Tanium™ Client Management User Guide

Tanium Client version: All

Tanium Client Management service version: 2.1.351

April 30, 2024

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 services provided 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 and has most recently completed certification against the WCAG 2.1 / VPAT 2.3 standards for all major product modules in summer 2021. In the recent testing the Tanium Console UI achieved supports or partially supports for all applicable WCAG 2.1 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 best efforts to address any gaps quickly, as is feasible, given the severity of the issue and scope of the changes. These objectives are factored 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 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, email Tanium Support at support@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 their respective owners.

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

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

Table of contents

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.

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 details on using a third-party tool with Tanium installers, refer to the documentation for that tool.

For an illustrated example of a Tanium Client deployment, see Network connectivity, ports, and firewalls on page 72.

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
- 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 Zone Server, peers with other Tanium Clients, and distributes files, see Tanium Client concepts on page 20.

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.

Client deployment

Deploy the Tanium Client 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. You can target by single IP, computer name, IP or CIDR range, or label that you define in Tanium™ Discover.

To deploy clients, create client configurations and credentials. Then use those configurations to create deployments, which are targeted at specific sets of unmanaged endpoints. The Tanium Module Server installs the Tanium Client on the targeted endpoints. Depending on the results, you can reuse the configurations to try deployments again or target different sets of 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 for use in manual deployment.

CLIENT CONFIGURATIONS

Create client configurations that are specific to a deployment. The settings in a client configuration include the version of the Tanium Client to deploy and the Tanium Server or Zone Server with which to associate the client. Client configurations can also contain tags, which identify the endpoints after the client is installed.

CREDENTIALS

Configure a list of credentials that the Module Server uses to sign in to endpoints for installation of the Tanium Client. The Module Server attempts to install the Tanium Client on endpoints using each set of credentials in the order in which you defined them.

DEPLOYMENTS

Create and run a deployment that defines the targeted endpoints and deploys the Tanium Client to those endpoints. You can also choose whether to upgrade or reinstall existing clients that are in the targeted group.

Client health monitoring

After clients are installed, you can use Client Management to continuously monitor client health. 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 that apply client settings (such as logging level and cache size) to different groups of clients.

Client upgrade

Use client upgrades in Client Management to upgrade 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. Create a one-time upgrade to upgrade clients within a specified window of time. 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.

Interoperability with other Tanium products

DISCOVER

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

INDEX

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

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

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 Tanium Trends User Guide: Importing the initial gallery.

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. By default, 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 by default at a randomized interval of 30 to 90 seconds. 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.

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.

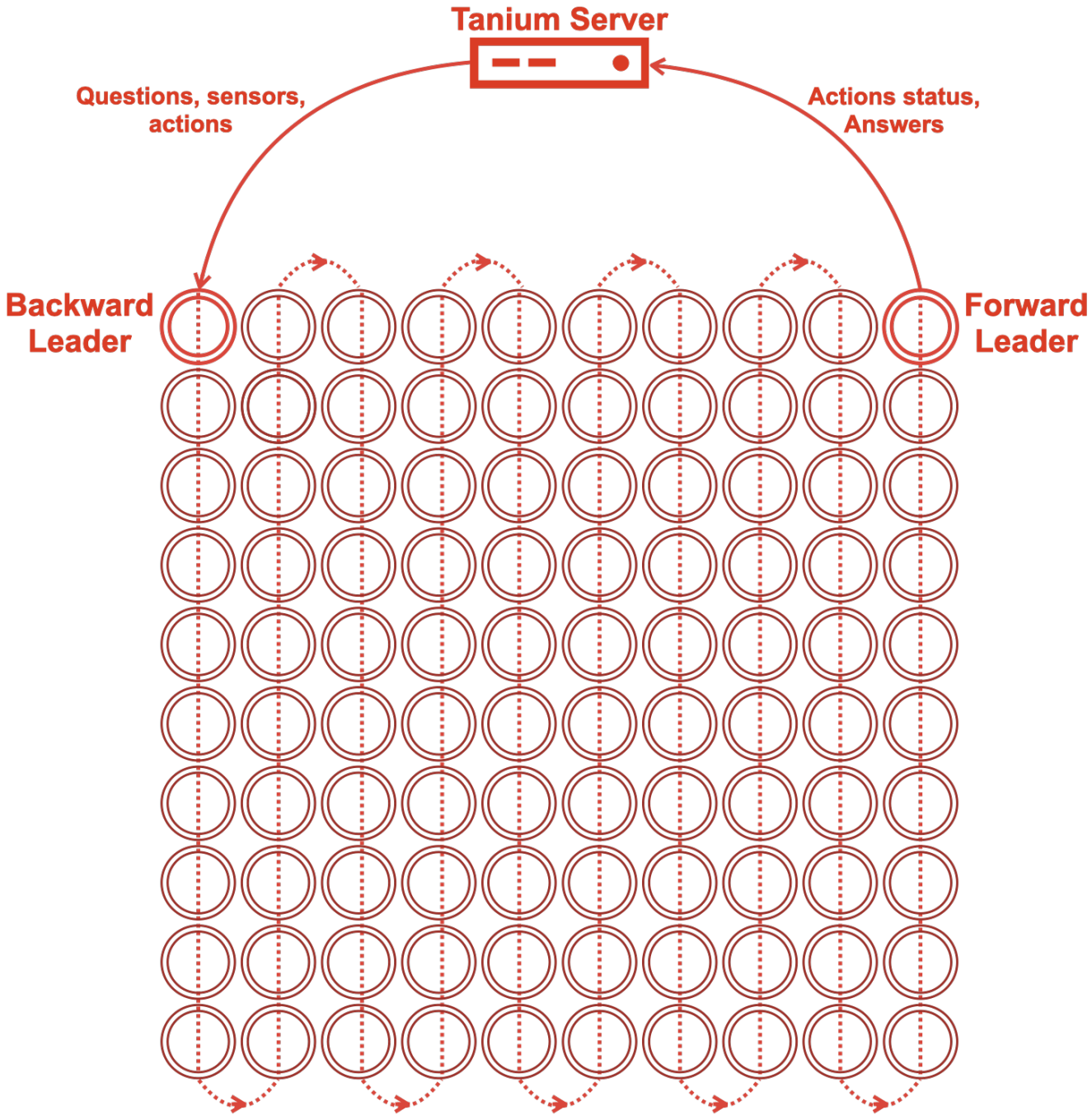
To customize client peering settings to suit your deployment, see Configuring Tanium Client peering on page 202.

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 sensors, 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.

Tanium Clients establish outgoing connections to backward peers for file distribution (see File distribution on page 24).

Figure 1: Tanium Client linear chain



Forward and backward reflection

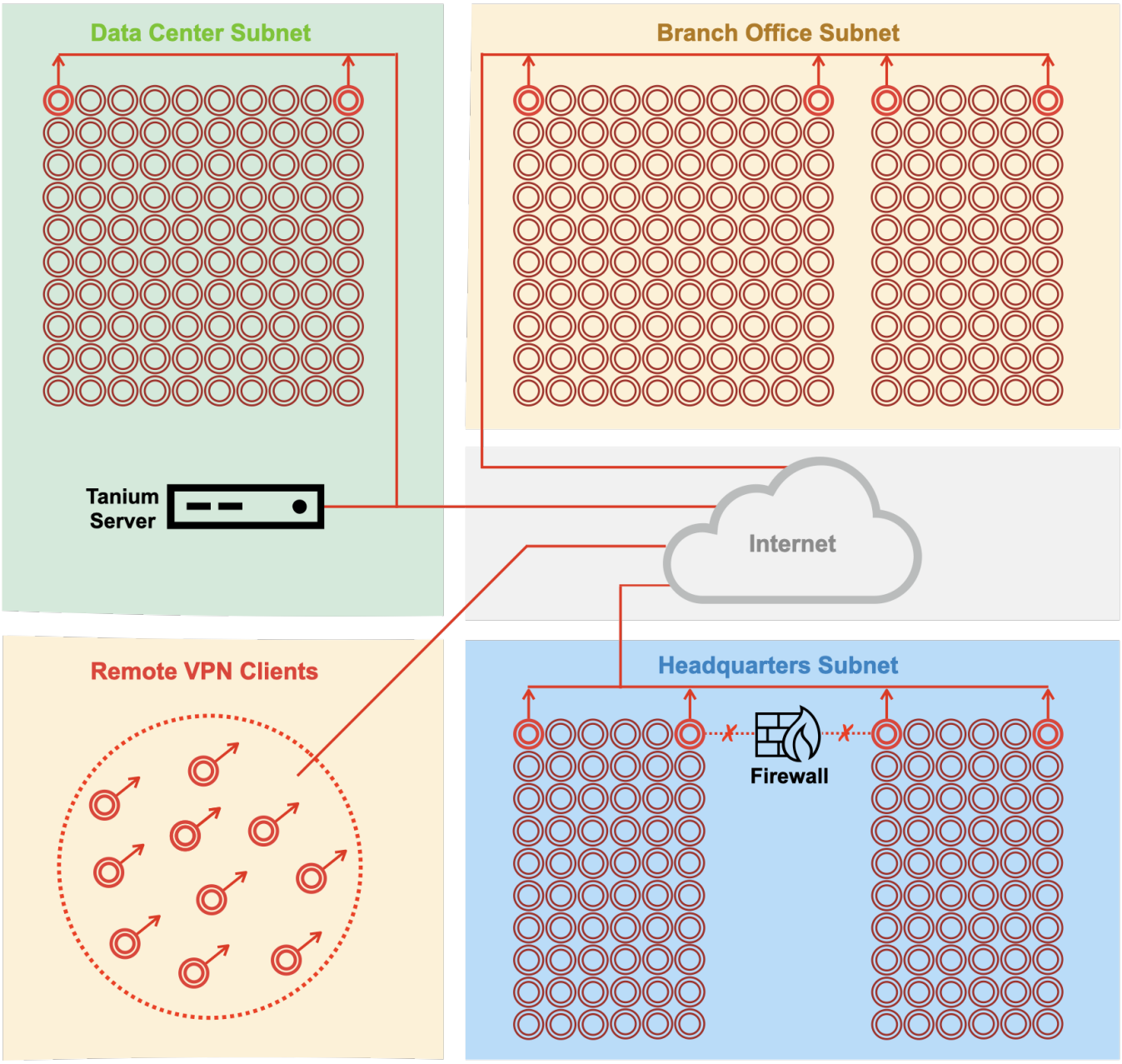
Tanium peer communication is designed to accommodate new clients that come online, to route around clients that are removed or stop communicating effectively, and to *reflect* around network-level blockages, such as firewall blocking. *Forward reflection* occurs if a Tanium Client cannot establish an 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 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



Satellites

Satellites are specific Tanium Clients that you designate to run certain targeted, secure workloads on behalf of the Module Server, such as non-line-of-sight scans in Discover or remote authenticated scans in Comply.

Because the server might need to send sensitive, encrypted data (such as credentials) to a satellite when running a workload, you must verify each endpoint that you designate as a satellite to prevent spoofing attacks. Any such sensitive data is never sent using the linear chain, nor is it stored on-disk on the satellite.

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

For more information about managing satellites, see Tanium Direct Connect User Guide: 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.

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 supports Transport Layer Security (TLS) for encrypted communication in connections from Tanium Clients to the Tanium Server or Zone Server. Tanium Client 7.4 or later uses TLS communication by default between client peers. For details, see the Tanium Appliance User Guide: Securing Tanium Server, Zone Server, and Tanium Client access or Tanium Core Platform User Guide for Windows Deployments: 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 Endpoint Configuration User Guide: Managing endpoint tools.

Each client extension and tool has required security exclusions to allow the Tanium processes to run without interference. See Reference: Endpoint security exclusions on page 315 and for Windows-based Tanium Core Platform deployments, Tanium Core Platform User Guide for Windows Deployments: Tanium Core Platform server security exclusions, or the requirements section for each solution.

Client extensions can run in separate processes, or together in a single process, depending on whether *client extension shared process mode* is enabled. See Endpoint Configuration User Guide: Manage client extension shared process mode.

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 Tanium Endpoint Configuration User Guide: Identify and resolve issues with endpoint tools or client extensions.

For a list of client extensions used for each solution, see Reference: Client extensions used for Tanium solutions on page 429.

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 OS versions for Tanium Client hosts (continued) on page 61 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. See Hardware requirements on page 63 for baseline RAM and disk space requirements.

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 (continued) on page 67 table provides links to the user guide sections that list these requirements.

Windows endpoints must have the following root certificate authority (CA) certificates because they are required to verify the integrity of the Tanium Client binaries:

- DigiCert Assured ID Root CA
  (thumbprint `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
  (thumbprint `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
  (thumbprint `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
  (thumbprint `92:C1:58:8E:85:AF:22:01:CE:79:15:E8:53:8B:49:2F:60:5B:80:C6`)

For certificate downloads, see DigiCert: Download DigiCert root and intermediate certificates, and for more information about installing certificates, see DigiCert Support.

Supported operating systems

The following table lists supported operating systems and versions for endpoints connected to an on-premises Tanium installation and the versions of the Tanium Client that are supported for each OS version in an on-premises Tanium installation. The table also indicates Client Management service support for each OS version.

You cannot use Client Management to install a Tanium Client version earlier than 7.4.7.1094.

Supported OS versions for Tanium Client hosts

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
Microsoft Windows Server	• Windows Server 2022 • Windows Server 2019 (currently supported releases in the Long-Term Servicing Channel and the last supported release in the Semi-Annual Channel) • Windows Server 2016 • Windows Server 2012, 2012 R2 • Windows Server 2008 R2	x86	7.4.10.1086 7.4.10.1075 7.4.10.1067 7.4.10.1060 7.4.10.1054 7.4.10.1034 7.4.9.1077 7.4.9.1062 7.4.9.1046 7.4.8.1054 7.4.8.1042 7.4.7.1183 7.4.7.1179 7.4.7.1130 7.4.7.1094 7.4.5.1225 7.4.5.1220 7.4.5.1219 7.4.5.1204 7.4.4.1362 7.4.4.1250 7.4.2.2073 7.4.2.2063 7.4.2.2033 7.4.1.1955 7.2.314.3660 7.2.314.3657 7.2.314.3632 7.2.314.3584 7.2.314.3476	✅	• Standard, Enterprise, and Datacenter editions are supported, with or without the Server Core option enabled. The Nano Server option is not supported. • Some Tanium sensors and packages require unrestricted access to Windows Management Instrumentation (WMI) queries, VBScript execution in Windows Script Host (WSH), and PowerShell. If you restrict any of these features on endpoints, Tanium functionality is limited. • For Tanium Client versions 7.2.314.3584 and later, PowerShell-based sensors require PowerShell 3.0 or later. You must update the default PowerShell on Windows Server 2008 or Windows Server 2008 R2 for PowerShell-based sensors to work on those endpoints. • Tanium™ Endpoint Configuration and Tanium modules do	

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
	Windows Server 2008	x86	7.2.314.3660 7.2.314.3657 7.2.314.3632 7.2.314.3584 7.2.314.3476	✗		

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
Microsoft Windows Workstation	• Windows 11 • Windows 10 (currently supported releases in both the Semi-Annual Channel and the Long-Term Servicing Channel) • Windows 8 • Windows 7 (SP1)	x86	7.4.10.1086 7.4.10.1075 7.4.10.1067 7.4.10.1060 7.4.10.1054 7.4.10.1034 7.4.9.1077 7.4.9.1062 7.4.9.1046 7.4.8.1054 7.4.8.1042 7.4.7.1183 7.4.7.1179 7.4.7.1130 7.4.7.1094 7.4.5.1225 7.4.5.1220 7.4.5.1219 7.4.5.1204 7.4.4.1362 7.4.4.1250 7.4.2.2073 7.4.2.2063 7.4.2.2033 7.4.1.1955 7.2.314.3660 7.2.314.3657 7.2.314.3632 7.2.314.3584 7.2.314.3476	✅	• Tanium Client 7.4.10.1054 or later supports running the x86 binary on Windows 11 endpoints with Arm processors. Windows RT is not supported. Arm processor support on Windows 11 also requires Tanium Client Management 1.12.150. Support for each solution might require a specific minimum version of that solution, and some solutions have specific limitations for Windows 11 endpoints with Arm processors. For more information, see the release notes and User Guide for each solution. • Some Tanium sensors and packages require unrestricted access to Windows Management Instrumentation (WMI) queries, VBScript execution in Windows Script Host (WSH), and PowerShell. If you restrict any of these features on endpoints, Tanium functionality is	

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes
macOS	• macOS 14 Sonoma • macOS 13 Ventura • macOS 12 Monterey • macOS 11 Big Sur	Universal x86-64	7.4.10.1086 7.4.10.1075 7.4.10.1067 7.4.10.1060 7.4.10.1054 7.4.10.1034 7.4.9.1077 7.4.9.1062 7.4.9.1046 7.4.8.1054 7.4.8.1042 7.4.7.1183 7.4.7.1179 7.4.7.1130 7.4.7.1094 7.4.5.1225 7.4.5.1220 7.4.5.1219 7.4.5.1204 7.4.4.1362 7.4.4.1250 7.4.2.2073 7.4.2.2063 7.4.2.2033 7.4.1.1955 7.2.314.3660 7.2.314.3657 7.2.314.3632 7.2.314.3608 7.2.314.3476 7.2.314.3236	✅	• The universal binary is available only in Tanium Client 7.4.9.1046 or later. • 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. • Tanium recommends replacing the x86-64 binary with the universal binary on all Mac computers running macOS 11 or later. 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 or perform a reinstallation that includes wiping data with Tanium Client Management. If you upgrade the x86-64 client in

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
	• macOS 10.15 Catalina • macOS 10.14 Mojave • macOS 10.13 High Sierra	x86-64	7.4.10.1086 7.4.10.1075 7.4.10.1067 7.4.10.1060 7.4.10.1054 7.4.10.1034 7.4.9.1077 7.4.9.1062 7.4.9.1046 7.4.8.1054 7.4.8.1042 7.4.7.1183 7.4.7.1179 7.4.7.1130 7.4.7.1094 7.4.5.1225 7.4.5.1220 7.4.5.1219 7.4.5.1204 7.4.4.1362 7.4.4.1250 7.4.2.2073 7.4.2.2063 7.4.2.2033 7.4.1.1955 7.2.314.3660 7.2.314.3657 7.2.314.3632 7.2.314.3608 7.2.314.3476 7.2.314.3236	✅	• **(macOS 10.15 or later)** Apple introduced the app notarization requirement as a security process in macOS 10.15. If you enable the requirement, you must install Tanium Client 7.2.314.3608 or later on endpoints that run macOS 10.15 or later. • **(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 107 (for deployment with Client Management) or Deploy the Tanium Client to macOS endpoints using the installer on page 145. • **(macOS 10.14 or later)** The Tanium Core Platform requires Tanium™ Default Content 7.1.7 or later to	

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
Linux	Amazon Linux 2023	x86-64 ARM64	7.4.10.1086 7.4.10.1075 7.4.10.1067		• Support for ARM64 architecture for each solution requires a specific minimum version of that solution. For more information, see solution release notes.	

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
	Amazon Linux 2 LTS	x86-64 ARM64	7.4.10.1086 7.4.10.1075 7.4.10.1067 7.4.10.1060 7.4.10.1054 7.4.10.1034 7.4.9.1077 7.4.9.1062 7.4.9.1046 7.4.8.1054 7.4.8.1042 7.4.7.1183 7.4.7.1179 7.4.7.1130 7.4.7.1094 7.4.5.1225 7.4.5.1220 7.4.5.1219 7.4.5.1204 7.4.4.1362 7.4.4.1250 7.4.2.2073 7.4.2.2063 7.4.2.2033 7.4.1.1955 7.2.314.3660 7.2.314.3657 7.2.314.3632 7.2.314.3584 7.2.314.3476		• ARM64 support is available only in Tanium Client 7.4.7.1130 or later. • Support for ARM64 architecture for each solution requires a specific minimum version of that solution. For more information, see solution release notes.	

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
	Amazon Linux 1 AMI (2018.03)	x86-64	7.4.10.1086 7.4.10.1075 7.4.10.1067 7.4.10.1060 7.4.10.1054 7.4.10.1034 7.4.9.1077 7.4.9.1062 7.4.9.1046 7.4.8.1054 7.4.8.1042 7.4.7.1183 7.4.7.1179 7.4.7.1130 7.4.7.1094 7.4.5.1225 7.4.5.1220 7.4.5.1219 7.4.5.1204 7.4.4.1362 7.4.4.1250 7.4.2.2073 7.4.2.2063 7.4.2.2033 7.4.1.1955 7.2.314.3660 7.2.314.3657 7.2.314.3632 7.2.314.3584 7.2.314.3476			

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
	Debian 12.x	x86-64 ARM	7.4.10.1086 7.4.10.1075	✅		

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
	Debian 11.x	x86-64	7.4.10.1086 7.4.10.1075 7.4.10.1067 7.4.10.1060 7.4.10.1054 7.4.10.1034 7.4.9.1077 7.4.9.1062 7.4.9.1046 7.4.8.1054 7.4.8.1042	✅		

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
	Debian 10.x	x86-64	7.4.10.1086 7.4.10.1075 7.4.10.1067 7.4.10.1060 7.4.10.1054 7.4.10.1034 7.4.9.1077 7.4.9.1062 7.4.9.1046 7.4.8.1054 7.4.8.1042 7.4.7.1183 7.4.7.1179 7.4.7.1130 7.4.7.1094 7.4.5.1225 7.4.5.1220 7.4.5.1219 7.4.5.1204 7.4.4.1362 7.4.4.1250 7.4.2.2073 7.4.2.2063			

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
	Debian 9.x, 8.x	x86 x86-64	7.4.10.1086 7.4.10.1075 7.4.10.1067 7.4.10.1060 7.4.10.1054 7.4.10.1034 7.4.9.1077 7.4.9.1062 7.4.9.1046 7.4.8.1054 7.4.8.1042 7.4.7.1183 7.4.7.1179 7.4.7.1130 7.4.7.1094 7.4.5.1225 7.4.5.1220 7.4.5.1219 7.4.5.1204 7.4.4.1362 7.4.4.1250 7.4.2.2073 7.4.2.2063 7.4.2.2033 7.4.1.1955 7.2.314.3660 7.2.314.3657 7.2.314.3632 7.2.314.3584 7.2.314.3476			

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
	Debian 7.x, 6.x	x86-64	7.2.314.3660 7.2.314.3657 7.2.314.3632 7.2.314.3584 7.2.314.3476	✅	• TSDB-CX, which is a client extension 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.	

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
	Oracle Linux 9.x	x86-64 ARM64	7.4.10.1086 7.4.10.1075 7.4.10.1067 7.4.10.1060 7.4.10.1054 7.4.10.1034 7.4.9.1077 7.4.9.1062	✅	• ARM64 support is available only in Tanium Client 7.4.10.1034 or later. • Support for ARM64 architecture for each solution requires a specific minimum version of that solution. For more information, see solution release notes.	

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
	Oracle Linux 8.x	x86-64 ARM64	7.4.10.1086 7.4.10.1075 7.4.10.1067 7.4.10.1060 7.4.10.1054 7.4.10.1034 7.4.9.1077 7.4.9.1062 7.4.9.1046 7.4.8.1054 7.4.8.1042 7.4.7.1183 7.4.7.1179 7.4.7.1130 7.4.7.1094 7.4.5.1225 7.4.5.1220 7.4.5.1219 7.4.5.1204 7.4.4.1362 7.4.4.1250 7.4.2.2073 7.4.2.2063 7.2.314.3660 7.2.314.3657 7.2.314.3632		• ARM64 support is available only in Tanium Client 7.4.10.1034 or later. • Support for ARM64 architecture for each solution requires a specific minimum version of that solution. For more information, see solution release notes.	

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
	Oracle Linux 7.x	x86 x86-64	7.4.10.1086 7.4.10.1075 7.4.10.1067 7.4.10.1060 7.4.10.1054 7.4.10.1034 7.4.9.1077 7.4.9.1062 7.4.9.1046 7.4.8.1054 7.4.8.1042 7.4.7.1183 7.4.7.1179 7.4.7.1130 7.4.7.1094 7.4.5.1225 7.4.5.1220 7.4.5.1219 7.4.5.1204 7.4.4.1362 7.4.4.1250 7.4.2.2073 7.4.2.2063 7.2.314.3660 7.2.314.3657 7.2.314.3632			

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
	Oracle Linux 6.x	x86 x86-64	7.4.10.1086 7.4.10.1075 7.4.10.1067 7.4.10.1060 7.4.10.1054 7.4.10.1034 7.4.9.1077 7.4.9.1062 7.4.9.1046 7.4.8.1054 7.4.8.1042 7.4.7.1183 7.4.7.1179 7.4.7.1130 7.4.7.1094 7.4.5.1225 7.4.5.1220 7.4.5.1219 7.4.5.1204 7.4.4.1362 7.4.4.1250 7.4.2.2073 7.4.2.2063 7.2.314.3660 7.2.314.3657 7.2.314.3632		• TSDB-CX, which is a client extension 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.	

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
	Oracle Linux 5.x	x86-64	7.4.10.1086 7.4.10.1075 7.4.10.1067 7.4.10.1060 7.4.10.1054 7.4.10.1034 7.4.9.1077 7.4.9.1062 7.4.9.1046 7.4.8.1054 7.4.8.1042 7.4.7.1183 7.4.7.1179 7.4.7.1130 7.4.7.1094 7.4.5.1225 7.4.5.1220 7.4.5.1219 7.4.5.1204 7.4.4.1362 7.4.4.1250 7.4.2.2073 7.4.2.2063 7.4.2.2033 7.4.1.1955 7.2.314.3660 7.2.314.3657 7.2.314.3632 7.2.314.3584 7.2.314.3476 7.2.314.3236	✅	• TSDB-CX, which is a client extension 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.	

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
	• Red Hat Enterprise Linux (RHEL) 9.x • AlmaLinux 9.x • Rocky Linux 9.x	x86-64 ARM64	7.4.10.1086 7.4.10.1075 7.4.10.1067 7.4.10.1060 7.4.10.1054 7.4.10.1034 7.4.9.1077 7.4.9.1062 7.4.9.1046	✅	• ARM64 support is available only in Tanium Client 7.4.10.1034 or later. • Support for ARM64 architecture for each solution requires a specific minimum version of that solution. For more information, see solution release notes.	

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
	• Red Hat Enterprise Linux (RHEL) 8.x • CentOS 8.x • AlmaLinux 8.x • Rocky Linux 8.x	x86-64 ARM64	7.4.10.1086 7.4.10.1075 7.4.10.1067 7.4.10.1060 7.4.10.1054 7.4.10.1034 7.4.9.1077 7.4.9.1062 7.4.9.1046 7.4.8.1054 7.4.8.1042 7.4.7.1183 7.4.7.1179 7.4.7.1130 7.4.7.1094 7.4.5.1225 7.4.5.1220 7.4.5.1219 7.4.5.1204 7.4.4.1362 7.4.4.1250 7.4.2.2073 7.4.2.2063 7.4.2.2033 7.4.1.1955 7.2.314.3660 7.2.314.3657 7.2.314.3632 7.2.314.3584	✅	• ARM64 support is available only in Tanium Client 7.4.10.1034 or later. • Support for ARM64 architecture for each solution requires a specific minimum version of that solution. For more information, see solution release notes. • **(CentOS 8.x)** CentOS Stream is a separate distribution and is not supported. • In Client Management, you can deploy only Tanium Client 7.4.5.1204 or later to AlmaLinux or Rocky Linux.	

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
	• Red Hat Enterprise Linux (RHEL) 7.x • CentOS 7.x	x86 x86-64	7.4.10.1086 7.4.10.1075 7.4.10.1067 7.4.10.1060 7.4.10.1054 7.4.10.1034 7.4.9.1077 7.4.9.1062 7.4.9.1046 7.4.8.1054 7.4.8.1042 7.4.7.1183 7.4.7.1179 7.4.7.1130 7.4.7.1094 7.4.5.1225 7.4.5.1220 7.4.5.1219 7.4.5.1204 7.4.4.1362 7.4.4.1250 7.4.2.2073 7.4.2.2063 7.4.2.2033 7.4.1.1955 7.2.314.3660 7.2.314.3657 7.2.314.3632 7.2.314.3584 7.2.314.3476	✅		

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
	• Red Hat Enterprise Linux (RHEL) 6.x • CentOS 6.x	x86 x86-64	7.4.10.1086 7.4.10.1075 7.4.10.1067 7.4.10.1060 7.4.10.1054 7.4.10.1034 7.4.9.1077 7.4.9.1062 7.4.9.1046 7.4.8.1054 7.4.8.1042 7.4.7.1183 7.4.7.1179 7.4.7.1130 7.4.7.1094 7.4.5.1225 7.4.5.1220 7.4.5.1219 7.4.5.1204 7.4.4.1362 7.4.4.1250 7.4.2.2073 7.4.2.2063 7.4.2.2033 7.4.1.1955 7.2.314.3660 7.2.314.3657 7.2.314.3632 7.2.314.3584 7.2.314.3476		• TSDB-CX, which is a client extension 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.	

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
	• Red Hat Enterprise Linux (RHEL) 5.x • CentOS 5.x	x86 x86-64	7.4.10.1086 7.4.10.1075 7.4.10.1067 7.4.10.1060 7.4.10.1054 7.4.10.1034 7.4.9.1077 7.4.9.1062 7.4.9.1046 7.4.8.1054 7.4.8.1042 7.4.7.1183 7.4.7.1179 7.4.7.1130 7.4.7.1094 7.4.5.1225 7.4.5.1220 7.4.5.1219 7.4.5.1204 7.4.4.1362 7.4.4.1250 7.4.2.2073 7.4.2.2063 7.4.2.2033 7.4.1.1955 7.2.314.3660 7.2.314.3657 7.2.314.3632 7.2.314.3584 7.2.314.3476 7.2.314.3236	✅	• **(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 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.	

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
	• SUSE Linux Enterprise Server (SLES) 15 • openSUSE 15.x	x86-64	7.4.10.1086 7.4.10.1075 7.4.10.1067 7.4.10.1060 7.4.10.1054 7.4.10.1034 7.4.9.1077 7.4.9.1062 7.4.9.1046 7.4.8.1054 7.4.8.1042 7.4.7.1183 7.4.7.1179 7.4.7.1130 7.4.7.1094 7.4.5.1225 7.4.5.1220 7.4.5.1219 7.4.5.1204 7.4.4.1362 7.4.4.1250 7.4.2.2073 7.4.2.2063 7.4.2.2033 7.4.1.1955 7.2.314.3660 7.2.314.3657 7.2.314.3632			

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
	• SUSE Linux Enterprise Server (SLES) 12 • openSUSE 12.x	x86-64	7.4.10.1086 7.4.10.1075 7.4.10.1067 7.4.10.1060 7.4.10.1054 7.4.10.1034 7.4.9.1077 7.4.9.1062 7.4.9.1046 7.4.8.1054 7.4.8.1042 7.4.7.1183 7.4.7.1179 7.4.7.1130 7.4.7.1094 7.4.5.1225 7.4.5.1220 7.4.5.1219 7.4.5.1204 7.4.4.1362 7.4.4.1250 7.4.2.2073 7.4.2.2063 7.4.2.2033 7.4.1.1955 7.2.314.3660 7.2.314.3657 7.2.314.3632 7.2.314.3584			

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
	• SUSE Linux Enterprise Server (SLES) 11.3, 11.4 • openSUSE 11.3, 11.4	x86-64	7.2.314.3660 7.2.314.3657 7.2.314.3632 7.2.314.3584	✅	• TSDB-CX, which is a client extension 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.	

