

Tanium™ Core Platform User Guide

Autonomous IT. Unstoppable Business.

2025H2 Semiannual Release

Version 7.8.2.XXXX

August 14, 2026

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

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

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

This documentation may provide access to or information about content, products (including hardware and software), and 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. We certify against the WCAG 2.2 / VPAT 2.5 standards for all major product modules. Tanium performs ongoing reassessments as appropriate, given the scope and type of changes to the UI and product features from release to release. In the most recent testing, the Tanium Console UI achieved supports or partially supports for all applicable WCAG 2.2 criteria. Tanium can make available any VPAT reports on a module-by-module basis as part of a larger solution planning process for any customer or prospect.

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

Tanium welcomes customer input on making solutions accessible based on your Tanium modules and assistive technology requirements. Accessibility requirements are important to the Tanium customer community and we are committed to prioritizing these compliance efforts as part of our overall product roadmap. Tanium maintains transparency on our progress and milestones and welcomes any further questions or discussion around this work. Contact your sales representative, Tanium Support 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/

© 2026 Tanium Inc. All Rights Reserved

© 2026 Tanium Inc. All rights reserved.

Table of contents

Overview of Tanium™ Core Platform Servers in a Windows environment **13**

Tanium infrastructure types 13

Tanium Server 13

Tanium Module Server 14

Tanium Zone Server 15

Zone Server Caching 15

Zone Server High Availability 15

Tanium Core Platform topology 18

Tanium Core Platform requirements in a Windows environment **20**

Installation package and license files 20

Server version and host system requirements 20

Compatibility among components in a Tanium release 24

Tanium™ Semiannual Release 2025H2 24

Maintenance releases 24

Upgrade process 25

Upgrading Tanium Core Platform and Tanium solutions 25

Upgrading the Tanium Endpoint Configuration Toolset and Tanium Client 25

Internet access, network connectivity, and firewalls 26

Internet Protocol (IP) support 26

Internet URLs 26

Server throughput and latency 27

Proxy server 27

Ports and firewalls 27

SSL/TLS certificates 31

Administrator account permissions 31

Administrator accounts for installations and upgrades 31

Administrator accounts for post-installation/upgrade activities 32

© 2026 Tanium Inc. All Rights Reserved

Installing the Tanium Server **34**
Before you begin 34
Set up a database server 35
Create and configure the database server 36
Manage the Tanium database collation mode 37
Install the Tanium Server 37
Relocate the package file repository 41
Next steps 42
Installing the Tanium Module Server **43**
Install and automatically register the Module Server 43
Before you begin 43
Run the installer 44
Install and manually register the Module Server 47
Before you begin 47
Run the installer 48
(Optional) Configure a connection between the Module Server and a remote PostgreSQL database 51
Update the Module Server certificate 52
Next steps 53
Installing the Tanium Zone Server **54**
Before you begin 54
Install the Tanium Zone Server 54
Install the Zone Server Hub 55
Install the Zone Server 56
Configure ports for traffic from Zone Server Hubs and Tanium Clients 58
Manage caching on the Zone Server and Zone Server Hub 59
Manage Zone Server caching 59
Manage Zone Server Hub caching 59
Configure Tanium Clients to register with the Zone Server 60
Initial Tanium Client deployment 60
Existing Tanium Client deployment 62

© 2026 Tanium Inc. All Rights Reserved

Configuring proxy server settings in a Windows deployment ... **66**
Overview of proxy server connections ... 66
Types of proxy servers ... 67
TDownloader user context ... 67
Tanium Console: Configure proxy settings ... 67
Configure proxy settings ... 68
Installing Tanium Servers in an active-active HA cluster ... **72**
HA cluster requirements and limitations ... 72
Before you begin ... 72
Deploy the HA cluster ... 74
HA configuration notes ... 75
Securing Tanium Console, API, and Module Server access in a Windows deployment ... **77**
Overview of certificates and keys ... 77
Tanium Console and API ... 77
Signed and encrypted SAML authentication on the Tanium Server ... 78
Module Server communication ... 79
SSL/TLS connection processes and setup tasks ... 80
CA-issued Tanium Server SOAP certificates ... 82
Certificate requirements ... 82
(Optional) Enable HTTP Strict Transport Security for Tanium Console access ... 86
Securing Tanium Server, Zone Server, and Tanium Client access in a Windows deployment ... **87**
Overview of TLS in the Tanium Core Platform ... 87
Communication protocols ... 87
TLS communication process ... 89
Supported cipher suites ... 89
TLS options, and defaults ... 89
HSM integration ... 90
(Optional) Configure the TLS requirement for Tanium Client connections ... 90
Configure TLS on Tanium Clients ... 90
Verify the TLS connections ... 91

© 2026 Tanium Inc. All Rights Reserved

Update the TLS configuration when you make changes to key pair ... 91
Verifying the deployment to your Windows environment ... 92
Configuring smart card authentication in a Windows deployment ... 99
Requirements ... 99
Create a certificate ... 99
Extract the certificates ... 100
Create a new certificate file ... 103
Configure CAC ... 104
Step 1: Copy the certificate to the Tanium Server installation directory ... 104
Step 2: Add Windows registry keys on Tanium Server host ... 104
Troubleshoot smart card authentication ... 108
Securing keys with an HSM in a Windows deployment ... 110
HSM integration overview ... 110
Integrate with an HSM ... 110
Before you begin ... 110
Integrate the Tanium deployment with an HSM ... 111
Verify an HSM integration ... 112
Disable an HSM integration ... 113
Update token PINS, names, or IDs ... 113
Troubleshoot an HSM integration ... 114
Upgrading Tanium Core Platform Servers in a Windows deployment ... 115
Upgrading to a new semiannual release or maintenance release ... 115
Tanium™ Semiannual Release 2025H2 ... 115
Maintenance releases ... 115
Upgrade process ... 115
Upgrading Tanium Core Platform and Tanium solutions ... 115
Upgrading the Tanium Endpoint Configuration Toolset and Tanium Client ... 116
Server upgrade overview ... 116
Before you begin ... 117
Order of Tanium Core Platform Server upgrades ... 117

© 2026 Tanium Inc. All Rights Reserved

Upgrade the Tanium Server ... 118
Upgrade a standalone (non-HA) or primary (HA) Tanium Server ... 118
Upgrade a secondary (HA) Tanium Server ... 119
Upgrade the Tanium Module Server ... 120
Before you begin ... 120
Upgrade the Tanium Module Server ... 120
Upgrade the Tanium Zone Server ... 121
Upgrade the Zone Server Hub ... 122
Upgrade the dedicated Zone Server ... 122
Upgrade solutions and verify the Servers upgrade ... 122
Troubleshooting installation and upgrade in a Windows environment ... 123
Basic troubleshooting tips ... 123
Back up Tanium Core Platform Servers and databases ... 124
Best practices for backups ... 124
Back up the Servers and database ... 125
Common issues and solutions ... 127
Troubleshoot Server installation and upgrade issues ... 128
Verify file integrity ... 129
Manage Windows services for core platform Servers ... 130
Review and update Server settings ... 131
Troubleshoot connectivity among core platform Servers ... 132
Generate and review logs ... 133
Uninstall Tanium ... 134
Uninstall the Tanium Core Platform ... 134
Uninstall a Tanium Core Platform Server ... 134
Remove Tanium databases ... 135
Uninstall a Tanium solution or Tanium Client ... 135
Contact Tanium Support ... 137
Reviewing logs and troubleshooting Tanium Core Platform in a Windows deployment ... 138
Logging levels ... 138

© 2026 Tanium Inc. All Rights Reserved

Troubleshooting workflow 139
Before you begin 139
Troubleshoot issues during Server deployment or solution operations 140
Log and report types 141
Action scheduler log 142
Authentication log 143
Console local error log 143
Database upgrade log 143
Download catalog cleaner log 143
HTTP connection log 144
Installation logs 144
LDAP log 144
Module plugin history log 144
Module-provided privileges log 145
Package cache cleaner log 145
Package download log 145
PKI log 146
PKI TLS log 146
PostgreSQL installation log 146
RBAC log 147
Server logs 147
Solution logs and support packages 148
TDownloader log 149
TPAN report 150
Workbenches manager log 150
Log rollover 151
Rollover for plain text logs 152
Rollover for ZIP logs 152
Create a custom log for Tanium Core Platform Servers 152
Reference: Host system resource guidelines 156

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform Server host systems ... 156
Operating system support ... 156
Resource requirements ... 156
PostgreSQL server host system ... 157
SQL server host system ... 158
Operating system support ... 158
Resource requirements ... 158
Tanium Core Platform Server security exclusions ... 160
Tanium Core Platform folders ... 160
Tanium Core Platform system processes ... 161
Tanium binary file signers ... 161
Module Server solution folders ... 162
Solution-specific exclusions ... 162
Asset ... 164
Automate ... 164
Benchmark ... 164
Blob Service ... 165
Certificate Manager ... 165
Client Management ... 165
Cloud Workloads ... 166
Comply ... 166
Connect ... 166
Criticality ... 167
Deploy ... 167
Direct Connect ... 167
Directory Query ... 167
Discover ... 168
Endpoint Configuration ... 168
End-User Notifications ... 168
Enforce ... 169

© 2026 Tanium Inc. All Rights Reserved

Engage ... 169
Gateway ... 169
Guide ... 169
Health Check ... 170
Impact ... 170
Integrations Gallery ... 170
Integrity Monitor ... 170
Investigate ... 171
Patch ... 171
Performance ... 171
Provision ... 172
RDB Service ... 172
Reporting ... 172
Reputation ... 172
Reveal ... 173
Screen Sharing ... 173
Secrets Service ... 173
System User Service ... 173
Threat Response ... 174
Trends ... 174
Zero Trust ... 175
Reference: Tanium Core Platform Command-line interface in a Windows deployment ... 176
CLI examples ... 177
Display help ... 177
Display config help ... 178
Example: List configuration settings ... 178
Example: Set configuration values ... 179
Example: Set configuration values ... 179
Example: Register the Module Server with the Tanium Server ... 179
Example: Configure global settings ... 181

© 2026 Tanium Inc. All Rights Reserved

Example: Add an administrator user 181

Reference: Deployment-related Tanium Core Platform settings in a Windows deployment 182

Configure settings using the command line 182

Deployment-related settings reference 183

Reference: Default installation directories for Tanium Core Platform Servers 194

Reference: Default installation directory for the Tanium Client 195

Tanium Core Platform and Tanium Client Export Commodity Classification (Windows deployments) 196

© 2026 Tanium Inc. All Rights Reserved

Overview of Tanium™ Core Platform Servers in a Windows environment

This guide describes requirements and procedures for installing the following Tanium Core Platform Servers on customer-provided Windows infrastructure:

- Tanium™ Server
- Tanium™ Module Server
- Tanium™ Zone Server (including the Tanium™ Zone Server Hub)

Tanium infrastructure types

Tanium Core Platform Servers support the following infrastructure options:

- Tanium™ Cloud (recommended). For more information, see Tanium Cloud User Guide.
- Hardened physical or virtual Tanium™ Appliance. For more information, see the Tanium Appliance User Guide.
- Windows installation on customer-provided hardware, as described in this guide.

Tanium Server

The Tanium Server is the server that communicates with Tanium™ Clients, other Tanium Core Platform Servers, and the `content.tanium.com` servers that host Tanium content packs. Tanium Clients communicate with the Tanium Server directly or through a Tanium Zone Server that acts as a proxy. The Tanium Server also runs the Tanium™ Console and API services.

You can install the Tanium Server on a dedicated host that is separate from the Tanium Module Server and database server, or on an all-in-one host that all three servers share. Use a dedicated host for enterprise production and lab environments (see Tanium Core Platform topology on page 18); the all-in-one architecture is just for proof-of-concept deployments.

You can deploy two Tanium Servers in an active-active high availability (HA) cluster to ensure continuous availability in the event of an outage or scheduled maintenance. HA deployments have the following characteristics:

Tanium Client connections

Tanium Clients use a Tanium Server list to automatically find a backup Server if the primary Tanium Server assigned to them is unavailable.

Tanium Zone Server connections

You can configure failover connections from the Tanium Servers through Zone Server Hubs to HA Zone Servers. This ensures that both Zone Servers can continue serving Tanium Clients if one Tanium Server goes down. For more information, see Zone Server High Availability on page 15.

© 2026 Tanium Inc. All Rights Reserved

Shared database

Tanium Servers in an HA cluster read and write to one shared database. Each Server creates an entry for itself in the **tanium** database that identifies it to the other Servers in the cluster. Follow database administration best practices to ensure availability of the database server and to ensure that the Tanium databases and related database objects are backed up routinely. For more information, see Set up a database server on page 35.

Tanium Console

Each HA cluster member has a Tanium Console with its own URL.

Tanium™ solution modules

The modules are installed on a Tanium Module Server that all the Tanium Servers in an HA cluster share. However, to make the modules available in all the Tanium Servers, you must import the modules through Tanium Console on each cluster member. The Module Server does not support HA.

HA cluster communication

Each Tanium Server passes Tanium messages (such as answers to questions) and package files to the other HA cluster members over port 17472. When you upload package files to a Tanium Server, it automatically synchronizes the files to the other HA cluster members.



HA clustering is not required to scale Tanium capacity or improve performance. You can resize the host system hardware and operating systems of standalone Tanium Core Platform Servers to meet your capacity and performance requirements. For more information, see Reference: Host system sizing guidelines.

To install a standalone (non-HA) Tanium Server on a dedicated Windows Server host, see Installing Tanium Server. To install Tanium Servers in an HA deployment, see Installing the Tanium Server in an active-active HA cluster.

Tanium Module Server

The Tanium Module Server runs application services and stores files for Tanium solution modules, such as Tanium™ Patch. Tanium users can use Tanium Console to manage and use solution modules. The Module Server communicates directly only with the Tanium Server. Endpoints receive packages through the Tanium Server or Zone Server.

In production deployments, you install the Module Server on a dedicated host (not shared with the Tanium Server) to prevent intentional or accidental scripts from having a direct impact on the Tanium Server. For the procedure, see Installing Tanium Module Server.



In a limited proof-of-concept (POC) deployment only, you can install the Module Server and Tanium Server on the same host.

© 2026 Tanium Inc. All Rights Reserved

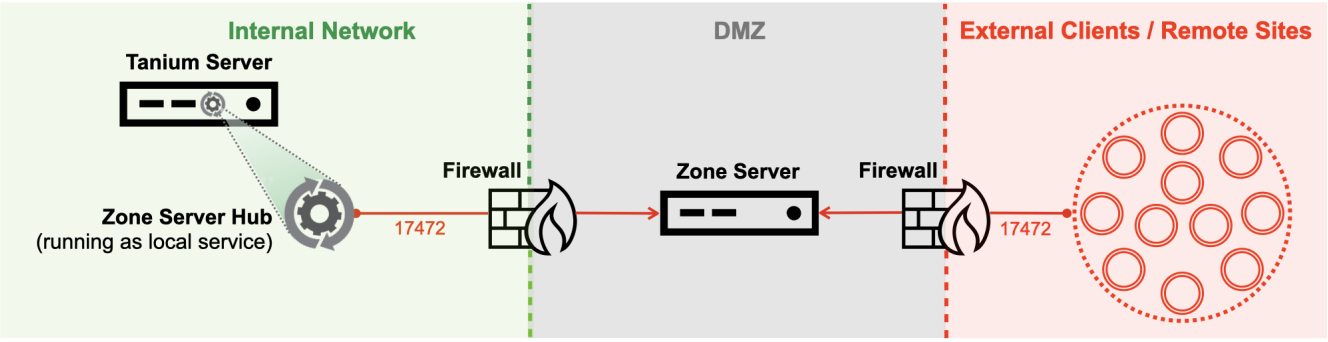
Tanium Zone Server

In Tanium deployments, Tanium Clients initiate connections with the Tanium Server. However, enterprise network security policies typically do not allow endpoints that reside in an external, untrusted network to initiate connections to resources such as the Tanium Server that reside in a trusted, internal network. To enable the Tanium Server to manage external endpoints, deploy one or more Tanium Zone Servers in your DMZ to proxy communication from the external endpoints. For the procedure, see Installing the Tanium Zone Server.

The Zone Server is installed as a service on a device in the DMZ. It communicates with the Tanium Server through a Tanium Zone Server Hub process that you install on a host computer in the internal network, typically the Tanium Server host computer. You configure Tanium Clients on external endpoints to register with the Zone Server as if it were the primary Tanium Server.

The following figure illustrates Zone Server and hub communication.

Zone Server deployment



*By default, the Zone Server uses the same port (17472 by default) for traffic from Zone Server Hubs and Tanium Clients. However, as a best practice to improve the security of the Zone Server, configure separate ports for the hubs and Clients (see Configure ports for traffic from Zone Server Hubs and Tanium Clients).

Zone Server Caching

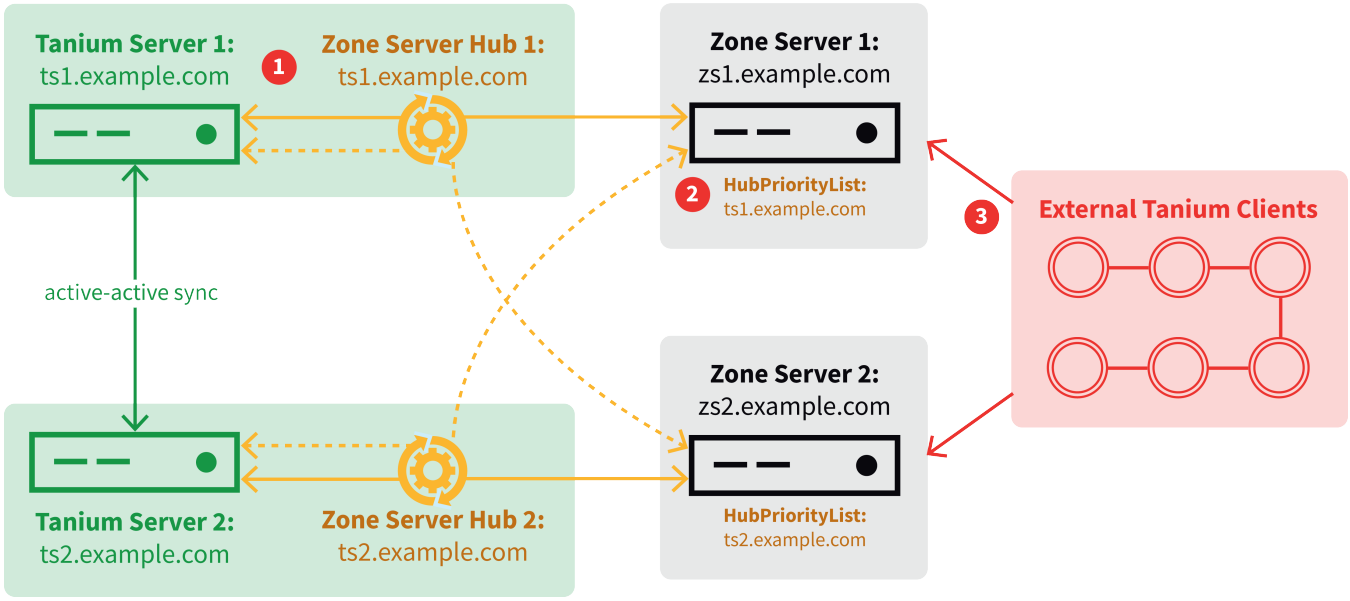
To optimize Tanium system performance, the Zone Server caches action package files and files requested through the Tanium Client API. It provides these resources to Tanium Clients without having to re-request them from the Tanium Server. If necessary to prevent over-consumption of disk space on the Zone Server, you can configure a maximum cache size. In deployments where the Zone Server Hub runs on the Tanium Server host, the hub does not have its own cache but uses the Tanium Server cache. If the hub is on a dedicated host, you must enable the cache on the hub. To configure the cache on the Zone Server or hub, see Manage caching on the Zone Server and Zone Server Hub.

