

Figure 14. Client Status page in Tanium Console



The following table lists the information that the **Client Status** page displays for each Tanium Client.

Tip: Certain columns are hidden by default. To show or hide columns, click Customize Columns and select (show) or clear (hide) column names.

Client Status columns

Column	Description
Host Name	Endpoint host name.
Computer ID	The computer ID uniquely identifies each managed endpoint that connects to the Tanium Server at any given moment. The Server assigns the ID when the Tanium Client registers. The computer ID might change when a Client re-registers after certain events, such as: • The endpoint is re-imaged or cloned. • A new OS is installed on the endpoint.

©2026 Tanium Inc. All Rights Reserved

Column	Description
	• The endpoint is a virtual machine (VM) that is reverted to a previous state. The Client records every computer ID that the Server has assigned over the history of registrations for that Client. However, only the last assigned ID counts towards the maximum managed endpoints that your Tanium license specifies. **Note:** The **Computer ID** column shows the same value as the **Computer ID** sensor. If you issue a question with the sensor, the Client returns all the computer IDs that the Tanium Server has assigned to the host. For more information about how the Server assigns the ID, see Information about registration and ComputerID .
Network Location (from Client)	Client IP address returned from a sensor on the Client.
Network Location (from Server)	Client IP address recorded on the Tanium Server or Zone Server during the last registration.
Direction	A circle represents the Client and arrows represent its connections. For a list of possible connection states, see the table Table 33. Tanium Client peer connection states on page 269 .
Valid Key	`No` indicates an issue with the public key that the Tanium Client uses to secure communication with other Tanium Core Platform components. Perform one of the following tasks to resolve the issue: • Reinstall the Tanium Client. For more information, see Deploying the Tanium Client. • Redeploy the key. For more information, see Download infrastructure configuration files (keys).
Using TLS	This column indicates whether Clients are (`Yes`) or are not (`No`) using Transport Layer Security (TLS) for communication with the Tanium Server or Zone Server .
Send State	• **Normal**: The Client is sending data to its backward and forward peers. • **None**: The Client is not sending data to its forward or backward peers. • **Forward Only**: The Client is sending data to its forward peer but not to its backward peer. • **Backward Only**: The Client is sending data to its backward peer but not to its forward peer.
Receive State	• **Normal**: The Client is receiving data from its backward and forward peers. • **None**: The Client is not receiving data from its forward or backward peers.

©2026 Tanium Inc. All Rights Reserved

Column	Description
	• **Next Only**: The Client is receiving data from its forward peer but not from its backward peer. • **Previous Only**: The Client is receiving data from its backward peer but not from its forward peer.
Status	• **Normal**: The Client is communicating normally. • **Slow Link**: The Client has connections with abnormally slow throughput. • **Leader**: The Client is communicating with the Tanium Server or Zone Server because it is a backward leader, a forward leader, a neighborhood leader, or a Client with no peer connections (such as a Client in an isolated subnet). • **Blocked**: The Client is not communicating reliably.
Last Registration	Date and time when the Tanium Client last registered with the Tanium Server or Zone Server.
Protocol Version (hidden by default)	Tanium Protocol version. For more information about the protocol, see TLS communication.
Version	Tanium Client version.

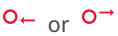
The **Direction** column displays icons that use the following conventions to depict Tanium Client connection states:

- An up arrow indicates a connection with the Tanium Server or Zone Server.
- Side arrows pointing away from the Client indicate outbound connections to peers.
- Side arrows pointing at the Client indicate inbound connections from peers.
- Side arrows on the right side of Clients indicate the state of connections to forward peers.
- Side arrows on the left side of Clients indicate the state of connections to backward peers.
- Side arrows with dashed lines indicate slow connections.

You can use the **Direction** column to understand why a Tanium Client is a leader and to identify connection issues. The following table lists the possible connection states:

©2026 Tanium Inc. All Rights Reserved

Tanium Client peer connection states

Attribute	Value	Description
Leader	Backward 	The Client is a backward leader that terminates one end of a linear chain. It typically has the lowest IP address in its linear chain.
	Forward 	The Client is a forward leader that terminates one end of a linear chain. It typically has the highest IP address in its linear chain.
	Neighborhood 	The Client is designated as a neighborhood leader because its linear chain has reached the maximum number of Clients.
	Isolated 	The Client is an isolated leader that connects only to the Tanium Server or Zone Server , and has no connections to other Clients. The Client might be isolated because its IP address falls within the range of an isolated subnet or because it has no peers in its local subnet with which to connect.
Neighbor	No side arrows 	This is the same as an isolated leader.
	Single side arrow 	The Client has a neighborhood list of peers but has not established a peer connection. This state generally results from a misconfiguration, such as when a host-based firewall on the endpoint does not allow inbound connections to the Client.
	Double side arrows	The Client has a neighborhood list of peers and has connected with peers.
Client state	Normal	A Client represented by an empty circle is communicating normally. Any of the above neighbor or leader arrows might apply.
	Blocked	A Client represented by a circle with an X is not communicating reliably with connected peers (when the Client displays neighbor arrows) or with the Tanium Server or Zone Server (when the Client displays a leader arrow). Unreliable communication might result from a network issue or host resource issue, such as an anti-virus program that slows the Client.

©2026 Tanium Inc. All Rights Reserved

Export Tanium Client status details

About this task

Export information in the **Client Status** page as a CSV file or, if you have the **Administrator** reserved role, as a JSON file.

1. From the Main menu, go to **Administration** > **Configuration** > **Client Status**.
2. Edit the default filter settings to show only the Clients for which you want to export information. You can also enter text in the **Filter items** field to filter the grid by host name, computer ID, network location, send/receive state, status, or version. Skip this step if you want to export information for all Clients.
3. Select rows in the grid to export information for specific Tanium Clients. Skip this step if you want to export information for all Clients.
4. Click Export .
5. (Optional) Edit the default export **File Name**.

   > **Note:** The file suffix (.csv or .json) changes automatically based on the **Format** selection.

6. Select an **Export Data** option:
   - **All**: Export information for all Clients that have registered, regardless of whether the grid is filtered to exclude them
   - **Selected**: Export information only for the Clients that you selected in the grid
   - **Filtered**: Export information only for the Clients that the grid filters include
7. Select the file **Format**:
   - **List of Clients**: Export the information as a CSV file.
   - **Client Definitions** (**Administrator** reserved role only): Export the information as a JSON file.
8. Click **Export**.
   The Tanium Server exports the file to the downloads folder on the system that you used to access Tanium Client Management.

Copy Tanium Client status details

©2026 Tanium Inc. All Rights Reserved

About this task

Copy information from the **Client Status** page to your clipboard to paste the information into a message, text file, or spreadsheet. Each row in the grid is a comma-separated value string.

1. From the Main menu, go to **Administration** > **Configuration** > **Client Status**.
2. Perform one of the following steps:
   - Copy row information: Select one or more rows and click Copy .
   - Copy cell information: Hover over the cell, click Options , and click Copy .

Deploy actions to remediate Client registration or connectivity issues

About this task

You can deploy actions to Tanium Clients to remediate issues that you observe in the **Client Status** page. For example, if you want certain Clients to register with a Tanium Zone Server instead of the Tanium Server, you can deploy the **Set Tanium Server Name List** package to change the **ServerNameList** setting on those Clients.

1. From the Main menu, go to **Administration** > **Configuration** > **Client Status**.
2. Select the Tanium Clients (up to 100) to which you want to deploy actions and click **Deploy Action**.
3. Deploy the action.
4. Review the **Client Status** grid to verify that the action produced the expected result.

Use questions to review peering settings

About this task

The content-only solution Tanium™ Default Content includes sensors that you can use in questions to examine settings for Tanium Client peer communication:

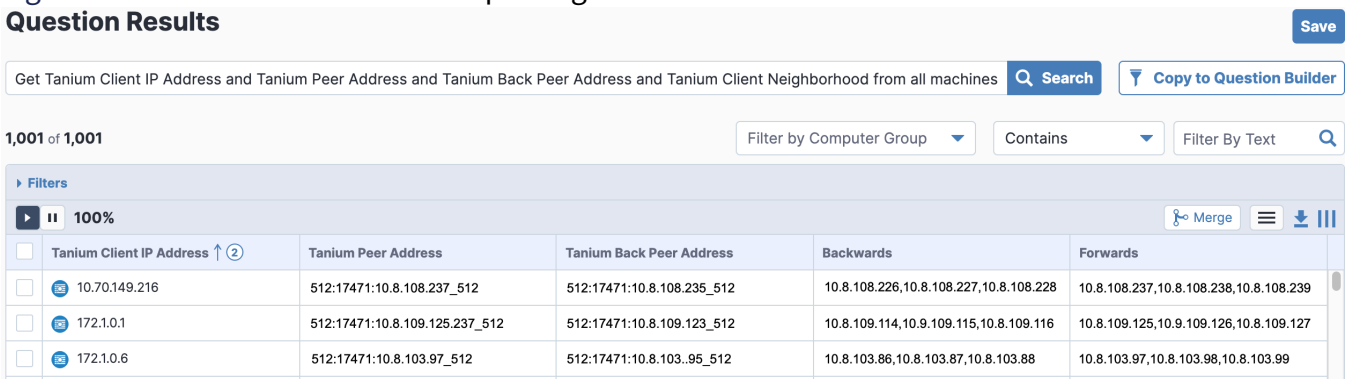
- **Tanium Client IP Address**
- **Tanium Peer Address**
- **Tanium Back Peer Address**

©2026 Tanium Inc. All Rights Reserved

- **Tanium Client Neighborhood**

The following example is a dynamic question that uses these sensors. Note that the results for the **Tanium Client Neighborhood** sensor display in the **Backwards** and **Forwards** columns:

Figure 15. Sensors for Tanium Client peering information



Examine the Tanium Client configuration

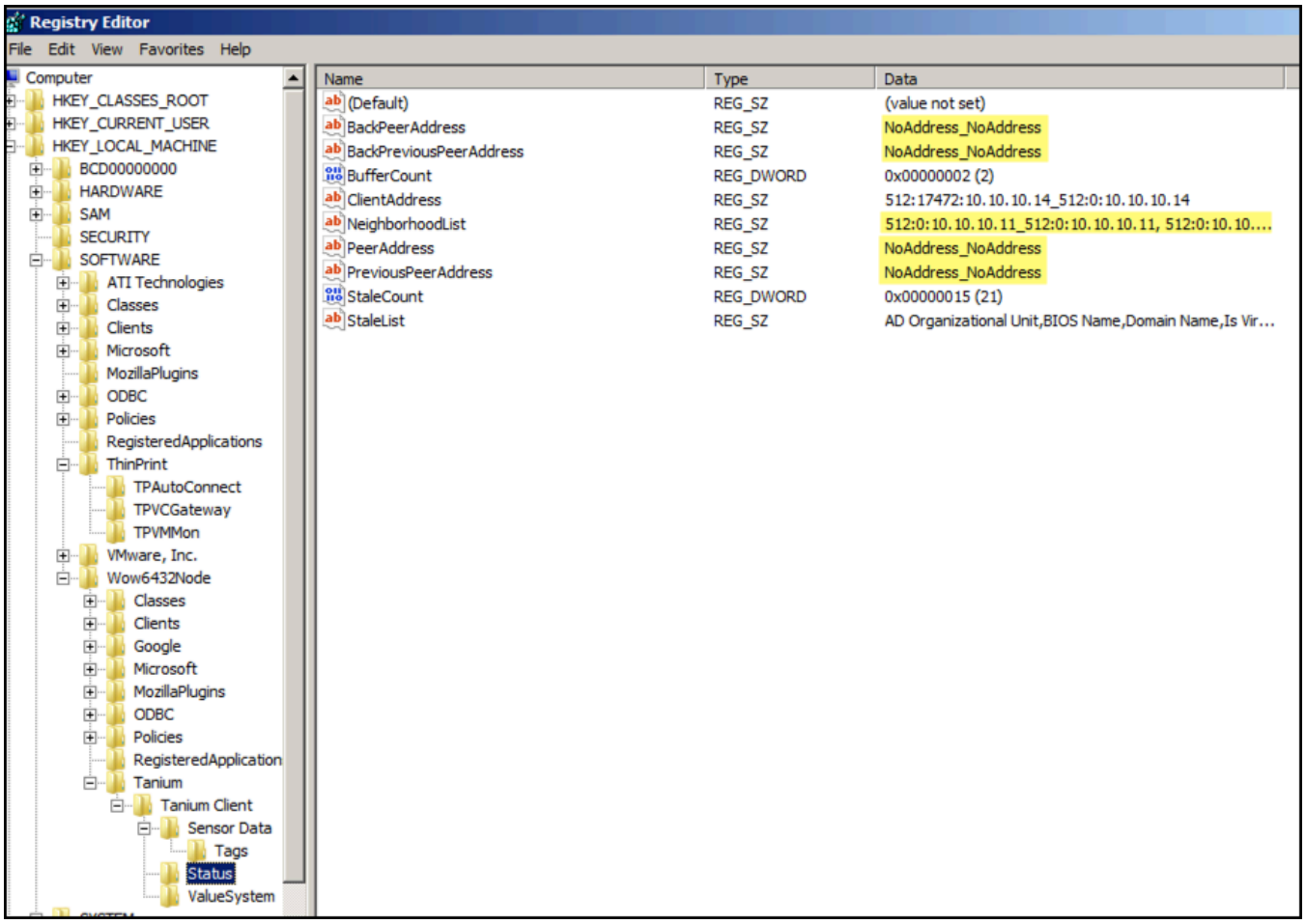
About this task

You can check the peer address lists in the Tanium Client settings on an individual Client.

The following is an example of a Windows registry for a Tanium Client that has peering disabled through the isolated subnets configuration. The **NeighorhoodList** setting still lists peers, but their ports are set to 0 to prevent the Client from connecting with those peers.

Figure 16. Peering information in Windows Registry

©2026 Tanium Inc. All Rights Reserved



The following example shows CLI output for the neighborhood and peering information in the Tanium Client database:

```
$ sudo ./TaniumClient config list
Keys:
  - ComputerID: 3235161864
  - DatabaseEpoch: 2017-11-01 17:54:19.073914
  - HostDomainName: cloud.tanium.comtam.local
  - LastGoodServerName: taas-example1-zs.cloud.tanium.comzs1.tam.local
  - LogVerbosityLevel: 1
  - RegistrationCount: 3333
  - Resolver: nslookup
  - ServerName: taas-example1-zs.cloud.tanium.comzs1.tam.local
  - ServerNameList: taas-example1-zs.cloud.tanium.com,taas-
example2-zs.cloud.tanium.comts1.tam.local,zs1.tam.local
  - ServerPort: 17472
  - Status:
    - Status.BackPeerAddress: 512:17472:10.10.10.40_512:0:10.10.10.40
    - Status.BackPreviousPeerAddress: NoAddress_NoAddress
    - Status.BufferCount: 2
    - Status.ClientAddress: 512:17472:10.10.10.51_512:0:10.10.10.51
    - Status.NeighborhoodList: 512:17472:10.10.10.13_512:0:10.10.10.13,
      512:17472:10.10.10.40_512:0:10.10.10.40, 512:17472:10.10.10.51_512:0:10.10.10.51
    - Status.PeerAddress: NoAddress_NoAddress
    - Status.PreviousPeerAddress: 512:17473:10.10.10.11_512:0:10.10.10.11
    - Status.StaleCount: 34
```

©2026 Tanium Inc. All Rights Reserved

```
    - Status.StaleList: Operating System,NAT IP Address,Online,OS Platform,Available Patches,
      Running Processes Memory Usage,Tanium Client Version,Disk Used Percentage,Reboot
Required,
      Tanium Client Core Health,Is Virtual,Disk Free Space,tempsensor_33,Installed
Applications,
      Comply - Compliance Aggregates,Has Tanium Standard Utilities,Has Patch Tools,Installed
Patches,
      Manufacturer,Has Hardware Tools,Is Windows,Chassis Type,Is Mac,IOC Detect Tools
Version,
      Comply - Vulnerability Aggregates,Patch Cab Out of Date,IP Address,Uptime,Network
Adapters,
      Is Linux,Open Ports,Running Processes
  - ValueSystem:
    - ValueSystem.0 0: 1
    - ValueSystem.CorrelationDecisionHaste: 1
    - ValueSystem.CorrelationRequiredConfidence: 0.69999999999999996
    - ValueSystem.CorrelationThresholdMultiplier: 1
    - ValueSystem.CorrelationVolumeMultiplier: 0.01
    - ValueSystem.PrevalenceDecisionHaste: 1
    - ValueSystem.PrevalenceRequiredConfidence: 0.69999999999999996
    - ValueSystem.PrevalenceVolumeMultiplier: 1
    - ValueSystem.ValueThreshold: 0.10000000000000001
  - Version:
```

Customize listening ports

The Client uses the listening port to receive communications from peer Clients that are in the same linear chain. By default, the Client listens for communication from peer Clients on the port specified for the **ServerPort** setting. You can configure a specific custom listening port, or you can randomize the listening port at intervals.

Important: Work with your network administrator to configure firewalls on endpoints in linear chains to allow incoming connections on any port that the Tanium Client uses to process requests. The process is TaniumClient.exe on Windows endpoints and TaniumClient or taniumclient on other endpoints.

Note: Endpoints in isolated subnets or that otherwise do not have valid peers do not open the listening port and do not require firewall rules to allow incoming traffic on this port. For more information, see Configure isolated subnets on page 255.

©2026 Tanium Inc. All Rights Reserved

Best Practice:

- If you configure listening port settings, use the same values for all Clients in the same subnet.
- Configure listening port settings in Tanium Console. For more information, see Modify default Client settings in Tanium Console on page 323.

Configure a custom listening port

To configure a specific custom listening port for Client communication, configure the **ListenPort** setting on all Clients. When you configure a value for the **ListenPort** setting, it overrides the **ServerPort** setting for communication between Clients.

Note:

- If you enable **EnableRandomListeningPort**, do not configure **ListenPort** because the Client overwrites the value whenever it selects a new port.
- Changes to **ListenPort** automatically affect the Tanium Client API port, which is one port number higher. For example, if you set **ListenPort** to 17473, the Client API port becomes 17474.

Randomize listening ports

You can configure the Tanium Client to randomly select a new listening port at intervals.

Best Practice: Randomize listening ports only if it is required by rules in your organization. Using randomized listening ports requires more complex firewall rules to allow Client communication, and it makes troubleshooting issues with Client communication more difficult.

©2026 Tanium Inc. All Rights Reserved

Note:

By default, the port number for the Tanium Client API is one number greater than the Client listening port. However, if you enable randomization for the listening port, the API port remains fixed at 17473, except under the following conditions:

- The Client is installed on the same host as the Tanium Server or Zone Server. (This installation is not a best practice. For more information, see Compatibility among components in a Tanium release on page 56.)
- A port other than the default 17472 is configured for Tanium traffic on the Server.

When you have enabled randomization for the listening port and these conditions apply, the Client API port on the Server host is one number greater than the Server port. For example, if you change the Tanium Server **ServerPort** setting from the default 17472 to 17473, the Client API port on the Server host changes to 17474.

The following Client settings on the control randomization of the listening port:

EnableRandomListeningPort

Enables (`1`) or disables (`0`) the randomized selection of a new listening port at intervals. The Client uses the port for communication from peer Clients. If another application is already using the selected port, the Client selects another port immediately instead of at the next interval.

Note: If you change **EnableRandomListeningPort** from enabled to disabled, you must also remove the **ListenPort** setting or set it to the desired port. Otherwise, the port that the Client last randomly selected before you disabled **EnableRandomListeningPort** becomes the permanent listening port.

RandomListeningPortMin

Specifies the low end of the range of ports from which the Client randomly selects a listening port if you enabled **EnableRandomListeningPort**. The default is port `32000`.

©2026 Tanium Inc. All Rights Reserved

RandomListeningPortMax

Specifies the high end of the range of ports from which the Client randomly selects a listening port if you enabled **EnableRandomListeningPort**. The default is port `64000`

RandomListeningPortTTLInHours

Specifies the interval in hours at which the Client selects a new listening port if you enabled **EnableRandomListeningPort**. The default is `24` hours. Do not set the value lower than the Client reset interval, which by default is a random interval in the range of 2 to 6 hours.

RandomListeningPortExclusions

Specifies ports that the Client never selects as a listening port if you enable **EnableRandomListeningPort**. For example, to prevent port competition conflicts, you might specify ports that other applications use. If you specify multiple exclusions, use a comma to separate each port. By default, the Client does not exclude any ports that are within the range that the **RandomListeningPortMin** and **RandomListeningPortMax** settings define.

©2026 Tanium Inc. All Rights Reserved

Monitoring, managing, and maintaining Tanium Clients

The subsequent topics in this section provide information on general monitoring, management, and maintenance of Tanium Clients.

- Monitoring Tanium Clients on page 278
- Managing Tanium Clients on page 288
- Managing Client settings and Index configurations on page 318
- Maintaining Tanium Clients on page 331
- Upgrading Tanium Clients on page 342
- Uninstalling Tanium Clients on page 351

Monitoring Tanium Clients

The **Client Status** page shows information about the state of Tanium Client registration and connectivity, and enables you to deploy actions to remediate issues.



Note:

Client Status read permission is required to see the **Client Status** page. The **Administrator** reserved role has this permission.

The **Client Status** page shows information for all Clients that meet the specified filter criteria, regardless of whether those Clients are in computer groups that are assigned to your user account or persona. However, computer group assignments still determine to which Clients you can deploy actions.

The **Client Status** page does not show information for endpoints managed using entity providers. For more information, see Entity providers.

For information about remediating issues with Client peering, see Verify or remediate Tanium Client

©2026 Tanium Inc. All Rights Reserved

peering and leader connections on page 264.

View the status of Tanium Client registration and communication

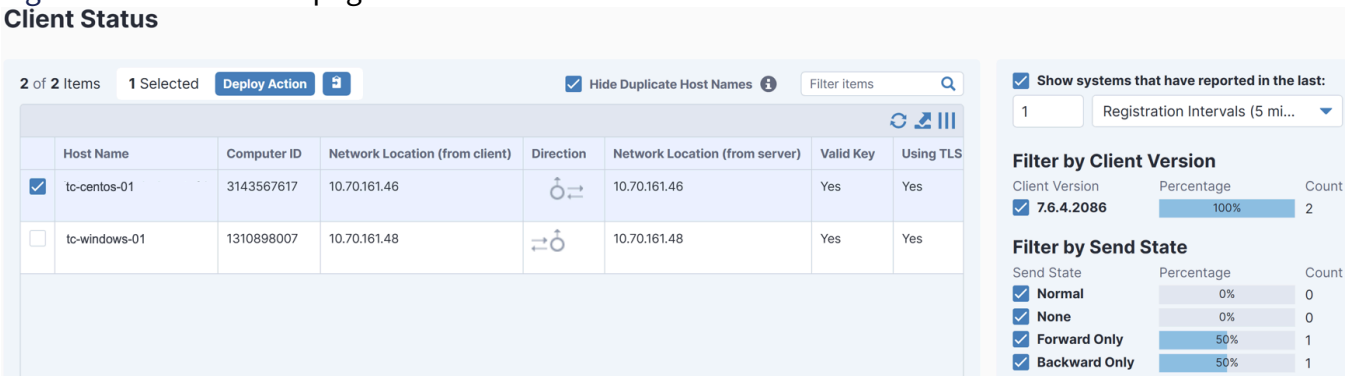
1. From the Main menu, go to **Administration** > **Configuration** > **Client Status**.
2. (Optional) Edit the default filter settings to view details only for specific Clients. You can also enter text in the **Filter items** field to filter the grid by host name, computer ID, network location, send/receive state, status, or version.
3. (Optional) Select **Hide Duplicate Host Names** (it is selected by default) to show only one row for each **Host Name**, containing only the information from the last time the Client registered. If you clear the checkbox, the grid shows a separate row for each registration in which the Tanium Server assigned a different Computer ID on page 280 to the host.

   Note: In the **<#> of <#> Items** count, the first number shows the number of grid rows, which changes based on the filters that you specify. The second number shows the unfiltered number of registered Clients, which changes based on whether you select **Hide Duplicate Host Names**.

   Tip: To check if the count of managed endpoints is within the limit of your Tanium license, select **Hide Duplicate Host Names** and set the filter **Show systems that have reported in the last** to `30 Days`. To see the most accurate count for purposes other than license usage, go to the Tanium **Home** page, **Environment Status** section, and check the **Total Endpoints**. For more information, see View environment status.

CLIENT STATUS COLUMNS AND CONNECTION STATES

Figure 17. Client Status page in Tanium Console



©2026 Tanium Inc. All Rights Reserved

The following table lists the information that the **Client Status** page displays for each Tanium Client.

Tip: Certain columns are hidden by default. To show or hide columns, click Customize Columns and select (show) or clear (hide) column names.

Client Status columns

Column	Description
Host Name	Endpoint host name.
Computer ID	The computer ID uniquely identifies each managed endpoint that connects to the Tanium Server at any given moment. The Server assigns the ID when the Tanium Client registers. The computer ID might change when a Client re-registers after certain events, such as: • The endpoint is re-imaged or cloned. • A new OS is installed on the endpoint. • The endpoint is a virtual machine (VM) that is reverted to a previous state. The Client records every computer ID that the Server has assigned over the history of registrations for that Client. However, only the last assigned ID counts towards the maximum managed endpoints that your Tanium license specifies. **Note:** The **Computer ID** column shows the same value as the **Computer ID** sensor. If you issue a question with the sensor, the Client returns all the computer IDs that the Tanium Server has assigned to the host. For more information about how the Server assigns the ID, see Information about registration and ComputerID .
Network Location (from Client)	Client IP address returned from a sensor on the Client.
Network Location (from Server)	Client IP address recorded on the Tanium Server or Zone Server during the last registration.
Direction	A circle represents the Client and arrows represent its connections. For a list of possible connection states, see the table Table 35. Tanium Client peer connection states on page 282 .
Valid Key	`No` indicates an issue with the public key that the Tanium Client uses to secure communication with other Tanium Core Platform components.

©2026 Tanium Inc. All Rights Reserved

Column	Description
	Perform one of the following tasks to resolve the issue: • Reinstall the Tanium Client. For more information, see Deploying the Tanium Client. • Redeploy the key. For more information, see Download infrastructure configuration files (keys).
Using TLS	This column indicates whether Clients are (`Yes`) or are not (`No`) using Transport Layer Security (TLS) for communication with the Tanium Server or Zone Server .
Send State	• **Normal**: The Client is sending data to its backward and forward peers. • **None**: The Client is not sending data to its forward or backward peers. • **Forward Only**: The Client is sending data to its forward peer but not to its backward peer. • **Backward Only**: The Client is sending data to its backward peer but not to its forward peer.
Receive State	• **Normal**: The Client is receiving data from its backward and forward peers. • **None**: The Client is not receiving data from its forward or backward peers. • **Next Only**: The Client is receiving data from its forward peer but not from its backward peer. • **Previous Only**: The Client is receiving data from its backward peer but not from its forward peer.
Status	• **Normal**: The Client is communicating normally. • **Slow Link**: The Client has connections with abnormally slow throughput. • **Leader**: The Client is communicating with the Tanium Server or Zone Server because it is a backward leader, a forward leader, a neighborhood leader, or a Client with no peer connections (such as a Client in an isolated subnet). • **Blocked**: The Client is not communicating reliably.
Last Registration	Date and time when the Tanium Client last registered with the Tanium Server or Zone Server .
Protocol Version (hidden by default)	Tanium Protocol version. For more information about the protocol, see TLS communication .
Version	Tanium Client version.

The **Direction** column displays icons that use the following conventions to depict Tanium Client connection states:

©2026 Tanium Inc. All Rights Reserved

- An up arrow indicates a connection with the Tanium Server or Zone Server.
- Side arrows pointing away from the Client indicate outbound connections to peers.
- Side arrows pointing at the Client indicate inbound connections from peers.
- Side arrows on the right side of Clients indicate the state of connections to forward peers.
- Side arrows on the left side of Clients indicate the state of connections to backward peers.
- Side arrows with dashed lines indicate slow connections.

You can use the **Direction** column to understand why a Tanium Client is a leader and to identify connection issues. The following table lists the possible connection states:

Tanium Client peer connection states

Attribute	Value	Description
Leader	Backward 	The Client is a backward leader that terminates one end of a linear chain. It typically has the lowest IP address in its linear chain.
	Forward 	The Client is a forward leader that terminates one end of a linear chain. It typically has the highest IP address in its linear chain.
	Neighborhood	The Client is designated as a neighborhood leader because its linear chain has reached the maximum number of Clients.
	Isolated 	The Client is an isolated leader that connects only to the Tanium Server or Zone Server , and has no connections to other Clients. The Client might be isolated because its IP address falls within the range of an isolated subnet or because it has no peers in its local subnet with which to connect.
Neighbor	No side arrows	This is the same as an isolated leader.
	Single side arrow  or 	The Client has a neighborhood list of peers but has not established a peer connection. This state generally results from a misconfiguration, such as when a host-based firewall on the endpoint does not allow inbound connections to the Client.

©2026 Tanium Inc. All Rights Reserved

Attribute	Value	Description
	Double side arrows	The Client has a neighborhood list of peers and has connected with peers.
Client state	Normal	A Client represented by an empty circle is communicating normally. Any of the above neighbor or leader arrows might apply.
	Blocked	A Client represented by a circle with an X is not communicating reliably with connected peers (when the Client displays neighbor arrows) or with the Tanium Server or Zone Server (when the Client displays a leader arrow). Unreliable communication might result from a network issue or host resource issue, such as an anti-virus program that slows the Client.

EXPORT TANIUM CLIENT STATUS DETAILS

About this task

Export information in the **Client Status** page as a CSV file or, if you have the **Administrator** reserved role, as a JSON file.

1. From the Main menu, go to **Administration** > **Configuration** > **Client Status**.
2. Edit the default filter settings to show only the Clients for which you want to export information. You can also enter text in the **Filter items** field to filter the grid by host name, computer ID, network location, send/receive state, status, or version. Skip this step if you want to export information for all Clients.
3. Select rows in the grid to export information for specific Tanium Clients. Skip this step if you want to export information for all Clients.
4. Click Export .
5. (Optional) Edit the default export **File Name**.

   Note: The file suffix (.csv or .json) changes automatically based on the **Format** selection.

6. Select an **Export Data** option:

©2026 Tanium Inc. All Rights Reserved

- **All**: Export information for all Clients that have registered, regardless of whether the grid is filtered to exclude them
- **Selected**: Export information only for the Clients that you selected in the grid
- **Filtered**: Export information only for the Clients that the grid filters include

7. Select the file **Format**:
   - **List of Clients**: Export the information as a CSV file.
   - **Client Definitions** (**Administrator** reserved role only): Export the information as a JSON file.
8. Click **Export**.
   The Tanium Server exports the file to the downloads folder on the system that you used to access Tanium Client Management.

COPY TANIUM CLIENT STATUS DETAILS

About this task

Copy information from the **Client Status** page to your clipboard to paste the information into a message, text file, or spreadsheet. Each row in the grid is a comma-separated value string.

1. From the Main menu, go to **Administration** > **Configuration** > **Client Status**.
2. Perform one of the following steps:
   - Copy row information: Select one or more rows and click Copy .
   - Copy cell information: Hover over the cell, click Options , and click Copy .

Monitor the Client health overview in Client Management

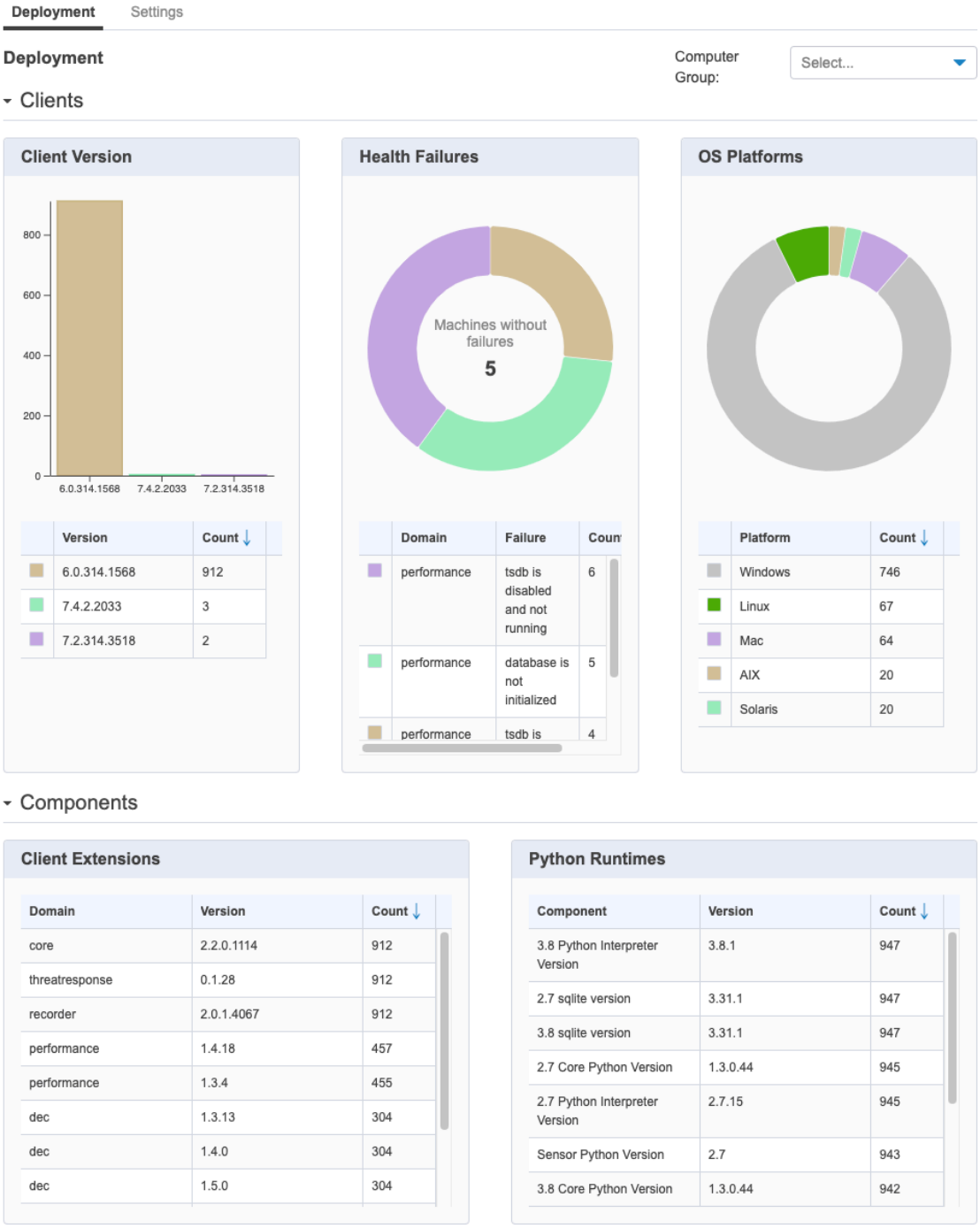
About this task

Review a summary of health information about deployed Tanium Clients in Client Management.

1. From the Main menu, go to **Shared Services** > **Client Management**.
2. Go to **Client Health**.
3. Click the tab that contains the information that you want to view.
   - Click the **Deployment** tab to view a summary of Client deployment information, such as Client versions, health check failures, operating systems, installed Client Extensions, and Python runtime versions.

©2026 Tanium Inc. All Rights Reserved

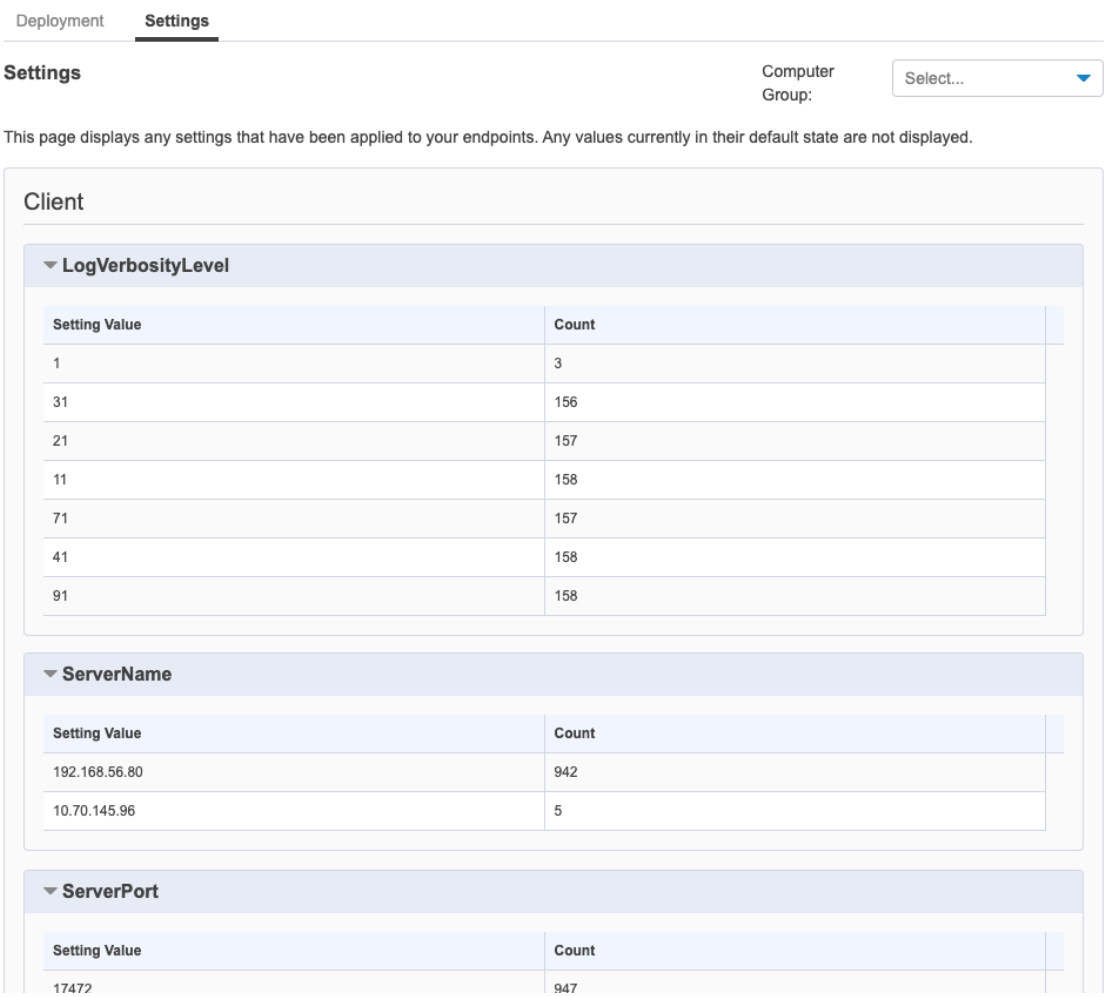
Figure 18. Client Health Deployment tab



- Click the **Settings** tab to view a summary of Client settings, such as log verbosity level, Server name, Server port, and various component information. This overview can help identify settings that have been changed from defaults.

Figure 19. Client Health Settings tab

©2026 Tanium Inc. All Rights Reserved



4. (Optional) Select a **Computer Group** to filter the summary information.
5. (Optional) To further investigate a data set using the associated question results, click View question results in Interact. For more information about working with question results, see Managing question results.

Next steps

©2026 Tanium Inc. All Rights Reserved

Tip:

To resolve Client Extension failures, see the following sections:

- To resolve Client Index Extension failures, see Reference: Common health check issues.
- To resolve Client Recorder Extension failures, see Troubleshooting the Client Recorder Extension.
- To resolve failures associated with Client Extensions for other Tanium solutions, see Troubleshoot solution-specific issues and Identify and resolve issues with endpoint tools or Client Extensions.

Access detailed Client health and troubleshooting information on an endpoint

About this task

You can directly connect to a Windows, Linux, or macOS endpoint from Client Management to view detailed Client health information and to access and collect information that can be useful for troubleshooting.

Tip: For additional information about troubleshooting the Tanium Client, see Troubleshooting Tanium Clients and Client Management on page 356.

©2026 Tanium Inc. All Rights Reserved

Note:

Direct Connect has the following restrictions:

- You can directly connect only to an endpoint that has an IPv4 address.
- To connect to endpoints with action lock turned on, you must enable the **Bypass Action Lock** setting in Direct Connect. To access this setting, from the Direct Connect **Overview** page, click Settings  and select **Endpoint Connection**. For more information, see Configure Direct Connect and Managing action locks.

1. From the Main menu, go to **Shared Services** > **Client Management**.
2. Go to **Client Health**.
3. In the **Single Endpoint View** search box, enter all or part of an IP address or a computer name.
   Matching results are displayed after the search completes.
4. From the search results, click the computer name.
   Client Management opens the Endpoint Details page in Single Endpoint View (SEV).
5. Click the **Client Health** tab and, if the endpoint is not yet **Connected**, click **Direct Connect**.
   From the **Client Health** tab, you can view and download Client logs and action logs, and gather troubleshooting information from the endpoint. For more information, see Tanium Reporting User Guide: View and download Tanium Client logs and Tanium Reporting User Guide: Collect troubleshooting information.