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
	Ubuntu 22.04 LTS	x86-64	7.4.10.1086 7.4.10.1075 7.4.10.1067 7.4.10.1060 7.4.10.1054 7.4.10.1034 7.4.9.1077 7.4.9.1062 7.4.9.1046 7.4.8.1054 7.4.8.1042	✅		

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
		ARM64	7.4.10.1086 7.4.10.1075	✅		

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
	Ubuntu 20.04 LTS	x86-64	7.4.10.1086 7.4.10.1075 7.4.10.1067 7.4.10.1060 7.4.10.1054 7.4.10.1034 7.4.9.1077 7.4.9.1062 7.4.9.1046 7.4.8.1054 7.4.8.1042 7.4.7.1183 7.4.7.1179 7.4.7.1130 7.4.7.1094 7.4.5.1225 7.4.5.1220 7.4.5.1219 7.4.5.1204 7.4.4.1362 7.4.4.1250 7.4.2.2073 7.4.2.2063			

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
	Ubuntu 18.04 LTS	x86-64	7.4.10.1086 7.4.10.1075 7.4.10.1067 7.4.10.1060 7.4.10.1054 7.4.10.1034 7.4.9.1077 7.4.9.1062 7.4.9.1046 7.4.8.1054 7.4.8.1042 7.4.7.1183 7.4.7.1179 7.4.7.1130 7.4.7.1094 7.4.5.1225 7.4.5.1220 7.4.5.1219 7.4.5.1204 7.4.4.1362 7.4.4.1250 7.4.2.2073 7.4.2.2063 7.4.2.2033 7.4.1.1955 7.2.314.3660 7.2.314.3657 7.2.314.3632 7.2.314.3584 7.2.314.3476			

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
	Ubuntu 16.04 LTS	x86-64	7.4.10.1086 7.4.10.1075 7.4.10.1067 7.4.10.1060 7.4.10.1054 7.4.10.1034 7.4.9.1077 7.4.9.1062 7.4.9.1046 7.4.8.1054 7.4.8.1042 7.4.7.1183 7.4.7.1179 7.4.7.1130 7.4.7.1094 7.4.5.1225 7.4.5.1220 7.4.5.1219 7.4.5.1204 7.4.4.1362 7.4.4.1250 7.4.2.2073 7.4.2.2063 7.4.2.2033 7.4.1.1955 7.2.314.3660 7.2.314.3657 7.2.314.3632 7.2.314.3584 7.2.314.3476			

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
	Ubuntu 14.04 LTS	x86-64	7.4.10.1086 7.4.10.1075 7.4.10.1067 7.4.10.1060 7.4.10.1054 7.4.10.1034 7.4.9.1077 7.4.9.1062 7.4.9.1046 7.4.8.1054 7.4.8.1042 7.4.7.1183 7.4.7.1179 7.4.7.1130 7.4.7.1094 7.4.5.1225 7.4.5.1220 7.4.5.1219 7.4.5.1204 7.4.4.1362 7.4.4.1250 7.4.2.2073 7.4.2.2063 7.4.2.2033 7.4.1.1955 7.2.314.3660 7.2.314.3657 7.2.314.3632 7.2.314.3584 7.2.314.3476			

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes
AIX	IBM AIX 7.1 TL4 or later	POWER	7.4.10.1086 7.4.10.1075 7.4.10.1067 7.4.10.1060 7.4.10.1054 7.4.10.1034 7.4.9.1077 7.4.9.1062 7.4.9.1046 7.4.8.1054 7.4.8.1042 7.4.7.1183 7.4.7.1179 7.4.7.1130 7.4.7.1094 7.4.5.1225 7.4.5.1220 7.4.5.1219 7.4.5.1204 7.4.4.1362 7.4.4.1250 7.2.314.3660 7.2.314.3657 7.2.314.3632 7.2.314.3584		• The Tanium Client for AIX requires a 64-bit operating system and the IBM XL C++ runtime environment file set (`xlC.rte`), and, in most cases, the IBM LLVM runtime libraries file set (`libc++.rte`). For specific requirements for each file set and installation steps, see Prepare for deployment to Linux, macOS, Solaris, or AIX endpoints on page 107 (for deployment using Client Management) or Deploy the Tanium Client to AIX endpoints using a package file on page 162. • Summary client health information in Client Management includes AIX endpoints, but you cannot use Direct Connect to access detailed client health information. • Tanium™ Endpoint Configuration and Tanium modules do not support AIX versions earlier than 7.1 TL4. On these versions of

Supported OS versions for Tanium Client hosts (continued)

Operating system	OS Version	Available Executables	Tanium Client Version	Supported by Client Management	Notes	
	• IBM AIX 7.1 TL1 (Service Pack 10 or later) • IBM AIX 7.1 TL2 • IBM AIX 7.1 TL3	POWER	7.2.314.3660 7.2.314.3657 7.2.314.3632 7.2.314.3584	✗		
Solaris	• Oracle Solaris 11 • Oracle Solaris 10 U8 or higher	SPARC x86	7.4.10.1086 7.4.10.1075 7.4.10.1067 7.4.10.1060 7.4.10.1054 7.4.10.1034 7.4.9.1077 7.4.9.1062 7.4.9.1046 7.4.8.1054 7.4.8.1042 7.4.7.1183 7.4.7.1179 7.4.7.1130 7.4.7.1094 7.4.5.1225 7.4.5.1220 7.4.5.1219 7.4.5.1204 7.4.4.1362 7.4.4.1250 7.4.2.2073 7.4.2.2063 7.4.2.2033 7.4.1.1955 7.2.314.3660 7.2.314.3657 7.2.314.3632 7.2.314.3584	✓	• The Tanium Client for Solaris requires SUNWgccruntime on Solaris 10 and 11.0–11.3. • 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

Table 1 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 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 297 for details)
- ❌: No support

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.

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.

Table 1: 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	✅	✅	✅	❌

Table 1: Tanium Client OS product support (continued)

Product	Windows	macOS	Linux	Solaris and AIX
Direct Connect	—	✓	✓	✗
Screen Sharing add-in for Direct Connect	✓	—	✗	✗
Discover	✓	✓	✓	—
Endpoint Configuration	✓	✓	✓	✓
End-User Notifications	✓	—	✗	✗
Enforce	✓	✓	—	✗
Engage	✓	✗	✗	✗
Impact	✓	✗	✗	✗
Integrity Monitor	✓	✗	✓	—
Investigate	✓	✓	✓	✗
Mac Device Enrollment	✗	✓	✗	✗
Patch	✓	✓	—	✗
Performance	✓	✓	✓	✗
Provision	✓	—	—	✗
Reveal	✓	✓	✓	✗
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 for guidance on specific configurations.

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 (continued) on page 67 table.)

Additional hardware requirements for specific modules

Product	Additional available disk space	Minimum RAM required
Tanium™ Comply	200 MB	2 GB[1]
Tanium™ Deploy	2 GB[2]	2 GB[1]
Tanium™ Integrity Monitor	1 GB[3,4]	4 GB
Tanium™ Investigate	3 GB[4]	4 GB
Tanium™ Patch	5 GB[2]	2 GB[1,5]
Tanium™ Performance	100 MB plus the amount specified in the **Database maximum size** parameter (1 GB by default)[6]	2 GB[1]
Tanium™ Software Bill of Materials (SBOM) add-in for Tanium™ Asset	1 GB[3]	2 GB[1]
Tanium™ Reveal	2 GB[3,4]	2 GB[1]

Additional hardware requirements for specific modules (continued)

Product	Additional available disk space	Minimum RAM required
Tanium™ Threat Response	3 GB[3,4]	4 GB

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

[2] 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.

[3] This solution uses Tanium™ Index. Specific disk space requirements for Index depend on the file system on the endpoint. Depending on these factors, the disk space that is required on the endpoint might be greater than the amount listed here. A general guideline is that the database size is an additional 1 MB per 1 GB of files on disk.

[4] This solution uses Tanium™ Recorder. Specific disk space requirements for Recorder depend on the number of events recorded on the endpoint. Depending on these factors, the disk space that is required on the endpoint might be greater than the amount listed here.

[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.

Module and service requirements

Click the links in the following table to see the minimum Tanium Client version (Tanium dependencies) and client endpoint requirements for each Tanium module and shared service.

Solution-specific requirements for the Tanium Client and endpoints

Product	Tanium Dependencies	Endpoint Requirements
Tanium™ Asset	Core platform dependencies	Endpoints
Tanium™ Software Bill of Materials (SBOM) add-in for Asset	Core platform dependencies	Endpoints
Tanium™ Benchmark	Core platform dependencies	Endpoints
Tanium™ Certificate Manager	Core platform dependencies	Endpoints
Tanium™ Client Management	Core platform dependencies (following this section)	The following sections: • Table 1 (in this section) • Port requirements for Client Management • Security exclusions for Client Management

Solution-specific requirements for the Tanium Client and endpoints (continued)

Product	Tanium Dependencies	Endpoint Requirements
Tanium™ Comply	Core platform dependencies	Endpoints
Tanium™ Connect	Core platform dependencies	N/A
Tanium™ Criticality	Core platform dependencies	N/A
Tanium™ Deploy	Core platform dependencies	Endpoints
Tanium™ Direct Connect	Core platform dependencies	Endpoints
Tanium™ Screen Sharing add-in for Direct Connect	No additional requirements	Endpoints
Tanium™ Directory Query	Core platform dependencies	N/A
Tanium™ Discover	Core platform dependencies	Endpoints
Tanium™ Endpoint Configuration	Core platform dependencies	Endpoints
Tanium™ End-User Notifications	Core platform dependencies	Endpoints
Tanium™ Enforce	Core platform dependencies	Endpoints
Tanium™ Engage	Core platform dependencies	Endpoints
Tanium™ Feed	Core platform dependencies	N/A
Tanium™ Gateway	Core platform dependencies	N/A
Tanium™ Health Check	Core platform dependencies	N/A
Tanium™ Impact	Core platform dependencies	Endpoints
Tanium™ Integrity Monitor	Core platform dependencies	Endpoints
Tanium™ Interact	Core platform dependencies	Endpoints
Tanium™ Investigate	Core platform dependencies	Endpoints
Tanium™ Mac Device Enrollment	Core platform dependencies	Endpoints
Tanium™ Network Quarantine	Core platform dependencies	Endpoints
Tanium™ Patch	Core platform dependencies	Endpoints
Tanium™ Performance	Core platform dependencies	Endpoints
Tanium™ Provision	Core platform dependencies	Endpoints
Tanium™ Reporting	Core platform dependencies	N/A

Solution-specific requirements for the Tanium Client and endpoints (continued)

Product	Tanium Dependencies	Endpoint Requirements
Tanium™ Reputation	Core platform dependencies	N/A
Tanium™ Reveal	Core platform dependencies	Endpoints
Tanium™ Threat Response	Core platform dependencies	Endpoints
Tanium™ Trends	Core platform dependencies	N/A
Tanium™ Zero Trust	Core platform dependencies	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 OS versions for Tanium Client hosts (continued) on page 61.

- **Windows**
  - 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

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
- **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™ Core Platform servers**: 7.5.2.3531 or later
- **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 a supported Tanium Client (see Supported OS versions for Tanium Client hosts (continued) on page 61).

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.

Some Client Management dependencies have their own dependencies, which you can see by clicking the links in the lists of Required dependencies on page 69 and Feature-specific dependencies on page 69. Note that the links open the user guides for the latest version of each solution, not necessarily the minimum version that Client Management requires.

When you install Endpoint Configuration (or a version of Client Management between 1.5 and 1.12, which included Endpoint Configuration):

- Make sure you upgrade each module that uses Endpoint Configuration to a version from after support for Endpoint Configuration was introduced (follow links for Tanium Dependencies from and see the release notes for each module).
- After Endpoint Configuration is installed, do not use the **Initial Content - Python** solution to deploy Python to endpoints that support Endpoint Configuration (see Tanium Endpoint Configuration User Guide: Endpoints).

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 Tanium Console User Guide: 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. See Tanium Console User Guide: Import all modules and services.

IMPORT SPECIFIC SOLUTIONS

If you select only Client Management to import and are using Tanium Core Platform 7.5.2.3531 or later with Tanium Console 3.0.72 or later, 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.

If you select only Client Management to import and you are using Tanium Core Platform 7.5.2.3503 or earlier with Tanium Console 3.0.64 or earlier, you must manually import or update required dependencies. See Tanium Console User Guide: Import, re-import, or update specific solutions.

REQUIRED DEPENDENCIES

Client Management has the following required dependencies at the specified minimum versions:

- Tanium™ Direct Connect 2.9.75 or later
- Tanium™ Endpoint Configuration 2.0.208 or later
- Tanium™ RDB 1.2.11 or later
- Tanium™ Reporting 1.32.62 or later
- Tanium™ Secrets 1.0.41 or later
- Tanium™ System User service 1.0.77 or later
- Tanium™ Trends 3.9.127 or later

FEATURE-SPECIFIC DEPENDENCIES

Client Management has the following feature-specific dependencies at the specified minimum versions:

- Tanium Interact 2.4.50 or later is required to view charts on the Client Management **Overview** page
  Interact 3.0 or later requires Tanium Core Platform 7.6.1 or later
- Tanium Discover 3.1 or later is required to target endpoints based on Discover tags

Client extensions

Tanium Endpoint Configuration installs client extensions for Client Management on endpoints. Client Extensions perform tasks that are common to certain Tanium solutions. The Tanium Client uses code signatures to verify the integrity of each client extension prior to loading the extension on the endpoint. Each client extension has required security exclusions to allow the Tanium processes to run without interference. See Security exclusions for more information. Client extensions can run in separate processes, or together in a single process, depending on whether *client extension shared process mode* is enabled. See Endpoint Configuration User Guide: Manage client extension shared process mode. The following client extensions perform Client Management functions:

- Client Deployment CX - Provides the satellite functionality for Tanium Client deployments in Client Management. Tanium Client Management installs this client extension only on satellite endpoints used for client deployments. Client Management distributes this client extension to a satellite endpoint the first time you start a client deployment that uses that satellite.
- Config CX - Provides installation and configuration of extensions on endpoints. Tanium Endpoint Configuration installs this client extension.
- Core CX - Provides a management framework API for all other client extensions and exposes operating system metrics. Tanium Endpoint Configuration installs this client extension.
- DEC CX - Provides a direct connection between endpoint and Module Server. Tanium Direct Connect installs this client extension. This is a feature-specific dependency for Client Management.
- Discover CX - Performs satellite-based Nmap scans. Tanium Discover installs this client extension. This is a feature-specific dependency for Client Management.
- Extras CX - Provides a helper library that contains re-usable functions for various client extensions to use. Tanium Asset, Tanium Discover, Tanium Integrity Monitor, Tanium Investigate, and Tanium Threat Response install this client extension. This is a feature-specific dependency for Client Management.
- Support CX - Provides the ability to gather troubleshooting content from endpoints through Tanium Client Management. Tanium Client Management installs this client extension.
- TSDB CX - Collects metrics about the Tanium Client and client extensions. Tanium Client Management installs this client extension.

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 Tanium Core Platform User Guide for Windows Deployments: Host system sizing guidelines.

Compatibility between Tanium Core Platform servers and Tanium Clients

Tanium Clients can connect only to Tanium Core Platform servers (Tanium Server, Tanium Module Server, and Tanium Zone Server) that run the same Tanium™ Protocol version as the clients or a later version than the clients. Servers at version 7.3 and clients at version 7.2 run Tanium Protocol 314. Servers and clients at version 7.4 or later run Tanium Protocol 315. Effectively, this means that

servers are backward-compatible with earlier clients; for example, servers at version 7.5 support Tanium Client 7.2 and 7.4, but Tanium Client 7.4.x cannot connect to servers at version 7.3.

NOTE

For details about the Tanium Protocol, see Tanium Appliance User Guide: Securing Tanium Server, Zone Server, and Tanium Client access or Tanium Core Platform User Guide for Windows Deployments: Securing Tanium Server, Zone Server, and Tanium Client access.

The release numbers for Tanium Core Platform servers and Tanium Clients have the format *<major release>.<minor release>.<point release>.<build>*, such as 7.5.6.1137. Clients can connect to the servers when their major and minor release numbers match regardless of whether the point release and build numbers match. For example, Tanium Client 7.4.5 can connect to Tanium Server 7.4.2.

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 105). These accounts and permissions are necessary only during deployment, and they can be removed or changed after you successfully deploy clients.

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 134.

- 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

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 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.

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 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 114.

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.

Default port requirements for Tanium Client

Source	Destination	Port	Protocol	Purpose
Tanium Client	Peer clients	17472	TCP	Used for communication between the Tanium Client and peer clients[1]
Peer clients	Tanium Client	17472	TCP	Used for communication between the Tanium Client and peer clients[1]
Tanium Client	Tanium Server	17472	TCP	Used for communication between the Tanium Client and the Tanium Server[3]
Tanium Client	Zone Server[2]	17472	TCP	Used for communication between the Tanium Client and the Zone Server[3]
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	Tanium Server	17486	TCP	Outbound communication from the Tanium Client and inbound communication to the Tanium Server for direct endpoint connections using Direct Connect[3]

[1] You can change the port that clients use for peer communication. See Customize listening ports on page 221.

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

[3] Tanium Core Platform servers can use custom ports for communication with Tanium Client. For more information, see Configuring connections to the Tanium Core Platform on page 188.

Table 2: 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]
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	TCP	Used by the Zone Server for Module Server connections. The default port number is `17487`. If needed, you can specify a different port number when you configure the Zone Proxy.
		17488	TCP	Allows communication between the Zone Server and the Module Server. On TanOS, the Direct Connect Zone Proxy installer automatically opens port `17488` on the Zone Server. This port must be manually opened on Windows.

[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 defaults to SMBv3 when it is 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.

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. See Tanium Appliance User Guide: Network connectivity and firewall or Tanium Core Platform User Guide for Windows Deployments: 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** setting. You can also change the port that clients use for peer communication by configuring the **ListenPort** or **EnableRandomListeningPort** setting. (See Customize listening ports on page 221.) 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 Tanium Appliance User Guide: Network connectivity and firewall or Tanium Core Platform User Guide for Windows Deployments: Ports and firewalls. For more information about client peering settings, see Configuring Tanium Client peering on page 202.

NOTE

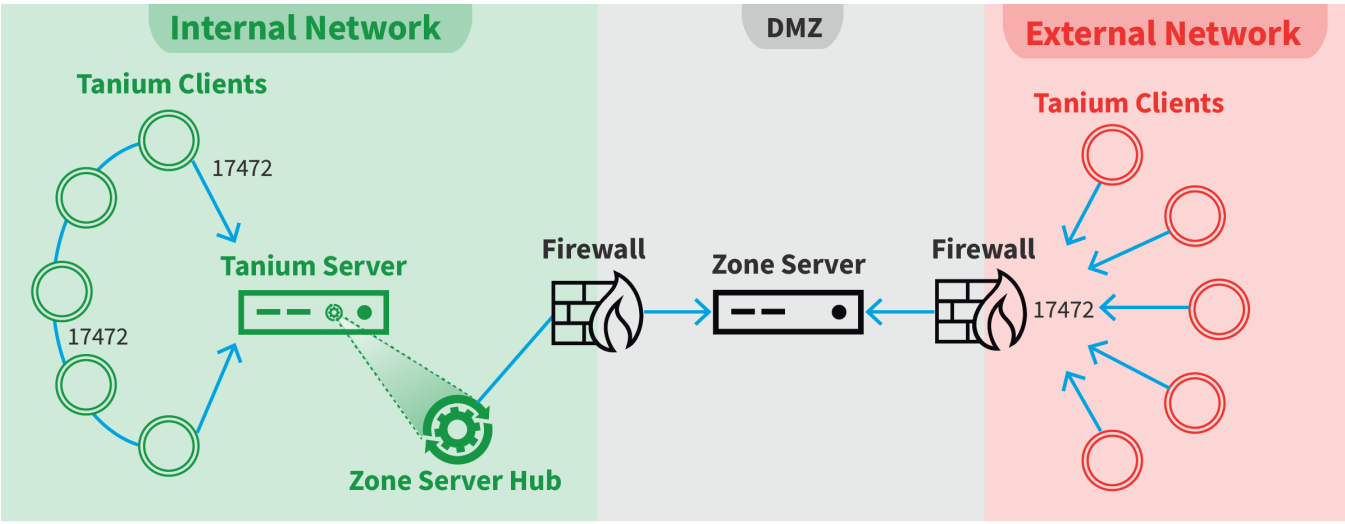
- **macOS:** The Tanium Client service is signed to automatically allow communication through the default macOS firewall. However, the client installation process does not modify any host-based firewall that is in use. For more information about managing macOS firewalls, see Manage macOS firewall rules on page 241.

  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. See Manage pop-ups for Tanium Client upgrades on page 241.
- **Linux:** For more information about managing Linux firewalls, see Manage Linux firewall rules on page 244.
- 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. See Compatibility between Tanium Core Platform servers and Tanium Clients on page 70.
- 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 222.
- 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 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 107 and Deploying the Tanium Client using Client Management on page 105.

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 Configure isolated subnets on page 208). 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 Protocol and is encrypted with TLS 1.2. You must disable any form of deep packet inspection or SSL/TLS decryption 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 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. The configuration of these exclusions varies depending on AV software. For a list of all security exclusions to define across Tanium, see Tanium Client Management Guide: Reference: Endpoint security exclusions and for Windows-based Tanium Core Platform deployments, Tanium Core Platform User Guide for Windows Deployments: Tanium Core Platform server security exclusions.

> **NOTE** If the required exclusions are not configured, or if Tanium suspects AV interference, Tanium might require you to remove the AV software temporarily for the purposes of troubleshooting and restore it once troubleshooting is complete.

Security exclusions for Tanium Client

Some antivirus (AV) software might require excluding the installation directories of the Tanium Client from real-time inspection. Typically, configuring trusted exclusions also involves setting a policy to ignore the input and output of Tanium binaries. The configuration of these exclusions varies based on the AV 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. See Network connectivity, ports, and firewalls on page 72.
- **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 details, see Solution-specific exclusions on page 318.

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

Target Device	Installation folder
Windows x86 endpoints	`C:\Program Files\Tanium\Tanium Client`
Windows x64 endpoints	`C:\Program Files (x86)\Tanium\Tanium Client`
macOS endpoints	`/Library/Tanium/TaniumClient`
Linux, Solaris, AIX endpoints	`/opt/Tanium/TaniumClient`

Tanium requires that security applications allow (not block, quarantine, or otherwise process) the following system processes. The <*Tanium Client*> variable indicates the Tanium Client installation directory, which is configurable during client installation.

Security exclusions for Tanium Client processes

Target Device	Notes	Process
Windows endpoints		<*Tanium Client*>\TaniumClient.exe
		<*Tanium Client*>\TaniumCX.exe
		<*Tanium Client*>\Tools\StdUtils\7za.exe
		<*Tanium Client*>\Tools\StdUtils\runasuser.exe
		<*Tanium Client*>\Tools\StdUtils\runasuser64.exe
		<*Tanium Client*>\Tools\StdUtils\TaniumExecWrapper.exe
		<*Tanium Client*>\Tools\StdUtils\TaniumFileInfo.exe
		<*Tanium Client*>\Tools\StdUtils\TPowerShell.exe
macOS, Linux, Solaris, AIX endpoints		<*Tanium Client*>/TaniumClient
		<*Tanium Client*>/taniumclient
		<*Tanium Client*>/TaniumCX
	macOS endpoints running the universal Tanium Client binary only	<*Tanium Client*>/TaniumCX.app/Contents/MacOS/TaniumCX
		<*Tanium Client*>/Tools/StdUtils/TaniumExecWrapper
		<*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, which is configurable during client installation.

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

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 installed	Process	`<Tanium Installation Directory>\Tanium Direct Connect Zone Proxy\twsm.exe`

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`

Client Management security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	During client installation; x64 endpoints	Process	`C:\Program Files (x86)\Tanium\SetupClient.exe`

Client Management security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	During client installation; x86 endpoints	Process	`C:\Program Files\Tanium\TaniumClientBootstrap.exe`

Client Management security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	During client installation; x86 endpoints	Process	`C:\Program Files\Tanium\SetupClient.exe`

Client Management security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	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 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
	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 satellite profiles only)	Folder	C:\Program Files\Npcap
	When Discover is installed; (Distributed level 3, distributed level 4, and satellite profiles only)	Process	<*Tanium Client*>\Tools\Discover\nmap\nmap.exe

Client Management security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
macOS	During client installation	Process	`/Library/Tanium/TaniumClientBootstrap`
	During client installation	Process	`/Library/Tanium/SetupClient`
	During client installation	Process	`<Tanium Client>/SetupClient`
		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`
	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`
	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`

Client Management security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
Linux	During client installation	Process	`/opt/Tanium/TaniumClientBootstrap`
	During client installation	Process	`/opt/Tanium/SetupClient`
	During client installation	Process	`<Tanium Client>/SetupClient`
		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 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 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`

Client Management security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
Solaris and AIX	During client installation	Process	`/opt/Tanium/TaniumClientBootstrap`
	During client installation	Process	`/opt/Tanium/SetupClient`
	During client installation	Process	`<Tanium Client>/SetupClient`

INTERNET URL REQUIRED FOR CLIENT MANAGEMENT

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

The following tables list the role permissions required to use Client Management. To review a summary of the predefined roles, see Set up Client Management users on page 97.

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.

For more information about role permissions and associated content sets, see Tanium Core Platform User Guide: Managing RBAC.

NOTE

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

Table 3: Client Management user role permissions

Permission	Client Management Administrator [1,2,3]	Client Management User[3]	Client Management Read-Only User[3]	Client Management Upgrade Operator	Client Management Endpoint Configuration Approver[2]
Client-Management API Access the Client Management API	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✗

Table 3: Client Management user role permissions (continued)

Permission	Client Management Administrator [1,2,3]	Client Management User[3]	Client Management Read-Only User[3]	Client Management Upgrade Operator	Client Management Endpoint Configuration Approver[2]
Client-Management Client Version Access and manage the versions of the Tanium Client used in deployments and upgrades	✓ READ WRITE	✓ READ	✓ READ	✗	✗
Client-Management Credential Access the credentials list (cannot view associated passwords or key data)	✓ READ WRITE	✓ READ	✓ READ	✗	✗
Client-Management Deployment Access data in client deployments	✓ READ WRITE EXECUTE	✓ READ	✓ READ	✗	✗
Client-Management Direct Connect to an endpoint using Direct Connect and read data from that endpoint	✓ CONNECT	✗	✗	✗	✗
Client-Management Discover API Access the Client Management Discover API	✓ EXECUTE	✗	✗	✗	✗
Client-Management Endpoint Configuration / Client Management Endpoint Configuration Approve Endpoint Configuration items for Client Management	✗	✗	✗	✗	✓ APPROVE

Table 3: Client Management user role permissions (continued)

Permission	Client Management Administrator [1,2,3]	Client Management User[3]	Client Management Read-Only User[3]	Client Management Upgrade Operator	Client Management Endpoint Configuration Approver[2]
Client-Management Index Configuration Manage client Index configurations	✓ READ WRITE DEPLOY	✓ READ	✓ READ	✗	✗
Client-Management Profile Support Bundle Access the Client Management support bundle	✓ READ	✗	✗	✗	✗
Client-Management Settings Configuration Manage client settings configurations	✓ READ WRITE DEPLOY	✓ READ	✓ READ	✗	✗
Client-Management Trends Supply data to Trends and view charts from Trends in Client Management	✓ READ WRITE	✓ READ	✓ READ	✗	✗
Client-Management Upgrade Manage and run client upgrades	✓ READ WRITE	✓ READ	✓ READ	✓ READ WRITE	✗
Client-Management View View client health charts	✓ HEALTH	✓ HEALTH	✓ HEALTH	✓ HEALTH	✗
Client-Management Download installation packages for the Tanium Client when using Client Management in Tanium Cloud	✓ DOWNLOAD	✗	✗	✗	✗

Table 3: Client Management user role permissions (continued)

Permission	Client Management Administrator [1,2,3]	Client Management User[3]	Client Management Read-Only User[3]	Client Management Upgrade Operator	Client Management Endpoint Configuration Approver[2]
Clientmanagement View the Client Management workbench	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW	✗

[1] This role provides module permissions for Tanium Direct Connect. You can view which Direct Connect permissions are granted to this role in Tanium Console. For more information, see Tanium Direct Connect User Guide: User role requirements.

[2] This role provides module permissions for Tanium Endpoint Configuration. You can view which Endpoint Configuration permissions are granted to this role in the Tanium™ Console. For more information, see Tanium Endpoint Configuration User Guide: User role requirements.

[3] This role provides module permissions for Tanium Trends. You can view which Trends permissions are granted to this role in Tanium Console. For more information, see Tanium Trends User Guide: User role requirements.

Table 4: Provided 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 Upgrade Operator	Client Management Endpoint Configuration Approver
Action Group	Administration	✓ READ	✓ READ	✓ READ	✓ READ	✗
Computer Group	Administration	✓ READ	✓ READ	✓ READ	✓ READ	✗
User Group	Administration	✓ READ	✓ READ	✓ READ	✓ READ	✗
Endpoint Configuration	Platform Content	✓ READ WRITE	✓ READ	✓ READ	✗	✓ APPROVE DISMISS REJECT SHOW READ

Table 4: Provided Client Management Administration and Platform content user role permissions (continued)

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

Table 4: Provided Client Management Administration and Platform content user role permissions (continued)

Permission	Role Type	Client Management Administrator	Client Management User	Client Management Read-Only User	Client Management Upgrade Operator	Client Management Endpoint Configuration Approver
Trends View Recent	Platform Content	✓ RESULTS	✓ RESULTS	✓ RESULTS	✗	✗

To view which content set permissions are granted to a role, see Tanium Console User Guide: View effective role permissions.

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 Tanium Console User Guide: Configure a custom role, and for information about assigning user roles, see Tanium Core Platform User Guide: Manage role assignments for a user.

For more information and descriptions of content sets and permissions, see Tanium Core Platform User Guide: Managing roles.

Installing Client Management

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

- **Automatic configuration with default settings** (Tanium Core Platform 7.4.2 or later only): 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 93.
- **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 94.

Before you begin

- Read the release notes.
- Review the Tanium Client and Client Management requirements on page 26.
- Assign the correct roles to users for Client Management. Review the User role requirements for Client Management on page 87.
    - 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

(Tanium Core Platform 7.4.5 or later only) You can set the Client Management action group to target the **No Computers** filter group by enabling restricted targeting before importing Client Management. This option enables you to control tools deployment through scheduled actions that are created during the import and that target the Tanium Client Management action group. For example, you might want to test tools on a subset of endpoints before deploying the tools to all endpoints. In this case, you can manually deploy the tools to an action group that you configured to target only the subset. To configure an action group, see Tanium Console User Guide: Managing action groups. To enable or disable restricted targeting, see Tanium Console User Guide: Dependencies, default settings, and tools deployment.

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`.

To import Client Management and configure default settings, see Tanium Console User Guide: Import all modules and services. After the import, verify that the correct version is installed. See Verify Client Management version on page 94.

Import Client Management with custom settings

To import Client Management without automatically configuring default settings, be sure to clear the **Apply All Tanium recommended configurations** check box while performing the steps in Tanium Console User Guide: Import, re-import, or update specific solutions. After the import, verify that the correct version is installed. See Verify Client Management version on page 94.

To configure the Client Management action group, see Configure the Client Management action group on page 96.

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. See Solution dependencies.

1. Install the dependencies as described in Tanium Console User Guide: Import, re-import, or update specific solutions.
2. From the Main menu, go to **Administration > Shared Services > Client Management** to open the Client Management **Overview** page and verify that 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 **Administration > Shared Services > Client Management**.
3. To display version information, click Info .

Upgrade Client Management

For the steps to upgrade Client Management, see Tanium Console User Guide: Import, re-import, or update specific solutions. After the upgrade, verify that the correct version is installed. See Verify Client Management version on page 94.

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 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 113.

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. See Migrating client deployments from Client Management versions earlier than 2.1 on page 95.
- **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. See Manage client deployments on page 113.

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

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 **Client Management** menu, go to **Client Deployments**.
2. Click the name of a deployment that as migrated from an earlier version, and then click **Clone**.
3. Enter a **Name** and optionally a **Description** for the deployment.
4. Adjust settings as needed, and run the new deployment or save the settings as a new template. See Deploy clients on page 114.

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.

For information about installing Endpoint Configuration, see Tanium Endpoint Configuration User Guide: 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 Client Management on page 87. For more information about enabling and using configuration approvals in Endpoint Configuration, see Tanium Endpoint Configuration User Guide: Managing approvals.

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 Tanium Console User Guide: Managing action locks.

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

Configure the Client Management action group

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 87.

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 Tanium Core Platform User Guide: Manage role assignments for a user.