Zone Server High Availability

You can deploy two Zone Servers and two Zone Server Hubs in an active-active HA configuration to ensure continuous availability in the event of an outage or scheduled maintenance. The following figure illustrates a deployment that has HA pairs of Tanium Servers, Zone Server Hubs, and Zone Servers. In this example, the Zone Server Hubs run locally on the Tanium Servers.

© 2026 Tanium Inc. All Rights Reserved

Zone Server HA deployment



The following connections (matching the numbers in the figure Zone Server HA deployment on page 16) ensure continuous availability in this deployment:

1 Each Zone Server Hub connects to a single Tanium Server.

2 Each Zone Server Hub connects to both Zone Servers.

You can configure the **HubPriorityList** setting on each Zone Server to specify the preferred Zone Server Hub from which the Server receives Tanium Client content (such as sensor definitions, configuration information, and action package files).

BEST PRACTICE

In deployments with multiple Zone Servers and hubs, configure the **HubPriorityList** to ensure that each Zone Server receives content from its closest hub. Configuring this setting also optimizes hub usage by ensuring that each hub serves one Zone Server instead of one hub servicing both Servers. For more information, see Installing the Tanium Zone Server.

In the figure Zone Server HA deployment on page 16, the **HubPriorityList** on Zone Server 1 (zs1.example.com) specifies Zone Server Hub 1 (ts1.example.com). Therefore, as long as ts1.example.com is available, zs1.example.com receives Client content only from that hub. In the figure, solid lines indicate the connections when the priority hub is available. If the priority hub goes down, the Zone Server receives Client content from the other hub; in the figure, dotted lines indicate the failover connections.

3 Tanium Clients register through both Zone Servers so that both Tanium Servers can manage the Clients. The Tanium Servers synchronize with each other to ensure active-active availability.

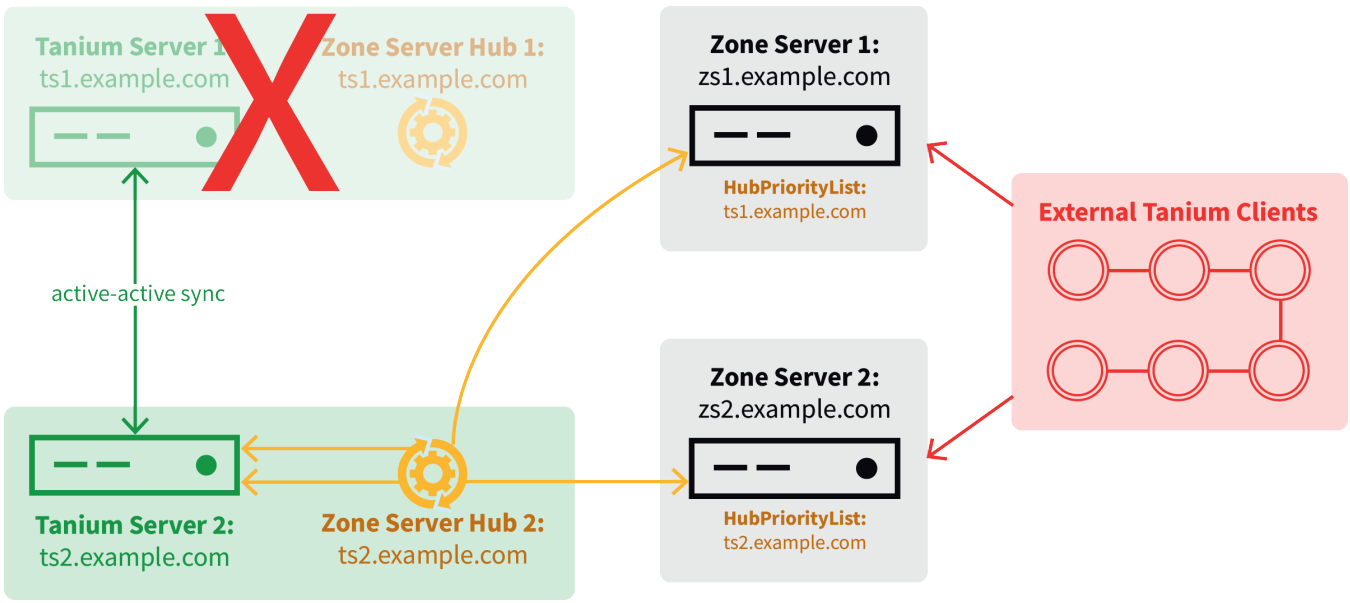
NOTE

The Zone Servers do not perform HA synchronization, and neither do the hubs.

© 2026 Tanium Inc. All Rights Reserved

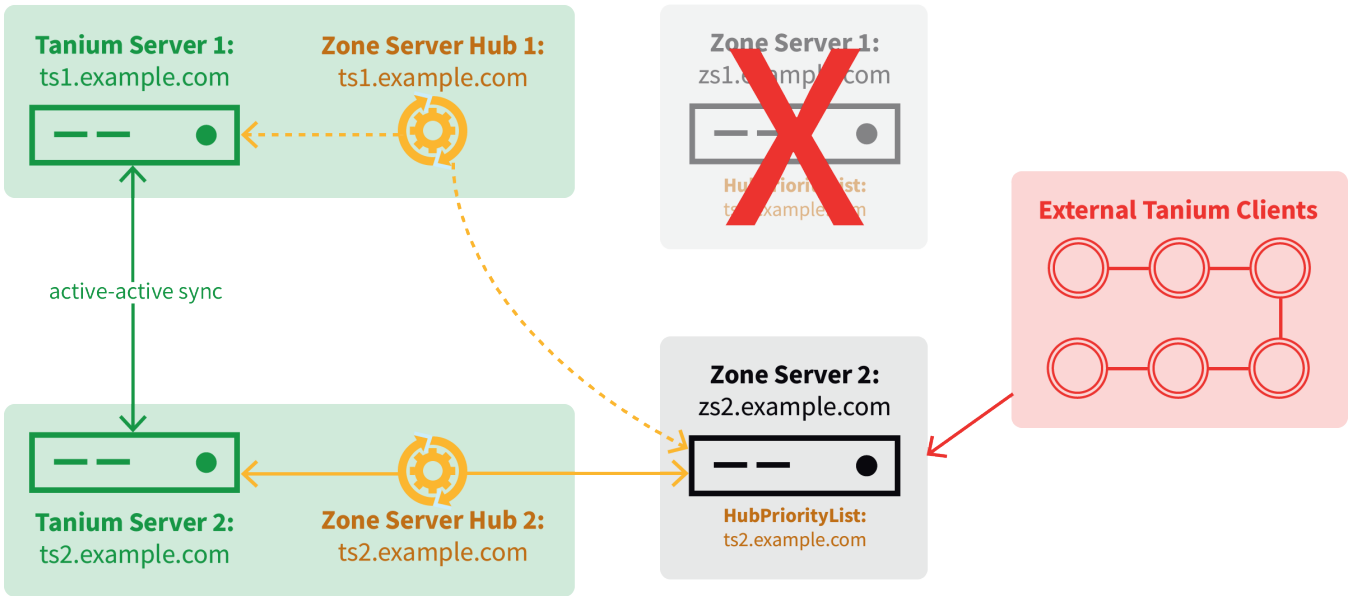
An HA deployment ensures that you can continue managing endpoints if one Tanium Server or Zone Server, or one of each, goes down. In this example, if Tanium Server 1 (ts1.example.com) goes down, Zone Server Hub 2 forwards Tanium Client content from Tanium Server 2 (ts2.example.com) to Zone Server 1 (zs1.example.com), which can therefore continue serving Clients. The following figure illustrates this scenario.

Tanium Server failover in an HA deployment



If Zone Server 1 goes down in this example, Zone Server 2 (zs2.example.com) continues receiving Tanium Client content from its priority hub, Zone Server Hub 2 (ts2.example.com). The connection from Zone Server Hub 1 (ts1.example.com) to zs2.example.com remains a standby connection as long as ts2.example.com is available. The following figure illustrates this scenario.

Zone Server failover in an HA deployment



© 2026 Tanium Inc. All Rights Reserved

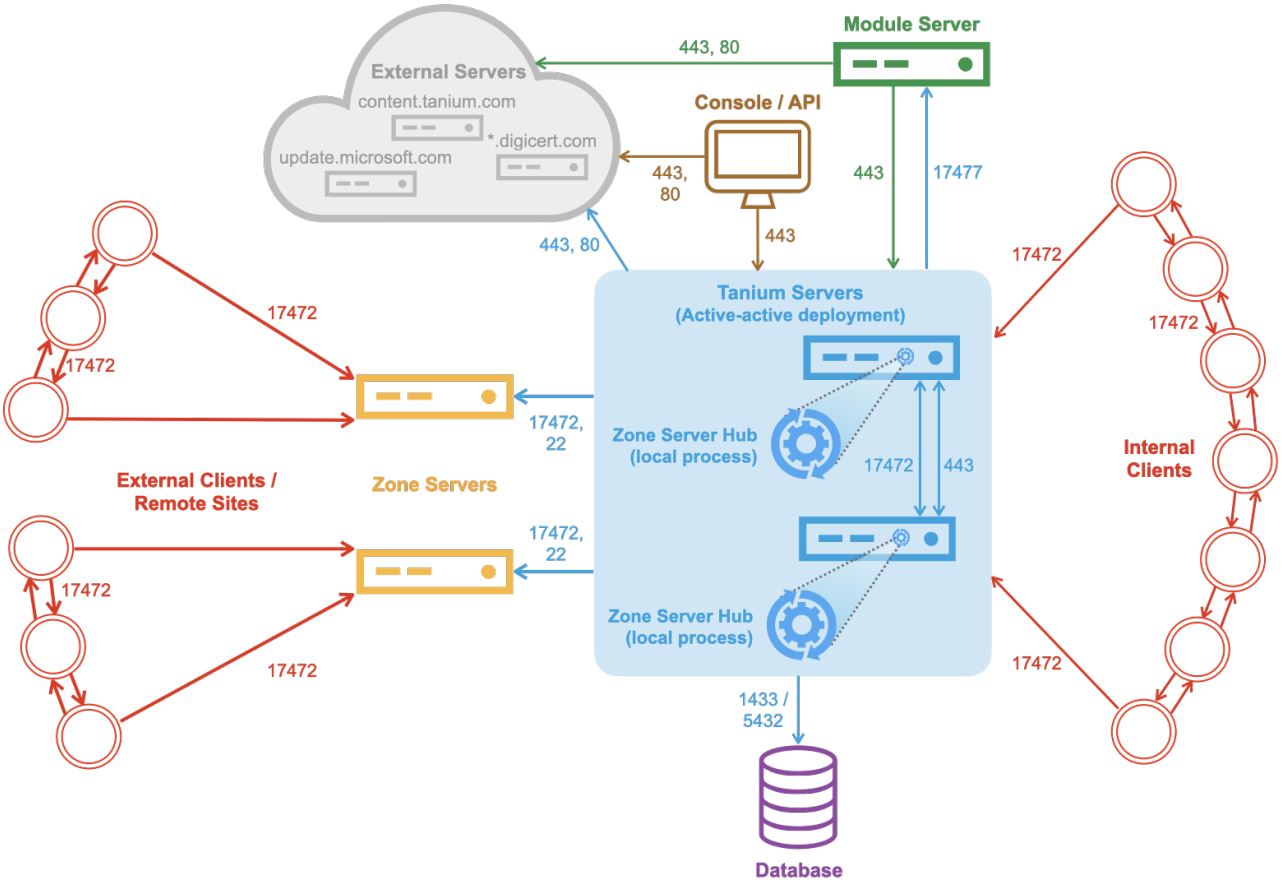
IMPORTANT

When using the Tanium Core Platform to manage external endpoints, be mindful that they might not have the same access to internal resources as internal endpoints. Target actions so that Tanium Clients on external endpoints do not attempt to access resources on the internal network, such as an Active Directory server.

Tanium Core Platform topology

In an enterprise production deployment, the Tanium Server, Tanium Module Server, and database server must reside on separate hosts, as the following figure illustrates. In a proof-of-concept (POC) deployment, these three servers reside on the same host. However, the POC architecture is intended for demonstration purposes only and does not support enterprise deployments. As a best practice, use the production environment architecture for the enterprise lab environment that you use to qualify software upgrades and test content solutions. The following figure illustrates a production or lab deployment in an HA configuration.

Enterprise production or enterprise lab deployment



BEST PRACTICE

To improve the security of the Zone Server, configure separate ports for traffic from Zone Server Hubs and Tanium Clients (see Configure ports for traffic from Zone Server Hubs and Tanium Clients).

© 2026 Tanium Inc. All Rights Reserved

NOTE

For the topology of deployments that use a proxy server between Tanium Core Platform Servers and external servers, see Tanium Console User Guide: Overview of proxy servers.

Tanium™ Direct Connect uses additional ports for communication between Tanium Clients and the Module Server. For more information, see Tanium Direct Connect User Guide: Host and network security requirements.

For more information about the port requirements of other Tanium modules and shared services, see Tanium Appliance User Guide: Network connectivity and firewall or Tanium Core Platform User Guide for Windows Deployments: Ports and firewalls.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform requirements in a Windows environment

This topic summarizes the requirements for installing Tanium Core Platform Servers.



For the host system requirements of the Tanium Client, see Tanium Client Management User Guide: Tanium Client and Client Management requirements.

Installation package and license files

Tanium provides the following installation package files and license file required to install the Tanium Server, Tanium Module Server, and Tanium Zone Server:

- `SetupServer.exe`
- `SetupModuleServer.exe`
- `SetupZoneServer.exe`
- `tanium.license`

The installation package for each of these three Servers must have the same build number (for example, if you are installing Tanium Core Platform 7.8.2.2345 on one server, you must install 7.8.2.2345 on all servers; you cannot install 7.8.2.1234 on a different Tanium Core Platform server). To complete the procedures in this guide, be sure you can copy these files to, and between, the host computers.

Download the installation package from the **Artifacts** section of your Tanium Account. For more information, see Tanium Account User Guide: View Tanium artifacts.

The license is bound to the hostname you assign to the Tanium Server. In high availability (HA) deployments, the license must specify the hostnames of both Tanium Servers. Contact Tanium Support on page 137 if the Server hostnames change.

Server version and host system requirements

The Server hardware and software requirements on page 21 table summarizes basic requirements for Tanium Core Platform and database servers that are installed on customer-provided Windows infrastructure. For detailed version specifications and sizing guidelines, see Reference: Host system resource guidelines on page 156.

Tanium solutions (modules and shared services) might have additional requirements for Tanium Core Platform Servers. The Solution-specific requirements for Tanium Core Platform Servers on page 21 table provides links to the User Guide sections that list these requirements.

© 2026 Tanium Inc. All Rights Reserved

NOTE

The Standard, Enterprise, and Datacenter editions of the following Windows Server platforms are supported. The Server Core and Nano Server options are not supported.

Server hardware and software requirements

Server	Hardware	Operating System	Software
Tanium Server	CPU cores: 8 to 80 Memory: 32 to 512 GB Disk: 250 GB to 3 TB Disk array IOPS: 2,500	• Windows Server 2022 • Windows Server 2019 • Windows Server 2016	A web browser is required to use Tanium Console: see Tanium Console User Guide: Web browser requirements.
Database Server	CPU cores: 4 to 32 Memory: 8 to 48 GB Disk: 150 GB to 750 GB Database size: 20 GB to 500 GB Disk array IOPS: 2,000	• Windows Server 2022 • Windows Server 2019 • Windows Server 2016	• Microsoft SQL Server 2019 or later • PostgreSQL Server 9.5 or later (Contact Tanium Support on page 137 for guidance on host computer specifications and PostgreSQL Server version specifications.)
Tanium Module Server	CPU cores: 8 to 80 Memory: 32 to 512 GB Disk: 150 GB to 300 GB Disk array IOPS: 2,500	• Windows Server 2022 • Windows Server 2019 • Windows Server 2016	
Tanium Zone Server	CPU cores: 8 to 80 Memory: 16 to 256 GB Disk: 250 GB to 3 TB Disk array IOPS: 2,500	• Windows Server 2022 • Windows Server 2019 • Windows Server 2016	

Click the links in the following table to see the minimum Tanium Core Platform version (Tanium dependencies) and other platform Server requirements for each Tanium module and shared service.