Managing Tanium Clients

The following sections provide information about management tasks for the Tanium Client across all operating systems.

Additionally, the subsequent topics in this section provide information about managing the Tanium Client on each operating system.

- Manage the client on Windows on page 293

©2026 Tanium Inc. All Rights Reserved

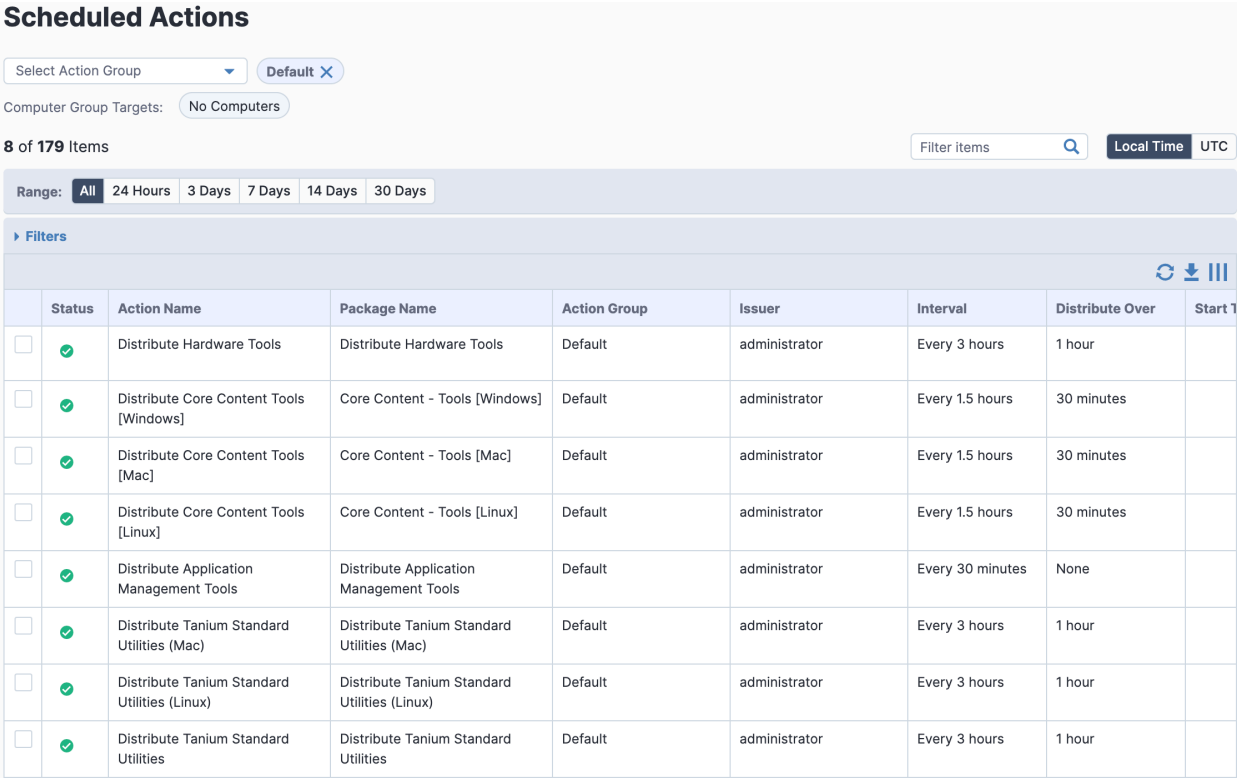
- Manage the client on macOS on page 305
- Manage the client on Linux on page 308
- Manage the client on Solaris on page 315
- Manage the client on AIX on page 316

Use built-in saved questions, sensors, and packages

The Tanium Server imports the Tanium™ Default Content pack when you initially sign in to Tanium Console. This content pack contains a key set of saved questions, sensors, and packages that you can use to collect information from endpoints and take actions. The content pack also includes saved questions and scheduled actions that relate to the deployment of the Tanium Client. To access Tanium Client-related content, access the following Tanium Console pages:

- From the Main menu, go to **Administration** > **Actions** > **Scheduled Actions**, select **Default** for the **Action Group**, and review the actions that are scheduled to run.

  Figure 20. Default scheduled actions for the Tanium Client

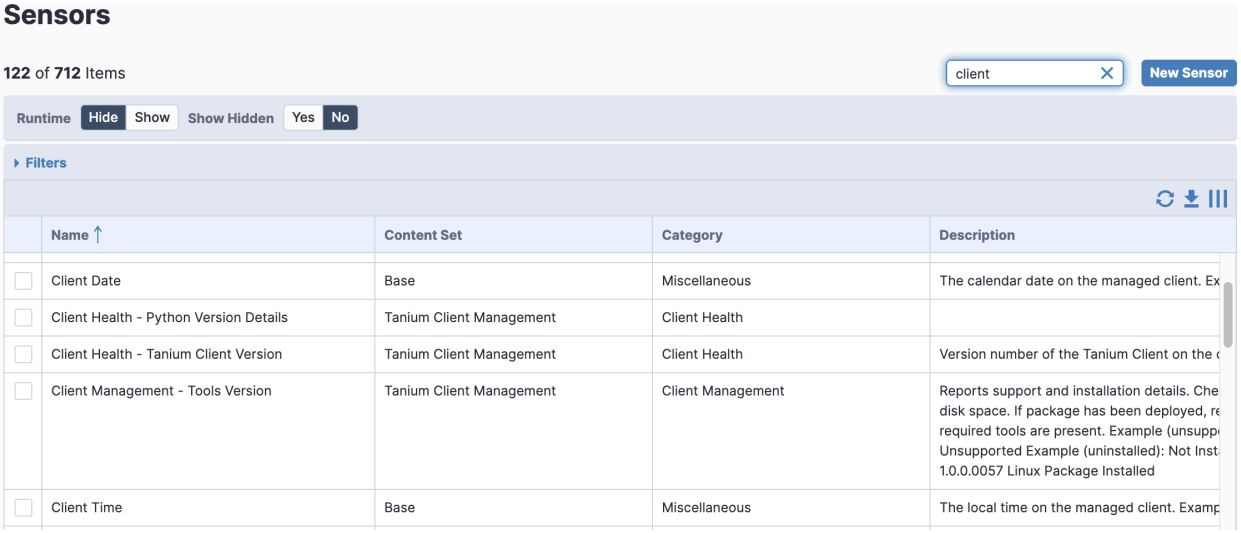


Status	Action Name	Package Name	Action Group	Issuer	Interval	Distribute Over	Start T
	Distribute Hardware Tools	Distribute Hardware Tools	Default	administrator	Every 3 hours	1 hour	
	Distribute Core Content Tools [Windows]	Core Content - Tools [Windows]	Default	administrator	Every 1.5 hours	30 minutes	
	Distribute Core Content Tools [Mac]	Core Content - Tools [Mac]	Default	administrator	Every 1.5 hours	30 minutes	
	Distribute Core Content Tools [Linux]	Core Content - Tools [Linux]	Default	administrator	Every 1.5 hours	30 minutes	
	Distribute Application Management Tools	Distribute Application Management Tools	Default	administrator	Every 30 minutes	None	
	Distribute Tanium Standard Utilities (Mac)	Distribute Tanium Standard Utilities (Mac)	Default	administrator	Every 3 hours	1 hour	
	Distribute Tanium Standard Utilities (Linux)	Distribute Tanium Standard Utilities (Linux)	Default	administrator	Every 3 hours	1 hour	
	Distribute Tanium Standard Utilities	Distribute Tanium Standard Utilities	Default	administrator	Every 3 hours	1 hour	

- From the Main menu, go to **Administration** > **Content** > **Sensors** and search for client-related sensors.

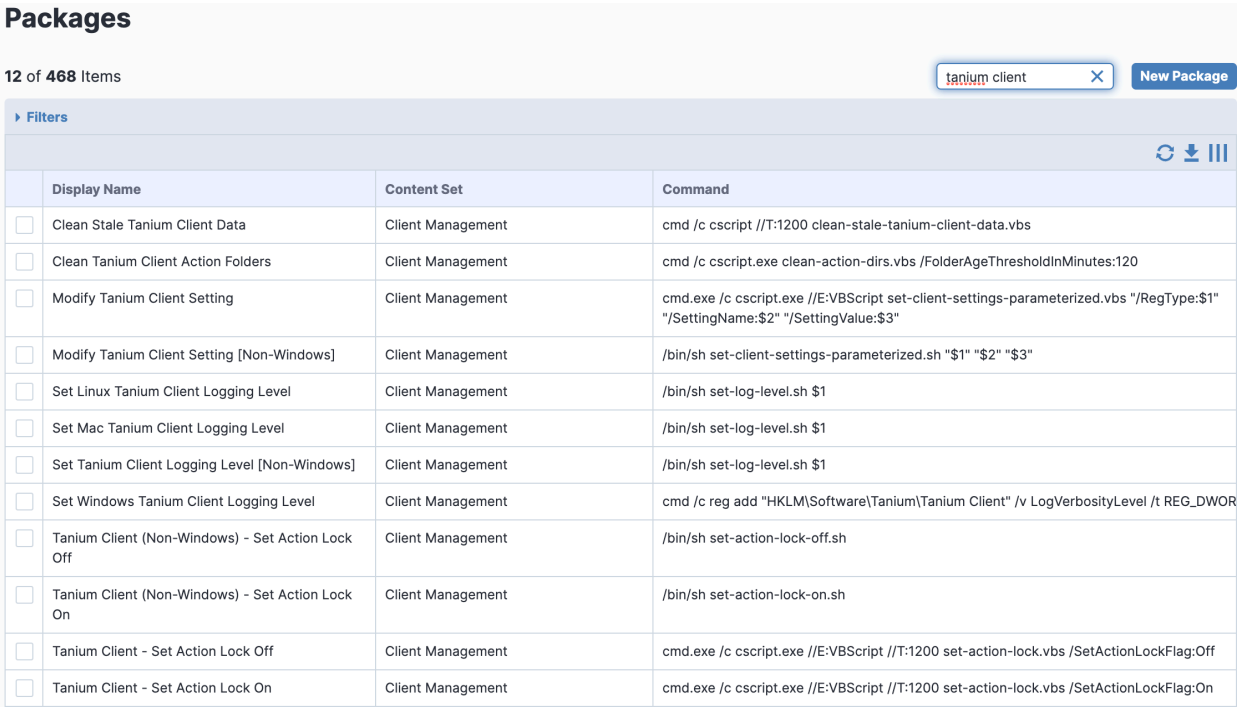
  Figure 21. Client-related sensors

©2026 Tanium Inc. All Rights Reserved



- From the Main menu, go to **Administration** > **Content** > **Packages** and search for client-related packages.

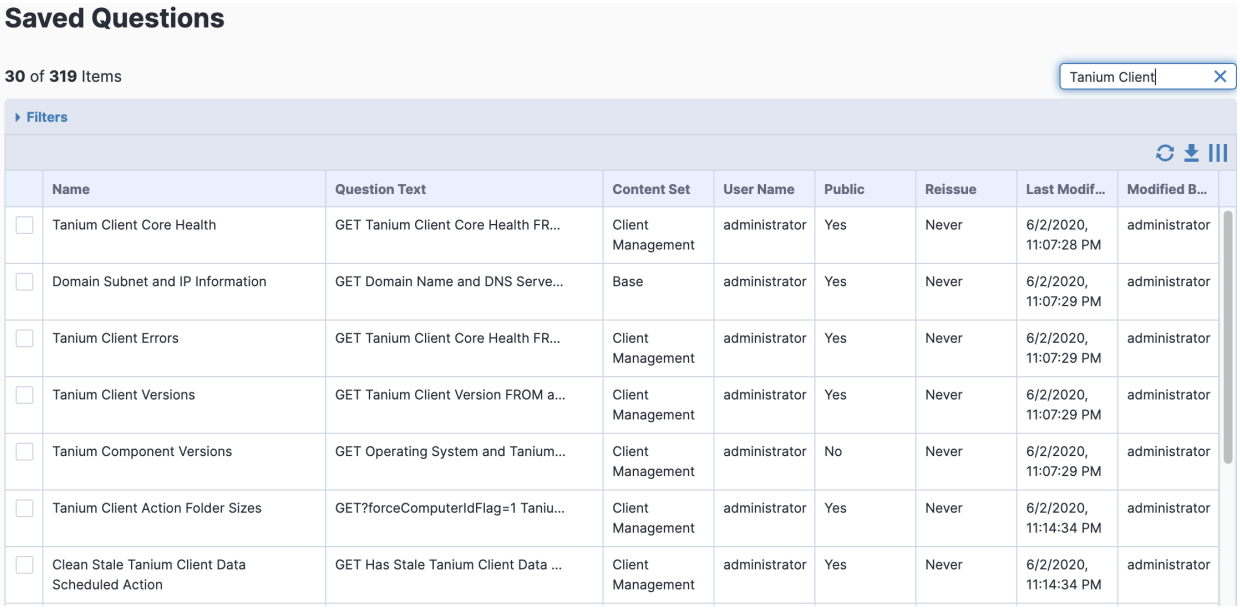
Figure 22. Client-related packages



- From the Main menu, go to **Administration** > **Content** > **Saved Questions** and search for client-related questions.

Figure 23. Client-related saved questions

©2026 Tanium Inc. All Rights Reserved



(Non-Windows only) Manage custom tags in the CustomTags.txt file

On non-Windows endpoints, you can add a file that contains custom tags to the Tanium Client installation directory to enable using the tags to identify the endpoint in Tanium workflows. For example, you could use the tag `Lab` to identify endpoints used in a testing lab. You could then ask a question that uses the `Custom Tags` sensor and specifies the `Lab` tag, or you could create a computer group that selects computers based on the tag.

Tip: You can use the Tanium packages named **Custom Tagging - Add Tags** and **Custom Tagging - Add Tags (Non-Windows)** to deploy tags at scale, including to Windows endpoints. For more information, see Manage custom tags for computer groups.

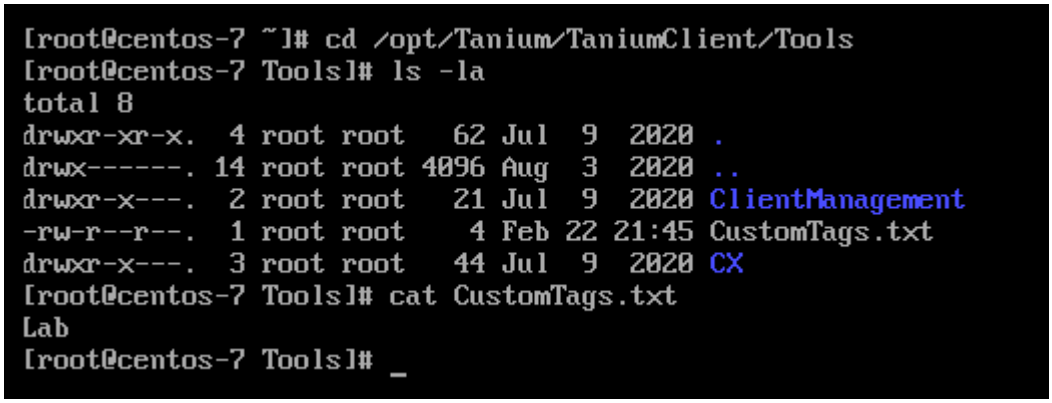
ADD TAGS TO THE CUSTOMTAGS.TXT FILE

1. Create a file named CustomTags.txt in the Tools subdirectory of the installation directory on page 490.
2. Open the file in a text editor and add tags as strings. Enter one string per line, and do not use spaces.
3. Save the file. A restart of the endpoint or Tanium Client service is not required.
   The following example shows a Tanium Client installation directory that includes a custom

©2026 Tanium Inc. All Rights Reserved

tag named `Lab`:

Figure 24. CustomTags.txt file in the Tanium Client Tools directory



EXAMPLE: USE CUSTOM TAGS TO CREATE A COMPUTER GROUP

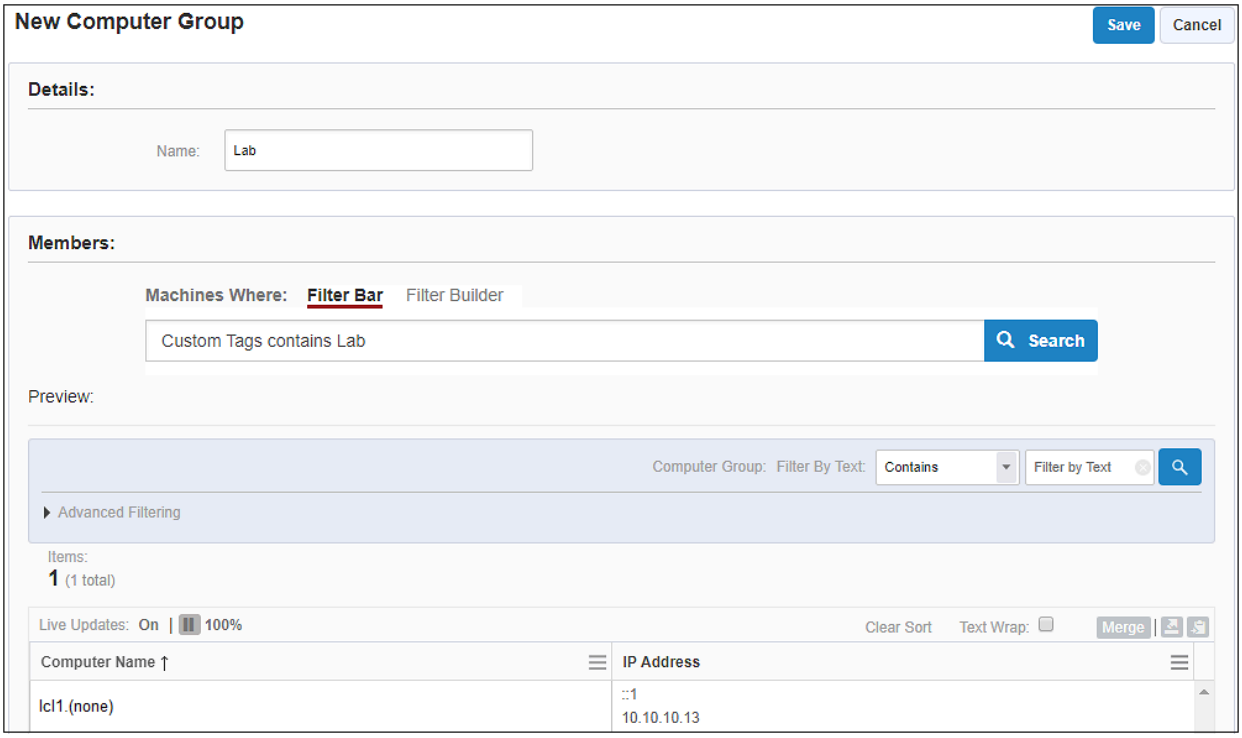
About this task

After you add custom tags, you can use them to create a computer group as follows.

1. From the Main menu, go to **Administration** > **Permissions** > **Computer Groups** and click **New Group**.
2. Enter a **Name** to identify the group.
   In the **Filter Bar**, use the **Custom Tags** sensor to define group membership, as shown in the figure Figure 25. Using custom tags to select a computer group on page 292.

   Figure 25. Using custom tags to select a computer group

©2026 Tanium Inc. All Rights Reserved



3. Save your changes.

Manage the Tanium Client on Windows

The Tanium Client is installed as a service with a **Startup Type** set to **Automatic** on Windows endpoints. The default installation directory is C:\Program Files (x86)\ for 64-bit versions of Windows, or C:\Program Files\ for 32-bit versions of Windows.

Related information

- Deploy the Tanium Client to Windows endpoints using the installer on page 155
- Preparing the Tanium Client on a Windows OS image on page 194
- Uninstall the Tanium Client on Windows on page 351
- Client version and operating system requirements on page 29
- Managing Client settings and Index configurations on page 318
- Tanium Client settings reference on page 393

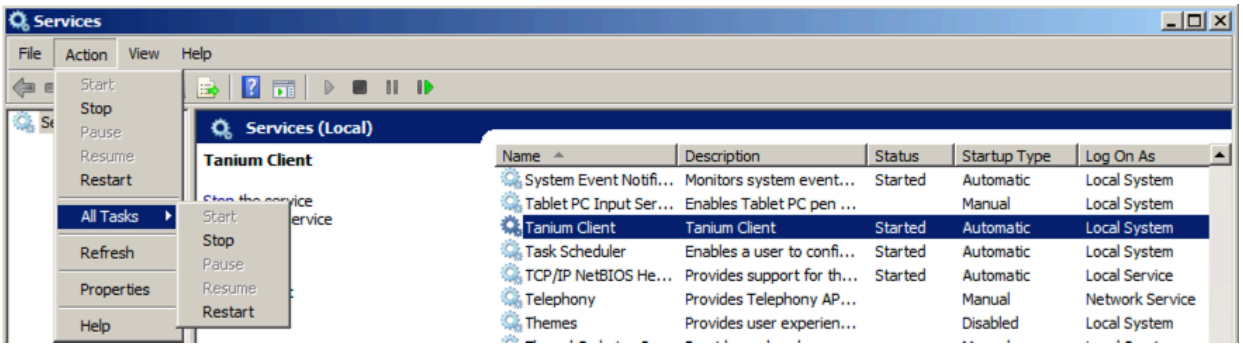
MANAGE THE TANIUM CLIENT SERVICE ON WINDOWS

About this task

Use the Windows **Services** application to stop, start, or restart the **Tanium Client** service on Windows endpoints:

©2026 Tanium Inc. All Rights Reserved

1. Click **Start** > **Run**. Type `services.msc` and click **OK**.
2. Select the **Tanium Client** service and then select an action in the **Action** > **All Tasks** menu.
   Figure 26. Tanium Client service



MANAGE TAMPER PROTECTION

The protocols that the Client uses to communicate with the Tanium Server and peer Clients are designed to be secure and prevent rogue sensors or actions, and digital signing prevents an attacker from causing the Client to run sensors or packages that the Tanium Server did not issue. However, the Tanium Client is a traditional Win32 application on Windows. By default, it appears in the Add/Remove Programs list, and users with local administrator rights can manage the service and access the Tanium Client installation directory.

The anti-tamper feature prevents end users from taking the following actions on Windows endpoints where it is enabled:

- Stopping or restarting the Tanium Client service
- Stopping Tanium Client processes
- Uninstalling the Tanium Client
- Tampering with Tanium Client files or registry entries

©2026 Tanium Inc. All Rights Reserved

Important:

The restriction on uninstalling the Tanium Client applies to all processes, not only to end users. When anti-tamper is enabled on an endpoint, you cannot reinstall the Tanium Client remotely (including through Client Management) even when using a system-level process. If you need to reinstall a Tanium Client on an endpoint where anti-tamper is enabled, you must first disable anti-tamper on that endpoint. For more information, see Disable the anti-tamper feature on an offline endpoint on page 298.

Additionally, when anti-tamper is enabled, Tanium processes cannot see certain registry locations that are not owned by Tanium. A query that targets one of these locations from a Tanium process returns an empty or "not found" result that looks the same as a key that does not exist.

This restriction applies only to the Tanium Client and the processes it starts, including TaniumScript, Python, PowerShell, cmd, and VBScript sensor and package hosts, and Client Extensions such as Comply, Threat Response, and Direct Connect. It does not affect other processes on the endpoint, such as Registry Editor, a PowerShell session that a user starts, or Windows Management Instrumentation (WMI).

Registry locations hidden from Tanium processes when anti-tamper is enabled

Registry location	Effect in a Tanium process
HKLM\SOFTWARE\Microsoft\AMSI\Providers and HKLM\SOFTWARE\WOW6432Node\Microsoft\AMSI\Providers	Enumerating subkeys returns no entries. However, you can open or read a provider subkey by its GUID name.
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\AppCertDlls	Enumerating values returns no entries. Reading a value directly fails with an access denied error.
The `AppInit_Dlls` value under HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows (and the equivalent WOW6432Node key)	Reading the value returns "not found". Other values in the key read normally.
The `Debugger` value under any HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\<executable> key	Reading the value returns "not found". A Tanium process also cannot open its own Image File Execution Options key.
The `DatabasePath` and `DatabaseType` values under HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\InstalledSDB	Reading the values returns "not found".
The `AutoRun` value under HKLM\SOFTWARE\Microsoft\Command Processor	Reading the value returns "not found" when the reader is cmd.exe (for example, a batch script sensor).

For example, the **Registry Key Subkeys** sensor returns "Key/Value not found" for HKLM\Software\Microsoft\AMSI\Providers on an endpoint that has anti-tamper enabled.

To enable the anti-tamper feature, configure an anti-tamper recovery password and then configure

©2026 Tanium Inc. All Rights Reserved

and deploy a Client settings configuration with the **Enable Anti-Tamper** setting selected. For more information, see Managing Client settings in Client Management on page 324.

Tip: This feature does not require the **Client Service Hardening** content pack to be installed.



Best Practice:

- Perform regular audits of unmanaged assets to look for and remediate systems with missing or non-functioning Clients, regardless of whether you have enabled the anti-tamper feature on Windows Clients. For more information, see Audit and remediate disconnected Tanium Clients on page 332.
- If you choose to harden the Tanium Client on Windows endpoints, use the anti-tamper feature instead of Client Service Hardening features where possible.

©2026 Tanium Inc. All Rights Reserved

Important:

- If you have used the features of the **Client Service Hardening** content pack to limit control of Tanium Client services, use the **Client Service Hardening - Set Service Permissions to Defaults** package to remove these restrictions before you enable the anti-tamper feature on those Clients. For more information, see Unharden the Tanium Client on Windows on page 302. The anti-tamper feature replaces the service permissions control of Client Service Hardening. Though leaving this restriction in place from Client Service Hardening does not affect the functionality of the anti-tamper feature, doing so can cause the service permissions to unexpectedly remain restricted if you disable anti-tamper.
- You can use the Client Service Hardening features to limit permission to view files in the Tanium Client directory and to hide the Tanium Client from the Windows Add/Remove Programs list in conjunction with the anti-tamper feature, but keep in mind that **Client Service Hardening** packages cannot function on an endpoint while the anti-tamper feature is enabled. Also, if you limit permissions on the Tanium Client directory to the LOCAL SYSTEM user account and you need to unlock a Tanium Client that is not connected to the Tanium Server, you must use the LOCAL SYSTEM user account to disable the anti-tamper feature.

Configure the anti-tamper recovery password

About this task

You can use the anti-tamper recovery password to unlock the anti-tamper feature on endpoints that are offline or where Tanium Client is otherwise unable to communicate with the Tanium Server.

Change the anti-tamper recovery password in Client Management.

1. From the Main menu, go to **Shared Services >** Client Management.
2. From the Client Management menu, go to **Configuration Management** > **Anti-Tamper Recovery**.
3. Click **Change Password**.
4. Enter and confirm the new password and then click **Save**.

©2026 Tanium Inc. All Rights Reserved

Important: After you change the password, the new password takes effect on endpoints only as you deploy or redeploy a Client settings configuration with the anti-tamper feature enabled to those endpoints. For more information, see Redeploy settings configurations to update the anti-tamper recovery password on endpoints on page 298. On any endpoints that last received the Client settings configuration before the password change, including endpoints that did not receive a Client settings deployment because they were offline, the previous password applies.

Redeploy settings configurations to update the anti-tamper recovery password on endpoints

About this task

After you change the anti-tamper recovery password, you must redeploy settings configurations that have the **Enable Anti-Tampering** setting selected to update the password on endpoints.

1. From the Main menu, go to **Shared Services >** Client Management.
2. From the Client Management menu, go to **Configuration Management** > **Settings Configurations**.
3. In the row for each settings configuration that has the **Enable Anti-Tampering** setting selected, click Actions ⋮ and select **Deploy**.

Disable the anti-tamper feature on an offline endpoint

About this task

If an endpoint that has the anti-tamper feature enabled is offline or is otherwise unable to communicate with the Tanium Server, you can unlock anti-tamper locally on the endpoint using the anti-tamper recovery password.

Best Practice: Use this method only on endpoints where the Tanium Client is unable to communicate with the Tanium Server. If the Tanium Client is connected, configure and deploy a Client settings configuration with **Enable Anti-Tampering** setting cleared. For more information, see Managing Client settings in Client Management on page 324. If you manually unlock an endpoint and it is later online and receives a settings configuration with the setting enabled, the deployed settings configuration re-enables anti-tamper on the endpoint.

©2026 Tanium Inc. All Rights Reserved

1. Retrieve the anti-tamper recovery password from Client Management:
    a. From the Main menu, go to **Shared Services >** Client Management.
    b. From the Client Management menu, go to **Configuration Management** > **Anti-Tamper Recovery**.
    c. Beside the **Recover Password**, click **Show** and take note of the displayed recovery password.

    Important: On any endpoints that last received the Client settings configuration before a password change, including endpoints that did not receive a Client settings deployment because they were offline, you must use the previously configured recovery password that was last deployed to the endpoint to unlock anti-tamper. To view a previous recovery password, click Show  beside an entry in the **Password History** section of the **Anti-Tamper Recovery** page.

2. At the command line on the endpoint that you want to unlock, enter the following command, using the recovery password you retrieved:
    - `%ProgramData%\Tanium\TaniumAntitamperUnlock.exe antitamper unlock [password]`

    The utility is installed in the %ProgramData%\Tanium folder, outside the Tanium Client directory, so it remains available if **Client Service Hardening** limits access to that directory.

    Tip: Including the password in the command is optional. If you omit the password, the command is interactive and prompts you to enter the password, which is masked during entry.

    Note: It might take up to 30 seconds to disable anti-tamper.

    Best Practice: Change the recovery password after you use it to unlock offline endpoints. For more information, see Configure the anti-tamper recovery password on page 297 and Redeploy settings configurations to update the anti-tamper recovery password on endpoints on page 298.

Determine whether anti-tamper is enabled on endpoints

©2026 Tanium Inc. All Rights Reserved

Ask a question using the **Tanium Driver Status** sensor to determine whether endpoints have anti-tamper enabled. The sensor returns `EnableAntiTamper: 1` to indicate that anti-tamper is enabled on an endpoint. For example:

```
Get Tanium Driver Status from all machines with Is Windows contains true
```

MANAGE CLIENT SERVICE HARDENING FEATURES

Certain client hardening features are provided by the **Client Service Hardening** content pack. Use the saved question dashboards in the **Client Service Hardening** content pack to review restrictions on user access to the Tanium Client on Windows endpoints. Deploy actions with the packages that are associated with the saved questions to adjust those restrictions. For more information about deploying packages, see Deploying actions.



Best Practice:

If you choose to harden the Tanium Client on Windows endpoints, use the anti-tamper feature instead of Client Service Hardening features where possible. The anti-tamper feature provides enhanced functionality with easier deployment and easier recovery of disconnected Tanium Clients. For more information, see Manage tamper protection on page 294. You can still use the **Client Service Hardening** content pack together with the anti-tamper feature if you need to restrict viewing the contents of the Tanium Client directory or to hide Tanium Client from the Add/Remove Programs list. The anti-tamper feature fully replaces the service permissions control feature of Client Service Hardening.



Best Practice: Perform regular audits of unmanaged assets to look for systems with missing or non-functioning Clients, regardless of whether you have hardened the Tanium Client on Windows. For more information, see Audit and remediate disconnected Tanium Clients on page 332.

Install the Client Service Hardening content pack

1. Sign in to Tanium Console as a user who is assigned the Administrator reserved role.

©2026 Tanium Inc. All Rights Reserved

2. From the Main menu, go to **Administration** > **Content** > **Solutions**.
3. In the **Content** section, select the **Client Service Hardening** row and click **Import Solution**.
4. Review the list of packages and sensors and click **Begin Import**.

Access the Client Service Hardening dashboards

About this task

The Client Service Hardening dashboards in Interact provide easy access to review and manage access restrictions for the Tanium Client.

1. From the Main menu, go to **Modules** > **Interact**.
2. In the **Categories** section, select **Client Service Hardening**.

Limit permission to start and stop Tanium Client services to the SYSTEM account

1. In the **Dashboards** section in Interact, click **Control Service State Permissions** to issue the dashboard question.
2. Select the **Service Control is set to default permissions** row and click **Deploy Action**.
3. For **Deployment Package**, select **Client Service Hardening - Allow Only Local SYSTEM to Control Service**.
4. Click **Show Preview To Continue**, review the list of targeted endpoints, and then click **Deploy Action**.

   Important: Remove this restriction before you enable the anti-tamper feature on Clients. For more information, see Unharden the Tanium Client on Windows on page 302 and Manage tamper protection on page 294. The anti-tamper feature replaces the service permissions control of Client Service Hardening. Though leaving this restriction in place from Client Service Hardening does not affect the functionality of the anti-tamper feature, doing so can cause the service permissions to unexpectedly remain restricted if you disable anti-tamper.

Limit permission to view or modify files in the Tanium Client directory to the SYSTEM account

1. In the **Dashboards** section in Interact, click **Set Client Directory Permissions** to issue the

©2026 Tanium Inc. All Rights Reserved

dashboard question.

2. Select the **Not Restricted** row, as well as any rows that indicate a restriction other than `NT AUTHORITY\SYSTEM` (such as `Restricted - BUILTIN\Administrators`) and click **Deploy Action**.
3. For **Deployment Package**, select **Client Service Hardening - Set SYSTEM only permissions on Tanium Client directory**.
4. Click **Show Preview To Continue**, review the list of targeted endpoints, and then click **Deploy Action**.

Hide the Tanium Client from the Windows Add/Remove Programs list

Hiding the Tanium Client from the Windows **Add/Remove Programs** list or the **Programs** menu does not affect the security of the Client. A user with permissions to uninstall an application can still launch the uninstallation manually. Hiding the Tanium Client from the **Add/Remove Programs** list helps to reduce accidental uninstallations and casual tampering by end users.

1. In the **Dashboards** section in Interact, click **Hide From Add-Remove Programs** to issue the dashboard question.
2. In the section for the **Tanium Client Visible in Add-Remove Programs** saved question, select the **No** row and click **Deploy Action**.
3. For **Deployment Package**, leave **Client Service Hardening - Hide Client from Add-Remove Programs** selected.
4. Click **Show Preview To Continue**, review the list of targeted endpoints, and then click **Deploy Action**.

Unharden the Tanium Client on Windows

Use Packages to unharden the Tanium Client

If an endpoint is communicating with your Tanium Server, you can unharden the Tanium Client using the following packages that correspond to each hardening package:

- **Client Service Hardening - Set Service Permissions to Defaults**
- **Client Service Hardening - Reset permissions on Tanium Client directory**

©2026 Tanium Inc. All Rights Reserved

- **Client Service Hardening - Show Client in Add-Remove Programs**

Tip: You can access these packages from the Client Service Hardening dashboards, similarly to the preceding steps provided for hardening.

Unharden Tanium Client that is not reporting to the Tanium Server

About this task

If an endpoint is not communicating with your Tanium Server, and you have limited permission for Tanium Client services or the Tanium Client directory to the LOCAL SYSTEM account, you must unharden the Tanium Client from the command line. You can use the PsExec command line utility to run packages as the LOCAL SYSTEM user account, which is not installed with Windows but is available as a download from Microsoft.

1. Download and install the PsExec command line utility from Microsoft.
2. From the Main menu in Tanium Console, go to **Administration** > **Content** > **Packages**.
3. Open the **Client Service Hardening - Reset permissions on Tanium Client directory** package.
4. In the **Files** section, click Download to download the reset_directory_permissions.vbs script file.
5. Return to the **Packages** page and open the **Client Service Hardening - Set Service Permissions to Defaults** package.
6. In the **Files** section, click Download to download the set-service-permissions-back-to-default.vbs script file.
7. Transfer both script files to a temporary location on the endpoint.
8. Open a command prompt as administrator on the endpoint, and run the following commands to unharden the Client:

```
psexec /accepteula /s cmd.exe cscript //E:VBScript //T:120
path_to_script\reset_directory_permissions.vbs

psexec /accepteula /s cmd.exe cscript //E:VBScript //T:120
```

©2026 Tanium Inc. All Rights Reserved

```
path_to_script\set-service-permissions-back-to-default.vbs
```

9. Delete the script files from the endpoint.
10. (Optional) To uninstall the Tanium Client, run the following command, replacing the path with the actual path to the Tanium Client if necessary:
    `C:\Program Files (x86)\Tanium\Tanium Client\uninst.exe /S`

ENCRYPT THE CLIENT STATE AND SENSOR QUERIES STORED ON THE CLIENT

About this task

Use the **StateProtectedFlag** Client setting to enable encryption of the Client state and sensor queries stored on the Client. This encryption is not required for the security of the Tanium Client, but it might be required for compliance with certain regulations. This setting does not require the Client Service Hardening content pack.

1. In Interact, ask a question to target the Windows endpoints on which you want to enable encryption: `Get Tanium Client Explicit Setting[StateProtectedFlag] from all machines with Is Windows contains true`
2. Select the endpoints from the results and click **Deploy Action**.
3. For **Deployment Package**, select **Modify Tanium Client Setting** and configure the following settings:
    - For **RegType**, select **REG_DWORD**.
    - For **ValueName**, enter `StateProtectedFlag`.
    - For **ValueData**, enter `1`.
4. Click **Show Preview To Continue**, review the list of targeted endpoints, and then click **Deploy Action**.

©2026 Tanium Inc. All Rights Reserved

Tip:

- Alternatively, you can use the command line on an endpoint to configure the **StateProtectedFlag** Client setting. For more information, see Reference: Tanium Client settings and CLI on page 393.
- You can modify the default value for this setting for endpoints where the setting is not configured. For more information, see Modify default Client settings in Tanium Console on page 323.
- To disable this encryption, either remove the **StateProtectedFlag** Client setting, or set it to `0`.

Manage the Tanium Client on macOS

The Tanium Client is installed as a system service on macOS endpoints. The Client files are located in the /Library/Tanium/TaniumClient directory.

Related information

- Deploy the Tanium Client to macOS endpoints using the installer on page 165
- Preparing the Tanium Client on a macOS image on page 197
- Uninstall the Tanium Client on macOS on page 352
- Client version and operating system requirements on page 29
- Managing Client settings and Index configurations on page 318
- Tanium Client settings reference on page 393

MANAGE MACOS FIREWALL RULES

The Tanium Client service is signed to automatically allow communication through the default macOS firewall. The Client installation process does not modify any host-based firewall that might be in use. A network security administrator must ensure that host and network firewalls are configured to allow inbound and outbound TCP traffic on the ports that the Client uses for Tanium traffic (default 17472).

©2026 Tanium Inc. All Rights Reserved

Note: For more information about port and firewall requirements for the Tanium Client, see Network connectivity, ports, and firewalls on page 63.

Firewall commands for macOS

Tasks	Commands
View port 17472 status	`sudo /usr/libexec/ApplicationFirewall/socketfilterfw --listapps | awk \ '/TaniumClient/ {getline; print $0}'`
Add Tanium Client to firewall	`sudo /usr/libexec/ApplicationFirewall/socketfilterfw --add \ /Library/Tanium/TaniumClient/TaniumClient`
Unblock Tanium Client in firewall	`sudo /usr/libexec/ApplicationFirewall/socketfilterfw --unblockapp \ /Library/Tanium/TaniumClient/TaniumClient`
Remove Tanium Client from firewall	`sudo /usr/libexec/ApplicationFirewall/socketfilterfw --remove \ /Library/Tanium/TaniumClient/TaniumClient`
Block Tanium Client in firewall	`sudo /usr/libexec/ApplicationFirewall/socketfilterfw --blockapp \ /Library/Tanium/TaniumClient/TaniumClient`

MANAGE POP-UPS FOR TANIUM CLIENT UPGRADES

When you upgrade the Tanium Client on endpoints that have a firewall enabled on macOS 10.14 (Mojave) or later, end users might see a pop-up prompting them to allow connections for the Tanium Client. To prevent the pop-up, either configure a firewall rule (best practice) or configure the **System Settings** on the endpoints. You can perform this task for multiple endpoints by configuring a policy or profile through a User Approved Mobile Device Management (UAMDM) tool. Contact Tanium Support on page 392 if you need help ensuring that an environment is ready before the Tanium Client upgrade.

Best Practice: For increased security, configuring a firewall rule to prevent the connections pop-up is preferable to configuring the **System Settings**. However, only endpoints running macOS 10.14.4 or later support this method.

©2026 Tanium Inc. All Rights Reserved

Configure an MDM policy or profile for multiple endpoints

About this task

When you configure a firewall rule or **System Settings** through a policy or profile, the specific steps depend on your UAMDM. Contact Tanium Support on page 392 for the procedure. The general steps are as follows:

1. Create the policy or profile.
2. Add a firewall or security setting to the policy or profile.
3. Add com.tanium.taniumclient.plist to the allowed connections.

   Note: Users cannot see that the Tanium Client is allowed in the firewall unless you provide those users access to the Tanium Client installation directory on page 490.

Configure a firewall rule on a single endpoint

About this task

You require read-only access to the /Library/Tanium/TaniumClient directory to perform this task.