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 configurations and client credentials

  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 configurations and client credentials

  NOTE

  No user can view passwords in existing credentials.

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

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 configurations, client credentials, and client deployments.

Client Management Operator

Assign the **Client Management Operator** role to users who investigate issues with specific clients.

This role can 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.

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:

TIP

- **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 Tanium Console User Guide: Configure a custom role, and for information about assigning user roles, see Tanium Core Platform User Guide: Manage role assignments for a user.

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

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 113.

1. From the Client Management **Overview** page, click Settings  .
2. 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.
3. 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 deployments and upgrades

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. You can manually cache other specific versions that you want to use in client deployments or upgrades.

NOTE

You cannot use Client Management to install a Tanium Client version earlier than 7.4.7.1094.

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

If you cannot enable communication between your Tanium Module Server and content.tanium.com, you must manually import Tanium Clients instead of caching versions from the online manifest.

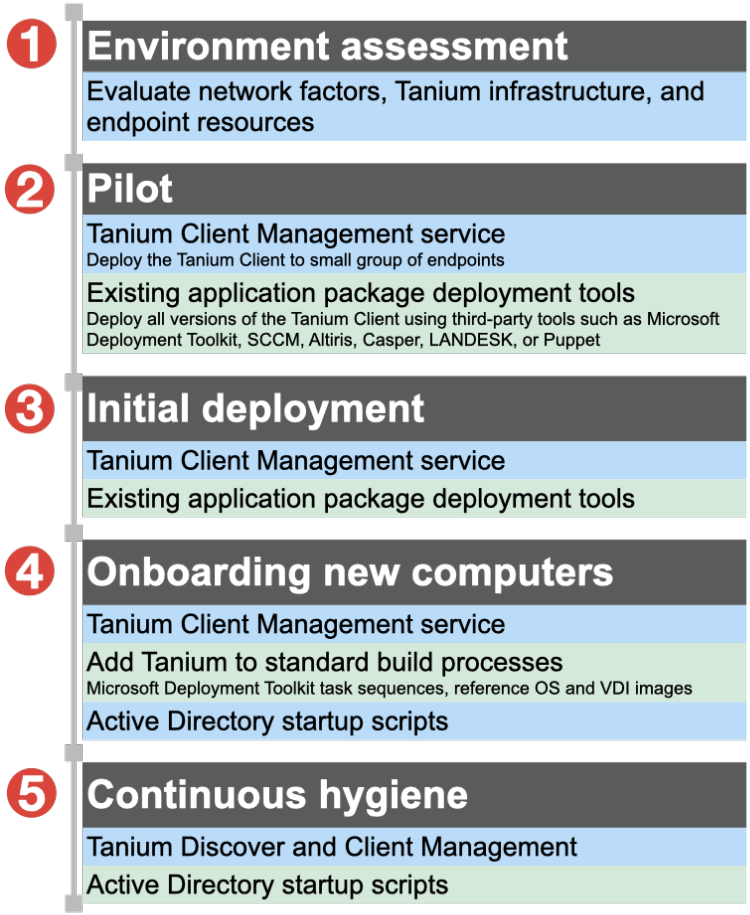
1. Contact Tanium Support to obtain a ZIP file with the installation packages.
2. From the Main menu, go to **Administration > Shared Services > Client Management**.
3. Click **Upload Tanium Client**, click **Select Client ZIP file**, select the file, and click **Upload**.

> 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.

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



The information on this page helps you carefully plan the deployment; review the following best practices for each phase. The subsequent topics in this section cover the methods and steps to deploy Tanium Client.

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 72.
- **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 Core Platform Deployment Guide for Windows and Tanium Appliance Deployment 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 194.

  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 20.

  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 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 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 310 and Preparing the Tanium Client on a virtual desktop infrastructure (VDI) instance on page 183.

  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. See Tanium Console User Guide: 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.

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.

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 188 and Configuring Tanium Client peering on page 202.

Determine deployment methods and pilot the deployment

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 details, see the Deploying the Tanium Client using Client Management on page 105.
- **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 details 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 134.
- **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 details 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 134.

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 Server. For more information about the requirements to deploy clients with Client Management, see Tanium Client and Client Management requirements on page 26.

This guide does not describe third-party tool-specific procedures for deploying the Tanium Client. For details on using a third-party tool with Tanium installers, refer to the documentation for that tool.

Deploy to an initial set of endpoints

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.

TIP

To monitor containers on endpoints, install and configure the Tanium™ Client Container on those endpoints after you deploy the Tanium Client. For more information see Tanium Containers User Guide.

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. See Preparing the Tanium Client on OS images on page 167. 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 onboarding macOS endpoints, you can use Tanium™ Mac Device Enrollment. Mac Device Enrollment supports macOS 11 or later. For more information, see Tanium Mac Device Enrollment User Guide.

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 for details.

Use Tanium™ Discover to scan for previously unmanaged or even unknown endpoints. For more 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 225.

For an overview of Tanium Client maintenance tasks, see Maintaining Tanium Clients on page 262.

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 Tanium Appliance User Guide: 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.

NOTE

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 225 and Access detailed client health and troubleshooting information on an endpoint on page 228.

NOTE

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 134.

TIP

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 167.

Plan deployment targeting

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

- A single IP adresses 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

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 Management.

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, 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 default client deployment template, create a deployment template, download the `tanium-init.dat` file, and deploy the client using an installer or package file. 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 Tanium Discover User Guide: Labels.

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. See Deploying the Tanium Client using Client Management on page 105.

(Optional) Prepare a satellite for use with automatic deployment

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 Tanium Appliance User Guide: Enable FIPS 140-3 mode.

An endpoint that you use as a satellite to deploy the Tanium Client must meet certain requirements. See Requirements for satellites used for Tanium Client deployment in Client Management on page 67.

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 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 134.
2. Create a satellite in Tanium Direct Connect. See Tanium Direct Connect User Guide: 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. 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:

- 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 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.

2. 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 73.
3. Configure any host-based firewalls or other security tools on endpoints that might interfere with a remote installation that is initiated through SSH. For more information, see Port requirements for Tanium Client and Client Management on page 73.
4. (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.
   - If you use Tanium™ Mac Device Enrollment, the necessary Privacy Preferences Policy Control (PPPC) permissions are automatically installed on endpoints during device enrollment. In that case, creating a custom PPPC payload with the permissions listed here is not necessary.

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 26.

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.

If you use Mac Device Configuration Profile policies in Tanium Enforce 2.3 or later, the PPPC payload is available in each policy. See Tanium Enforce User Guide: Create a Mac Device Configuration Profile policy.

The team identifier for Tanium applications is TZTPM3VTUU.

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 version 7.2.314.3608 or later.

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

5. (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
   ```

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

   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
   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`

7. (AIX only) If they are not yet installed, install the IBM XL C++ runtime libraries file set (`xlC.rte`) and, if indicated in the following table, the IBM LLVM runtime libraries file set (`libc++.rte`). The required `xlC.rte` version and the requirement for `libc++.rte` depend on the AIX version:

AIX version	Tanium Client version	`xlC.rte` version	`libc++.rte` required?
7.1.1–7.1.3	7.2	13.1.3.1 or later	When `xlC.rte` version 16.1.0.0 or later is installed, or when required by an installed module or shared service. See Solution-specific requirements for the Tanium Client and endpoints (continued) on page 67 for links to specific requirements.
7.1.4 or later	All supported versions	16.1.0.0 or later	Yes

   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, if required, the `libc++.rte` bundle:

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

      If the appropriate version of each bundle is already installed where required, skip to Deploying the Tanium Client using Client Management on page 105. 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.

8. If you use the root account to install, make sure the sshd_config allows root login.

9. 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. 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
   - 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)

     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 134.
   - 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)

   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.

2. 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.

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

3. 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. For more information, see Port requirements for Tanium Client and Client Management on page 73.
4. 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 73.
5. 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.

6. 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

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

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. See Deploy clients on page 114.

1. From the Client Management menu, click **Client Installations > Client Deployment Templates**, and then click **Create Client Deployment Template**.
2. Enter a **Name** and optionally a **Description** for the template.

3. Configure client deployment settings as detailed in General client deployment settings on page 122.
4. Click **Save**.

(Optional) Designate a template as the default

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

1. From the Client Management menu, click **Client Installations > Client Deployment Templates**.
2. 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 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

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. If you are using Tanium Server 7.5 or later, 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 7.4.7 or later 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 Client Management menu, click **Client Installations > Client Deployment Templates**.
2. Click the name of a client deployment template.
3. On the **Show Client Deployment Template** page, click Download tanium-init.dat.
4. Deploy Tanium Client using the appropriate installer or package file and the `tanium-init.dat` file you downloaded. See Deploying the Tanium Client using an installer or package file on page 134.

Deploy clients

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 Client Management menu, click **Client Installations > Client Deployments**, and then click **Create Client Deployment**.

   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.

2. (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, the settings from that template are already applied.

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

4. Configure the client deployment settings.

- Configure the **Deployment Details**:

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 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.

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 Tanium Discover User Guide: 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.

Section	Setting	Description
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**. TIP For specific requirements for authentication and permissions, see Account permissions for Client Management on page 71.

Section	Setting	Description
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 106. 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 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 Tanium Appliance User Guide: Enable FIPS 140-3 mode.

- Complete the **Deployment Configuration** as detailed in General client deployment settings on page 122. If you started from a template, edit these settings only as necessary.

5. (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**.
6. Review the **Deployment Summary**. To deploy the client to the targeted endpoints, click **Deploy**.

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. (See Verify the Tanium Client installation on page 187.)

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. TIP To manage the client versions that are available for this setting, see Manage versions of the Tanium Client available for deployments and upgrades on page 99. NOTE You cannot use Client Management to install a Tanium Client version earlier than 7.4.7.1094.
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**. TIP To view the installation log, see View the deployment status and endpoint installation logs on page 131.

Section	Setting	Description
Installation options	Installation Directory on Windows	(Optional) Enter a custom installation directory for Windows endpoints. Leave blank to use the default installation directory. IMPORTANT • The installation directory must be located on a local fixed drive on each endpoint. • 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 134.

Section	Setting	Description
	Installation Directory on non-Windows	(Optional) Enter a custom installation directory for non-Windows endpoints. Leave blank to use the default installation directory. 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`.

Section	Setting	Description
	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 63.

Section	Setting	Description
	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 63.
	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. BEST PRACTICE For general management of upgrades to existing clients, create upgrade deployments that target computer groups. See Upgrade Tanium Clients using Client Management on page 270. • **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**.

Section	Setting	Description
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. 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. You can configure the default value for this setting. See Configure the default server names and server port for Tanium Client deployments on page 99.

Section	Setting	Description
	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. See Configure the default server names and server port for Tanium Client deployments on page 99.

Section	Setting	Description
	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. For more information about using a proxy server, see Connect through an HTTPS forward proxy server on page 194.

Section	Setting	Description
	Log Level	(Optional) Enter a log level for the Tanium Client on targeted endpoints. The following values are best practices for specific use cases: • `0`: Use this value to disable logging; use for clients installed on sensitive endpoints or virtual desktop infrastructure (VDI) endpoints. • `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 This value does not affect the verbosity of the client installation log during deployment. For troubleshooting client installations, enable the Verbose Logging on page 122 setting.
	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 298. 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 310.
	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.
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

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 Client Management menu, click **Client Installations > Client Deployments**, and then click the name of the deployment you want to view.

   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.

2. 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.
3. (Optional) To view the installation log for an endpoint, click Endpoint Details  in the row for the endpoint.

To help troubleshoot installation issues, you can increase the verbosity of the installation log. Enable the Verbose Logging setting, and then reissue the deployment.

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. (See Verify the Tanium Client installation on page 187.)

Reissue a deployment

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.

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. See Cloning Client deployments migrated from versions earlier than 2.1 on page 95.

1. From the Client Management menu, click **Client Installations > Client Deployments**, and then click the name of the deployment you want to reissue.
2. 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 .

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. See Deploy clients on page 114 and General client deployment settings on page 122.
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 71.

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.

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.

BEST PRACTICE

Use Client Management to create a client deployment template and then download the `tanium-init.dat` file for use in alternative deployment. If you are using Tanium Server 7.5 or later, 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 113 and (Optional) Download a tanium-init.dat file for alternative deployment on page 114.

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 105.

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 310.

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 167.

Deploy the Tanium Client to Windows endpoints using the installer

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

If you encounter issues when deploying the Tanium Client, examine the Tanium Client installation log.

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 for the client application files and related content files.
- Creates the Tanium Client Windows registry 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**.

For information about managing the Tanium Client service or uninstalling the Tanium Client after deployment, see Manage the Tanium Client on Windows on page 237.

Prepare for installation

1. Ensure that the Windows endpoint meets the basic requirements for the Tanium Client.
2. Sign in to the Windows endpoint with a local user or domain account that has administrative permissions.
3. Use the Tanium Client Management service to download the client installer bundle to the Windows endpoint. For the procedure, see (Optional) Download a tanium-init.dat file for alternative deployment on page 114.
   The bundle contains includes the following files for Windows installations:
   - `SetupClient.exe`
   - `tanium-init.dat` (Tanium Client 7.4 or later)
   - `tanium.pub` (Tanium Client 7.2)

You can also download `tanium-init.dat` or `tanium.pub` through Tanium Console (see Tanium Console User Guide: Download infrastructure configuration files (keys)) and request `SetupClient.exe`

from Tanium Support (see Contact Tanium Support on page 297). However, the installation process for Tanium Client 7.4 or later requires fewer manual configuration steps if you download `tanium-init.dat` through Client Management.

Be careful not to allow the `tanium-init.dat` or `tanium.pub` 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 these files do not contain private keys and cannot be used to provide control over a Tanium environment, a user with malicious intent could use them to connect an unapproved client and use this unauthorized access to learn how your organization is using Tanium.

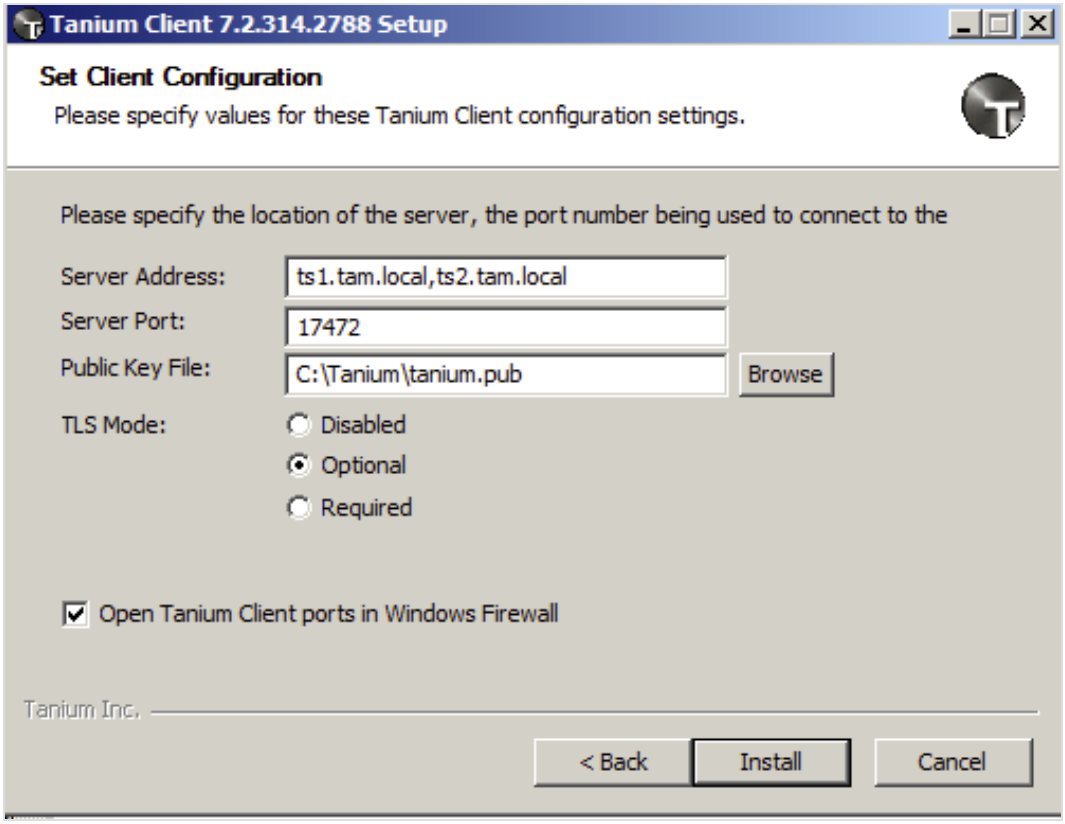
4. Copy the installer bundle to a temporary directory on the Windows endpoint and unzip the bundle.

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 client version and the source of the installation files:
   - **Tanium Client 7.4 or later**: 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. The installer uses default values, or if you are using Tanium Server 7.5 or later and installing Tanium Client 7.4.7 or later, the settings configured in the installation bundle. Otherwise, you must manually specify the **Initialization File** (`tanium-init.dat`) and other settings.

     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.

- **Tanium Client 7.2**: Specify the **Public Key File** (`tanium.pub`), **TLS Mode**, and other settings.



4. (Optional) Use the CLI on Windows endpoints to configure additional Tanium Client settings 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 254.
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. (See Verify the Tanium Client installation on page 187.)

Install the Tanium Client on Windows using the command line

You can use the endpoint command-line interfrace (CLI) to install the Tanium Client. For details on using the CLI, see CLI on Windows endpoints on page 313.

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.

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>]
   ```

   Tanium Client command-line installation syntax (continued) on page 142 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 (Tanium Server 7.5 or later with Tanium Client 7.4.7 or later) or otherwise the default values, except for ServerNameListand requires only the following arguments:
     - `/ServerAddress` sets the **ServerNameList** and is required for Tanium Client 7.2. It is required for Tanum Client 7.4 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 (Tanium Client 7.4 or later) or `tanium.pub` file (Tanium Client 7.2) 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 Tanium Client command-line installation syntax (continued) on page 142 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 opens and prompts you to configure the settings.

   Tanium Client command-line installation examples (continued) on page 144 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 Tanium Client command-line installation syntax (continued) on page 142 describes, see Modify client settings on page 254.

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. (See Verify the Tanium Client installation on page 187.)

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. Using internally defined FQDNs or aliases is strongly recommended. Use a comma to separate the entry for each server. If you specify one value for this option, it populates the ServerName registry entry. If you specify multiple values, they populate the **ServerNameList** registry entry. For Tanium Client 7.4 or later, omit `/ServerAddress` during the initial installation if the `tanium-init.dat` file specifies the **ServerNameList** (see the client installation types). If `tanium-init.dat` does not specify the **ServerNameList**, or you are installing Tanium Client 7.2, you must include `/ServerAddress` during installation. You can omit this argument when reinstalling or upgrading any version of the client. TIP: You can optionally set the port that the Tanium Client uses to communicate with the Tanium Server by appending `:<port_number>` to the server address (for example, `ts1.local.com:12345`). The `/ServerAddress` port overrides the `/ServerPort` value.
/ServerPort	The port that the Tanium Client uses for communication with the Tanium Server and with peers. When using Tanium Server 7.5 or later and installing Tanium Client 7.4.7 or later, you can omit this argument if the `tanium-init.dat` file came from a Client Management client configuration. 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 details, see ServerPort.

Tanium Client command-line installation syntax (continued)

Argument	Guidance
/LogVerbosityLevel	The level of logging on the endpoint. When using Tanium Server 7.5 or later and installing Tanium Client 7.4.7 or later, you can omit this argument if the `tanium-init.dat` file came from a Client Management client configuration. 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 use cases: • `0`: Use this value to disable logging; use for clients installed on sensitive endpoints or virtual desktop infrastructure (VDI) endpoints. • `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.
/KeyPath	The full path and file name that the Tanium Client installer program uses to locate the `tanium-init.dat` file (Tanium Client 7.4 or later) or `tanium.pub` file (Tanium Client 7.2) and copy it to the Tanium Client installation directory. 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 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` or `tanium.pub` 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` (Tanium Client 7.4 or later) or `tanium.pub` (Tanium Client 7.2) must be in the same directory as `SetupClient.exe`. For examples of how to run silent installations, see Tanium Client command-line installation examples (continued) on page 144. NOTE Make sure to use a capital letter for this argument.

Tanium Client command-line installation syntax (continued)

Argument	Guidance
/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 install the Tanium Client on a local fixed drive. 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 Tanium Client command-line installation examples (continued) on page 144. 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.
/ReportingTLSMode	This setting applies only to Tanium Client 7.2. The possible values are: • `0` (TLS not used) • `1` (TLS required) • `2` (TLS optional) BEST PRACTICE If you plan to use TLS, initially set this option to 2 (optional). When TLS is optional, the Tanium Client tries to connect over TLS. If the TLS connection fails, the client tries a non-TLS connection.

Tanium Client command-line installation syntax (continued)

Argument	Guidance
/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 details, see Configure proxy connections with a PAC file on page 197.
/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 details, see Configure proxy connections without a PAC file on page 199.

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

If you are installing Tanium Client 7.4 or later, omit the `/ServerAddress` argument if the `tanium-init.dat` file came from a Client Management installation bundle. For details, see the client installation types.

If you are using Tanium Server 7.5 or later and installing Tanium Client 7.4.7 or later, also omit the `/ServerPort` and `/LogVerbosityLevel` arguments if the `tanium-init.dat` file came from a Client Management installation bundle.

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` or public key file `tanium.pub` 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`

Tanium Client command-line installation examples (continued)

Example	Description

Silent installation TLS option	The following example specifies non-default values for a silent installation of Tanium Client 7.2:
	`SetupClient.exe /ServerAddress=ts1.example.com /ServerPort=63422 ^`
	`/LogVerbosityLevel=0 /ReportingTLSMode=1 /S`

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.

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

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.

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 241.

Prepare for installation

1. Ensure that the macOS endpoint meets the basic requirements for the Tanium Client.
2. 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). See Manage macOS firewall rules on page 241.
3. (macOS 10.14 or later only) Create a mobile device management (MDM) profile that provides the necessary permissions for the following Tanium applications.

- This step is critical for full support of Tanium Client functionality on macOS 10.14 or later.
- If you use Tanium™ Mac Device Enrollment, the necessary Privacy Preferences Policy Control (PPPC) permissions are automatically installed on endpoints during device enrollment. In that case, creating a custom PPPC payload with the permissions listed here is not necessary.

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

Application	Location	Required Permissions	Apple Events
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 26.

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.

If you use Mac Device Configuration Profile policies in Tanium Enforce 2.3 or later, the PPPC payload is available in each policy. See Tanium Enforce User Guide: Create a Mac Device Configuration Profile policy.

The team identifier for Tanium applications is TZTPM3VTUU.

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 version 7.2.314.3608 or later.

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

4. Sign in to the macOS endpoint.
5. Use the Tanium Client Management service to download the client installer bundle to the macOS endpoint. For the procedure, see (Optional) Download a tanium-init.dat file for alternative deployment on page 114.
   The bundle includes the following files for macOS installations:

- `TaniumClient-<version>-universal.pkg`
- `TaniumClient-<version>-x64.pkg`
- `tanium-init.dat` (Tanium Client 7.4 or later)
- `tanium.pub` (Tanium Client 7.2)

BEST PRACTICE

You can also download `tanium-init.dat` or `tanium.pub` through Tanium Console (see Tanium Console User Guide: Download infrastructure configuration files (keys)) and request `TaniumClient-<version>.pkg` from Tanium Support (see Contact Tanium Support on page 297). However, the installation process for Tanium Client 7.4 or later requires fewer manual configuration steps if you download `tanium-init.dat` through Client Management.

IMPORTANT

Be careful not to allow the `tanium-init.dat` or `tanium.pub` 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 these files do not contain private keys and cannot be used to provide control over a Tanium environment, a user with malicious intent could use them to connect an unapproved client and use this unauthorized access to learn how your organization is using Tanium.

6. Copy the installer bundle to a temporary directory on the macOS endpoint and unzip the bundle.

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.

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 or for Tanium Client 7.2 installations) Use the CLI (see CLI on non-Windows endpoints on page 314) to configure the following basic Tanium Client settings.

ServerName 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. **IMPORTANT** If the `tanium-init.dat` file for Tanium Client 7.4 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 7.4.5 or later is already installed to view the `ServerNameList` that the `tanium-init.dat` file specifies. For Tanium Client 7.2, you must specify `ServerName` or `ServerNameList`.
LogVerbosityLevel	The level of logging on the endpoint. The following values are best practices for specific use cases: • `0`: Use this value to disable logging; use for clients installed on sensitive endpoints or virtual desktop infrastructure (VDI) endpoints. • `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 For information about configuring additional settings, see Modify client settings on page 254 and Tanium Client settings reference on page 298.

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. (Tanium Client 7.4 or later) 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. (See Verify the Tanium Client installation on page 187.)

Install the Tanium Client on macOS using the command line

To install the Tanium Client, you must have root or sudo permissions to run the **installer** command. For details on using the CLI, see CLI on non-Windows endpoints on page 314.

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
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 or for Tanium Client 7.2 installations) Use the CLI (see CLI on non-Windows endpoints on page 314) to configure the following basic Tanium Client settings.

ServerName 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. **IMPORTANT** If the `tanium-init.dat` file for Tanium Client 7.4 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 7.4.5 or later is already installed to view the `ServerNameList` that the `tanium-init.dat` file specifies. For Tanium Client 7.2, you must specify `ServerName` or `ServerNameList`.

LogVerbosityLevel	The level of logging on the endpoint. The following values are best practices for specific use cases: • `0`: Use this value to disable logging; use for clients installed on sensitive endpoints or virtual desktop infrastructure (VDI) endpoints. • `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.

For information about configuring additional settings, see Modify client settings on page 254 and Tanium Client settings reference on page 298.

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. (Tanium Client 7.4 or later) 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. (See Verify the Tanium Client installation on page 187.)

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`.

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 the Tanium Client after deployment, see Manage the Tanium Client on Linux on page 244.

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 for other means to obtain the package file for your Linux distribution.

- 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 OS versions for Tanium Client hosts (continued) on page 61.

Table 5: 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 12.x	`taniumclient-<client_version>-debian12_amd64.deb` `taniumclient-<client_version>-debian12_arm64.deb`
Debian 11.x	`taniumclient-<client_version>-debian11_amd64.deb`

Table 5: Tanium Client package files for Linux (continued)

Linux Distribution	Latest Installation Package Files
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 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 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 15.x	TaniumClient-<*client_version*>-1.sle15.i586.rpm TaniumClient-<*client_version*>-1.sle15.x86_64.rpm
SUSE Linux Enterprise Server (SLES) / OpenSUSE 12.x	TaniumClient-<*client_version*>-1.sle12.i586.rpm TaniumClient-<*client_version*>-1.sle12.x86_64.rpm

Table 5: Tanium Client package files for Linux (continued)

Linux Distribution	Latest Installation Package Files
SUSE Linux Enterprise Server (SLES) / OpenSUSE 11.x	`TaniumClient-<client_version>-1.sle11.i586.rpm` `TaniumClient-<client_version>-1.sle11.x86_64.rpm`
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

Use the endpoint CLI to install the Tanium Client. For details on using the CLI, see CLI on non-Windows endpoints on page 314.

1. Ensure that the Linux endpoint meets the basic requirements for the Tanium Client.
2. Ensure that host and network firewalls are configured to allow inbound and outbound TCP traffic on the ports that the Tanium Client uses. See Manage Linux firewall rules on page 244.
3. 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**.
4. Use the Tanium Client Management service to download the client installer bundle to the Linux endpoint. For the procedure, see (Optional) Download a tanium-init.dat file for alternative deployment on page 114.
   The bundle contains the following files:
   - Installer package files for each Linux distribution (such as `TaniumClient-7.4.4.1250-1.oel8.x86_64.rpm`)
   - `tanium-init.dat` (Tanium Client 7.4 or later)
   - `tanium.pub` (Tanium Client 7.2)

   BEST PRACTICE

   You can also download `tanium-init.dat` or `tanium.pub` through Tanium Console (see Tanium Console User Guide: Download infrastructure configuration files (keys)) and request the installer package from Tanium Support (see Contact Tanium Support on page 297). However, the installation process for Tanium Client 7.4 or later requires fewer manual configuration steps if you download `tanium-init.dat` through Client Management.

Be careful not to allow the `tanium-init.dat` or `tanium.pub` 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 these files do not contain private keys and cannot be used to provide control over a Tanium environment, a user with malicious intent could use them to connect an unapproved client and use this unauthorized access to learn how your organization is using Tanium.

5. Copy the installer bundle to a temporary directory on the Linux endpoint and unzip the bundle:

```
unzip linux-client-bundle.zip
```

6. (Optional) To use a directory other than the default 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
```

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

7. 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-7.4.4.1362-1.oel6.x86_64.rpm
```

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

```
sudo dpkg -i taniumclient_7.4.4.1362-debian6_amd64.deb
```

8. Copy `tanium-init.dat`(Tanium Client 7.4 or later) or `tanium.pub` (Tanium Client 7.2) to the installation directory. For example:

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

9. (For `tanium-init.dat` files that do not include client settings or for Tanium Client 7.2 installations) Use the CLI (see CLI on non-Windows endpoints on page 314) to configure the following basic Tanium Client settings.

ServerName 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. **IMPORTANT** If the `tanium-init.dat` file for Tanium Client 7.4 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 7.4.5 or later is already installed to view the `ServerNameList` that the `tanium-init.dat` file specifies. For Tanium Client 7.2, you must specify `ServerName` or `ServerNameList`.
LogVerbosityLevel	The level of logging on the endpoint. The following values are best practices for specific use cases: • `0`: Use this value to disable logging; use for clients installed on sensitive endpoints or virtual desktop infrastructure (VDI) endpoints. • `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 For information about configuring additional settings, see Modify client settings on page 254 and Tanium Client settings reference on page 298.

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
```

10. Start the Tanium Client service. (See Manage the Tanium Client service on Linux on page 247.)

11. 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. (See Verify the Tanium Client installation on page 187.)

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.

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 details on using the CLI, see CLI on non-Windows endpoints on page 314.

For information about managing the Tanium Client service or uninstalling the Tanium Client after deployment, see Manage the Tanium Client on Solaris on page 250.

Prepare for installation

1. Ensure that the Solaris endpoint meets the basic requirements for the Tanium Client.
2. Work with your network security team to 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). See Network connectivity, ports, and firewalls on page 72.
   The installation process does not modify any host-based firewall that might be in use.
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
   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`

Install the Tanium Client on Solaris using the command line

1. Sign in to the Solaris endpoint.
2. Copy the installer file `TaniumClient-<client_version>-SunOS-5.10-<platform>.pkg` to a temporary location on the Solaris endpoint.
3. Use the Tanium Client Management service to download the client installer bundle to the Solaris endpoint. For the procedure, see (Optional) Download a tanium-init.dat file for alternative deployment on page 114.

   The bundle contains the following files:

   - `TaniumClient-<version>-SunOS-5.10.i386.pkg.tar.gz`
   - `TaniumClient-<version>-SunOS-5.10.sparc.pkg.tar.gz`
   - `tanium-init.dat` (Tanium Client 7.4 or later)

- `tanium.pub` (Tanium Client 7.2)

You can also download `tanium-init.dat` or `tanium.pub` through Tanium Console (see Tanium Console User Guide: Download infrastructure configuration files (keys)) and request the installer package from Tanium Support (see Contact Tanium Support on page 297). However, the installation process for Tanium Client 7.4 or later requires fewer manual configuration steps if you download `tanium-init.dat` through Client Management.

Be careful not to allow the `tanium-init.dat` or `tanium.pub` 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 these files do not contain private keys and cannot be used to provide control over a Tanium environment, a user with malicious intent could use them to connect an unapproved client and use this unauthorized access to learn how your organization is using Tanium.

4. Copy the installer bundle to the same temporary directory as the installer file and unzip the bundle.
5. (Optional) To use a directory other than the default 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
```

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

6. 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.

7. (For `tanium-init.dat` files that do not include client settings or for Tanium Client 7.2 installations) Use the CLI (see CLI on non-Windows endpoints on page 314) 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` (for Tanium Server 7.5 or later and Tanium Client 7.4.7 or later) or manually set `Resolver=nslookup` using the CLI.