Solution-specific requirements for Tanium Core Platform Servers

Product	Tanium Dependencies	Server Requirements
Tanium™ Asset	Core platform dependencies	Tanium Module Server
Tanium™ Software Bill of Materials (SBOM) add-in for Asset	Core platform dependencies	No additional requirements
Tanium™ Automate	No additional requirements	No additional requirements
Tanium™ Benchmark	Core platform dependencies	Tanium Module Server

© 2026 Tanium Inc. All Rights Reserved

Solution-specific requirements for Tanium Core Platform Servers (continued)

Product	Tanium Dependencies	Server Requirements
Tanium™ Certificate Manager	Core platform dependencies	No additional requirements
Tanium™ Client Management	Core platform dependencies	• Tanium Module Server • Compatibility among components in a Tanium release
Tanium™ Cloud Workloads	Core platform dependencies	No additional requirements
Tanium™ Comply	Core platform dependencies	No additional requirements
Tanium™ Connect	Core platform dependencies	Tanium Module Server
Tanium™ Console	Core platform dependencies	Core Platform resources
Tanium™ Criticality	Core platform dependencies	Tanium Module Server
Tanium™ Deploy	Core platform dependencies	Tanium Server and Module Server
Tanium™ Direct Connect	Core platform dependencies	• Tanium Module Server • Zone proxy server requirements
Tanium™ Screen Sharing add-in for Direct Connect	No additional requirements	No additional requirements
Tanium™ Directory Query	Core platform dependencies	No additional requirements
Tanium™ Discover	Core platform dependencies	Tanium Module Server
Tanium™ Endpoint Configuration	Core platform dependencies	Tanium Module Server
Tanium™ End-User Notifications	Core platform dependencies	Tanium Module Server
Tanium™ Enforce	Core platform dependencies	Tanium Module Server

© 2026 Tanium Inc. All Rights Reserved

Solution-specific requirements for Tanium Core Platform Servers (continued)

Product	Tanium Dependencies	Server Requirements
Tanium™ Engage	Core platform dependencies	Tanium Module Server
Tanium™ Gateway	Core platform dependencies	Tanium Module Server
Tanium™ Guide	Core platform dependencies	Tanium Module Server
Tanium™ Health Check	Core platform dependencies	Tanium Module Server
Tanium™ Impact	Core platform dependencies	Tanium Module Server
Tanium™ Integrations Gallery	Core platform dependencies	No additional requirements
Tanium™ Integrity Monitor	Core platform dependencies	No additional requirements
Tanium™ Interact	Core platform dependencies	No additional requirements
Tanium™ Investigate	Core platform dependencies	Tanium Module Server
Tanium™ Network Quarantine	Core platform dependencies	Tanium Module Server
Tanium™ Patch	Core platform dependencies	Tanium Server and Module Server computer resources
Tanium™ Performance	Core platform dependencies	No additional requirements
Tanium™ Provision	Core platform dependencies	Tanium Module Server
Tanium™ Reporting	Core platform dependencies	Tanium Module Server
Tanium™ Reputation	Core platform dependencies	Tanium Module Server

© 2026 Tanium Inc. All Rights Reserved

Solution-specific requirements for Tanium Core Platform Servers (continued)

Product	Tanium Dependencies	Server Requirements
Tanium™ Reveal	Core platform dependencies	Tanium Module Server
Tanium™ Threat Response	Core platform dependencies	Tanium Module Server
Tanium™ Trends	Core platform dependencies	Tanium Module Server
Tanium™ Zero Trust	Core platform dependencies	No additional requirements

Compatibility among components in a Tanium release

Tanium™ Semiannual Release 2025H2

Tanium™ Semiannual Release 2025H2 includes new versions of the following components:

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

For version and support information, see 2025H2 release notes.

For more information about Tanium releases, see Tanium Console User Guide: Tanium releases.

Maintenance releases

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

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

© 2026 Tanium Inc. All Rights Reserved

BEST PRACTICE

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

Upgrade process

UPGRADING TANIUM CORE PLATFORM AND TANIUM SOLUTIONS

You must use the versions of Tanium Core Platform and Tanium solutions that are provided in a semiannual release together, or the later versions of each component that are provided in maintenance releases that upgrade the semiannual release. When upgrading to a new semiannual release, you must upgrade these components at the same time, beginning with Tanium Core Platform. For specific upgrade steps, see Upgrading Tanium Core Platform Servers in a Windows deployment on page 115.

IMPORTANT

- After you start the upgrade process for a new semiannual release, you cannot access Tanium solutions until you finish upgrading both the platform and solutions. Make sure to plan a maintenance window with enough time to complete all upgrades.
- As a best practice, upgrade to the latest maintenance release available for semiannual release 2025H2. Do not upgrade to a maintenance release that has an earlier release date than the currently installed maintenance release. For example, if you have a maintenance release from Februrary 1 currently installed, install a maintenance release of the 2025H2 semiannual release from February 1 or later.

UPGRADING THE TANIUM ENDPOINT CONFIGURATION TOOLSET AND TANIUM CLIENT

You deploy the Tanium Endpoint Configuration Toolset and, optionally, the Tanium Client to endpoints using the change management feature of Tanium Endpoint Configuration. For more information, see Tanium Endpoint Configuration User Guide: Managing endpoint tool upgrade rollouts. If you do not enable Client upgrades in the change management feature, or if you need to upgrade the Tanium Client in upgrade rings for which Client upgrades are not yet enabled, you must upgrade the Tanium Client on endpoints using Client Management or other means to maintain a supported configuration. For more information, see Tanium Client Management User Guide: Upgrading Tanium Clients. Tanium Semiannual Release 2025H2 supports all Tanium Client versions that the Tanium Core Platform supports. Each semiannual release supports the current endpoint configuration toolset and the two previous toolset releases.

BEST PRACTICE

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

BEST PRACTICE

Do not install the Tanium Client on the same host as a Tanium Core Platform Server. Managing Tanium Core Platform Servers as endpoints requires significantly more complex access restrictions in Tanium. Tanium users with management rights over Tanium Core Platform Servers might be able to circumvent access restrictions within Tanium or inadvertently deploy actions that interfere with Tanium functionality. If you choose to install the

© 2026 Tanium Inc. All Rights Reserved

BEST PRACTICE

Client on Tanium Core Platform Server machines, you must carefully restrict access to computer groups that include Tanium Core Platform Servers, such as `All Computers`, `All Servers`, and `All Windows`. You cannot use Tanium Client Management to install the Client on the Tanium Module Server.

Internet access, network connectivity, and firewalls

Internet Protocol (IP) support

All supported versions of the Tanium Core Platform use TCP/IP to communicate over IPv4 and IPv6 networks. Contact Tanium Support on page 137 if you need IPv6 support. You must work with your network administrator to ensure that the Tanium components are provisioned with IP addresses and can use DNS to resolve host names.

Internet URLs

During installation and ongoing operations, the Tanium Server and the web browser that you use to access Tanium Console must connect to the following URLs to import updates to Tanium Core Platform components and modules:

- `https://content.tanium.com`
- `http://*.digicert.com`

  Module imports fails if the Certificate Revocation List is blocked or inaccessible.

If your enterprise network uses SSL intercept technologies, such as man-in-the-middle (MITM) proxies, you must configure them so that they do not prevent the Tanium Server and Tanium Module Server from downloading files from these locations.

If your enterprise security policy does not allow the Tanium Server to access these locations directly, you can use proxy servers. For more information, see Configuring proxy server settings.

NOTE

You must also enable Tanium Clients to download files from Internet URLs to run certain sensors and packages. For more information, see Tanium Console User Guide: Managing allowed URLs.

The Tanium Server might need to connect to additional URLs based on the solutions you import. For the required URLs for each solution, see the following links:

- Asset
- Deploy
- Discover
- Direct Connect
- Enforce
- Health Check

© 2026 Tanium Inc. All Rights Reserved

- Patch
- Provision
- Reputation

Server throughput and latency

The Tanium Server must be able to connect to the Tanium database server and Module Server. In an HA deployment, the Tanium Servers must be able to connect to each other over a reliable Ethernet connection. All these connections require a minimum throughput of 1 Gbps and a maximum round-trip latency of 30 ms.

Proxy server

If your enterprise network environment requires outbound Internet connections to traverse a proxy server, you can configure the proxy settings as described under Tanium Console User Guide: Configuring proxy server settings.

Ports and firewalls

The following table summarizes the Tanium processes and default values for ports used in Tanium Core Platform communication. Host and network firewalls might require configuration to allow the specified processes to send and receive TCP data over the listed ports. The Tanium installer opens required ports in the Windows host firewall. You must work with your network security administrator to ensure the platform components can communicate through any security barriers (such as firewalls) in their communication path. Your security administrator might also need to create rules to exempt or exclude Tanium processes that run on the host computers from blocking by antivirus or processing by encryption or other security and management stack software. For more information, see Tanium Core Platform Server security exclusions on page 160.



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.

Network communication ports used by Tanium Core Platform components

Source	Destination	Port	Protocol	Purpose
All Tanium Core Platform servers	update.microsoft.com	80, 443	TCP	Download and install updates to Windows Server
Console/API users	content.tanium.com *.digicert.com	443	TCP	Download and install solutions to the Tanium Core Platform
Console/API users	Tanium Servers	443	TCP	Tanium Console/API user workstation (browser) communication with Tanium Servers
Module Servers	Tanium Servers	443	TCP	Module Server communication with Tanium Servers

© 2026 Tanium Inc. All Rights Reserved

Network communication ports used by Tanium Core Platform components (continued)

Source	Destination	Port	Protocol	Purpose
Module Servers	Zone Servers[1]	17487	TCP	Used by Zone Servers for Module Server connections using Direct Connect. The default port number is `17487`. If needed, you can specify a different port number when you configure the zone proxy.
		17488	TCP	Used by the Module Server to provision the Zone Proxy on the Zone Server. After the Zone Proxy is provisioned, used for connection status and diagnostics. This port number is not configurable.
Tanium Clients	Tanium Clients Tanium Servers Zone Servers	17472	TCP	Communication between Tanium Clients (`TaniumClient.exe`), communication between the Clients and the Tanium Servers or Zone Servers
Tanium Clients (external)	Zone Servers[1]	17486	TCP	Used by Zone Servers for endpoint connections to external Clients using Direct Connect. The default port number is `17486`. If needed, you can specify a different port number when you configure the zone proxy.
Tanium Clients (internal)	Module Servers	17475	TCP	Used by the Module Server for endpoint connections to internal Clients using Direct Connect.
Tanium Servers	LDAP servers	389, 636	TCP	(Optional) External LDAP communications for Tanium Console authentication
Tanium Servers	Module Servers	17477	TCP	Tanium Server communication with Module Servers
Tanium Servers	Tanium database	1433, 5432	TCP	Tanium Server communication with the Tanium database: SQL server (`Sqlservr.exe`) or PostgreSQL server (`postgres.exe`)
Tanium Servers	Tanium Servers	443, 17472	TCP	Communication between active-active Tanium Servers
Tanium Servers, Module Servers	content.tanium.com *.digicert.com	443	TCP	Tanium Server (`TaniumReceiver.exe`) or Module Server (`TaniumModuleServer.exe`) communication with content.tanium.com to import updates to Tanium Core Platform components and modules
Zone Server Hub	Zone Servers[1]	17472	TCP	Zone Server Hub (`TaniumZoneServer.exe`) communication with Zone Servers (`TaniumZoneServer.exe`)

[1] These ports are required only when you use a Zone Server.

BEST PRACTICE

To improve the security of the Zone Server, configure separate ports for traffic from Zone Server Hubs and Tanium Clients. For more information, see Configure ports for traffic from Zone Server Hubs and Tanium Clients.

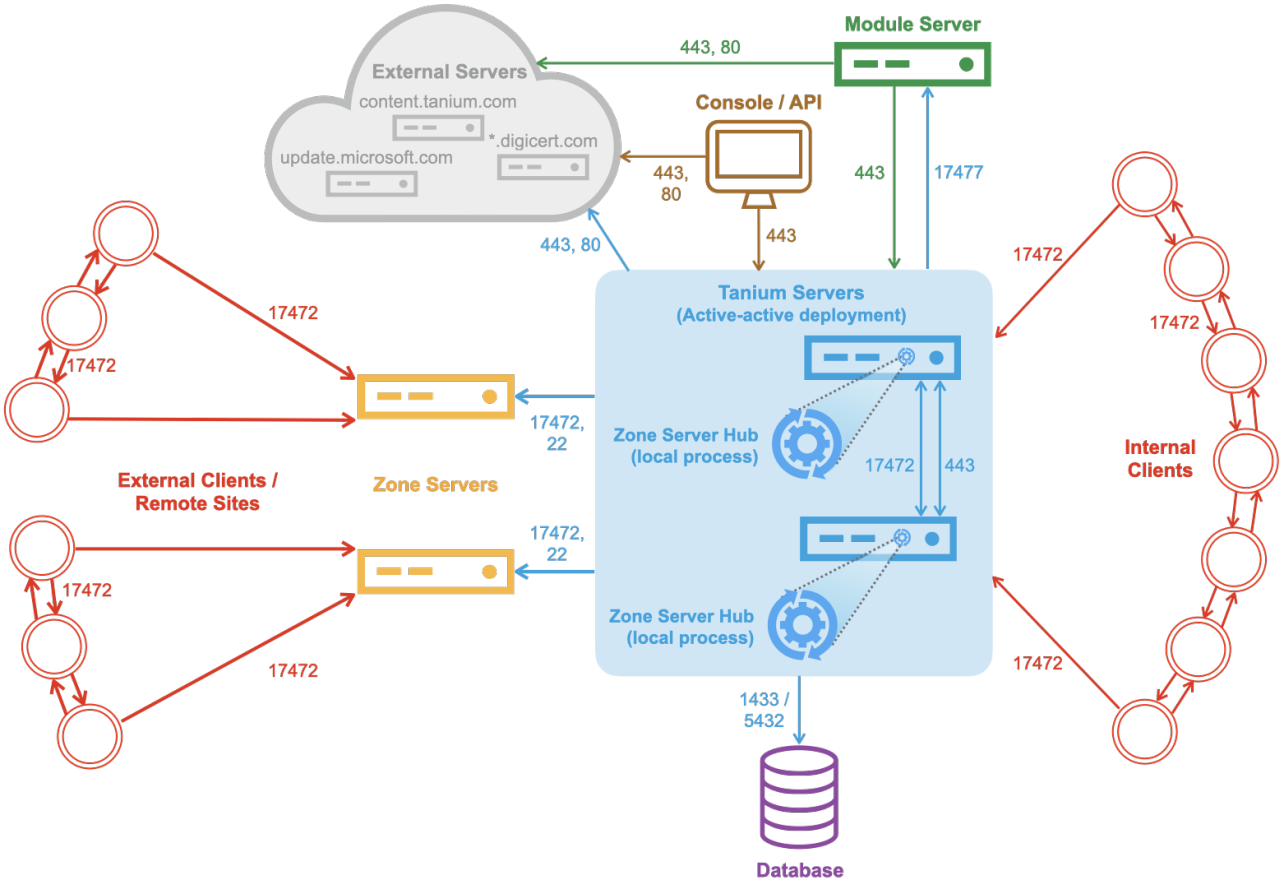
© 2026 Tanium Inc. All Rights Reserved

NOTE

Do not allow a Tanium Server, a Module Server, or a Zone Server Hub to accept inbound connections from the internet. On a Zone Server, allow only the Tanium Client port to accept inbound connections from the internet.

The following figure illustrates how the Tanium Core Platform uses ports in an active-active deployment with Windows infrastructure:

Network communication ports



NOTE

- For the topology of deployments that use a proxy server between Tanium Core Platform Servers and external servers, see Tanium Console User Guide: Overview of proxy servers.
- Tanium™ Direct Connect uses additional ports for communication between Tanium Clients and the Module Server. For more information, see Tanium Direct Connect User Guide: Host and network security requirements.
- For the ports that Tanium Client Management requires for deployment of Tanium Client, see Tanium Client Management User Guide: Network connectivity, ports, and firewalls.

© 2026 Tanium Inc. All Rights Reserved

To see additional port requirements that are specific to modules and shared services, click the following links to access the associated user guides:

- Asset
- Automate: No additional port requirements
- Benchmark
- Certificate Manager: No additional port requirements
- Client Management
- Cloud Workloads: No additional port requirements
- Comply
- Connect
- Criticality
- Deploy
- Direct Connect
- Directory Query
- Discover
- Endpoint Configuration
- End-User Notifications
- Enforce
- Engage
- Gateway
- Guide
- Health Check
- Impact
- Integrations Gallery
- Integrity Monitor
- Interact
- Investigate
- Patch
- Performance
- Provision
- Reporting

© 2026 Tanium Inc. All Rights Reserved

- Reputation
- Reveal
- Threat Response
- Trends
- Zero Trust

SSL/TLS certificates

SSL/TLS certificate and key exchanges secure connections to the Tanium™ Console or Tanium™ API, as well as connections between the Tanium Server and Tanium Module Server. When you run the Server installation wizards, they prompt you to generate a self-signed certificate or specify the location of a certificate that was issued by a commercial certificate authority (CA) or your own enterprise CA.



To facilitate troubleshooting, use the self-signed certificates during initial installation and replace them with CA-issued certificates later. This practice enables you to separate potential installation issues from TLS connection issues.

For more information, see Securing Tanium Console, API, and Module Server access in a Windows deployment on page 77.

Administrator account permissions

Work with your Microsoft Active Directory (AD) administrator to provision the accounts needed during Tanium Core Platform installations or upgrades and for post-installation or post-upgrade activities. To change accounts or update their passwords, see Tanium Console User Guide: Windows service accounts.

Administrator accounts for installations and upgrades

The following table lists the administrator accounts required to install or upgrade Tanium Core Platform Servers, create Tanium databases, or deploy Tanium Clients. You can use a single service account to install the Tanium Server and to create databases on the SQL or PostgreSQL server, as long as the account has the all required group memberships and permissions for those servers. You can also use a single service account to install the Zone Server and Zone Server Hub. You must use a separate service account to install the Module Server.

© 2026 Tanium Inc. All Rights Reserved

Administrator account permissions required for installations and upgrades

Service	Account Type	Host System	Required Group or Permissions	Account Purpose
Tanium Server and Tanium databases	AD service account*	Tanium Server host	Administrator, interactive sign in	This service account installs and upgrades the Tanium Server software.
		SQL Server host	Sysadmin on the SQL instance	When running the installer from the Tanium Server, this service user connects remotely to the SQL Server and creates the **tanium** and **tanium_archive** databases.
		PostgreSQL Server host	Administrator	When running the installer from the Tanium Server, this service user connects remotely to the PostgreSQL Server and creates the **tanium** and **tanium_archive** databases.
Tanium Module Server	AD service account*	Tanium Module Server host	Administrator	This service account installs and upgrades the Tanium Module Server software.
Tanium Zone Server and Zone Server Hub	Local user or AD	Tanium Zone Server host	Administrator, interactive sign in	This service account installs and upgrades the Tanium Zone Server software.
		Tanium Zone Server Hub host	Administrator, interactive sign in	This service account installs and upgrades the Tanium Zone Server Hub software.

*You can use the LocalSystem account in a POC deployment, but not in a production deployment.

Administrator accounts for post-installation/upgrade activities

The following table lists the administrator accounts required for regular, ongoing operations performed after installations or upgrades, including running the services for Tanium Core Platform Servers and Tanium Clients, and accessing Tanium databases. If you reuse the accounts used for installations and upgrades, first reduce the account permissions to those specified in the following table. You can use a single service account to run the Tanium Server service and access the Tanium databases. You can also use a single service account to run the Zone Server and Zone Server Hub services. You must use a separate service account to run the Module Server service.