1. On the macOS endpoint, go to **System Settings** > **Network** > **Firewall**.
2. If necessary, click Unlock, enter administrator credentials, and click **Unlock**.
3. Add a firewall rule: Click **Options**, click Add **+**, navigate to the /Library/Tanium/TaniumClient/ directory, select **taniumclient**, and click **Add**.
4. Click **OK** to apply the rule.

Configure the System Settings on a single endpoint

About this task

All endpoints that run macOS 10.14.x or later support configuring System Settings to prevent the connections pop-up.

1. On the macOS endpoint, go to **System Settings** > **Network** > **Firewall**.
2. If necessary, click Unlock, enter administrator credentials, and click **Unlock**.

©2026 Tanium Inc. All Rights Reserved

3. Click **Options**, select **Automatically allow downloaded signed software to receive incoming connections**, and click **OK**.

MANAGE THE TANIUM CLIENT SERVICE ON MACOS

On the macOS endpoint, open **Terminal** and use the listed launchctl commands to complete the following actions:

- Start the Tanium Client service:

  ```
  sudo launchctl load /Library/LaunchDaemons/
  com.tanium.taniumclient.plist
  ```

- Stop the Tanium Client service:

  ```
  sudo launchctl unload /Library/LaunchDaemons/
  com.tanium.taniumclient.plist
  ```

- Remove the Tanium Client from the launch list:

  ```
  sudo launchctl remove com.tanium.taniumclient
  ```

Manage the Tanium Client on Linux

The Tanium Client is installed as a system service on Linux endpoints. The default installation directory for Tanium Client files is /opt/Tanium/TaniumClient.

Related information

- Deploy the Tanium Client to Linux endpoints using package files on page 173
- Preparing the Tanium Client on a Linux OS image on page 200
- Uninstall the Tanium Client on Linux on page 354
- Client version and operating system requirements on page 29
- Managing Client settings and Index configurations on page 318
- Tanium Client settings reference on page 393

MANAGE LINUX FIREWALL RULES

The installation process does not modify any host-based firewall that might be in use. A network security administrator must ensure that host and network firewalls are configured to allow inbound

©2026 Tanium Inc. All Rights Reserved

and outbound TCP traffic on the ports that the Client uses for Tanium traffic (default 17472).

> **Note:** For more information about port and firewall requirements for the Tanium Client, see Network connectivity, ports, and firewalls on page 63.

The following subsections list example commands for managing Linux firewalls based on default distributions of Linux.

- Amazon Linux on page 309
- Debian on page 309
- CentOS, AlmaLinux, Rocky Linux, Oracle Linux, Red Hat Linux on page 309
- OpenSUSE and SLES on page 311
- Ubuntu on page 313

Amazon Linux

By default, the iptables utility for managing the firewall is not configured on Amazon Linux AMI (2016.09, 2017.09, 2018.3) or Amazon Linux 2 LTS. To add, remove, deny, or view the status of ports that the Tanium Client uses, check your Amazon Web Services (AWS) security group instead.

Debian

By default, the iptables utility for managing the firewall is not configured on Debian 6.x, 7.x, 8.x, or 9.x.

CentOS, AlmaLinux, Rocky Linux, Oracle Linux, Red Hat Linux

Version 7.x or later

The following table lists the commands for managing firewall rules for versions 7.x or later of CentOS, Oracle Linux, or Red Hat Linux, or version 8.x or later of AlmaLinux or Rocky Linux:

©2026 Tanium Inc. All Rights Reserved

Firewall commands for CentOS, Oracle Linux, or Red Hat Linux 7.x or later; AlmaLinux or Rocky Linux 8.x or later

Tasks	Commands
View rules for port 17472	`sudo firewall-cmd --list-all-zones | grep 17472`

Add or allow port 17472	1. List the zones.
	`sudo firewall-cmd --list-all-zones`
	2. For each relevant `<zone_name>` (such as `default` and where `ssh` is present), run:
	`sudo firewall-cmd --permanent --zone=<zone_name> --add-port=17472/tcp`
	3. Restart the firewall.
	`sudo systemctl restart firewalld`

Remove or deny port 17472	1. List the zones.
	`sudo firewall-cmd --list-all-zones`
	2. For each relevant `<zone_name>` where port 17472 is present, run:
	`sudo firewall-cmd --permanent --zone=<zone_name> --remove-port=17472/tcp`
	3. Restart the firewall.
	`sudo systemctl restart firewalld`

Versions 5.x and 6.x

The following table lists the commands for managing firewall rules for versions 5.x and 6.x of CentOS, Oracle Linux, and Red Hat Linux.



Note: The iptables command is for IPv4. For IPv6, use the ip6tables command.

Firewall commands for CentOS, Oracle Linux, Red Hat Linux 5.x and 6.x

Tasks	Commands
Check the firewall	`iptables -L -n --line-numbers | egrep -i "^Chain|REJECT *all"`

©2026 Tanium Inc. All Rights Reserved

Tasks	Commands
status	The firewall is enabled when a `REJECT *all` rule is present.
View rules for port 17472	`sudo iptables -L -n | grep 17472`

Add or allow port 17472	1. Check the firewall status.
	`sudo iptables -L -n --line-numbers | egrep -i "^Chain|REJECT *all"`
	2. For each `<chain_name>` with a `REJECT all` rule, run the following command, where `<line>` is the line number of the rule.
	`sudo iptables -I <chain_name> <line> -p tcp -m state --state NEW \ --dport 17472 -j ACCEPT`
	For example, if the chain is `RH-Firewall-1-INPUT` and the `REJECT all` rule is on line 10, run:
	`sudo iptables -I RH-Firewall-1-INPUT 10 -p tcp -m state --state NEW \ --dport 17472 -j ACCEPT`
	3. Save your changes and restart the iptables service.
	`sudo service iptables save`
	`sudo service iptables restart`

Remove or deny port 17472	1. List the chains.
	`sudo iptables -L -n | egrep -i "^Chain|17472"`
	2. For each `<chain_name>`, run:
	`sudo iptables -D <chain_name> -p tcp -m state --state NEW --dport 17472 -j ACCEPT`
	3. Save your changes and restart the iptables service.
	`sudo service iptables save`
	`sudo service iptables restart`

OpenSUSE and SLES

Version 15.x

The following table lists the commands for managing firewall rules for versions 15.x of OpenSUSE

©2026 Tanium Inc. All Rights Reserved

and SUSE Linux Enterprise Server (SLES):

Firewall commands for OpenSUSE and SLES 15.x

Tasks	Commands
View rules for port 17472	`sudo firewall-cmd --list-all-zones | grep 17472`

Add or allow port 17472	1. List the zones.
	`sudo firewall-cmd --list-all-zones`
	2. For each relevant `<zone_name>` (such as `default` and where `ssh` is present), run:
	`sudo firewall-cmd --permanent --zone=<zone_name> --add-port=17472/tcp`
	3. Restart the firewall.
	`sudo systemctl restart firewalld`

Remove or deny port 17472	1. List the zones.
	`sudo firewall-cmd --list-all-zones`
	2. For each relevant `<zone_name>` where port 17472 is present, run:
	`sudo firewall-cmd --permanent --zone=<zone_name> --remove-port=17472/tcp`
	3. Restart the firewall.
	`sudo systemctl restart firewalld`

Version 11.x and 12.X

The following table lists the commands for managing firewall rules for versions 11.x and 12.x of OpenSUSE and SUSE Linux Enterprise Server (SLES):

Firewall commands for OpenSUSE and SLES 11.x and 12.x

Tasks	Commands
View rules for port 17472	`sudo grep "FW_SERVICES_EXT_TCP=" /etc/sysconfig/SuSEfirewall2 | egrep "[ \"]17472[ \"]"`
Add or allow port	1. Open the /etc/sysconfig/SuSEfirewall2 file for editing, add port 17472 to the line

©2026 Tanium Inc. All Rights Reserved

Tasks	Commands
17472	`FW_SERVICES_EXT_TCP=`, and save your changes. 2. Restart the firewall. `sudo SuSEfirewall2 start`
Remove or deny port 17472	1. Open the /etc/sysconfig/SuSEfirewall2 file for editing, remove port 17472 from the line `FW_SERVICES_EXT_TCP=`, and save your changes. 2. Restart the firewall. `sudo SuSEfirewall2 start`

Ubuntu

The following table lists the commands for managing firewall rules for Ubuntu:

Firewall commands for Ubuntu

Tasks	Commands

View port 17472 status	`sudo ufw status | grep 17472`
	or
	`sudo iptables -L -n | grep 17472`

Allow port 17472	`sudo ufw allow 17472/tcp`
Remove port 17472	`sudo ufw delete allow 17472/tcp`
Deny port 17472	`sudo ufw deny 17472/tcp`

MANAGE THE TANIUM CLIENT SERVICE ON LINUX

Linux service commands vary according to Linux distribution. This documentation provides examples but is not a reference for each Linux distribution. If you are not already familiar with installing and managing services on your target Linux distribution, review the documentation for the particular Linux operating system before you begin.

©2026 Tanium Inc. All Rights Reserved

Tanium Client service commands by Linux distribution

Linux distributions and versions	Typical commands

Versions that use the systemd daemon (all distributions)
• Amazon Linux (all supported versions)
• Debian (all supported versions)
• Oracle Linux (version 7 and later)
• Red Hat / CentOS (version 7 and later)
• AlmaLinux / Rocky Linux (all supported versions)
• SUSE / OpenSUSE (version 12 and later)
• Ubuntu (version 16 and later)
	`systemctl start taniumclient`
	`systemctl stop taniumclient`
	`systemctl status taniumclient`

Versions that use the init daemon (Debian-based distributions)
• Ubuntu (version 14)
	`service taniumclient start`
	`service taniumclient stop`
	`service taniumClient status`

Versions that use the init daemon (RPM-based distributions)
• Oracle Linux (versions 5, 6)
• Red Hat / CentOS (versions 5, 6)
• SUSE / OpenSUSE (versions 11.3, 11.4)
	`service TaniumClient start`
	`service TaniumClient stop`
	`service TaniumClient status`

MOVE AN EXISTING INSTALLATION OF THE TANIUM CLIENT ON LINUX

About this task

The Tanium Client must store data in the default installation directory on page 490. For this reason, in some environments, the size of the /opt/Tanium directory might exceed the space allowed within the /opt directory. If there is not enough space in the default directory, use a symbolic link to move the Client and data to another directory.

1. Sign in to the endpoint using an account that has administrative privileges, or that is listed in the sudoers file to allow the account you are using to use sudo.
2. Stop the Tanium Client service. For more information, see Manage the Tanium Client service on Linux on page 313.
3. Move the Tanium Client to a new directory. For example, to move the Tanium Client from the

©2026 Tanium Inc. All Rights Reserved

default installation directory to the /appbin/Tanium directory, run the following command:

```
mv /opt/Tanium /appbin
```



Important: The new directory must be located on a local fixed drive.

4. Create a symbolic link. For example, if you want to use the directory /appbin/Tanium, run the following command:

```
ln -s /appbin/Tanium /opt/Tanium
```

5. Start the Tanium Client service. For more information, see Manage the Tanium Client service on Linux on page 313.

Manage the Tanium Client on Solaris

The Tanium Client is installed as a system service on Solaris endpoints. The Tanium Client files are installed by default in the /opt/Tanium/TaniumClient directory.

Related information

- Deploy the Tanium Client to Solaris endpoints using a package file on page 181
- Preparing the Tanium Client on a Solaris OS image on page 203
- Uninstall the Tanium Client on Solaris on page 355
- Client version and operating system requirements on page 29
- Managing Client settings and Index configurations on page 318
- Tanium Client settings reference on page 393

MANAGE THE TANIUM CLIENT SERVICE ON SOLARIS

To run svcadm commands, you must sign in to the endpoint as the root user or as a user who can use the sudo utility to run commands with root permissions.

Run the listed commands to complete the following actions:

- Start the Tanium Client service: `svcadm enable taniumclient`
- Stop the Tanium Client service: `svcadm disable taniumclient`
- Restart the Tanium Client service: `svcadm restart taniumclient`

©2026 Tanium Inc. All Rights Reserved

- Display the status of the Tanium Client service: `svcs taniumclient`

MOVE AN EXISTING INSTALLATION OF THE TANIUM CLIENT ON SOLARIS

About this task

The Tanium Client must store data in the default installation directory on page 490. For this reason, in some environments, the size of the /opt/Tanium directory might exceed the space allowed within the /opt directory. If there is not enough space in the default directory, use a symbolic link to move the Client and data to another directory.

1. Sign in to the endpoint using an account that has administrative privileges, or that is listed in the sudoers file to allow the account you are using to use sudo.
2. Use the following command to stop the Tanium Client service:

   ```
   svcadm disable taniumclient
   ```

3. Move the Tanium Client to a new directory. For example, to move the Tanium Client from the default installation directory to the /appbin/Tanium directory, run the following command:

   ```
   mv /opt/Tanium /appbin
   ```

   Important: The new directory must be located on a local fixed drive.

4. Create a symbolic link, and set the `PKG_NONABI_SYMLINKS` environment variable to `true`. For example, if you want to use the directory /appbin/Tanium, run the following command:

   ```
   ln -s /appbin/Tanium /opt/Tanium
   PKG_NONABI_SYMLINKS=true
   export PKG_NONABI_SYMLINKS
   ```

5. Use the following command to start the Tanium Client service:

   ```
   svcadm enable taniumclient
   ```

Manage the Tanium Client on AIX

The Tanium Client is installed as a system service on AIX endpoints. The default installation directory for Tanium Client files is /opt/Tanium/TaniumClient.

©2026 Tanium Inc. All Rights Reserved

Related information

- Deploy the Tanium Client to AIX endpoints using a package file on page 188
- Preparing the Tanium Client on an AIX OS image on page 206
- Uninstall the Tanium Client on AIX on page 355
- Client version and operating system requirements on page 29
- Managing Client settings and Index configurations on page 318
- Tanium Client settings reference on page 393

MANAGE THE TANIUM CLIENT SERVICE ON AIX

The Tanium Client on AIX uses the IBM AIX System Resource Controller (SRC) to manage the Client service:

- Start the Tanium Client service: `startsrc -s taniumclient`
- Stop the Tanium Client service: `stopsrc -s taniumclient`
- Verify that the Tanium Client service is available: `lssrc -s taniumclient`

MOVE AN EXISTING INSTALLATION OF THE TANIUM CLIENT ON AIX

About this task

The Tanium Client must store data in the default installation directory on page 490. For this reason, in some environments, the size of the /opt/Tanium directory might exceed the space allowed within the /opt directory. If there is not enough space in the default directory, use a symbolic link to move the Client and data to another directory.

1. Sign in to the endpoint using an account that has administrative privileges, or that is listed in the sudoers file to allow the account you are using to use sudo.
2. Use the following command to stop the Tanium Client service:

   ```
   stopsrc -s taniumclient
   ```

3. Move the Tanium Client to a new directory. For example, to move the Tanium Client from the default installation directory to the /appbin/Tanium directory, run the following command:

   ```
   mv /opt/Tanium /appbin
   ```

©2026 Tanium Inc. All Rights Reserved

> **Important:** The new directory must be located on a local fixed drive.

4. Create a symbolic link. For example, if you want to use the directory /appbin/Tanium, run the following command:

```
ln -s /appbin/Tanium /opt/Tanium
```

5. Use the following command to start the Tanium Client service:

```
startsrc -s taniumclient
```

Managing Client settings and Index configurations

Tanium Client settings are stored in Windows registry on page 491 settings on Windows endpoints, or in an SQLite database on non-Windows endpoints.

> **Best Practice:** Do not edit Tanium Client keys and values in the Windows registry. Use one of the methods in Modify Client settings on page 320 to configure Client settings.

For the list of Client settings that you can review or configure, see Tanium Client settings reference on page 393.

You can also use Tanium Client Management to manage Tanium Index configurations, including exclusions and blockout window.

Review Client settings

Use any of the methods in this section to review Client settings. A setting that has not been configured on a Client uses the default value that is configured in Tanium Console (see Modify default Client settings in Tanium Console on page 323), or if no value is configured in Tanium Console, the default that is listed in the Tanium Client settings reference on page 393 applies.

CLIENT HEALTH VIEW

Use the Client Health view in the Client Management service to review a summary of Client settings that are configured across endpoints or detailed Client settings on individual endpoints.

©2026 Tanium Inc. All Rights Reserved

Summary view

About this task

Use the main Client Health view to review a summary of Client settings that have been changed from their defaults on some endpoints and the count of endpoints on which each setting has been changed.

1. From the Main menu, go to **Shared Services** > **Client Management**.
2. Go to **Client Health**.
3. Click the **Settings** tab.
4. (Optional) Select a **Computer Group** to filter the summary information.

Detail view

About this task

Connect directly to an endpoint to view each Client setting that has been configured for that endpoint.

1. In the **Single Endpoint View** search box in the Client Health view, enter all or part of an IP address or a computer name.
   Matching results are displayed after the search completes.
2. From the search results, click the computer name.
   Client Management opens the Endpoint Details page in Single Endpoint View (SEV).
3. Click the **Client Health** tab and, if the endpoint is not yet **Connected**, click **Direct Connect**.
   Scroll down to view Client settings for the endpoint.

TANIUM CLIENT EXPLICIT SETTING SENSOR

Ask a question using the `Tanium Client Explicit Setting` sensor to review Client settings on endpoints. For example, the following question returns the **LogVerbosityLevel** setting for endpoints that have a computer name that includes `Lab`:

```
Get Tanium Client Explicit Setting[LogVerbosityLevel] from all machines with Computer Name
contains Lab
```

©2026 Tanium Inc. All Rights Reserved

For more information about working with question results, see Managing question results.

COMMAND LINE INTERFACE (CLI)

Use the CLI to review Client settings locally on an individual endpoint or to retrieve Client settings in a script.

- **Windows:** `TaniumClient config get <SettingName>`
- **Non-Windows:** `sudo ./TaniumClient config get <SettingName>`

For detailed information about using the CLI, see Tanium Client command line interface (CLI) on page 413.

Modify Client settings

Use any of the methods in this section to modify Client settings as necessary.

For the list of Client settings that you can configure, see Tanium Client settings reference on page 393. A setting that has not been configured on a Client uses the default value that is configured in Tanium Console (see Modify default Client settings in Tanium Console on page 323), or if no value is configured in Tanium Console, the default that is listed in the reference applies.

SETTINGS CONFIGURATIONS IN CLIENT MANAGEMENT

For certain Client settings (including all VDI-related settings on page 407, and the specific settings noted in the Tanium Client settings reference on page 393), you can use the Client Management service to create settings configurations that apply those settings to different groups of Clients. For more information and the steps to create Client settings configurations, see Managing Client settings in Client Management on page 324.

PACKAGES

About this task

Deploy the **Modify Tanium Client Setting** or **Modify Tanium Client Setting [Non-Windows]** package to configure a Client setting on all targeted endpoints. Because Windows and non-Windows endpoints require separate packages to update settings, repeat the steps for both types of endpoints.

©2026 Tanium Inc. All Rights Reserved

1. In Interact, ask a question to target the Windows endpoints on which you want to modify a Client setting.
2. Select the endpoints to target and click **Deploy Action**.

   Tip: You can drill-down or merge questions to refine the results before selecting endpoints. For more information, see Managing question results.

3. For **Deployment Package**, select one of the following packages:
   - **Modify Tanium Client Setting** for Windows endpoints
   - **Modify Tanium Client Setting [Non-Windows]**
4. Configure the following settings:
   - (Windows only) For **RegType**, select the Windows registry value type that is listed in the Tanium Client settings reference on page 393 for the setting that you want to modify.
   - (Non-Windows only) For **Type**, select the non-Windows setting type that is listed in the Tanium Client settings reference on page 393 for the setting that you want to modify.
   - For **ValueName**, enter the name of the setting that you want to modify, as listed in the Tanium Client settings reference on page 393.
   - For **ValueData**, enter the value to configure for the setting on targeted endpoints.

©2026 Tanium Inc. All Rights Reserved

Tip:

For the following frequently used settings, you can use specific packages that let you enter only the value to configure.

- LogVerbosityLevel: Use the **Set Windows Tanium Client Logging Level** or **Set Tanium Client Logging Level [Non-Windows]** package.
- ServerName: Use the **Set Tanium Server Name** or **Set Tanium Server Name [Non-Windows]** package.
- ServerNameList: Use the **Set Tanium Server Name List** or **Set Tanium Server Name List [Non-Windows]** package.

5. (Optional) In the **Deployment Schedule** section, configure a schedule for the action.

   Best Practice: If some target endpoints might be offline when you initially deploy the action, select **Recurring Deployment** and set a reissue interval.

6. In the **Targeting Criteria** section, make sure that the settings target only endpoints that meet the following criteria:
   - The targeted endpoints require the updated setting.
   - The targeted endpoints run an operating system that matches the selected package (Windows or non-Windows).

7. Click **Show Preview To Continue**, review the list of targeted endpoints, and then click **Deploy Action**.

   Important: Clients do not apply the updated setting until you manually restart them or wait for the automatic Client reset, which by default is a random interval in the range of 2 to 6 hours.

8. (Optional) Restart the Tanium Client service on each endpoint to apply the updated setting immediately:
   - Manage the Tanium Client service on Windows on page 293
   - Manage the Tanium Client service on macOS on page 308

©2026 Tanium Inc. All Rights Reserved

- Manage the Tanium Client service on Linux on page 313
- Manage the Tanium Client service on Solaris on page 315
- Manage the Tanium Client service on AIX on page 317

9. Review the setting on the targeted Clients to verify that it has been correctly updated. For more information, see Review Client settings on page 318.

COMMAND LINE INTERFACE (CLI)

Use the CLI to configure Client settings locally on an individual endpoint or from a script.

- **Windows:** `TaniumClient config set <SettingName> <Value>`
- **Non-Windows:** `sudo ./TaniumClient config set <SettingName> <Value>`

For detailed information about using the CLI, see Tanium Client command line interface (CLI) on page 413.

DEPLOYMENT WITH CLIENT MANAGEMENT

You can configure specific Client settings for newly installed Clients during deployment with Client Management. For more information, see Deploying the Tanium Client using Client Management on page 125.

Modify default Client settings in Tanium Console

About this task

Many Client settings have a default value that applies when the setting is not configured on a Client, as listed in the Tanium Client settings reference on page 393. You can modify the default value for a Client setting in the advanced settings in Tanium Console. This default applies to any managed endpoint that does not have the setting explicitly configured locally.

1. From the Main menu, go to **Administration** > **Configuration** > **Settings** > **Advanced Settings** and click the **Client** tab.
2. Edit or add a setting as necessary:
   - If the setting for which you want to configure a default appears in the list, click the

©2026 Tanium Inc. All Rights Reserved

name of the setting, enter a new **Value**, and click **Save**.

- If the setting for which you want to configure a default does not appear in the list, click **Add Setting**, configure the following properties, and click **Save**:
    - For **Setting Type**, select **Client**.
    - For **Platform Setting Name**, enter the name of the setting from the Tanium Client settings reference on page 393.
    - For **Value Type**, select **Text** for a setting that lists "REG_SZ" as the registry value type or "STRING" as the setting type, or select **Numeric** for a setting that lists "REG_DWORD" as the registry value type or "NUMERIC" as the setting type.
    - For **Value**, enter the value to use as the default for the Client setting.

Managing Client settings in Client Management

Use the Client Management service to manage Client settings to different groups of Clients.

CREATE AND DEPLOY A CLIENT SETTINGS CONFIGURATION

About this task

Create a settings configuration to configure general Client settings for a group of Clients.

1. From the Main menu, go to **Shared Services >** Client Management.
2. Go to **Configuration Management** > **Settings Configurations** and click **Create Settings Configuration**.

   Tip: To edit an existing settings configuration, click the name of the configuration, and click **Edit**. When you edit a configuration, you must manually redeploy it.
3. Enter a **Name** for the profile configuration.
4. Click **Select Computer Groups**, select the computer groups where you want the settings configuration to apply, and click **Save**.

©2026 Tanium Inc. All Rights Reserved

5. Configure the following general Client settings.

General Tanium Client settings in Client Management

Setting Name	Description
Cache Size	The size limit, in MB, for the file cache on an endpoint. The default is `2048`. For more information, see Chunk caching on page 27.
Logging Level	The level of logging on an endpoint. The following values are best practices for specific scenarios: • `1` (default): Use this value during normal operation. • `41`: Use this value during troubleshooting. • `91` or higher: Use this value for full logging, for short periods of time only. **Note:** A value of `0` disables logging. As a best practice, do not disable logging.
Extensions Logging Level	The level of logging for Client Extensions (such as the Tanium™ Client Recorder Extension and Tanium™ Index) on an endpoint. The following values are best practices for specific scenarios: • `11` (default): Use this value during normal operation. • `41`: Use this value during troubleshooting. • `91` or higher: Use this value for full logging, for short periods of time only. **Note:** A value of `0` disables logging. As a best practice, do not disable logging.

6. If you are creating a settings configuration that applies to virtual desktop infrastructure (VDI) endpoints, select **Enable VDI Settings**, and configure the following VDI settings. Configuring these settings on individual endpoints overrides the values configured in Platform Settings (**Administration** > **Configuration** > **Settings** > **Advanced Settings**) and can reduce resource use on VDI endpoints when you set the best practice values for VDI. For more information about tuning settings for VDI endpoints, see Tuning Tanium Client settings for VDI endpoints and other endpoints with limited resources on page 407.

©2026 Tanium Inc. All Rights Reserved

Client Setting	Default Value	Best Practice Value for VDI	Explanation
RandomSensorDelayInSeconds	0	5	By default, sensors run immediately. This setting delays the execution of any sensor by a random time up to 5 seconds, which reduces concurrent execution of sensors and packages. **Note:** If poor performance occurs on VDI infrastructure, you can increase this value incrementally up to `20`.
MaxAgeMultiplier	1	2	Each sensor has a **Max Sensor Age** setting that determines how long the Client caches sensor results for subsequent questions that include the same sensor. This setting causes the Client to multiply the maximum age configured for each sensor by 2, which doubles the time results are cached for each sensor and reduces sensor executions.
MinDistributeOverTimeInSeconds	0	60	Each action has a **Distribute Over** setting that randomizes the distribution of that action over the specified time. By default, no minimum applies, and some actions might be configured for immediate distribution. This setting forces all actions to distribute over at least 1 minute.
SaveClientStateIntervalInSeconds	300	1800	By default, the Client state is written to disk every 5 minutes. This setting increases the time to 30 minutes to reduce disk writes.

7. To prevent end users from stopping the Tanium Client service or tampering with Tanium Client files or registry entries on Windows endpoints, select **Enable Anti-Tamper**.

©2026 Tanium Inc. All Rights Reserved

Note:

- To enable this setting, you must have configured an anti-tamper recovery password in Client Management. For the steps, see Configure the anti-tamper recovery password on page 297.
- For general information about using tamper protection, see Manage tamper protection on page 294.
- This feature requires Tanium Client 7.6.4.2033 or later. If you enable this setting, only endpoints with Tanium Client 7.6.4.2033 or later will be targeted by this settings configuration.

8. Click **Save**.
9. To deploy the settings configuration to the selected computer groups, click Actions in the row for the configuration, and select **Deploy**.

PRIORITIZE CLIENT SETTINGS CONFIGURATIONS

About this task

The order of the configurations in the Settings Configurations list determines the priority of each configuration. If multiple configurations target an endpoint, the configuration with the highest priority takes effect on the endpoint. You can reorder the list to adjust the priority of each configuration.

1. From the Main menu, go to **Shared Services >** Client Management.
2. Go to **Configuration Management** > **Settings Configurations**, and click **Prioritize**.
3. Drag the configurations in the list to reorder them according to priority, and then click **Prioritize**.

Managing Index configurations in Client Management

Create an Index configuration to configure Index exclusions, the maximum Index database size, and blockout windows for a group of endpoints.

An Index exclusion keeps files and paths that match a regular expression out of file system indexes on

©2026 Tanium Inc. All Rights Reserved

endpoints. Excluding unnecessary files from indexing can reduce resource use. For example, consider creating an exclusion if you have an application that writes to a temp file. With an exclusion, the temp file is not indexed and hashed every time it changes.

An Index blockout window prevents Index from indexing and hashing during certain times when endpoints are normally in use, to reduce resource use.

For more information about Index, see Tanium Client Index Extension User Guide.

Important: Index exclusions that you define in Client Management apply globally to all Tanium solutions that use Index, such as Integrity Monitor, Reveal, and Threat Response. Exclusions that you add in other solutions are not visible in Client Management; make sure to view the exclusions in each solution to understand the full list of exclusions that apply for that solution. Furthermore, exclusions defined in Threat Response also apply globally. To remove a global exclusion, it must not remain in either an Index configuration in Client Management or Index exclusions in Threat Response.

Note: Exclusions prevent Index from including any indicated files in the Index database. However, Index still reads the metadata of excluded files in some situations, such as when the file exists within a high priority path.

CREATE INDEX EXCLUSIONS

About this task

First, create a set of Index exclusions that can be reused across multiple Index configurations.

1. From the Main menu, go to **Shared Services >** Client Management.
2. Go to **Configuration Management** > **Index Exclusions** and click **Create Index Exclusion**.
3. Enter a **Name** for the exclusion.
4. Select the **Operating System** where the exclusion applies.
5. Enter a **Regular Expression** that identifies the files or paths to be excluded.
   For example, to exclude the Windows paging file, swap file, and hibernation file, enter the following regular expression:

©2026 Tanium Inc. All Rights Reserved

```
\\(pagefile|swapfile|hiberfil)\.sys
```

> **Important:**
> The case sensitivity of Index exclusions depends on the operating system of the endpoint:
>
> - **Windows and macOS:** Index exclusions are case-insensitive.
> - **Linux, AIX, and Solaris:** Index exclusions are case-sensitive.

6. Click **Save**.

(OPTIONAL) IMPORT OR EXPORT INDEX EXCLUSIONS

You can export and then import Index exclusions in JSON format to share or move them between Tanium environments.

Export Index exclusions

1. From the Main menu, go to **Shared Services >** Client Management.
2. Go to **Configuration Management** > **Index Exclusions**.
3. To export all exclusions, click **Export All**, or select specific exclusions and click **Actions** > **Export**.

Import Index exclusions

1. From the Main menu, go to **Shared Services >** Client Management.
2. Go to **Configuration Management** > **Index Exclusions** and click **Import**.
3. Click **Select Index Exclusions JSON file** and use the file dialog to select a JSON file that contains exported Index exclusions.
4. Click **Upload**.

CREATE AN INDEX CONFIGURATION

1. From the Main menu, go to **Shared Services >** Client Management.

©2026 Tanium Inc. All Rights Reserved

2. Go to **Configuration Management** > **Index Configurations** and click **Create Index Configuration**.

   Tip: To edit an existing settings configuration, click the name of the configuration, and click **Edit**. When you edit a configuration, you must manually redeploy it.

3. Enter a **Name** for the profile configuration.
4. Click **Select Computer Groups**, select the computer groups where you want the settings configuration to apply, and click **Save**.
5. Configure any settings that you want to apply to the configuration:
   - To configure a maximum database size that applies to each endpoint, select **Max Index Database Size** and configure a maximum size.

     If you have enabled a maximum database size and the Index database on an endpoint reaches the configured size, Index stops indexing and hashing files on that endpoint. This condition appears in TPAN reports.

     Best Practice: Though this setting provides a fail-safe to avoid filling the storage on an endpoint if unexpected files cause the database to grow quickly, use exclusions as much as possible to avoid indexing temporary files and other unnecessary files.

   - In the **Index and Hashing Blockout Windows** section, configure the times during which you don't want to index and hash files on endpoints.
     - Select how the configured times apply on each endpoint:
       - **Local Endpoint Time:** The configured times apply to each endpoint based on the local time configured on that endpoint. The configured windows occur according to each time zone.
       - **UTC:** The configured times represent Coordinated Universal Time (UTC). The configured windows occur at the same time on all endpoints according to UTC and regardless of time zones.
     - Configure the days and times for blockout windows:

©2026 Tanium Inc. All Rights Reserved

- (Optional) Click **Add Business Hours** to add the typical business hours, which you can then edit.
- Click **Add Custom Window** to configure days and times for a blockout window.

> **Note:** Blockout windows cannot span midnight in a single window. To create a blockout window that spans midnight (for example, 10:00 PM to 4:00 AM), create two separate windows: one from 10:00 PM to 11:59 PM and one from 12:00 AM to 4:00 AM. Index treats 11:59 PM (23:59) as midnight (00:00), so the two windows are contiguous with no gap.

- To apply Index exclusions, click **Select Exclusions**, select the exclusions to apply to this configuration, and click **Confirm**.

6. Click **Save**.
7. To deploy the Index configuration to the selected computer groups, click Actions in the row for the configuration, and select **Deploy**.

PRIORITIZE INDEX CONFIGURATIONS

About this task

The order of the configurations in the Index Configurations list determines the priority of each configuration. If multiple configurations target an endpoint, the configuration with the highest priority takes effect on the endpoint. You can reorder the list to adjust the priority of each configuration.

1. From the Main menu, go to **Shared Services >** Client Management.
2. Go to **Configuration Management** > **Index Configurations**, and click **Prioritize**.
3. Drag the configurations in the list to reorder them according to priority, and then click **Prioritize**.

Maintaining Tanium Clients

Perform regular maintenance tasks to ensure that Tanium Clients are connected in good health, so

©2026 Tanium Inc. All Rights Reserved

that Tanium successfully performs scheduled activities on all the targeted endpoints and does not overuse endpoint or network resources. If Tanium Clients are not performing as expected, you might need to troubleshoot issues or change settings. For related procedures, see Troubleshooting Tanium Clients and Client Management on page 356.

For information about general management of Tanium Clients, see Managing Tanium Clients on page 288.

Configure automated maintenance

AUDIT AND REMEDIATE DISCONNECTED TANIUM CLIENTS

About this task

In some cases, users with local administrative rights might be able to uninstall the Tanium Client, stop the Tanium Client service, or tamper with Tanium Client files. Use Tanium Discover to regularly audit endpoints to which you have deployed the Tanium Client, and automatically redeploy the Tanium Client to previously managed endpoints that have become unmanaged.

1. Configure a profile in Discover that scans endpoints to which you have deployed the Tanium Client. For more information, see Scan types.
2. Configure an automatic label in Discover (such as `Disconnected`) with conditions that identify endpoints on which you expect the Tanium Client to be installed. For more information, see Automatically label interfaces.

   Note:

   Discover labels must have the following settings to be used with Client Management:

   - **Type**: Automatic
   - **Activity**: Retain
   - **Retain Activity**: Label
3. (Optional) Configure a Connect destination to alert you of newly unmanaged endpoints that the label identifies. For more information, see Export interface data to a Connect destination.
4. Configure a recurring deployment in Client Management that targets the Discover label you

©2026 Tanium Inc. All Rights Reserved

created. For more information, see Deploying the Tanium Client using Client Management on page 125.

Note: If redeploying the Tanium Client is unsuccessful or does not successfully reconnect the endpoint, other issues might be preventing the Tanium Client from connecting or registering. For troubleshooting information, see Troubleshoot issues with connection and registration on page 357.

Tip: To reduce the likelihood of casual tampering by users with local administrator rights on Windows, you can take measures to harden the Tanium Client on Windows. For more information, see Manage Client Service Hardening features on page 300. Performing regular audits of unmanaged assets is a best practice regardless of whether you have hardened the Tanium Client on Windows.

Perform weekly maintenance

CHECK THE ENDPOINT LEADER PERCENTAGE

About this task

In linear chains of Tanium Clients, minimizing the percentage of endpoints that function as leaders helps to reduce bandwidth usage in communications with Tanium Servers and Tanium™ Zone Servers. The leader percentage varies among networks and no specific percentage is ideal for all networks. However, unexpected changes in the percentage might indicate network issues that your networking team must address. For example, a sharp increase in the percentage might cause excessive wide area network (WAN) traffic. Therefore, monitor changes in the leader percentage over time by recording the percentage at weekly intervals.

Note: For more information about leaders, linear chains, and how the Servers evaluate subnet boundaries, see Client peering.

1. Configure the TPAN report if it is not already configured. For more information, see Configuring Health Check.
2. Open the latest TPAN report and select the **Tuning** page.

©2026 Tanium Inc. All Rights Reserved

3. Check the value of **What's the actual or anticipated leader count percentage?** Typically, this value does not change significantly unless your network changes in ways that affect the number and size of Client subnets.

4. If the leader percentage changes more than expected, investigate the possible causes. The percentage might change if:
    - Subnets join or leave your network. Check the endpoint count on page 334 to see if the number of managed endpoints has changed. If the change is due to new subnets, verify that they are authorized to join your network. If the change is due to subnets no longer registering with Tanium Servers or Tanium Zone Servers, verify whether network disruptions or misconfigurations are responsible.

    - A shift occurs between the number of users who are connecting within your internal network and the number who are connecting through virtual private network (VPN) connections. Typically, VPN endpoints do not peer with each other and therefore each one is effectively a leader. For more information, see Configure isolated subnets.

5. Contact Tanium Support on page 392 for help optimizing the leader count, if necessary.

CHECK THE ENDPOINT COUNT

About this task

The number of managed endpoints might fluctuate as endpoints join or leave your network. View the number of managed endpoints to check for potential anomalies and track changes in the weekly count to project future growth. Contact Tanium Support on page 392 to update your license for a higher number of maximum managed endpoints if necessary.

1. Sign in to Tanium Console with a user account that has **Unrestricted Management Rights** for computer groups. The **Administrator** reserved role provides those management rights and you can also switch to a persona that has them.

2. Go to the Tanium **Home** page to check the **Total Endpoints**. This field displays the most accurate tally of online and offline managed endpoints that have registered with the Tanium Server or Zone Server within the retention period (default is 30 days). For more information, see View environment status.

3. Perform one of the following steps if the endpoint count is:
    - Lower than expected: Investigate whether network disruptions or misconfigurations

©2026 Tanium Inc. All Rights Reserved

prevent endpoints from registering.

- Higher than expected: Verify that the new endpoints are authorized to join your network.

Tip: You can configure an automatic Discover label and a Connect destination to alert you when endpoints become unmanaged. For more information, see Audit and remediate disconnected Tanium Clients.

REVIEW AND UPDATE TAGS

If you use computer groups for which membership is based on custom tags or enhanced tags, review which endpoints have which tags. Deploy changes to the tags and configure new computer groups if necessary.

Review and update enhanced tags

For information about reviewing and updating enhanced tags, sign in to the Tanium™ Knowledge Base and see the Enhanced Tags Documentation.

Review and update custom tags

1. Determine which endpoints have which tags. For more information, see Review custom tags.
2. Add or remove custom tags if necessary. For more information, see Manage computer group membership through custom tags.
3. Create or delete computer groups with tag-based membership if necessary. For more information, see Managing computer groups.

   Note: You cannot change the membership definition of existing computer groups. You must delete existing groups and recreate them with the correct definition.
4. Add or edit action groups to target tag-based computer groups if necessary. For more information, see Managing action groups.

Perform monthly maintenance

©2026 Tanium Inc. All Rights Reserved

Perform the following tasks to review the state of the Tanium Clients running on endpoints, as well as Client communication and registration with Tanium Servers and Zone Servers. If you observe Client issues that require resolution, see Troubleshooting Tanium Clients and Client Management on page 356.

REVIEW AND REMEDIATE TANIUM CLIENT HEALTH AND CLIENT EXTENSION ISSUES

About this task

Perform the following tasks to review the state of the Tanium Clients running on endpoints, as well as Client communication and registration with Tanium Servers and Zone Servers. If you observe Client issues that require resolution, see Troubleshooting Tanium Clients and Client Management.

1. From the Main menu, go to **Shared Services** > **Client Management**.
2. Go to **Client Health** and click the **Deployment** tab to review the **Health Failures** panel. This panel shows failures associated with Tanium™ Client Extensions. Perform the remaining steps if you need to troubleshoot Client Extension issues.
3. Click Interact in the **Health Failures** panel to display the question results that provide the panel data.
4. Retrieve any additional details from endpoints that you need to diagnose Client Extension issues. For more information, see Managing question results.
5. To resolve Client Extension failures, see the following sections:
    - To resolve Client Index Extension failures, see Reference: Common health check issues.
    - To resolve Client Recorder Extension failures, see Troubleshooting the Client Recorder Extension.
    - To resolve failures associated with Client Extensions for other Tanium solutions, see Troubleshoot solution-specific issues and Identify and resolve issues with endpoint tools or Client Extensions.

REVIEW AND ADJUST THE DISTRIBUTION OF TANIUM CLIENT REGISTRATION TRAFFIC

About this task

Tanium Clients must register with a Tanium Server or Zone Server for the Client hosts to function as managed endpoints. As Clients and Client subnets are added to or removed from your network, you

©2026 Tanium Inc. All Rights Reserved

might have to update client-server connections to optimize registration traffic.

Each Tanium Client connects to only one Tanium Server or Zone Server at a time. However, to avoid a single point of failure, you can configure the **ServerNameList** setting with a list of servers to which the Client can attempt a connection.



Note: For more information about client-server connections, see Configuring connections to the Tanium Core Platform.