ServerName 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. IMPORTANT If the `tanium-init.dat` file for Tanium Client 7.4 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 7.4.5 or later is already installed to view the `ServerNameList` that the `tanium-init.dat` file specifies. For Tanium Client 7.2, you must specify `ServerName` or `ServerNameList`.
LogVerbosityLevel	The level of logging on the endpoint. The following values are best practices for specific use cases: • `0`: Use this value to disable logging; use for clients installed on sensitive endpoints or virtual desktop infrastructure (VDI) endpoints. • `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.
Resolver	Add the `Resolver=nslookup` setting to enable host name resolution.

NOTE

For information about configuring additional settings, see Modify client settings on page 254 and Tanium Client settings reference on page 298.

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
```

8. Copy the `tanium-init.dat` file or `tanium.pub` file from the Tanium Server to the Tanium Client installation directory on the Solaris endpoint.
9. Run the following command to start the Tanium Client service:

   ```
   svcadm enable taniumclient
   ```

10. 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. (See Verify the Tanium Client installation on page 187.)

Perform unattended Tanium Client installation

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
   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

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`.

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 details on using the CLI, see CLI on non-Windows endpoints on page 314.

For information about managing the Tanium Client service or uninstalling the Tanium Client after deployment, see Manage the Tanium Client on AIX on page 252.

Prepare for installation

1. Ensure that the AIX endpoint meets the basic requirements for the Tanium Client.
2. Work with your network security team to 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). See Network connectivity, ports, and firewalls on page 72.

   The installation process does not modify any host-based firewall that might be in use.
3. If they are not yet installed, install the IBM XL C++ runtime libraries file set (`xlC.rte`) and, if indicated in the following table, the IBM LLVM runtime libraries file set (`libc++.rte`). The required `xlC.rte` version and the requirement for `libc++.rte` depend on the AIX version:

AIX version	Tanium Client version	`xlC.rte` version	`libc++.rte` required?
7.1.1–7.1.3	7.2	13.1.3.1 or later	When `xlC.rte` version 16.1.0.0 or later is installed, or when required by an installed module or shared service. See Solution-specific requirements for the Tanium Client and endpoints (continued) on page 67 for links to specific requirements.
7.1.4 or later	All supported versions	16.1.0.0 or later	Yes

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, if required, the `libc++.rte` bundle:

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

If the appropriate version of each bundle is already installed where required, skip to Install the Tanium Client on AIX using the command line on page 163. 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.

Install the Tanium Client on AIX using the command line

1. Sign in to the target endpoint.
2. Copy the Tanium Client installer file `TaniumClient-<client_version>-powerpc.pkg` to a temporary location on the target endpoint.
3. Use the Tanium Client Management service to download the client installer bundle to the AIX endpoint. For the procedure, see (Optional) Download a tanium-init.dat file for alternative deployment on page 114.
   The bundle contains the following files:
   - `TaniumClient-<version>-powerpc.pkg`
   - `tanium-init.dat` (Tanium Client 7.4 or later)
   - `tanium.pub` (Tanium Client 7.2)

You can also download `tanium-init.dat` or `tanium.pub` through Tanium Console (see Tanium Console User Guide: Download infrastructure configuration files (keys)) and request the installer package from Tanium Support (see Contact Tanium Support on page 297). However, the installation process for Tanium Client 7.4 or later requires fewer manual configuration steps if you download `tanium-init.dat` through Client Management.

IMPORTANT

Be careful not to allow the `tanium-init.dat` or `tanium.pub` 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 these files do not contain private keys and cannot be used to provide control over a Tanium environment, a user with malicious intent could use them to connect an unapproved client and use this unauthorized access to learn how your organization is using Tanium.

4. Copy the installer bundle to a temporary directory and unzip the bundle:

```
unzip aix-client-bundle.zip
```

NOTE

You must first install the unzip utility if it is not already installed on the AIX endpoint.

5. (Optional) To use a directory other than the default 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.

6. 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
```

7. (For `tanium-init.dat` files that do not include client settings or for Tanium Client 7.2 installations) Use the CLI (see CLI on non-Windows endpoints on page 314) 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` (for Tanium Server 7.5 or later and Tanium Client 7.4.7 or later) or manually set `Resolver=nslookup` using the CLI.

ServerName 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. **IMPORTANT** If the `tanium-init.dat` file for Tanium Client 7.4 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 7.4.5 or later is already installed to view the `ServerNameList` that the `tanium-init.dat` file specifies. For Tanium Client 7.2, you must specify `ServerName` or `ServerNameList`.
LogVerbosityLevel	The level of logging on the endpoint. The following values are best practices for specific use cases: • `0`: Use this value to disable logging; use for clients installed on sensitive endpoints or virtual desktop infrastructure (VDI) endpoints. • `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.
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 254 and Tanium Client settings reference on page 298.

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
```

8. Copy the `tanium-init.dat` file or `tanium.pub` file to the Tanium Client installation directory on the AIX endpoint.
9. Use the following command to start the Tanium Client service:

```
startsrc -s taniumclient
```

10. 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. (See Verify the Tanium Client installation on page 187.)

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 following sections describe best practices for preparing the Tanium Client on OS images.

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.

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

Refer to Microsoft documentation for complete details on Windows OS imaging.

Prepare the Tanium Client on a reference computer:

1. Install the Tanium Client. See the endpoint requirements and Deploy the Tanium Client to Windows endpoints using the installer on page 135. During the installation, make sure you do the following:
    - Configure the appropriate server settings. See Configuring connections to the Tanium Core Platform on page 188.
    - 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. See CLI on Windows endpoints on page 313 and Tanium Client settings reference on page 298.
5. Perform the following deletions in the Tanium Client installation directory.
    - Delete the following directories, including subdirectories and files:
        - `Downloads`
        - `Logs`
        - `Backup`
    - (Tanium Client 7.4 or later) Delete `pki.db`.
    - (Optional) For an image that you plan to use for a long period of time without updates, also delete the following directories and files:
        - **Directories:**
            - `Extensions`
            - `Tools`

- **Files:**
  - `TaniumClientExtensions.dll`
  - `TaniumClientExtensions.dll.sig`

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

Do not delete the `Tools` directory without also deleting the `Extensions` directory and the listed files.

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.

6. Obtain the latest `tanium-init.dat` file (version 7.4 or later) or `tanium.pub` file (version 7.2) and add it to the client.
   a. From the Main menu in Tanium Console, go to **Administration > Configuration > Tanium Server > Infrastructure Configuration Files**.
   b. Click **Download** in the **Clients v7.4+ and Zone Server** or **Clients v7.2** section, depending on which file you need.
   c. Copy the downloaded file into the Tanium Client installation directory.

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).

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 Tanium Client 7.4 or later. For more information about managing client configurations in Client Management, see Deploying the Tanium Client using Client Management on page 105. 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 114.

Be careful not to allow the `tanium-init.dat` or `tanium.pub` 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.

IMPORTANT

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

7. 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.

Preparing the Tanium Client on a macOS image

Refer to Apple documentation for complete details on macOS imaging.

Prepare the Tanium Client on a reference computer:

Prepare the Tanium Client on a reference computer:

1. Install the Tanium Client. See the endpoint requirements and Deploy the Tanium Client to macOS endpoints using the installer on page 145. During the installation, make sure you do the following:
   - Configure the appropriate server settings. See Configuring connections to the Tanium Core Platform on page 188.
   - 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. See CLI on non-Windows endpoints on page 314 and Tanium Client settings reference on page 298.
5. Perform the following deletions in the Tanium Client installation directory.
   - Delete the following directories, including subdirectories and files:
     - `Downloads`
     - `Logs`
     - `Backup`
   - (Tanium Client 7.4 or later) Delete `pki.db`.
   - (Optional) For an image that you plan to use for a long period of time without updates, also delete the following directories and files:
     - **Directories:**
       - `Extensions`
       - `Tools`

- **Files:**
  - `libTaniumClientExtensions.dylib`
  - `libTaniumClientExtensions.dylib.sig`

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

Do not delete the `Tools` directory without also deleting the `Extensions` directory and the listed files.

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.

6. Obtain the latest `tanium-init.dat` file (version 7.4 or later) or `tanium.pub` file (version 7.2) and add it to the client.
   a. From the Main menu in Tanium Console, go to **Administration > Configuration > Tanium Server > Infrastructure Configuration Files**.
   b. Click **Download** in the **Clients v7.4+ and Zone Server** or **Clients v7.2** section, depending on which file you need.
   c. Copy the downloaded file into the Tanium Client installation directory.

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).

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 Tanium Client 7.4 or later. For more information about managing client configurations in Client Management, see Deploying the Tanium Client using Client Management on page 105. 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 114.

Be careful not to allow the `tanium-init.dat` or `tanium.pub` 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.

IMPORTANT

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

7. 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.

Preparing the Tanium Client on a Linux OS image

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. See the endpoint requirements and Deploy the Tanium Client to Linux endpoints using package files on page 151. Be sure to use the Tanium Client installation package file for your particular Linux distribution, as listed under Deploying the Tanium Client using an installer or package file on page 134. During the installation, make sure you do the following:
    - Configure the appropriate server settings. See Configuring connections to the Tanium Core Platform on page 188.
    - Leave the **LogVerbosityLevel** setting at the default of `1`.
2. Stop the Tanium Client service daemon by entering the service command for your Linux distribution. See Manage the Tanium Client service on Linux on page 247.
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. See CLI on non-Windows endpoints on page 314 and Tanium Client settings reference on page 298.
6. Perform the following deletions in the Tanium Client installation directory.
    - Delete the following directories, including subdirectories and files:
        - `Downloads`
        - `Logs`
        - `Backup`
    - (Tanium Client 7.4 or later) Delete `pki.db`.

- (Optional) For an image that you plan to use for a long period of time without updates, also delete the following directories and files:
  - **Directories:**
    - `Extensions`
    - `Tools`
  - **Files:**
    - `libTaniumClientExtensions.so`
    - `libTaniumClientExtensions.so.sig`

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

  Do not delete the `Tools` directory without also deleting the `Extensions` directory and the listed files.

  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 (version 7.4 or later) or `tanium.pub` file (version 7.2) and add it to the client.
   a. From the Main menu in Tanium Console, go to **Administration > Configuration > Tanium Server > Infrastructure Configuration Files**.
   b. Click **Download** in the **Clients v7.4+ and Zone Server** or **Clients v7.2** section, depending on which file you need.
   c. Copy the downloaded file into the Tanium Client installation directory.

   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).

   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 Tanium Client 7.4 or later. For more information about managing client configurations in Client Management, see Deploying the Tanium Client

using Client Management on page 105. 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 114.

NOTE

IMPORTANT

Be careful not to allow the `tanium-init.dat` or `tanium.pub` 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 these files do not contain private keys and cannot be used to provide control over a Tanium environment, a user with malicious intent could use them 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.

Preparing the Tanium Client on a Solaris OS image

Prepare the Tanium Client on a reference computer:

1. Install the Tanium Client. See the endpoint requirements and Deploy the Tanium Client to Solaris endpoints using a package file on page 156. During the installation, make sure you do the following:
   - Configure the appropriate server settings. See Configuring connections to the Tanium Core Platform on page 188.
   - 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. See CLI on non-Windows endpoints on page 314 and Tanium Client settings reference on page 298.
6. Perform the following deletions in the Tanium Client installation directory.
   - Delete the following directories, including subdirectories and files:
     - `Downloads`
     - `Logs`
     - `Backup`
   - (Tanium Client 7.4 or later) Delete `pki.db`.
   - (Optional) For an image that you plan to use for a long period of time without updates, also delete the following directories and files:
     - **Directories:**
       - `Extensions`
       - `Tools`

- **Files:**
  - `libTaniumClientExtensions.so`
  - `libTaniumClientExtensions.so.sig`

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

Do not delete the `Tools` directory without also deleting the `Extensions` directory and the listed files.

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 (version 7.4 or later) or `tanium.pub` file (version 7.2) and add it to the client.
   a. From the Main menu in Tanium Console, go to **Administration > Configuration > Tanium Server > Infrastructure Configuration Files**.
   b. Click **Download** in the **Clients v7.4+ and Zone Server** or **Clients v7.2** section, depending on which file you need.
   c. Copy the downloaded file into the Tanium Client installation directory.

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).

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 Tanium Client 7.4 or later. For more information about managing client configurations in Client Management, see Deploying the Tanium Client using Client Management on page 105. 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 114.

Be careful not to allow the `tanium-init.dat` or `tanium.pub` 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.

IMPORTANT

Though these files do not contain private keys and cannot be used to provide control over a Tanium environment, a user with malicious intent could use them 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.

Preparing the Tanium Client on an AIX OS image

Prepare the Tanium Client on a reference computer:

1. Install the Tanium Client. See the endpoint requirements and Deploy the Tanium Client to AIX endpoints using a package file on page 162. During the installation, make sure you do the following:
   - Configure the appropriate server settings. See Configuring connections to the Tanium Core Platform on page 188.
   - 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. See CLI on non-Windows endpoints on page 314 and Tanium Client settings reference on page 298.
6. Perform the following deletions in the Tanium Client installation directory.
   - Delete the following directories, including subdirectories and files:
     - `Downloads`
     - `Logs`
     - `Backup`
   - (Tanium Client 7.4 or later) Delete `pki.db`.
   - (Optional) For an image that you plan to use for a long period of time without updates, also delete the following directories and files:
     - **Directories:**
       - `Extensions`
       - `Tools`

- **Files:**
  - `libTaniumClientExtensions.so`
  - `libTaniumClientExtensions.so.sig`

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

Do not delete the `Tools` directory without also deleting the `Extensions` directory and the listed files.

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 (version 7.4 or later) or `tanium.pub` file (version 7.2) and add it to the client.
   a. From the Main menu in Tanium Console, go to **Administration > Configuration > Tanium Server > Infrastructure Configuration Files**.
   b. Click **Download** in the **Clients v7.4+ and Zone Server** or **Clients v7.2** section, depending on which file you need.
   c. Copy the downloaded file into the Tanium Client installation directory.

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).

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 Tanium Client 7.4 or later. For more information about managing client configurations in Client Management, see Deploying the Tanium Client using Client Management on page 105. 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 114.

Be careful not to allow the `tanium-init.dat` or `tanium.pub` 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.

IMPORTANT

Though these files do not contain private keys and cannot be used to provide control over a Tanium environment, a user with malicious intent could use them 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.

Preparing the Tanium Client on a virtual desktop infrastructure (VDI) instance

For licensing and performance considerations that apply in VDI environments, see Assess the environment where you are deploying the Tanium Client on page 101.

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. See Tanium Console User Guide: 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 168
   - Preparing the Tanium Client on a Linux OS image on page 174
   - Preparing the Tanium Client on a macOS image on page 171
   - Preparing the Tanium Client on a Solaris OS image on page 177
   - Preparing the Tanium Client on an AIX OS image on page 180

   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, 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 Tanium Console User Guide: 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 image. For more information, see Tanium Console User Guide: 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`.

   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, 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:
    - Manage the Tanium Client service on Windows on page 237
    - Manage the Tanium Client service on macOS on page 242
    - Manage the Tanium Client service on Linux on page 247
    - Manage the Tanium Client service on Solaris on page 250
    - Manage the Tanium Client service on AIX on page 252
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>`

Table 6: Best practice client settings for VDI instances

Client Setting	Default Value	Best Practice Value for VDI	Explanation
RandomSensorDelayInSeconds	0	20	By default, sensors run immediately. This setting delays the execution of any sensor by a random time up to 20 seconds, which reduces concurrent execution of sensors and packages.
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.

Table 6: Best practice client settings for VDI instances (continued)

Client Setting	Default Value	Best Practice Value for VDI	Explanation
LogVerbosityLevel	1	0	Disable logging to reduce disk writes. Temporarily re-enable logging on individual endpoints for troubleshooting.
Logs.extensions.LogVerbosityLevel	11	0	Disable Tanium™ Client Extensions logging to reduce disk writes. Temporarily re-enable logging on individual endpoints for troubleshooting.
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.

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.

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 310.

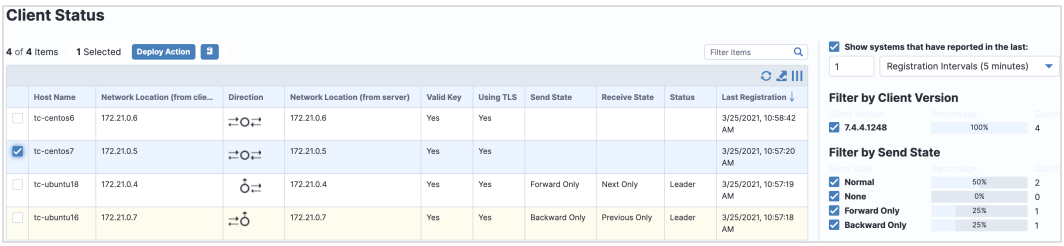
Verify the Tanium Client installation

> **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).



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.

For the settings that connect Tanium Clients through HTTPS proxy servers, see Connect through an HTTPS forward proxy server on page 194.

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.

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.

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.

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 in the Tanium Client configuration (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**.

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.

You can set the port that the Tanium Client uses to communicate with servers by appending `:<port_number>` to **ServerName** (for example, `ts1.local.com:443`). The **ServerName** port overrides the **ServerPort** setting in the Tanium Client configuration (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**.

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 221

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.

Table 7: Default content related to ServerNameList, ServerName, and ServerPort

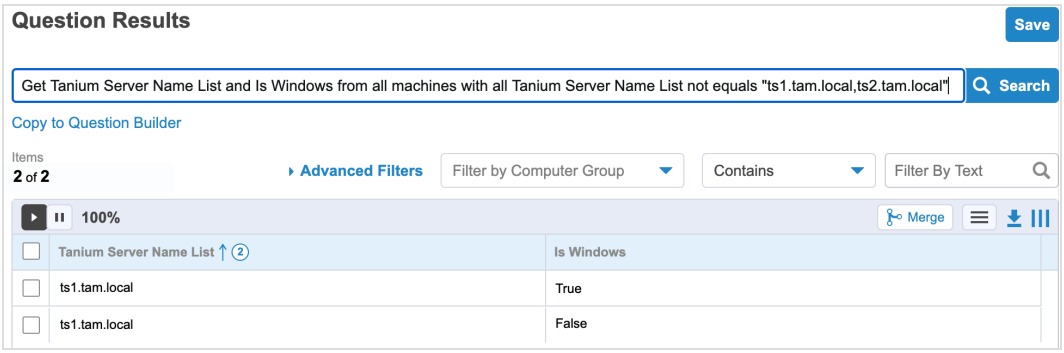
Content	Object Name	Usage
Sensors	Tanium Server Name	Returns the current value of **ServerName** from the Tanium Client. For a client on which **ServerNameList** is configured, you can use the sensor to identify the Tanium Server or Zone Server with which the client currently connects. For example: `Get 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 298.
Packages	Set Tanium Server Name	Sets the **ServerName** value on Windows endpoints and restarts the Tanium Client service. The **ServerName** setting is in the Windows registry.
	Set Tanium Server Name [Non-Windows]	Sets the **ServerName** value on non-Windows endpoints and restarts the Tanium Client system service. The **ServerName** setting is in an SQLite database and is set through a CLI command.
	Set Tanium Server Name List	Sets the **ServerNameList** value on Windows endpoints and restarts the Tanium Client service. The **ServerNameList** setting is in the Windows registry.
	Set Tanium Server Name List [Non-Windows]	Sets the **ServerNameList** value on non-Windows endpoints and restarts the Tanium Client system service. The **ServerNameList** setting is in an SQLite database and is set through a CLI command.

Configure clients to connect with multiple Tanium Servers

The following procedure provides an example of how to use the objects listed in Table 7 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.

For an example of how to set the **ServerNameList** on Tanium Clients that register with a Zone Server, see Tanium Core Platform User Guide for Windows Deployments: Configure Tanium Clients to register with the Zone Server.

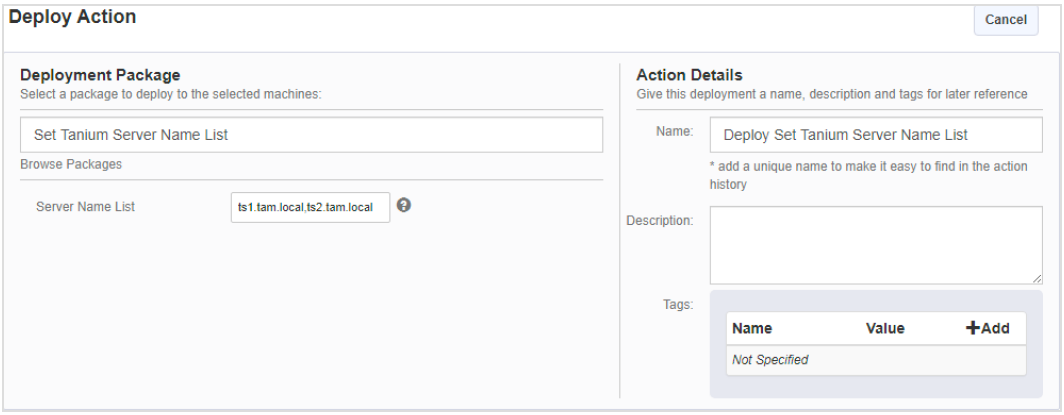
1. Delete any existing scheduled actions that configure **ServerNameList** or **ServerName** to prevent conflicts with the new actions that you create for those settings.
2. Use Tanium Interact to ask a question that identifies the Tanium Clients that require an updated **ServerNameList**.
   The following 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 with all Tanium Server Name List not equals "ts1.tam.local,ts2.tam.local"`



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**.

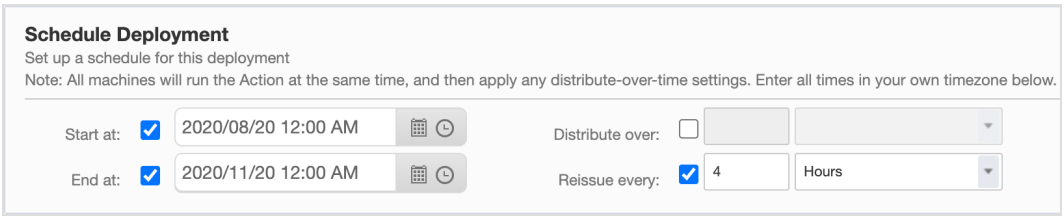
> **NOTE** Windows endpoints and non-Windows endpoints require different packages. If you are updating both Windows and non-Windows endpoints, complete this procedure separately for each group.

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.



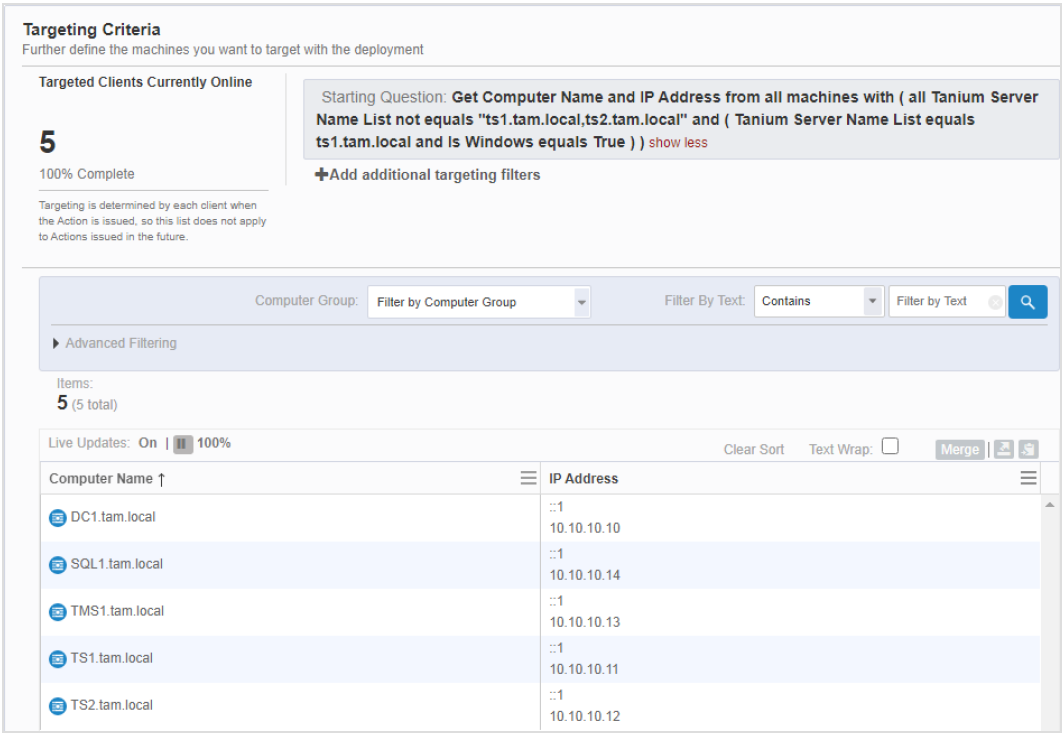
6. Set a schedule for the action.

> **BEST PRACTICE**
>
> Set a reissue interval if some target endpoints might be offline when you initially deploy the action.

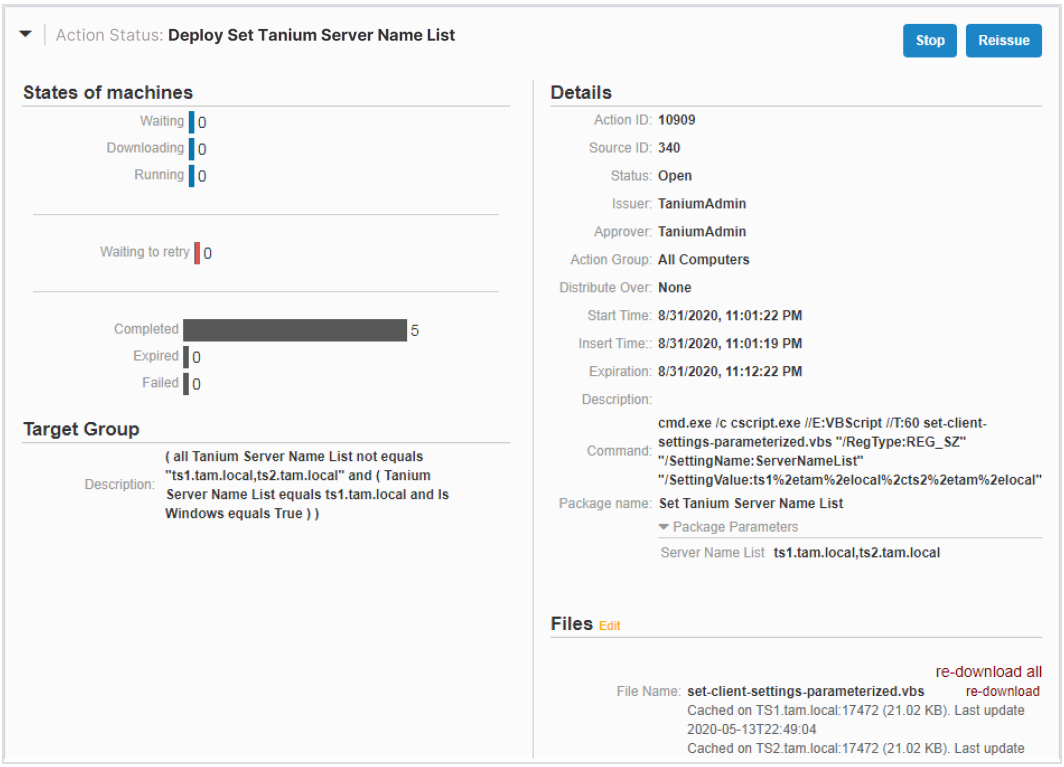


7. In the **Targeting Criteria** section, ensure the settings target Windows endpoints or non-Windows endpoints based on the package that you selected.

8. Click **Show preview to continue** and verify that the targeting is correct.



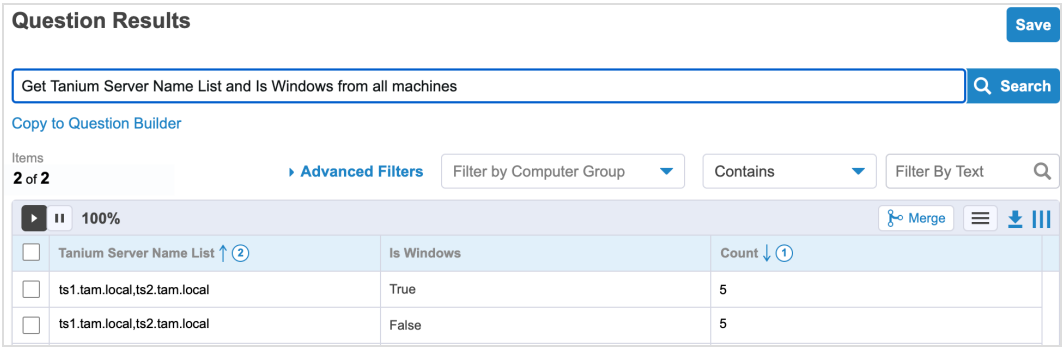
9. Click **Deploy Action** and review the action status to verify that the action completes without errors. For more information about the action status, see Tanium Console User Guide: View action status.



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.



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 7.4.2.2033 or later to establish a TLS tunnel through an HTTPS forward proxy server. 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 Tanium Appliance User Guide: Securing Tanium Server, Zone Server, and Tanium Client access or Tanium Core Platform User Guide for Windows Deployments: Securing Tanium Server, Zone Server, and Tanium Client access.

To use a proxy server with Tanium Clients, your environment must meet the following requirements:

- Tanium Client 7.4.2.2033 or later must be installed on endpoints that connect through the proxy server.
- The proxy server uses the HTTP CONNECT method for TLS tunneling.
- The proxy server must not require authentication.
- The proxy server does 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.

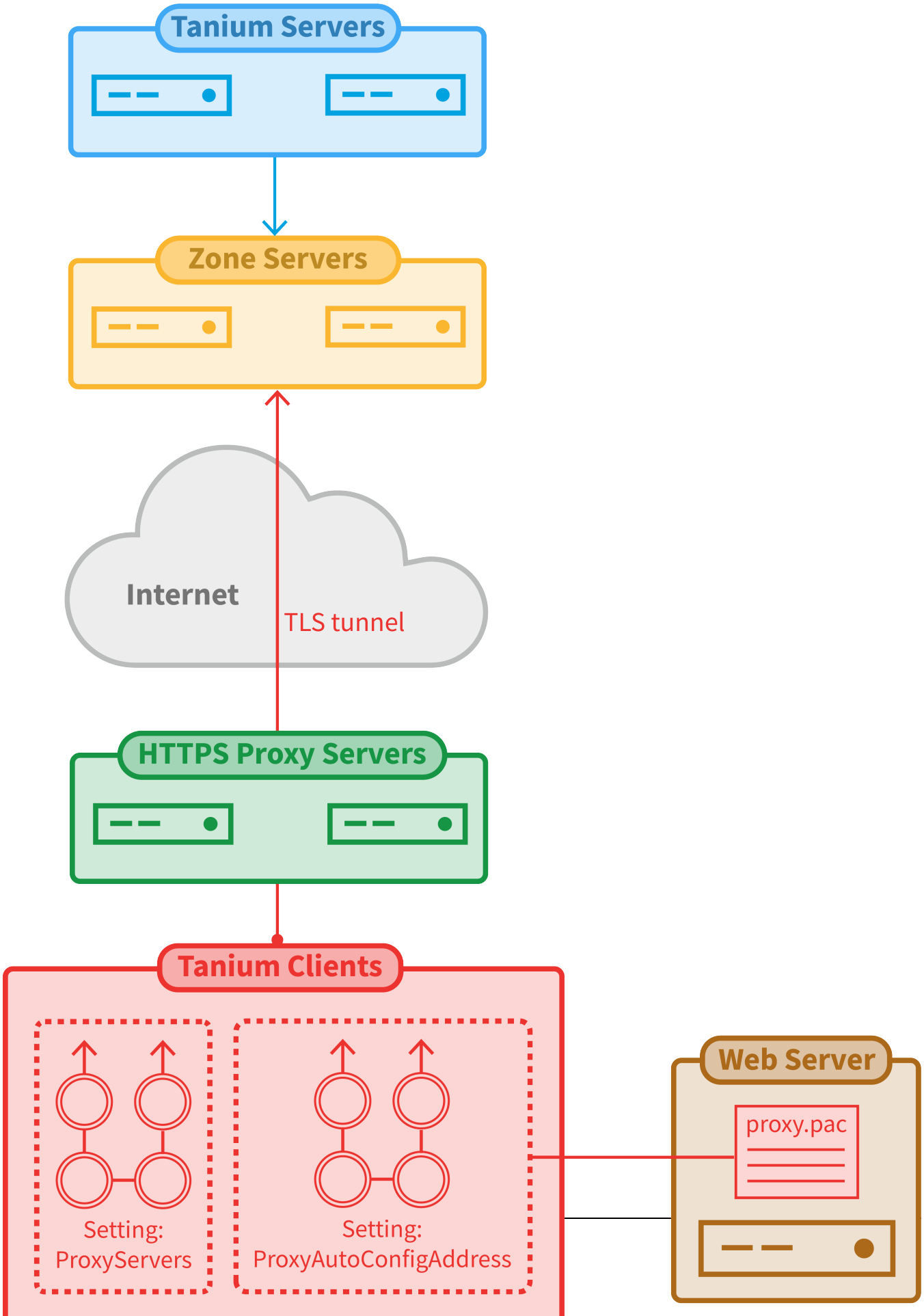
As an alternative to connecting through a proxy server, you can use a Tanium Cloud Access Point to facilitate communication from networks that have restricted access to Tanium Cloud. For more information, see Tanium Appliance User Guide: Installing and managing a Tanium Cloud Access Point.

The steps to connect to a proxy depend on whether the endpoints can access a proxy auto configuration (PAC) file, which is available only for Windows endpoints. A PAC file defines how web browsers connect to specific hosts (such as a Tanium Server FQDN), directly or through a proxy server, and defines how the browsers select the correct proxy for each URL. Configure the **ProxyAutoConfigAddress** setting on endpoints that can access a PAC file and the **ProxyServers** setting on endpoints that cannot. Configure only one of the settings on any single endpoint: if you configure both, the Tanium Client uses only **ProxyAutoConfigAddress** and ignores **ProxyServers**.

If no proxy servers are available, the Tanium Client falls back to connecting directly with 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 5: Connecting through an HTTPS proxy server to Tanium Core Platform servers


Tanium Servers
Zone Servers
Internet
TLS tunnel
HTTPS Proxy Servers
Tanium Clients
Setting:
ProxyServers
Setting:
ProxyAutoConfigAddress
Web Server
proxy.pac

Before you begin

Work with your network administration team to perform the following tasks before connecting 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. See Network connectivity, ports, and firewalls on page 72.
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.

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 Managment to create a client configuration, and then download an installation bundle for use in another deployment method. For more information, see Deploying the Tanium Client using Client Management on page 105.

BEST PRACTICE

Configure proxy server settings during client deployment.

Configure proxy connections with a PAC file

For Tanium Clients on Windows endpoints, you can configure proxy connections using a PAC file if one is available. 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.

CONFIGURE PROXY CONNECTIONS DURING CLIENT DEPLOYMENT

Configure Tanium Clients to use a PAC file by setting **ProxyAutoConfigAddress** during client installation. See Deploying the Tanium Client using Client Management on page 105 or Deploy the Tanium Client to Windows endpoints using the installer on page 135 for the steps to install the client.

Table 8: Methods to set a PAC file URL during deployment

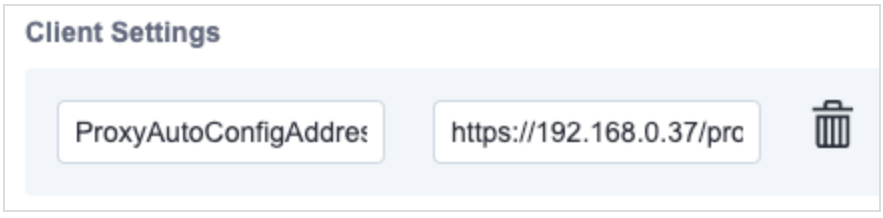
Installation method	Method to set ProxyAutoConfigAddress
Client Management	Include the **ProxyAutoConfigAddress** setting and the URL of the PAC file as a key and value in client settings. For more information, see Deploying the Tanium Client using Client Management on page 105. 

Table 8: Methods to set a PAC file URL during deployment (continued)

Installation method	Method to set ProxyAutoConfigAddress
Command-line interface (CLI)	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. See Install the Tanium Client on Windows using the command line on page 137.

Installation wizard	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 PROXY CONNECTIONS AFTER CLIENT DEPLOYMENT

You can configure Tanium Clients to use a PAC file after the initial client deployment, or change the file on clients that already use a PAC file.

1. Go to the Tanium **Home** page and ask the following question to identify the proxy servers with which Tanium Clients currently connect, if any:
   `Get Tanium Client Explicit Setting[ProxyAutoConfigAddress] and Tanium Client Explicit Setting [ProxyServers] from all machines`
2. Select the results for clients that do not already use the PAC file that you want and click **Deploy Action**.
3. Configure the package settings:
   - **Deployment Package**: Select **Modify Tanium Client Setting**.
   - **RegType**: Select **REG_SZ**.
   - **ValueName**: Enter `ProxyAutoConfigAddress`.
   - **ValueData**: Enter the new PAC file URL and file name in the format `http[s]://<PAC file URL>/<PAC file name>.pac`.
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.
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.
8. Ask the following question to verify that clients have the updated **ProxyAutoConfigAddress** setting:
   `Get Tanium Client Explicit Setting[ProxyAutoConfigAddress] from all machines`

   IMPORTANT

   Clients do not apply the updated setting until you manually restart them or wait for the automatic client reset, which by default occurs at a random interval in the range of two to six hours.
9. (Optional) Restart the Tanium Client service on each endpoint to apply the updated proxy setting immediately. For the steps, see Manage the Tanium Client service on Windows on page 237.

Configure proxy connections without a PAC file

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.

CONFIGURE PROXY CONNECTIONS DURING CLIENT DEPLOYMENT

Configure Tanium Clients to connect through proxy servers by setting **ProxyServers** during installation. For installation procedures, see Deploying the Tanium Client using an installer or package file on page 134.

Table 9: Methods to set proxy server addresses during deployment

Installation method	OS	Method to set ProxyServers
Client Management	Any	Include the **ProxyServers** setting and the addresses of proxy servers as a key and value in client settings. For more information, see Deploying the Tanium Client using Client Management on page 105. 

Table 9: Methods to set proxy server addresses during deployment (continued)

Installation method	OS	Method to set ProxyServers

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>"`

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>"`

	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>"`

CONFIGURE PROXY CONNECTIONS AFTER CLIENT DEPLOYMENT

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 servers with which Tanium Clients currently connect, if any:
   `Get Tanium Client Explicit Setting[ProxyServers] and Is Windows from all machines`
2. Select the results for either Windows or non-Windows endpoints that require new or updated proxy connections and click **Deploy Action**.

   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**.
    - **ValueName**: Enter `ProxyServers`.
    - **ValueData**: Enter 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>`.
4. (Optional) In the **Schedule Deployment** section, set a schedule for the action.

    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
    - 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.
8. Ask the following question to verify that clients have the correct **ProxyServers** setting.
    `Get Tanium Client Explicit Setting[ProxyServers] and Is Windows from all machines`

    Clients do not apply the updated setting until you manually restart them or wait for the automatic client reset, which by default occurs at a random interval in the range of two to six hours.
9. (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 237
    - Manage the Tanium Client service on macOS on page 242
    - Manage the Tanium Client service on Linux on page 247
    - Manage the Tanium Client service on Solaris on page 250
    - Manage the Tanium Client service on AIX on page 252

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 details about how Tanium Client peering works and related concepts, see Client peering on page 20.

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. See Customize listening ports on page 221.

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 to configure a few key settings that further optimize peer communication based on the characteristics of your network. For example, separate settings apply to clients that connect directly to the Tanium Server than to clients that connect to a Tanium Zone Server. Focus on the following objectives when tuning the settings:

- **LAN peering only**: The default address mask (IPv4) and address prefix (IPv6) settings are designed to prevent Tanium Client peering across WANs. For details, see Address mask and prefix settings on page 204.
- **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 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 206.
- **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 Figure 6). For more information, see Configure isolated subnets on page 208.
- **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 applies the most restrictive rule to determine the subnet for that client. For example, if the default address mask defines a /24 subnet, and the 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.

In Tanium Core Platform 7.4.3 or later, Tanium Servers write subnet configurations to the Tanium database and automatically synchronize them in an active-active deployment. In Tanium Core Platform 7.4.6 or later, 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 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.

Figure 6 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 Figure 6, 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.

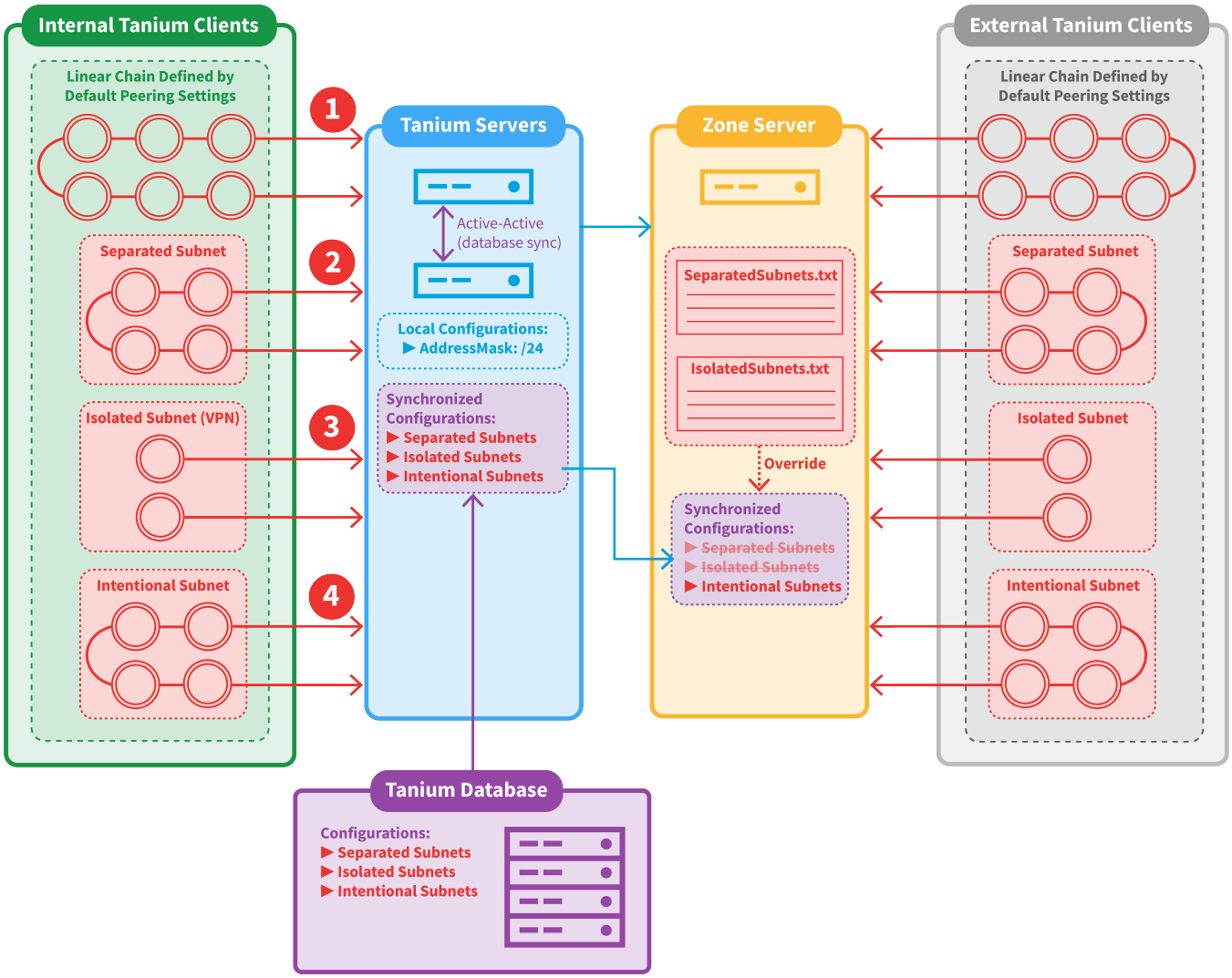
4 **Intentional subnets configuration**

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 6: Tanium Client peering



Address mask and prefix settings

Contact Tanium Support to help determine the appropriate values for the following Tanium Client peering settings.

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:

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. See Configure isolated subnets on page 208.

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.

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 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 to determine the optimum value for peering in IPv6 networks.

Configure separated subnets

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 on page 204). 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 leader connections on page 214.

Figure 6 shows an example deployment with separated subnets.

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.

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 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 `;` or `#` character before any optional comments.
   See the following example:

   ```
   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
   ```


   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

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 server. Because Zone Servers do not synchronize custom subnet configurations, each 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 on page 207.
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.

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.
4. Use the menu to specify subnets in CIDR format.

Configure isolated subnets

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 work as expected after the clients register, see Verify or remediate Tanium Client peering and leader connections on page 214.

Figure 6 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 File distribution on page 24.
- 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

BEST PRACTICE

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.

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 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 `;` or `#` character before any optional comments.
   See the following example:

   ```
   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**.