© 2026 Tanium Inc. All Rights Reserved

Administrator account permissions required for post-installation/upgrade activities

Service	Account Type	Host System	Required Group or Permissions	Account Purpose
Tanium Server and Tanium databases	AD service account*	Tanium Server host	User-level permissions	This service account runs the Tanium Server service. The service runs in the context of the Local System or the AD account, depending on the option you select when installing the Server.
		SQL Server host	DBO on Tanium databases	This service user account accesses the **tanium** and **tanium_archive** databases. If you use the same account for running the Tanium Server service, the account must be able to connect remotely to the SQL Server. The account requires **db_owner** role membership for the Tanium databases. Assign the View Server state permission as a best practice to enable the Tanium Server to access data faster than the DBO role alone.
		PostgreSQL Server host	User-level permissions	This service user account accesses the **tanium** and **tanium_archive** databases. If you use the same account for running the Tanium Server service, the account must be able to connect remotely to the PostgreSQL Server.
Tanium Module Server	AD service account*	Tanium Module Server host	Administrator	This service account runs the Tanium Module Server service. The service runs in the context of the Local System account.
Tanium Zone Server and Zone Server Hub	Local user or AD	Tanium Zone Server host	User-level permissions	This service account runs the Tanium Zone Server service. The service runs in the context of the Local System or the AD account, depending on the option you select when installing the Server.
		Tanium Zone Server Hub host	User-level permissions	This service account runs the Tanium Zone Server Hub service. The service runs in the context of the Local System or the AD account, depending on the option you select when installing the Server.

*You can use the LocalSystem account in a POC deployment, but not in a production deployment.

© 2026 Tanium Inc. All Rights Reserved

Installing the Tanium Server

This topic describes how to install a standalone Tanium Server on a dedicated Windows Server host. For more information about the Tanium Server and its deployment options, see Tanium Server on page 13. To install Tanium Servers in a high availability (HA) deployment, see Installing Tanium Servers in an active-active HA cluster on page 72.

The Tanium Server installer performs the following actions:

- Installs any necessary database tools, such as Microsoft SQL Server client tools and utilities.
- Creates the Tanium databases on a remote database server and initializes the database tables in those databases.
- Opens required ports in the local host computer Windows Firewall.
- Installs the Tanium Server on the local host computer and starts the Tanium Server service. The service starts the application server that hosts Tanium Console. The certificate and private key that you specify during installation establish Hypertext Transfer Protocol Secure (HTTPS) access to Tanium Console and the Tanium API.

Before you begin

Ensure that you meet the following requirements before installing the Tanium Server:

- **Installer**: Ensure that you have the correct version of the installer (`SetupServer.exe`) and that you can access it. The installation package for all Tanium Core Platform servers must have the same build number (for example, if you are installing Tanium Core Platform 7.8.2.2345 on one server, you must install 7.8.2.2345 on all servers; you cannot install 7.8.2.1234 on a different Tanium Core Platform server). Download the installation package from the **Artifacts** section of your Tanium Account. For more information, see Tanium Account User Guide: View Tanium artifacts.
- **Tanium license**: Ensure that you can access the Tanium license file: `tanium.license`.
- **Host requirements**: The host systems for the Tanium Server and database server must meet the hardware, software, and network connectivity requirements suitable for your deployment: see Tanium Core Platform requirements in a Windows environment on page 20, Resource requirements on page 156, and SQL server host system on page 158 or PostgreSQL server host system on page 157.
- **Network accessibility**: Ensure that the host system for the Tanium Server has a fully qualified domain name (FQDN) that is accessible from any computer from which a user will access Tanium Console.
- **User accounts**: Your Microsoft Active Directory administrator must configure the accounts that your team needs for the Tanium Core Platform deployment: see Administrator account permissions on page 31.
- **Firewall rules**: Your network administrator must configure firewall rules to allow communication on the TCP ports that the Tanium Core Platform uses: see Internet access, network connectivity, and firewalls on page 26.
- **Security exclusions**: Your security team must configure exceptions to host-based security policies to allow Tanium processes to operate smoothly and at optimal performance: see Tanium Client Management Guide: Reference: Endpoint security exclusions and for Windows-based Tanium Core Platform deployments, see Tanium Core Platform User Guide for Windows Deployments: Tanium Core Platform Server security exclusions.

© 2026 Tanium Inc. All Rights Reserved

- **Certificates and keys**: If you want to use a certificate issued by a certificate authority (CA) for securing connections from user systems to the Tanium Server for Tanium Console or API access, ensure that the CA-issued certificate and associated private key are present on the Tanium Server. The certificate file name must be `SOAPServer.crt` and the key file name must be `SOAPServer.key`. During installation, you can select a CA-issued certificate or configure the Tanium Server to generate a self-signed certificate.

  To facilitate troubleshooting, use the self-signed certificate during initial installation and replace it with a CA-issued certificate later. This practice enables you to separate potential installation issues from TLS connection issues.

  For more information, see Securing Tanium Console, API, and Module Server access in a Windows deployment on page 77.

- **Database server**: Your database administrator must create a database server for the Tanium Core Platform deployment: see Set up a database server on page 35.

- **Secondary Logon service**: The Windows Secondary Logon service (seclogon) on the host computer for the Tanium Server must have its **Startup type** set to **Automatic** or **Manual** (not **Disabled**) during installation of the Tanium Server . If the Secondary Logon service is disabled, the installation cannot connect to the database server (even if it is being installed locally), and the installation of the Tanium database fails. The Secondary Logon service is required only during installation and upgrades.

If you are upgrading from Tanium Core Platform 7.5.6 or earlier to a semi-annual release for the first time (including Tanium Core Platform 7.6.2 or later), upgrade all solutions before you install the release bundle that includes Tanium Core Platform 7.6.2 or later. For information about upgrading solutions, see Tanium Console User Guide: Import, re-import, or update specific solutions. When you upgrade to subsequent semi-annual releases, a separate upgrade of solutions is not necessary or possible. You can optionally use the change management feature in Endpoint Configuration to manage a staged rollout of the endpoint tools that enable upgraded solution functionality on endpoints. For more information, see Endpoint Configuration User Guide: Managing Tanium Client and endpoint tool upgrade rollouts.

Set up a database server

Before installing the Tanium Server, your database administrator must set up a database server for the Tanium Core Platform deployment. The Tanium Server installer creates the Tanium database on this server. In production deployments, the database must run on a standalone server that allows remote connections from the Tanium Server. In a proof-of-concept (POC) deployment, you can install the Tanium database locally on the Tanium Server.



In an HA deployment, the Tanium Servers share the Tanium database. Therefore, even if the database is local to one Tanium Server, the peer Tanium Server must connect to it remotely.

© 2026 Tanium Inc. All Rights Reserved

Create and configure the database server

1. Choose the database type, Microsoft SQL (MSSQL) or PostgreSQL, and create the database server. For information about creating the server, see the MSSQL or PostgreSQL documentation.

   IMPORTANT

   Contact Tanium Support on page 137 first if you want a PostgreSQL server. A special distribution of PostgreSQL Server is required.

   BEST PRACTICE

   By default, the connection between the Tanium Server and standalone database server is not encrypted, but configuring encryption is a best practice.

2. Configure a privileged domain administrator account that you can use to create the Tanium databases when you run the installer: see Administrator account permissions on page 31.

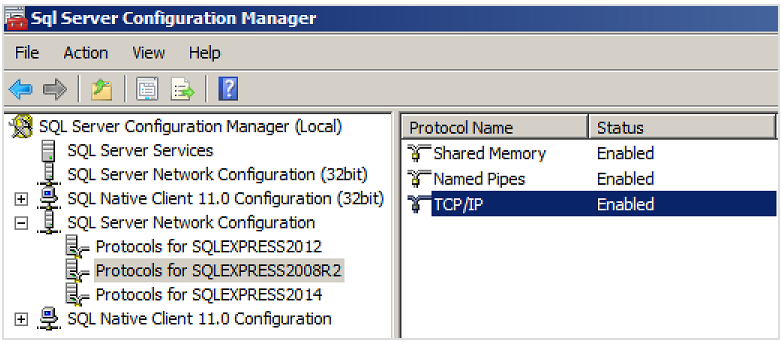
3. (SQL server only) Configure the SQL instance to allow remote connections:

   a. Sign in to the database server as an administrator.

   b. Open the **SQL Server Configuration Manager** program.

   c. In the navigation pane, open the **SQL Server Network Configuration** node and select the protocols for your database instance (for example, **Protocols for SQLEXPRESS2012**).

   d. In the display pane, right-click **TCP/IP** and select **Enable**.



4. (SQL server only, best practice) Install the **Microsoft SQL Server Management Studio** program on the Tanium Server host computer.

   Microsoft SQL Server Management Studio is optional, but most administrators find it useful to verify database transactions and to manage the databases. If you install **Microsoft SQL Server Management Studio** before you run the installer, the installer does not prompt you to download and install the Microsoft SQL Server utilities (see SQL Command Line Utilities Not Found on page 38).

© 2026 Tanium Inc. All Rights Reserved

Manage the Tanium database collation mode

The Tanium Server installer creates the Tanium database with the default collation mode of your database server. The collation mode controls which characters are available to use in the names (identifiers) of configuration objects, such as computer groups or sensors. Be sure to set a default collation mode that allows all the characters that you plan to use for object names. Some collations do not support Supplemental Unicode characters beyond the Basic Multilingual Plane. The following steps describe how to set the collation mode on an SQL server:

1. Sign in to the Tanium Server as an administrator.
2. Open the **Microsoft SQL Server Management Studio** program.
3. In the navigation pane, right-click the **tanium** database and select **Properties**.
4. In the **Select a page** section, select **Options**.
   The **Collation** drop-down list shows the current collation mode.
5. If necessary, select a new **Collation** and click **OK**.

Install the Tanium Server

1. Sign in to the host system as a local administrator or domain user with administrator permissions.
2. Copy the installer (`SetupServer.exe`) and license to a temporary location.
3. Right-click the installer and select **Run as administrator**.
4. Complete the installation wizard. The following table provides guidelines for key settings.

Tanium Server installation wizard settings

Settings	Guidelines
Database Server Type	Select the type of database to use: • **PostgreSQL Server** Install a remote (production deployments) or local (proof-of-concept (POC) deployments) database server and utilities. • **Microsoft SQL Server** The installer displays additional pages for selecting database server and client utilities options.

© 2026 Tanium Inc. All Rights Reserved

Tanium Server installation wizard settings (continued)

Settings	Guidelines
Postgres Not Found	If you set the **Database Server Type** to **PostgreSQL Server** and the installer cannot find a local PostgreSQL Server installation, the following options appear: • **Install and configure local Postgres Server.** This option supports only POC deployments. • **Use remote Postgres Server.** This option supports production deployments. • **Exit the installer now.** Select this option if you are not ready to make the connection to the remote PostgreSQL Server.
SQL Command Line Utilities Not Found	If you set the **Database Server Type** to **Microsoft SQL Server** and the installer cannot find a local SQL Server installation and SQL utilities, the following options appear: • **Download and Install SQL 2012 Native Client and SQL 2012 Command Line Utilities now.** Select this option to install the utilities necessary to connect to a remote SQL server and create databases. If you select this option, and the Tanium installer detects that these utilities are already present on the host system, it does not overwrite the existing installation; it simply does not call the Microsoft installer for the utilities. • **Download and Install SQL Server 2014 SP2 Express Edition with Tools now.** Select this option only for limited, proof-of-concept (POC) deployments. • **Exit the installer now. (Download and install manually)** Select this option if you want to install the utilities yourself. After you have done so, if you re-run the Tanium installer, you can select the first option, and the Tanium installer will verify that the utilities are present and not call the Microsoft installer.  SQL Server 2014 SP2 Express takes substantially longer to download than SQL 2012 Native Client. Therefore, if you plan to use a remote database server, select **Download and Install SQL 2012 Native Client and SQL 2012 Command Line Utilities now** or download the files from Microsoft using the links that the installation wizard provides.
Choose type of installation	• **Custom Install**: Select this option for production deployments. • **Express Install**: Select this option only for limited, POC deployments.

© 2026 Tanium Inc. All Rights Reserved

Tanium Server installation wizard settings (continued)

Settings	Guidelines
Choose Service Account for Tanium Server and Database Access	**Specify Account** This option is required for production deployments. Specify a service account that can connect to the remote database server and has permissions to create databases. The account you specify will also run the Tanium Server service on the local host computer. Specify the following details: • **User Name**: Enter only the account name portion of the credentials, such as `taniumsvc`. • **Domain**: Enter the domain name, such as `example.com`. • **Password**: Enter the account password.
	Local System Account This option is supported only if you set the **Database Server Type** to **Microsoft SQL Server** and you are setting up a limited POC deployment where the Tanium Server and database server are on the same local host system.
Choose Install Location	The default is `C:\Program Files\Tanium\Tanium Server`.  For additional security in enterprise production deployments, install the Tanium Server on a non-system hard drive.
License Configuration	Click **Browse**, navigate to the directory where you copied the Tanium license file (`tanium.license`), select the file, and click **Open**.
Key Database Restoration	The Tanium Server uses a `pki.db` file to store the Tanium root keys and subordinate keys that are required for TLS communication among Tanium Core Platform components (see Managing Tanium keys). Select the source for this file: • **Generate a new key database**: The Tanium Server creates a new `pki.db` file. • **Restore a key database from backup**: If you saved the `pki.db` file from a previous installation of this Tanium Server, copy it to a temporary location on the current server host, click **Browse**, select the file, and click **Open**. Note that you must also restore the Tanium database associated with the backup `pki.db` file to enable Tanium Clients to connect to that Tanium Server. The installer puts the `pki.db` file in the Tanium Server installation folder.
Server Console/API Port	Specify the Tanium Server inbound port for traffic from Tanium Console and the Tanium API. The default is 443.

© 2026 Tanium Inc. All Rights Reserved

Tanium Server installation wizard settings (continued)

Settings	Guidelines
SSL Certificate and Key	The Tanium Server uses the SSL/TLS certificate (`SOAPServer.crt`) and private key (`SOAPServer.key`) to secure communication with Tanium Console or API users and communication with the Module Server. • **Generate Self-Signed Certificate and Key** If you select this option, the installer generates a self-signed certificate and private key. For the **Server Host Name**, specify the FQDN of the Tanium Server. For example, `ts1.example.com` or `ts1.example.com`. If you are deploying an HA pair, specify the FQDN for both Servers, separated by a comma (no spaces). For example, `ts1.example.com,ts2.example.com`. • **Use Existing Certificate and Key** To use a CA-issued certificate, select the certificate file and associated private key file. For more information, see Securing Tanium Console, API, and Module Server access in a Windows deployment on page 77.
Server Port	Specify the Tanium Server inbound port for traffic from Tanium Clients that are in the internal network. The default is 17472.
SQL server and database	If you set the **Database Server Type** to **Microsoft SQL Server**, you have the following options: • **Use Local Database** This option is supported only for POC deployments. When SQL Server is installed on the local host computer, you can select a database server from the **Local Instance** list box. • **Use Remote Database** Select this option and specify the path to the remote database server in the **Remote SQL Path** field. In most cases, the syntax is *<hostname>\<database instance name>*, such as `SQL1\SQLEXPRESS`. However, if you use both the default SQL instance name (MSSQLSERVER) and default port (1433), the syntax is just *<hostname>*. Click **Test** to test the connection. If the SQL Server listens on a custom-assigned port (not 1433), specify the port in the **Remote SQL Path**. For example, `SQL1\SQLEXPRESS,1444`.

© 2026 Tanium Inc. All Rights Reserved

Tanium Server installation wizard settings (continued)

Settings	Guidelines
Postgres Configuration	If you set the **Database Server Type** to **PostgreSQL Server**, specify the following settings: • **Server Port**: The default is 17472. • **Server**: Specify `localhost` (default) for a local server, or the FQDN or IP address of the remote server. You must enter IPv6 addresses within square brackets (for example, [2001:db8::1]). • **Options**: Specify additional parameters to pass in the connection. Typically, this is dbname and port. For example, `dbname=postgres port=5432 user=postgres`. Click **Test** to test the connection.
Install local Tanium Module Server	Select this option only if you are installing a POC deployment in which the Tanium Server and Module Server run on the same host system.
Open Tanium Ports in Windows Firewall	Select this option to open Tanium Server ports in the Windows Firewall. Ports 443 and 17472 are the default port numbers.
Set Administrator Account	(Fresh installation only) Set the **Username** and **Password** for the initial Tanium Console administrator account. This is the account that you will use when you first sign in to the Console. Subsequently, you can create additional users. For Active Directory accounts, use DOMAIN\username or UPN format. For example, `TAM\TaniumAdmin` or `TaniumAdmin@TAM`. For local accounts, use MACHINE\username syntax.
Choose Start Menu Folder	(Fresh installation only) Select a folder for the Tanium Server in the Windows **Start** menu. The default is `Tanium Server`.

Relocate the package file repository

The Tanium Server downloads package files that are associated with actions and stores them in the `<Tanium Server installation directory>\Downloads` directory by default. Optionally, you can change the directory if another drive on the server has better resources for storing package downloads.

To monitor repository usage and manually clear expired files, see Tanium Console User Guide: Manage the package file repository.

1. Create the new package downloads directory (such as `E:\Tanium\Downloads`) if it does not already exist.
2. Verify that the Tanium Server and Tanium database are properly backed up. For more information, see Back up Tanium Core Platform Servers and databases on page 124.
3. Sign in to the Tanium Server host as the **Administrator** user.
4. Open the Windows **Services** program, right-click the **Tanium Server** service, and select **Stop**.

© 2026 Tanium Inc. All Rights Reserved

5. Copy all the files and subdirectories from `<Tanium Server installation directory>\Downloads` to the new directory.
6. Open a **Command Prompt** and navigate to the Tanium Server installation directory:

   ```
   cd <installation directory>
   ```

7. Configure the Tanium Server to use the new package downloads directory:

   ```
   TaniumReceiver config set-string DownloadPath <downloads directory>
   ```

8. Open the Windows **Services** program, right-click the **Tanium Server** service, and select **Start**.
9. Verify that the Server uses the new directory for package downloads:
   a. Sign in to Tanium Console as a user who is assigned the **Administrator** reserved role.
   b. From the Main menu, go to **Administration > Configuration > Package File Repository**.
   c. Verify that the **Download Cache Folder Path** shows the new directory.
10. Remove the original `Downloads` directory from the Tanium Server.

Next steps

1. Install the remote Module Server. For more information, see Installing the Tanium Module Server on page 43.
2. (Optional) Integrate the Tanium Server with a hardware security module (HSM) if your organization uses an HSM to store and manage digital keys. For more information, see Securing keys with an HSM in a Windows deployment on page 110.

© 2026 Tanium Inc. All Rights Reserved

Installing the Tanium Module Server

This topic describes how to install a Tanium Module Server on a dedicated Windows Server host. For more information about the Module Server and its deployment options, see Tanium Module Server on page 14.

The Module Server installer performs the following actions:

- Opens TCP port 17477 in the local host computer Windows Firewall.
- Installs the Module Server on the host computer and starts the service.