To determine which servers are processing Client registrations and, if necessary, to rebalance registration traffic among them:

1. From the Main menu, go to **Shared Services** > **Client Management**.
2. Go to **Client Health** and click the **Settings** tab.
3. Review the **ServerNameList** setting to determine whether Clients are connecting to the correct servers.
4. Review the **ServerName** setting to verify that Client connections are balanced among Zone Servers.
5. Deploy actions with packages that reset the **ServerNameList** settings if necessary to connect Clients to different Servers. For more information, see Content for configuring connections to Tanium Core Platform Servers.
6. Add Zone Servers if necessary to rebalance Client registration traffic and then repeat step 5 to connect Clients to those Servers. For more information, see the procedure for your Tanium infrastructure:
    - Installing an Appliance Array: Review the tasks for adding Array members and assigning roles.
    - Installing the Tanium Zone Server

REVIEW AND UPDATE TANIUM CLIENT LOGGING LEVELS

About this task

Tanium Clients generate logs that can help you troubleshoot issues. Higher logging levels record more details about events on Clients but also consume more Client resources. The default logging

©2026 Tanium Inc. All Rights Reserved

level is `1`. Review Client logging levels and adjust them if necessary to ensure new endpoints that join your network have optimal logging levels.

Best Practice: Make sure to keep the logging level at `1` to minimize disk writes on Clients that run on sensitive endpoints, endpoints with limited resources, or virtual desktop infrastructure (VDI) endpoints.

Note: For more information about logging levels, see Tanium Appliance User Guide: Reviewing logs and troubleshooting Tanium Core Platform or Tanium Core Platform User Guide for Windows Deployments: Reviewing logs and troubleshooting Tanium Core Platform.

For Tanium™ Client Containers, the default logging level is `10` and you cannot change it through actions. Contact Tanium Support on page 392 to change the logging level on Client Containers.

For more information about logs on Tanium Clients, see Troubleshooting Tanium Clients and Client Management.

1. From the Main menu, go to **Shared Services** > **Client Management**.
2. Go to **Client Health** and click the **Settings** tab.
   If the logging level is set to a value other than the default `1` on any Clients, the **LogVerbosityLevel** setting displays the **Count** of Clients for each value. If all Clients have the default value, the page does not display the setting.

   Tip: To verify that the logging level is set to the best practice value of `1` for Clients on VDI endpoints, select **All Virtual Machines** in the **Computer Group** drop-down.
3. To update the logging level on Clients, see Managing Client settings and configurations in Client Management.

REVIEW AND UPDATE TANIUM CLIENT SETTINGS

1. From the Main menu, go to **Shared Services** > **Client Management**.

©2026 Tanium Inc. All Rights Reserved

2. Go to **Client Health** and click the **Settings** tab.
3. Verify that the setting values are correct and that the **Count** column indicates they apply to the expected number of Clients.
4. To update settings, see Managing Client settings and configurations in Client Management.

REVIEW AND UPGRADE TANIUM CLIENT VERSIONS

About this task

The best practice is to run the latest Tanium Client version on all endpoints, and to maintain a supported configuration, you must install at least the version of the Tanium Client that matches the endpoint toolset installed on an endpoint. However, you might occasionally have earlier Client versions installed to temporarily support legacy configurations. Endpoints might also run an earlier Client version if an upgrade process failed.

Note: For more information about Client versions, see Client version and host system requirements.

Best Practice: Enable Client upgrades in the change management feature in Endpoint Configuration to streamline Client upgrades and to more easily maintain a supported configuration. For more information, see Endpoint Configuration: Managing Tanium Client and endpoint tool upgrade rollouts.

Determine which endpoints are running a Client that is not at the latest version and decide whether to accept the earlier versions or upgrade the Clients:

1. From the Main menu, go to **Shared Services** > **Client Management**.
2. Review the **Health** dashboard to see the **Client Version** panel.
3. If any endpoints are running an earlier Client version, click the **Client Version** title and then click Interact in the **Client Version** panel to display the question results that provide the panel data.
4. Retrieve any details from endpoints that you need to determine whether the versions are appropriate, or upgrades are required, or upgrades failed.

©2026 Tanium Inc. All Rights Reserved

For example, select a **Filter by Computer Group** option (such as **All Windows**) or update the question as needed. For information about retrieving additional details, see Managing question results.

Tip: You can use the `Upgrade Ring` field in the `Endpoint Configuration - Change Management Status` sensor to filter endpoints according to the earliest upgrade ring with which they are associated. For example, ask the question: `Get OS Platform and Client Health - Tanium Client Version from all machines with Endpoint Configuration - Change Management Status:Upgrade Ring contains 4`.

5. Upgrade the Client on any endpoints that require the latest version. For more information, see Upgrading Tanium Clients.
6. Troubleshoot Client upgrade issues if necessary. For more information, see Troubleshooting Tanium Clients and Client Management.

REVIEW AND UPDATE TANIUM CLIENT SUBNETS

Separated subnets, intentional subnets, and isolated subnets provide methods for modifying the default peering behavior of Tanium Clients. Default peering settings define the boundaries of Client subnets in the Tanium linear chain architecture. As subnets are added to or removed from your network, you might have to update the Client subnet configurations. For example, add isolated subnets for any new virtual private networks (VPNs).



Note: For more information about Client peering and subnets, see Configuring Tanium Client peering.

Review and update isolated subnets

About this task

Configure isolated subnets for Tanium Clients that are in VPNs. VPN Clients have local IP addresses in a special VPN address block, but their host endpoints are actually not close to each other. If VPN Clients are not isolated, they use WAN links for peering and latency is significantly greater than for

©2026 Tanium Inc. All Rights Reserved

client-to-server connections.

1. From the Main menu, go to **Administration** > **Configuration** > **Subnets** and review the **Isolated Subnets**. If necessary, consult your networking team to determine if the configurations require updates.
2. Update isolated subnet configurations if necessary. For more information, see Configure isolated subnets.

Review and update separated subnets

About this task

Configure separated subnet configurations to apply more granular subnet boundaries for Tanium linear chains than the default boundaries.

1. From the Main menu, go to **Administration** > **Configuration** > **Subnets** and review the **Separated Subnets**. If necessary, consult your networking team to determine if the configurations require updates.
2. Update separated subnet configurations if necessary. For more information, see Configure separated subnets.

Review and update intentional subnets

About this task

In a network configuration that uses network address translation (NAT), you might have to configure intentional subnets to ensure that Clients in the same subnet can peer with each other.

1. From the Main menu, go to **Administration** > **Configuration** > **Client Status**.
   The **Network Location (from Client)** values indicate which Clients are in the same subnet based on the **AddressMask** setting. For more information, see Address mask and prefix settings.

   The **Network Location (from Server)** column indicates the NAT IP addresses of Clients.
2. Select the endpoints that are in the same subnet but are not peering because their NAT IP addresses differ.
3. Click Export, set the **Format** to **List of Clients - CSV**, and click **Export**.

©2026 Tanium Inc. All Rights Reserved

4. From the Main menu, go to **Administration** > **Configuration** > **Subnets** and compare the **Intentional Subnets** configurations to the exported list of Clients.
5. Update the intentional subnet configurations if necessary to enable peering among Clients in the same subnets. For more information, see Configure intentional subnets.

Upgrading Tanium Clients

The following procedures describe how to upgrade the Tanium Client to a newer version on managed endpoints.

©2026 Tanium Inc. All Rights Reserved

Important:

- Each version of the endpoint toolset that is deployed through Endpoint Configuration includes a specific version of the Tanium Client, which Tanium recommends that you install with the toolset. It is a best practice to upgrade the Tanium Client on endpoints using the change management feature. To do so, you must enable Tanium Client upgrades in the upgrade ring configuration. For more information about the endpoint toolset and managing Tanium Client upgrades with toolset deployment, see Tanium Endpoint Configuration User Guide: Managing Tanium Client and endpoint tool upgrade rollouts. If you do not enable this setting, you can upgrade to the required version of the Tanium Client on endpoints using Client Management or other means.

- If you have Tanium Client 7.2 installed on endpoints in an upgraded environment, you cannot upgrade Tanium Client 7.2 directly to version 7.6 or later. To upgrade an endpoint with version 7.2 installed to version 7.6 or later, you must either perform a reinstallation of the Tanium Client that includes wiping Client data on page 138, or perform an intermediate upgrade to version 7.4, after which you can upgrade to the latest version. You can use Upgrade Tanium Clients using Client Management on page 346 or a package on page 349 to perform the intermediate upgrade, but keep in mind that you cannot use Client Management to install a version earlier than 7.4.7.1094. Perform this upgrade before upgrading Tanium Core Platform to the 2025H1 or later semiannual release. For information about to caching a 7.4 version of the Tanium Client for an intermediate upgrade, see Manage versions of the Tanium Client available for legacy deployments on page 115. For the specific versions of Tanium Client supported on each operating system, see Client version and operating system requirements on page 29.

- If you are upgrading a legacy environment from a version of Tanium Client earlier than 7.2.314.3608 on macOS endpoints, this version and later has a different code signing requirement from earlier versions. If you are creating a Privacy Preferences Policy Control (PPPC) custom payload, see Prepare for deployment to Linux, macOS, Solaris, or AIX endpoints on page 129 (for deployment with Client Management) or Deploy the Tanium Client to macOS endpoints using the installer on page 165.

Best practices

Review the following best practices before upgrading Tanium Clients:

©2026 Tanium Inc. All Rights Reserved

- Enable Client upgrades in the change management feature in Endpoint Configuration to streamline Client upgrades and to more easily maintain a supported configuration. For more information, see Endpoint Configuration: Managing Tanium Client and endpoint tool upgrade rollouts. If upgrading Clients in the change management feature is not yet feasible in your environment, upgrade using Client Management as described in Upgrade Tanium Clients using Client Management on page 346, instead of using third-party software. In cases where third-party software is necessary, see the documentation for that software.

- Upgrade without uninstalling and reinstalling Tanium Clients. If you uninstall Clients, you lose any custom data that is associated with them.

- Test the upgrade process in a lab environment that resembles the production environment as closely as possible. For example, use a lab environment that has similar Tanium Client versions, operating systems (OSs), and deployed Tanium module tools.

- Deploy the upgrade in stages.

    - Start with non-essential endpoints.

    - Deploy the upgrade to one OS type at a time.

    - Deploy the upgrade in batches to prevent unforeseen issues from affecting too many endpoints simultaneously.

  Tip: The change management feature of Endpoint Configuration provides an easy method to upgrade Clients in such stages. For more information, see Endpoint Configuration: Managing Tanium Client and endpoint tool upgrade rollouts.

- Plan for temporary peering disruption during the upgrade. Because Tanium Clients peer only with other Clients on the same minor version, the number of forward and backward leaders and WAN bandwidth consumption can temporarily increase. To minimize the impact, complete upgrades as quickly as possible within each subnet and avoid leaving mixed minor versions in the same subnet for an extended period. For more information, see Tanium Client version compatibility for peering on page 25.

- Tanium recommends the universal binary on all Mac computers running macOS 11 or later, and replacing the x86-64 binary if it is already installed. The universal binary is supported and runs natively on both Intel-based Mac computers running macOS 11 or later and Apple

©2026 Tanium Inc. All Rights Reserved

"M" series-based Mac computers. However, you cannot upgrade an existing installation of the x86-64 version of the Tanium Client directly to the Universal version. You must first uninstall the existing Tanium Client on page 352 or perform a reinstallation that includes wiping data with Tanium Client Management on page 138. If you upgrade the x86-64 Client in Client Management on page 346 or allow the change management feature in Endpoint Configuration to upgrade the Client, it installs a newer version of the x86-64 Client.

- After upgrading all version 7.2 Tanium Clients in your environment to version 7.6.2 or later, disable the legacy version of the Tanium Protocol used only for 7.2 and earlier clients (v314). For more information, see Disable the legacy Tanium Protocol used only for 7.2 and earlier clients on page 350.

Before you begin

- Read the release notes for the target version of Tanium Client, as well as all earlier versions that were released since the currently installed version, to understand the enhancements, bug fixes, and known issues that those versions include.

- Verify that the required security exclusions are in place on your endpoints, including any exclusions that were added for newer Tanium Client versions. Review the release notes for the target version and Reference: Endpoint security exclusions on page 416 for new or changed exclusions.

- Verify that your endpoints are running a supported endpoint toolset version. For more information about managing endpoint toolset versions, see Endpoint Configuration: Managing Tanium Client and endpoint tool upgrade rollouts.

- If you deploy upgrades to endpoints that have a firewall enabled on macOS 10.14 (Mojave) or later, perform the steps under Manage pop-ups for Tanium Client upgrades on page 306.

- **macOS:** If you previously created a Privacy Preferences Policy Control (PPPC) custom payload for a legacy environment with a version of the Tanium Client earlier than 7.2.314.3608 and you are upgrading to a new version of Tanium Client, you must update the code signing requirement. For more information about creating a PPPC custom payload, see Prepare for deployment to Linux, macOS, Solaris, or AIX endpoints on page 129 (for deployment with Client Management) or Deploy the Tanium Client to macOS endpoints using the installer on page 165.

©2026 Tanium Inc. All Rights Reserved

Assess the impact of upgrading on your environment

About this task

To help plan the stages of the upgrade to minimize the impact on your environment, determine the scope of the upgrade and appropriate groups of endpoints to target:

1. Ask the following question, where `<target_client_version>` is the version to which you are upgrading:
   `Get Tanium Client Version from all machines with Tanium Client Version < <target_client_version>`

   The question results indicate the number of endpoints that require upgrades.

2. If you want to evaluate the impact on specific types of endpoints (such as critical servers), you can apply a drill-down question such as `Operating System` or `Organizational Unit` (see Drill down into results).

Enable Tanium Client upgrades in change management

The best-practice upgrade method is to enable Client upgrades in the change management feature in Endpoint Configuration. This mechanism enables you to streamline Client upgrades and to more easily maintain a supported configuration. For more information, see Endpoint Configuration: Managing Tanium Client and endpoint tool upgrade rollouts.

Upgrade Tanium Clients using Client Management

Client Management handles upgrades to the Tanium Client on endpoints that have earlier versions installed. A Client upgrade targets specific computer groups and upgrades any endpoints in those groups to the specified version as the endpoints become available. You can create a one-time upgrade to upgrade Clients within a specified window of time, or you can create an ongoing upgrade to keep Clients upgraded to the latest version of the Tanium Client or to upgrade Clients that are later added to the targeted group to a selected version.

©2026 Tanium Inc. All Rights Reserved

Tip: When you use the change management feature in Endpoint Configuration to manage Client upgrades, Endpoint Configuration automatically creates and uses Client upgrades in Client Management.

By default, Client upgrades of either type use recurring scheduled actions that have an expiration period of twenty minutes and re-issue time of every hour. This configuration allows even a one-time upgrade to upgrade endpoints that might not be online when deployment of the upgrade starts but that you expect to be online at some point during the window of time defined for the upgrade.

Note: Client Management cannot upgrade endpoints with action locks turned on. For more information, see Managing action locks.

Tip: If you imported Client Management on Tanium Core Platform 7.6 or later with automatic configuration, a Client upgrade named `TCM CMI x.y Client Upgrade` was created to automatically upgrade all endpoints in the `All Computers` computer group to the latest version of the Tanium Client. You can modify this Client upgrade as desired.

CREATE A CLIENT UPGRADE

Before you begin

Important: Before you create an upgrade, make sure that the Tanium Server has cached the versions of the Tanium Client that you need. For more information, see Manage versions of the Tanium Client available for legacy deployments on page 115.

1. From the Main menu, go to **Shared Services >** Client Management.
2. Go to **Client Upgrades**.
3. Click **Create Client Upgrade**.
4. Enter a **Name** for the Client upgrade.

©2026 Tanium Inc. All Rights Reserved

5. (Optional) To deploy a version of the Tanium Client other than the latest, click Edit in the **Content to deploy** section, and then select the **Client Version** to deploy.
   Leave **Auto-upgrade to latest version** selected to deploy the latest version of the Client. In an ongoing upgrade, this option also keeps targeted Clients upgraded to the latest version as new versions become available.

6. In the **Endpoints to target** section, click **Computer Groups**, and select the computer groups to be upgraded.

7. Click Edit in the **Deployment type and schedule** section, and configure the following settings:
   - For **Deployment Type**, select **Ongoing** or **One-Time**.

     Best Practice: Use a one-time upgrade with an end time for an upgrade to a specific version so that it does not run indefinitely even after you upgrade all the Tanium Clients.

   - Select the **Deployment Time Zone** and configure the **Start Time** at which deployment of the upgrade will begin. For a one-time upgrade, configure the **End Time** at which deployment of the upgrade will end.

     Best Practice: If you are configuring a one-time upgrade, make sure that the **Start Time** and **End Time** define a period of time during which you expect each targeted endpoints to be online at some point. The upgrade window can span multiple days if necessary.

   - (Optional) Adjust the **Distribute Over Time** setting. This setting determines the period of time over which distribution of the upgrade action is randomized and helps balance resource use.

     Best Practice: Distribute the upgrade over time to prevent upgrades from occurring on all the targeted endpoints simultaneously.

8. Click **Preview to Continue** and review the **Version status of targeted endpoints**.

9. Click **Deploy** to create the upgrade. The action for the Client upgrade is issued at the **Start Time** you configured.

©2026 Tanium Inc. All Rights Reserved

> **Note:** You can later edit an ongoing upgrade, or you can edit a one-time upgrade before the **Start Time** has passed.

Alternatively, you can create a deployment in Client Management that is configured to upgrade endpoints with an existing Tanium Client. For more information, see Deploying the Tanium Client using Client Management on page 125.

Upgrade Tanium Clients using a package

About this task

In cases where you want to upgrade the Client on an individual endpoint or a small number or endpoints that do not comprise an entire computer group, you can target those endpoints and manually deploy actions that use the **Client Management - Upgrade [Windows]** and **Client Management - Upgrade [Non-Windows]** packages. For more information about deploying packages, see Deploying actions.

1. In Interact, target the endpoints on which you want to upgrade the Tanium Client. For example, ask a question that targets a specific operating system and a Tanium Client older than a certain version: `Get Tanium Client Version from all machines with ( Is Windows contains true and Tanium Client Version < 7.9.3.xxxx )`
2. In the results, drill down as necessary, and select the endpoints that you want to upgrade.
3. Click **Deploy Action**.
4. For the **Deployment Package**, select **Client Management - Upgrade [Windows]** or **Client Management - Upgrade [Non-Windows]**, depending on the endpoints you are targeting.
5. Select a **Client Version** to install.
6. Click **Show preview to continue**.
7. A results grid appears at the bottom of the page showing you the targeted endpoints for your action. If you are satisfied with the results, click **Deploy Action**.

Verify the upgrade

About this task

After an upgrade completes, confirm that the targeted endpoints are online and report the target

©2026 Tanium Inc. All Rights Reserved

Tanium Client version. If you upgrade in stages, verify each stage before you start the next one.

1. Ask the following question, where `<target_client_version>` is the version to which you upgraded:
   `Get Tanium Client Version from all machines with Tanium Client Version < <target_client_version>`

   The results list the endpoints that still report an earlier version.

2. Compare the number of endpoints that respond to questions with the number that responded before the upgrade. Endpoints that no longer respond might be offline or might have had a problem during the upgrade.

3. Investigate endpoints that still report an earlier version or that stopped responding. For information about finding and remediating endpoints that are not reporting, see Audit and remediate disconnected Tanium Clients on page 332.

Disable the legacy Tanium Protocol used only for 7.2 and earlier clients

About this task

After you have upgraded all version 7.2 Tanium Clients in your environment to version 7.6.2 or later, it is a best practice to disable the legacy version of the Tanium Protocol used only for 7.2 and earlier clients (v314) to reduce security surface area. This version of the protocol is deprecated, and it will be turned off by default in a future semiannual release.

Important: Perform this procedure only after you have fully confirmed that all necessary endpoints that have Tanium Client 7.2 installed have been upgraded. Depending on the upgrade method and your environment, it might take significant time (up to multiple days) or manual intervention for all endpoints to come online and receive the upgrade. If you disable the legacy version of the Tanium Protocol while there are still version 7.2 Tanium Clients in your environment, those Clients will be unable to communicate with the Tanium Server, even if you re-enable the legacy version.

1. From the Main menu, go to **Administration** > **Configuration** > **Settings** > **Advanced Settings**.

2. In the **Name** column, click **enable_protocol_314_flag**.

3. Set the **Value** to `0` and click **Save**.

©2026 Tanium Inc. All Rights Reserved

Uninstalling Tanium Clients

Uninstall the Tanium Client on Windows

You can use various tools to uninstall the Tanium Client.

Best Practice: Restart a Windows endpoint after you uninstall the Tanium Client to allow removal of files that are in use during the initial uninstallation process.

Related information

- Deploy the Tanium Client to Windows endpoints using the installer on page 155
- Manage the Tanium Client on Windows on page 293
- Preparing the Tanium Client on a Windows OS image on page 194
- Client version and operating system requirements on page 29
- Managing Client settings and Index configurations on page 318
- Tanium Client settings reference on page 393

USE A TANIUM PACKAGE TO DEPLOY AN UNINSTALLATION PROGRAM

About this task

You can use the Tanium Core Platform to remove the Tanium Client from targeted endpoints. The uninst.exe program is in the Tanium Client installation directory on page 490.

1. From the Main menu in Tanium Console, go to **Administration** > **Configuration** > **Settings**.
2. In the **Packages** section, set **Run Commands in Process Group** to **ON**, and click **Save All**.
3. From the Main menu, go to **Administration** > **Content** > **Packages**, click **New Package**, and configure a package that issues the uninstall command. The following is an example of the command to perform a silent uninstallation:

   ```
   cmd.exe /C ..\..\uninst.exe /S
   ```

   You must clear the selection for **Launch this package command in a process group**.
4. Create a scheduled action to distribute the package to targeted computers. For more information, see Deploying actions.

©2026 Tanium Inc. All Rights Reserved

> **Note:** The uninstallation program stops the Tanium Client service and removes the application files, so the Tanium Client will no longer be present to write `Completed` to the respective action log. Consequently, do not rely on the final action status reported in Tanium Console to determine success or failure of the uninstallation action.

> **Best Practice:** Since most packages should be created to run in a process group, return the set **Run Commands in Process Group** to **OFF** after you create the uninstallation package. This setting prevents users from creating packages with the **Launch this package in a process group** setting turned off. For more information, see Create a Package.

USE ADD/REMOVE PROGRAMS

A user with Local Administrator rights on the endpoint can remove the Tanium Client through either the Windows Control Panel **Add/Remove Programs** or Programs and Features applet.

UNINSTALLATION PROGRAM

Double-click the uninst.exe program icon or execute the program from a command prompt.

The uninstall executable supports the /S command line parameter to perform a silent uninstall from a command prompt, script, package, or BAT file: `uninst.exe /S`

Uninstall the Tanium Client on macOS

Related information

- Deploy the Tanium Client to macOS endpoints using the installer on page 165
- Manage the Tanium Client on macOS on page 305
- Preparing the Tanium Client on a macOS image on page 197
- Client version and operating system requirements on page 29
- Managing Client settings and Index configurations on page 318
- Tanium Client settings reference on page 393

UNINSTALL WITHOUT USING A SCRIPT

1. On the macOS endpoint, open **Terminal**.

©2026 Tanium Inc. All Rights Reserved

2. Run the following command to stop the Tanium Client and remove it from the launch list:
   `sudo launchctl remove com.tanium.taniumclient`

3. Remove the following files and directories if they exist:
   - /Library/LaunchDaemons/com.tanium.taniumclient.plist
   - /Library/LaunchDaemons/com.tanium.trace.recorder.plist
   - /Library/LaunchDaemons/com.Tanium.tanium-client-upgrade.plist
   - /Library/LaunchDaemons/com.Tanium.taniumclientupgrade.plist
   - /Library/LaunchDaemons/com.Tanium.taniumecfreset.plist
   - /Library/Tanium/TaniumClient/ (directory)
   - /var/db/receipts/com.tanium.client.bom
   - /var/db/receipts/com.tanium.client.plist
   - /var/db/receipts/com.tanium.taniumclient.TaniumClient.pkg.bom [1]
   - /var/db/receipts/com.tanium.taniumclient.TaniumClient.pkg.plist [1]

   [1] These files appear only if a version of the Tanium Client earlier than 7.2.314.3608 was installed on the endpoint.

   Note: The files present in the installation depend on your Tanium environment and the solutions used with an endpoint. Some of the listed files might not be included in your installation, and additional files might be present.

UNINSTALL USING A SCRIPT

To uninstall the Tanium Client silently from a command line, you can use a shell script such as the following:

```
#!/bin/bash

if [[ $(/usr/bin/id -u) -ne 0 ]]; then
     echo "Not running as root or using sudo"
     exit
```

©2026 Tanium Inc. All Rights Reserved

```
fi

launchctl unload /Library/LaunchDaemons/com.tanium.taniumclient.plist
launchctl remove com.tanium.taniumclient > /dev/null 2>&1
rm /Library/LaunchDaemons/com.tanium.taniumclient.plist
rm /Library/LaunchDaemons/com.tanium.trace.recorder.plist
rm /Library/LaunchDaemons/com.Tanium.tanium-client-upgrade.plist
rm /Library/LaunchDaemons/com.Tanium.taniumclientupgrade.plist
rm /Library/LaunchDaemons/com.Tanium.taniumecfreset.plist
rm -rf /Library/Tanium/
rm /var/db/receipts/com.tanium.taniumclient.TaniumClient.pkg.bom
rm /var/db/receipts/com.tanium.taniumclient.TaniumClient.pkg.plist
rm /var/db/receipts/com.tanium.client.bom
rm /var/db/receipts/com.tanium.client.plist
```

Note: This script is an example and might require changes, depending on your Tanium environment and the solutions used with endpoints. Some of the removed files might not be included in your installation, and additional files might be present.

Uninstall the Tanium Client on Linux

To uninstall the Tanium Client, run one of the following CLI commands, depending on the distribution type:

- RPM-based Linux distributions such as Red Hat or SUSE:

  ```
  rpm -e $(rpm -qa --queryformat "%{NAME}\n"| grep -e '[Tt]anium[Cc]lient')
  ```

  Note: This command might require `sudo`, depending on the environment.

- Debian-based Linux distributions:

  ```
  dpkg -P taniumclient
  ```

Related information

- Deploy the Tanium Client to Linux endpoints using package files on page 173
- Manage the Tanium Client on Linux on page 308
- Preparing the Tanium Client on a Linux OS image on page 200
- Client version and operating system requirements on page 29
- Managing Client settings and Index configurations on page 318
- Tanium Client settings reference on page 393

©2026 Tanium Inc. All Rights Reserved

Uninstall the Tanium Client on Solaris

To uninstall the Tanium Client on Solaris, run the following command, where the `-A` flag directs pkgrm to uninstall in the current zone only: `pkgrm -A TaniumClient`

Related information

- Deploy the Tanium Client to Solaris endpoints using a package file on page 181
- Manage the Tanium Client on Solaris on page 315
- Preparing the Tanium Client on a Solaris OS image on page 203
- Client version and operating system requirements on page 29
- Managing Client settings and Index configurations on page 318
- Tanium Client settings reference on page 393

Uninstall the Tanium Client on AIX

To uninstall the Tanium Client on AIX, run the following command: `installp -u TaniumClient`

Related information

- Deploy the Tanium Client to AIX endpoints using a package file on page 188
- Manage the Tanium Client on AIX on page 316
- Preparing the Tanium Client on an AIX OS image on page 206
- Client version and operating system requirements on page 29
- Managing Client settings and Index configurations on page 318
- Tanium Client settings reference on page 393

©2026 Tanium Inc. All Rights Reserved

Troubleshooting Tanium Clients and Client Management

This section identifies resources that you can use when troubleshooting issues with the Tanium Client and with Client Management.

Basic tips

- Client health: Review Client health information in the Client Management service to help identify general issues with the Tanium Client on endpoints. For more information, see Monitor the Client health overview in Client Management on page 284 and Access detailed Client health and troubleshooting information on an endpoint on page 287.
- Version: Make sure that a supported version of the Tanium Client is installed.
- Requirements: Ensure your environment meets the host system and network requirements. For more information, see Tanium Client and Client Management requirements on page 29.
- Access: If you encounter failed access messages when running a Tanium Client installer, examine the permissions for the signed in user.
- Installation: For Tanium Client installation issues:
    - Review the Tanium Client Management service logs or the Client installation logs in the Tanium Client Management deployment if you used that service to deploy the Clients. For more information, see Troubleshoot Client Management on page 387.
    - Examine the Tanium Client installation log on page 357 on the endpoints.
    - Make sure the endpoint has enough available space on the disk or partition where you are installing the Client. For more information, see Hardware requirements on page 45. If you are using Client Management for deployment, see Deploy Clients on page 138 for information about setting the installation directory and the space required on endpoints to proceed with deployment.

©2026 Tanium Inc. All Rights Reserved

- Connection and registration: For more information, see Troubleshoot issues with connection and registration on page 357.
- Client settings: For more information, see Managing Client settings and Index configurations on page 318 and Tanium Client settings reference on page 393.
- Actions: For issues that occur when deploying actions, see Review action logs and associated files to troubleshoot actions and packages on page 366 and Review action history logs to troubleshoot or audit actions on page 369.
- Sensors: For issues related to sensors, see Review sensor history logs to troubleshoot or audit sensor activity on page 370 and Review and manage sensor quarantines to troubleshoot sensors on page 377.
- Tanium Client service: For more information, see Verify that the Tanium Client service and process are running on an endpoint on page 359.

Review the Tanium Client installation log to troubleshoot installation on Windows

If you encounter issues with your installation on Windows endpoints, examine Install.log in the Tanium Client installation directory on page 490 to identify actions that failed during the installation. The Tanium Client installer generates this log file to record a chronology of the actions that the installer performed. Each time the installer runs (that is, for each installation and upgrade), it appends the actions for that execution to the end of the existing log file.

Troubleshoot issues with connection and registration

If the Tanium Client fails to connect or register with the Tanium Server or Zone Server, does not establish the expected peer connections, or fails to respond to questions, review the Tanium Client logs on page 364, and check the following items.

Tip: Use the CLI to adjust the log verbosity level as necessary on a Client that is not registering.

For more information, see Example 2: Set and confirm log verbosity level on page 413.

©2026 Tanium Inc. All Rights Reserved

Check the Client status

1. From the Main menu, go to **Administration** > **Configuration** > **Client Status**. Filter the list as necessary to help locate the endpoint.
   For more information about the **Client Status** page, see Verify or remediate Tanium Client peering and leader connections on page 264.

2. If the endpoint does not appear in the current list, select **Show systems that have reported in the last**, and adjust the time period to determine if the endpoint has previously reported. If the endpoint previously reported, consider whether there were changes near the **Last Registration** time on the endpoint or the network that might have affected the connectivity of the Tanium Client.

3. If the endpoint does not appear, or if **No** appears in the **Valid Key** column, check the public key (tanium-init.dat) for the Client. For more information, see Review or reset the public key to troubleshoot connection issues on page 373.

4. If the endpoint is not currently reporting and the Client appears to have a valid key, proceed to the next troubleshooting task.

Perform a test registration of the Tanium Client from the endpoint

On Tanium Client 7.7.3.8176 or later, you can manually perform a test registration of the Tanium Client using the following CLI command on the endpoint:

- Windows: `TaniumClient test registration <path-to-tanium-init.dat>`
- Non-Windows: `./TaniumClient test registration <path-to-tanium-init.dat>`

This test evaluates the steps of the registration process and provides feedback that can assist in diagnosing connection issues and other issues that prevent successful registration. You must specify a tanium-init.dat file with which to test the registration. By default, the tanium-init.dat file currently in use by the Client is located in the Backup directory within the Tanium Client installation directory on page 490.

```
[root@myendpoint TaniumClient]# ./TaniumClient test registration Backup/tanium-init.dat
Using tanium-init.dat from "Backup/tanium-init.dat"
Local config values:
  Key: LastGoodServerName, value: example-zsb1.cloud.tanium.com
  Key: Path, value: /opt/Tanium/Tanium Client
  Key: RegistrationSecret, value: 7808df8d-5099-df09-1def-4daf29c358be
```

©2026 Tanium Inc. All Rights Reserved

```
  Key: ServerName, value: example-zsb1.cloud.tanium.com
  Key: ServerNameList, value: example-zsb1.cloud.tanium.com:17472,example-
zsb2.cloud.tanium.com:17472
Resolved server address:
  Server name: example-zsb2.cloud.tanium.com
  IP address: 10.10.149.16
  New connection:
    Type: plain
    Established from: 192.168.0.136:54590
    Established to: 10.10.149.16:17472
    Server challenge:
      Status: success
  New connection:
    Type: tls
    Established from: 192.168.0.136:54616
    Established to: 10.10.149.16:17472
    Certificate:
      Subject: /CN=ocitaniumzoneserver2.tanium.local TLS 27/role=ZoneServer TLS
      Issuer: /CN=taniumserver2.tanium.local/role=Root/serialNumber=1
      Tanium perms has: ZoneServer TLS
      Valid from: 2025-04-25 12:47:56 +0000
      Valid until: 2025-06-25 12:47:56 +0000
      Public key algorithm: EC
      Public key SHA512 short fingerprint: 8d:d5:06:61:9d:f9
    Client registration:
      Status: success
  Result: success
Resolved server address:
  Server name: example-zsb1.cloud.tanium.com
  IP address: 10.10.45.27
  New connection:
    Type: plain
    Established from: 192.168.0.136:54617
    Established to: 10.10.45.27:17472
    Server challenge:
      Status: success
  New connection:
    Type: tls
    Established from: 192.168.0.136:54618
    Established to: 10.10.45.27:17472
    Certificate:
      Subject: /CN=ocitaniumzoneserver1.tanium.local TLS 27/role=ZoneServer TLS
      Issuer: /CN=taniumserver1.tanium.local/role=Root/serialNumber=1
      Tanium perms has: ZoneServer TLS
      Valid from: 2025-04-25 12:47:57 +0000
      Valid until: 2025-06-25 12:47:57 +0000
      Public key algorithm: EC
      Public key SHA512 short fingerprint: 3f:1c:bf:04:d0:be
    Client registration:
      Status: success
  Result: success
No more server names to resolve.
```

Verify that the Tanium Client service and process are running on an endpoint

Check the status of the Tanium Client service and, if necessary, restart it:

- Manage the Tanium Client service on Windows on page 293

©2026 Tanium Inc. All Rights Reserved

- Manage the Tanium Client service on macOS on page 308
- Manage the Tanium Client service on Linux on page 313
- Manage the Tanium Client service on Solaris on page 315
- Manage the Tanium Client service on AIX on page 317

Additionally you can use the following commands to verify that the Tanium Client process is running:

- Windows: `tasklist | findstr /i "TaniumClient"`
- Non-Windows: `ps -eaf | grep -i TaniumClient`

If the Tanium Client service, process, or installation directory on page 490 does not exist, reinstall the Tanium Client. For more information, see Deploying the Tanium Client using Client Management on page 125 and Deploying the Tanium Client using an installer or package file on page 153.

Verify port accessibility and security exclusions

Make sure that communication on port 17472 (or the otherwise configured custom port) is allowed by any firewalls and other security applications.

Make sure that security exclusions are in place for Tanium Client directories and processes. For more information, see Security exclusions for Tanium Client on page 71.

Verify server connection settings

For server connection issues, use the following commands to review and verify the Server connection settings for the Client.

Tanium Server connection settings for Tanium Client troubleshooting

Setting	OS	
Tanium Server and Zone Server FQDNs or IP addresses	Windows	`TaniumClient config get ServerNameList`
	Non-Windows	`sudo ./TaniumClient config get ServerNameList`

©2026 Tanium Inc. All Rights Reserved

Setting	OS	
Tanium Server port (if the port is not specified in **ServerNameList**)	Windows	`TaniumClient config get ServerPort`
	Non-Windows	`sudo ./TaniumClient config get ServerPort`
Proxy servers (where used)	Windows	`TaniumClient config get ProxyServers`
	Non-Windows	`sudo ./TaniumClient config get ProxyServers`
Proxy auto configuration (PAC) file (where used)	Windows	`TaniumClient config get ProxyAutoConfigAddress`
Automatic proxy detection (where used)	Windows	`TaniumClient config get ProxyAutoDetect`

If any settings are incorrect, or for more information about server connections, see Configuring connections to the Tanium Core Platform on page 230.

For peer connection issues, see Configuring Tanium Client peering on page 247.

Test DNS resolution

If you use fully qualified domain names for the Tanium Servers and Zone Servers that are specified for **ServerNameList**, use the following command to test the DNS resolution for each Server name:

```
nslookup <server_FQDN>
```

If the command does not return one or more IP addresses for the server name, there is likely an issue with DNS resolution. Work with your network administrator to resolve the issue.

Test network connectivity and port accessibility

1. If ICMP ping traffic is allowed, use the following command to ping each server:
   `ping <server_FQDN/IP_address>`

   If the ping receives timely responses, you can skip to step 3.

2. If the ping does not receive responses even though ICMP traffic is allowed and the Server is

©2026 Tanium Inc. All Rights Reserved

known to be up, there might be a network routing issue. Use one of the following commands to verify a possible route to the server:

- Windows: `tracert <server_FQDN/IP_address>`
- Non-Windows: `traceroute <server_FQDN/IP_address>`

If the route cannot be completed, work with your network administrator to resolve the issue.

3. To verify that the endpoint can communicate with port 17472 (or the otherwise configured custom port), use one of the following commands:
   - Windows PowerShell: `Test-NetConnection -ComputerName <server_FQDN/IP_address> -Port 17472`
   - Non-Windows: `nc -vz <server_FQDN/IP_address> 17472`

   If the connection fails, work with your network administrator to make sure that communication on port 17472 (or the otherwise configured custom port) is allowed by any firewalls and other security applications.

Collect troubleshooting information from endpoints

About this task

You can use Client Management to directly connect to an endpoint and collect a bundle of logs and other artifacts, sometimes referred to as an *Endpoint Must Gather* (EMG).

1. From the Main menu, go to **Shared Services** > **Client Management**.
2. From the Client Management menu, click **Client Health**.
3. In the **Single Endpoint View** search box, enter all or part of an IP address or a computer name.
   Matching results appear after the search completes.
4. From the search results, click the computer name.
   Client Management opens the Endpoint Details page in Single Endpoint View (SEV).
5. Click the **Client Health** tab and, if the endpoint is not yet **Connected**, click **Direct Connect**.
6. In the **Available Steps** grid, select the domains (types of logs and artifacts) for which you want to gather troubleshooting information.

©2026 Tanium Inc. All Rights Reserved

For Patch information, select the **Core** and **Patch** domains.

For Comply information, select the **Comply** domain and then select **Comply Database**, **Comply Extension Data**, and **Comply Intel**.

For Endpoint Management for Operational Technology entity provider information, select the **Core** domain and then select **Tanium Client Logs**. Select the **Entity** domain and then select **Config Data**, **Entity Log**, and **Entity Provider Metadata**.

7. Click **Gather from Endpoint**.
   The selected logs and artifacts are gathered from the endpoint. The package appears in the **Must Gathers** section, and the name of the package corresponds with its time stamp.

8. When **Finished** appears in the **Run State** column, select the package and click **Download** to download a ZIP file that contains the troubleshooting information.
   For more information about collecting troubleshooting information in Single Endpoint View, see Tanium Reporting User Guide: Collect troubleshooting information.

   For more information about how to connect directly to endpoints, see Tanium Direct Connect User Guide.

   For more information about Client health features in Client Management, see Tanium Client Management User Guide: Monitor the Client health overview in Client Management and Tanium Client Management User Guide: Access detailed Client health and troubleshooting information on an endpoint.

Access individual endpoint logs in Client Management

About this task

You can use Client Management to directly connect to an endpoint and view and download individual logs.

1. From the Main menu, click **Shared Services** > **Client Management**.
2. From the Client Management menu, click **Client Health**.
3. In the **Single Endpoint View** search box, enter all or part of an IP address or a computer name.
   Matching results are displayed after the search completes.

©2026 Tanium Inc. All Rights Reserved

4. From the search results, click the computer name.
   Client Management opens the Endpoint Details page in Single Endpoint View (SEV).

5. Click the **Client Health** tab and, if the endpoint is not yet **Connected**, click **Direct Connect**. Select a log to view. For more information, see Tanium Reporting User Guide: View and download Tanium Client logs.

6. (Optional) To download the log, click **Download**.

Review Tanium Client logs to troubleshoot connections and other Client issues

Review Tanium Client logs to help you troubleshoot Client issues. For example, a Client might not answer questions or appear in Tanium Console (**Administration** > **Configuration** > **Client Status**) because that Client cannot connect to the Tanium Server or Zone Server. In this case, you can review the Client logs to determine whether the connection failed due to an invalid server IP address, DNS resolution failure, missing Tanium public key file, or firewall rule.

The Tanium Client writes new Client logs to the file log0.txt. The default maximum log file size is 10 MB. When log0.txt reaches the maximum size, the Client renames it log1.txt and then creates a new log0.txt. When log0.txt again reaches the maximum, the Client renames log1.txt as log2.txt, again renames log0.txt as log1.txt, and again creates a new log0.txt. The process of rolling logs whenever log0.txt reaches the maximum size continues until 10 logs exist: log0.txt to log9.txt.