Configure isolated subnets that are specific to Zone Servers

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.

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

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 Address mask and prefix settings on page 204.

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 (see Tanium Appliance User Guide: Reference: Tanium Core Platform command-line interface or Tanium Core Platform User Guide for Windows Deployments: Reference: Command-line interface).
3. Navigate to the Zone Server installation folder:

   ```
   > cd <Zone Server>
   ```

4. Configure the **AddressMask** local setting to specify /32 subnet boundaries (single hosts):

   ```
   > TaniumZoneServer config set AddressMask 4294967295
   ```

For more information, see Address mask and prefix settings on page 204.

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 on page 209.

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.

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.
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.

Figure 6 shows an example deployment with intentional subnets.

IMPORTANT

Intentional subnets require Tanium Core Platform 7.5.3 or later and Tanium Client 7.4.7.1130 or later. Using the **PeerNeighborhood** client setting requires Tanium Core Platform 7.5.5 or later.

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 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 > 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 subnet mask, which is the default peering range (see Overview of Tanium Client peering settings).

Table 10: 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

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:
    - 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 approriate 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 Table 10, 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.
     - **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 on page 213.

   - 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 on page 214.
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 on page 214.

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.
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.

Using the **PeerNeighborhood** client setting to define intentional subnets requires Tanium Core Platform 7.5.5 or later.

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 Modify client settings on page 254.

VERIFY INTENTIONAL SUBNETS

After you configure intentional subnets, wait for the next client-reset interval before verifying that the subnets work as expected. 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

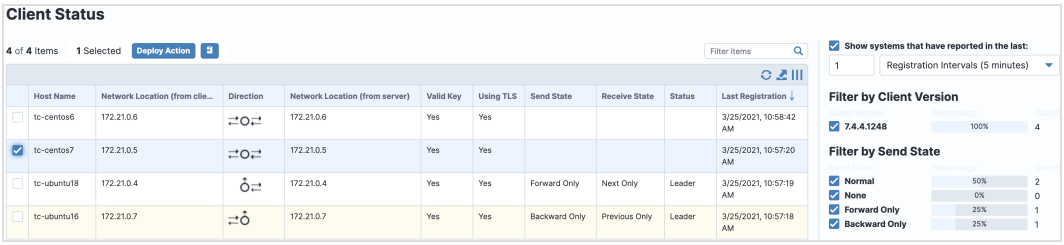
The **Client Status** page displays information about the state of Tanium Client registration and connectivity, and enables you to deploy actions to remediate issues.

NOTE

You require a role with **Client Status** read permission is required to see the **Client Status** page. The **Administrator** reserved role has this permission.

View the status of Tanium Client registration and communication

1. From the Main menu, go to **Administration > Configuration > Client Status**.
2. (Optional) To display status details only for specific Tanium Clients, edit the default filter settings, such as the registration intervals and connection status. 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.



The following table lists the information that the **Client Status** page displays for each Tanium Client.

TIP

Certain columns are hidden by default. To display or hide columns, click Customize Columns and select (display) or clear (hide) column names.

Table 11: Client Status columns

Column	Description
Host Name	Endpoint host name.
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 Table 12.
Valid Key	No indicates an issue with the public key that the Tanium Client uses to secure communication with other Tanium Core Platform components. To resolve the issue, reinstall the Tanium Client (see Deploying the Tanium Client) or redeploy the key (see Tanium Console User Guide: Download infrastructure configuration files (keys)).

Table 11: Client Status columns (continued)

Column	Description
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 details 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:

Table 12: 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.
	Double side arrows 	The client has a neighborhood list of peers and has connected with peers in the indicated direction.
Client state	Normal 	The client is communicating normally.
	Blocked 	The client is not communicating reliably. This 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

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. Select rows in the grid to export information for specific Tanium Clients. If you want to export information for all clients, skip this step.
3. Click Export  .
4. (Optional) Edit the default export **File Name** .

   The file suffix (`.csv` or `.json`) changes automatically based on the **Format** selection.
5. Select an **Export Data** option: information for **All** clients in the grid or only for the **Selected** clients.
6. Select the file **Format**: **JSON** (**Administrator** reserved role only) or **CSV**.
7. 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

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

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.

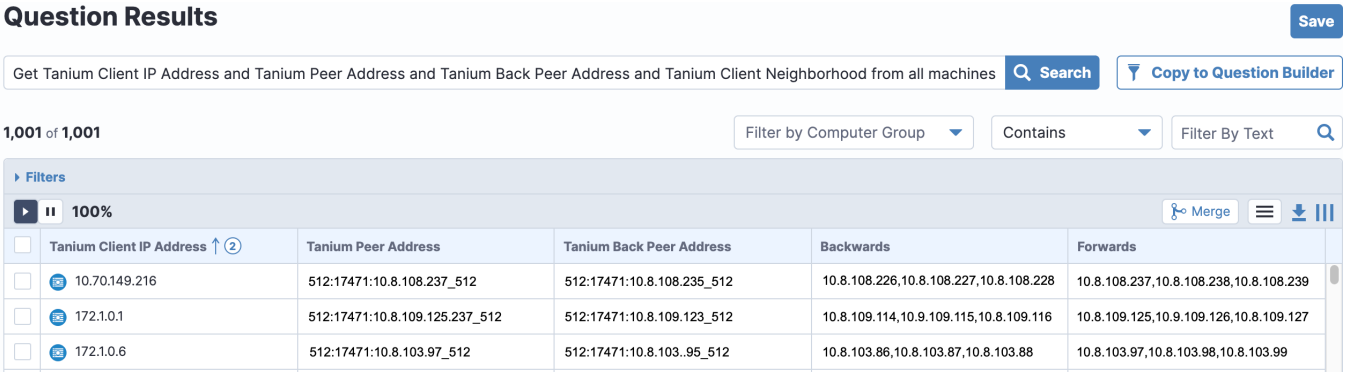
Use questions to review peering settings

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**
- **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 7: Sensors for peering information

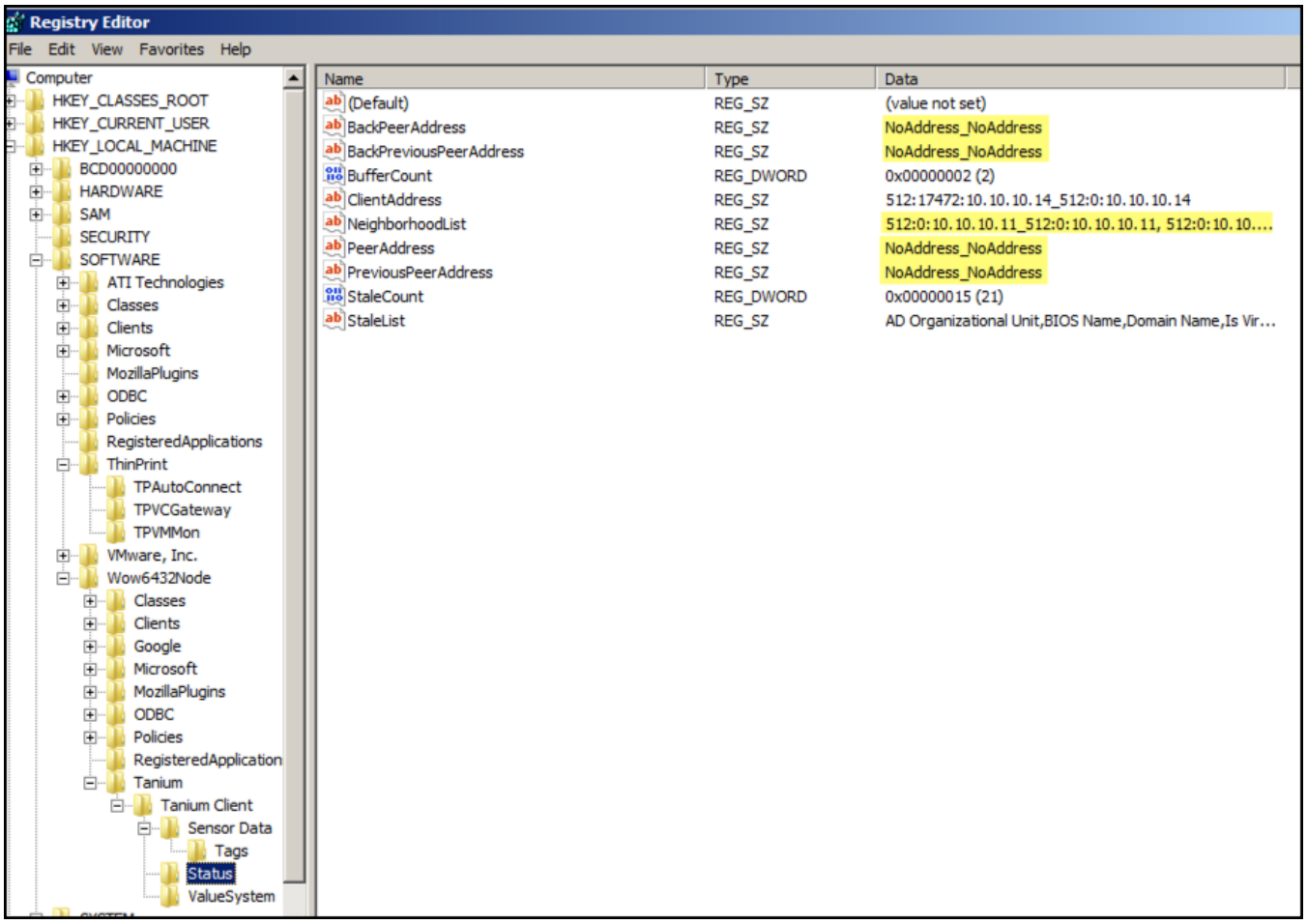


Examine the Tanium Client configuration

You can check the peer address lists in the Tanium Client settings on an individual Tanium 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 8: Peering information in Windows Registry