If possible, run the installer and specify connection settings to automatically register with the Tanium Server. Otherwise, complete the manual registration workflow.

Install and automatically register the Module Server

The Module Server installer supports automatic registration with the Tanium Server. Automatic registration performs the following tasks:

- Generates required certificates: `trusted.crt` on the Module Server host and `trusted-module-servers.crt` on the Tanium Server host. The Servers use these certificates to validate the certificates used for mutual authentication: `SOAPServer.crt` on the Tanium Server and `ssl.crt` on the Module Server. For more information, see Securing Tanium Console, API, and Module Server access in a Windows deployment on page 77.
- Creates required Windows Registry entries on both the Module Server and Tanium Server host computers.

Before you begin

Ensure the following prerequisites are met and take the following actions:

- **Installer version**: Ensure that you have the right version of the installer (`SetupModuleServer.exe`). The installation package for all Tanium Core Platform servers must have the same build number (for example, if you are installing Tanium Core Platform 7.8.2.2345 on one server, you must install 7.8.2.2345 on all servers; you cannot install 7.8.2.1234 on a different Tanium Core Platform server). Download the installation package from the **Artifacts** section of your Tanium Account. For more information, see Tanium Account User Guide: View Tanium artifacts.
- **Host requirements**: The host system must meet the hardware, software, and network connectivity requirements suitable for your deployment: see Tanium Core Platform requirements in a Windows environment on page 20 and Resource requirements on page 156.
- **Firewall rules**: Your network security administrator must configure network firewall rules to allow communication between the Tanium Server and Module Server on TCP port 17477: see Internet access, network connectivity, and firewalls on page 26.

© 2026 Tanium Inc. All Rights Reserved

- **Security exclusions**: Your security team must configure exceptions to host-based security policies to allow Tanium processes to operate smoothly and at optimal performance: see Tanium Client Management Guide: Reference: Endpoint security exclusions and for Windows-based Tanium Core Platform deployments, see Tanium Core Platform User Guide for Windows Deployments: Tanium Core Platform Server security exclusions.
- **Certificates and keys**: If you want to use a certificate issued by a certificate authority (CA) to secure connections to the Module Server, ensure that the CA-issued certificate and associated private key are present on the Module Server. The certificate file name must be `ssl.crt` and the key file name must be `ssl.key`. During installation, you can select a CA-issued certificate or configure the Module Server to generate a self-signed certificate.

  As a best practice to facilitate troubleshooting, use the self-signed certificate during initial installation and replace it with a CA-issued certificate later. This practice enables you to separate potential installation issues from TLS connection issues.

  For more information, see Securing Tanium Console, API, and Module Server access in a Windows deployment on page 77.
- **Secondary Logon service**: The Windows Secondary Logon service (seclogon) on the host computer for the Tanium Module Server must have its **Startup type** set to **Automatic** or **Manual** (not **Disabled**) during installation of the Tanium Module Server . If the Secondary Logon service is disabled, the installation cannot connect to the database server (even if it is being installed locally), and the installation of the Tanium database fails. The Secondary Logon service is required only during installation and upgrades.
- **Local Module Server**: If a local Module Server is installed on the Tanium Server host computer, perform the following steps on the Tanium Server host computer:
  1. Stop the **Tanium Server** service: open the Windows **Services** application, right-click **Tanium Server**, and select **Stop**.
  2. Stop and disable the **Tanium Module Server** service in the Windows **Services** application:
     a. Right-click **Tanium Module Server** and select **Stop**.
     b. Right-click **Tanium Module Server**, select **Properties**, set the **Startup type** to **Disabled**, and click **OK**.
  3. Go to the Windows Registry `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Tanium\Tanium Server` and clear the setting (value `127.0.0.1`) for the Module Server.
  4. Restart the **Tanium Server** service: in the Windows **Services** application, right-click **Tanium Server**, and select **Restart**.

Run the installer

1. Sign in to the Module Server host system as an administrator user.
2. Copy the installer (`SetupModuleServer.exe`) to a temporary location on the Module Server host.
3. Right-click `SetupModuleServer.exe` and select **Run as administrator**.
4. Complete the installation wizard. The following table provides guidelines for key settings.

© 2026 Tanium Inc. All Rights Reserved

Tanium Module Server installation wizard settings

Settings	Guidelines
Choose Install Location	The default is `C:\Program Files\Tanium\Tanium Module Server`.
Postgres Not Found	(Fresh installation only) If the installer does not detect an existing installation of PostgreSQL, you can either install a local instance or configure a connection to an external instance. IMPORTANT: Even if you connect the Module Server to a remote PostgreSQL instance, you must keep a local instance installed on the Module Server. The Tanium™ Relational Database (RDB) service always requires certain binaries to exist in the local instance, although you can stop the instance from running. • **Install and configure local Postgres Server**: Install the default local instance of PostgreSQL. You can select this option to install a local instance that provides the binaries that the Tanium RDB service requires and still configure a connection to a remote PostgreSQL server. You configure the remote connection in a separate step in the installation wizard. • **Use remote Postgres Server**: Select this option if you want to connect to an external instance of PostgreSQL, and you do not want installer to install a local instance of PostgreSQL. You configure the remote connection in a separate step in the installation wizard. You must install a local instance of PostgreSQL separately, and you must follow the steps in (Optional) Configure a connection between the Module Server and a remote PostgreSQL database on page 51 to configure `external_db.json`. TIP: To troubleshoot issues related to the default PostgreSQL installation, see PostgreSQL installation log on page 146.

Choose Service Account for Tanium Module Server	The security best practice is to specify a service account other than the Local System account to install the Module Server and run the Module Server service on the local host computer.
	
	• **Specify Account** (best practice)
	  ◦ **User Name**: Enter only the account name portion of the credentials, such as `taniumsvc`.
	  ◦ **Domain**: Enter the domain name, such as `example.com`.
	  ◦ **Password**: Enter the account password.
	• **Local System Account**

Module Server Port	Specify the Module Server inbound port for traffic from the Tanium Server. The default is 17477.

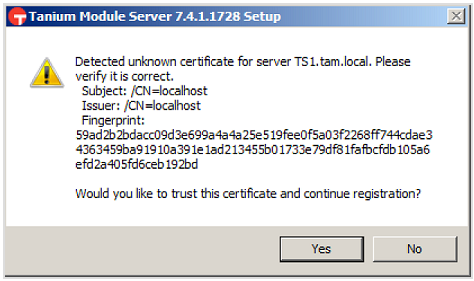
© 2026 Tanium Inc. All Rights Reserved

Tanium Module Server installation wizard settings (continued)

Settings	Guidelines
SSL/TLS Certificate	The Module Server uses the SSL/TLS certificate (`ssl.crt`) and private key (`ssl.key`) to secure connections from the Tanium Server. • **Generate Self-Signed Certificate and Key** If you do not have a CA-issued certificate, select this option to make the installer generate a self-signed certificate and private key. For the **Server Hostname**, specify the FQDN of the Module Server, such as `tms1.example.com`. • **Use Existing Certificate and Key** To use a CA-issued certificate, select the certificate file and associated private key file. For more information, see Securing Tanium Console, API, and Module Server access in a Windows deployment on page 77.
Module Postgres Configuration	Configure the connection to the PostgreSQL database server: • **Server**: Specify `localhost` (default) for a local server, or the FQDN or IP address of the remote server. You must enter IPv6 addresses within square brackets (for example, [2001:db8::1]). • **Options**: Specify additional parameters to pass in the connection. Typically, this is dbname and port. For example, `dbname=postgres port=5432 user=postgres`. You can use any parameter key words that PostgreSQL supports for database connection strings. For more information, see the PostgreSQL documentation. Click **Test** to test the connection. Any settings you configure in `external_db.json` override the settings you configure here when you install the Tanium RDB service. For more information, see (Optional) Configure a connection between the Module Server and a remote PostgreSQL database on page 51.
Register with Tanium Server	Select **Register with the Tanium Server** and specify connection information for registration with the Tanium Server: • **Tanium Server Hostname**: Specify the IP address or FQDN of the Tanium Server. In a high availability (HA) deployment, specify only the primary Tanium Server. • **Admin username**: Enter the user name of the Tanium Console administrator that you specified when installing the Tanium Server. • **Admin password**: Enter the password of the Tanium Console administrator that you specified when installing the Tanium Server. For upgrades, you have the option to select **Manually specify Tanium Server certificate** and use the default **Certificate** for securing communication between the Tanium Server and Module Server.
Choose Start Menu Folder	(Fresh installation only) Select a folder for the Module Server in the Windows **Start** menu. The default is `Tanium Module Server`.

© 2026 Tanium Inc. All Rights Reserved

Tanium Module Server installation wizard settings (continued)

Settings	Guidelines
Trust Tanium Server certificate	When the installer displays a dialog that identifies the certificate that the Tanium Server uses to authenticate to the Module Server, verify that the certificate details are correct.  On a new installation, the certificate is the `SOAPServer.crt` file. If you are re-running the installer, the certificate is `trusted.crt`. The **Fingerprint** is the hash of the certificate public key. If the certificate is valid, click **Yes** to register the Module Server with the Tanium Server.

Install and manually register the Module Server

The Module Server installer supports manual registration in case the Tanium Server is unavailable when you run the installer.

Before you begin

Ensure the following prerequisites are met and take the following actions:

- **Installer version**: Ensure that you have the right version of the installer (`SetupModuleServer.exe`). The installation package for all Tanium Core Platform servers must have the same build number (for example, if you are installing Tanium Core Platform 7.8.2.2345 on one server, you must install 7.8.2.2345 on all servers; you cannot install 7.8.2.1234 on a different Tanium Core Platform server). Contact Tanium Support on page 137 for details.
- **Host requirements**: The host system must meet the hardware, software, and network connectivity requirements suitable for your deployment: see Tanium Core Platform requirements in a Windows environment on page 20 and Resource requirements on page 156.
- **Firewall rules**: Your network security administrator must configure network firewall rules to allow communication between the Tanium Server and Module Server on TCP port 17477: see Internet access, network connectivity, and firewalls on page 26.
- **Security exclusions**: Your security team must configure exceptions to host-based security policies to allow Tanium processes to operate smoothly and at optimal performance: see Tanium Client Management Guide: Reference: Endpoint security exclusions and for Windows-based Tanium Core Platform deployments, see Tanium Core Platform User Guide for Windows Deployments: Tanium Core Platform Server security exclusions.

© 2026 Tanium Inc. All Rights Reserved

- **Certificates and keys**: Copy the `SOAPServer.crt` file from the Tanium Server host (installation directory) to the Module Server host so that you can select it when you run the installer.

  If you want to use a certificate issued by a certificate authority (CA) to secure connections to the Module Server, ensure that the CA-issued certificate and associated private key are present on the Module Server. The certificate file name must be `ssl.crt` and the key file name must be `ssl.key`. During installation, you can select a CA-issued certificate or configure the Module Server to generate a self-signed certificate.

  To facilitate troubleshooting, use the self-signed certificate during initial installation and replace it with a CA-issued certificate later. This practice enables you to separate potential installation issues from TLS connection issues.

  For more information, see Securing Tanium Console, API, and Module Server access in a Windows deployment on page 77.

- **Secondary Logon service**: The Windows Secondary Logon service (seclogon) on the host computer for the Tanium Module Server must have its **Startup type** set to **Automatic** or **Manual** (not **Disabled**) during installation of the Tanium Module Server . If the Secondary Logon service is disabled, the installation cannot connect to the database server (even if it is being installed locally), and the installation of the Tanium database fails. The Secondary Logon service is required only during installation and upgrades.

- **Local Module Server** If a local Module Server is installed on the Tanium Server host computer, perform the following steps on the Tanium Server host computer:

  1. Stop the **Tanium Server** service: open the Windows **Services** application, right-click **Tanium Server**, and select **Stop**.
  2. Stop and disable the **Tanium Module Server** service in the Windows **Services** application:
     a. Right-click **Tanium Module Server** and select **Stop**.
     b. Right-click **Tanium Module Server**, select **Properties**, set the **Startup type** to **Disabled**, and click **OK**.
  3. Go to the Windows Registry `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Tanium\Tanium Server` and clear the setting (value `127.0.0.1`) for the Module Server.
  4. Restart the **Tanium Server** service: in the Windows **Services** application, right-click **Tanium Server**, and select **Restart**.

Run the installer

1. Sign in to the Module Server host system as an administrator user.
2. Copy the installation package file (`SetupModuleServer.exe`) to a temporary location on the Module Server host.
3. Right-click `SetupModuleServer.exe` and select **Run as administrator**.

© 2026 Tanium Inc. All Rights Reserved

4. Complete the installation wizard. The following table provides guidelines for key settings.

Tanium Module Server installation wizard settings for manual registration

Settings	Guidelines
Choose Install Location	The default is `C:\Program Files\Tanium\Tanium Module Server`.
Postgres Not Found	(Fresh installation only) If the installer does not detect an existing installation of PostgreSQL, you can either install a local instance or configure a connection to an external instance. IMPORTANT: Even if you connect the Module Server to a remote PostgreSQL instance, you must keep a local instance installed on the Module Server. The Tanium™ Relational Database (RDB) service always requires certain binaries to exist in the local instance, although you can stop the instance from running. • **Install and configure local Postgres Server**: Install the default local instance of PostgreSQL. You can select this option to install a local instance that provides the binaries that the Tanium RDB service requires and still configure a connection to a remote PostgreSQL server. You configure the remote connection in a separate step in the installation wizard. • **Use remote Postgres Server**: Select this option if you want to connect to an external instance of PostgreSQL, and you do not want installer to install a local instance of PostgreSQL. You configure the remote connection in a separate step in the installation wizard. You must install a local instance of PostgreSQL separately, and you must follow the steps in (Optional) Configure a connection between the Module Server and a remote PostgreSQL database on page 51 to configure `external_db.json`. TIP: To troubleshoot issues related to the default PostgreSQL installation, see PostgreSQL installation log on page 146.

Choose Service Account for Tanium Module Server	The security best practice is to specify a service account other than the Local System account to install the Module Server and run the Module Server service on the local host computer.
	
	• **Specify Account** (best practice)
	  ◦ **User Name**: Enter only the account name portion of the credentials, such as `taniumsvc`.
	  ◦ **Domain**: Enter the domain name, such as `example.com`.
	  ◦ **Password**: Enter the account password.
	• **Local System Account**: Select this option to install software and run the Module Server service in the context of the Local System account.

Module Server Port	Specify the Module Server inbound port for traffic from the Tanium Server. The default is 17477.

© 2026 Tanium Inc. All Rights Reserved

Tanium Module Server installation wizard settings for manual registration (continued)

Settings	Guidelines
SSL/TLS Certificate	The Module Server uses the SSL/TLS certificate (`ssl.crt`) and private key (`ssl.key`) to secure connections from the Tanium Server. • **Generate Self-Signed Certificate and Key** If you do not have a CA-issued certificate, select this option to make the installer generate a self-signed certificate and private key. For the **Server Hostname**, specify the FQDN of the Module Server, such as `tms1.example.com`. • **Use Existing Certificate and Key** To use a CA-issued certificate, select the certificate file and associated private key file. For more information, see Securing Tanium Console, API, and Module Server access in a Windows deployment on page 77.
Module Postgres Configuration	Configure the connection to the PostgreSQL database server: • **Server**: Specify `localhost` (default) for a local server, or the FQDN or IP address of the remote server. You must enter IPv6 addresses within square brackets (for example, [2001:db8::1]). • **Options**: Specify additional parameters to pass in the connection. Typically, this is dbname and port. For example, `dbname=postgres port=5432 user=postgres`. You can use any parameter key words that PostgreSQL supports for database connection strings. For more information, see the PostgreSQL documentation. Click **Test** to test the connection. Any settings you configure in `external_db.json` override the settings you configure here when you install the Tanium RDB service. For more information, see (Optional) Configure a connection between the Module Server and a remote PostgreSQL database on page 51.
Manually specify Tanium Server certificate	Select **Manually specify Tanium Server certificate** and select the **Certificate** that secures communication between the Tanium Server and Module Server. On a new installation, the file is the `SOAPServer.crt` file that was copied from the Tanium Server. If you are re-running the installer and want to use the Tanium Server certificate created by the previous run of the installer, browse and select the `trusted.crt` file in the installation directory.
Choose Start Menu Folder	(Fresh installation only) Select a folder for the Module Server in the Windows **Start** menu. The default is `Tanium Module Server`.

5. Manually register the Module Server with the Tanium Server: see Example: Register the Module Server with the Tanium Server on page 179.
   The registration process generates an SSL/TLS certificate file named `ssl.crt` in the Module Server installation directory.
6. Copy `ssl.crt` to the Tanium Server installation directory and rename it `trusted-module-servers.crt`.

© 2026 Tanium Inc. All Rights Reserved

7. Configure the Tanium Server to use the remote Module Server:
    a. Sign in to the Tanium Server host.
    b. Open the Windows **Services** application and stop the **Tanium Server** service.
    c. Go to the following location in the Windows registry:
    `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Tanium\Tanium Server`
    d. Find the ModuleServer key and change it to the FQDN of the remote Module Server.
    e. Restart the **Tanium Server** service in the Windows **Services** application.

    > NOTE
    > If you previously installed a local Module Server, leave the **Tanium Module Server** service stopped and disabled on the Tanium Server. The Tanium Server must use only the remote Module Server.

    f. Sign in to the Module Server host.
    g. Open the Windows **Services** application and restart the services for the **Tanium Module Server** and all Tanium modules and shared services.

(Optional) Configure a connection between the Module Server and a remote PostgreSQL database

By default, the Module Server installer creates a local PostgreSQL database instance as the storage system for Tanium solutions. If your organization prefers to use its own database infrastructure, you can connect the Module Server to a remote PostgreSQL instance. The remote instance must use the same major PostgreSQL version as the default local instance. For example, if the local instance uses version 12.3.4, the remote instance can use any 12.x.x version.

> TIP
> You can also specify basic configuration for this connection in the installation wizard when you install the Module Server. If you do not create an `external_db.json` file, then when you install the Tanium™ Relational Database (RDB) service, it uses the connection settings that you specified in the Module Server installation wizard. If you create an `external_db.json` file before installing Tanium RDB, the settings that you specify in that file override any settings that you specified during the Module Server installation.

> IMPORTANT
> Even if you connect the Module Server to a remote PostgreSQL instance, you must keep a local instance installed on the Module Server. The Tanium™ Relational Database (RDB) service always requires certain binaries to exist in the local instance, although you can stop the instance from running. If you use a local instance separate from the default, you must follow these steps, and you must specify the `pg_install_dir` property in `external_db.json`. The location that you specify must contain a `bin` subdirectory that contains PostgreSQL binaries.