When log0.txt reaches the maximum size again after that, the Client compresses log9.txt as a file named log10.zip. When log0.txt again reaches 10 MB, the Client renames log10.zip as log11.zip and again compresses log9.txt as a file named log10.zip. The ZIP file rollover process continues until 10 ZIP files exist, log10.zip to log19.zip. When log0.txt reaches 10 MB again after that, the Client creates a new log10.zip without renaming log19.zip as a new file, effectively dropping the old log19.zip information upon renaming log18.zip as the new log19.zip.

The logging level is configurable (see LogVerbosityLevel on page 393). The location for log files is also configurable (see LogPath on page 393). The default is < Tanium Client installation directory on page 490 >/Logs.

©2026 Tanium Inc. All Rights Reserved

Tip: You can ask a question using the `Tanium Client Logging Level` sensor to determine the log verbosity level on endpoints.

You can use Client Management to directly connect to an endpoint and retrieve Client logs. For more information, see Access individual endpoint logs in Client Management on page 363.

Network Configuration errors reported in the log

The error message `Network Config Timed Out` or `Failed to download netconfig at startup` commonly appears when a Tanium Client fails to connect or register with the Tanium Server or Zone Server. To troubleshoot this error message, see Troubleshoot issues with connection and registration on page 357.

Cache-related errors reported in the log

Cache-related errors that are reported in a Client log are often caused by low disk space on the endpoint. Make sure the endpoint has enough available space on the disk or partition where the Client is installed. For disk space requirements, see Hardware requirements on page 45.

On a Linux endpoint, you can move the Tanium Client if the partition where it is installed does not have enough free space. For more information, see Move an existing installation of the Tanium Client on Linux on page 314.

Logging levels

The logging level determines how much detail Tanium Clients record in logs, from 0 (no logging) to 99 (the highest level of detail). Select a level that provides just enough detail for you to understand what happened during an event. If you set the level too high, logs might contain so much detail that finding a particular event becomes difficult, especially if the logs roll over quickly and you must search across multiple files. Furthermore, when the number of log files reaches the maximum, the oldest files are deleted and you lose their record of events.

The following logging levels are best practices for specific scenarios:

- 1: Normal (default) logging level. At this level, logs typically record error conditions (such as failed operations) but few informational messages (such as successful operations).

©2026 Tanium Inc. All Rights Reserved

- 11: Best practice value for long-term troubleshooting. At this level, logs generally record enough information to help you understand the history of issues that occur. You can leave the level at 11 indefinitely without the logs being cluttered with less useful information or rolling over too quickly.
- 41: Best practice value for temporary troubleshooting. At this level, logs record details that are useful for diagnosing specific issues. When you finish troubleshooting the issue, the best practice is to revert to a lower logging level.
- 91 or higher: Most detailed logging level for advanced debugging. Because this level causes logs to roll over quickly and include details that are excessive for most scenarios, use it only for short periods and then revert to a lower logging level.



Note:

A value of `0` disables logging. As a best practice, do not disable logging.

The logging level that you set on a Tanium Client applies to all the log types on that Client, except for custom logs. To change the log level, configure the **LogVerbosityLevel** setting on the Client. For more information, see Reference: Tanium Client settings and CLI (LogVerbosityLevel) on page 393 and Modify Client settings on page 320. For more information about the logging level impact on custom logs, or to change the level, see Create a custom log for a Tanium Client on page 371.

Review action logs and associated files to troubleshoot actions and packages

When a package does not seem to work after you deploy it through an action, review action logs and the files associated with the action to help troubleshoot. Each time the Tanium Client receives an action message with an instruction set to execute, the Client creates an action log file named Action_*<ID>*.log, where *<ID>* is the action identifier. The action log contains the CLI output associated with the action command. The Tanium Client stores any files that are required to deploy an action package in Action_*ID* directories.

Both action logs and Action_*<ID>* directories are in the < Tanium Client installation directory on page 490 >/Downloads directory. The Tanium Client removes action logs from its host after a configurable

©2026 Tanium Inc. All Rights Reserved

interval (see Action log and package cleanup on page 369).

Tip:

Tanium Console displays the **Action ID** in the **Action** > **Action History** and **Action Status** pages (see Deploying actions). The **Action Status** page provides options for accessing action log information from multiple endpoints. For more information, see View action status.

Action history logs on page 369 provide a longer history of which actions a managed endpoint has run, but without the CLI output and other details.

Action_*<ID>* directories

Each Action_*<ID>* directory contains all the files that are required to deploy an action package. For example, if you deploy a package that has five files, the Tanium Client places each file in the Action_*<ID>* directory after it finishes downloading. After all five files download, the action status changes from `Preparing Files` to `Running` on the **Action Status** page. Even if a deployed package has no associated package files, the Tanium Client creates an empty Action_*<ID>* directory for it. The Tanium Client removes Action_*<ID>* directories from its host after a configurable interval (see Action log and package cleanup on page 369).

Access action logs in Client Management

About this task

You can use Client Management to directly connect to an endpoint and view and download individual logs.

1. From the Main menu, click **Shared Services** > **Client Management**.
2. From the Client Management menu, click **Client Health**.
3. In the **Single Endpoint View** search box, enter all or part of an IP address or a computer name.
   Matching results are displayed after the search completes.
4. From the search results, click the computer name.

©2026 Tanium Inc. All Rights Reserved

Client Management opens the Endpoint Details page in Single Endpoint View (SEV).

5. Click the **Client Health** tab and, if the endpoint is not yet **Connected**, click **Direct Connect**.
6. Go to the **Actions** section and select a previously run action for which you want to view the log.
   For more information, see Tanium Reporting User Guide: View and download Tanium Client logs.
7. (Optional) To download the log, click **Download**.

Action log contents

Action logs record each phase of an action:

- Downloading Files

  During this phase, the action log entry indicates the files are downloading:

  ```
  2016-11-28 14:12:30 +0000|Downloading Files.
  2016-11-28 14:12:30 +0000|Files Failed Verification
  ```

  Although it appears to be an error condition, the message "Files Failed Verification" indicates simply that the Client does not have the necessary files in its local cache, so it asks for the necessary files from its peers. This indicates normal behavior.

- Running

  During this phase, the action log notes that the action is currently running. Following this entry, the log displays anything echoed from the package:

  ```
  2016-11-28 14:12:37 +0000|Files Verified, running action.
  ```

- Completed

  When the action finishes running, the log records a completion entry under the standard output capture of the action.

  ```
  2016-11-28 14:12:37 +0000|Command Completed
  ```

©2026 Tanium Inc. All Rights Reserved

Important: Completion does not indicate success. For example, an action to execute a command might complete even if the command itself fails. For example, the command line for the package might not match the name of the distributed file or the command might fail to distribute a file. Managed endpoints show that the action completed, even though nothing occurred. Optionally, consider adding a validation query to the package to have the action status indicate success or failure.

Action log and package cleanup

The Tanium Client checks hourly, or immediately upon resetting (typically every two to six hours), whether any Action_*<ID>*.log files are over seven days old and deletes them if they are. The Tanium Client also checks hourly, or immediately upon resetting, whether any corresponding Action_*<ID>* directories have expired, and deletes them if they have. This process ensures that the endpoint does not consume more disk space than necessary for Tanium actions. Contact Tanium Support on page 392 if you want to preserve action logs or action directories for a longer time.

Review action history logs to troubleshoot or audit actions

When you troubleshoot or audit actions on managed endpoints, review the action history logs to see which actions ran, their start and run times, and associated commands. Although the Action logs on page 366 record more details, the Tanium Client preserves action history logs for a longer period (their individual log files are smaller) and therefore they provide a longer chronology of actions. The Tanium Client archives the first 10 MB of action history logs as plain-text files. After reaching the 10 MB threshold, the Client archives the oldest logs as ZIP files before adding new logs as plain-text files. The log rollover process is as follows:

Plain text logs files

The Tanium Client creates a new action-history0.txt file whenever an action runs. When that file reaches 1 MB in size, the Client renames action-history0.txt as action-history1.txt and creates a new action-history0.txt. When action-history0.txt again reaches 1 MB, the Client renames action-history1.txt as action-history2.txt, again renames action-history0.txt as action-history1.txt, and again creates a new action-history0.txt. The process of rolling logs whenever action-history0.txt reaches 1 MB continues until 10 logs exist: action-history0.txt to action-history9.txt.

ZIP log files

After recording 10 MB of plain-text action history logs, the Tanium Client compresses action-

©2026 Tanium Inc. All Rights Reserved

history9.txt as a file named action-history10.zip. When action-history0.txt again reaches 1 MB, the Client renames action-history10.zip as action-history11.zip and again compresses action-history9.txt as a file named action-history10.zip. The ZIP file rollover process continues until 10 ZIP files exist, action-history10.zip to action-history19.zip. When action-history10.zip reaches 1 MB again after that, the Client creates a new action-history10.zip without renaming action-history19.zip as a new file, effectively dropping the old action-history19.zip information upon renaming action-history18.zip as the new action-history19.zip.

The Tanium Client stores action history logs in the <Tanium Client installation directory on page 490>/Logs directory.

You can use Client Management to directly connect to an endpoint and retrieve action history logs. For more information, see Access individual endpoint logs in Client Management on page 363.

Review sensor history logs to troubleshoot or audit sensor activity

When you troubleshoot or audit sensor activity on managed endpoints, review the sensor history logs to see the following information about each sensor that ran:

- Sensor identity, by name and hash value
- Start and run times
- Size in bytes
- Parameter values (the logs identify parameterized sensors as temp sensors)
- Number of answer strings and associated hash value

The Tanium Client archives the first 10 MB of sensor history logs as plain-text files. After reaching the 10 MB threshold, the Client archives the oldest logs as ZIP files before adding new logs as plain-text files. The log rollover process is as follows:

Plain text logs files

The Tanium Client creates a new sensor-history0.txt file each time a sensor runs. When that file reaches 1 MB in size, the Client renames sensor-history0.txt as sensor-history1.txt, and creates a new sensor-history0.txt. When sensor-history0.txt again reaches 1 MB, the Client renames sensor-history1.txt as sensor-history2.txt, again renames sensor-history0.txt as sensor-

©2026 Tanium Inc. All Rights Reserved

history1.txt, and again creates a new sensor-history0.txt. The process to roll the logs whenever sensor-history0.txt reaches 1 MB continues until 10 logs exist: sensor-history0.txt to sensor-history9.txt.

ZIP log files

After recording 10 MB of plain-text sensor history logs, the Tanium Client compresses sensor-history9.txt as a file named sensor-history10.zip. When sensor-history0.txt again reaches 1 MB, the Client renames sensor-history10.zip as sensor-history11.zip and again compresses sensor-history9.txt as a file named sensor-history10.zip. The ZIP file rollover process continues until 10 ZIP files exist, sensor-history10.zip to sensor-history19.zip. When sensor-history10.zip reaches 1 MB again after that, the Client creates a new sensor-history10.zip without renaming sensor-history19.zip as a new file, effectively dropping the old sensor-history19.zip information upon renaming sensor-history18.zip as the new sensor-history19.zip.

The Tanium Client stores sensor history logs in the <Tanium Client installation directory on page 490>/Logs directory.

You can use Client Management to directly connect to an endpoint and retrieve sensor history logs. For more information, see Access individual endpoint logs in Client Management on page 363.

Create a custom log for a Tanium Client

About this task

If you want to troubleshoot only specific information in predefined Tanium logs, you can configure a Tanium Client to filter the logs based on a regular expression and to copy the matching content to a custom log. Custom logs are especially useful if you set a high logging level for the predefined logs such that they roll over too quickly and record too much information for you to easily find specific issues. You can create as many custom logs as necessary and base each one on a different filter. After you configure a new log type, the Tanium Client creates a custom log file upon recording an event in a predefined log that matches the regular expression. Thereafter, whenever the predefined logs record additional events that match the filter, the client copies those records to the custom log.

©2026 Tanium Inc. All Rights Reserved

Best Practice: Log filtering can consume significant resources on a client, especially if you set a high logging level. Therefore, the best practice is to remove custom logs after you finish a troubleshooting session. For more information, see the logging level setting in the CLI command options for custom logs on page 372 table.

Tip: You can also configure custom logs on a Tanium Core Platform Server. For more information, see Create a custom log for Tanium Core Platform Servers (Tanium Appliance deployments) or Create a custom log for Tanium Core Platform Servers (Windows deployments).

Perform the following procedure with the options listed in the CLI command options for custom logs on page 372 table, using the `TaniumClient` CLI executable on the applicable endpoint.

1. Sign in to the host system of the Tanium Core Platform Server or Tanium Client.
2. Open the **Command Prompt** (Windows) or, if necessary, the **Terminal** (non-Windows) and navigate (cd) to the Tanium Client installation directory on page 490.
3. Configure a regular expression for the custom log.
   - Windows: `TaniumClient config set Logs.<log prefix>.FilterRegex "<filter regex>"`
   - Non-Windows: `sudo ./TaniumClient config set Logs.<log prefix>.FilterRegex "<filter regex>"`
4. (Optional) Set the logging level of the custom log. If you skip this step, the default level is 1.
   - Windows: `TaniumClient config set Logs.<log prefix>.LogVerbosityLevel <logging level>`
   - Non-Windows: `sudo ./TaniumClient config set Logs.<log prefix>.LogVerbosityLevel <logging level>`

CLI command options for custom logs

©2026 Tanium Inc. All Rights Reserved

CLI command options for custom logs

Executable/ Option	Description
Log prefix	The log file prefix. The client automatically appends a number to the prefix and adds the suffix (.txt) upon generating the log. For example, if you enter `CompletedRegistrations` as the prefix for a custom client log, the first file that the Client generates for that log type is CompletedRegistrations0.txt .
Filter regex	The regular expression to use for filtering the predefined logs. The Server or Client copies log entries that match the filter to the custom log. **Note:** The filter applies only to log messages, not to thread names, thread IDs, or timestamps.
Logging level	The logging level of the custom log. For more information, see Logging levels on page 365 . **Important:** Higher logging levels consume more resources on the client . If different custom log types have different levels, the client generates all log types at the highest level that is set for any custom log type. This ensures that filter matching applies to all log messages at the highest configured level. However, in this case, each log file still contains only the level of detail that corresponds to the level you set for its log type. For example, you might set the logging level to 1 for predefined logs on the client and set the level to 91 for a custom log. In this case, the client generates log messages at level 91 for all log types and the custom log contains messages at level 91, but the predefined logs contain messages only at level 1.

Review or reset the public key to troubleshoot connection issues

About this task

You can review or reset the public key to help resolve connection issues that are related to an invalid key.

1. Access the operating system CLI on the endpoint and change directory (cd) to the Tanium Client installation directory on page 490.
2. Enter the following command:
   - Windows: `TaniumClient pki show`
   - Non-Windows: `./TaniumClient pki show`

   The output displays information about the current public key. Make sure that the command

©2026 Tanium Inc. All Rights Reserved

returns licenses for the appropriate servers, the status for each server is `trusted`, and the fingerprint for each license matches the fingerprint on the Server. For more information, see Managing Tanium keys.

```
[root@myendpoint TaniumClient]# ./TaniumClient pki show
taniumserver1.tanium.local Root 1
  perms has:
  perms grant: All, Server TLS, ZoneServer TLS, Client TLS, Message Signing, Hub TLS,
Module Content Signing, CX Socket TLS
  valid from: 2025-05-21 16:41:25 +0000
  valid to: 2026-05-22 23:59:59 +0000
  public key type: EC
  status: trusted
  fingerprint: a2:3e:f7:7d:b1:13

    taniumserver1.tanium.local Message Signing 10
      perms has: Message Signing
      perms grant:
      valid from: 2025-05-21 16:41:25 +0000
      valid to: 2025-11-22 16:41:25 +0000
      public key type: EC
      status: trusted
      fingerprint: c5:66:b9:73:0a:7e

taniumserver2.tanium.local Root 1
  perms has:
  perms grant: All, Server TLS, ZoneServer TLS, Client TLS, Message Signing, Hub TLS,
Module Content Signing, CX Socket TLS
  valid from: 2025-05-21 16:41:30 +0000
  valid to: 2026-05-22 23:59:59 +0000
  public key type: EC
  status: trusted
  fingerprint: b4:63:ae:3a:a0:b4

    taniumserver2.tanium.local Client TLS CA 11
      perms has:
      perms grant: Client TLS
```

©2026 Tanium Inc. All Rights Reserved

```
  valid from: 2025-05-21 16:41:30 +0000
  valid to: 2025-11-22 16:41:30 +0000
  public key type: EC
  status: trusted
  fingerprint: be:32:44:a6:39:1c

    localhost
      perms has: Client TLS
      perms grant:
      valid from: 2025-05-21 19:46:03 +0000
      valid to: 2025-05-29 19:46:03 +0000
      public key type: EC
      status: owned
      fingerprint: 02:5c:17:51:28:d5

taniumserver2.tanium.local Message Signing 10
  perms has: Message Signing
  perms grant:
  valid from: 2025-05-21 16:41:30 +0000
  valid to: 2025-11-22 16:41:30 +0000
  public key type: EC
  status: trusted
  fingerprint: 32:30:9a:60:51:68
```

3. (Optional) Reset the key with a new tanium-init.dat file.
    a. From the Main menu in Tanium Console, go to **Administration** > **Configuration** > **Infrastructure**.

    b. Click **Download**.

    c. Copy the downloaded file into the Tanium Client installation directory.

    d. Stop the Tanium Client service on the endpoint.

    e. From the CLI on the endpoint, enter the following command:

        - Windows: `TaniumClient pki reset tanium-init.dat`
        - Non-Windows: `./TaniumClient pki reset tanium-init.dat`

©2026 Tanium Inc. All Rights Reserved

CAUTION:

Non-Windows: If you are signed in as a non-root user, you must use the `sudo` command and set the HOME environment variable appropriately. Resetting the key without doing so causes the Client to be unable to register with the Tanium Server. Use the following steps in this scenario:

i. Use the following command to verify that you can access the encryption key necessary to encrypt the registration secret:

```
sudo -u root ls -lh ~root/.tanium-user-key-encryption.key
```

ii. If this file is present in the context of the root user, use the following command to reset the public key:

```
sudo -u root HOME=/var/root/ /Library/Tanium/TaniumClient/
TaniumClient pki reset /Library/Tanium/TaniumClient/tanium-
init.dat
```

iii. Use the following command and verify that the `RegistrationSecret` setting reports `(protected)`, which indicates that it is present and can be decrypted:

```
sudo -u root HOME=/var/root/ /Library/Tanium/TaniumClient/
TaniumClient config get RegistrationSecret
```

f. Restart the Tanium Client service on the endpoint.

©2026 Tanium Inc. All Rights Reserved

Tip:

For the procedures to stop and restart the Tanium Client service, see the following sections:

- Manage the Tanium Client service on Windows on page 293
- Manage the Tanium Client service on macOS on page 308
- Manage the Tanium Client service on Linux on page 313
- Manage the Tanium Client service on Solaris on page 315
- Manage the Tanium Client service on AIX on page 317

Important:

Be careful not to allow the tanium-init.dat file to be distributed or stored outside of your organization, such as in a publicly accessible source code repository or any other location accessible from the public internet. Limit the distribution to specific use in the deployment of Tanium Clients.

Though this file does not contain private keys and cannot be used to provide control over a Tanium environment, a user with malicious intent could use it to connect an unapproved Client and use this unauthorized access to learn how your organization is using Tanium.

Review and manage sensor quarantines to troubleshoot sensors

To remove sensors from quarantine through the operating system CLI on the endpoint instead of Tanium Console, see Remove all sensors from quarantine on page 379.

Overview of sensor quarantines

Enforcing *sensor quarantines* prevents sensors from running on an endpoint for the current question or action if those sensors exceeded the runtime timeout during a previous question or action. Quarantines are useful for limiting the impact on endpoint resources, such as CPU utilization, when questions and actions use excessively long-running sensors. The non-configurable timeout is set to

©2026 Tanium Inc. All Rights Reserved

one minute.

By default, quarantines are not enforced: after a sensor exceeds the one-minute timeout, the Tanium Client stops the sensor from running any longer and assigns it quarantined status but the sensor still runs for future questions or actions until it finishes or times out again. When quarantines are not enforced, the Client uses quarantined status just to record that the sensor timed out. After the Client assigns quarantine status, the status does not automatically revert to unquarantined if the sensor later finishes running for another question or action. You must manually Remove sensors from quarantine to change their status. Otherwise, the **Quarantined Sensors** page shows the cumulative results for any sensor that ever timed out on an endpoint since the initial Tanium Client installation.

The Tanium Client stops any sensor at the moment it exceeds the timeout regardless of whether you enable enforcement. Each Client quarantines sensors and enforces the quarantines independently. Consequently, a sensor might be quarantined on some endpoints and not on others. When a Client quarantines a sensor, Interact shows the following message in the **Question Results** grid: `TSE-Error: Sensor evaluation timed out`.



Important: The message `TSE-Error: Sensor evaluation timed out` means only that the Client could not finish executing the sensor within the one-minute timeout. If some Clients return this message while other do not for the same sensor, the cause is usually an issue on the endpoints where the quarantine occurs. For example, Clients might not finish running the sensor within the timeout if their host endpoints have insufficient resources or if interactions with anti-virus software on the endpoints cause unexpected delays.

When you issue a question that uses a sensor that is already quarantined and enforcement is enabled, the **Question Results** grid displays `TSE-Error: The sensor is quarantined`. The Tanium Client adds entries to the Client logs and sensor history logs when it quarantines a sensor or prevents an already quarantined sensor from running.

If temporary sensors exceed the one-minute timeout, the Tanium Client quarantines the original sensor as well as all current and future temporary sensors that are based on the original sensor. The Tanium Server creates a temporary sensor for questions that use parameterized sensors. For more information, see Questions with parameterized sensors.

©2026 Tanium Inc. All Rights Reserved

Best Practice: When enforcement is enabled, quarantined sensors do not run when you use them for targeting endpoints, even if the sensors are members of computer groups. However, quarantined sensors might skew the targeting of a question that has a vague *from* clause, such as `from all machines with Is Windows not equals true`. In this case, Windows endpoints on which the Is Windows sensor is quarantined would match the condition `not equals true` because their response would be `TSE-Error: The sensor is quarantined` rather than `true`. To avoid such outcomes, make the target clause as specific as possible and do not use negative matching conditions such as `not equals true`.

View quarantined sensors

About this task

If the Tanium Client does not answer a question, you can determine whether the associated sensors are quarantined. To see a list of all the quarantined sensors on all endpoints, see Manage sensor quarantines. To list all the quarantined sensors on a specific endpoint, perform the following steps:

1. Access the operating system CLI on the endpoint and change directory (cd) to the Tanium Client installation directory on page 490.
2. Enter the following command.
   - Windows: `TaniumClient quarantine list`
   - Non-Windows: `./TaniumClient quarantine list`

   The output lists the quarantined sensors by name and associated hash value.

Remove all sensors from quarantine

About this task

In some cases, enabling the Tanium Client to answer questions that use quarantined sensors might be more important than limiting the impact that long sensor run times have on the resources of an endpoint. Note that even after you remove the sensors from quarantine, if they exceed the timeout in a future question, the Tanium Client will then stop the sensors and quarantine them again without answering the question. To remove sensors from quarantine through Tanium Console, see Manage sensor quarantines. To remove sensors from quarantine through the operating system CLI on the endpoint, perform the following steps:

1. Access the operating system CLI on the endpoint and change directory (cd) to the Tanium Client installation directory on page 490.

©2026 Tanium Inc. All Rights Reserved

2. Enter the following command:
    - Windows: `TaniumClient quarantine clear`
    - Non-Windows: `./TaniumClient quarantine clear`

    The output displays the number of sensors removed from quarantine.

Remove a single sensor from quarantine

About this task

To remove a sensor from quarantine through Tanium Console, see Manage sensor quarantines. To remove a sensor from quarantine through the operating system CLI on the endpoint, perform the following steps:

1. Access the operating system CLI on the endpoint and change directory (cd) to the Tanium Client installation directory.
2. Enter the following command to see the hash values associated with quarantined sensors.
    - Windows: `TaniumClient quarantine list`
    - Non-Windows: `./TaniumClient quarantine list`
3. Enter the following command, where *<sensor_hash>* is the hash associated with the sensor that you want to unquarantine:
    - Windows: `TaniumClient quarantine remove <sensor_hash>`
    - Non-Windows: `./TaniumClient quarantine remove <sensor_hash>`

    Note: If you modify a sensor, Tanium Clients that receive its new definition automatically remove that sensor from quarantine.

Enable or disable enforcement of quarantined sensors

After you enable quarantine enforcement, Tanium Clients do not answer questions that use quarantined sensors and those sensors do not run for actions. After you disable enforcement, Clients still quarantine sensors and log quarantine events, but do not prevent those sensors from running.

Note: Your user account must have a role with the **Global Settings** write permission to enable or disable quarantine enforcement. Users with the **Administrator** reserved role have this permission.

©2026 Tanium Inc. All Rights Reserved

The first time you enable enforcement, you must add the **EnableSensorQuarantine** setting to the platform settings on the Tanium Server as follows. By default, enforcement is disabled and the setting does not appear in Tanium Console. After you add the setting, the Tanium Server applies it to all Tanium Clients.

1. Access Tanium Console.
2. From the Main menu, go to **Administration** > **Configuration** > **Settings** > **Advanced Settings**, and click **Add Setting**.
3. Enter the following values and click **Save**.
    - **Setting Type** = **Server**
    - **Platform Setting Name** = `EnableSensorQuarantine`
    - **Value Type** = `Numeric`
    - **Value** = `1`

Perform the following steps if you want to change the enforcement setting after adding it to the platform settings:

1. From the Main menu, go to **Administration** > **Configuration** > **Settings** > **Advanced Settings**.
2. In the **Name** column, click **EnableSensorQuarantine**, set the value to `1` to enable enforcement or `0` to disable enforcement, and click **Save**.

If you want to change the enforcement setting in specific Clients instead of all Clients, add or edit the EnableSensorQuarantine on page 393 setting in the local configuration of those Clients.

Identify and resolve issues with Client Extensions

About this task

Use the following steps to troubleshoot issues with the Client Extensions that Client Management installs and uses. During troubleshooting, consider environmental factors such as security exclusions, file locks, CPU usage, RAM usage, and disk failures.

©2026 Tanium Inc. All Rights Reserved

Tip: For more information about the Client Extensions that Client Management installs and uses, see Client Extensions on page 55.

1. If endpoints have Client Extension shared process mode enabled and you need to troubleshoot resource usage or crashes in the combined TaniumCX.exe or TaniumCX process, disable shared process mode on the affected endpoints, and then reproduce the issue if possible. For more information, see Manage Client Extension shared process mode.

2. To review the health of Client Extensions or to start an investigation into an existing error, ask a question using the `Client Extensions - Status` sensor.
   The results of these questions help to identify endpoints with errors and provide a starting point to deploy actions that might help correct the issue. Filter the results and drill down as necessary to investigate results that indicate errors.

   Tip: Consider whether endpoints with errors share common characteristics, such as operating system, domain or organization unit, or the antivirus software that is installed.

3. Target one or more endpoints with errors, and uninstall tools that report errors without blocking reinstallation. For more information, see Remove Client Management tools from endpoints on page 385 and Endpoint Configuration User Guide: Uninstall a tool installed by Endpoint Configuration.

   CAUTION: When you perform a hard uninstallation of some tools, the uninstallation also removes data that is associated with the tool from the endpoint. This data might include important historical or environmental data. If data that you want to keep is associated with the tool, make sure you perform only a soft uninstallation of the tool.

   Wait for automatic reinstallation of the tool. If the reinstallation does not resolve the issue, continue to the next step.

4. Ask a question using the `Endpoint Configuration - Tools Status Details` sensor, and include filters to limit the results to the tool that you are investigating. For example:
   `Get Endpoint Configuration - Tools Status Details having Endpoint Configuration - Tools Status Details:Tool Name contains <Tool_Name> from all machines with Endpoint Configuration -`

©2026 Tanium Inc. All Rights Reserved

`Tools Status:Tool Name contains <Tool_Name>`

Review the columns in the results for specific information about errors. The following table provides guidance for some common error conditions:

Potential errors returned by the Endpoint Configuration - Tools Status Details sensor

Error Condition	Possible Resolution
No error appears, but an available new version has not been installed	Review the **Targeted Version** column to make sure that the endpoint has received the latest manifest. If the targeted version does not yet show the updated version, the Endpoint Configuration manifest has not updated on the endpoint, usually for one of the following reasons: • The manifest update is still pending. Either wait for the manifest to update and then review the results again, or follow the steps in Endpoint Configuration User Guide: Verify and manually update the Endpoint Configuration manifest. • Action lock is enabled on the endpoint. Follow the steps in Endpoint Configuration User Guide: Verify and manually update the Endpoint Configuration manifest to identify endpoints with action lock turned on. • Client Management is no longer installed, or it is no longer targeting the endpoint. In some cases, Client Management might stop targeting an endpoint because it no longer needs the endpoint for a particular workload. Consider whether Client Management should still target the endpoint: • If it is expected or intentional that Client Management no longer targets the endpoint, you can optionally uninstall Client Management tools and dependencies. For more information, see Remove Client Management tools from endpoints on page 385. • If Client Management should still target the endpoint, make sure that the Client Management action group includes the endpoint, and make sure Client Management targets the endpoint in any expected configurations or profiles. Then, either wait for the manifest to update and then review the results again, or follow the steps in Endpoint Configuration User Guide: Verify and manually update the Endpoint Configuration manifest.
Installation Blocker: `Unmet`	If no **Failure Message** or **Failure Step** appears, the endpoint might be waiting for the dependencies to install. Wait to see if the condition resolves on its own. If this condition remains for an extended period, ask the question again and review any error information

©2026 Tanium Inc. All Rights Reserved

Error Condition	Possible Resolution
`Dependencies: [ Tool name ]`	in other columns, especially the **Failing Dependency** column.
`Failing Dependency:[ Tool name ]`	Ask the question: `Endpoint Configuration - Tools Status Details having Endpoint Configuration - Tools Status Details:Tool Name contains [Tool name] from all machines with Endpoint Configuration - Tools Status:Tool Name contains [Tool name]` Investigate further errors with the tool. If the dependency has not been installed on an endpoint, ask the question: `Get Endpoint Configuration - Tools Retry Status from all machines with Computer Name equals Computer_Name` to review the retry status for the tool installation. For more information, see Review tool installations that are scheduled for a retry .
Manually Blocked: `blocked`	The tool was previously blocked, either manually or during a previous uninstallation. Unblock the tool. For more information, see Block or unblock tools from installing on an endpoint .

5. Review the Extensions logs on the endpoint. Take note of entries that include `fail` or `error`. For more information, see Review the Extensions log for an endpoint on page 384.

Next steps

For additional help, collect all logs for Client Management on page 387, and contact Tanium Support on page 392.

Review the Extensions log for an endpoint

About this task

Use Client Management to directly connect to an endpoint and view and download extension logs.

1. From the Main menu, go to **Shared Services** > **Client Management**.
2. From the Client Management menu, click **Client Health**.
3. In the **Direct Connect** search box, enter all or part of an IP address or a computer name. Matching results are displayed after the search completes.

©2026 Tanium Inc. All Rights Reserved

4. From the search results, click the computer name to connect to the endpoint.
5. Click the **Logs** tab, and select an extensions[#].log file.
6. (Optional) To download the log, click **Download**.

Next steps

For additional help, collect all logs for Client Management on page 387, and contact Tanium Support on page 392.

Remove Client Management tools from endpoints

About this task

You can deploy an action to remove Client Management tools from an endpoint or computer group. Separate actions are available for Windows and non-Windows endpoints.

1. In Interact, target the endpoints from which you want to remove the tools. For example, ask a question that targets a specific operating system:`Get Endpoint Configuration - Tools Status from all machines with Is Windows equals true`
2. In the results, select the row for Client Management, drill down as necessary, and select the targets from which you want to remove Client Management tools. For more information, see Tanium Interact User Guide: Drill Down.
3. Click **Deploy Action**.
4. For the **Deployment Package**, select **Endpoint Configuration - Uninstall Tool [Windows]** or **Endpoint Configuration - Uninstall Tool [Non-Windows]**, depending on the endpoints you are targeting.
5. For **Tool Name**, select Client Management.
6. (Optional) By default, after the tools are removed they cannot be reinstalled. To allow tools to be automatically reinstalled, clear the selection for **Block reinstallation**. Re-installation occurs almost immediately.

©2026 Tanium Inc. All Rights Reserved

Note:

If reinstallation is blocked, you must unblock it manually:

- To allow Client Management to reinstall tools, deploy the **Endpoint Configuration - Unblock Tool [Windows]** or **Endpoint Configuration - Unblock Tool [Non-Windows]** package (depending on the targeted endpoints).
- If you reinstall tools manually, select **Unblock Tool** when you deploy the **Endpoint Configuration - Reinstall Tool [Windows]** or **Endpoint Configuration - Reinstall Tool [Non-Windows]** package.

7. (Optional) To remove all Client Management databases and logs from the endpoints, clear the selection for **Soft uninstall**.

   CAUTION: When you perform a hard uninstallation of some tools, the uninstallation also removes data that is associated with the tool from the endpoint. This data might include important historical or environmental data. If data that you want to keep is associated with the tool, make sure you perform only a soft uninstallation of the tool.

8. (Optional) To also remove any tools that were dependencies of the Client Management tools that are not dependencies for tools from other solutions, select **Remove unreferenced dependencies**.

9. (Optional) In the **Deployment Schedule** section, configure a schedule for the action.

   Tip: If some target endpoints might be offline when you initially deploy the action, select **Recurring Deployment** and set a reissue interval.

10. Click **Show preview to continue**.

11. A results grid appears at the bottom of the page showing you the targeted endpoints for your action. If you are satisfied with the results, click **Deploy Action**.

    Note: If you have enabled Endpoint Configuration approval, tool removal must be approved in Endpoint Configuration before tools are removed from endpoints.

©2026 Tanium Inc. All Rights Reserved

Troubleshoot Client Management

To send information to Tanium for troubleshooting, collect logs and other relevant information.

Collect logs

About this task

You can save Client Management logs as a ZIP file that you can download with your browser.

1. From the Main menu, go to **Shared Services >** Client Management.
2. From the Client Management **Overview** page, click Help ?.
3. In the **Collect Information for Support Requests** section, click **Collect**.
4. After the package is created, click **Download**. A tanium-client-management-support.zip file downloads to the local download directory.
5. Attach the ZIP file to your Tanium Support case form or contact Tanium Support on page 392.

View and configure logs

ADJUST LOG LEVEL

1. From the Client Management **Overview** page, click Help ?.
2. For **Log Level**, select the level of information to record in the service log and click **Save**.

ADJUST LOG RETENTION

1. From the Client Management **Overview** page, click Settings ⚙.
2. In the **Data Retention Settings** section, for **Service Logs (days)**, enter the number of days that service logs should be retained and click **Save Settings**.

View Client deployment logs

About this task

©2026 Tanium Inc. All Rights Reserved

To troubleshoot deployment issues in Client Management, you can view the installation log for each endpoint in a deployment.

1. From the Main menu, go to **Shared Services >** Client Management.
2. Go to **Client Installations** > **Client Deployments**, and then click the name of the deployment you want to view.
3. In the **Endpoint details** section view the list of targeted endpoints with status information. Use the **Filter items** box to find specific endpoints, or sort the table by the desired column to help find endpoints with a particular installation status or result.
4. In the row for an endpoint you want to investigate, click Endpoint Details to view the installation log.
5. To further troubleshoot, increase the verbosity of the installation log. Enable the Verbose Logging on page 144 setting, and then reissue the deployment on page 151.

Troubleshoot deployment issues

Issue: For a Windows endpoint, Endpoint Installation Status = `ERROR_CONNECTION_FAIL` with the following log message:

```
WindowsConnection: Failed to open remote WMI session: Failed to connect to <endpoint> as
user: Error code 2147942405: Access is denied.
```

Possible causes:

- The satellite or Module Server cannot communicate with the targeted endpoint.
- The satellite or Module Server cannot authenticate with the targeted endpoint.
- Windows-based satellite or Module Server: There is a compatibility issue with the Distributed Component Object Model (DCOM) Remote Protocol between the two hosts.

  In this case, the Windows System event log on the targeted endpoint contains the following message:

  ```
  The server-side authentication level policy does not allow the user <domain\user
  name> SID user SID from address <satellite or Module Server IP> to activate DCOM
  server. Please raise the activation authentication level at least to
  RPC_C_AUTHN_LEVEL_PKT_INTEGRITY in Client application.
  ```

©2026 Tanium Inc. All Rights Reserved

Solution: Check the following items:

- Check the user name provided with the credentials. Credentials must be active and not disabled. Check that the domain is added correctly, for example: `domain\username` for a domain account, or `username` for a local endpoint account. For more information, see Manage endpoint credentials on page 152.
- Check the password provided with the credentials to make sure it is not disabled or expired.
- Check both the target endpoint firewall and network device firewalls. The satellite or Module Server might be blocked from initiating a connection to the target endpoint by a firewall. WMI port 135, SMB port 445, and SSH port 22 must be open. Use the following testing techniques to check the ports:
    - Test Network connections:
        - Windows PowerShell: `Test-NetConnection -ComputerName ip_address -Port port_number`
        - Non-Windows: `nc -vz ip_address port_number`
    - In an Appliance deployment, check TanOS network status. For more information, see View system status.
- If the satellite used for deployment is a Windows endpoint, or if the Module Server is Windows-based in a Module Server deployment, apply the latest Windows updates to both hosts, which resolves compatibility issues with the DCOM Remote Protocol. For more information, see Microsoft Support: KB5004442—Manage changes for Windows DCOM Server Security Feature Bypass (CVE-2021-26414).

ISSUE: ENDPOINT INSTALLATION STATUS = ERROR_CONNECTION_FAIL WITH SSH CONNECTION LOG MESSAGE

Logs for the deployment contain a message similar to the following:

```
Command resulted in error: Error: Connection to 'SSH Client for '192.168.24.11'' was not established
```

Cause: Client Management is attempting an SSH deployment and cannot communicate with the endpoint, or cannot authenticate with the endpoint.

©2026 Tanium Inc. All Rights Reserved

Solution: Check the following items:

- Verify the Client Configuration and deployment settings. You might be targeting a Windows endpoint with a deployment while only using SSH as a connection method. For more information, see Deploying the Tanium Client using Client Management on page 125 and Deploying the Tanium Client using Client Management on page 125.
- Verify that the targeted Linux endpoint has SSH enabled and configured on port 22.
- Check the user name provided with the credentials. Credentials must be active and not disabled. Check that the domain is added correctly, for example: `domain\username` for a domain account, or `username` for a local endpoint account. For more information, see Manage endpoint credentials on page 152.
- Check the password provided with the credentials to make sure it is not disabled or expired.

ISSUE: ENDPOINT INSTALLATION STATUS = ERROR_INSTALL_FAIL WITH CERTIFICATE LOG MESSAGE

Logs for the deployment contain a message similar to the following:

```
verifying Tanium Installer: verifying installer signature: A certificate chain could not be
built to a trusted root authority.
```

Cause: The required trusted root certificates are not installed on the target Windows endpoint. Alternatively, if you are using a satellite for deployment, the satellite might have failed to authenticate.

Solution: Check the following items:

- Make sure that the required trusted root certificates are installed on the endpoint. For more information, see Trusted root certificate requirements on Windows endpoints on page 61.
- If you are using a satellite for deployment, delete and re-create the satellite in Direct Connect. For more information, see Managing satellites.

ISSUE: SATELLITE-BASED DEPLOYMENT FAILS WITH SATELLITE CONNECTION LOG MESSAGE

Logs for the deployment contain a message similar to the following:

```
Deployment Failed. getting deployment connection for deployment 1: getting satellite
connection
```

©2026 Tanium Inc. All Rights Reserved

Cause: Client deployment tools might have failed to deploy to the satellite used in the deployment.

Solution: Check the following items:

- Make sure the satellite is online and accessible to the endpoints in the deployment
- Make sure that you have allowed Client deployment tools in any security applications. For more information, see Security exclusions for Client Management on page 74.
- Retry the deployment. Client Management installs Client deployment tools on a satellite the first time you start a Client deployment that uses that satellite. Retrying the deployment also retries deployment of Client deployment tools to the satellite before deployment of Tanium Client.

Uninstall Client Management

1. From the Main menu, click **Administration** > **Configuration** > **Solutions**.
2. In the **Content** section, select the **Client Management** row.
3. Click Delete Selected . Click **Uninstall** to complete the process.

Get support for the Tanium Client

Tanium Support is your first contact for help when troubleshooting the initial deployment and for optimizing the speed and scale of your deployment as the number of managed endpoints grows. As necessary, Tanium Support can help adjust Tanium Client-related settings, including:

- Tanium Client registration frequency
- Connections between Tanium Clients and Tanium Core Platform Servers
- Client-to-client connections
- Bandwidth
- File caching

If you require further assistance from Tanium Support, include version information for Tanium Core Platform components and, if applicable, Tanium Client Management. Also include specific details on dependencies, such as the host system hardware and OS details. Finally, indicate if your installation

©2026 Tanium Inc. All Rights Reserved

uses a non-default installation directory on page 490 for the Tanium Client.