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: tam.local
  - LastGoodServerName: zs1.tam.local
  - LogVerbosityLevel: 1
  - RegistrationCount: 3333
  - Resolver: nslookup
  - ServerName: zs1.tam.local
  - ServerNameList: ts1.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
  - 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: 7.5.6.1137
```

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.

Work with your network administrator to configure your endpoint firewalls 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.

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. See Modify default client settings in Tanium Console on page 257.

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.

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. See Compatibility between Tanium Core Platform servers and Tanium Clients on page 70.)
- 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.

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`.

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.

Monitoring, managing, and maintaining Tanium Clients

These sections provide information on the following activities to manage the Tanium Client:

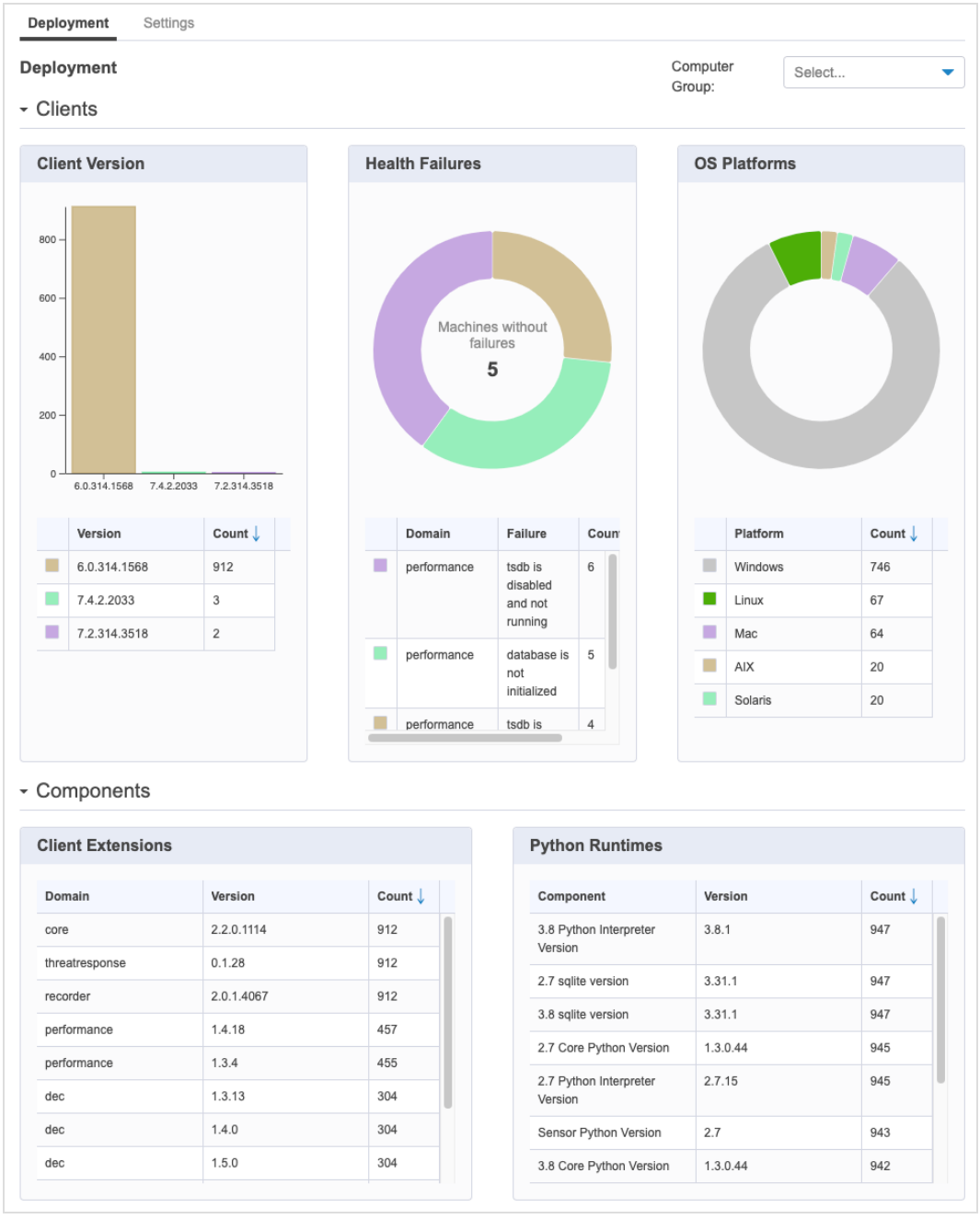
- Monitoring Tanium Client health and accessing client logs
- General management of Tanium Clients, such as using built-in content, managing the Tanium Client service on each operating system, and managing certain operating system features related to the Tanium Client
- Regular maintenance to keep Tanium Clients connected and in good health
- Upgrading the Tanium Client
- Uninstalling the Tanium Client

Monitoring Tanium Clients

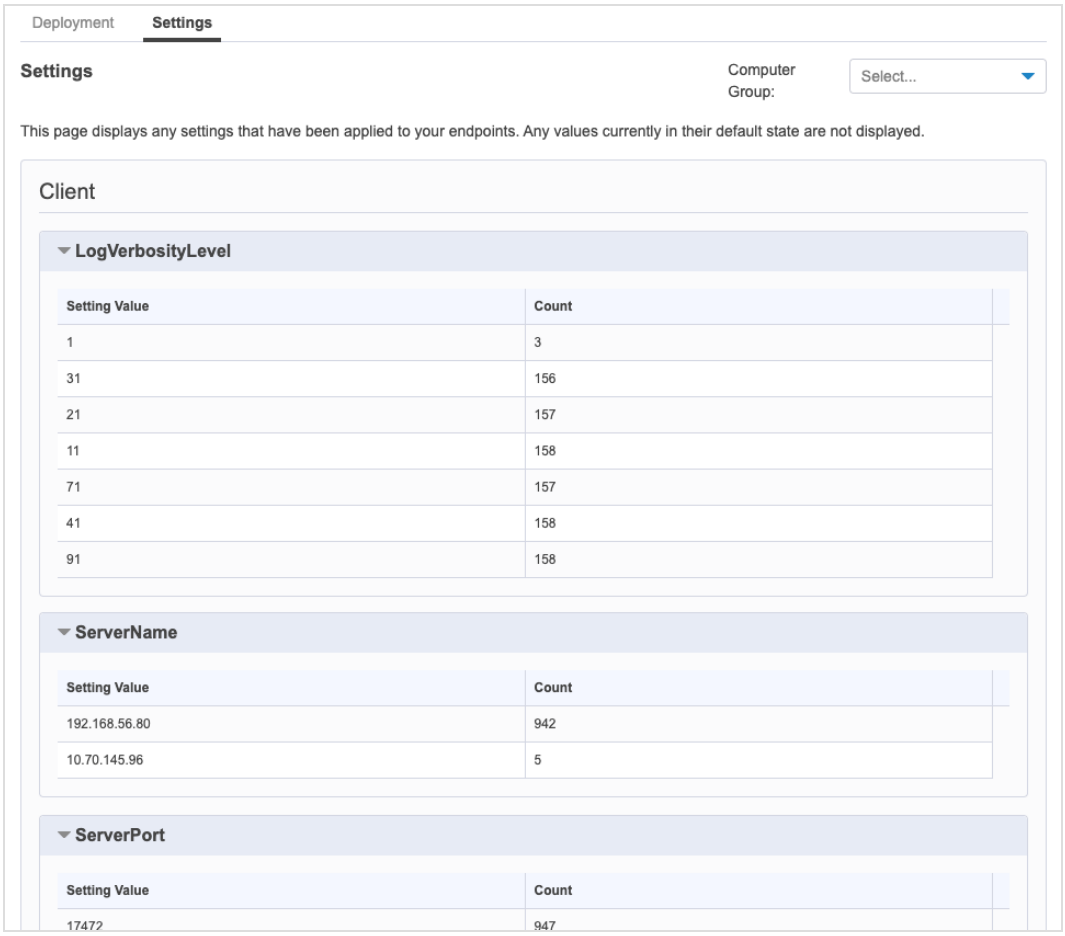
Monitor the client health overview in Client Management

Review a summary of health information about deployed Tanium Clients in Client Management.

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



- 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.



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 Tanium Interact User Guide: Managing question results.

TIP

To resolve client extension failures, see the following sections:

- To resolve Client Index Extension failures, see Tanium Client Index Extension User Guide: Reference: Common health check issues.
- To resolve Client Recorder Extension failures, see Tanium Client Recorder Extension User Guide: Troubleshooting the Client Recorder Extension.
- To resolve failures associated with client extensions for other Tanium solutions, see Tanium Console User Guide: Troubleshoot solution-specific issues and Tanium Endpoint Configuration User Guide: Identify and resolve issues with endpoint tools or client extensions.

Access detailed client health and troubleshooting information on an endpoint

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.

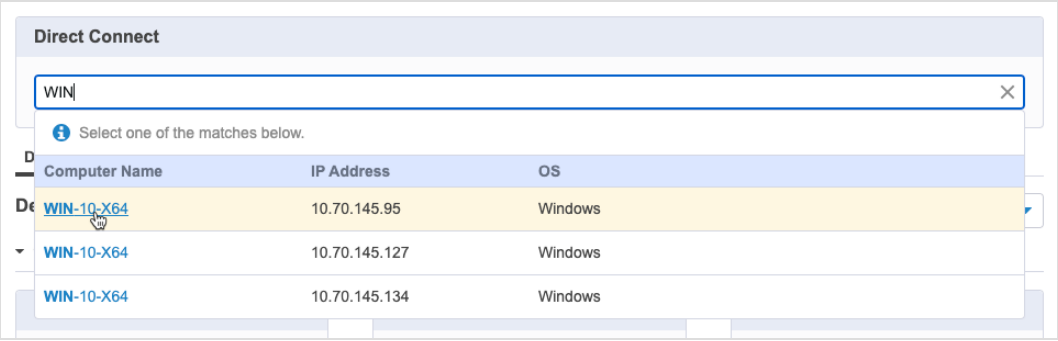
TIP

For additional information about troubleshooting the Tanium Client, see Troubleshooting Tanium Clients and Client Management on page 277.

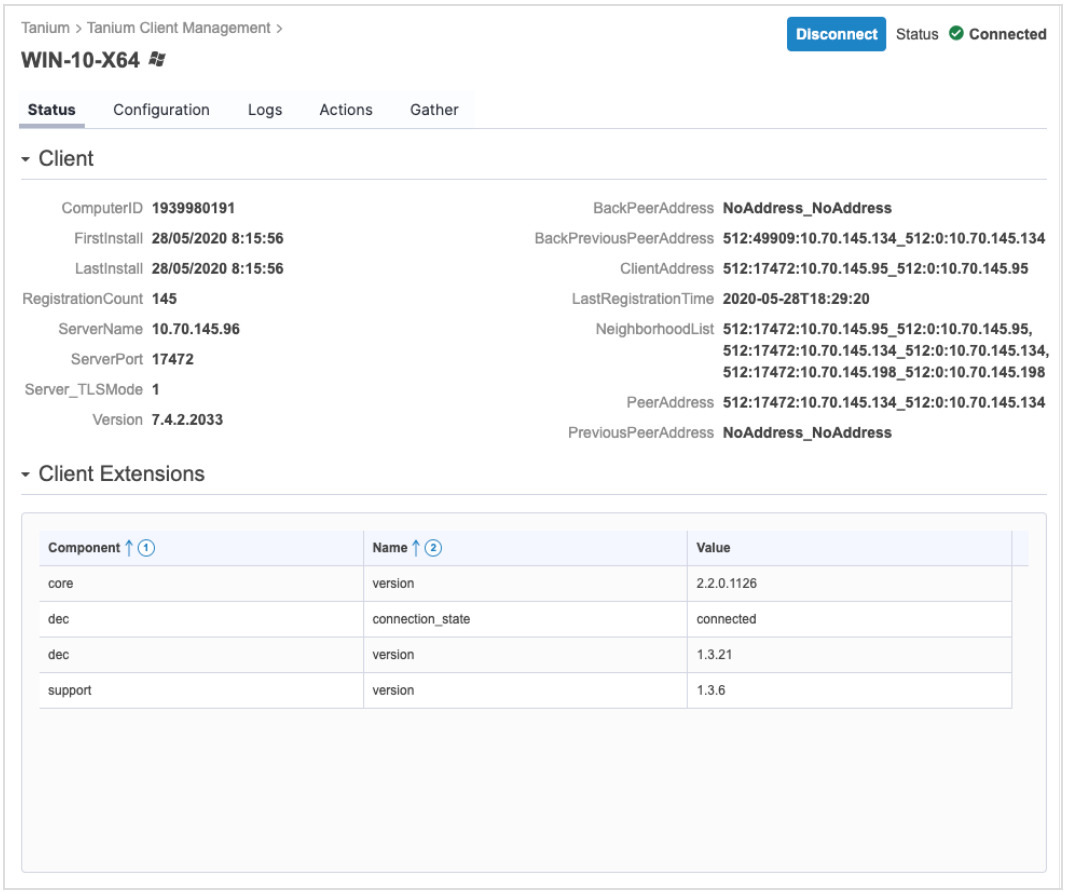
NOTE

- 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 Tanium Direct Connect User Guide: Configure Direct Connect and Tanium Console User Guide: Managing action locks.

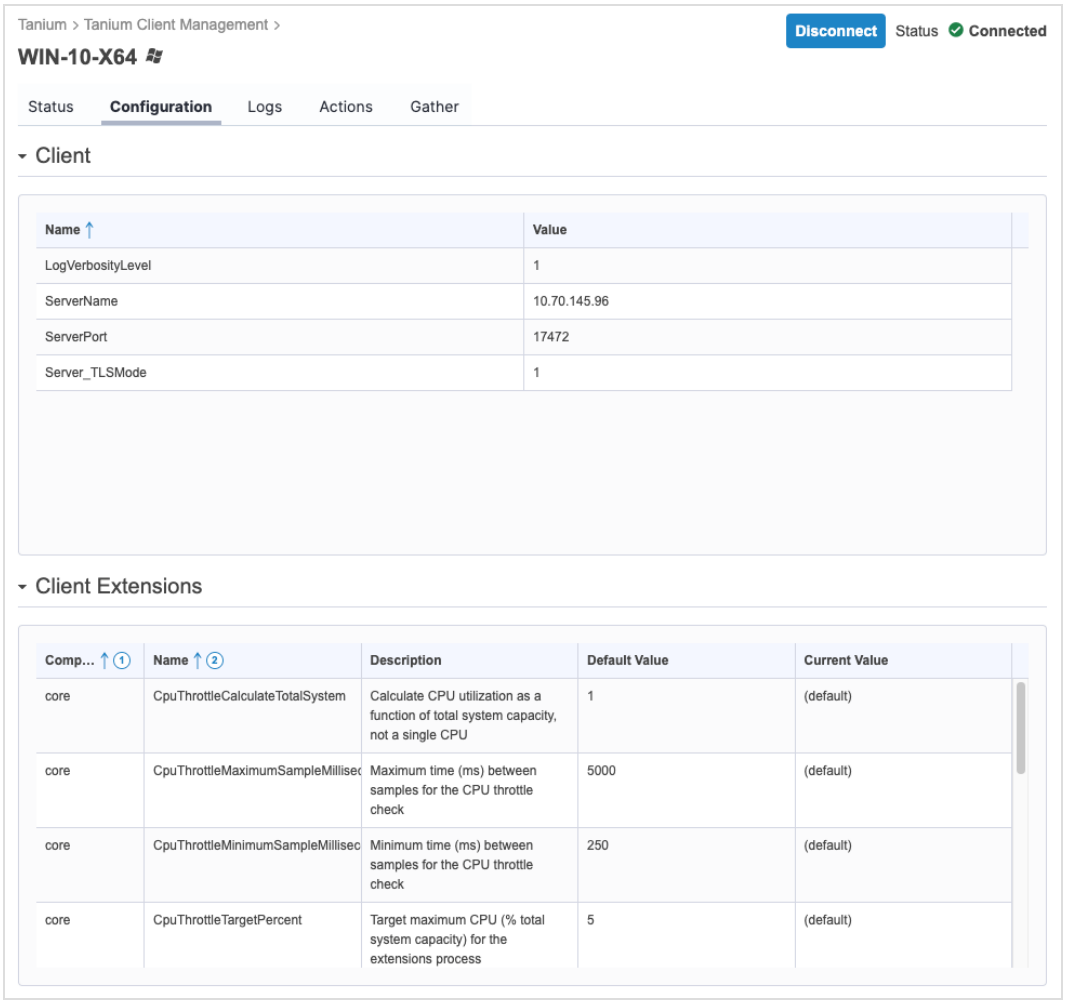
1. From the Main menu, go to **Administration > Shared Services > Client Management**.
2. From the **Client Management** menu, go to **Client Health**.
3. In the **Direct Connect** search box, enter all or part of an IP address or a computer name.
   Matching results are displayed after the search completes.
4. From the search results, click the computer name to connect to the endpoint.



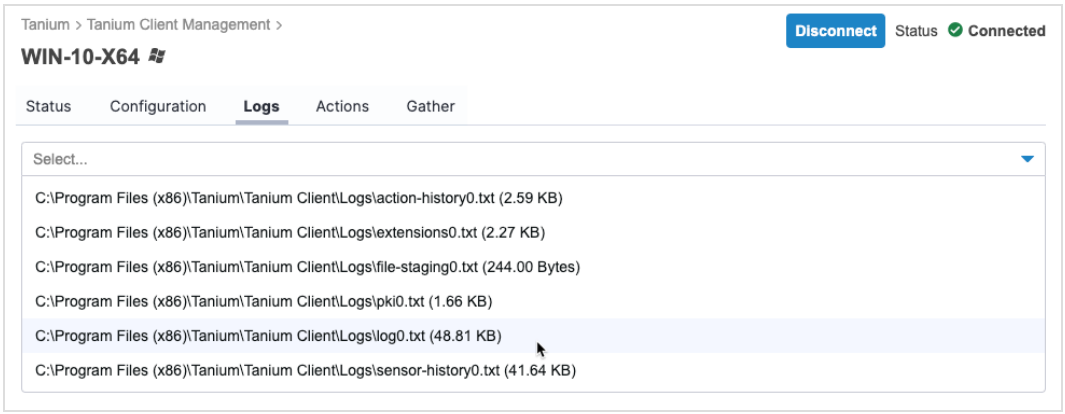
5. Click a tab to view the detailed client health information for the endpoint.
   - **Status**: View status information about the connected endpoint, such as the computer ID, the first and last client installation time stamps, the installed client version, client and peer address information, and client extension information, including any health check failures.



- **Configuration**: View information about client settings for the connected endpoint, such as log verbosity level, server name, server port, and various settings for client extensions.

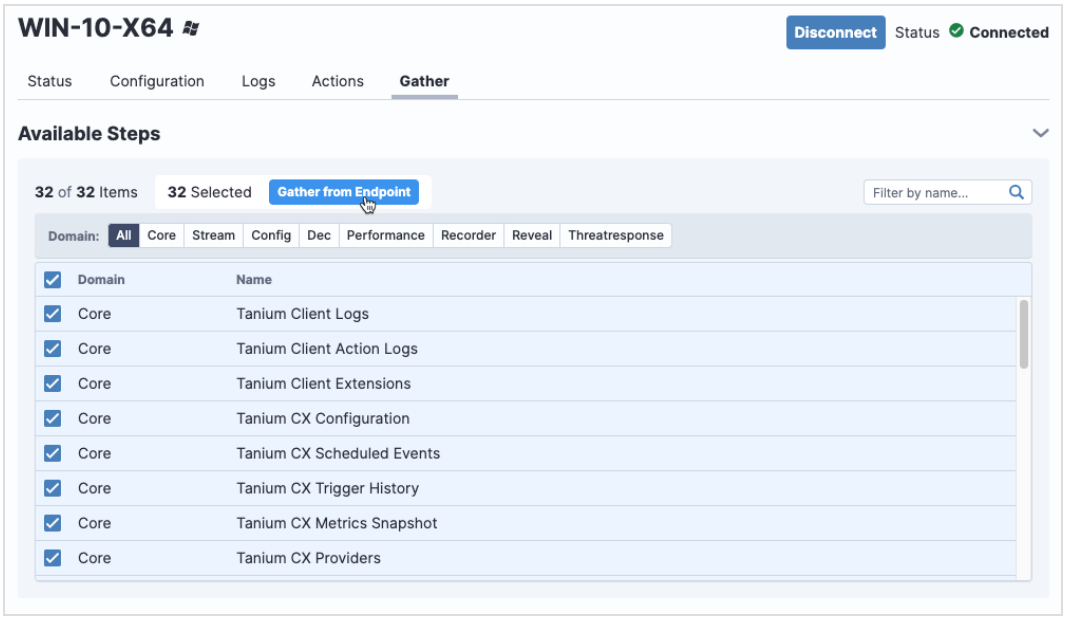


- **Logs**: View and download logs from the connected client. Select a log to view or download. For more information about reviewing logs for troubleshooting, see Review the Tanium Client installation log to troubleshoot installation on Windows on page 278 and Review Tanium Client logs to troubleshoot connections and other client issues on page 281.



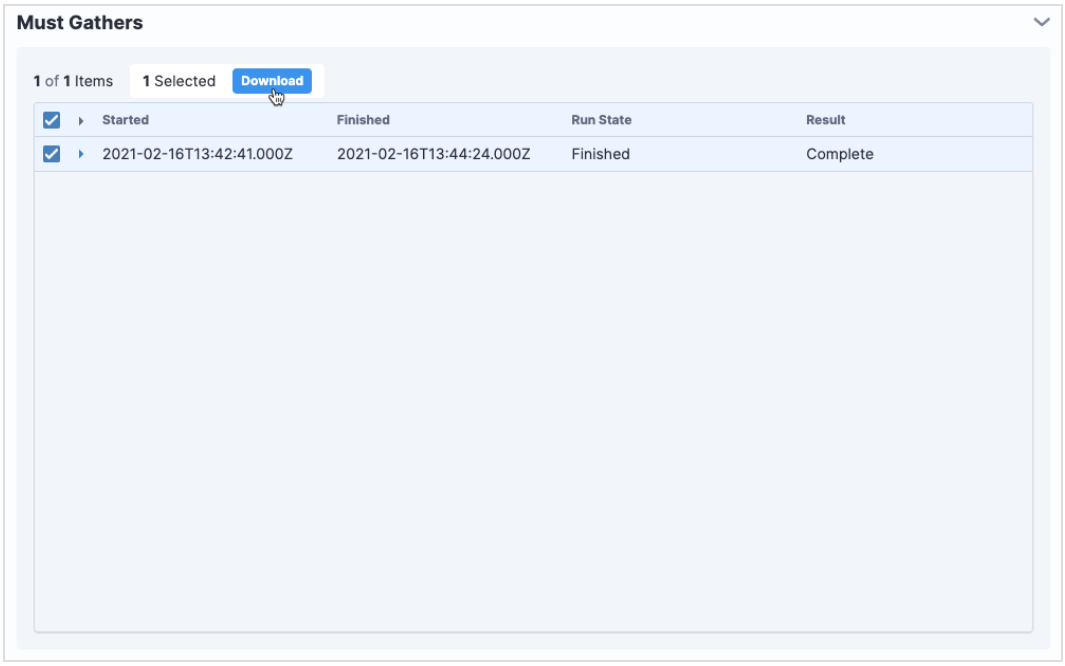
- **Actions**: View and download action logs from the connected client. Select a previously run action for which you want to view or download the log. For more information about reviewing action logs for troubleshooting, see Review action logs and associated files to troubleshoot actions and packages on page 282.
- **Gather**: Collect a bundle of logs and other artifacts from a connected endpoint to help resolve issues.

  a. To filter the available logs and artifacts, click a button in the **Domain** section. Click **Gather from Endpoint**.



  The selected logs and artifacts are gathered from the endpoint. The package appears in the **Must Gathers** section, named with its time stamp.

b. When **Finished** appears in the **Run State** column, select the package and click **Download** to download a ZIP file that contains the troubleshooting information.



6. When you finish reviewing client health information for the endpoint, click **Disconnect** to disconnect from the endpoint and return to the client health summary.

NOTE

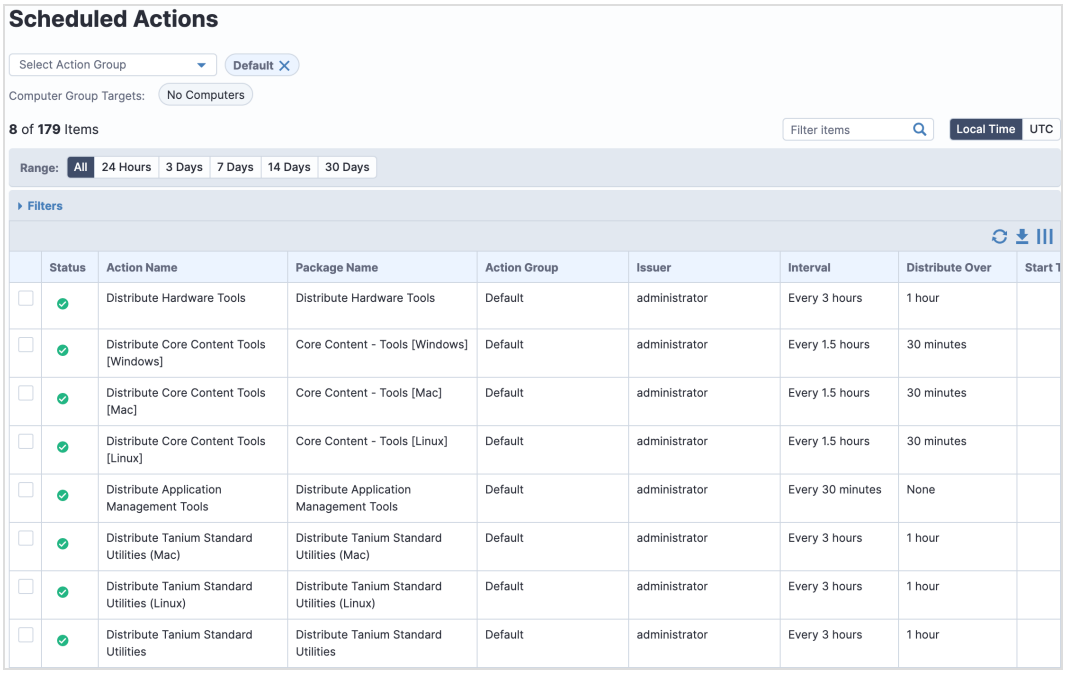
If the connection to the endpoint times out, click **Reconnect** to reestablish the connection.

Managing Tanium Clients

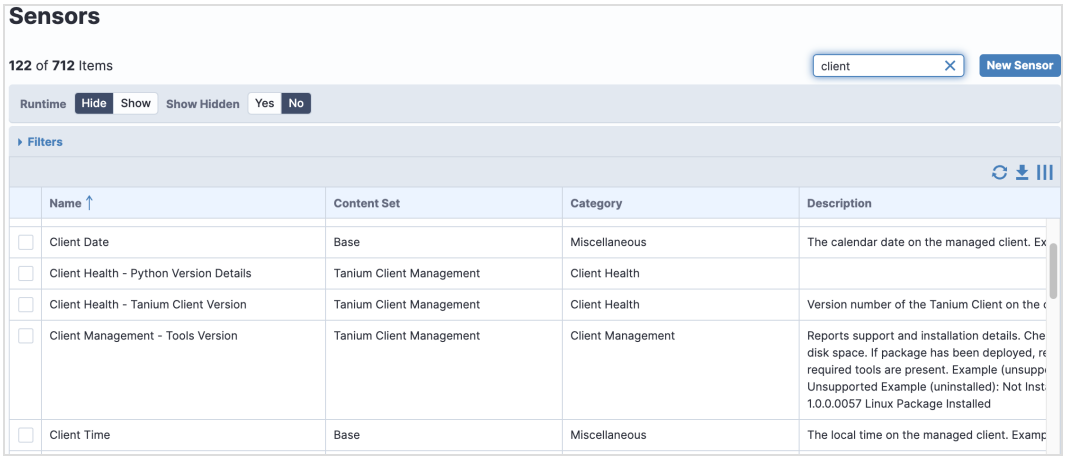
Use built-in saved questions, sensors, and packages

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:

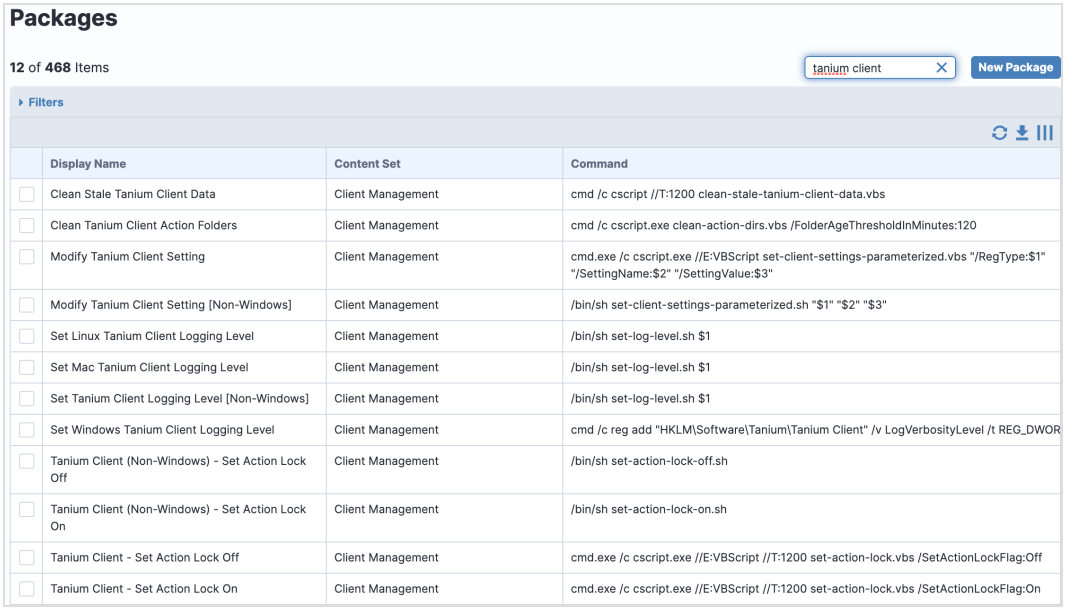
- Go to **Administration > Actions > Scheduled Actions**, select **Default** for the **Action Group**, and review the actions that are scheduled to run.



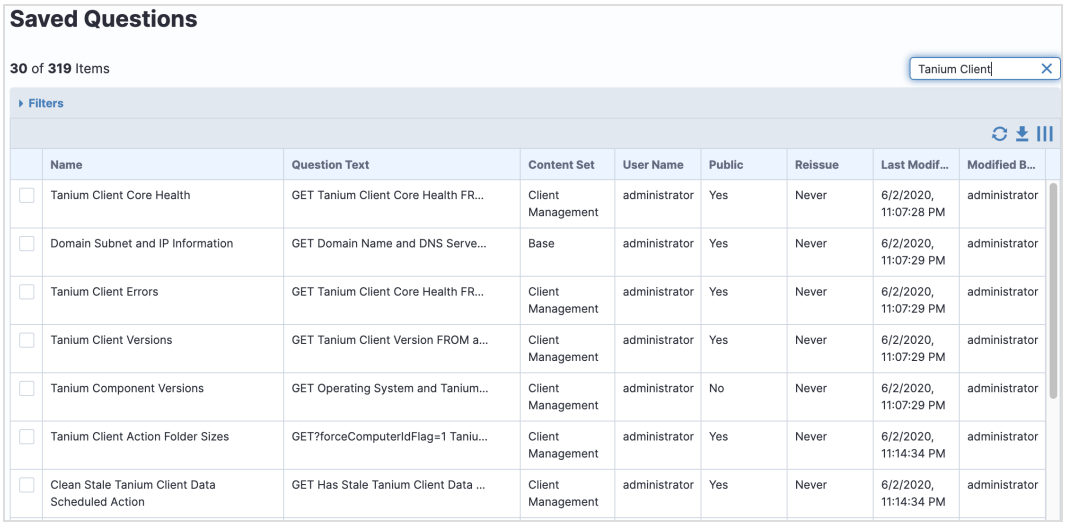
- Go to **Administration > Content > Sensors** and search for client-related sensors.



- Go to **Administration > Content > Packages** and search for client-related packages.



- Go to **Administration > Content > Saved Questions** and search for client-related questions.



Name	Question Text	Content Set	User Name	Public	Reissue	Last Modif...	Modified B...
Tanium Client Core Health	GET Tanium Client Core Health FR...	Client Management	administrator	Yes	Never	6/2/2020, 11:07:28 PM	administrator
Domain Subnet and IP Information	GET Domain Name and DNS Serve...	Base	administrator	Yes	Never	6/2/2020, 11:07:29 PM	administrator
Tanium Client Errors	GET Tanium Client Core Health FR...	Client Management	administrator	Yes	Never	6/2/2020, 11:07:29 PM	administrator
Tanium Client Versions	GET Tanium Client Version FROM a...	Client Management	administrator	Yes	Never	6/2/2020, 11:07:29 PM	administrator
Tanium Component Versions	GET Operating System and Tanium...	Client Management	administrator	No	Never	6/2/2020, 11:07:29 PM	administrator
Tanium Client Action Folder Sizes	GET?forceComputerIdFlag=1 Taniu...	Client Management	administrator	Yes	Never	6/2/2020, 11:14:34 PM	administrator
Clean Stale Tanium Client Data Scheduled Action	GET Has Stale Tanium Client Data ...	Client Management	administrator	Yes	Never	6/2/2020, 11:14:34 PM	administrator

(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 Tanium Console User Guide: 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.
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 tag named `Lab`:

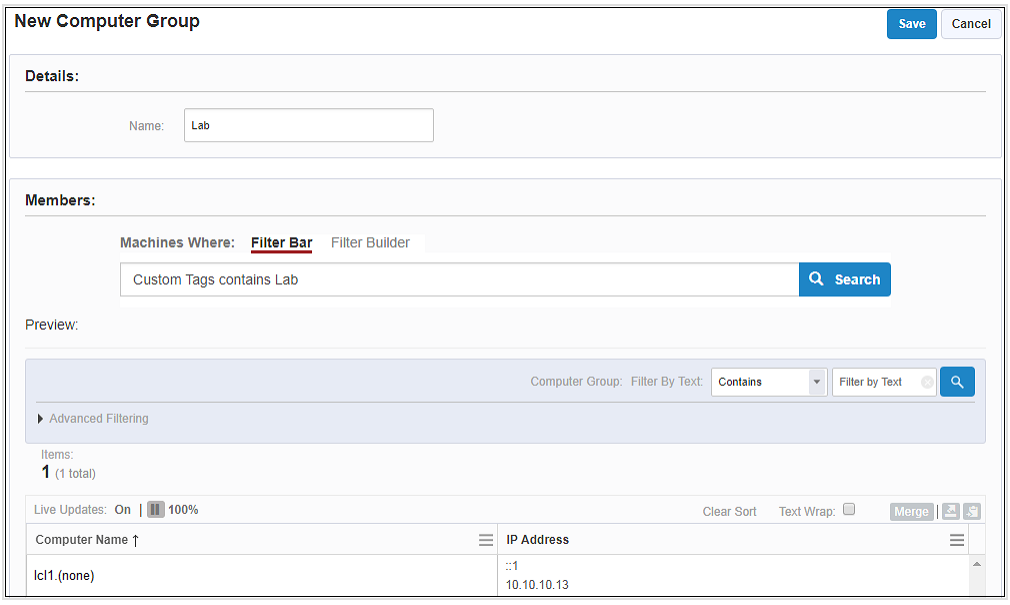
```
[root@centos-7 ~]# cd /opt/Tanium/TaniumClient/Tools
[root@centos-7 Tools]# ls -la
total 8
drwxr-xr-x.  4 root root   62 Jul  9  2020 .
drwx------. 14 root root 4096 Aug  3  2020 ..
drwxr-x---.  2 root root   21 Jul  9  2020 ClientManagement
-rw-r--r--.  1 root root    4 Feb 22 21:45 CustomTags.txt
drwxr-x---.  3 root root   44 Jul  9  2020 CX
[root@centos-7 Tools]# cat CustomTags.txt
Lab
[root@centos-7 Tools]# _
```

Example: Use custom tags to create a computer group

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 Figure 9.

Figure 9: Using custom tags to select a computer group



3. Save your changes.

Manage the Tanium Client on Windows

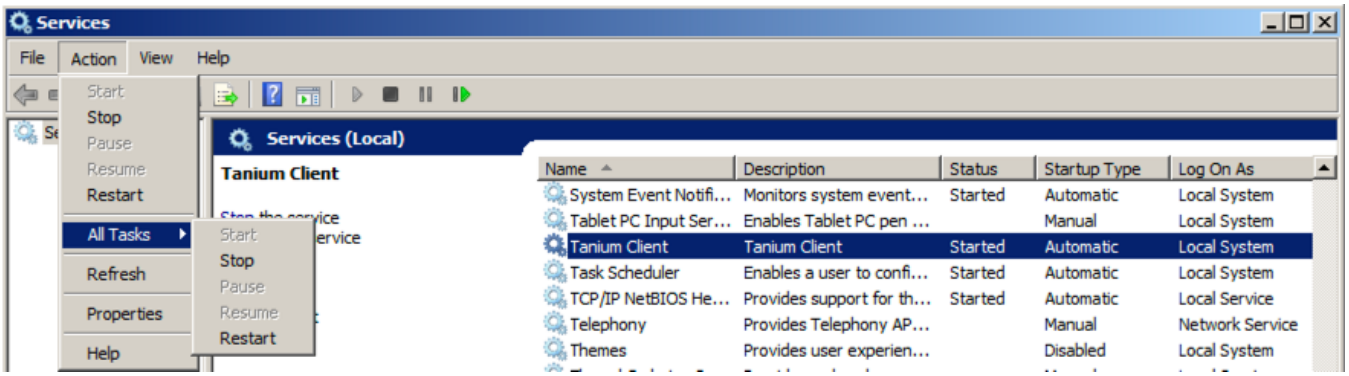
The Tanium Client is installed as a service with a **Startup Type** set to **Automatic** on Windows endpoints. The default installation directory is `C:\Program Files (x86)\` for 64-bit versions of Windows, or `C:\Program Files\` for 32-bit versions of Windows.

Manage the Tanium Client service on Windows

Use the Windows **Services** application to stop, start, or restart the **Tanium Client** service on Windows endpoints:

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 10: Tanium Client service



(Optional) Harden the Tanium Client on Windows

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. You can take additional measures to protect the Tanium Client itself from casual tampering by end users with local administrator rights.

Optional client hardening features are provided by the **Client Service Hardening** content pack and the **StateProtectedFlag** client setting. 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 Tanium Console User Guide: Deploying actions.

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. Regularly auditing and remediating disconnected clients reduces the need to take extra steps to harden the Tanium Client. For more information, see Audit and remediate disconnected Tanium Clients on page 262.

Install the Client Service Hardening content pack

1. Sign in to Tanium Console as a user who is assigned the Administrator reserved role.
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

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**.

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 dashboard question..
2. Select the **Not Restricted** row 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**.

Encrypt the client state and sensor queries stored on the client

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**.

- Alternatively, you can use the command line on an endpoint to configure the **StateProtectedFlag** client setting. See Reference: Tanium Client settings and CLI on page 298.
- You can modify the default value for this setting for endpoints where the setting is not configured. See Modify default client settings in Tanium Console on page 257.
- To disable this encryption, either remove the **StateProtectedFlag** client setting, or set it to `0`.

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**
- **Client Service Hardening - Show Client in Add-Remove Programs**

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

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 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. 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 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`

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.

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).

For details about port and firewall requirements for the Tanium Client, see Network connectivity, ports, and firewalls on page 72.

Table 13: 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 Preferences** 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 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 Preferences**. However, only endpoints running macOS 10.14.4 or later support this method.

CONFIGURE AN MDM POLICY OR PROFILE FOR MULTIPLE ENDPOINTS

When you configure a firewall rule or **System Preferences** through a policy or profile, the specific steps depend on your UAMDM. Contact Tanium Support 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.

CONFIGURE A FIREWALL RULE ON A SINGLE ENDPOINT

You require read-only access to the `/Library/Tanium/TaniumClient` directory to perform this task.

1. Go to **System Preferences > Security & Privacy**.
2. Click Unlock, enter administrator credentials, and click **Unlock**.
3. Add a firewall rule: Click **Firewall 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 PREFERENCES ON A SINGLE ENDPOINT

All endpoints that run macOS 10.14.x or later support configuring System Preferences to prevent the connections pop-up.

1. Go to **System Preferences > Security & Privacy**.
2. Click Unlock, enter administrator credentials, and click **Unlock**.
3. Click **Firewall 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`.

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 and outbound TCP traffic on the ports that the client uses for Tanium traffic (default 17472).

> NOTE
>
> For details about port and firewall requirements for the Tanium Client, see Network connectivity, ports, and firewalls on page 72.

The following subsections list example commands for managing Linux firewalls based on default distributions of Linux.

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. To add, remove, deny, or view the status of ports that the Tanium Client uses, check your Amazon Web Services (AWS) security group instead.

CentOS, AlmaLinux, Rocky Linux, Oracle Linux, Red Hat Linux

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.

Table 14: Firewall commands for CentOS, Oracle Linux, Red Hat Linux 5.x and 6.x

Tasks	Commands
Check the firewall status	`iptables -L -n --line-numbers | egrep -i "^Chain|REJECT *all"` 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`

VERSION 7.X AND 8.X

The following table lists the commands for managing firewall rules for versions 7.x and 8.x of CentOS, Oracle Linux, or Red Hat Linux, or version 8.x of AlmaLinux or Rocky Linux:

Table 15: Firewall commands for CentOS, Oracle Linux, or Red Hat Linux 7.x or 8.x; AlmaLinux or Rocky Linux 8.x

Tasks	Commands
View rules for port 17472	`sudo firewall-cmd --list-all-zones | grep 17472`

Table 15: Firewall commands for CentOS, Oracle Linux, or Red Hat Linux 7.x or 8.x; AlmaLinux or Rocky Linux 8.x (continued)

Tasks	Commands

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`

OpenSUSE and SLES

VERSION 15.X

The following table lists the commands for managing firewall rules for versions 15.x of OpenSUSE and SUSE Linux Enterprise Server (SLES):

Table 16: 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):

Table 17: 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 17472	1. Open the `/etc/sysconfig/SuSEfirewall2` file for editing, add port 17472 to the line `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 10.04, 14.04, 16.04, and 18.04 LTS:

Table 18: 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.

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

The Tanium Client must store data in the default installation directory. 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 247.
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
   ```

   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 247.