© 2026 Tanium Inc. All Rights Reserved

1. Determine how Tanium solutions must authenticate to the remote PostgreSQL instance:
    - **PostgreSQL administrator credentials**: Record the user name and password that are used for administrator access to the PostgreSQL instance.
    - **SSL/TLS certificates**: If the PostgreSQL instance is configured to use TLS for communication with Tanium solutions, acquire the certificate authority (CA) root certificate of the instance. On the database server, the PGSSLROOTCERT environment variable indicates the location of the CA certificate. If the instance is configured for mutual TLS (mTLS) authentication instead of credentials authentication, you must also acquire the TLS certificate and associated private key of the instance. On the database server, the PGSSLCERT and PGSSLKEY environment variables indicates the locations of the certificate and key.
2. Sign in to the Module Server.
3. Create a JSON file named `external_db.json` with the following contents. The file must reside in the *<Module Server installation directory>*`\services\rdb-files` directory. Enter only the values that apply. For example, enter either the administrator user name and password or the contents of the certificates and private key based on whether the PostgreSQL instance is configured for credential or certificate authentication. The default PostgreSQL port is 5432.

```
{
   "server": {
   "host": "<IP address or hostname of the PostgreSQL instance>",
   "port": 5432,
   "pg_admin_username": "<PostgreSQL administrator user name>",
   "pg_admin_password": "<PostgreSQL administrator password>",
   "pg_ssl_root_pem": "<contents of the TLS CA certificate>",
   "pg_ssl_key_pem": "<contents of the TLS private key>",
   "pg_ssl_cert_pem": "<contents of the TSL certificate>"
   "pg_install_dir": <absolute path to the local PostgreSQL installation directory>
   }
}
```

4. Open the Windows **Services** application, right-click **Tanium RDB Service**, and select **Restart**.

Update the Module Server certificate

Registration ensures secure communication between the Module Server and the Tanium Server. If you update the Module Server certificate `ssl.crt`, you must repeat the registration, either by re-running the installer or using the CLI. After registration, you must restart the services for the **Tanium Module Server** and all Tanium modules and shared services through the Windows **Services** application. For more information, see Securing Tanium Console, API, and Module Server access in a Windows deployment on page 77.

© 2026 Tanium Inc. All Rights Reserved

Next steps

If your deployment will include a Tanium Zone Server, install it: see Installing the Tanium Zone Server on page 54. Otherwise, verify the deployment: see Verifying the deployment to your Windows environment on page 92.

© 2026 Tanium Inc. All Rights Reserved

Installing the Tanium Zone Server

Install a Tanium Zone Server in your DMZ to proxy communication from external endpoints to the Tanium Server. You can install the Zone Server Hub on the same host as the Tanium Server or on a dedicated host. You can deploy two Zone Servers and two Zone Server Hubs in an active-active high availability (HA) configuration to ensure continuous availability in the event of an outage or scheduled maintenance. For more information about the Zone Server, Zone Server Hub, and deployment options, see Tanium Zone Server on page 15.

Before you begin

Ensure that you meet the following requirements before installing the Zone Server:

- **Installer version**: Ensure that you have the right version of the installer (`SetupZoneServer.exe`). The installation package for all Tanium Core Platform servers must have the same build number (for example, if you are installing Tanium Core Platform 7.8.2.2345 on one server, you must install 7.8.2.2345 on all servers; you cannot install 7.8.2.1234 on a different Tanium Core Platform server). Download the installation package from the **Artifacts** section of your Tanium Account. For more information, see Tanium Account User Guide: View Tanium artifacts.
- **Host requirements**: The host system must meet the hardware, software, and network connectivity requirements suitable for your deployment: see Tanium Core Platform requirements in a Windows environment on page 20 and Resource requirements on page 156.
- **Firewall rules**: Your network administrator must configure firewall rules to allow communication from the Zone Server Hub to the Zone Server on the port that you configured for that traffic. The default is TCP port 17472 but you can specify a different port: see Configure ports for traffic from Zone Server Hubs and Tanium Clients on page 58.
- **Security exclusions**: Your security team must configure exceptions to host-based security policies to allow Tanium processes to operate smoothly and at optimal performance: see Tanium Client Management Guide: Reference: Endpoint security exclusions and for Windows-based Tanium Core Platform deployments, see Tanium Core Platform User Guide for Windows Deployments: Tanium Core Platform Server security exclusions.
- **Initialization bundle**: If you are performing a fresh installation of the Zone Server and Zone Server Hub, download the Tanium™ initialization bundle (`tanium-init.dat`). The Zone Server and Hub use the file to secure communication with the Tanium Server. For the download procedure, see Tanium Console User Guide: Download infrastructure configuration files (keys).

Install the Tanium Zone Server

This section provides procedures for the following workflow:

1. Run the installer on the Zone Server Hub host computer. In this example, the Tanium Server host computer is also the Zone Server Hub host computer.
2. Run the installer on one or more Zone Server host computers in the DMZ.

The Tanium Zone Server installer takes the following actions:

© 2026 Tanium Inc. All Rights Reserved

- Opens TCP port 17472 in the local host computer Windows Firewall.
- Installs Tanium Zone Server Hub or Zone Server on the local host computer and starts the service.

Install the Zone Server Hub

Perform the following steps for each Zone Server Hub.

1. Sign in as an administrator user on the internal network host system where you will install the Zone Server Hub.
2. Copy the installer (`SetupZoneServer.exe`) to a temporary location on the hub host.
3. (Fresh installations only) Copy the initialization file (`tanium-init.dat`) from the Tanium Server to a temporary location on the hub host if you will install the hub on a dedicated host. If you will install the hub on the Tanium Server host, you can find the file in the Tanium Server installation folder.
4. Right-click `SetupZoneServer.exe` and select **Run as administrator**.
5. Complete the installation wizard. The following table provides guidelines for key settings.

Tanium Zone Server Hub installation wizard settings

Settings	Guidelines
Choose Install Location	The default installation folder is `C:\Program Files (x86)\Tanium\Tanium Zone Server`.
Zone Server Type	Select **Zone Server Hub**.
Choose Service Account for Tanium Zone Server	**Specify Account**: Define a service account to run the Tanium Zone Server service on the local host computer: • **User Name**: Enter only the account name portion of the credentials, such as `taniumsvc`. • **Domain**: Enter the domain name, such as `example.com`. • **Password**: Enter the account password.
	Local System Account: Select this option to install software and run the service in the context of the Local System account. Because this account grants higher operating system privileges than are necessary for Zone Server operations, the best practice is to not select this option for production deployments.
Initialization File	(Fresh installations only) Specify the file path of the `tanium-init.dat` file.
Server Address	Specify the fully qualified domain name (FQDN) or IP address of the Tanium Server. You must enter IPv6 addresses within square brackets (for example, `[2001:db8::1]`).
Server Port	The inbound port on which the Zone Server Hub receives traffic from the Tanium Server and Zone Server. The default is 17472.

© 2026 Tanium Inc. All Rights Reserved

6. (Non-local hub only) If the Zone Server Hub resides on a different host than the Tanium Server, sign in to the Tanium Server CLI and configure the `AllowedHubs` setting:

   a. Navigate to the Tanium Server installation folder:

   ```
   $ cd <Tanium Server>
   ```

   b. Enable (best practice) or disable enforcement of the `AllowedHubs` setting. The default value `1` specifies that the Tanium Server enforces the setting: only hubs listed in `AllowedHubs` can communicate with the Tanium Server. The value `0` enables any hub to communicate with the Tanium Server regardless of the `AllowedHubs` setting.

   ```
   $ TaniumReceiver config set EnforceAllowedHubs [1|0]
   ```

   c. If you enabled enforcement of `AllowedHubs`, configure it as follows, where `<hub1,hub2...>` is a comma-separated list of hubs that are authorized to communicate with this Tanium Server. Specify the hubs by FQDN or IP address. You must enter IPv6 addresses within square brackets (for example, `[2001:db8::1]`). The default value is 127.0.0.1 (localhost).

   ```
   $ TaniumReceiver config set AllowedHubs <hub1,hub2...>
   ```

7. (Non-local hub only) If the Zone Server Hub resides on a different host than the Tanium Server, enable the file cache and set its maximum size: see Manage caching on the Zone Server and Zone Server Hub on page 59.

Install the Zone Server

Perform the following steps for each Zone Server.

1. Sign in to the Tanium Zone Server host computer as an administrator user.
2. Copy the installer (`SetupZoneServer.exe`) to a temporary location on the Zone Server.
3. (Fresh installation only) Copy the initialization file (`tanium-init.dat`) from the Tanium Server to a temporary location on the Zone Server.
4. Right-click the `SetupZoneServer.exe` file and select **Run as administrator**.
5. Complete the installation wizard. The following table provides guidelines for key settings.

Tanium Zone Server installation wizard settings

Settings	Guidelines
Choose Install Location	The default is `C:\Program Files (x86)\Tanium\Tanium Zone Server`.
Zone Server Type	Select **Zone Server**.

© 2026 Tanium Inc. All Rights Reserved

Tanium Zone Server installation wizard settings (continued)

Settings	Guidelines
Choose Service Account for Tanium Zone Server	**Specify Account**: Define a service account to run the Tanium Zone Server service on the local host computer: • **User Name**: Enter only the account name portion of the credentials, such as `taniumsvc`. • **Domain**: Enter the domain name, such as `example.com`. • **Password**: Enter the account password.
	Local System Account: Select this option to install software and run the service in the context of the Local System account. Because this account grants higher operating system privileges than are necessary for Zone Server operations, the best practice is to not select this option for production deployments.
Initialization File	(Fresh installations only) Specify the file path of the `tanium-init.dat` file.
IP addresses or FQDNs of allowed Zone Server Hubs	Enter a comma-separated list of IP addresses or FQDNs for the Zone Server Hubs that are authorized to communicate with this Zone Server. You must enter IPv6 addresses within square brackets (for example, [2001:db8::1]). In an HA deployment, specify both Zone Server Hubs. TIP This installation setting populates the `AllowedHubs` setting on the Zone Server. To change this setting at a later time, configure it using the following command on the Zone Server, where `<hub1,hub2...>` is a comma-separated list of the allowed hubs. `$ TaniumZoneServer config set AllowedHubs <hub1,hub2...>`

6. (HA only) As a best practice, specify the preferred Zone Server Hub from which the Zone Server receives Tanium Client content, such as action packages (see Tanium Zone Server for details). Sign in to the Zone Server CLI (see Reference: Tanium Core Platform Command-line interface in a Windows deployment on page 176) and run the following commands:

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

```
$ TaniumZoneServer config set HubPriorityList <hub IP address or FQDN>
```

7. (Best Practice) Configure separate ports on the Zone Server for traffic from Zone Server Hubs and Tanium Clients: see Configure ports for traffic from Zone Server Hubs and Tanium Clients on page 58.

8. Enable trust between the Zone Server Hub and Tanium Server, and map Zone Servers to the hub: see Tanium Console User Guide: Managing Zone Servers and hubs.

© 2026 Tanium Inc. All Rights Reserved

9. If the Zone Server requires different separated subnets or isolated subnets than the Tanium Server, configure them as described in Tanium Client Management User Guide: Configuring Tanium Client peering.
10. Configure the connections from Tanium Clients that must register with the Zone Server: see Configure Tanium Clients to register with the Zone Server on page 60.
11. If necessary to prevent over-consumption of disk space on the Zone Server, configure a maximum file cache size: see Manage caching on the Zone Server and Zone Server Hub on page 59.
12. Verify the deployment: see Verifying the deployment to your Windows environment on page 92.

Configure ports for traffic from Zone Server Hubs and Tanium Clients

By default, the Zone Server uses the same incoming port (default is 17472) for traffic from Zone Server Hubs and Tanium Clients. As a best practice to improve the security of the Zone Server, configure separate ports:

1. Sign in to the Zone Server host as an administrator user.
2. Access the CLI (see Reference: Tanium Core Platform Command-line interface in a Windows deployment on page 176).
3. Navigate to the Zone Server installation folder:

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

4. Configure the port for traffic from Tanium Clients:

   ```
   > TaniumZoneServer config set ZoneServerPort <port>
   ```

   If Tanium Clients are already configured to communicate with the Zone Server, the best practice is to leave this port number unchanged and edit only the port for traffic from Zone Server Hubs.

5. Configure the port for traffic from Zone Server Hubs:

   ```
   > TaniumZoneServer config set ZoneServerPortForHub <port>
   ```

6. If traffic between the Zone Server and Zone Server Hubs traverses a firewall, configure the firewall to allow only hubs that are in the AllowedHubs list to connect to the port that you specified in the ZoneServerPortForHub setting. For information about configuring the firewall, see your firewall documentation. To see which hubs are in the AllowedHubs list, run the following command:

   ```
   > TaniumZoneServer config get AllowedHubs
   ```

7. Access the Windows Services program and restart the `Tanium ZoneServer` service.

© 2026 Tanium Inc. All Rights Reserved

8. Delete and recreate the Zone Server Hub-to-Zone Server mappings of the Zone Server for which you configured separate ports.

   For more information, see Tanium Console User Guide: Delete a Zone Server Hub-to-Zone Server mapping and Tanium Console User Guide: Map Zone Servers to a Zone Server Hub.

Manage caching on the Zone Server and Zone Server Hub

To optimize performance for the Tanium Core Platform, the Zone Server caches package files for actions and files requested through the Tanium Client API. The Zone Server provides these resources to Tanium Clients without having to re-request them from the Tanium Server.This file cache is disabled by default on the Zone Server Hub because in most deployments the hub is installed on the Tanium Server, which has its own cache. However, if the hub is installed on a dedicated host, you must enable it to perform the same caching as the Zone Server. By default, the cache uses a maximum of 20% disk space on the Zone Server and on the hub on a dedicated host, but you can change that limit.



Set the maximum cache size to whichever is the lesser value between 200GB and 60% of available disk space on the drive where the Zone Server or hub is installed.

When you set the cache size, the Zone Server or Zone Server Hub automatically removes all the files that are currently in the cache (`<Zone Server/hub>\Cache\HotCacheFile`).

Manage Zone Server caching

1. From the Main menu, go to **Administration > Configuration > Settings > Advanced Settings** and click **Add Setting.**
2. Configure the following parameters and click **Save**:
   - **Setting Type**: Select **Server**
   - **Platform Setting Name**: Enter `zs_hot_cache_limit_in_MB`.
   - **Value Type**: Select **Numeric**
   - **Value**: Enter the maximum storage space in megabytes for the Zone Server cache. The default is 0 (20% of disk space).

Manage Zone Server Hub caching

If the Zone Server Hub is installed on the Tanium Server, the hub cache is unnecessary.

If the Zone Server Hub is installed on a dedicated host, configure the cache as follows:

1. Sign in to the hub host as an administrator user.
2. Access the hub CLI (see Reference: Tanium Core Platform Command-line interface in a Windows deployment on page 176) and run the following commands:

   ```
   $ cd <Zone Server Hub>
   ```

© 2026 Tanium Inc. All Rights Reserved

```
$ TaniumZoneServer config set EnableFileCache 1
```

3. Open the Windows Services program and restart the `Tanium ZoneServer` service.
4. Sign in to Tanium Console.
5. From the Main menu, go to **Administration > Configuration > Settings > Advanced Settings** and click **Add Setting**.
6. Configure the following setting and click **Save**:
   - **Setting Type**: Select **Server**
   - **Name**: Enter `hub_hot_cache_limit_in_MB`.
   - **Value Type**: Select **Numeric**
   - **Value**: Enter the maximum storage space in megabytes for the hub cache. The default is 0 (20% of disk space).

Configure Tanium Clients to register with the Zone Server

To configure Tanium Clients to register with a Zone Server, you must add it to the **ServerNameList** setting on each Client. This setting can specify multiple Zone Servers and Tanium Servers. When attempting to connect, the Client randomly selects one Server at a time in the list and registers only with the first Server for which the Client can resolve the IP address. To ensure that Clients connect and register with the correct Server, work with your network administrator to review your Domain Name System (DNS) configuration. For example, external Clients typically resolve the IP addresses of Zone Servers in the DMZ but not of Tanium Servers in the internal network. By contrast, internal Clients typically resolve the IP addresses of Tanium Servers in the internal network but not of Zone Servers in the DMZ.

The steps to configure Tanium Clients to register with the Zone Server depend on whether you have already deployed the Clients.

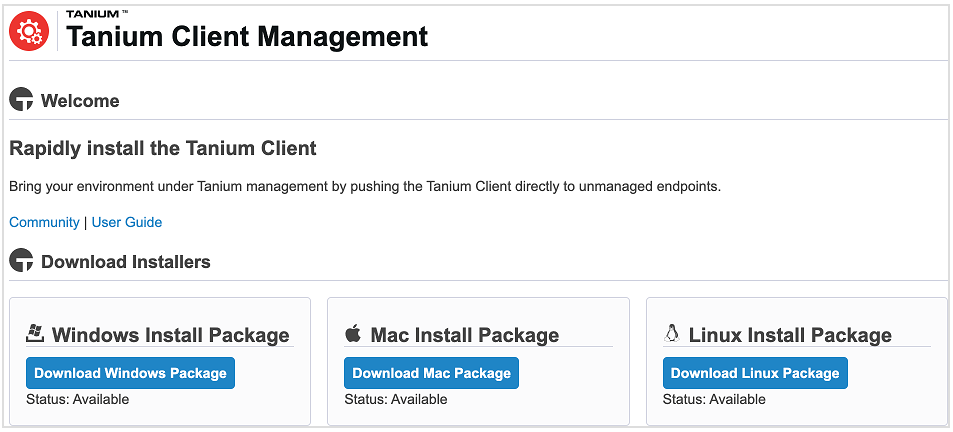
Initial Tanium Client deployment

Perform the following steps if you have not yet deployed the Tanium Clients that must register with the Zone Server:

1. Use Tanium™ Client Management to download installer bundles as described under Tanium Client Management User Guide: Download the installation bundle for alternative deployment.
   Each endpoint OS type requires a separate bundle. Each bundle contains the following files, which you use when deploying the Clients:
   - Installer file to install the Tanium Client, such as `SetupClient.exe` for Windows endpoints.

     NOTE The Linux bundle contains an installer for each supported Linux distribution.
   - Initialization file (`tanium-init.dat`) to secure connections between the Tanium Client and other Tanium Core Platform components.

© 2026 Tanium Inc. All Rights Reserved



2. Deploy the Tanium Client to endpoints as described in the Tanium Client Management User Guide. For the **ServerNameList** setting, specify the FQDN or IP address of each Zone Server and Tanium Server.

   You must enter IPv6 addresses within square brackets (for example, `[2001:db8::1]`).

   > NOTE
   >
   > In the Tanium Client installation wizard for Windows, you specify the ServerNameList value in the **Server Address** field.

   > BEST PRACTICE
   >
   > Specify FQDNs for this setting.