Contact Tanium Support

To contact Tanium Support for help, sign in to the Tanium Customer Community.

For more information about submitting a support case, see Case Submission Form.

©2026 Tanium Inc. All Rights Reserved

Reference: Tanium Client settings and CLI

Tanium Client settings reference

For information about reviewing and modifying Client settings, see Managing Client settings and Index configurations on page 318. Tanium Client settings are written to the Windows registry on page 491 on Windows endpoints and to an SQLite database on non-Windows endpoints.

Tanium Client settings

Setting Name	Applies to OS Platforms	Windows Registry Value Type	Non-Windows Setting Type	Description	Modify
ClientCacheLimitInMB [1]	All supported	REG_DWORD	NUMERIC	The size limit, in MB, for the file cache on an endpoint. The default is `2048`. For more information, see Chunk caching on page 27.	As necessary
ComputerID	All supported	REG_DWORD	NUMERIC	Value that the Tanium Server assigned to the Client to uniquely identify and track each managed endpoint.	No
CX.patch.EnableDeployments	Windows	REG_DWORD	NUMERIC	For emergency override scenarios where you need to disable Patch deployments. This setting does not affect Patch applicability scans. Valid values: • `0`: Disables Patch deployments	As necessary

©2026 Tanium Inc. All Rights Reserved

Setting Name	Applies to OS Platforms	Windows Registry Value Type	Non-Windows Setting Type	Description	Modify
				• `remove`: Deletes the setting and returns the system to the default configuration	
DatabaseEpoch	All supported	REG_SZ	STRING	Typically, this setting indicates the date and time when the Tanium Server was deployed.	No
DisableExtension_patch	Windows	REG_DWORD	NUMERIC	For emergency override scenarios where you need to disable Patch applicability scanning and Patch deployments. Valid values: • `1`: Disables Patch applicability scanning and Patch deployments • `remove`: Deletes the setting and returns the system to the default configuration	As necessary
EnableRandomListeningPort	All supported	REG_DWORD	NUMERIC	Enables (`1`) or disables (`0`) the randomized selection of a new listening port at intervals. The Client uses the port for communication from peer Clients. If another application is already using the selected port, the Client selects another port immediately instead of at the next interval. By default, **EnableRandomListeningPort** is disabled and the Client uses a fixed listening port (default is 17472). For more information and best practices, see Customize listening ports on page 274 .	As necessary

©2026 Tanium Inc. All Rights Reserved

Setting Name	Applies to OS Platforms	Windows Registry Value Type	Non-Windows Setting Type	Description	Modify
				Best Practice: Randomize listening ports only if it is required by rules in your organization. Using randomized listening ports requires more complex firewall rules to allow Client communication, and it makes troubleshooting issues with Client communication more difficult.	
EnableSensorQuarantine	All supported	REG_DWORD	NUMERIC	Add this setting and set the value to 1 if you want to enable the enforcement of sensor quarantines on a particular endpoint. By default, the setting is not present and enforcement is disabled. If you already added the setting, you can disable enforcement by setting the value to 0. You can also use Tanium Console to enable or disable enforcement for all endpoints. For more information, see Enable or disable enforcement of quarantined sensors on page 380 .	As necessary
FirstInstall	Windows	REG_SZ	N/A	Date and time of the initial Tanium Client installation.	No
HostDomainName	Non-Windows	N/A	STRING	Required only when the Client does not return the domain name correctly in question results. The value that you specify for this setting overrides the data that the Client OS would otherwise return.	As necessary

©2026 Tanium Inc. All Rights Reserved

Setting Name	Applies to OS Platforms	Windows Registry Value Type	Non-Windows Setting Type	Description	Modify
				Specify just the domain portion of the fully qualified domain name (FQDN). For example, if the FQDN is host.example.com , specify `example.com` .	
HostFQDN	Non-Windows	N/A	STRING	Another option (besides **HostDomainName**) for cases where the Client does not return the hostname and domain name correctly in question results. The value that you specify for this setting overrides the data that the Client OS would otherwise return. Specify the complete FQDN, including hostname, such as `host.example.com` .	As necessary
LastInstall	Windows	REG_SZ	N/A	Date and time of latest Tanium Client installation.	No
LastGoodServerName	All supported	REG_SZ	STRING	The name of the Tanium Server or Zone Server with which the Tanium Client last connected successfully. If the Client cannot reach a Server that the **ServerNameList** or **ServerName** setting specifies, the Client tries to connect to the Server that **LastGoodServerName** specifies. You do not set **LastGoodServerName** ; the Client defines it automatically.	No

©2026 Tanium Inc. All Rights Reserved

Setting Name	Applies to OS Platforms	Windows Registry Value Type	Non-Windows Setting Type	Description	Modify
				Tip: To avoid this fallback behavior during testing, troubleshooting, or migration scenarios, delete the **LastGoodServerName** value.	
ListenPort	All supported	REG_DWORD	NUMERIC	This setting specifies the port on which the Client listens for communication from peer Clients. By default, this setting is empty, and the Client listens for communication from peer Clients on the port specified for the **ServerPort** setting. When you configure a value for the **ListenPort** setting, it overrides the ServerPort on page 393 setting for communication between Clients. For more information and best practices, see Customize listening ports on page 274 .	As necessary
LogFileSize	All supported	REG_DWORD	NUMERIC	The size threshold in bytes that Tanium Client logs on page 364 must reach before the Client rotates them.	As necessary
LogPath	All supported	REG_SZ	STRING	By default, the Tanium Client writes its logs to the < *Tanium Client* >/Logs subdirectory. You can use the **LogPath** setting to define an alternative absolute path for the logs. For example: LogPath=/tmp .	As necessary
LogVerbosityLevel [1]	All supported	REG_DWORD	NUMERIC	The level of logging on an endpoint. The following values are best	As

©2026 Tanium Inc. All Rights Reserved

Setting Name	Applies to OS Platforms	Windows Registry Value Type	Non-Windows Setting Type	Description	Modify
				practices for specific scenarios: • `1` (default): Use this value during normal operation. • `41`: Use this value during troubleshooting. • `91` or higher: Use this value for full logging, for short periods of time only. **Note:** A value of `0` disables logging. As a best practice, do not disable logging. **Note:** By default, this setting is not present if you did not set the logging level when deploying the Tanium Client.	necessary

©2026 Tanium Inc. All Rights Reserved

Setting Name	Applies to OS Platforms	Windows Registry Value Type	Non-Windows Setting Type	Description	Modify
				Tip: • You can ask a question using the `Tanium Client Logging Level` sensor to determine the log verbosity level on endpoints. • If you are using a package to configure this setting, you can use the **Set Windows Tanium Client Logging Level** or **Set Tanium Client Logging Level [Non-Windows]** package.	
Logs.extensions.LogVerbosityLevel [1]	All Supported	REG_DWORD	NUMERIC	The level of logging for Client Extensions (such as the Tanium™ Client Recorder Extension and Tanium™ Index) on an endpoint. The following values are best practices for specific scenarios: • `11` (default): Use this value during normal operation. • `41`: Use this value during troubleshooting. • `91` or higher: Use this value for full logging, for short periods of time only.	

©2026 Tanium Inc. All Rights Reserved

Setting Name	Applies to OS Platforms	Windows Registry Value Type	Non-Windows Setting Type	Description	Modify
				Note: A value of `0` disables logging. As a best practice, do not disable logging.	
Path	Windows	REG_SZ	N/A	Path to the Tanium Client installation directory on page 490 . If none is specified, the Tanium Client assumes the default path for the OS. **Tip:** For Linux, Solaris, and AIX, you can use symbolic links. For more information, see the following sections: • Move an existing installation of the Tanium Client on Linux on page 314 • Move an existing installation of the Tanium Client on Solaris on page 316 • Move an existing installation of the Tanium Client on AIX on page 317	As necessary
PeerNeighborhood	All Supported	REG_SZ	STRING	A neighborhood name that designates Clients that should be	

©2026 Tanium Inc. All Rights Reserved

Setting Name	Applies to OS Platforms	Windows Registry Value Type	Non-Windows Setting Type	Description	Modify
				allowed to peer regardless of NAT IP. For more information, see Configure intentional subnets on page 260 .	
ProxyAutoConfigAddress	Windows	REG_SZ	N/A	The URL and file name (in the format `http[s]://<PAC file URL>/<PAC file name>.pac`) of a proxy auto configuration (PAC) file that the Tanium Client can access. The PAC file defines how Clients connect to the Tanium Server or Zone Server: directly or through a Hypertext Transfer Protocol Secure (HTTPS) proxy server. The Client downloads the file from the URL that you specify and runs a script that the file contains to select the correct proxy for connecting to a particular Server. If no proxy is available, the Client falls back to connecting directly with the Tanium Server or Zone Server. For more information, see Configure proxy connections during Client deployment with a PAC file (Windows endpoints only) on page 242 .	As necessary
ProxyAutoDetect	Windows	REG_DWORD	NUMERIC	Enables detection of an existing proxy configuration from the Windows registry on an endpoint. Set a value of `1` to enable. Omit this setting or set a value of `0` to disable.	As necessary
ProxyServers	All supported	REG_SZ	STRING	The IP address or FQDN, and port number, of the HTTPS proxy server through which the Tanium Client connects to the Tanium	As necessary

©2026 Tanium Inc. All Rights Reserved

Setting Name	Applies to OS Platforms	Windows Registry Value Type	Non-Windows Setting Type	Description	Modify
				Server or Zone Server . You can specify multiple proxies as a comma-separated list in the format "`<proxy1>:<port>,...,<proxyN>:<port>`". The Client tries to connect to the proxies in the order that you list them. After any single connection succeeds, the Client stops trying to connect with more proxies. If no proxy is available, the Client falls back to connecting directly with the Tanium Server or Zone Server . For more information, see Configure specific proxy servers during Client deployment on page 241 .	
RandomListeningPortExclusions	All supported	REG_DWORD	NUMERIC	Specifies ports that the Client never selects as a listening port if you enable **EnableRandomListeningPort** . For example, to prevent port competition conflicts, you might specify ports that other applications use. If you specify multiple exclusions, use a comma to separate each port. By default, the Client does not exclude any ports that are within the range that the **RandomListeningPortMin** and **RandomListeningPortMax** settings define. For more information and best practices, see Customize listening ports on page 274 .	As necessary
RandomListeningPortMax	All supported	REG_DWORD	NUMERIC	Specifies the high end of the range of ports from which the Client randomly selects a listening port if you enabled **EnableRandomListeningPort** . The default is port `64000` . For	As necessary

©2026 Tanium Inc. All Rights Reserved

Setting Name	Applies to OS Platforms	Windows Registry Value Type	Non-Windows Setting Type	Description	Modify
				more information and best practices, see Customize listening ports on page 274 .	
RandomListeningPortMin	All supported	REG_DWORD	NUMERIC	Specifies the low end of the range of ports from which the Client randomly selects a listening port if you enabled **EnableRandomListeningPort** . The default is port `32000` . For more information and best practices, see Customize listening ports on page 274 .	As necessary
RandomListeningPortTTLInHours	All supported	REG_DWORD	NUMERIC	Specifies the interval in hours at which the Client selects a new listening port if you enabled **EnableRandomListeningPort** . The default is `24` hours. Do not set the value lower than the Client reset interval, which by default is a random interval in the range of 2 to 6 hours. For more information and best practices, see Customize listening ports on page 274 .	As necessary
RegistrationCount	All supported	REG_DWORD	NUMERIC	Count of completed registrations. This value, in conjunction with the **ComputerID** , enables the Tanium Server to detect duplicate Computer IDs. If the **RegistrationCount** value that the Tanium Server maintains does not match the value that the Client reports, the Server assigns a new, unique **ComputerID** to the endpoint to resolve the apparent **ComputerID** duplication. For more	No

©2026 Tanium Inc. All Rights Reserved

Setting Name	Applies to OS Platforms	Windows Registry Value Type	Non-Windows Setting Type	Description	Modify
				information, see Information about registration and ComputerID (all operating systems) on page 194 .	
RegistrationSecret	All supported	REG_SZ	STRING	Indicates that the encrypted public key used to authenticate with the Tanium Server is present. The encrypted key is shown only when you use the `config list-protected` command. Otherwise, this setting shows the value `(protected)` when the key is present and can be decrypted. **Note:** Non-Windows: If you are signed in as a non-root user, this setting reports the error `Error applying configuration: Failed to finalize decryption` because the key cannot be decrypted in the context of the current user. This is not an issue for normal Tanium Client operation. However, if you need to reset the public key to troubleshoot connection issues, you must use the `sudo` command and set the `HOME` environment variable appropriately. For more information, see Review or reset the public key to troubleshoot connection issues on page 373 .	No
ReportingTLSMode, OptionalTLSMinAttemptCount, OptionalTLSBackoffIntervalSeconds, OptionalTLSMaxBackoffSeconds, Server_ReportingTLSMode,	All supported	REG_DWORD	NUMERIC	Tanium Core Platform supports TLS communication for connections from Tanium Clients to the Tanium Server or Zone Server and for communication between Tanium Client peers. For more information, see the Securing Tanium Server, Zone Server, and Tanium Client access or Securing Tanium Server, Zone Server,	As necessary

©2026 Tanium Inc. All Rights Reserved

Setting Name	Applies to OS Platforms	Windows Registry Value Type	Non-Windows Setting Type	Description	Modify
Server_OptionalTLSMinAttemptCount, Server_OptionalTLSBackoffIntervalSeconds, Server_OptionalTLSMaxBackoffSeconds				and Tanium Client access .	
Resolver	Non-Windows	N/A	STRING	Program to invoke for resolving the IP address of the Tanium Server . The default is getent . For AIX and Solaris, set this to nslookup . The options are as follows: getent , getenta , host , nslookup , dig , and res_search .	As necessary
ServerName	All supported	REG_SZ	STRING	FQDN or IP address of the Tanium Server or Zone Server with which the Client tries to connect. For more information, see ServerName on page 231 . **Best Practice:** If you are manually configuring this setting, specify an FQDN. **Tip:** If you are using a package to configure this setting, you can use the **Set Tanium Server Name** or **Set Tanium Server Name [Non-Windows]** package.	As necessary
ServerNameList	All supported	REG_SZ	STRING	Comma-separated list of Tanium Server and Zone Server FQDNs or IP addresses with which the Client can try to connect. For more	As necessary

©2026 Tanium Inc. All Rights Reserved

Setting Name	Applies to OS Platforms	Windows Registry Value Type	Non-Windows Setting Type	Description	Modify
				information, see ServerNameList on page 230 .  **Best Practice:** Specify FQDNs for this setting. **Tip:** If you are using a package to configure this setting, you can use the **Set Tanium Server Name List** or **Set Tanium Server Name List [Non-Windows]** package.	
ServerPort	All supported	REG_DWORD	NUMERIC	The port to use for client-server and, by default, client-client communication. The default is 17472. For more information, see ServerPort on page 232 .  **Note:** If you configure the ListenPort on page 393 or EnableRandomListeningPort on page 393 setting, it overrides **ServerPort** for client-client communication. For more information, see Customize listening ports on page 274 .	As necessary
StateProtectedFlag	All supported	REG_DWORD	NUMERIC	Enables encryption of the Client state and sensor queries stored on the Client	As necessary

©2026 Tanium Inc. All Rights Reserved

Setting Name	Applies to OS Platforms	Windows Registry Value Type	Non-Windows Setting Type	Description	Modify
				Note: By default, read access to the Tanium Client directory is restricted for non-Administrators. However, encrypting the Client state and sensor queries can provide additional protection. For information about additional measures to protect the Tanium Client on Windows endpoints, see Manage Client Service Hardening features on page 300 .	
Version	All supported	REG_SZ	STRING	Tanium Client version number.	No

[1] You can apply this setting using a settings configuration in Tanium Client Management. For more information, see Managing Client settings in Client Management on page 324 .

Tuning Tanium Client settings for VDI endpoints and other endpoints with limited resources

©2026 Tanium Inc. All Rights Reserved

Tip: For information about creating an image with the Tanium Client for VDI environments, see Preparing the Tanium Client on a virtual desktop infrastructure (VDI) instance on page 209.

If you are deploying the Tanium Client to virtual desktop infrastructure (VDI) instances or other endpoints with limited resources, you might need to adjust certain Client settings to help to reduce resource usage. The following table lists the best practice adjustments to Client settings for VDI instances. These settings help avoid concentrated resource usage on shared hardware. All settings in the following table are of the registry type REG_DWORD for Windows, or of the type NUMERIC for non-Windows. For information about reviewing and modifying Client settings, see Managing Client settings and Index configurations on page 318.

Best practice Client settings for VDI instances

Client Setting	Default Value	Best Practice Value for VDI	Explanation
RandomSensorDelayInSeconds	0	5	By default, sensors run immediately. This setting delays the execution of any sensor by a random time up to 5 seconds, which reduces concurrent execution of sensors and packages. **Note:** If poor performance occurs on VDI infrastructure, you can increase this value incrementally up to `20`.
MaxAgeMultiplier	1	2	Each sensor has a **Max Sensor Age** setting that determines how long the Client caches sensor results for subsequent questions that include the same sensor. This setting causes the Client to multiply the maximum age configured for each sensor by 2, which doubles the time results are cached for each sensor and reduces sensor executions.

©2026 Tanium Inc. All Rights Reserved

Client Setting	Default Value	Best Practice Value for VDI	Explanation
MinDistributeOverTimeInSeconds	0	60	Each action has a **Distribute Over** setting that randomizes the distribution of that action over the specified time. By default, no minimum applies, and some actions might be configured for immediate distribution. This setting forces all actions to distribute over at least 1 minute.
SaveClientStateIntervalInSeconds	300	1800	By default, the Client state is written to disk every 5 minutes. This setting increases the time to 30 minutes to reduce disk writes.



Best Practice: To minimize disk writes, leave **LogVerbosityLevel** and **Logs.extensions.LogVerbosityLevel** set to their default values of `1` and `11` respectively. Do not disable logging.

Tip: You can apply these settings using a settings configuration in Tanium Client Management. For more information, see Managing Client settings in Client Management on page 324.

©2026 Tanium Inc. All Rights Reserved

Best Practice:

Configure isolated subnets for virtual desktop infrastructure (VDI) instances in a high-density environment with shared storage or for any other virtual endpoints where concurrent disk I/O operations must be limited. Endpoints cache file chunks to share distributed files with peers, which requires multiple endpoints in the linear chain to concurrently read and write file chunks. Isolating an endpoint reduces the concurrent disk I/O that normally occurs when this cache is used to share files with peers. For more information, see File distribution.

For the configuration steps, see Configure isolated subnets on page 255.

To identify existing VDI Clients for tuning, ask a question appropriate for your environment, and then drill down as necessary. The following table lists example questions that you might ask to identify VDI clients.

Example questions to identify VDI Clients

Identification method	Example question

Model	`Get Is Virtual from all machines with Is Virtual equals yes`
	`Get Chassis Type from all machines with Chassis Type contains virtual`
	`Get Model from all machines with Model contains Standard PC`

Host name	`Get Computer Name contains VM-PC- from all machines`
Active Directory attributes	`Get AD Query - Computer Attributes[Description] contains " VDI " from all machines` `Get AD Query - Computer Groups equals VDI from all machines`
MAC address	`Get MAC Address starts with "00:1c:42" from all machines`

©2026 Tanium Inc. All Rights Reserved

Identification method	Example question
IP address	`Get Tanium Client Subnet matches "^192\.168\.(14|16|88|222)\.0\/23$" from all machines` `Get IP Address matches "^192\.168\.[0-2]\.\d{1,3}$" from all machines`
Hardware	`Get Disk Drive Details having Disk Drive Details:Name equals QEMU HARDDISK ATA Device from all machines`

Tip: To help simplify management of VDI endpoints, consider creating computer groups with custom tag-based membership and applying corresponding custom tags to VDI endpoints. For more information, see Manage custom tags for computer groups.

You can also adjust these settings to increase performance on physical endpoints with hardware specifications near the minimum requirements for the Tanium Client on page 45, cloud-hosted endpoints, and endpoints where CPU performance must be prioritized, but the appropriate values depend on your environment and business requirements. For assistance with tuning these settings, contact Tanium Support on page 392.

The performance of certain features in some Tanium solutions also depends on the resources available on endpoints. For links to requirements for specific Tanium solutions, see Module and service requirements on page 47.

Peering settings reference

When Tanium Clients register with the Tanium Server, they also receive values for settings that relate to peering and sensor data. Clients write these settings to the `Status` registry subkey on Windows endpoints and to the SQLite database (client.db) on non-Windows

©2026 Tanium Inc. All Rights Reserved

endpoints. You do not edit these settings, but their values might help you understand expected behavior when troubleshooting peering. You can ask questions to see the values of some of these settings. For more information, see Use questions to review peering settings on page 271. Contact Tanium Support on page 392 for more assistance.

Tanium Client peer settings

Setting Name	Description
BackPeerAddress	Address details for the current backward peer. Use the **Tanium Back Peer Address** sensor (**Client Management** content set) to see the value for this setting.
BackPreviousPeerAddress	Address details for the previous backward peer.
BufferCount	Number of buffered messages that are currently queued for the Tanium Client to process. Use the **Tanium Buffer Count** sensor (**Client Management** content set) to see the value for this setting.
ClientAddress	Address details for the Client host endpoint. Use the **Tanium Client IP Address** sensor (**Base** content set) to see the value for this setting.
NeighborhoodList	Connection details that the Tanium Server provides for up to ten forward and ten backward peers. Use the **Tanium Client Neighborhood** sensor (**Client Management** content set) to see neighborhood information.
PeerAddress	Address details for the current forward peer. Use the **Tanium Peer Address** sensor (**Client Management** content set) to see the value for this setting.
PreviousPeerAddress	Address details for the previous forward peer.
StaleCount	Count of sensors with stale data.
StaleList	List of sensors with stale data.

©2026 Tanium Inc. All Rights Reserved

Tanium Client command line interface (CLI)

CLI on Windows endpoints

Tanium Client settings are written to the Windows registry on page 491. The executable program for the CLI, TaniumClient.exe, is in the Tanium Client installation directory on page 490. The following examples demonstrate useful CLI commands:

- Display TaniumClient.exe syntax, commands, and options: `TaniumClient --help`
- Display the configuration (config) command syntax and actions: `TaniumClient config --help`
- Display the current configuration settings: `TaniumClient config list`

For the complete list of Client settings that are configurable using the CLI, see Tanium Client settings reference on page 393.

EXAMPLE 1: SET AND CONFIRM SERVER NAMES

The following example shows how to set and confirm the fully qualified domain names (FQDNs) of the Tanium Server with which the Tanium Client can connect in an active-active deployment:

```
cmd-prompt> TaniumClient config set ServerNameList ts1.tam.local,ts2.tam.local
cmd-prompt> TaniumClient config get ServerNameList
ts1.tam.local,ts2.tam.local
```

EXAMPLE 2: SET AND CONFIRM LOG VERBOSITY LEVEL

The following example shows how to configure the log verbosity level to level 41 for troubleshooting. Configuring this value using the CLI can be useful to help troubleshoot a Client that is not registering with the Tanium Server.

©2026 Tanium Inc. All Rights Reserved

```
cmd-prompt> TaniumClient config set LogVerbosityLevel 41
cmd-prompt> TaniumClient config get LogVerbosityLevel
41
```

EXAMPLE 3: REQUIRE TLS

The following example shows how to configure the connection between Tanium Client and the Tanium Server to require TLS, and then to confirm that TLS is required:

```
cmd-prompt> TaniumClient config set TLSMode 1
cmd-prompt> TaniumClient config get TLSMode
1
```

CLI on non-Windows endpoints

Tanium Client settings are written to an SQLite database. The executable program for the CLI, TaniumClient, is in the Tanium Client installation directory on page 490. You must either run it as root or use `sudo` to elevate permissions. The following examples demonstrate useful CLI commands:

- Display TaniumClient syntax, commands, and options: `sudo ./TaniumClient --help`
- Display the configuration (config) command syntax and actions: `sudo ./TaniumClient config -h`
- Display the current configuration settings: `sudo ./TaniumClient config list`

For the complete list of Client settings that are configurable using the CLI, see Tanium Client settings reference on page 393.

The following example shows how to set and confirm the FQDNs of the Tanium Server with which the Tanium Client can connect in an active-active deployment:

```
cmd-prompt> sudo ./TaniumClient config set ServerNameList ts1.tam.local,ts2.tam.local
cmd-prompt> sudo ./TaniumClient config get ServerNameList
```

©2026 Tanium Inc. All Rights Reserved

```
ts1.tam.local,ts2.tam.local
```

The following example shows how to configure the connection between Tanium Client and the Tanium Server to require TLS, and then to confirm that TLS is required:

```
cmd-prompt> sudo ./TaniumClient config set TLSMode 1
cmd-prompt> sudo ./TaniumClient config get TLSMode
1
```

©2026 Tanium Inc. All Rights Reserved

Reference: Endpoint security exclusions

If antivirus (AV) or other security software is in use in the environment to monitor and block unknown host system processes, Tanium requires that a security administrator create exclusions to allow the Tanium processes to run without interference. This software can include security applications that are included with an endpoint operating system, such as fapolicyd on some Linux distributions, or Microsoft Defender on Windows. You might need to exclude the Tanium Client installation directories from real-time inspection on some AV or other host-based security software. Typically, you also configure a policy to ignore the input and output of Tanium binaries. How you configure these exclusions varies based on your security software.



Note:

- In certain implementations, creating the security exclusions and optimizations described in the following sections might increase the attack vulnerability of a system and might expose devices to various security threats. Using advanced AV software that permits detailed exclusions potentially reduces risk while limiting Tanium performance impacts. Tanium recommends rigorously testing any exclusions or optimizations in a lab environment to thoroughly understand any impact on security and performance before implementation. Tanium also strongly recommends that you involve your AV vendor and security teams in reviewing these guidelines before applying them.
- If the required exclusions are not configured, or if Tanium suspects interference from AV or security software, Tanium might require you to remove or disable the AV or security software temporarily for the purposes of troubleshooting and restore it once troubleshooting is complete.

©2026 Tanium Inc. All Rights Reserved

Important: For the additional security exclusions that apply to Tanium Core Platform Servers in a Windows-based deployment, see Tanium Core Platform Server security exclusions.

Tanium Client folders

If you plan to implement exclusions on a folder-by-folder basis, the following table lists Tanium Client folders that Tanium requires AV and other host-based security applications exclude from real-time scans. Include subfolders of these locations when you create the exception rules.

Note: Whenever a new action runs on a managed endpoint, the Tanium Client adds a subfolder to contain the associated package files. The parent folder is *<Tanium Client installation folder>*/Downloads and the subfolder is named Action_*<ID>*, where *<ID>* is the action identifier. Include the Action_*<ID>* subfolders when you create exception rules for Tanium Clients.

The listed folder paths are the defaults. If you changed the folder locations to non-default paths, create rules based on the actual locations.

Security exclusions for Tanium Client folders Download as CSV

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows x86		Folder	C:\Program Files\Tanium\Tanium Client
Windows x64		Folder	C:\Program Files (x86)\Tanium\Tanium Client
macOS		Folder	/Library/Tanium/TaniumClient
Linux, Solaris, AIX		Folder	/opt/Tanium/TaniumClient

Important: For additional folder exclusions that Tanium requires during Tanium Client installation, see Security exclusions for Client Management on page 74.

Tanium Client system processes

©2026 Tanium Inc. All Rights Reserved

The following table lists Tanium Client system processes that Tanium requires allowing (not blocking, quarantining, or otherwise processing). The *<Tanium Client>* variable indicates the Client installation folder.

Security exclusions for Tanium Client processes Download as CSV

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows		Process	< *Tanium Client* >\TaniumClient.exe
		Process	< *Tanium Client* >\TaniumCX.exe
	Windows endpoints running Tanium Client 7.9.3	Process	< *Tanium Client* >\TaniumScriptRunner32.exe
		Process	< *Tanium Client* >\Tools\StdUtils\7za.exe
		Process	< *Tanium Client* >\Tools\StdUtils\runasuser.exe
		Process	< *Tanium Client* >\Tools\StdUtils\runasuser64.exe
		Process	< *Tanium Client* >\Tools\StdUtils\TaniumExecWrapper.exe
		Process	< *Tanium Client* >\Tools\StdUtils\TaniumFileInfo.exe
		Process	< *Tanium Client* >\Tools\StdUtils\TPowerShell.exe
macOS, Linux, Solaris, AIX		Process	< *Tanium Client* >/TaniumClient
		Process	< *Tanium Client* >/taniumclient
		Process	< *Tanium Client* >/TaniumCX
	macOS endpoints running the universal Tanium Client binary only	Process	< *Tanium Client* >/TaniumCX.app/Contents/MacOS/TaniumCX

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	< *Tanium Client* >/Tools/StdUtils/TaniumExecWrapper
		Process	< *Tanium Client* >/Tools/StdUtils/distribute-tools.sh

Note:

The following tools and files have specific requirements for the Tanium Client:

- Microsoft Group Policy Objects (GPO) or other central management tools for managing host firewalls: Tanium recommends creating rules to allow inbound and outbound TCP traffic across the port that the Client uses for Tanium traffic (default 17472) and port 17486 on any managed endpoints. For more information, see Network connectivity, ports, and firewalls on page 63.
- Windows Update offline scan file (Wsusscn2.cab): The Tanium Client uses Wsusscn2.cab to assess endpoints for installed or missing operating system and application security patches. If your endpoint security solutions scan archive files, see the Microsoft KB for information on configuring those tools to interact appropriately with the Wsusscn2.cab file.
- McAfee Host Intrusion Detection (in older versions of McAfee security software): Tanium recommends marking the Tanium Client as both **Trusted for Firewall** and Trusted for IPS.

Tanium binary file signers

Some security products base exclusion rules on file signers. Tanium uses an extended validation (EV) code-signing certificate with the following signers for the Tanium-generated binary files of Tanium Clients. Tanium also uses this certificate to sign VBS and PS1 files within action packages:

©2026 Tanium Inc. All Rights Reserved

Tanium binary file signers

Operating system	Signer
Windows	Files are signed by: Subject: jurisdictionC=US/jurisdictionST=Delaware/businessCategory=Private Organization/serialNumber=4332270, C=US, ST=CA, L=Emeryville, O=Tanium Inc., CN=Tanium Inc.
macOS	The following Apple developer ID is used to sign and notarize files: Tanium Inc. (TZTPM3VTUU)

Solution endpoint exclusions

The following sections list additional processes, folders, and files on

that Tanium requires a security administrator to configure as exclusions in security software to enable the latest versions of Tanium modules and shared services to work. To view version-specific exclusions for any Tanium solution, see the PDF Archive.

If the required exclusions are not configured, or if Tanium suspects interference from AV or security software, Tanium might require you to remove or disable the AV or security software temporarily for the purposes of troubleshooting and restore it once troubleshooting is complete.

Asset endpoint exclusions

Asset security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows	For integration with Flexera	Process	*<Tanium Client>* \Tools\EPI\TaniumEndpointIndex.exe
		File	*<Tanium Client>* \extensions\TaniumSoftwareManager.dll

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>* \extensions\TaniumSoftwareManager.dll.sig
		File	*<Tanium Client>* \TaniumClientExtensions.dll
		File	*<Tanium Client>* \TaniumClientExtensions.dll.sig
		File	<Tanium Client>\extensions\TaniumIndex.dll
		File	<Tanium Client>\extensions\TaniumIndex.dll.sig
		File	<Tanium Client>\extensions\index\index.db
		File	<Tanium Client>\extensions\index\index.db-shm
		File	<Tanium Client>\extensions\index\index.db-wal
		File	*<Tanium Client>* \extensions\SupportCX.dll
		File	*<Tanium Client>* \extensions\SupportCX.dll.sig
		File	*<Tanium Client>* \extensions\TaniumConfig.dll
		File	*<Tanium Client>* \extensions\TaniumConfig.dll.sig
macOS	For integration with Flexera	Process	*<Tanium Client>* /Tools/EPI/TaniumEndpointIndex
		File	*<Tanium Client>* /extensions/libTaniumSoftwareManager.dylib
		File	*<Tanium Client>* /extensions/libTaniumSoftwareManager.dylib.sig
		File	*<Tanium Client>* /libTaniumClientExtensions.dylib
		File	*<Tanium Client>* /libTaniumClientExtensions.dylib.sig
		File	<Tanium Client>/extensions/libTaniumIndex.dylib

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	<Tanium Client>/extensions/libTaniumIndex.dylib.sig
		File	<Tanium Client>/extensions/index/index.db
		File	<Tanium Client>/extensions/index/index.db-shm
		File	<Tanium Client>/extensions/index/index.db-wal
		File	*<Tanium Client>* /extensions/libSupportCX.dylib
		File	*<Tanium Client>* /extensions/libSupportCX.dylib.sig
		File	*<Tanium Client>* /extensions/libTaniumConfig.dylib
		File	*<Tanium Client>* /extensions/libTaniumConfig.dylib.sig
Linux	For integration with Flexera	Process	*<Tanium Client>* /Tools/EPI/TaniumEndpointIndex
		File	*<Tanium Client>* /extensions/libTaniumSoftwareManager.so
		File	*<Tanium Client>* /extensions/libTaniumSoftwareManager.so.sig
		File	*<Tanium Client>* /libTaniumClientExtensions.so
		File	*<Tanium Client>* /libTaniumClientExtensions.so.sig
		File	<Tanium Client>/extensions/libTaniumIndex.so
		File	<Tanium Client>/extensions/libTaniumIndex.so.sig
		File	<Tanium Client>/extensions/index/index.db
		File	<Tanium Client>/extensions/index/index.db-shm
		File	<Tanium Client>/extensions/index/index.db-wal

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>* /extensions/libSupportCX.so
		File	*<Tanium Client>* /extensions/libSupportCX.so.sig
		File	*<Tanium Client>* /extensions/libTaniumConfig.so
		File	*<Tanium Client>* /extensions/libTaniumConfig.so.sig

Benchmark endpoint exclusions

Benchmark security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Process
Windows		Process	*<Tanium Client>* \TaniumCX.exe
		File	*<Tanium Client>* \extensions\TaniumRisk.dll
		Folder	*<Tanium Client>* \Tools\CertificateManager
Linux		Process	*<Tanium Client>* /TaniumCX
		File	*<Tanium Client>* /libTaniumRisk.so
		Folder	*<Tanium Client>* /Tools/CertificateManager
macOS		Process	*<Tanium Client>* /TaniumCX
		File	*<Tanium Client>* /libTaniumRisk.dylib
		Folder	*<Tanium Client>* /Tools/CertificateManager

Certificate Manager endpoint exclusions

©2026 Tanium Inc. All Rights Reserved

Certificate Manager security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows		Folder	*<Tanium Client>* \python312
		File	*<Tanium Client>* \TPython\TPython.bat
		Folder	*<Tanium Client>* \TPython312
		Process	*<Tanium Client>* \python312\TPython.exe
		Process	*<Tanium Client>* \TaniumCX.exe
		Process	*<Tanium Client>* \Tools\StdUtils\TaniumExecWrapper.exe
		Folder	*<Tanium Client>* \Tools\CertificateManager
Linux		Process	*<Tanium Client>* /TPython/TPython
		Folder	*<Tanium Client>* /TPython312
		Process	*<Tanium Client>* /python312/python
		Process	*<Tanium Client>* /python312/bin/pybin
		Process	*<Tanium Client>* /TaniumCX
		Process	*<Tanium Client>* /Tools/StdUtils/TaniumExecWrapper
		Folder	*<Tanium Client>* /Tools/CertificateManager
macOS		Process	*<Tanium Client>* /TPython/TPython
		Folder	*<Tanium Client>* /TPython312
		Folder	*<Tanium Client>* /python312
		Process	*<Tanium Client>* /python312/python

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	*<Tanium Client>* /python312/bin/pybin
		Process	*<Tanium Client>* /TaniumCX
		Process	*<Tanium Client>* /Tools/StdUtils/TaniumExecWrapper
		Folder	*<Tanium Client>* /Tools/CertificateManager

Client Management endpoint exclusions

Client Management security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows	During Client installation; x64 endpoints	Process	C:\Program Files (x86)\Tanium\TaniumClientBootstrap.exe
	During Client installation; x64 endpoints	Process	C:\Program Files (x86)\Tanium\SetupClient.exe
	During Client upgrade; x64 endpoints	Process	C:\Program Files (x86)\Tanium\TaniumClientUpgrade\SetupClient.exe
	During Client installation; x86 endpoints	Process	C:\Program Files\Tanium\TaniumClientBootstrap.exe
	During Client installation; x86 endpoints	Process	C:\Program Files\Tanium\SetupClient.exe

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	During Client upgrade; x86 endpoints	Process	C:\Program Files\Tanium\TaniumClientUpgrade\SetupClient.exe
	During Client installation	Process	*<Tanium Client>* \SetupClient.exe
		File	*<Tanium Client>* \TaniumClientExtensions.dll
		File	*<Tanium Client>* \TaniumClientExtensions.dll.sig
		Process	*<Tanium Client>* \TaniumCX.exe
	Satellites used for Client deployment; installed on a satellite the first time you start a Client deployment that uses that satellite	File	*<Tanium Client>* \extensions\TaniumClientDeploy.dll
	Satellites used for Client deployment; installed on a satellite the first time you start a Client deployment that uses that satellite	File	*<Tanium Client>* \extensions\TaniumClientDeploy.dll.sig
	When Direct	File	*<Tanium Client>* \extensions\TaniumDEC.dll

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	Connect is installed		
	When Direct Connect is installed	File	*<Tanium Client>* \extensions\TaniumDEC.dll.sig
	When Discover is installed; satellite profiles only	File	*<Tanium Client>* \extensions\TaniumDiscover.dll
	When Discover is installed; satellite profiles only	File	*<Tanium Client>* \extensions\TaniumDiscover.dll.sig
	When Discover is installed; satellite profiles only	File	*<Tanium Client>* \extensions\TaniumExtras.dll
	When Discover is installed; satellite profiles only	File	*<Tanium Client>* \extensions\TaniumExtras.dll.sig
		File	*<Tanium Client>* \extensions\TaniumTSDB.dll
		File	*<Tanium Client>* \extensions\TaniumTSDB.dll.sig
	When	Folder	C:\Program Files\Npcap

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	Discover is installed; (Distributed level 3, distributed level 4, and satellite profiles only)		
	When Discover is installed; (Distributed level 3, distributed level 4, and satellite profiles only)	Process	*<Tanium Client>* \Tools\Discover\nmap\nmap.exe
	x86 endpoints	Process	*<Tanium Client>* \tools\driver\TaniumDriverCtl.exe
	x64 endpoints	Process	*<Tanium Client>* \tools\driver\TaniumDriverCtl64.exe
	x86 endpoints	Process	*<Tanium Client>* \tools\driver\TaniumDriverSvc.exe
	x64 endpoints	Process	*<Tanium Client>* \tools\driver\TaniumDriverSvc64.exe
		Process	*<Tanium Client>* \tools\driver\service\TaniumDriverSvc.exe
		File	*<Tanium Client>* \tools\driver\TaniumProcessMonitor.dll
		File	*<Tanium Client>* \tools\driver\TaniumProcessMonitor64.dll
macOS	During Client installation using the	File	*<Tanium Client>* /TaniumClient-*-universal.pkg

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	universal binary; * represents the Tanium Client version, which can be substituted where wildcards are not allowed.		
	During Client installation using the x64 binary; * represents the Tanium Client version, which can be substituted where wildcards are not allowed.	File	*<Tanium Client>* /TaniumClient-*-x64.pkg
	During upgrade of a Client using the universal binary; * represents the Tanium Client version, which can be substituted	File	*<Tanium Client>* /Downloads/TaniumClient-*-universal.pkg

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	where wildcards are not allowed.		
	During upgrade of a Client using the x64 binary; * represents the Tanium Client version, which can be substituted where wildcards are not allowed.	File	*<Tanium Client>* /Downloads/TaniumClient-*-x64.pkg
		File	*<Tanium Client>* /libTaniumClientExtensions.dylib
		File	*<Tanium Client>* /libTaniumClientExtensions.dylib.sig
		Process	*<Tanium Client>* /TaniumCX
	Endpoints running the universal Tanium Client binary	Process	*<Tanium Client>* /TaniumCX.app/Contents/MacOS/TaniumCX
	When Direct Connect is installed	File	*<Tanium Client>* /extensions/libTaniumDEC.dylib
	When Direct Connect is	File	*<Tanium Client>* /extensions/libTaniumDEC.dylib.sig

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	installed		
	When Discover is installed (Distributed level 3, distributed level 4, and satellite profiles only)	Process	*<Tanium Client>* /Tools/Discover/nmap/nmap
	When Discover is installed (Satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumDEC.dylib
	When Discover is installed (Satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumDEC.dylib.sig
	When Discover is installed (Satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumDiscover.dylib
	When Discover is installed (Satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumDiscover.dylib.sig