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.

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`
- Display the status of the Tanium Client service: `svcs taniumclient`

Move an existing installation of the Tanium Client on Solaris

The Tanium Client must store data in the default installation directory. 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
   ```

   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`.

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

The Tanium Client must store data in the default installation directory. 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
   ```

   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 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 254 to configure client settings.

For the list of client settings that you can review or configure, see Tanium Client settings reference on page 298.

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 257), or if no value is configured in Tanium Console, the default that is listed in the Tanium Client settings reference 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.

SUMMARY VIEW

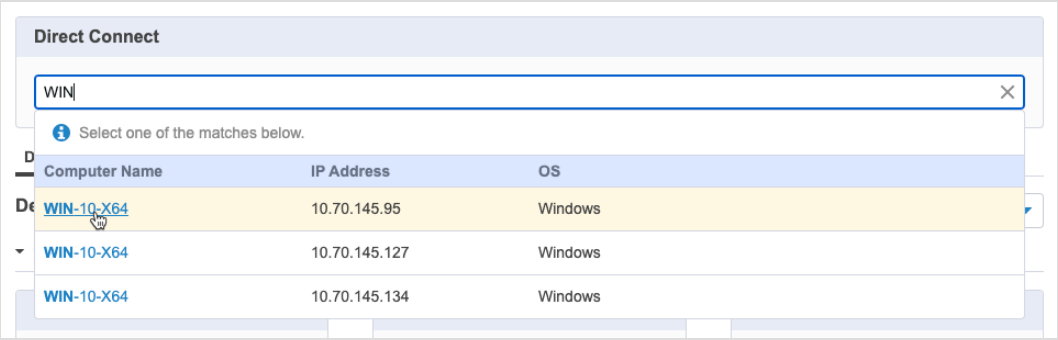
Use the main Client Health view to review a summary of client settings that have been changed from their defaults on some endpoints and the count of endpoints on which each setting has been changed.

1. From the Main menu, go to **Administration > Shared Services > Client Management**.
2. From the **Client Management** menu, go to **Client Health**.
3. Click the **Settings** tab.
4. (Optional) Select a **Computer Group** to filter the summary information.

DETAIL VIEW

Connect directly to an endpoint to view each client setting that has been configured for that endpoint.

1. In the **Direct Connect** 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 to connect to the endpoint.



3. Click the **Configuration** tab to view client settings for the endpoint.
4. When you finish reviewing client health information for the endpoint, click **Disconnect** to disconnect from the endpoint and return to the client health summary.

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
```

For more information about working with question results, see Tanium Interact User Guide: 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 313.

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 298.

Settings configurations in Client Management

For certain client settings (including all VDI-related settings, and the specific settings noted in the Tanium Client settings (continued) on page 310), 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 profiles, see Managing client settings and Index configurations in Client Management on page 257.

Packages

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.

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**.

   You can drill-down or merge questions to refine the results before selecting endpoints. For more information, see Tanium Interact User Guide: 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 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 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.
   - For **ValueData**, enter the value to configure for the setting on targeted endpoints.

   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.

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**.

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 237
   - Manage the Tanium Client service on macOS on page 242
   - Manage the Tanium Client service on Linux on page 247
   - Manage the Tanium Client service on Solaris on page 250
   - Manage the Tanium Client service on AIX on page 252
9. Review the setting on the targeted clients to verify that it has been correctly updated. See Review client settings on page 253.

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 313.

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 105.

Modify default client settings in Tanium Console

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 (continued) on page 310. 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 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 (continued) on page 310.
        - 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 and Index configurations in Client Management

Use the Client Management service to manage client settings and Index configurations to different groups of clients.

Create and deploy a client settings configuration

Create a settings configuration to configure general client settings for a group of clients.

1. From the Client Management menu, click **Configuration Management > Settings Configurations**, and click **Create Settings Configuration**.

    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.

2. Enter a **Name** for the profile configuration.

3. Click **Select Computer Groups**, select the computer groups where you want the settings configuration to apply, and click **Save**.

4. Configure the following general client settings.

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 24.
Logging Level	The level of logging on an endpoint. The following values are best practices for specific use cases: • `0`: Use this value to disable logging; use for clients installed on sensitive endpoints or virtual desktop infrastructure (VDI) endpoints. • `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.
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 use cases: • `0`: Use this value to disable logging; use for clients installed on sensitive endpoints or virtual desktop infrastructure (VDI) endpoints. • `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.

5. 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 310.

Client Setting	Default Value	Best Practice Value for VDI	Explanation
RandomSensorDelayInSeconds	0	20	By default, sensors run immediately. This setting delays the execution of any sensor by a random time up to 20 seconds, which reduces concurrent execution of sensors and packages.

Client Setting	Default Value	Best Practice Value for VDI	Explanation
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.

6. Click **Save**.
7. To deploy the settings configuration to the selected computer groups, click Actions in the row for the configuration, and select **Deploy**.

Create and deploy an Index configuration

Create an Index configuration to configure Index exclusions 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 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.

CREATE INDEX EXCLUSIONS

First, create a set of Index exclusions that can be reused across multiple Index configurations.

1. From the Client Management menu, click **Configuration Management > Index Exclusions**, and click **Create Index Exclusion**.
2. Enter a **Name** for the exclusion.
3. Select the **Operating System** where the exclusion applies.
4. 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:
   `\\(pagefile|swapfile|hiberfil)\.sys`

   Do not include a trailing slash in folder or directory exclusions. Index exclusions that end with trailing slashes indicate that all files in the directory are indexed, but Index does not add them to the Index database. Including a trailing slash in folder or directory exclusions can unnecessarily increase resource use on the endpoints.
5. Click **Save**.

CREATE AN INDEX CONFIGURATION

1. From the Client Management menu, click **Configuration Management > Settings Configurations**, and click **Create Index Configuration**.

   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.
2. Enter a **Name** for the profile configuration.
3. Click **Select Computer Groups**, select the computer groups where you want the settings configuration to apply, and click **Save**.
4. 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:
    - (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.

5. Click **Select Exclusions**, select the Index 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 configurations

The order of the configurations in each 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 Client Management menu, click **Configuration Management > Settings Configurations** or **Configuration Management > Index Configurations**, and click **Prioritize**.
2. 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 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. See Troubleshooting Tanium Clients and Client Management on page 277 for related procedures.

For information about general management of Tanium Clients, see Managing Tanium Clients on page 233.

Configure automated maintenance

Audit and remediate disconnected Tanium Clients

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 Tanium Discover User Guide: 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 Tanium Discover User Guide: 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 Tanium Discover User Guide: Export interface data to a Connect destination.
4. Configure a recurring deployment in Client Managementthat targets the Discover label you created. See Deploying the Tanium Client using Client Management on page 105.

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 278.

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 (Optional) Harden the Tanium Client on Windows on page 237. 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

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 details about leaders, linear chains, and how the servers evaluate subnet boundaries, see Client peering on page 20.

1. Configure the TPAN report if it is not already configured. See Tanium Health Check User Guide: Configuring Health Check.
2. Open the latest TPAN report and select the **Tuning** page.
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 263 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. See Configure isolated subnets on page 208.
5. Contact Tanium Support on page 297 for help optimizing the leader count, if necessary.

Check the endpoint count

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 to ensure compliance with your Tanium license:

- 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 details, see Tanium Console User Guide: View environment status.

  If the endpoint count is lower than expected, investigate whether network disruptions or misconfigurations prevent endpoints from registering. If the count is higher than expected, verify that the new endpoints are authorized to join your network.

  You can configure an automatic Discover label and a Connect destination to alert you when endpoints become unmanaged. See Audit and remediate disconnected Tanium Clients on page 262.

- Go to **Administration > Configuration > Client Status** to check the endpoint count as it relates to your Tanium license, regardless of whether it matches the **Total Endpoints** value on the Tanium **Home** page. For details, see Tanium Console User Guide: View managed endpoints count for license compliance.

  Track changes in the weekly endpoint count to project future growth. Contact Tanium Support on page 297 to update your license for a higher number of maximum managed endpoints if necessary.

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 the steps to review and update 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. See Tanium Console User Guide: Review custom tags.
2. Add or remove custom tags if necessary. See Tanium Console User Guide: Manage custom tags for computer groups.
3. Create or delete computer groups with tag-based membership if necessary. See Tanium Console User Guide: Managing computer groups.

   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. See Tanium Console User Guide: Managing action groups.

Perform monthly maintenance

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 277.

Review and remediate Tanium Client health and client extension issues

1. From the Main menu, go to **Administration > Shared Services > Client Management**.
2. From the Client Management menu, select **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. See Tanium Console User Guide: Managing question results.
5. To resolve client extension failures, see the following sections:
    - To resolve Client Index Extension failures, see Tanium Client Index Extension User Guide: Reference: Common health check issues.
    - To resolve Client Recorder Extension failures, see Tanium Client Recorder Extension User Guide: Troubleshooting the Client Recorder Extension.
    - To resolve failures associated with client extensions for other Tanium solutions, see Tanium Console User Guide: Troubleshoot solution-specific issues and Tanium Endpoint Configuration User Guide: Identify and resolve issues with endpoint tools or client extensions.

Review and adjust the distribution of Tanium Client registration traffic

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 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.

For details about client-server connections, see Configuring connections to the Tanium Core Platform on page 188.

To determine which servers are processing client registrations and, if necessary, to rebalance registration traffic among them:

1. From the Main menu, go to **Administration > Shared Services > Client Management**.
2. From the Client Management menu, select **Client Health** and click the **Settings** tab.
3. Scroll to 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. See Content for configuring connections to Tanium Core Platform servers on page 190.
6. Add Zone Servers if necessary to rebalance client registration traffic and then repeat step 5 to connect clients to those servers. See the procedure for your Tanium infrastructure:
   - Tanium Appliance User Guide: Installing an Appliance Array: See the tasks for adding array members and assigning roles.
   - Tanium Core Platform User Guide for Windows Deployments: Installing the Tanium Zone Server

Review and update Tanium Client logging levels

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 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

Set the logging level to `0` (logging disabled) for clients that run on sensitive endpoints, endpoints with limited resources, or virtual desktop infrastructure (VDI) endpoints.

NOTE

For details 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 297 to change the logging level on Client Containers.

For details about logs on Tanium Clients, see Troubleshooting Tanium Clients and Client Management on page 277.

1. From the **Client Management** menu, 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 `0` for clients on VDI endpoints, select **All Virtual Machines** in the **Computer Group** drop-down.

2. To update the logging level on clients, see Managing client settings and Index configurations in Client Management on page 257.

Review and update Tanium Client settings

1. From the **Client Management** menu, go to **Client Health** and click the **Settings** tab.
2. Verify that the setting values are correct and that the **Count** column indicates they apply to the expected number of clients.
3. To update settings, see Managing client settings and Index configurations in Client Management on page 257.

Review and upgrade Tanium Client versions

The best practice is to run the latest Tanium Client version on all endpoints. However, in certain cases, temporarily running earlier client versions might be acceptable for some endpoints. For example, if you are rolling out client upgrades in phases, one group of endpoints at a time, you might want to finish testing the upgrade for the first phase before upgrading more endpoints in the next phase. Endpoints might also run an earlier client version if the upgrade process failed.

For details about client versions, see Client version and operating system requirements on page 26.

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 **Administration > Client Management**.
2. Scroll to 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.
   For example, select a **Filter by Computer Group** option (such as **All Windows**) or issue a drill-down question. For the steps to retrieve additional details, see Tanium Console User Guide: Managing question results.
5. Upgrade the client on any endpoints that require the latest version. See Upgrading Tanium Clients on page 269.
6. Troubleshoot client upgrade issues if necessary. See Troubleshooting Tanium Clients and Client Management on page 277.

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).

For details about client peering and subnets, see Configuring Tanium Client peering on page 202.

REVIEW AND UPDATE ISOLATED SUBNETS

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 client-to-server connections.

1. 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. See Configure isolated subnets on page 208.

REVIEW AND UPDATE SEPARATED SUBNETS

Configure separated subnet configurations to apply more granular subnet boundaries for Tanium linear chains than the default boundaries.

1. 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. See Configure separated subnets on page 206.

REVIEW AND UPDATE INTENTIONAL SUBNETS

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 on page 205 setting. See AddressMask on page 205.
   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**.
4. 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. See Configure intentional subnets on page 211.

Upgrading Tanium Clients

The following procedures describe how to upgrade the Tanium Client to a newer version on managed endpoints.

Best practices

Review the following best practices before upgrading Tanium Clients:

- When possible, upgrade using Client Management as described in Upgrade Tanium Clients using Client Management on page 270, instead of using third-party software. In cases where third-party software is preferable or necessary, refer to 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.
    - Consider organizing computer groups to help manage upgrade stages. See Tanium Console User Guide: Create a computer group.
- Tanium recommends replacing the x86-64 binary with the universal binary on all Mac computers running macOS 11 or later. 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 or perform a reinstallation that includes wiping data with Tanium Client Management. If you upgrade the x86-64 client in Client Management, it installs a newer version of the x86-64 client.

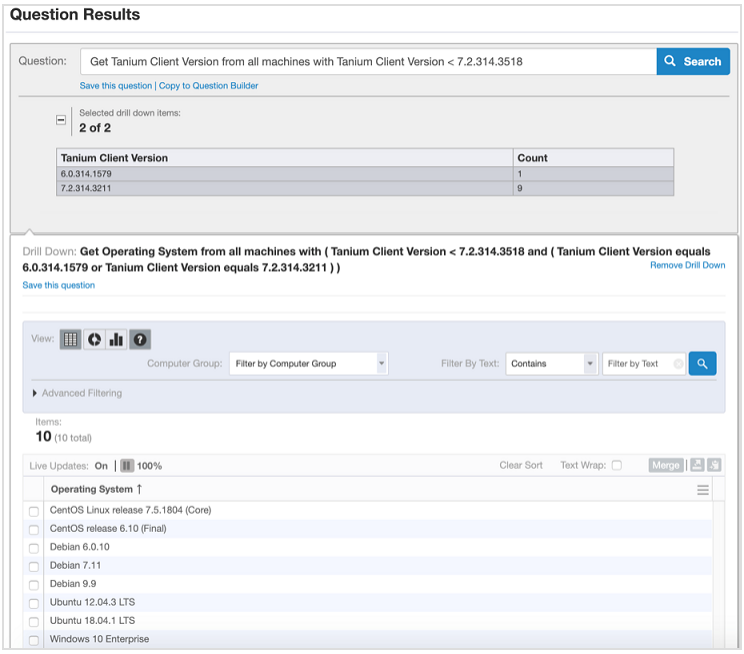
Before you begin

- 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.
- 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 241.
- **macOS:** If you previously created a Privacy Preferences Policy Control (PPPC) custom payload for a version of the Tanium Client earlier than 7.2.314.3608 and you are upgrading to version 7.2.314.3608 or later, 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 107 (for deployment with Client Management) or Deploy the Tanium Client to macOS endpoints using the installer on page 145.

Assess the impact of upgrading on your environment

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 Tanium Console User Guide: Drill down into results).



Upgrade Tanium Clients using Client Management

Use client upgrades in Client Management to upgrade 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. Create a one-time upgrade to upgrade clients within a specified window of time. 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.

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 Tanium Console User Guide: Managing action locks.

Create a client upgrade

IMPORTANT

Before you create an upgrade, make sure that the Tanium Server has cached the versions of the Tanium Client that you need. See Manage versions of the Tanium Client available for deployments and upgrades on page 99.

1. From the Client Management menu, click **Client Upgrades**.
2. Click **Create Client Upgrade**.
3. Enter a **Name** for the client upgrade.
4. (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.
5. In the **Endpoints to target** section, click **Computer Groups**, and select the computer groups to be upgraded.
6. 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.

  Distribute the upgrade over time to prevent upgrades from occurring on all the targeted endpoints simultaneously.

7. Click **Preview to Continue** and review the **Version status of targeted endpoints**.
8. Click **Deploy** to create the upgrade. The action for the client upgrade is issued at the **Start Time** you configured.

   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 105.

Upgrade Tanium Clients using a package

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 Tanium Console User Guide: 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 < 7.4.7.1179 )`
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**.

Uninstalling Tanium Clients

Uninstall the Tanium Client on Windows

You can use various tools to uninstall the Tanium Client.

Use a Tanium package to deploy an uninstallation program

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.

1. Access Tanium Console.
2. From the Main menu, go to **Administration > Configuration > Settings**.
3. In the **Packages** section, set **Run Commands in Process Group** to **ON**, and click **Save All**.
4. 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**.
5. Create a scheduled action to distribute the package to targeted computers. See Tanium Console User Guide: Deploying actions.

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.

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 Tanium Console User Guide: 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

Uninstall without using a script

1. On the macOS endpoint, open **Terminal**.
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.

   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
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`

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`

Uninstall the Tanium Client on AIX

To uninstall the Tanium Client on AIX, run the following command: `installp -u TaniumClient`

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. See Monitor the client health overview in Client Management on page 225 and Access detailed client health and troubleshooting information on an endpoint on page 228.
- **Version**: Contact Tanium Support to verify that the Tanium Client version is a recommended version.
- **Requirements**: Ensure your environment meets the host system and network requirements. See Tanium Client and Client Management requirements on page 26.
- **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. See Troubleshoot Client Management on page 294).
    - Examine the Tanium Client installation log on the endpoints.
    - Make sure the endpoint has enough available space on the disk or partition where you are installing the client. See Hardware requirements on page 63. If you are using Client Management for deployment, see Deploying the Tanium Client using Client Management on page 105 for information about setting the installation directory and the space required on endpoints to proceed with deployment.
- **Connection and registration**: See Troubleshoot issues with connection and registration on page 278.
- **Client settings:** See Managing client settings and Index configurations on page 253 and Tanium Client settings reference on page 298.
- **Actions**: For issues that occur when deploying actions, see Review action logs and associated files to troubleshoot actions and packages on page 282 and Review action history logs to troubleshoot or audit actions on page 284.
- **Sensors**: For issues related to sensors, see Review sensor history logs to troubleshoot or audit sensor activity on page 285 and Review and manage sensor quarantines to troubleshoot sensors on page 288.
- **Tanium Client service**: See Verify that the Tanium Client service and process are running on an endpoint on page 279.

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 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, and check the following items.

Check the client status

1. From the Main menu, go to **Administration > Configuration > Client StatusAdministration > Management > 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 214.
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.pub` or `tanium-init.dat`) for the client:
   - **Tanium Client 7.2:** Make sure that the `tanium.pub` file is located in the Tanium Client installation directory and that its hash matches that of the `tanium.pub` file on the Tanium Server. For the steps to download the `tanium.pub` file from the Tanium Server, see Tanium Console User Guide: Download infrastructure configuration files (keys). Use one of the following commands to determine the MD5 hash of each `tanium.pub` file:
     - **Windows:** `CertUtil -hashfile <path_to_file>\tanium.pub`
     - **macOS:** `md5 <path_to_file>/tanium.pub`
     - **Linux:** `md5sum <path_to_file>/tanium.pub`
     - **Solaris:** `digest -a md5 -v <path_to_file>/tanium.pub`
     - **AIX:** `csum -h MD5 <path_to_file>/tanium.pub`
   - **Tanium Client 7.4:** See Review or reset the public key to troubleshoot connection issues (Tanium Client 7.4 only) on page 286.
4. If the endpoint is not currently reporting and the client appears to have a valid key, proceed to the next troubleshooting task.

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 237
- Manage the Tanium Client service on macOS on page 242
- Manage the Tanium Client service on Linux on page 247
- Manage the Tanium Client service on Solaris on page 250
- Manage the Tanium Client service on AIX on page 252

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 does not exist, reinstall the Tanium Client. For more information, see Deploying the Tanium Client using Client Management on page 105 and Deploying the Tanium Client using an installer or package file on page 134.

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 77.

Verify server connection settings

For server connection issues, use the following commands to review and verify the server connection settings for the client.

Setting	OS	
Tanium Server and Zone Server FQDNs or IP addresses	Windows	`TaniumClient config get ServerNameList`
	Non-Windows	`sudo ./TaniumClient config get ServerNameList`
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`

If any settings are incorrect, or for more information about server connections, see Configuring connections to the Tanium Core Platform on page 188.

For peer connection issues, see Configuring Tanium Client peering on page 202.

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 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 you 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

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, click **Administration > 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.
4. From the search results, click the computer name to connect to the endpoint.

5. Click the **Gather** tab. In the **Domain** section, and select the domain and category name for which you want to gather troubleshooting information. You can optionally filter the category list by domain.

6. 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.
7. 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 connecting directly to endpoints, see Tanium Direct Connect User Guide.

For more information about using client health features in Client Management, see Managing Tanium Clients on page 233 and Managing Tanium Clients on page 233.

Access individual endpoint logs in Client Management

You can use Client Management to directly connect to an endpoint and view and download individual logs.

1. From the Main menu, click **Administration > 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.
4. From the search results, click the computer name to connect to the endpoint.
5. Click the **Logs** tab, and select a log to view.
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 LogVerbosityLevel1 on page 302). The location for log files is also configurable (see LogPath on page 302). The default is <*Tanium Client installation directory*>/Logs.

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 281.

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 278.

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 63.

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 248.

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*>/Downloads directory. The Tanium Client removes action logs from its host after a configurable interval (see Action log and package cleanup on page 284).

TIP

Tanium Console displays the **Action ID** in the **Action > Action History** and **Action Status** pages (see Tanium Console User Guide: Deploying actions). The **Action Status** page provides options for accessing action log information from multiple endpoints. See Tanium Console User Guide: View action status.

Action history logs 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 284).

Access action logs in Client Management

You can use Client Management to directly connect to an endpoint and view and download individual logs.

1. From the Main menu, click **Administration > 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.
4. From the search results, click the computer name to connect to the endpoint.
5. Click the **Actions** tab, and select a previously run action for which you want to view the log.
6. (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
  ```

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 (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 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 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-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*>/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 281.

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-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*>/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 281.

Review or reset the public key to troubleshoot connection issues (Tanium Client 7.4 only)

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.
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 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 Tanium Console User Guide: Managing Tanium keys.

```
[root@myendpoint TaniumClient]# ./TaniumClient pki show
taniumserver1.mydomain.com Root 0
  perms has:
  perms grant: All, Server TLS, ZoneServer TLS, Client TLS, Message Signing, Hub TLS
  valid from: 2020-05-19 14:25:35 +0000
  valid to: 2021-05-20 20:14:47 +0000
  status: trusted
  fingerprint: xx:xx:xx:xx:xx:xx

    taniumserver1.mydomain.com Message Signing 2
      perms has: Message Signing
      perms grant:
      valid from: 2021-05-14 06:26:27 +0000
      valid to: 2021-11-11 06:26:27 +0000
      status: trusted
      fingerprint: xx:xx:xx:xx:xx:xx

taniumserver2.mydomain.com Root 0
  perms has:
  perms grant: All, Server TLS, ZoneServer TLS, Client TLS, Message Signing, Hub TLS
  valid from: 2020-05-19 14:25:38 +0000
  valid to: 2021-05-20 20:14:50 +0000
  status: trusted
  fingerprint: xx:xx:xx:xx:xx:xx

    zoneserver2.mydomain.com
      perms has:
      perms grant: Client TLS
      valid from: 2021-06-06 01:26:39 +0000
      valid to: 2021-12-04 01:26:39 +0000
      status: trusted
      fingerprint: xx:xx:xx:xx:xx:xx

        localhost
          perms has: Client TLS
          perms grant:
          valid from: 2021-06-24 18:53:14 +0000
          valid to: 2021-07-02 18:53:14 +0000
          status: owned
          fingerprint: xx:xx:xx:xx:xx:xx

    taniumserver2.mydomain.com Message Signing 2
      perms has: Message Signing
      perms grant:
      valid from: 2021-05-14 06:26:51 +0000
      valid to: 2021-11-11 06:26:51 +0000
      status: trusted
      fingerprint: xx:xx:xx:xx:xx:xx
```

3. (Optional) Reset the key with a new `tanium-init.dat` file.

    a. From the Main menu in Tanium Console, go to **Administration > Configuration > Tanium Server > Infrastructure Configuration Files**.

    b. In the **Clients v7.4+ and Zone Server** section, 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`

    f. Restart the Tanium Client service on the endpoint.

For the procedures to stop and restart the Tanium Client service, see the following sections:

- Manage the Tanium Client service on Windows on page 237
- Manage the Tanium Client service on macOS on page 242
- Manage the Tanium Client service on Linux on page 247
- Manage the Tanium Client service on Solaris on page 250
- Manage the Tanium Client service on AIX on page 252

Be careful not to allow the `tanium-init.dat` or `tanium.pub` 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 these files do not contain private keys and cannot be used to provide control over a Tanium environment, a user with malicious intent could use them 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

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 one minute.

By default, quarantines are not enforced: after a sensor exceeds the timeout and stops running, the sensor has quarantined status but still runs for future questions or actions until it completes or times out. In this case, the Tanium Client uses the quarantined status just to record that the sensor timed out.

Regardless of whether you enable enforcement, the Tanium Client stops any sensor at the moment it exceeds the timeout. Each client quarantines sensors and enforces the quarantines independently. Consequently, a sensor might be quarantined on some endpoints and not on others.

When a Tanium Client quarantines a sensor, Tanium Console displays the following message in the **Question Results** grid: `TSE-Error: Sensor evaluation timed out`. 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.

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

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 Tanium Console User Guide: 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.
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

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 Tanium Console User Guide: 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.
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

To remove a sensor from quarantine through Tanium Console, see Tanium Console User Guide: 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>`

If you modify a sensor, Tanium Clients that receive its new definition automatically remove that sensor from quarantine.

Add a sensor to quarantine

You can manually quarantine a sensor on an endpoint if you anticipate that running the sensor will negatively affect the endpoint.

Quarantining a sensor does not automatically enable quarantine enforcement.

1. In the URL field of the browser that you use to access Tanium Console, enter `https://<Tanium Server>/hash/<sensor>`. For the *<Tanium Server>*, enter the Tanium Server FQDN or IP address. The *<sensor>* must match the sensor name that Tanium Console displays with respect to capitalization and spaces.
   The browser displays the hash value associated with the sensor.
2. Access the operating system CLI on the endpoint and change directory (**cd**) to the Tanium Client installation directory.
3. Enter the following command.
   - **Windows:** `TaniumClient quarantine add <sensor_hash>`
   - **Non-Windows:** `./TaniumClient quarantine add <sensor_hash>`

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.

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.

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 setting in the local configuration of those clients.

Identify and resolve issues with client extensions

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.

To review the client extensions that Client Management installs and uses, see Client extensions.

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. See Endpoint Configuration User Guide: 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` or `Client Management - Tools Version` 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.

   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. See Remove Client Management tools from endpoints and Endpoint Configuration User Guide: Uninstall a tool installed by Endpoint Configuration.

   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 Client Management from all machines with Endpoint Configuration - Tools Status:Tool Name contains Client Management`

   Review the columns in the results for specific information about errors. The following table provides guidance for some common error conditions:

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. See Remove Client Management tools from endpoints. ◦ 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 Dependencies: [Tool name]`	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 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 Endpoint Configuration User Guide: 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. See Endpoint Configuration User Guide: 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`. See Review the Extensions log for an endpoint on page 294.

For additional help, collect all logs for Tanium Client Management, and contact Tanium Support.

Review the Extensions log for an endpoint

Use Client Management to directly connect to an endpoint and view and download extension logs.

1. From the Main menu, go to **Administration > 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.
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**.

For additional help, collect all logs for Tanium Client Management, and contact Tanium Support.

Troubleshoot Client Management

To send information to Tanium for troubleshooting, collect logs and other relevant information.

Collect logs

You can save Client Management logs as a ZIP file that you can download with your browser.

1. From the Client Management **Overview** page, click Help  .
2. In the **Collect Information for Support Requests** section, click **Collect**.
3. After the package is created, click **Download**.
   A `tanium-client-management-support.zip` file downloads to the local download directory.
4. Attach the ZIP file to your Tanium Support case form or contact Tanium Support.

View and configure logs

On Windows infrastructure, Tanium Client Management records service logs in the `client-management.log` file in the `\Program Files\Tanium\Tanium Module Server\services\client-management-files` directory on the Module Server.

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

To troubleshoot deployment issues in Client Management, you can view the installation log for each endpoint in a deployment.

1. From the Client Management menu, click **Client Installations > Client Deployments**, and then click the name of the deployment you want to view.
2. 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.
3. In the row for an endpoint you want to investigate, click Endpoint Details  to view the installation log.
4. To further troubleshoot, increase the verbosity of the installation log. Enable the Verbose Logging setting, and then reissue the deployment.

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.
  ```

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. See Manage endpoint credentials on page 132.
- 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_addressport_number`
    - In an appliance deployment, check TanOS network status. See Tanium Appliance Deployment Guide: 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.

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. See Deploying the Tanium Client using Client Management on page 105 and Deploying the Tanium Client using Client Management on page 105.
- 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. See Manage endpoint credentials on page 132.
- Check the password provided with the credentials to make sure it is not disabled or expired.

Uninstall Client Management

Uninstalling versions of Client Management between 1.5 and 1.12 also uninstalls Endpoint Configuration and affects all Tanium solutions. Contact Tanium support before you 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.

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
```

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. See Security exclusions for Client Management on page 78.
- 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.

Contact Tanium Support

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 uses a non-default installation directory for the Tanium Client.

To contact Tanium Support for help, sign in to https://community.tanium.com/s/contactsupport.

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 253.

Table 19: 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 24.	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
DatabaseEpoch	All supported	REG_SZ	STRING	Typically, this setting indicates the date and time when the Tanium Server was deployed.	No

Table 19: Tanium Client settings (continued)

Setting Name	Applies to OS Platforms	Windows Registry Value Type	Non-Windows Setting Type	Description	Modify
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 details and best practices, see Customize listening ports on page 221.  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.	As necessary

Table 19: Tanium Client settings (continued)

Setting Name	Applies to OS Platforms	Windows Registry Value Type	Non-Windows Setting Type	Description	Modify
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 details, see Enable or disable enforcement of quarantined sensors on page 291.	As necessary
FirstInstall	All supported	REG_SZ	STRING	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. Specify just the domain portion of the fully qualified domain name (FQDN). For example, if the FQDN is `host.example.com`, specify `example.com`.	As necessary
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	All supported	REG_SZ	STRING	Date and time of latest Tanium Client installation.	No

Table 19: Tanium Client settings (continued)

Setting Name	Applies to OS Platforms	Windows Registry Value Type	Non-Windows Setting Type	Description	Modify
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. TIP To avoid this fallback behavior during testing, troubleshooting, or migration scenarios, delete the **LastGoodServerName** value.	No
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 setting for communication between clients. For details and best practices, see Customize listening ports on page 221.	As necessary
LogFileSize	All supported	REG_ DWORD	NUMERIC	The size threshold in bytes that Tanium Client logs must reach before the client rotates them.	As necessary

Table 19: Tanium Client settings (continued)

Setting Name	Applies to OS Platforms	Windows Registry Value Type	Non-Windows Setting Type	Description	Modify
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 practices for specific use cases: • `0`: Use this value to disable logging; use for clients installed on sensitive endpoints or virtual desktop infrastructure (VDI) endpoints. • `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: By default, this setting is not present if you did not set the logging level when deploying the Tanium Client. TIP: 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.	As necessary

Table 19: Tanium Client settings (continued)

Setting Name	Applies to OS Platforms	Windows Registry Value Type	Non-Windows Setting Type	Description	Modify
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 use cases: • `0`: Use this value to disable logging; use for clients installed on sensitive endpoints or virtual desktop infrastructure (VDI) endpoints. • `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.	