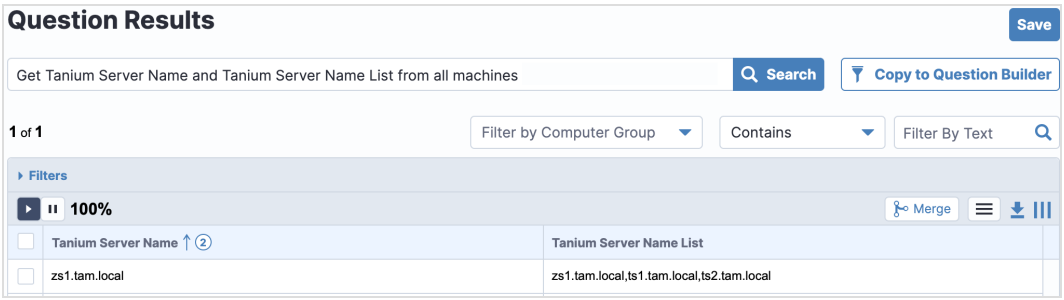
3. Work with your network administrator to ensure that Tanium Clients that must register with the Zone Server cannot resolve the IP address of the Tanium Server.

   This step is necessary to prevent Clients from bypassing the Zone Server and connecting directly with the Tanium Server.

4. Use Tanium Interact to issue a question that returns the value of the **ServerName** and **ServerNameList** settings from Tanium Clients. The **ServerName** is the FQDN or IP address of the Server with which Clients currently connect.

   ```
   Get Tanium Server Name and Tanium Server Name List from all machines
   ```

5. In the **Question Results** grid, verify that the **Tanium Server Name** value displays the Zone Server for any Clients that must register with it, and verify that the **Tanium Server Name List** value includes all the Servers that you specified.

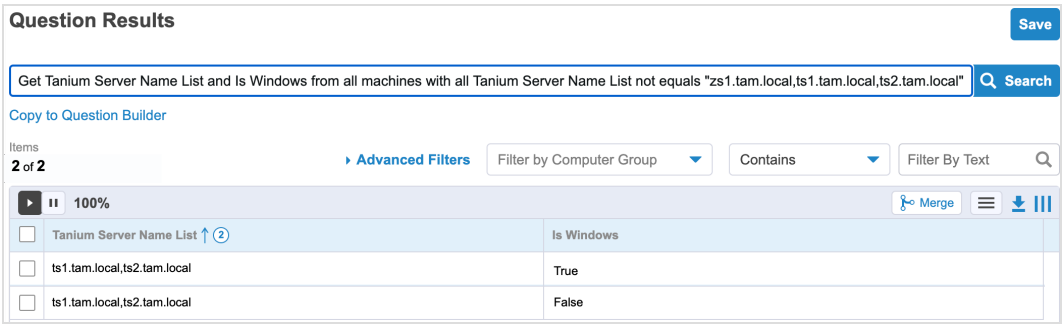


© 2026 Tanium Inc. All Rights Reserved

Existing Tanium Client deployment

Perform the following steps to change the **ServerNameList** setting on Tanium Clients that you want to register with the Zone Server. In a deployment with both Windows and non-Windows endpoints, repeat the steps for both types of endpoints.

1. Delete any existing scheduled actions that configure the **ServerNameList** or **ServerName** to prevent conflicts with the new actions that you create for those settings.
2. Use Tanium Interact to issue a question that identifies the Tanium Clients that do not yet register with the Zone Server.
   The following example identifies Tanium Clients in a deployment where the Zone Server FQDN is `zs1.tam.local` and the active-active Tanium Servers are `ts1.tam.local` and `ts2.tam.local`.
   `Get Tanium Server Name List and Is Windows from all machines with all Tanium Server Name List not equals “zs1.tam.local,ts1.tam.local,ts2.tam.local"`

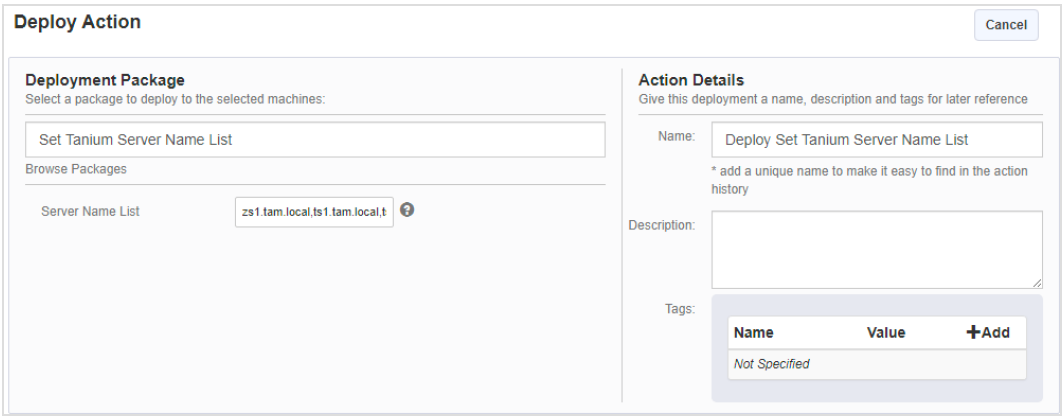


3. In the **Question Results** grid, select the Windows or non-Windows endpoints (not both) that must register with the Zone Server and click **Deploy Action**.
4. Specify one of the following as a **Deployment Package**:
   - **Set Tanium Server Name List** for Windows endpoints
   - **Set Tanium Server Name List [Non-Windows]** for non-Windows endpoints
5. Enter the FQDN or IP address of each Zone Server and Tanium Server in the **Server Name List** field.
   You must enter IPv6 addresses within square brackets (for example, `[2001:db8::1]`).

BEST PRACTICE

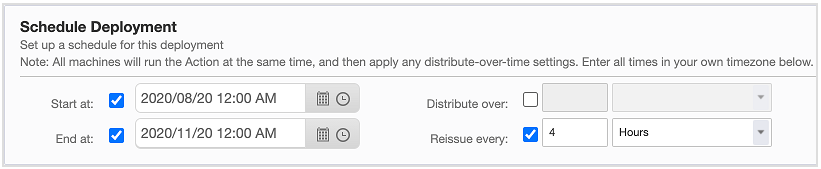
Specify FQDNs for this setting.

© 2026 Tanium Inc. All Rights Reserved



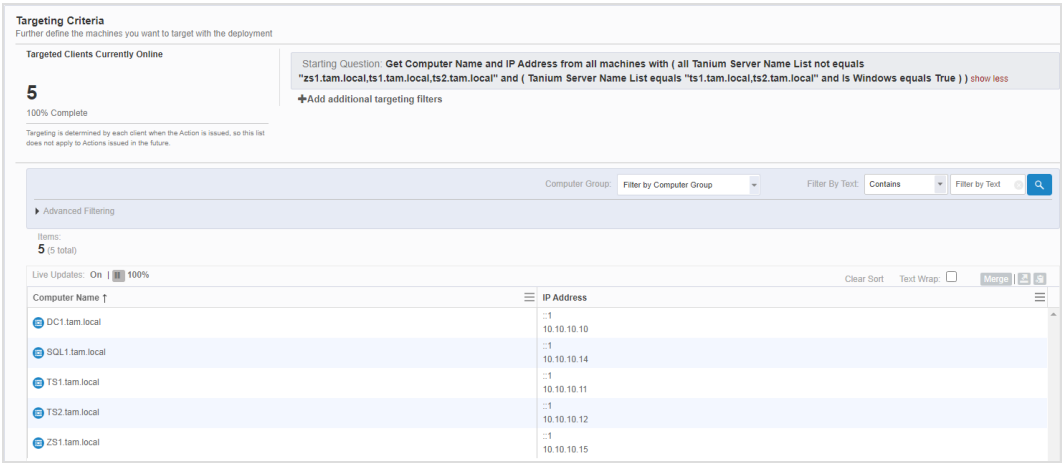
6. Set a schedule for the action.

> **TIP** Consider setting a reissue interval if some target endpoints might be offline when you initially deploy the action.



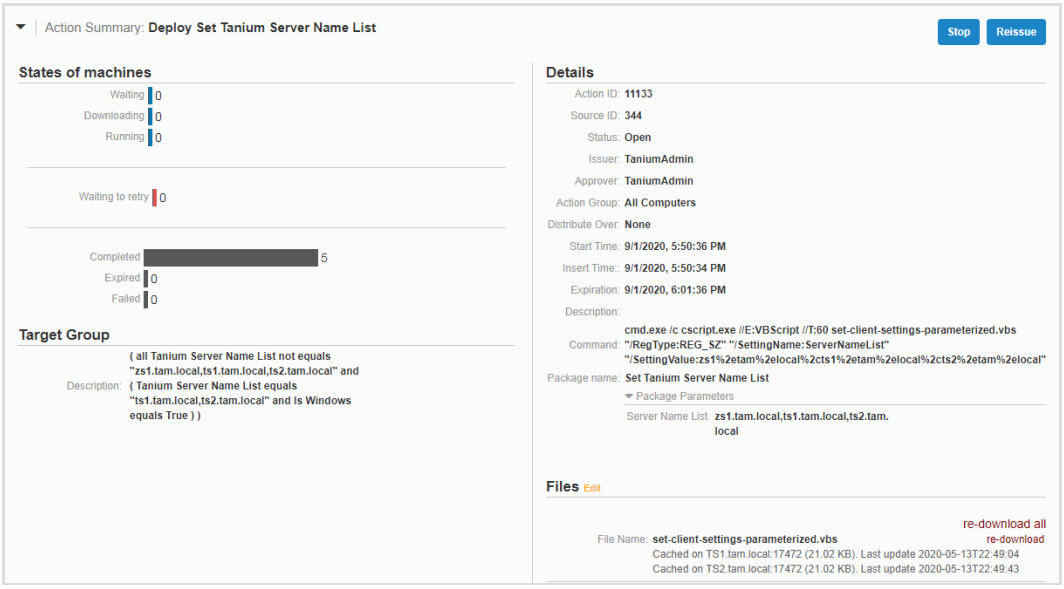
7. In the **Targeting Criteria** section, ensure that the settings specify only Windows endpoints or non-Windows endpoints based on the package that you selected

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



© 2026 Tanium Inc. All Rights Reserved

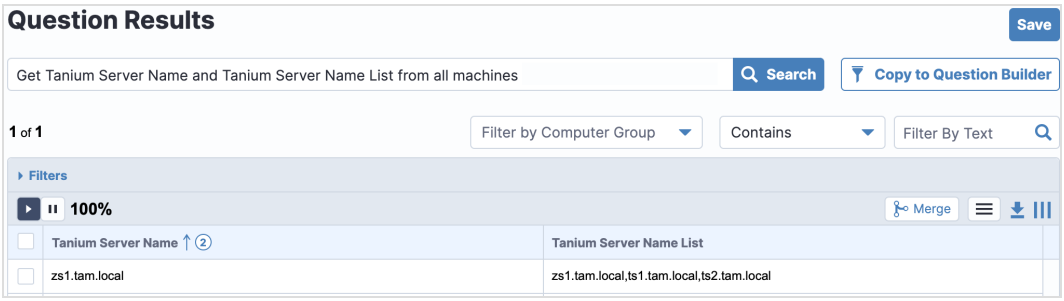
9. Click **Deploy Action** and review the action status to verify that the action completes without errors.



10. Use Tanium Interact to issue a question that returns the **ServerName** and **ServerNameList** values from Tanium Clients. The **ServerName** is the FQDN or IP address of the Server with which Clients currently connect. If the action succeeded, the **ServerName** indicates the Zone Server for at least some Clients and the **Tanium Server Name List** value lists all the correct Servers (`zs1.tam.local,ts1.tam.local,ts2.tam.local`, in this example).

> **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. Whether a particular Tanium Client connects to the Zone Server or Tanium Server depends on the Domain Name System (DNS) configuration of your network.

```
Get Tanium Server Name and Tanium Server Name List from all machines
```



© 2026 Tanium Inc. All Rights Reserved

11. Work with your network administrator to ensure that the Tanium Clients that must register with the Zone Server cannot resolve the IP address of the Tanium Server.

    This step is necessary to prevent those Clients from bypassing the Zone Server and connecting directly with the Tanium Server.

© 2026 Tanium Inc. All Rights Reserved

Configuring proxy server settings in a Windows deployment

Overview of proxy server connections

Some organizations use proxy servers for traffic between internal servers and the Internet. If your organization uses proxies and its security policy does not allow Tanium Core Platform Servers to access Internet locations directly, configure access through the proxies. The Tanium Server and Tanium Module Server connect to the Internet to download content and module software updates from Tanium, and to download necessary files from other remote sources. Individual Tanium solutions might also have requirements to access the Internet.

To configure Tanium Client to connect through a Hypertext Transfer Protocol Secure (HTTPS) proxy server to the Tanium Server or Tanium Zone Server, see Tanium Client Management User Guide: Connect through an HTTPS proxy server.

The Tanium Server and Module Server use the Tanium Downloader (TDownloader) utility to securely download files. To configure access through proxies, configure TDownloader settings on both Servers.



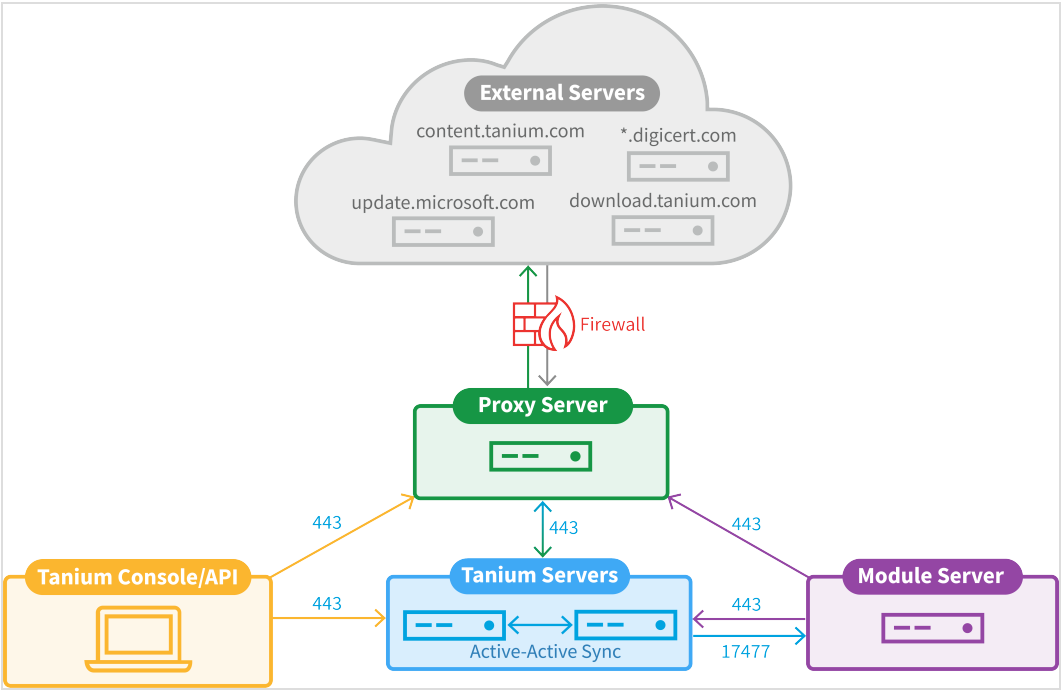
For a list of sites that Tanium Core Platform Servers access, see Internet URLs on page 26.

A remote source might have its own requirements, such as certificate authentication or user authentication. For more information, see Tanium Console User Guide: Managing remote authentication.

To troubleshoot proxy server issues, see TDownloader log on page 149.

© 2026 Tanium Inc. All Rights Reserved

Figure 1: Tanium deployment with proxy server



Types of proxy servers

The Tanium Core Platform supports two types of proxies in a Windows deployment:

- **Basic**: A strictly IP address-based proxy server allows a specified list of servers to traverse the proxy and access the network or Internet. Add the IP addresses or fully qualified domain names of the Tanium Server and Module Server to the access list of the proxy server. If the proxy server requires authentication, configure the account ID and password.
- **NTLM**: If the proxy server is set up to use Microsoft NT LAN Manager (NTLM), and you configure the Tanium Server service to run in the context of a service account that has sufficient permissions to traverse the proxy server, you do not have to configure an account ID and password.

TDownloader user context

For Tanium deployments on customer-provided Windows Infrastructure, TDownloader runs in the context of the Tanium Server service account user that was specified during installation.

Tanium Console: Configure proxy settings

In most cases, use Tanium Console to configure proxy settings unless you must configure the settings before you can access the Console. For more information, see the Tanium Console User Guide: Configuring proxy server settings.

© 2026 Tanium Inc. All Rights Reserved

Configure proxy settings

In most cases, use Tanium Console to configure proxy settings. In some circumstances, you might need to configure proxy settings before you have access to Tanium Console. If necessary, you can configure proxy settings on the Tanium Server or Module Server host.



The proxy server configuration is stored in configuration files on the Tanium Server. Tanium Servers do not automatically synchronize the configuration files among active-active peers. If you change these settings in active-active deployments, be sure to perform the procedure on both Tanium Servers.

Use the following commands on each Tanium Core Platform Server to configure these settings:

- **Tanium Server**
  - Display the current settings: `TaniumReceiver config list`
  - View the value configured for a setting: `TaniumReceiver config get SettingName`
  - Configure a setting: `TaniumReceiver config set SettingNamevalue`
- **Tanium Module Server**
  - Display the current settings: `TaniumModuleServer config list`
  - View the value configured for a setting: `TaniumModuleServer config get SettingName`
  - Configure a setting: `TaniumModuleServer config set SettingNamevalue`
- **TDownloader on the Tanium Server or Tanim Module Server**
  - Display the current settings: `TDownloader config list`
  - View the value configured for a setting: `TDownloader config get SettingName`
  - Configure a setting: `TDownloader config set SettingNamevalue`

© 2026 Tanium Inc. All Rights Reserved

Platform settings used with proxy servers

Settings	Platform components	Guidelines
BypassCRLCheckHostList	Tanium Server Module Server TDownloader	List the servers that the Tanium Server or Module Server can trust without checking a certificate revocation list (CRL). The Tanium Server and Module Server perform a CRL check on all servers that are not in this list, and do not download files from a server that fails the check. Specify the servers by FQDN or IP address. You must enter IPv6 addresses within square brackets (for example, `[2001:db8::1]`). Configure this setting in the TDownloader configuration on the Tanium Server and Module Server. Configure this setting in the Tanium Server and Module Server configurations. If you configure the Tanium Server and Module Server to access Internet sites through a proxy server, you can configure BypassCRLCheckHostList through Tanium Core Platform. For more information, see Tanium Console User Guide: Configuring proxy server settings.
BypassProxyHostList	Tanium Server Module Server TDownloader	If you configure the Tanium Core Platform to access Internet sites through a proxy server, enter a comma-separated list of FQDNs or IP addresses for the hosts that do not go through the proxy server. You do not have to enter `127.0.0.1`, `localhost`, or the Module Server, but enter active-active Tanium Servers if necessary. You must enter IPv6 addresses within square brackets (for example, `[2001:db8::1]`). Specify literal values. All supported Tanium Core Platform versions allow wildcards. Configure this setting in the TDownloader configuration on the Tanium Server and Module Server. Configure this setting in the Tanium Server and Module Server configurations. For more information, see Tanium Console User Guide: Configuring proxy server settings.
ForceIPV6	Tanium Server Module Server TDownloader	In deployments where traffic between Tanium Core Platform Servers and the Internet traverses a proxy server, TDownloader resolves the proxy address as an IPv4 address by default. If the proxy server has an IPv6 address, add ForceIPV6 with a value of `1`. ForceIPV6 is a TDownloader setting on the Tanium Server and Module Server in both Appliance and Windows deployments. The setting is hidden by default and its default value is `0`. Contact Tanium Support for guidance before adding this setting (see Contact Tanium Support). For more information about proxy server settings, see Configuring proxy server settings.