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	When Discover is installed (Satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumExtras.dylib
	When Discover is installed (Satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumExtras.dylib.sig
		File	*<Tanium Client>* /extensions/libTaniumTSDB.dylib
		File	*<Tanium Client>* /extensions/libTaniumTSDB.dylib.sig
Linux	During Client installation; <Installation-package-file> represents the .rpm or .deb file for the target Linux distribution. For more information see Tanium Client package files for Linux Tanium Client package files for Linux on	File	*<Tanium Client>* /<Installation-package-file>

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	page 175 .		
	During Client upgrade; <Installation-package-file> represents the .rpm or .deb file for the target Linux distribution. For more information, see Tanium Client package files for Linux Tanium Client package files for Linux on page 175 .	File	*<Tanium Client>* /downloads/<Installation-package-file>
		File	*<Tanium Client>* /libTaniumClientExtensions.so
		File	*<Tanium Client>* /libTaniumClientExtensions.so.sig
		Process	*<Tanium Client>* /TaniumCX
	Satellites used for Client deployment; installed on a satellite the first time you	File	*<Tanium Client>* /extensions/libTaniumClientDeploy.so

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	start a Client deployment that uses that satellite		
	Satellites used for Client deployment; installed on a satellite the first time you start a Client deployment that uses that satellite	File	*<Tanium Client>* /extensions/libTaniumClientDeploy.so.sig
	When Direct Connect is installed	File	*<Tanium Client>* /extensions/libTaniumDEC.so
	When Direct Connect is installed	File	*<Tanium Client>* /extensions/libTaniumDEC.so.sig
	When Discover is installed; (Distributed level 3, distributed level 4, and satellite profiles only)	Folder	*<Tanium Client>* /Tools/Discover/nmap/nmap
	When	File	*<Tanium Client>* /extensions/libTaniumDiscover.so

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	Discover is installed (Satellite profiles only)		
	When Discover is installed (Satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumDiscover.so.sig
	When Discover is installed (Satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumExtras.so
	When Discover is installed (Satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumExtras.so.sig
		File	*<Tanium Client>* /extensions/libTaniumTSDB.so
		File	*<Tanium Client>* /extensions/libTaniumTSDB.so.sig
Solaris	During Client installation on x86 endpoints; * represents the Tanium Client version, which can be	File	*<Tanium Client>* /TaniumClient-*-SunOS-5.10.i386.pkg.tar.gz

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	substituted where wildcards are not allowed.		
	During Client installation on SPARC endpoints; * represents the Tanium Client version, which can be substituted where wildcards are not allowed.	File	*<Tanium Client>* /TaniumClient-*-SunOS-5.10.sparc.pkg.tar.gz
	During Client upgrade on x86 endpoints; * represents the Tanium Client version, which can be substituted where wildcards are not allowed.	File	*<Tanium Client>* /downloads/TaniumClient-*-SunOS-5.10.i386.pkg.tar.gz
	During Client upgrade on SPARC endpoints; *	File	*<Tanium Client>* /downloads/TaniumClient-*-SunOS-5.10.sparc.pkg.tar.gz

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	represents the Tanium Client version, which can be substituted where wildcards are not allowed.		
AIX	During Client installation; * represents the Tanium Client version, which can be substituted where wildcards are not allowed.	File	*<Tanium Client>* /TaniumClient-*-powerpc.pkg
	During Client upgrade; * represents the Tanium Client version, which can be substituted where wildcards are not allowed.	File	*<Tanium Client>* /downloads/TaniumClient-*-powerpc.pkg

Client Management server exclusions

©2026 Tanium Inc. All Rights Reserved

Client Management security exclusions for Tanium Core Platform Servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	*<Module Server>* \services\client-management-service\node.exe
		Process	*<Module Server>* \services\client-profile-service\TaniumClientProfileService.exe
	When Direct Connect is installed	Process	*<Module Server>* \services\direct-connect-service\TaniumDirectConnectService.exe
	When Discover is installed	Process	*<Module Server>* \services\discover-service\node.exe
	When Discover is installed	Process	*<Module Server>* \plugins\content\discover-proxy\proxyplugin.exe
		Process	*<Module Server>* \services\endpoint-configuration-service\ TaniumEndpointConfigService.exe
		Process	*<Module Server>* \services\twsm-v1\twsm.exe
Zone Server	When Direct Connect is installed	Process	<Tanium Installation Directory>\Tanium Direct Connect Zone Proxy\node.exe
	When Direct Connect	Process	<Tanium Installation Directory>\Tanium Direct Connect Zone Proxy\twsm.exe

©2026 Tanium Inc. All Rights Reserved

Target Device	Notes	Exclusion Type	Exclusion
	is installed		

Comply endpoint exclusions

Tanium Client Management security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows		Process	*<Tanium Client>* \TaniumCX.exe
	Required if using the Tanium Scan Engine	File	*<Tanium Client>* \extensions\comply\engines\joval\Joval-Utilities.jar
		File	*<Tanium Client>* \TaniumClientExtensions.dll
		File	*<Tanium Client>* \TaniumClientExtensions.dll.sig
		File	*<Tanium Client>* \extensions\TaniumComply.dll
		File	*<Tanium Client>* \extensions\TaniumComply.dll.sig
		File	*<Tanium Client>* \extensions\comply\data\comply.db
		File	*<Tanium Client>* \extensions\comply\data\current-ciscat-config.json
		File	*<Tanium Client>* \extensions\comply\data\current-intel-config.json
		File	*<Tanium Client>* \extensions\comply\data\current-java-config.json
		File	*<Tanium Client>* \extensions\comply\data\current-joval-config.json
		File	*<Tanium Client>* \extensions\comply\data\current-scan-config.json
		File	*<Tanium Client>* \extensions\comply\

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
			downloads\download.db
		Process	*<Tanium Client>* \extensions\comply\jre\bin\java.exe
		File	*<Tanium Client>* \Tools\Comply\run-assessment.vbs
		File	*<Tanium Client>* \Tools\Comply\delete-assessment.vbs
Linux/macOS/AIX		Process	*<Tanium Client>* /TaniumCX
	Required if using the Tanium Scan Engine	File	*<Tanium Client>* /extensions/comply/engines/joval/Joval-Utilities.jar
		File	*<Tanium Client>* /libTaniumClientExtensions.so
		File	*<Tanium Client>* /libTaniumClientExtensions.so.sig
		File	*<Tanium Client>* /extensions/libTaniumComply.so
		File	*<Tanium Client>* /extensions/libTaniumComply.so.sig
		File	*<Tanium Client>* /extensions/comply/data/comply.db
		File	*<Tanium Client>* /extensions/comply/data/current-ciscat-config.json
		File	*<Tanium Client>* /extensions/comply/data/current-intel-config.json
		File	*<Tanium Client>* /extensions/comply/data/current-java-config.json
		File	*<Tanium Client>* /extensions/comply/data/current-joval-config.json
		File	*<Tanium Client>* /extensions/comply/data/current-scan-config.json
		File	*<Tanium Client>* /extensions/comply/downloads/download.db
		Process	*<Tanium Client>* /extensions/comply/jre/bin/java
		File	*<Tanium Client>* /Tools/Comply/run-assessment.sh

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>* /Tools/Comply/delete-assessment.sh
SCC engine - Windows		Process	*<Tanium Client>* \extensions\comply\engines\scc\cscc.exe
		Process	*<Tanium Client>* \extensions\comply\engines\scc\lib32\cscc32.exe
		Process	*<Tanium Client>* \extensions\comply\engines\scc\lib64\cscc64.exe
		Process	*<Tanium Client>* \extensions\comply\engines\scc\scc.exe
		Process	*<Tanium Client>* \extensions\comply\engines\scc\lib32\scc32.exe
		Process	*<Tanium Client>* \extensions\comply\engines\scc\lib64\scc64.exe
SCC engine - Linux/macOS		Process	*<Tanium Client>* /extensions/comply/engines/scc/cscc
		File	*<Tanium Client>* /extensions/comply/engines/scc/cscc.bin
		Process	*<Tanium Client>* /extensions/comply/engines/scc/scc
		File	*<Tanium Client>* /extensions/comply/engines/scc/scc.bin
CIS-CAT engine-all supported endpoints		File	*<Tanium Client>* /extensions/comply/engines/ciscat/CISCAT.jar
CIS-CAT engine-Linux		File	*<Tanium Client>* /extensions/comply/engines/ciscat/CIS-CAT.sh
CIS-CAT engine-Windows		File	*<Tanium Client>* \extensions\comply\engines\ciscat\CIS-CAT.BAT

Deploy endpoint exclusions

For Windows endpoints, review and follow the Microsoft antivirus security exclusion recommendations for enterprise computers. For more information, see Microsoft Support: Virus scanning recommendations for Enterprise computers that are running currently supported versions of Windows (KB822158).

©2026 Tanium Inc. All Rights Reserved

Deploy security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows		Folder	*<Tanium Client>* \python312
		Process	*<Tanium Client>* \python312\TPython.exe
		File	*<Tanium Client>* \TPython\TPython.bat
		Folder	*<Tanium Client>* \TPython312
		Process	*<Tanium Client>* \Tools\SoftwareManagement\7za.exe
		Process	*<Tanium Client>* \TaniumCX.exe
		File	*<Tanium Client>* \extensions\TaniumSoftwareManager.dll
		File	*<Tanium Client>* \extensions\TaniumSoftwareManager.dll.sig
		File	*<Tanium Client>* \Tools\SoftwareManagement\data\software-management.db
		File	*<Tanium Client>* \Tools\SoftwareManagement\data\software-management.db-wal
		File	*<Tanium Client>* \Tools\SoftwareManagement\data\software-management.db-shm
	When deployments run, installer files and other software package files are downloaded to subdirectories of this directory.	File	*<Tanium Client>* \Tools\SoftwareManagement\data\temp\tasks

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>* \extensions\TaniumPerformance.dll
		File	*<Tanium Client>* \extensions\TaniumPerformance.dll.sig
		Process	*<Tanium Client>* \Tools\PerformanceTSDB\TaniumTSDB.exe
		File	*<Tanium Client>* \extensions\TaniumTSDB.dll
		File	*<Tanium Client>* \extensions\TaniumTSDB.dll.sig
		File	*<Tanium Client>* \extensions\SupportCX.dll
		File	*<Tanium Client>* \extensions\SupportCX.dll.sig
		File	*<Tanium Client>* \extensions\TaniumConfig.dll
		File	*<Tanium Client>* \extensions\TaniumConfig.dll.sig
		File	*<Tanium Client>* \extensions\performance\data\performance.db
		File	*<Tanium Client>* \extensions\performance\data\performance.db-shm
		File	*<Tanium Client>* \extensions\performance\data\performance.db-wal
Linux		Folder	*<Tanium Client>* /python312
		Process	*<Tanium Client>* /python312/bin/pybin
		Process	*<Tanium Client>* /python312/python
		Process	*<Tanium Client>* /TPython/TPython
		Folder	*<Tanium Client>* /TPython312
		Process	*<Tanium Client>* /TaniumCX
		File	*<Tanium Client>* /Tools/SoftwareManagement/data/software-management.db
		File	*<Tanium Client>* /Tools/SoftwareManagement/data/software-management.db-wal

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>* /Tools/SoftwareManagement/data/software-management.db-shm
	When deployments run, installer files and other software package files are downloaded to subdirectories of this directory.	File	*<Tanium Client>* /Tools/SoftwareManagement/data/temp/tasks
		File	*<Tanium Client>* /extensions/libTaniumSoftwareManager.so
		File	*<Tanium Client>* /extensions/libTaniumSoftwareManager.so.sig
		Process	*<Tanium Client>* /Tools/PerformanceTSDB/TaniumTSDB
		File	*<Tanium Client>* /extensions/libTaniumTSDB.so
		File	*<Tanium Client>* /extensions/libTaniumTSDB.so.sig
		File	*<Tanium Client>* /libTaniumClientExtensions.so
		File	*<Tanium Client>* /libTaniumClientExtensions.so.sig
		File	*<Tanium Client>* /extensions/libTaniumPerformance.so
		File	*<Tanium Client>* /extensions/libTaniumPerformance.so.sig
		File	*<Tanium Client>* /extensions/libSupportCX.so
		File	*<Tanium Client>* /extensions/libSupportCX.so.sig

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>* /extensions/libTaniumConfig.so
		File	*<Tanium Client>* /extensions/libTaniumConfig.so.sig
		File	*<Tanium Client>* /extensions/performance/data/performance.db
		File	*<Tanium Client>* /extensions/performance/data/performance.db-shm
		File	*<Tanium Client>* /extensions/performance/data/performance.db-wal
macOS	When deployments run, installer files and other software package files are downloaded to subdirectories of this directory.	File	*<Tanium Client>* /Tools/SoftwareManagement/data/temp/tasks
		Folder	*<Tanium Client>* /python312
		Process	*<Tanium Client>* /python312/bin/pybin
		Process	*<Tanium Client>* /python312/python
		Process	*<Tanium Client>* /TPython/TPython
		Folder	*<Tanium Client>* /TPython312
		Process	*<Tanium Client>* /TaniumCX
		File	*<Tanium Client>* /extensions/libTaniumSoftwareManager.dylib

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>* /extensions/libTaniumSoftwareManager.dylib.sig
		File	*<Tanium Client>* /Tools/SoftwareManagement/data/software-management.db
		File	*<Tanium Client>* /Tools/SoftwareManagement/data/software-management.db-wal
		File	*<Tanium Client>* /Tools/SoftwareManagement/data/software-management.db-shm
	When deployments run, installer files and other software package files are downloaded to subdirectories of this directory.	File	*<Tanium Client>* /Tools/SoftwareManagement/data/temp/tasks
		Process	*<Tanium Client>* /Tools/PerformanceTSDB/TaniumTSDB
		File	*<Tanium Client>* /extensions/libTaniumTSDB.dylib
		File	*<Tanium Client>* /extensions/libTaniumTSDB.dylib.sig
		File	*<Tanium Client>* /libTaniumClientExtensions.dylib
		File	*<Tanium Client>* /libTaniumClientExtensions.dylib.sig
		File	*<Tanium Client>* /extensions/libTaniumPerformance.dylib
		File	*<Tanium Client>* /extensions/libTaniumPerformance.dylib.sig
		File	*<Tanium Client>* /extensions/libSupportCX.dylib

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>* /extensions/libSupportCX.dylib.sig
		File	*<Tanium Client>* /extensions/libTaniumConfig.dylib
		File	*<Tanium Client>* /extensions/libTaniumConfig.dylib.sig
		File	*<Tanium Client>* /extensions/performance/data/performance.db
		File	*<Tanium Client>* /extensions/performance/data/performance.db-shm
		File	*<Tanium Client>* /extensions/performance/data/performance.db-wal

Direct Connect endpoint exclusions

Direct Connect security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows		File	*<Tanium Client>* \TaniumClientExtensions.dll
		File	*<Tanium Client>* \TaniumClientExtensions.dll.sig
		File	*<Tanium Client>* \extensions\TaniumDEC.dll
		File	*<Tanium Client>* \extensions\TaniumDEC.dll.sig
		Process	*<Tanium Client>* \TaniumCX.exe
macOS		File	*<Tanium Client>* /libTaniumClientExtensions.dylib
		File	*<Tanium Client>* /libTaniumClientExtensions.dylib.sig
		File	*<Tanium Client>* /extensions/libTaniumDEC.dylib
		File	*<Tanium Client>* /extensions/libTaniumDEC.dylib.sig

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	*<Tanium Client>* /TaniumCX
Linux		File	*<Tanium Client>* /libTaniumClientExtensions.so
		File	*<Tanium Client>* /libTaniumClientExtensions.so.sig
		File	*<Tanium Client>* /extensions/libTaniumDEC.so
		File	*<Tanium Client>* /extensions/libTaniumDEC.so.sig
		Process	*<Tanium Client>* /TaniumCX

Discover endpoint exclusions

Discover security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows		Process	*<Tanium Client>* \TaniumCX.exe
		File	*<Tanium Client>* \TaniumClientExtensions.dll
		File	*<Tanium Client>* \TaniumClientExtensions.dll.sig
		File	*<Tanium Client>* \extensions\SupportCX.dll
		File	*<Tanium Client>* \extensions\SupportCX.dll.sig
		File	*<Tanium Client>* \extensions\TaniumConfig.dll
		File	*<Tanium Client>* \extensions\TaniumConfig.dll.sig
		File	*<Tanium Client>* \extensions\discover\data\discover.db
		File	*<Tanium Client>* \extensions\discover\data\discover.db-wal

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>* \extensions\discover\data\discover.db-shm
	(Distributed level 3, distributed level 4, and satellite profiles only)	Folder	C:\Program Files\Npcap
	(Distributed level 3, distributed level 4, and satellite profiles only)	Process	*<Tanium Client>* \Tools\Discover\nmap\nmap.exe
	(When Direct Connect is installed; satellite profiles only)	File	*<Tanium Client>* \extensions\TaniumDEC.dll
	(When Direct Connect is installed; satellite profiles only)	File	*<Tanium Client>* \extensions\TaniumDEC.dll.sig
	(Satellite profiles only)	File	*<Tanium Client>* \extensions\TaniumDiscover.dll
	(Satellite profiles only)	File	*<Tanium Client>* \extensions\TaniumDiscover.dll.sig
	(Satellite profiles only)	File	*<Tanium Client>* \extensions\TaniumExtras.dll
	(Satellite profiles only)	File	*<Tanium Client>* \extensions\TaniumExtras.dll.sig
Linux		Process	*<Tanium Client>* /TaniumCX
		File	*<Tanium Client>* /libTaniumClientExtensions.so
		File	*<Tanium Client>* /libTaniumClientExtensions.so.sig
		File	*<Tanium Client>* /extensions/libSupportCX.so
		File	*<Tanium Client>* /extensions/libSupportCX.so.sig
		File	*<Tanium Client>* /extensions/libTaniumConfig.so
		File	*<Tanium Client>* /extensions/libTaniumConfig.so.sig
		File	*<Tanium Client>* /extensions/discover/data/discover.db
		File	*<Tanium Client>* /extensions/discover/data/discover.db-wal

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>* /extensions/discover/data/discover.db-shm
	(Distributed level 3, distributed level 4, and satellite profiles only)	Process	*<Tanium Client>* /Tools/Discover/nmap/nmap
	(When Direct Connect is installed; satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumDEC.so
	(When Direct Connect is installed; satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumDEC.so.sig
	(Satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumDiscover.so
	(Satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumDiscover.so.sig
	(Satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumExtras.so
	(Satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumExtras.so.sig
macOS		Process	*<Tanium Client>* /TaniumCX
		File	*<Tanium Client>* /libTaniumClientExtensions.dylib
		File	*<Tanium Client>* /libTaniumClientExtensions.dylib.sig
		File	*<Tanium Client>* /extensions/libSupportCX.dylib
		File	*<Tanium Client>* /extensions/libSupportCX.dylib.sig
		File	*<Tanium Client>* /extensions/libTaniumConfig.dylib
		File	*<Tanium Client>* /extensions/libTaniumConfig.dylib.sig
		File	*<Tanium Client>* /extensions/discover/data/discover.db
		File	*<Tanium Client>* /extensions/discover/data/discover.db-wal
		File	*<Tanium Client>* /extensions/discover/data/discover.db-shm

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	(Distributed level 3, distributed level 4, and satellite profiles only)	Process	*<Tanium Client>* /Tools/Discover/nmap/nmap
	(When Direct Connect is installed; satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumDEC.dylib
	(When Direct Connect is installed; satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumDEC.dylib.sig
	(Satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumDiscover.dylib
	(Satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumDiscover.dylib.sig
	(Satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumExtras.dylib
	(Satellite profiles only)	File	*<Tanium Client>* /extensions/libTaniumExtras.dylib.sig

End-User Notifications endpoint exclusions

End-User Notifications security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows		Folder	*<Tanium Client>* \python312
		Process	*<Tanium Client>* \python312\TPython.exe
		File	*<Tanium Client>* \TPython\TPython.bat
		Folder	*<Tanium Client>* \TPython312
		Process	<Parent of Tanium Client directory>\Tanium End User Notification Tools\UserSessionProxy.exe
		Process	<Parent of Tanium Client directory>\Tanium End User Notification Tools\bin\end-user-notifications.exe

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	Exclude from on-access or real-time scans	Folder	<Parent of Tanium Client directory>\Tanium End User Notification Tools
	64-bit OS versions	Folder	*<Tanium Client>* \Tools\EndUserNotifications\scripts
	64-bit OS versions	File	*<Tanium Client>* \Tools\EndUserNotifications\scripts\config.vbs
	64-bit OS versions	File	*<Tanium Client>* \Tools\EndUserNotifications\scripts\remove-end-user-notifications.vbs
	64-bit OS versions	File	*<Tanium Client>* \Tools\EndUserNotifications\scripts\is-self-service-enabled.vbs
macOS		Folder	*<Tanium Client>* /python312
		Process	*<Tanium Client>* /python312/bin/pybin
		Process	*<Tanium Client>* /python312/python
		Process	*<Tanium Client>* /TPython/TPython
		Folder	*<Tanium Client>* /TPython312
		Process	/Library/Tanium/EndUserNotifications/bin/end-user-notifications.app
		Process	(End-User Notifications 1.18.57 and later) /Library/Tanium/EndUserNotifications/bin/Launcher.app
		Folder	/Library/Tanium/EndUserNotifications

Enforce endpoint exclusions

©2026 Tanium Inc. All Rights Reserved

Enforce security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows		Process	*<Tanium Client>* \Tools\StdUtils\7za.exe
	x86 endpoints	Process	*<Tanium Client>* \Tools\Enforce\devcon32.exe
	x64 endpoints	Process	*<Tanium Client>* \Tools\Enforce\devcon64.exe
		Process	*<Tanium Client>* \Tools\Enforce\LocalPolicyTool.exe
		Folder	*<Tanium Client>* \python312
		File	*<Tanium Client>* \TPython\TPython.bat
		Folder	*<Tanium Client>* \TPython312
		Process	*<Tanium Client>* \python312\TPython.exe
		Process	*<Tanium Client>* \TaniumClient.exe
		Process	*<Tanium Client>* \TaniumCX.exe
		Process	*<Tanium Client>* \Tools\recorder\TaniumRecorderCtl.exe
		File	*<Tanium Client>* \extensions\TaniumRecorder.dll
		File	*<Tanium Client>* \extensions\TaniumRecorder.dll.sig
		File	*<Tanium Client>* \extensions\recorder\proc.bin
		File	*<Tanium Client>* \extensions\recorder\recorder.db
		File	*<Tanium Client>* \extensions\recorder\recorder.db-shm
		File	*<Tanium Client>* \extensions\recorder\recorder.db-wal
		File	C:\Windows\System32\drivers\TaniumRecorderDrv.sys

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	*<Tanium Client>* \tools\driver\service\ TaniumDriverSvc.exe
	x86 endpoints	Process	*<Tanium Client>* \tools\driver\TaniumDriverCtl.exe
	x86 endpoints	Process	*<Tanium Client>* \tools\driver\TaniumDriverSvc.exe
	x86 endpoints	File	*<Tanium Client>* \tools\driver\TaniumProcessMonitor.dll
	x64 endpoints	Process	*<Tanium Client>* \tools\driver\TaniumDriverCtl64.exe
	x64 endpoints	Process	*<Tanium Client>* \tools\driver\TaniumDriverSvc64.exe
	x64 endpoints	File	*<Tanium Client>* \tools\driver\ TaniumProcessMonitor64.dll
	x64 endpoints	File	C:\Windows\SysWOW64\TaniumProcessMonitor.dll
		Folder	*<Tanium Client>* \extensions\stream
macOS and Linux x86 and x64		Folder	*<Tanium Client>* /python312
		Process	*<Tanium Client>* /TPython/TPython
		Folder	*<Tanium Client>* /TPython312
		Process	*<Tanium Client>* /python312/python
		Process	*<Tanium Client>* /python312/bin/pybin
		Process	*<Tanium Client>* /TaniumClient
		Process	*<Tanium Client>* /TaniumCX

©2026 Tanium Inc. All Rights Reserved

Engage endpoint exclusions

Engage security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows		Process	*<Tanium Client>* \TaniumCX.exe
		File	*<Tanium Client>* \extensions\TaniumEndUser.dll
		Folder	<Parent of Tanium Client directory>\Tanium End User Notification Tools
macOS		Process	*<Tanium Client>* /TaniumCX
		Folder	/Library/Tanium/EndUserNotifications

Impact endpoint exclusions

Impact security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows		File	*<Tanium Client>* \TPython\TPython.bat
		Folder	*<Tanium Client>* \TPython312
		Process	*<Tanium Client>* \TPython312\TPython.exe
		Folder	*<Tanium Client>* \python312
		Process	*<Tanium Client>* \TaniumCX.exe
		File	*<Tanium Client>* \TaniumClientExtensions.dll
		File	*<Tanium Client>* \TaniumClientExtensions.dll.sig
	When Direct Connect is installed; satellite	File	*<Tanium Client>* \extensions\TaniumDEC.dll

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	sync only		
	When Direct Connect is installed; satellite sync only	File	*<Tanium Client>* \extensions\ TaniumDEC.dll.sig

Integrity Monitor endpoint exclusions

Integrity Monitor security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Process
Windows x86 and x64		File	<Tanium Client>\extensions\TaniumIndex.dll
		File	<Tanium Client>\extensions\TaniumIndex.dll.sig
		File	<Tanium Client>\extensions\TaniumIntegrityMonitor.dll
		File	<Tanium Client>\extensions\TaniumIntegrityMonitor.dll.sig
		File	<Tanium Client>\extensions\TaniumRecorder.dll
		File	<Tanium Client>\extensions\TaniumRecorder.dll.sig
		File	<Tanium Client>\extensions\recorder\proc.bin
		File	<Tanium Client>\extensions\recorder\recorder.db
		File	<Tanium Client>\extensions\recorder\recorder.db-shm
		File	<Tanium Client>\extensions\recorder\recorder.db-wal
		File	<Tanium Client>\extensions\index\index.db
		File	<Tanium Client>\extensions\index\index.db-shm

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Process
		File	<Tanium Client>\extensions\index\index.db-wal
		File	<Tanium Client>\TaniumClientExtensions.dll
		File	<Tanium Client>\TaniumClientExtensions.dll.sig
	Endpoints with Toolset version 2.7 or later	Folder	<Tanium Client>\python312
	Endpoints with Toolset version 2.7 or later	Folder	<Tanium Client>\TPython312
	Endpoints with a Toolset version earlier than 2.7	Process	<Tanium Client>\Python38\TPython.exe
	Endpoints with a Toolset version earlier than 2.7	Folder	<Tanium Client>\Python38
	Endpoints with	Process	<Tanium Client>\python312\TPython.exe

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Process
	Toolset version 2.7 or later		
		Process	<Tanium Client>\TaniumCX.exe
		Folder	<Tanium Client>\extensions\index
		Folder	<Tanium Client>\extensions\integrity-monitor
		File	C:\Windows\System32\drivers\TaniumRecorderDrv.sys
		File	C:\Windows\system32\drivers\TaniumProcessMonitor.dll
		Process	<Tanium Client>\tools\driver\service\TaniumDriverSvc.exe
	x86 endpoints	Process	<Tanium Client>\tools\driver\TaniumDriverCtl.exe
	x86 endpoints	Process	<Tanium Client>\tools\driver\TaniumDriverSvc.exe
	x86 endpoints	File	<Tanium Client>\tools\driver\TaniumProcessMonitor.dll
	x64 endpoints	Process	<Tanium Client>\tools\driver\TaniumDriverCtl64.exe
	x64 endpoints	Process	<Tanium Client>\tools\driver\TaniumDriverSvc64.exe
	x64 endpoints	File	<Tanium Client>\tools\driver\TaniumProcessMonitor64.dll
	x64 endpoints	File	C:\Windows\SysWOW64\TaniumProcessMonitor.dll

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Process
Linux x86 and x64		Process	<Tanium Client>/extensions/recorder/TaniumAuditPipe
		File	<Tanium Client>/libTaniumClientExtensions.so
		File	<Tanium Client>/libTaniumClientExtensions.so.sig
		File	<Tanium Client>/extensions/libTaniumIndex.so
		File	<Tanium Client>/extensions/libTaniumIndex.so.sig
		File	<Tanium Client>/extensions/libTaniumIntegrityMonitor.so
		File	<Tanium Client>/extensions/libTaniumIntegrityMonitor.so.sig
		File	<Tanium Client>/extensions/libTaniumRecorder.so
		File	<Tanium Client>/extensions/libTaniumRecorder.so.sig
		File	<Tanium Client>/extensions/recorder/proc.bin
		File	<Tanium Client>/extensions/recorder/recorder.db
		File	<Tanium Client>/extensions/recorder/recorder.db-shm
		File	<Tanium Client>/extensions/recorder/recorder.db-wal
		File	<Tanium Client>/extensions/recorder/recorder.auditpipe
		File	<Tanium Client>/extensions/index/index.db
		File	<Tanium Client>/extensions/index/index.db-shm
		File	<Tanium Client>/extensions/index/index.db-wal
		Process	<Tanium Client>/TaniumCX
	Endpoints with a Toolset	Process	<Tanium Client>/python38/python

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Process
	version earlier than 2.7		
	Endpoints with Toolset version 2.7 or later	Folder	<Tanium Client>/python312
	Endpoints with Toolset version 2.7 or later	Folder	<Tanium Client>/TPython312
	Endpoints with Toolset version 2.7 or later	Process	<Tanium Client>/python312/python
	Endpoints with Toolset version 2.7 or later	Process	<Tanium Client>/python312/bin/pybin
		Folder	<Tanium Client>/extensions/index
		Folder	<Tanium Client>/extensions/integrity-monitor

©2026 Tanium Inc. All Rights Reserved

Investigate endpoint exclusions

Investigate security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows x86 and x64		File	*<Tanium Client>* \extensions\SupportCX.dll
		File	*<Tanium Client>* \extensions\SupportCX.dll.sig
		File	*<Tanium Client>* \extensions\core\TaniumPythonCx.dll
		File	*<Tanium Client>* \extensions\core\TaniumPythonCx.dll.sig
		File	*<Tanium Client>* \TaniumClientExtensions.dll
		File	*<Tanium Client>* \TaniumClientExtensions.dll.sig
		Folder	*<Tanium Client>* \python312
		Process	*<Tanium Client>* \python312\TPython.exe
		File	*<Tanium Client>* \TPython\TPython.bat
		Folder	*<Tanium Client>* \TPython312
		Process	*<Tanium Client>* \TaniumCX.exe
		File	*<Tanium Client>* \extensions\TaniumDEC.dll
		File	*<Tanium Client>* \extensions\TaniumDEC.dll.sig
Linux x86 and x64		Process	*<Tanium Client>* /TaniumCX
		Folder	*<Tanium Client>* /python312
		Process	*<Tanium Client>* /python312/bin/pybin
		Process	*<Tanium Client>* /TPython/TPython

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		Folder	*<Tanium Client>* /TPython312
		File	*<Tanium Client>* /libTaniumClientExtensions.so
		File	*<Tanium Client>* /libTaniumClientExtensions.so.sig
		File	*<Tanium Client>* /libSupportCX.so
		File	*<Tanium Client>* /libSupportCX.so.sig
		File	*<Tanium Client>* /extensions/core/libTaniumPythonCx.so
		File	*<Tanium Client>* /extensions/core/libTaniumPythonCx.so.sig
		File	*<Tanium Client>* /extensions/libTaniumDEC.so
		File	*<Tanium Client>* /extensions/libTaniumDEC.so.sig
macOS		Process	*<Tanium Client>* /TaniumCX
		Process	*<Tanium Client>* /python312/bin/pybin
		File	*<Tanium Client>* /libTaniumClientExtensions.dylib
		File	*<Tanium Client>* /libTaniumClientExtensions.dylib.sig
		File	*<Tanium Client>* /extensions/core/libTaniumPythonCx.dylib
		File	*<Tanium Client>* /extensions/core/libTaniumPythonCx.dylib.sig
		File	*<Tanium Client>* /extensions/libTaniumDEC.dylib
		File	*<Tanium Client>* /extensions/libTaniumDEC.dylib.sig
		File	*<Tanium Client>* /extensions/libSupportCX.dylib
		File	*<Tanium Client>* /extensions/libSupportCX.dylib.sig

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion

[1] = TPython requires SHA2 support to allow installation.

Patch endpoint exclusions

For Windows endpoints, review and follow the Microsoft antivirus security exclusion recommendations for enterprise computers. For more information, see Microsoft Support: Virus scanning recommendations for Enterprise computers that are running currently supported versions of Windows (KB822158).

Patch security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows		Process	*<Tanium Client>* \TaniumCX.exe
		File	*<Tanium Client>* \TaniumClientExtensions.dll
		File	*<Tanium Client>* \TaniumClientExtensions.dll.sig
		File	*<Tanium Client>* \extensions\TaniumSoftwareManager.dll
		File	*<Tanium Client>* \extensions\TaniumSoftwareManager.dll.sig
		File	*<Tanium Client>* \Patch\lib\tanium-patch.min.vbs
		File	*<Tanium Client>* \Patch\scans\Wsusscn2.cab
		Process	*<Tanium Client>* \Patch\tools\active-user-sessions.exe
		File	*<Tanium Client>* \Patch\tools\run-patch-manager.min.vbs
		Process	*<Tanium Client>* \Patch\tools\TaniumExecWrapper.exe
		Process	*<Tanium Client>* \Patch\tools\TaniumFileInfo.exe

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	*<Tanium Client>* \Patch\tools\TaniumUpdateSearcher.exe
		Folder	*<Tanium Client>* \python312
		Process	*<Tanium Client>* \python312\TPython.exe
		Process	*<Tanium Client>* \Tools\Patch\7za.exe
		Folder	*<Tanium Client>* \TPython312
		File	*<Tanium Client>* \TPython\TPython.bat
	Endpoints with Toolset version 2.20 or later	File	*<Tanium Client>* \extensions\TaniumEndUser.dll
	Endpoints with Toolset version 2.20 or later	File	*<Tanium Client>* \extensions\TaniumEndUser.dll.cfg
	Endpoints with Toolset version 2.20 or later	File	*<Tanium Client>* \extensions\TaniumEndUser.dll.sig
	Endpoints with Toolset	File	*<Tanium Client>* \extensions\TaniumExtras.dll

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	version 2.20 or later		
	Endpoints with Toolset version 2.20 or later	File	*<Tanium Client>* \extensions\TaniumExtras.dll.cfg
	Endpoints with Toolset version 2.20 or later	File	*<Tanium Client>* \extensions\TaniumExtras.dll.sig
	Endpoints with Toolset version 2.20 or later	File	*<Tanium Client>* \extensions\TaniumPatch.dll
	Endpoints with Toolset version 2.20 or later	File	*<Tanium Client>* \extensions\TaniumPatch.dll.cfg
	Endpoints with Toolset	File	*<Tanium Client>* \extensions\TaniumPatch.dll.sig

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	version 2.20 or later		
	Endpoints with Toolset version 2.20 or later	Folder	*<Tanium Client>* \extensions\patch
	Endpoints with Toolset version 2.20 or later	Process	*<Tanium Client>* \extensions\patch\TaniumPatchEngine.exe
	Endpoints with Toolset version 2.20 or later	File	*<Tanium Client>* \extensions\patch\TaniumPatchEngine.sig
	Exclude from on-access or real-time scans	Folder	*<Tanium Client>*
Linux		File	*<Tanium Client>* /extensions/libTaniumSoftwareManager.so
		File	*<Tanium Client>* /extensions/libTaniumSoftwareManager.so.sig
		File	*<Tanium Client>* /libTaniumClientExtensions.so

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>* /libTaniumClientExtensions.so.sig
		Folder	*<Tanium Client>* /python312
		Process	*<Tanium Client>* /python312/bin/pybin
		Process	*<Tanium Client>* /python312/python
		Folder	*<Tanium Client>* /TPython312
		Process	*<Tanium Client>* /TPython/TPython

Performance endpoint exclusions

Performance security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows (x86 and x64)		File	*<Tanium Client>* \TaniumClientExtensions.dll
		File	*<Tanium Client>* \TaniumClientExtensions.dll.sig
		File	*<Tanium Client>* \extensions\TaniumDEC.dll
		File	*<Tanium Client>* \extensions\TaniumDEC.dll.sig
		File	*<Tanium Client>* \extensions\TaniumPerformance.dll
		File	*<Tanium Client>* \extensions\TaniumPerformance.dll.sig
		Process	*<Tanium Client>* \Tools\PerformanceTSDB\TaniumTSDB.exe
		File	*<Tanium Client>* \extensions\TaniumTSDB.dll
		File	*<Tanium Client>* \extensions\TaniumTSDB.dll.sig

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>* \extensions\SupportCX.dll
		File	*<Tanium Client>* \extensions\SupportCX.dll.sig
		File	*<Tanium Client>* \extensions\TaniumConfig.dll
		File	*<Tanium Client>* \extensions\TaniumConfig.dll.sig
		File	*<Tanium Client>* \extensions\performance\data\performance.db
		File	*<Tanium Client>* \extensions\performance\data\performance.db-shm
		File	*<Tanium Client>* \extensions\performance\data\performance.db-wal
		Folder	*<Tanium Client>* \ProgramData\Tanium\PerformanceAutoLogger
		Folder	*<Tanium Client>* \python312
		Process	*<Tanium Client>* \python312\TPython.exe
		File	*<Tanium Client>* \TPython\TPython.bat
		Folder	*<Tanium Client>* \TPython312
		Process	*<Tanium Client>* \TaniumCX.exe
		Folder	C:\ProgramData\Tanium\PerformanceAutoLogger
Linux (x86 and x64)		File	*<Tanium Client>* /libTaniumClientExtensions.so
		File	*<Tanium Client>* /libTaniumClientExtensions.so.sig
		File	*<Tanium Client>* /extensions/libTaniumDEC.so
		File	*<Tanium Client>* /extensions/libTaniumDEC.so.sig
		File	*<Tanium Client>* /extensions/libTaniumPerformance.so
		File	*<Tanium Client>* /extensions/libTaniumPerformance.so.sig

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	<*Tanium Client*> /Tools/PerformanceTSDB/TaniumTSDB
		File	<*Tanium Client*> /extensions/libTaniumTSDB.so
		File	<*Tanium Client*> /extensions/libTaniumTSDB.so.sig
		File	<*Tanium Client*> /extensions/libSupportCX.so
		File	<*Tanium Client*> /extensions/libSupportCX.so.sig
		File	<*Tanium Client*> /extensions/libTaniumConfig.so
		File	<*Tanium Client*> /extensions/libTaniumConfig.so.sig
		File	<*Tanium Client*> /extensions/performance/data/performance.db
		File	<*Tanium Client*> /extensions/performance/data/performance.db-shm
		File	<*Tanium Client*> /extensions/performance/data/performance.db-wal
		Folder	<*Tanium Client*> /python312
		Process	<*Tanium Client*> /python312/bin/pybin
		Process	<*Tanium Client*> /python312/python
		Process	<*Tanium Client*> /TPython/TPython
		Folder	<*Tanium Client*> /TPython312
		Process	<*Tanium Client*> /TaniumCX
macOS		File	<*Tanium Client*> /libTaniumClientExtensions.dylib
		File	<*Tanium Client*> /libTaniumClientExtensions.dylib.sig
		File	<*Tanium Client*> /extensions/libTaniumDEC.dylib
		File	<*Tanium Client*> /extensions/libTaniumDEC.dylib.so

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	<*Tanium Client*> /extensions/libTaniumPerformance.dylib
		File	<*Tanium Client*> /extensions/libTaniumPerformance.dylib.sig
		Process	<*Tanium Client*> /Tools/PerformanceTSDB/TaniumTSDB
		File	<*Tanium Client*> /extensions/libTaniumTSDB.dylib
		File	<*Tanium Client*> /extensions/libTaniumTSDB.dylib.sig
		File	<*Tanium Client*> /extensions/libSupportCX.dylib
		File	<*Tanium Client*> /extensions/libSupportCX.dylib.sig
		File	<*Tanium Client*> /extensions/libTaniumConfig.dylib
		File	<*Tanium Client*> /extensions/libTaniumConfig.dylib.sig
		File	<*Tanium Client*> /extensions/performance/data/performance.db
		File	<*Tanium Client*> /extensions/performance/data/performance.db-shm
		File	<*Tanium Client*> /extensions/performance/data/performance.db-wal
		Folder	<*Tanium Client*> /python312
		Process	<*Tanium Client*> /python312/python
		Process	<*Tanium Client*> /python312/bin/pybin
		Process	<*Tanium Client*> /TPython/TPython
		Folder	<*Tanium Client*> /TPython312
		Process	<*Tanium Client*> /TaniumCX

[1] = TPython requires SHA2 support to allow installation.