Table 19: Tanium Client settings (continued)

Setting Name	Applies to OS Platforms	Windows Registry Value Type	Non-Windows Setting Type	Description	Modify
Path	Windows	REG_SZ	N/A	Path to the Tanium Client installation directory. If none is specified, the Tanium Client assumes the default path for the OS. 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 248 • Move an existing installation of the Tanium Client on Solaris on page 250 • Move an existing installation of the Tanium Client on AIX on page 252	As necessary
PeerNeighborhood	All Supported	REG_SZ	STRING	A neighborhood name that designates clients that should be allowed to peer regardless of NAT IP. For details, see Configure intentional subnets on page 211.	

Table 19: Tanium Client settings (continued)

Setting Name	Applies to OS Platforms	Windows Registry Value Type	Non-Windows Setting Type	Description	Modify
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 details, see Configure proxy connections with a PAC file on page 197.	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 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 details, see Configure proxy connections without a PAC file on page 199.	As necessary

Table 19: Tanium Client settings (continued)

Setting Name	Applies to OS Platforms	Windows Registry Value Type	Non-Windows Setting Type	Description	Modify
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 details and best practices, see Customize listening ports on page 221.	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 details and best practices, see Customize listening ports on page 221.	As necessary
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 details and best practices, see Customize listening ports on page 221.	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 details and best practices, see Customize listening ports on page 221.	As necessary

Table 19: Tanium Client settings (continued)

Setting Name	Applies to OS Platforms	Windows Registry Value Type	Non-Windows Setting Type	Description	Modify
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 details, see Information about registration and ComputerID (all operating systems) on page 167.	No
ReportingTLSMode, OptionalTLSMinAttemptCount, OptionalTLSBackoffIntervalSeconds, OptionalTLSMaxBackoffSeconds, Server_ReportingTLSMode, Server_ OptionalTLSMinAttemptCount, Server_ OptionalTLSBackoffIntervalSeconds, Server_ OptionalTLSMaxBackoffSeconds	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 7.4 peers. For details, see the Tanium Appliance User Guide: Securing Tanium Server, Zone Server, and Tanium Client access or Tanium Core Platform User Guide for Windows Deployments: Securing Tanium Server, Zone Server, and Tanium Client access.	As necessary
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

Table 19: Tanium Client settings (continued)

Setting Name	Applies to OS Platforms	Windows Registry Value Type	Non-Windows Setting Type	Description	Modify
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 details, see ServerName on page 189. 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 details, see ServerNameList on page 188. 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.	As necessary

Table 19: Tanium Client settings (continued)

Setting Name	Applies to OS Platforms	Windows Registry Value Type	Non-Windows Setting Type	Description	Modify
ServerPort	All supported	REG_ DWORD	NUMERIC	The port to use for client-server and, by default, client-client communication. The default is 17472. For details, see ServerPort. NOTE If you configure the ListenPort or EnableRandomListeningPort setting, it overrides **ServerPort** for client-client communication. For more information, see Customize listening ports on page 221.	As necessary
StateProtectedFlag	All supported	REG_ DWORD	NUMERIC	Enables encryption of the client state and sensor queries stored on the client 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 (Optional) Harden the Tanium Client on Windows on page 237.	As necessary

Table 19: Tanium Client settings (continued)

Setting Name	Applies to OS Platforms	Windows Registry Value Type	Non-Windows Setting Type	Description	Modify
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. See Managing client settings and Index configurations in Client Management on page 257.

Tuning Tanium Client settings for VDI endpoints and other endpoints with limited resources

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 183.

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 253.

Table 20: Best practice client settings for VDI instances

Client Setting	Default Value	Best Practice Value for VDI	Explanation
RandomSensorDelayInSeconds	0	20	By default, sensors run immediately. This setting delays the execution of any sensor by a random time up to 20 seconds, which reduces concurrent execution of sensors and packages.
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.

Table 20: Best practice client settings for VDI instances (continued)

Client Setting	Default Value	Best Practice Value for VDI	Explanation
LogVerbosityLevel	1	0	Disable logging to reduce disk writes. Temporarily re-enable logging on individual endpoints for troubleshooting.
Logs.extensions.LogVerbosityLevel	11	0	Disable Tanium™ Client Extensions logging to reduce disk writes. Temporarily re-enable logging on individual endpoints for troubleshooting.
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.

You can apply these settings using a settings configuration in Tanium Client Management. See Managing client settings and Index configurations in Client Management on page 257.

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 on page 24. For the configuration steps, see Configure isolated subnets on page 208.

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.

Table 21: 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`

Table 21: Example questions to identify VDI clients (continued)

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`

To help simplify management of VDI endpoints, consider creating computer groups with custom tag-based membership and applying corresponding custom tags to VDI endpoints. See Tanium Console User Guide: 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, 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.

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 65.

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 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. See Use questions to review peering settings on page 218. Contact Tanium Support for more assistance.

Table 22: 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.

Table 22: Tanium Client peer settings (continued)

Setting Name	Description
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.

Tanium Client command line interface (CLI)

CLI on Windows endpoints

Tanium Client settings are written to the Windows registry. The executable program for the CLI, **TaniumClient.exe**, is in the Tanium Client installation directory. 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 298.

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
```

The following example shows how to configure the connection between Tanium Client 7.4 or later 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. 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 298.

The following example shows how to set and confirm the FQDNs of the Tanium Server with which the Tanium Client can connect 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
ts1.tam.local,ts2.tam.local
```

The following example shows how to configure the connection between Tanium Client 7.4 or later 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
```

Reference: Endpoint security exclusions

If security software is implemented in your environment to monitor and block unknown host system processes, Tanium requires that a security administrator create exclusions to allow Tanium Client processes to run without interference. Tanium recommends implementing advanced antivirus (AV) software that permits customized and detailed exclusions that typically do not block known Tanium processes. Some AV software might require excluding the installation directories of the Tanium Client from real-time inspection. Typically, configuring trusted exclusions also involves setting a policy to ignore the input and output of Tanium binaries. The configuration of these exclusions varies based on the AV software.

- 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 AV interference, Tanium might require you to remove the AV software temporarily for the purposes of troubleshooting and restore it once troubleshooting is complete.

For the additional security exclusions that apply to Tanium Core Platform servers in a Windows-based deployment, see Tanium Windows Deployment Guide: 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.

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

Target Device	Installation folder
Windows x86 endpoints	`C:\Program Files\Tanium\Tanium Client`
Windows x64 endpoints	`C:\Program Files (x86)\Tanium\Tanium Client`
macOS endpoints	`/Library/Tanium/TaniumClient`
Linux, Solaris, AIX endpoints	`/opt/Tanium/TaniumClient`

For additional folder exclusions that Tanium requires during Tanium Client installation, see Tanium Client Management User Guide: Security exclusions for Client Management.

Tanium Client system processes

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

Target Device	Notes	Process
Windows endpoints		<*Tanium Client*>\TaniumClient.exe
		<*Tanium Client*>\TaniumCX.exe
		<*Tanium Client*>\Tools\StdUtils\7za.exe
		<*Tanium Client*>\Tools\StdUtils\runasuser.exe
		<*Tanium Client*>\Tools\StdUtils\runasuser64.exe
		<*Tanium Client*>\Tools\StdUtils\TaniumExecWrapper.exe
		<*Tanium Client*>\Tools\StdUtils\TaniumFileInfo.exe
		<*Tanium Client*>\Tools\StdUtils\TPowerShell.exe

Security exclusions for Tanium Client processes (continued)

Target Device	Notes	Process
macOS, Linux, Solaris, AIX endpoints		`<Tanium Client>/TaniumClient`
		`<Tanium Client>/taniumclient`
		`<Tanium Client>/TaniumCX`
	macOS endpoints running the universal Tanium Client binary only	`<Tanium Client>/TaniumCX.app/Contents/MacOS/TaniumCX`
		`<Tanium Client>/Tools/StdUtils/TaniumExecWrapper`
		`<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. See Reference: Endpoint security exclusions on page 315.
- **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:

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-specific exclusions

The following sections list additional processes, folders, and files on the Tanium Client 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.

NOTE

- If the required exclusions are not configured, or if Tanium suspects AV interference, Tanium might require you to remove the AV software temporarily for the purposes of troubleshooting and restore it once troubleshooting is complete.
- The following sections use the <*Tanium Client*> variable to indicate the client installation folder.

- Directory Query on page 337
- Discover on page 337
- Endpoint Configuration on page 353
- End-User Notifications on page 353
- Enforce on page 355
- Engage on page 358
- Feed on page 358
- Gateway on page 358
- Health Check on page 358
- Impact on page 359
- Integrity Monitor on page 359
- Interact: The host and network security requirements of the Tanium Core Platform apply to Interact:
    - Tanium Client folders on page 315
    - Tanium Client system processes on page 316
- Investigate on page 369
- Mac Device Enrollment on page 371
- Patch on page 371
- Performance on page 373
- Provision on page 376
- RDB Service on page 378
- Reporting on page 378
- Reputation on page 378
- Reveal on page 378
- Screen Sharing on page 380
- Secrets Service on page 381
- System User Service on page 381
- Threat Response on page 381
- Trends on page 428
- Zero Trust on page 428

Asset

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
		File	<*Tanium Client*>\extensions\TaniumSoftwareManager.dll.sig
		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
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/libSupportCX.dylib
		File	<*Tanium Client*>/extensions/libSupportCX.dylib.sig
		File	<*Tanium Client*>/extensions/libTaniumConfig.dylib
		File	<*Tanium Client*>/extensions/libTaniumConfig.dylib.sig

Asset security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
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/libSupportCX.so
		File	<*Tanium Client*>/extensions/libSupportCX.so.sig
		File	<*Tanium Client*>/extensions/libTaniumConfig.so
		File	<*Tanium Client*>/extensions/libTaniumConfig.so.sig

Benchmark

Benchmark security exclusions for endpoints

Enpoint 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

Blob Service

No additional security exclusions are required.

Certificate Manager

Certificate Manager security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows		Process	<*Tanium Client*>\Python38\TPython.exe
		Folder	<*Tanium Client*>\Python38
		Process	<*Tanium Client*>\TaniumCX.exe
		Process	<*Tanium Client*>\Tools\StdUtils\TaniumExecWrapper.exe
		Folder	<*Tanium Client*>\Tools\CertificateManager
Linux		Process	<*Tanium Client*>/python38/python
		Process	<*Tanium Client*>/TaniumCX
		Process	<*Tanium Client*>/Tools/StdUtils/TaniumExecWrapper
		Folder	<*Tanium Client*>/Tools/CertificateManager
macOS		Process	<*Tanium Client*>/python38/python
		Process	<*Tanium Client*>/TaniumCX
		Process	<*Tanium Client*>/Tools/StdUtils/TaniumExecWrapper
		Folder	<*Tanium Client*>/Tools/CertificateManager

Client Management

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`

Client Management security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	During client installation; x64 endpoints	Process	`C:\Program Files (x86)\Tanium\SetupClient.exe`

Client Management security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	During client installation; x86 endpoints	Process	`C:\Program Files\Tanium\TaniumClientBootstrap.exe`

Client Management security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	During client installation; x86 endpoints	Process	`C:\Program Files\Tanium\SetupClient.exe`

Client Management security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	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 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
	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 satellite profiles only)	Folder	C:\Program Files\Npcap
	When Discover is installed; (Distributed level 3, distributed level 4, and satellite profiles only)	Process	<*Tanium Client*>\Tools\Discover\nmap\nmap.exe

Client Management security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
macOS	During client installation	Process	`/Library/Tanium/TaniumClientBootstrap`
	During client installation	Process	`/Library/Tanium/SetupClient`
	During client installation	Process	`<Tanium Client>/SetupClient`
		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`
	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`
	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`

Client Management security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
Linux	During client installation	Process	`/opt/Tanium/TaniumClientBootstrap`
	During client installation	Process	`/opt/Tanium/SetupClient`
	During client installation	Process	`<Tanium Client>/SetupClient`
		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 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 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`

Client Management security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
Solaris and AIX	During client installation	Process	`/opt/Tanium/TaniumClientBootstrap`
	During client installation	Process	`/opt/Tanium/SetupClient`
	During client installation	Process	`<Tanium Client>/SetupClient`

Comply

Comply 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\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\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

Comply security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
Linux/macOS/AIX		Process	<*Tanium Client*>/TaniumCX
		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
		File	<*Tanium Client*>/Tools/Comply/delete-assessment.sh
Tanium scan engine - all supported endpoints		File	<*Tanium Client*>/extensions/comply/engines/joval/Joval-Utilities.jar
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

Comply security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
CIS-CAT engine -Windows		File	<*Tanium Client*>\extensions\comply\engines\ciscat\CIS-CAT.BAT
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

Connect

No additional security exclusions are required.

Criticality

No additional security exclusions are required.

Deploy

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).

Deploy security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows	Required only for the Microsoft InPlace Upgrade packages	Folder	`C:\Deploy\Tanium`
		Process	`<Tanium Client>\Python38\TPython.exe`
		Folder	`<Tanium Client>\Python38`
		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`

Deploy security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
Linux		Process	<*Tanium Client*>/python38/python
		Folder	<*Tanium Client*>/python38
		Process	<*Tanium Client*>/TaniumCX
		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
		File	<*Tanium Client*>/extensions/libTaniumSoftwareManager.so
		File	<*Tanium Client*>/extensions/libTaniumSoftwareManager.so.sig
	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

Deploy security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
macOS		Process	`<Tanium Client>/python38/python`
		Folder	`<Tanium Client>/python38`
		Process	`<Tanium Client>/TaniumCX`
		File	`<Tanium Client>/extensions/libTaniumSoftwareManager.dylib`
		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`

Direct Connect

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
		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

Directory Query

No additional security exclusions are required.

Discover

Discover security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows		Process	`<Tanium Client>\TaniumCX.exe`

Discover security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	<*Tanium Client*>\Tools\Discover\nmap\vcredist_x86.exe

Discover security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\TaniumClientExtensions.dll`

Discover security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	<*Tanium Client*>\TaniumClientExtensions.dll.sig

Discover security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	<*Tanium Client*>\extensions\SupportCX.dll

Discover security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		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
		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

Discover security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
Linux		Process	`<Tanium Client>/TaniumCX`

Discover security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/libTaniumClientExtensions.so`

Discover security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/libTaniumClientExtensions.so.sig`

Discover security exclusions for endpoints (continued)

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
		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
	(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

Discover security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
macOS		Process	`<Tanium Client>/TaniumCX`

Discover security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/libTaniumClientExtensions.dylib`

Discover security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client >/libTaniumClientExtensions.dylib.sig`

Discover security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/libSupportCX.dylib`

Discover security exclusions for endpoints (continued)

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/discover/data/discover.db
		File	<*Tanium Client*>/extensions/discover/data/discover.db-wal
		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.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

Endpoint Configuration

No additional security exclusions are required.

End-User Notifications

End-User Notifications security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows	7.4.*x* clients	Process	`<Tanium Client>\Python38\TPython.exe`
	64-bit OS versions	Process	`C:\Program Files (x86)\Tanium\Tanium End User Notification Tools\UserSessionProxy.exe`
	32-bit OS versions	Process	`C:\Program Files\Tanium\Tanium End User Notification Tools\UserSessionProxy.exe`
	64-bit OS versions	Process	`C:\Program Files (x86)\Tanium\Tanium End User Notification Tools\bin\end-user-notifications.exe`
	32-bit OS versions	Process	`C:\Program Files\Tanium\Tanium End User Notification Tools\bin\end-user-notifications.exe`
	exclude from on-access or real-time scans (64-bit OS versions)	Folder	`C:\Program Files (x86)\Tanium\Tanium End User Notification Tools`
	exclude from on-access or real-time scans (32-bit OS versions)	Folder	`C:\Program Files\Tanium\Tanium End User Notification Tools`
		Folder	`C:\ProgramData\Tanium`
	64-bit OS versions	Folder	`C:\Program Files (x86)\Tanium\Tanium Client\Tools\EndUserNotifications\scripts`
	64-bit OS versions	File	`C:\Program Files (x86)\Tanium\Tanium Client\Tools\EndUserNotifications\scripts\config.vbs`
	64-bit OS versions	File	`C:\Program Files (x86)\Tanium\Tanium Client\Tools\EndUserNotifications\scripts\remove-end-user-notifications.vbs`

End-User Notifications security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
macOS	7.4.*x* clients	Process	`<Tanium Client>/python38/bin/pybin`
		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

Enforce security exclusions for endpoints

Target Device	Notes	Exclusion Type	Exclusion
Windows x86 endpoints		Process	<*Tanium Client*>\Tools\StdUtils\7za.exe
		Process	<*Tanium Client*>\Tools\Enforce\devcon32.exe
		Process	<*Tanium Client*>\Tools\Enforce\LocalPolicyTool.exe
	7.4.*x* clients 7.2.*x* clients	Process	<*Tanium Client*>\Python38\TPython.exe
	7.4.*x* clients 7.2.*x* clients	Folder	<*Tanium Client*>\Python38
		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
		Process	<*Tanium Client*>\tools\driver\TaniumDriverCtl.exe
		File	C:\Windows\System32\drivers\TaniumRecorderDrv.sys
		Process	<*Tanium Client*>\tools\driver\TaniumDriverSvc.exe
		Process	<*Tanium Client*>\tools\driver\service\TaniumDriverSvc.exe
		File	<*Tanium Client*>\tools\driver\TaniumProcessMonitor.dll
		Folder	<*Tanium Client*>\extensions\stream

Enforce security exclusions for endpoints (continued)

Target Device	Notes	Exclusion Type	Exclusion
Windows x64 endpoints		Process	<*Tanium Client*>\Tools\StdUtils\7za.exe
		Process	<*Tanium Client*>\Tools\Enforce\devcon64.exe
		Process	<*Tanium Client*>\Tools\Enforce\LocalPolicyTool.exe
	7.4.*x* clients 7.2.*x* clients	Process	<*Tanium Client*>\Python38\TPython.exe
	7.4.*x* clients 7.2.*x* clients	Folder	<*Tanium Client*>\Python38
		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
		Process	<*Tanium Client*>\tools\driver\service\TaniumDriverSvc.exe
		Process	<*Tanium Client*>\tools\driver\TaniumDriverCtl64.exe
		Process	<*Tanium Client*>\tools\driver\TaniumDriverSvc64.exe
		File	<*Tanium Client*>\tools\driver\TaniumProcessMonitor64.dll
		Folder	<*Tanium Client*>\extensions\stream

Enforce security exclusions for endpoints (continued)

Target Device	Notes	Exclusion Type	Exclusion
macOS and Linux x86 and x64 endpoints	7.4.*x* clients 7.2.*x* clients	Process	<*Tanium Client*>/python38/python
	7.4.*x* clients 7.2.*x* clients	Folder	<*Tanium Client*>/python38
		Process	<*Tanium Client*>/python38/bin/pybin
		Process	<*Tanium Client*>/TaniumClient
		Process	<*Tanium Client*>/TaniumCX

Engage

Engage security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows		File	<*Tanium Client*>\extensions\TaniumEndUser.dll
	7.4.*x* clients	Process	<*Tanium Client*>\Python38\TPython.exe
	7.4.*x* clients	Folder	<*Tanium Client*>\Python38
		Folder	C:\Program Files(x86)\Tanium\Tanium End User Notification Tools

Feed

No additional security exclusions are required.

Gateway

No additional security exclusions are required.

Health Check

No additional security exclusions are required.

Impact

Impact security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows		Process	<*Tanium Client*>\Python38\TPython.exe
		Folder	<*Tanium Client*>\Python38
		Process	<*Tanium Client*>\TaniumCX.exe
		File	<*Tanium Client*>\TaniumClientExtensions.dll
		File	<*Tanium Client*>\TaniumClientExtensions.dll.sig
	When Direct Connect is installed; satellite sync only	File	<*Tanium Client*>\extensions\TaniumDEC.dll
	When Direct Connect is installed; satellite sync only	File	<*Tanium Client*>\extensions\TaniumDEC.dll.sig

Integrity Monitor

Integrity Monitor security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Process
Windows x86 and x64		File	`<Tanium Client>\extensions\TaniumIndex.dll`

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	`<Tanium Client>\extensions\TaniumIndex.dll.sig`

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	<*Tanium Client*>\extensions\TaniumIntegrityMonitor.dll

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	<*Tanium Client*>\extensions\TaniumIntegrityMonitor.dll.sig

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	<*Tanium Client*>\extensions\TaniumRecorder.dll

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	<*Tanium Client*>\extensions\TaniumRecorder.dll.sig

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	<*Tanium Client*>\extensions\recorder\proc.bin

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		File	<*Tanium Client*>\extensions\recorder\recorder.db

Integrity Monitor security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Process
		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
		File	<*Tanium Client*>\TaniumClientExtensions.dll
		File	<*Tanium Client*>\TaniumClientExtensions.dll.sig
		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

Integrity Monitor security exclusions for endpoints (continued)

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
		Folder	<*Tanium Client*>/extensions/index
		Folder	<*Tanium Client*>/extensions/integrity-monitor

Investigate

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
	7.4.*x* clients, [1]	Process	<*Tanium Client*>\Python38\TPython.exe
	7.4.*x* clients	Folder	<*Tanium Client*>\Python38
		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
	7.4.*x* clients	Folder	<*Tanium Client*>/python38
	7.4.*x* clients	Process	<*Tanium Client*>/python38/python
		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

Investigate security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
macOS		Process	<*Tanium Client*>/TaniumCX
	7.4.*x* clients	Folder	<*Tanium Client*>/python38
	7.4.*x* clients	Process	<*Tanium Client*>/python38/python
		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

[1] = TPython requires SHA2 support to allow installation.

Mac Device Enrollment

No additional security exclusions are required.

Patch

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*>\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
		Process	<*Tanium Client*>\Patch\tools\TaniumUpdateSearcher.exe
	7.4.*x* clients	Process	<*Tanium Client*>\Python38\TPython.exe
		Folder	<*Tanium Client*>\Python38
		Process	<*Tanium Client*>\Tools\Patch\7za.exe
		Process	<*Tanium Client*>\Patch\tools\TaniumExecWrapper.exe
		File	<*Tanium Client*>\extensions\TaniumSoftwareManager.dll
		File	<*Tanium Client*>\extensions\TaniumSoftwareManager.dll.sig
	exclude from on-access or real-time scans	Folder	<*Tanium Client*>

Patch security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
Linux		File	<*Tanium Client*>/libTaniumClientExtensions.so
		File	<*Tanium Client*>/libTaniumClientExtensions.so.sig
	7.4.*x* clients	Process	<*Tanium Client*>/python38/bin/pybin
		Process	<*Tanium Client*>/python38/python
		Folder	<*Tanium Client*>/python38
		File	<*Tanium Client*>/extensions/libTaniumSoftwareManager.so
		File	<*Tanium Client*>/extensions/libTaniumSoftwareManager.so.sig
macOS		File	<*Tanium Client*>/libTaniumClientExtensions.so
		File	<*Tanium Client*>/libTaniumClientExtensions.so.sig
	7.4.*x* clients	Process	<*Tanium Client*>/python38/bin/pybin
		Process	<*Tanium Client*>/python38/python
		Folder	<*Tanium Client*>/python38
		File	<*Tanium Client*>/extensions/libTaniumSoftwareManager.dylib
		File	<*Tanium Client*>/extensions/libTaniumSoftwareManager.dylib.sig

Performance

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
		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\performance.db
		File	<*Tanium Client*>\extensions\performance\performance.db-shm
		File	<*Tanium Client*>\extensions\performance\performance.db-wal
	7.4.x clients	Folder	<*Tanium Client*>\Python38
	7.4.x clients[1]	Process	<*Tanium Client*>\Python38\TPython.exe
		Process	<*Tanium Client*>\TaniumCX.exe

Performance security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
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
		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/performance.db
		File	<*Tanium Client*>/extensions/performance/performance.db-shm
		File	<*Tanium Client*>/extensions/performance/performance.db-wal
	7.4.x clients	Folder	<*Tanium Client*>/python38
	7.4.x clients	Process	<*Tanium Client*>/python38/bin/pybin
		Process	<*Tanium Client*>/TaniumCX

Performance security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
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
		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/performance.db
		File	<*Tanium Client*>/extensions/performance/performance.db-shm
		File	<*Tanium Client*>/extensions/performance/performance.db-wal
	7.4.x clients	Folder	<*Tanium Client*>/python38
	7.4.x clients	Process	<*Tanium Client*>/python38/bin/pybin
		Process	<*Tanium Client*>/TaniumCX

[1] = TPython requires SHA2 support to allow installation.

Provision

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
		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

Provision security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
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

RDB Service

No additional security exclusions are required.

Reporting

No additional security exclusions are required.

Reputation

No additional security exclusions are required.

Reveal

Reveal 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\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

Reveal security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
macOS		Process	*<Tanium Client>*/TaniumCX
		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

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

Secrets Service

No additional security exclusions are required.

System User Service

No additional security exclusions are required.

Threat Response

Threat Response security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows x86 and x64		Process	`<Tanium Client>\Tools\IR\TaniumExecWrapper.exe`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	<*Tanium Client*>\Tools\IR\TanFileInfo.exe

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	`<Tanium Client>\Tools\IR\TaniumFileInfo.exe`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	`<Tanium Client>\Tools\IR\TaniumHandle.exe`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	<*Tanium Client*>\Tools\IR\TaniumListModules.exe

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\TaniumIndex.dll`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\TaniumIndex.dll.sig`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	`<Tanium Client>\Tools\recorder\TaniumRecorderCtl.exe`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\TaniumRecorder.dll`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\TaniumRecorder.dll.sig`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\SupportCX.dll`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\SupportCX.dll.sig`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	<*Tanium Client*>\extensions\recorder\proc.bin

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\recorder\recorder.db`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\recorder\recorder.db-shm`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\recorder\recorder.db-wal`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\index\index.db`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\index\index.db-shm`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\index\index.db-wal`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	x86 endpoints	Process	`<Tanium Client>\tools\driver\TaniumDriverCtl.exe`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	x64 endpoints	Process	`<Tanium Client>\tools\driver\TaniumDriverCtl64.exe`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	x86 endpoints	Process	`<Tanium Client>\tools\driver\TaniumDriverSvc.exe`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	x64 endpoints	Process	`<Tanium Client>\tools\driver\TaniumDriverSvc64.exe`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	<*Tanium Client*>\tools\driver\service\TaniumDriverSvc.exe

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		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
	1	Process	<*Tanium Client*>\Downloads\Action_*\TaniumFileTransfer.exe
	1	Process	<*Tanium Client*>\Downloads\Action_*\Winpmem.gb414603.exe
		Process	<*Tanium Client*>\Tools\IR\TaniumPersistenceAnalyzer.exe
		File	<*Tanium Client*>\Tools\IR\PowerForensics\PowerForensics.dll
	7.2.*x* clients, 3	Process	<*Tanium Client*>\Python27\TPython.exe
	7.4.*x* clients, 3	Process	<*Tanium Client*>\Python38\TPython.exe
	7.2.*x* clients	Folder	<*Tanium Client*>\Python27
	7.4.*x* clients	Folder	<*Tanium Client*>\Python38
		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

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
Linux x86 and x64		Process	`<Tanium Client>/extensions/recorder/TaniumAuditPipe`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	`<Tanium Client>/TaniumCX`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	`<Tanium Client>/Tools/IR/TaniumExecWrapper`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/libTaniumIndex.so`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/libTaniumIndex.so.sig`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	7.2.*x* clients	Folder	`<Tanium Client>/python27`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	7.2.*x* clients	Process	`<Tanium Client>/python27/python`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	7.2.*x* clients	Process	`<Tanium Client>/python27/bin/pybin`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	7.4.*x* clients	Folder	`<Tanium Client>/python38`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	7.4.*x* clients	Process	`<Tanium Client>/python38/python`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		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
		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
	[1],[2]	Process	<*Tanium Client*>/Downloads/Action_*/surge-collect
	[1],[2]	File	<*Tanium Client*>/Downloads/Action_*/surge.dat
	[1]	File	<*Tanium Client*>/Downloads/Action_*/linpmem-*.bin
	[1]	Process	<*Tanium Client*>/Downloads/Action_*/taniumfiletransfer

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
macOS		Process	`<Tanium Client>/TaniumCX`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	For macOS Universal only	Process	`<Tanium Client>/TaniumCX.app/Contents/MacOS/TaniumCX`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	`<Tanium Client>/Tools/IR/TaniumExecWrapper`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/libTaniumIndex.dylib`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/libTaniumIndex.dylib.sig`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	7.2.*x* clients	Folder	`<Tanium Client>/python27`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	7.2.*x* clients	Process	`<Tanium Client>/python27/python`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	7.4.*x* clients	Folder	`<Tanium Client>/python38`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	7.4.*x* clients	Process	`<Tanium Client>/python38/python`

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		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
		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
	[1],[2]	Process	<*Tanium Client*>/Downloads/Action_*/surge-collect
	[1],[2]	File	<*Tanium Client*>/Downloads/Action_*/surge.dat
	[1]	Process	<*Tanium Client*>/Downloads/Action_*/osxpmem.app/osxpmem

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	[1]	Process	*<Tanium Client>*/Downloads/Action_*/taniumfiletransfer

[1] = Where * corresponds to the action ID or the version of linpmem.

[2] = Exception is required if Volexity Surge is used for memory collection.

[3] = TPython requires SHA2 support to allow installation.

Trends

No additional security exclusions are required.

Zero Trust

No additional security exclusions are required.

Reference: Client extensions 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 Endpoint Configuration User Guide: Managing endpoint tools.

Each client extension and tool has required security exclusions to allow the Tanium processes to run without interference. See Reference: Endpoint security exclusions on page 315 and for Windows-based Tanium Core Platform deployments, Tanium Core Platform User Guide for Windows Deployments: Tanium Core Platform server security exclusions, or the requirements section for each solution.

Client extensions can run in separate processes, or together in a single process, depending on whether *client extension shared process mode* is enabled. See Endpoint Configuration User Guide: Manage client extension shared process mode.

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 Tanium Endpoint Configuration User Guide: Identify and resolve issues with endpoint tools or client extensions.

The following client extensions perform functions for Tanium solutions:

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-cx	Provides Comply functions on an endpoint	Comply
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, 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 satellite-based Nmap scans	Discover

Tool	Description	Solutions where used
end-user-cx	Provides a mechanism to send surveys to collect qualitative feedback from endpoint users	Engage
enforce-cx	Provides Enforce functions on an endpoint	Enforce
extras-cx	Provides a helper library that contains re-usable functions for various client extensions to use	Asset, 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, Deploy, Integrity Monitor, Reveal, Threat Response
integrity-monitor-cx	Provides Integrity Monitor functions on an endpoint	Integrity Monitor
performance-cx	Provides Performance functions on an endpoint	Investigate, Performance
provision-cx	Provides sensitive data and notifications about bundle or settings changes to a Provision endpoint	Provision
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
risk-cx	Provides Risk functions on the endpoint	Risk
swmgr-cx	Provides a catalog of all installed software on an endpoint	Asset, Comply, Deploy, Patch
threat-response-cx	Provides Threat Response functions on an endpoint	Threat Repsonse

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.

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.

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
```

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 Tanium Appliance User Guide: Export Commodity Classification or Tanium Core Platform User Guide for Windows Deployments: Export Commodity Classification.

Tanium prohibits software and hardware (both physical and virtual) installations in certain countries. Contact Tanium Support to determine whether a particular country is on the prohibited list.