©2026 Tanium Inc. All Rights Reserved

Provision endpoint exclusions

Provision security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows		Process	<*Tanium Client*> \TaniumCX.exe
		File	<*Tanium Client*> \TaniumClientExtensions.dll
		File	<*Tanium Client*> \TaniumClientExtensions.dll.sig
		File	<*Tanium Client*> \extensions\TaniumConfig.dll
		File	<*Tanium Client*> \extensions\TaniumConfig.dll.sig
		File	<*Tanium Client*> \extensions\TaniumDEC.dll
		File	<*Tanium Client*> \extensions\TaniumDEC.dll.sig
		File	<*Tanium Client*> \extensions\TaniumProvision.dll
		File	<*Tanium Client*> \extensions\TaniumProvision.dll.sig
		Process	<*Tanium Client*> \Tools\Provision\TaniumPXE.exe
		Folder	<*Tanium Client*> \Tools\Provision
Linux		Process	<*Tanium Client*> /TaniumCX
		File	<*Tanium Client*> /libTaniumClientExtensions.so
		File	<*Tanium Client*> /libTaniumClientExtensions.so.sig
		File	<*Tanium Client*> /extensions/libTaniumConfig.so
		File	<*Tanium Client*> /extensions/libTaniumConfig.so.sig
		File	<*Tanium Client*> /extensions/libTaniumDEC.so

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>* /extensions/libTaniumDEC.so.sig
		File	*<Tanium Client>* /extensions/libTaniumProvision.so
		File	*<Tanium Client>* /extensions/libTaniumProvision.so.sig
		Folder	*<Tanium Client>* /Tools/Provision
macOS		Process	*<Tanium Client>* /TaniumCX
		File	*<Tanium Client>* /libTaniumClientExtensions.so
		File	*<Tanium Client>* /libTaniumClientExtensions.so.sig
		File	*<Tanium Client>* /extensions/libTaniumConfig.so
		File	*<Tanium Client>* /extensions/libTaniumConfig.so.sig
		File	*<Tanium Client>* /extensions/libTaniumDEC.so
		File	*<Tanium Client>* /extensions/libTaniumDEC.so.sig
		File	*<Tanium Client>* /extensions/libTaniumProvision.so
		File	*<Tanium Client>* /extensions/libTaniumProvision.so.sig
		Folder	*<Tanium Client>* /Tools/Provision

Reveal endpoint exclusions

Reveal security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows		Process	<Tanium Client>\TaniumCX.exe

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	<Tanium Client>\TaniumClientExtensions.dll
		File	<Tanium Client>\TaniumClientExtensions.dll.sig
		File	<Tanium Client>\extensions\TaniumDEC.dll
		File	<Tanium Client>\extensions\TaniumDEC.dll.sig
		File	<Tanium Client>\extensions\TaniumIndex.dll
		File	<Tanium Client>\extensions\TaniumIndex.dll.sig
		File	<Tanium Client>\extensions\index\index.db
		File	<Tanium Client>\extensions\index\index.db-shm
		File	<Tanium Client>\extensions\index\index.db-wal
Linux		Process	<Tanium Client>/TaniumCX
		File	<Tanium Client>/libTaniumClientExtensions.so
		File	<Tanium Client>/libTaniumClientExtensions.so.sig
		File	<Tanium Client>/extensions/libTaniumDEC.so
		File	<Tanium Client>/extensions/libTaniumDEC.so.sig
		File	<Tanium Client>/extensions/libTaniumIndex.so
		File	<Tanium Client>/extensions/libTaniumIndex.so.sig
		File	<Tanium Client>/extensions/index/index.db
		File	<Tanium Client>/extensions/index/index.db-shm
		File	<Tanium Client>/extensions/index/index.db-wal
macOS		Process	<Tanium Client>/TaniumCX

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	<Tanium Client>/libTaniumClientExtensions.dylib
		File	<Tanium Client>/libTaniumClientExtensions.dylib.sig
		File	<Tanium Client>/extensions/libTaniumDEC.dylib
		File	<Tanium Client>/extensions/libTaniumDEC.dylib.sig
		File	<Tanium Client>/extensions/libTaniumIndex.dylib
		File	<Tanium Client>/extensions/libTaniumIndex.dylib.sig
		File	<Tanium Client>/extensions/index/index.db
		File	<Tanium Client>/extensions/index/index.db-shm
		File	<Tanium Client>/extensions/index/index.db-wal

Screen Sharing endpoint exclusions

Screen Sharing security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows		Process	C:\ProgramData\Projector Inc\ScreenMeet Support\ ScreenMeet.Support.exe
		Process	*<Tanium Client>* \Tools\ScreenSharing\ScreenMeet.Support.exe
	for 32-bit operating system versions only	File	C:\ProgramData\Projector Inc\ScreenMeet Support\ *<hash-value>* \webrtcnative-x86.dll
	for 64-bit operating system versions only	File	C:\ProgramData\Projector Inc\ScreenMeet Support\ *<hash-value>* \webrtcnative-x64.dll
macOS		File	/Applications/ScreenMeetSupport.app

©2026 Tanium Inc. All Rights Reserved

Threat Response endpoint exclusions

Threat Response security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows x86 and x64		Process	*<Tanium Client>* \Tools\IR\TaniumExecWrapper.exe
		Process	*<Tanium Client>* \Tools\IR\TaniumFileInfo.exe
		Process	*<Tanium Client>* \Tools\IR\TaniumHandle.exe
		File	*<Tanium Client>* \extensions\TaniumIndex.dll
		File	*<Tanium Client>* \extensions\TaniumIndex.dll.sig
		Process	*<Tanium Client>* \Tools\recorder\TaniumRecorderCtl.exe
		File	*<Tanium Client>* \extensions\TaniumRecorder.dll
		File	*<Tanium Client>* \extensions\TaniumRecorder.dll.sig
		File	*<Tanium Client>* \extensions\SupportCX.dll
		File	*<Tanium Client>* \extensions\SupportCX.dll.sig
		File	*<Tanium Client>* \extensions\recorder\proc.bin
		File	*<Tanium Client>* \extensions\recorder\recorder.db
		File	*<Tanium Client>* \extensions\recorder\recorder.db-shm
		File	*<Tanium Client>* \extensions\recorder\recorder.db-wal
		File	*<Tanium Client>* \extensions\index\index.db
		File	*<Tanium Client>* \extensions\index\index.db-shm
		File	*<Tanium Client>* \extensions\index\index.db-wal

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>* \extensions\TaniumStream.dll
		File	*<Tanium Client>* \extensions\TaniumStream.dll.cfg
		File	*<Tanium Client>* \extensions\TaniumStream.dll.sig
		File	*<Tanium Client>* \extensions\TaniumExtras.dll
		File	*<Tanium Client>* \extensions\TaniumExtras.dll.cfg
		File	*<Tanium Client>* \extensions\TaniumExtras.dll.sig
	x86 endpoints	Process	*<Tanium Client>* \tools\driver\TaniumDriverCtl.exe
	x64 endpoints	Process	*<Tanium Client>* \tools\driver\TaniumDriverCtl64.exe
	x86 endpoints	Process	*<Tanium Client>* \tools\driver\TaniumDriverSvc.exe
	x64 endpoints	Process	*<Tanium Client>* \tools\driver\TaniumDriverSvc64.exe
		Process	*<Tanium Client>* \tools\driver\service\TaniumDriverSvc.exe
		File	*<Tanium Client>* \tools\driver\TaniumProcessMonitor.dll
		File	*<Tanium Client>* \tools\driver\TaniumProcessMonitor64.dll
		File	*<Tanium Client>* \extensions\TaniumThreatResponse.dll
		File	*<Tanium Client>* \extensions\TaniumThreatResponse.dll.sig
		File	*<Tanium Client>* \extensions\core\TaniumPythonCx.dll
		File	*<Tanium Client>* \extensions\core\TaniumPythonCx.dll.sig
		Folder	*<Tanium Client>* \extensions\stream
		File	*<Tanium Client>* \TaniumClientExtensions.dll
		File	*<Tanium Client>* \TaniumClientExtensions.dll.sig

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	*<Tanium Client>* \Tools\IR\TaniumPersistenceAnalyzer.exe
		File	*<Tanium Client>* \Tools\IR\PowerForensics\PowerForensics.dll
	Where * corresponds to the action ID or the version of linpmem.	File	*<Tanium Client>* \Tools\IR\data\Action_*\PowerForensics.dll
	Where * corresponds to the action ID or the version of linpmem.	File	*<Tanium Client>* \Tools\IR\data\Action_*\PSTaniumFileTransfer_64.dll
	Where * corresponds to the action ID or the version of linpmem.	Process	*<Tanium Client>* \Tools\IR\data\Action_*\taniumfiletransfer_32.exe
	Where * corresponds to the action ID or the version of linpmem.	Process	*<Tanium Client>* \Tools\IR\data\Action_*\taniumfiletransfer_64.exe
	Where * corresponds to the action ID or the version of linpmem.	Process	*<Tanium Client>* \Tools\IR\data\Action_*\TaniumHandle_32.exe
	Where * corresponds to the action ID or the version of linpmem.	Process	*<Tanium Client>* \Tools\IR\data\Action_*\TaniumHandle_64.exe
	Where * corresponds to the action ID or the version of linpmem.	Process	*<Tanium Client>* \Tools\IR\data\Action_*\winpmem_mini_x64_rc2.exe
		File	*<Tanium Client>* \Tools\IR\PSTaniumFileTransfer.dll
		Process	*<Tanium Client>* \Tools\IR\TanFileInfo.exe
		Process	*<Tanium Client>* \Tools\IR\taniumfiletransfer.exe

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	*<Tanium Client>* \Tools\Copy\taniumfiletransfer.exe
		Process	*<Tanium Client>* \Tools\IR\py\incident_response_deps_platform\38-cp38-win32\taniumfiletransfer\taniumfiletransfer.exe
		Process	*<Tanium Client>* \Tools\IR\py\incident_response_deps_platform\312-cp312-win32\taniumfiletransfer\taniumfiletransfer.exe
		Process	*<Tanium Client>* \Tools\IR\TaniumHandle.exe
		Process	*<Tanium Client>* \Tools\IR\TaniumListModules.exe
		Process	*<Tanium Client>* \Tools\IR\TaniumPersistenceAnalyzer.exe
		File	*<Tanium Client>* \TPython\TPython.bat
		Folder	*<Tanium Client>* \TPython312
		Folder	*<Tanium Client>* \python312
		Process	*<Tanium Client>* \python312\TPython.exe
		Process	*<Tanium Client>* \TaniumCX.exe
		File	*<Tanium Client>* \extensions\TaniumDEC.dll
		File	*<Tanium Client>* \extensions\TaniumDEC.dll.sig
		File	C:\Windows\System32\drivers\TaniumRecorderDrv.sys
		File	C:\Windows\SysWOW64\TaniumProcessMonitor.dll
		File	C:\Windows\system32\drivers\TaniumProcessMonitor.dll
Linux x86 and x64		Process	*<Tanium Client>* /extensions/recorder/TaniumAuditPipe
		Process	*<Tanium Client>* /TaniumCX
		Process	*<Tanium Client>* /Tools/IR/TaniumExecWrapper

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>* /extensions/libTaniumIndex.so
		File	*<Tanium Client>* /extensions/libTaniumIndex.so.sig
		Folder	*<Tanium Client>* /python312
		Process	*<Tanium Client>* /python312/python
		Process	*<Tanium Client>* /python312/bin/pybin
		Process	*<Tanium Client>* /TPython/TPython
		Folder	*<Tanium Client>* /TPython312
		File	*<Tanium Client>* /libTaniumClientExtensions.so
		File	*<Tanium Client>* /libTaniumClientExtensions.so.sig
		File	*<Tanium Client>* /extensions/libSupportCX.so
		File	*<Tanium Client>* /extensions/libSupportCX.so.sig
		File	*<Tanium Client>* /extensions/libTaniumThreatResponse.so
		File	*<Tanium Client>* /extensions/libTaniumThreatResponse.so.sig
		File	*<Tanium Client>* /extensions/libTaniumRecorder.so
		File	*<Tanium Client>* /extensions/libTaniumRecorder.so.sig
		File	*<Tanium Client>* /extensions/recorder/proc.bin
		File	*<Tanium Client>* /extensions/recorder/recorder.db
		File	*<Tanium Client>* /extensions/recorder/recorder.db-shm
		File	*<Tanium Client>* /extensions/recorder/recorder.db-wal
		File	*<Tanium Client>* /extensions/recorder/recorder.auditpipe

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>* /extensions/index/index.db
		File	*<Tanium Client>* /extensions/index/index.db-shm
		File	*<Tanium Client>* /extensions/index/index.db-wal
		File	*<Tanium Client>* /extensions/core/libTaniumPythonCx.so
		File	*<Tanium Client>* /extensions/core/libTaniumPythonCx.so.sig
		File	*<Tanium Client>* /extensions/libTaniumDEC.so
		File	*<Tanium Client>* /extensions/libTaniumDEC.so.sig
		Folder	*<Tanium Client>* /extensions/stream
		File	*<Tanium Client>* /extensions/libTaniumStream.so
		File	*<Tanium Client>* /extensions/libTaniumStream.so.cfg
		File	*<Tanium Client>* /extensions/libTaniumStream.so.sig
		File	*<Tanium Client>* /extensions/TaniumExtras.so
		File	*<Tanium Client>* /extensions/TaniumExtras.so.cfg
		File	*<Tanium Client>* /extensions/TaniumExtras.so.sig
	Where * corresponds to the action ID or the version of linpmem.	File	<Tanium Client>/Downloads/Action_*/linpmem-*.bin
	Where * corresponds to the action ID or the version of linpmem.	Process	*<Tanium Client>* /Tools/IR/taniumfiletransfer
		File	*<Tanium Client>* /Tools/IR/linpmem_3.0rc2.bin
	Where * corresponds to the	File	*<Tanium Client>* /Downloads/Action_*/linpmem_3.0rc2.bin

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	action ID or the version of linpmem.		
		Process	*<Tanium Client>* /Tools/IR/py/incident_response/_deps/_platform/38-cp38-linux_x86_64/taniumfiletransfer/taniumfiletransfer
		Process	*<Tanium Client>* /Tools/IR/py/incident_response/_deps/_platform/312-cp312-linux_x86_64/taniumfiletransfer/taniumfiletransfer
macOS		Process	*<Tanium Client>* /TaniumCX
	For macOS Universal only	Process	*<Tanium Client>* /TaniumCX.app/Contents/MacOS/TaniumCX
		Process	*<Tanium Client>* /Tools/IR/TaniumExecWrapper
		File	*<Tanium Client>* /extensions/libTaniumIndex.dylib
		File	*<Tanium Client>* /extensions/libTaniumIndex.dylib.sig
		Folder	*<Tanium Client>* /python312
		Process	*<Tanium Client>* /python312/python
		Process	*<Tanium Client>* /python312/bin/pybin
		Process	*<Tanium Client>* /TPython/TPython
		Folder	*<Tanium Client>* /TPython312
		File	*<Tanium Client>* /libTaniumClientExtensions.dylib
		File	*<Tanium Client>* /libTaniumClientExtensions.dylib.sig
		File	*<Tanium Client>* /extensions/libTaniumThreatResponse.dylib
		File	*<Tanium Client>* /extensions/libTaniumThreatResponse.dylib.sig
		File	*<Tanium Client>* /extensions/libTaniumRecorder.dylib
		File	*<Tanium Client>* /extensions/libTaniumRecorder.dylib.sig

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>* /extensions/recorder/proc.bin
		File	*<Tanium Client>* /extensions/recorder/recorder.db
		File	*<Tanium Client>* /extensions/recorder/recorder.db-shm
		File	*<Tanium Client>* /extensions/recorder/recorder.db-wal
		File	*<Tanium Client>* /extensions/recorder/recorder.auditpipe
		File	*<Tanium Client>* /extensions/core/libTaniumPythonCx.dylib
		File	*<Tanium Client>* /extensions/index/index.db
		File	*<Tanium Client>* /extensions/index/index.db-shm
		File	*<Tanium Client>* /extensions/index/index.db-wal
		File	*<Tanium Client>* /extensions/core/libTaniumPythonCx.dylib.sig
		Folder	*<Tanium Client>* /extensions/stream
		File	*<Tanium Client>* /extensions/libTaniumDEC.dylib
		File	*<Tanium Client>* /extensions/libTaniumDEC.dylib.sig
		File	*<Tanium Client>* /extensions/libSupportCX.dylib
		File	*<Tanium Client>* /extensions/libSupportCX.dylib.sig
		File	*<Tanium Client>* /extensions/libTaniumStream.dylib
		File	*<Tanium Client>* /extensions/libTaniumStream.dylib.cfg
		File	*<Tanium Client>* /extensions/libTaniumStream.dylib.sig
		File	*<Tanium Client>* /extensions/libTaniumExtras.dylib
		File	*<Tanium Client>* /extensions/libTaniumExtras.dylib.cfg

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>* /extensions/libTaniumExtras.dylib.sig
		Process	*<Tanium Client>* /Tools/IR/taniumfiletransfer
	Where * corresponds to the action ID or the version of linpmem.	Process	*<Tanium Client>* /Tools/IR/data/Action_*/osxpmem.app
	Where * corresponds to the action ID or the version of linpmem.	File	*<Tanium Client>* /Tools/IR/data/Action_*/osxpmem.app/libs/libaff4.0.dylib
	Where * corresponds to the action ID or the version of linpmem.	File	*<Tanium Client>* /Tools/IR/data/Action_*/osxpmem.app/libs/libpcre.1.dylib
	Where * corresponds to the action ID or the version of linpmem.	File	*<Tanium Client>* /Tools/IR/data/Action_*/osxpmem.app/libs/libpcre++.0.dylib
	Where * corresponds to the action ID or the version of linpmem.	File	*<Tanium Client>* /Tools/IR/data/Action_*/osxpmem.app/libs/libraptor2.0.dylib
	Where * corresponds to the action ID or the version of linpmem.	File	*<Tanium Client>* /Tools/IR/data/Action_*/osxpmem.app/libs/libsnappy.1.dylib
	Where * corresponds to the action ID or the version of linpmem.	File	*<Tanium Client>* /Tools/IR/data/Action_*/osxpmem.app/libs/liburiparser.1.dylib
	Where * corresponds to the action ID or the version of linpmem.	File	*<Tanium Client>* /Tools/IR/data/Action_*/osxpmem.app/libs/libuuid.16.dylib
	Where * corresponds to the	File	*<Tanium Client>* /Tools/IR/data/Action_*/osxpmem.app/libs/libyaml-cpp.0.6.dylib

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
	action ID or the version of linpmem.		
		Procress	*<Tanium Client>* /Tools/IR/py/incident_response/_deps/_platform/312-cp312-macosx_10_11_x86_64/taniumfiletransfer/taniumfiletransfer
		Process	*<Tanium Client>* /Tools/IR/py/incident_response/_deps/_platform/38-cp38-macosx_10_11_x86_64/taniumfiletransfer/taniumfiletransfer

Solutions that require no additional security exclusions

The following Tanium solutions require no additional security exclusions beyond the Tanium Client folder, process, and binary signer exclusions.

The following solutions are named individually so that you can confirm that a specific solution requires no additional exclusions. If a solution is not listed on this page at all, it might not yet be documented here; contact Tanium Support on page 392 to confirm its requirements rather than assuming that none apply.

- Automate
- Blob Service
- Cloud Workloads
- Connect
- Criticality
- Directory Query
- Endpoint Configuration
- Gateway
- Guide

©2026 Tanium Inc. All Rights Reserved

- Health Check
- Integrations Gallery
- Jump Gate
- RDB Service
- Reporting
- Reputation
- Secrets Service
- System User Service
- Trends
- Zero Trust

©2026 Tanium Inc. All Rights Reserved

Reference: Client extensions and endpoint tools used for Tanium solutions

In addition to the Tanium Client binary, Tanium installs Client Extensions and other tools on endpoints to perform tasks that are common to certain Tanium solutions. Endpoint Configuration installs these tools as they are needed by those solutions. For information about managing installed endpoint tools, see Managing endpoint tools.

Tools are bundled together in a versioned toolset that contains a specific version of each tool. The Endpoint Configuration Toolset Solution provides upgrades to the toolset, and it imports upgraded versions of the entire toolset as available. You can use the change management feature of Endpoint Configuration to perform a staged rollout of each toolset that accommodates the software upgrade strategy for your organization. For more information, see Managing endpoint tool upgrade rollouts.

Each Client Extension and tool has required security exclusions to allow the Tanium processes to run without interference. For more information, see Reference: Endpoint security exclusions on page 416 and for Windows-based Tanium Core Platform deployments, Tanium Core Platform Server security exclusions, or the requirements section of each solution user guide in the Tanium Resource Center.

Client extensions can run in separate processes, or together in a single process, depending on whether *Client Extension shared process mode* is enabled. For more information, see Manage Client Extension shared process mode.

The Tanium Client applies a CPU throttle (5% of total CPU capacity) to limit the aggregate CPU usage of all Client Extensions on an endpoint, regardless of whether Client Extension shared process mode is enabled. When a single extension is active, it can use up to the full 5% allocation; when multiple extensions are active simultaneously, they share the available CPU within that limit. Long-running work such as indexing might run faster when no other extensions are competing for CPU.

©2026 Tanium Inc. All Rights Reserved

Note:

- After a Client Extension restart, the Client allows approximately 30 seconds before applying the throttle. Brief CPU peaks during this window are expected and allowed.
- The Client Recorder Extension is exempt from the CPU throttle to ensure reliable event recording. For more information, see Client Recorder Extension requirements.

The Tanium Client uses code signatures to verify the integrity of each Client Extension prior to loading the extension on the endpoint.

To troubleshoot issues with endpoint tools, see Identify and resolve issues with endpoint tools or Client Extensions.

The following Client Extensions and tools perform functions for Tanium solutions:

Note: Each solution includes a tool with the same name as the solution that appears in the Endpoint Configuration Toolset manifest but that does not appear in the following table. This tool is not deployed to the endpoint itself, but it manages the endpoint tooling dependencies for the solution, as listed in the table.

Tip: Some solution user guides provide an endpoint tooling reference specifically for that solution. Click a linked solution in the following table to view the reference for that solution.

Endpoint tools for Tanium Client Management

Tool	Description	Solutions where used
client-deploy-cx	Provides the satellite functionality for Tanium Client deployments in Client Management. Client Management installs this Client Extension only on satellite endpoints used for Client deployments, and only upon the first time you start a Client deployment that uses a particular satellite.	Client Management
Comply RAS	Provides a cryptography library for java for remote authenticated vulnerability assessments	Comply
Comply RUS	Provides Nmap for network unauthenticated vulnerability assessments	Comply
comply-cx	Provides Comply functions on an endpoint	Comply

©2026 Tanium Inc. All Rights Reserved

Tool	Description	Solutions where used
core-cx	Provides a management framework API for all other Client Extensions and exposes operating system metrics	All solutions that use Client Extensions
cx-config	Provides installation and configuration of extensions on an endpoint	All solutions that use Client Extensions
cx-stream	Provides the ability to gather large amounts of data from an endpoint and send it to an external destination	Enforce , Performance , Threat Response
cx-tsdb	Collects metrics about the Tanium Client and Client Extensions	Client Management
dec-cx	Provides a direct connection between an endpoint and Module Server	Direct Connect
discover-cx	Performs distributed ARP, NDP, Ping, Nmap scans, and satellite Nmap scans	Discover
Driver	The Tanium Driver, which records process and command-line events on supported Windows endpoints	Enforce , Integrity Monitor , Threat Response
end-user-cx	Provides a mechanism to send surveys to collect qualitative feedback from endpoint users	Engage
End-User Notifications	Provides End-User Notifications code	End-User Notifications
enforce-cx	Provides Enforce functions on an endpoint	Enforce
entity-cx	Provides management for entity providers and facilitates communication between the entity providers and Tanium Client	
extras-cx	Provides a helper library that contains re-usable functions for various client extensions to use	Asset , Certificate Manager , Comply, Deploy , Discover , Enforce , Integrity Monitor, Investigate, Patch , Performance , Reveal , Threat Response
index-cx	Provides the ability to index the local file systems on an endpoint	Asset , Certificate Manager , Deploy , Integrity Monitor , Reveal , Threat Response
integrity-monitor-cx	Provides Integrity Monitor functions on an endpoint	Integrity Monitor
Nmap	Network mapping tool used for certain scans in Comply and Discover	Comply, Discover
Npcap	Records process and command-line events on supported Windows endpoints to assist with Nmap scans	Discover , Profinet Entity Provider
performance-cx	Provides Performance functions on an endpoint	Deploy , Investigate, Performance
performance-tsdb	The Time Series Data Store in which performance stores metrics on the endpoint	Deploy , Investigate, Performance
provision-cx	Provides sensitive data and notifications about bundle or settings changes to a Provision endpoint	Provision
python27	Provides legacy TPython binary and libraries	Asset , Enforce , Impact, Initial Content - Python
python312	Provides TPython binary and libraries	Benchmark, Certificate Manager , Core Content, Deploy , End-User Notifications, Enforce , Impact, Incident Response, Initial Content - Python, Integrity Monitor , Patch , Performance , Recorder, Threat Response

©2026 Tanium Inc. All Rights Reserved

Tool	Description	Solutions where used
Recorder	Provides the ability to save event data on each endpoint and monitor the endpoint kernel and other low-level subsystems to capture a variety of events	Enforce , Integrity Monitor , Threat Response
Recorder BPF Support	Provides the ability to save event data using eBPF on Linux endpoints	Integrity Monitor , Threat Response
risk-cx	Provides Benchmark functions on the endpoint	Benchmark
Software Management	Provides the long-running Python Deploy process and platform-specific scripts	Deploy
SSL Server Audit	Provides endpoint functionality for packages in the SSL Audit content set	Core Content
swmgr-cx	Provides a catalog of all installed software on an endpoint	Asset , Certificate Manager , Comply, Deploy , Patch
Tanium EUSS	Provides End-User Self Service code	Deploy , Engage, Patch
threat-response-cx	Provides Threat Response functions on an endpoint	Threat Response

©2026 Tanium Inc. All Rights Reserved

Reference: Default installation directory for the Tanium Client

The following table lists the default installation paths for the Tanium Client on each operating system (OS). If you troubleshoot issues for an installation that uses a non-default path, note this when you Contact Tanium Support on page 392.

OS	Installation Directory
Windows (64-bit OS versions)*	\Program Files (x86)\Tanium\Tanium Client\
Windows (32-bit OS versions)*	\Program Files\Tanium\Tanium Client\
macOS	/Library/Tanium/TaniumClient
Linux, UNIX	/opt/Tanium/TaniumClient
* On both 64-bit and 32-bit versions of Windows, Tanium Client is installed as a 32-bit application.	

©2026 Tanium Inc. All Rights Reserved

Reference: Registry key paths for the Tanium Client

The following table lists the registry key paths used to store settings for the Tanium Client in Windows.

Registry key paths for Tanium Client settings on Windows

64-bit or 32-bit version of Windows	Registry Key Path
64-bit	HKEY_LOCAL_MACHINE\Software\Wow6432Node\Tanium\Tanium Client
32-bit	HKEY_LOCAL_MACHINE\Software\Tanium\Tanium Client

©2026 Tanium Inc. All Rights Reserved

Reference: Commands used during deployment with Client Management

If you restrict commands in the sudoers file on endpoints, the following commands must be allowed for the user account you use for deployment with Client Management:

```
awk cat chmod chown command df dpkg dpkg-query echo exit grep gunzip installer installp launchctl ln ls lslpp mkdir mv netstat pkgadd pkginfo pkgrm pkgutil rm rmdir rpm service sh startsrc stopsrc svcadm sw_vers systemctl TaniumClient tar test touch uname
```

©2026 Tanium Inc. All Rights Reserved

Tanium Client Export Commodity Classification

The Export Commodity Classification Automated Tracking System (CCATS) number for Tanium is G172792. The Export Control Classification Numbers (ECCNs) for Tanium Client is as follows:

Export Commodity Classification

Product	ECCN	License Exception	Authorized for Export (See Definitions List Below)
Tanium Client software	5D992.c	No License Required ("NLR")	All countries, except Embargoed Countries and the Crimea Region of Ukraine

For the ECCN information for Tanium Core Platform Server software, see Export Commodity Classification (Tanium Appliance deployments) or Export Commodity Classification (Windows deployments).

Important: Tanium prohibits software and hardware (both physical and virtual) installations in certain countries. Contact Tanium Support on page 392 to determine whether a particular country is on the prohibited list.

©2026 Tanium Inc. All Rights Reserved

General Client deployment settings

The following settings are often configured the same for multiple deployments. You can optionally configure these settings in a Client deployment template.

Section	Setting	Description
Content to deploy	Client Version	Select the version of the Tanium Client to install. **Important:** Each version of the endpoint toolset includes a specific version of the Tanium Client, which must be installed with the toolset to maintain a supported configuration. Endpoints with versions of the Tanium Client older than the associated toolset are unsupported. Deployment of previous versions of the Tanium Client is provided for temporary support of legacy deployments. For more information, see Managing Tanium Client and endpoint tool upgrade rollouts . **Tip:** To manage the Client versions that are available for this setting, see Manage versions of the Tanium Client available for legacy deployments on page 115 .
Method settings	SSH Ports	Enter the SSH port to use for deployment to non-Windows endpoints. The default port is 22. **Important:** Make sure that any firewalls or security applications do not block the specified port.
	Retry Delay	Enter the delay between connection retries to a single endpoint during the deployment. The value for this setting must be between 5 seconds and 15 minutes.
	Retry Limit	Enter the maximum number of attempts to make a connection to a single endpoint during the deployment. The maximum value for this setting is 30.
	Installation Limit	Enter the maximum number of concurrent installations during the deployment. The maximum value for this setting is 300.
	File Transfer	Enter the time-out for file transfers during the deployment. The maximum value for this setting is 60 minutes.

©2026 Tanium Inc. All Rights Reserved

Section	Setting	Description
	Timeout	
	Installation Validation Retry Limit	Enter the maximum number of attempts to check the health of a newly installed Tanium Client to validate the installation. The value for this setting must be between 3 and 75.
	Verbose Logging	If you need to troubleshoot Client installation issues, select **Enable verbose logging for Client installations on targeted endpoints** . **Tip:** To view the installation log, see View the deployment status and endpoint installation logs on page 150 .
	Skip Certificate Verification	Skip verification of the required trusted root certificates on endpoints prior to installation of the Tanium Client.  **Important:** Endpoints cannot verify the Tanium Client installer signature when this option is selected.  **Best Practice:** Do not enable this setting unless you have a critical need to deploy the Tanium Client to endpoints that do not yet have the required trusted root certificates. If you enable this setting for that purpose, install the required certificates as soon as possible.
Installation options	Installation Directory on Windows	(Optional) Enter a custom installation directory for Windows endpoints. Leave blank to use the default installation directory on page 490 .  **Important:** • You must specify an installation directory on a local fixed drive on each endpoint. A volume mounted in a directory on another volume is not supported. • The installation directory must be located on drive C for deployment with Client Management. To install Tanium Client on a different drive, you must use an alternative deployment method. For more information, see Deploying the Tanium Client using an installer or package file on page 153.
	Installation	(Optional) Enter a custom installation directory for non-Windows endpoints. Leave blank to use the

©2026 Tanium Inc. All Rights Reserved

Section	Setting	Description
	Directory on non-Windows	default installation directory on page 490 . **Important:** • The installation directory must be located on a local fixed drive on each endpoint. • (macOS endpoints) You cannot customize the installation directory on macOS. The fixed installation directory for macOS is /Library/Tanium/TaniumClient.
	Space Required (Windows)	(Optional) Enter the disk space that should be available on a targeted Windows endpoint for the Client to be installed. **Note:** The default of 3000 MB is sufficient for the Tanium Client itself, but the total space required depends on the modules that you use with each endpoint. For more information, see Hardware requirements on page 45 .
	Space Required (non-Windows)	(Optional) Enter the disk space that should be available on a targeted non-Windows endpoint for the Client to be installed. **Note:** The default of 3000 MB is sufficient for the Tanium Client itself, but the total space required depends on the modules that you use with each endpoint. For more information, see Hardware requirements on page 45 .
	Endpoints without the Tanium Client	To install the Client on unmanaged endpoints, select **Install Tanium Client** . **Tip:** This setting is enabled in a typical deployment. You might disable this setting if you are creating a deployment to specifically to reinstall the Tanium Client on endpoints that are already managed.
	Endpoints with an Installed Tanium Client	Select one of the following options: • **No action to endpoint:** Ignore endpoints where the Client is already installed. Select this option for a typical deployment to unmanaged endpoints. • **Install if newer Tanium Client version:** Install the version that you specified in the selected Client Configuration only on endpoints where an earlier version is currently installed.

©2026 Tanium Inc. All Rights Reserved

Section	Setting	Description
		Best Practice: For general management of upgrades to existing Clients, use the change management feature in Endpoint Configuration. To do so, you must enable Tanium Client upgrades in the upgrade ring configuration. For information about enabling this setting and managing upgrade rings and toolset promotions, see Managing Tanium Client and endpoint tool upgrade rollouts. If you do not use this feature, or if you need to upgrade the Tanium Client in upgrade rings for which Client upgrades are not yet enabled, use upgrade deployments that target computer groups to upgrade existing Tanium Clients. For more information, see Upgrade Tanium Clients using Client Management on page 346. • **Reinstall Tanium Client:** Reinstall existing Clients. Use this option to repair disabled or corrupt Clients. This selection provides additional options: **Clear Existing Data** and **Overwrite Connected Clients**. If neither of these options is selected, Client Management reinstalls Clients only on endpoints where the Client is not communicating properly with the Tanium Server and where the currently installed version is earlier than or the same as the version that you configure in a Client Configuration. Any data that the Client has collected remains on the Client. Select **Clear Existing Data** to wipe all Client data. If you select this option, the version that you deploy replaces *any* existing version, since the deployment first removes any version of the Client found on the endpoint. Select **Overwrite Connected Clients** to reinstall Clients that are still communicating with the Server. **Note:** macOS: If you are installing the universal version of the macOS client on an endpoint where the x86-64 version of the Client is installed, you must select **Clear Existing Data**. **Important:** Windows: If anti-tamper is enabled on a Windows endpoint, reinstallation through Client Management is not possible on that endpoint. You must disable anti-tamper on the endpoint before reinstalling the Tanium Client. For more information, see Manage tamper protection on page 294.
Client options	Server Names	Fully qualified domain names (FQDNs) or IP addresses of the Tanium Servers. In a deployment with Zone Servers, add their FQDNs or IP addresses. Use a comma to separate the entry for each Server. If you include a port for a listed Server by appending `: <port_number>` to the Server address, it

©2026 Tanium Inc. All Rights Reserved

Section	Setting	Description
		overrides the port specified for the **Server Port** setting. You can configure the default value for this setting. For more information, see Configure the default Server names and Server port for Tanium Client deployments on page 114.  **Best Practice:** Specify FQDNs for the **Server Names** setting.
	Server Port	The port that the Tanium Client uses for communication with the Tanium Server and with peers. You can configure the default value for this setting. For more information, see Configure the default Server names and Server port for Tanium Client deployments on page 114.
	Proxy	If deployed Clients must connect through a proxy server, select one of the following options: • **PAC file** (Windows endpoints only): Use a PAC file to configure the proxy on endpoints. Selecting this option automatically adds the **ProxyAutoConfigAddress** Client setting. Configure the URL of the PAC file for the value. • **Proxy server**: Use specific addresses to connect endpoints through a proxy server. Selecting this option automatically adds the **ProxyServers** Client setting. Configure the addresses of proxy servers for the value. Alternatively, to detect the proxy configuration in the registry on Windows endpoints, include the **ProxyAutoDetect** setting as a key with a value of `1` in **Client Settings**. For more information about using a proxy server, see Connect through an HTTPS forward proxy server on page 238.
	Log Level	(Optional) Enter a log level for the Tanium Client on targeted endpoints. The following values are best practices for specific scenarios: • `1` (default): Use this value during normal operation. • `41`: Use this value during troubleshooting. • `91` or higher: Use this value for full logging, for short periods of time only.  **Note:** A value of `0` disables logging. As a best practice, do not disable logging.  **Note:** This value does not affect the verbosity of the Client installation log during deployment. For troubleshooting Client installations, enable the Verbose Logging on page 495 setting.

©2026 Tanium Inc. All Rights Reserved

Section	Setting	Description
	Client Settings	(Optional) To change a default Client setting, click **Add Client Setting**, and then enter a **Key** and **Value**. For information about specific Client settings, see Tanium Client settings reference on page 393. **Note:** • If you selected **PAC file** for the **Proxy** setting, do not delete the **ProxyAutoConfigAddress** Client setting. If you selected **Proxy server** for the **Proxy** setting, do not delete the **ProxyServers** Client setting. • If you are deploying the Tanium Client to virtual desktop infrastructure (VDI) instances or other endpoints with limited resources, you might need to adjust certain Client settings to help to reduce resource usage. For more information, see Tuning Tanium Client settings for VDI endpoints and other endpoints with limited resources on page 407.
	Custom Tags	(Optional) To add a custom tag to the Client during deployment, click **Add Custom Tag** and enter a tag name. The `InstalledByTCM` tag is included by default so that you can later easily target Clients that were installed using Client Management. **Note:** Do not include spaces in a tag name.

©2026 Tanium Inc. All Rights Reserved

Individual Client deployment settings

Section	Setting	Description
Deployment Schedule	Deployment Type	Select **One-Time** for a deployment that you want to run once, or **Recurring** for a deployment that you want to automatically repeat. **Tip:** A recurring deployment appears on the **Scheduled Client Deployments** page and automatically creates individual one-time deployments according to the configured schedule. The individually created one-time deployments appear on the **Client Deployments** page.
	Recurrence Interval	Recurring deployments only: Specify the interval between each recurrence of the deployment.
	Deployment Time Zone	Select the time zone that applies for the deployment. This time zone applies to the **Start Time** and **End Time** if they are set for the deployment.
	Start Time	To start the deployment immediately, clear the selection for **Specify Start Time** . To schedule the deployment to start at a later time, select **Specify Start Time** and configure a time.  **Note:** The start time must be within 31 days. **Tip:** A scheduled one-time deployment appears on the **Scheduled Client Deployments** page and automatically creates an individual one-time deployment at the configured start time. Recurring deployments also appear there and automatically create individual one-time deployments according to the configured schedule. If you do not configure a start time for a recurring deployment, it is still classified as a scheduled deployment, and it uses the time at which you create the deployment as the start time. The individually created one-time deployments appear on the **Client Deployments** page.
	End Time	Recurring deployments only: To repeat the deployment indefinitely, clear the selection for **Specify End Time** . To stop repeating the deployment after a specific time, select **Specify End Time** and configure a time.  **Note:** The end time must be within one year.

©2026 Tanium Inc. All Rights Reserved

Section	Setting	Description
Endpoints to target	Targeting Method	Select a targeting method, and enter a list of IP addresses, a list of FQDNs or host names, an IP or CIDR range, or a Discover label. For information about configuring Discover labels, see Labels . **Note:** Discover labels must have the following settings to be used with Client Management: • **Type**: Automatic • **Activity**: Retain • **Retain Activity**: Label To define an additional target for the deployment, click **Add Target** . To remove a target, click Delete .
Endpoint credentials	Credentials to Authenticate with Targeted Endpoints	Add credential sets to try for the targeted endpoints. Each credential set is saved as a separate item that you can update at a later time as necessary. • If you are targeting Windows endpoints, configure each Windows credential combination to be tried during the deployment. 1. Click **+ Windows Credential Set**. 2. Enter a **Name** for the credential set. 3. Enter the **Username** and, as necessary, the **Domain** and **Password** for the account. 4. Click **Save**. • If you are targeting non-Windows endpoints, configure each non-Windows credential combination to be tried during the deployment. 1. Click **+ Non-Windows Credential Set**.

©2026 Tanium Inc. All Rights Reserved

Section	Setting	Description
		2. Enter a **Name** for the credential set. 3. Enter the **Username** and, as necessary, the **Domain**, **Password**, **SSH Key**, and **Keyphrase** for the account. **Note:** If you are using an SSH key, the private key is required in PEM format. Copy the contents of the PEM-formatted private key, paste the contents in the **SSH Key** field, and enter the passphrase in the **Keyphrase** field. When you use an SSH key for authentication, a user name is required, and a password is optional. However, endpoints typically still require a password for non-root users, unless the specified user is configured to use sudo without a password. 4. Click **Save**. **Tip:** For specific requirements for authentication and permissions, see Account permissions for Client Management on page 59.
Deployment method	Deployment Method	Select **Satellite** or **Tanium Module Server**. If you select **Satellite**, select the satellite you configured to use for deploying the Tanium Client. If you need to configure a satellite, see (Optional) Prepare a satellite for use with automatic deployment on page 128. **Note:** You can select still a supported satellite if its last known status is offline. In this case, the deployment will still try to connect, but the satellite must be back online for the deployment to proceed. **Important:** If FIPS mode is enabled on a Linux satellite, you cannot use that satellite to deploy the Tanium Client to Windows endpoints. **Important:** If you are using a Tanium Appliance-based deployment with FIPS mode enabled, you must use a satellite for deployment. For more information about FIPS mode, see Enable FIPS 140-3 mode.

©2026 Tanium Inc. All Rights Reserved