© 2026 Tanium Inc. All Rights Reserved

Platform settings used with proxy servers (continued)

Settings	Platform components	Guidelines
LogVerbosityLevel	Tanium Server (local) Module Server Zone Server TDownloader	Specify the logging level as a decimal value on the Tanium Client, Tanium Server, Module Server, or Zone Server. On the Tanium Server and Module Server, you can configure the logging level separately for TDownloader. For best practices and configuration, see Logging levels. NOTE: By default, this setting is not present on Tanium Clients unless you set the logging level when deploying Clients. TIP: If you deploy an action to configure this setting on Tanium Clients, use the **Set Windows Tanium Client Logging Level** or **Set Tanium Client Logging Level [Non-Windows]** package. BEST PRACTICE: On Tanium Clients that run on virtual desktop infrastructure (VDI) endpoints or endpoints with limited resources, disable logging to reduce disk writes. Temporarily re-enable logging on individual endpoints for troubleshooting.
ProxyPassword	Tanium Server Module Server TDownloader	For a proxy server that requires authentication, enter the password of the Tanium Console User Guide: ProxyUserid user that establishes a connection with the proxy server. Configure this setting in the TDownloader configuration on the Tanium Server and Module Server. Configure this setting in the Tanium Server and Module Server configurations. For more information, see Tanium Console User Guide: Configuring proxy server settings.
ProxyPort	Tanium Server Module Server TDownloader	Specify the proxy server listening port. Configure this setting in the TDownloader configuration on the Tanium Server and Module Server. Configure this setting in the Tanium Server and Module Server configurations. For more information, see Tanium Console User Guide: Configuring proxy server settings.

© 2026 Tanium Inc. All Rights Reserved

Platform settings used with proxy servers (continued)

Settings	Platform components	Guidelines
ProxyServer	Tanium Server Module Server TDownloader	Specify the IP address of the proxy server. Configure this setting in the TDownloader configuration on the Tanium Server and Module Server. Configure this setting in the Tanium Server and Module Server configurations. For more information, see Tanium Console User Guide: Configuring proxy server settings. NOTE: By default, the proxy server address is resolved as an IPv4 address. If the proxy server has an IPv6 address, you must enter it within brackets (for example, `[2001:db8::1]`) and configure the TDownloader setting Tanium Console User Guide: ForceIPV6 to `1`.
ProxyType	Tanium Server Module Server TDownloader	Specify the type of proxy server authentication. Configure this setting in the TDownloader configuration on the Tanium Server and Module Server. The possible values are `Basic`, `NTLM`, or `None`. Configure this setting in the Tanium Server and Module Server configurations. The possible values are `Basic` or `NTLM`. For more information, see Tanium Console User Guide: Configuring proxy server settings.
ProxyUserid	Tanium Server Module Server TDownloader	For a proxy server that requires authentication, specify the user ID of the account that establishes a connection with the proxy server. ProxyUserid is a TDownloader setting on the Tanium Server and Module Server. ProxyUserid is a Tanium Server and Module Server setting. For more information, see Tanium Console User Guide: Configuring proxy server settings.
TrustedHostList	Tanium Server (local) Module Server TDownloader	By default, the Tanium Server and Module Server validate the SSL/TLS certificate of remote servers when establishing connections to them (such as for downloading files). To bypass certificate validation for specific servers, enter their FQDN or IP address. You do not have to enter 127.0.0.1, localhost, the Tanium Module Server, or Tanium Servers (standalone or active-active). Wildcards are supported. You must enter IPv6 addresses within square brackets (for example, `[2001:db8::1]`). TrustedHostList is a TDownloader setting on the Tanium Server and Module Server. TrustedHostList is a Tanium Server and Module Server setting. For more information, see Tanium Console User Guide: Configuring proxy server settings.

© 2026 Tanium Inc. All Rights Reserved

Installing Tanium Servers in an active-active HA cluster

You can deploy two Tanium Servers in an active-active high availability (HA) cluster to ensure continuous availability in the event of an outage or scheduled maintenance. For more information about HA deployments, see Tanium Server on page 13. If the deployment includes HA Zone Servers, see Zone Server High Availability on page 15.

To install a standalone Tanium Server on a dedicated Windows Server host, see Installing the Tanium Server on page 34.

HA cluster requirements and limitations

An HA deployment has the following requirements:

- **Installer version**: Use the same installer for both Tanium Servers. All Tanium Core Platform servers must have the same build number (for example, if you are installing Tanium Core Platform 7.8.2.2345 on one server, you must install 7.8.2.2345 on all servers; you cannot install 7.8.2.1234 on a different Tanium Core Platform server). Contact Tanium Support on page 137 for details.
- **Host capacity**: Both Tanium Servers must meet or exceed the requirements for the total number of endpoints that your deployment targets. That means each Server must be able to independently handle load from the full deployment in the event of failure. For more information, see Resource requirements on page 156.
- **Peer-to-peer connectivity**: The Tanium Servers must be able to connect to each other over a reliable Ethernet connection. The connection requires a minimum throughput of 1 Gbps and a maximum round-trip latency of 30 ms.
- **Internet access**: Each Tanium Server must be able to access the Internet to download files from designated domains (see Internet URLs on page 26). Access can be direct or through a proxy server (see Tanium Console User Guide: Configuring proxy server settings).
- **Shared database and Tanium Module Server**: Each cluster member must be able to connect to the shared database server and shared Module Server. The connection requires a minimum throughput of 1 Gbps and a maximum round-trip latency of 30 ms.



You do not have to configure a Microsoft Windows cluster. The procedures provided here are based on two standalone Windows Server host computers.

Before you begin

Ensure the following conditions are met before installing the Tanium Servers:

© 2026 Tanium Inc. All Rights Reserved

- **Installer**: Ensure that you can access the Tanium Server installer: `SetupServer.exe`.
- **Tanium license**: Ensure that you can access the Tanium license file: `tanium.license`.
- **Host requirements**: The host systems must meet the hardware, software, and network connectivity requirements suitable for your deployment: see Tanium Core Platform requirements in a Windows environment on page 20.
- **User accounts**: Your Microsoft Active Directory administrator must configure the accounts that your team needs for the Tanium Core Platform deployment: see Administrator account permissions on page 31.
- **Firewall rules**: Your network administrator must configure firewall rules to allow communication on the TCP ports that the Tanium Core Platform uses. In addition to the ports that a standalone Tanium Server uses, Tanium Servers in an HA cluster send and receive HA-related data on port 17472 (TCP). For more information, see Internet access, network connectivity, and firewalls on page 26.
- **Security exclusions**: Your security team must configure exceptions to host-based security policies to allow Tanium processes to operate smoothly and at optimal performance: see Tanium Client Management Guide: Reference: Endpoint security exclusions and for Windows-based Tanium Core Platform deployments, see Tanium Core Platform User Guide for Windows Deployments: Tanium Core Platform Server security exclusions.
- **Certificates and keys**: If you want to use a certificate issued by a certificate authority (CA) for securing connections from user systems to the Tanium Servers for Tanium Console or API access, ensure that the CA-issued certificate and associated private key are present on the Tanium Servers. The certificate file name must be `SOAPServer.crt` and the key file name must be `SOAPServer.key`. During installation, you can select a CA-issued certificate or configure the Tanium Server to generate a self-signed certificate.

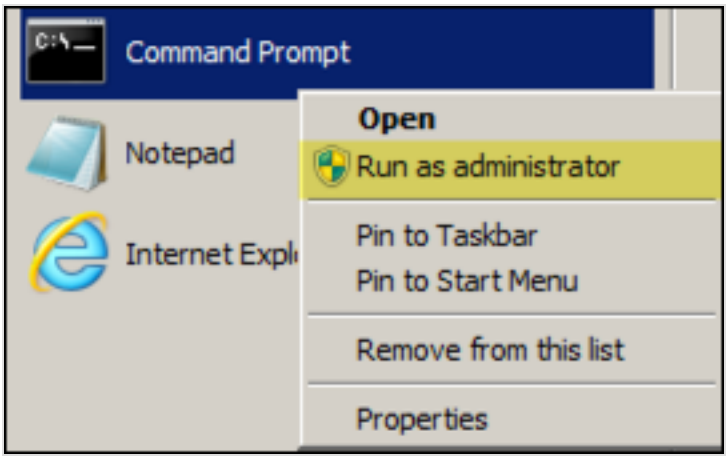
  To facilitate troubleshooting, use the self-signed certificate during initial installation and replace it with a CA-issued certificate later. This practice enables you to separate potential installation issues from TLS connection issues.

  For more information, see Securing Tanium Console, API, and Module Server access in a Windows deployment on page 77.
- **Database server**: Your database administrator must create a database server for the Tanium Core Platform deployment: see Set up a database server on page 35.

© 2026 Tanium Inc. All Rights Reserved

Deploy the HA cluster

1. Install the Tanium Server on the primary host computer as described in Install the Tanium Server on page 37.
2. Install the Tanium Module Server as described in Installing the Tanium Module Server on page 43.
3. Sign in to the secondary host computer and run the Command Prompt utility as the local administrator, which has the permissions required to create a folder in the `Program Files` directory.



4. Create the directory by running the following command, where `<drive>` is the target drive (such as `D`):
   `md "<drive>:\Program Files\Tanium\Tanium Server"`
5. Copy the following files from the Tanium Server installation directory on the primary host to the directory you just created on the secondary host:
   - `SOAPServer.crt`
   - `SOAPServer.key`
   - `tanium.license`

   IMPORTANT: Always follow the best practices of your organization for securely copying sensitive files. For example, use GNU Privacy Guard (GPG) to encrypt the files before copying and to decrypt when they are in place on the target Server.
6. If the primary Server has been deployed for days before you deploy the secondary Server, copy the `Strings` folder from the Tanium installation directory on the primary host to the same directory on the secondary host. This step is not necessary if you deploy both Servers at the same time.
7. Copy the installer (`SetupServer.exe`) to a temporary location on the secondary host.

© 2026 Tanium Inc. All Rights Reserved

8. Install the Tanium Server on the secondary host as described in Install the Tanium Server on page 37.

   NOTE

   Because you already copied the license to the appropriate directory, skip the step to copy it to a temporary location.

9. Register the remote Module Server with the second Tanium Server.

   NOTE

   Registration involves copying files between the Module Server and the Tanium Server. Both must be reachable when you issue the registration CLI command or else the command fails. For more information about using the CLI, see Reference: Tanium Core Platform Command-line interface in a Windows deployment on page 176.

   a. Access the CLI on the Module Server host and navigate to the Module Server installation directory:

   ```
   cmd-prompt>cd <Module Server>
   ```

   b. Issue the registration command, and specify a Tanium Console administrator user name and password when prompted:

   ```
   cmd-prompt>TaniumModuleServer register <Tanium_Server_FQDN>
   Enter administrator username: <username>
   Enter password for user '<username>':<password>
   Successfully completed registration.
   ```

10. Enable trust between the Tanium Servers to enable communication for HA synchronization and failover: see Tanium Console User Guide: Managing Tanium Server trust.

11. (Optional) Relocate the package file repository on page 41 on both Tanium Servers if you want to use a directory other than the default `<Tanium Server installation directory>\Downloads` directory.

12. (Optional) Integrate the Tanium Servers with a hardware security module (HSM) if your organization uses an HSM to store and manage digital keys. For more information, see Securing keys with an HSM in a Windows deployment on page 110.

13. Verify the deployment: see Verifying the deployment to your Windows environment on page 92.

HA configuration notes

Tanium Servers in an HA cluster do not automatically synchronize their Windows Registry settings. Therefore, you must repeat any changes to these settings on each Tanium Server in the cluster. Settings stored in the Windows Registry include:

- Log level
- Proxy server settings

© 2026 Tanium Inc. All Rights Reserved

- Bypass proxy settings
- Trusted host settings
- Bypass certificate revocation list (CRL) check settings

For the procedures to edit these settings, see the Tanium Console User Guide.

For guidelines on Tanium Server Windows Registry settings, see Reference: Deployment-related Tanium Core Platform settings in a Windows deployment on page 182.

© 2026 Tanium Inc. All Rights Reserved

Securing Tanium Console, API, and Module Server access in a Windows deployment

Overview of certificates and keys

Tanium user and module operations require connections to the Tanium Servers, Module Server, and Tanium module services. The Tanium Core Platform uses Secure Sockets Layer (SSL)/Transport Layer Security (TLS) certificates and keys to secure connections to the Tanium Server and Module Server (illustrated in Figure 3). For example, when you use Tanium™ Patch to deploy patches to endpoints, the Tanium Core Platform establishes connections in the following order:

1. User system (browser or CLI) to the Tanium Server (Tanium Console or API)
2. Tanium Server to Tanium Module Server
3. Module Server to Patch service
4. Patch service to Tanium Server

The Tanium Server and Module Server installers generate self-signed certificates. You can replace the self-signed certificates on Tanium Servers with certificates issued by a commercial certificate authority (CA) or your enterprise CA.

BEST PRACTICE

To facilitate troubleshooting, use the self-signed certificates during initial installation and replace them with CA-issued certificates later. This practice enables you to separate potential installation issues from TLS connection issues. Using a CA-issued certificate is highly recommended for Tanium Console and API access on the Tanium Server.

NOTE

Tanium Console and API access require user authentication through sign-in credentials, but not for securing the TLS connection.

To troubleshoot Console and API access issues, see Authentication log.

For more information about the Tanium™ Protocol that secures communication among the Tanium Servers, Zone Server, Zone Server Hub, and Tanium Clients, see Securing Tanium Server, Zone Server, and Tanium Client access. To manage the keys that the Tanium Protocol uses, see Tanium Console User Guide: Managing Tanium keys.

Tanium Console and API

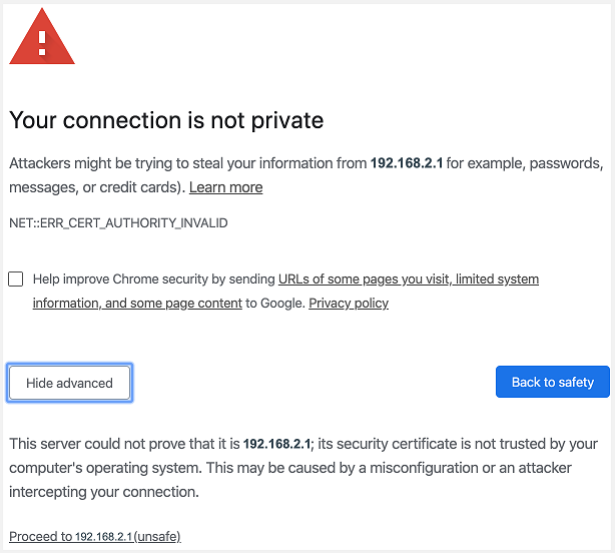
Users access Tanium Console or the Tanium API on the Tanium Server to perform Tanium operations such as issuing questions or deploying actions. The Console and API communicate over Hypertext Transfer Protocol Secure (HTTPS), which uses SSL/TLS certificates and keys to secure client-server connections. When a user accesses Tanium Console or the Tanium API, the user system

© 2026 Tanium Inc. All Rights Reserved

is the client and the Tanium Server is the server. To secure the connection, the Tanium Server presents its `SOAPServer.crt` certificate to prove its identity to the Client and uses its `SOAPServer.key` private key to complete the TLS handshake. For Console or API access, Clients do not have to prove their identity to secure the connection. Figure 3 illustrates these processes.

When you install the Tanium Server on a Windows server, you can choose between a self-signed certificate or (if one is available) a CA-issued certificate. If you use a self-signed certificate, users see a certificate validation error when they access Tanium Console or the Tanium API. The error occurs because the CA certificates on the user system cannot validate the self-signed certificate. The following figure shows an example of such an error when users try to connect from a browser to Tanium Console.

Figure 2: Certificate validation error



Even though browsers provide the option to access Tanium Console despite the error, avoiding that option is a security best practice. Therefore, Tanium highly recommends that you replace the self-signed `SOAPServer.crt` certificate with a CA-issued certificate. If the Tanium Server is currently using a self-signed certificate, you can replace it at any time.

Signed and encrypted SAML authentication on the Tanium Server

Some identity providers require a digital signature on Security Assertion Markup Language (SAML) requests from a service provider such as the Tanium Server. If you are using such an identity provider for Tanium Console authentication, you must provide a request-signing certificate (`SAMLEncryption.crt`) and private key (`SAMLEncryption.key`) to enable the identity provider to authenticate requests. The Server uses the key to sign the requests and the identity provider uses the certificate to validate the signature.

To determine the requirements of the SAML certificate and best practices for generating the certificate and key, see your identity provider documentation.

For more information about using a SAML identity provider with Tanium Console, see Tanium Console User Guide: Integrating with a SAML IdP.

© 2026 Tanium Inc. All Rights Reserved

Module Server communication

When users use Tanium Console or the Tanium API to work with Tanium modules, the Tanium Server communicates with the Tanium Module Server, the Module Server accesses the Tanium module services that it hosts (such as Patch), and the module services communicate back with the Tanium Server (see Figure 3).

The Tanium Server and Module Server communicate over HTTPS, and both Servers must prove their identities through certificates. The Tanium Server presents `SOAPServer.crt` to prove its identity, while the Module Server presents `ssl.crt`. The Servers use the associated private keys (`SOAPServer.key` and `ssl.key`) to complete the TLS handshake that secures the connection. To verify the Tanium Server identity, the Module Server checks that its `trusted.crt` file contains the `SOAPServer.crt` that the Tanium Server presented. In an active-active deployment, `trusted.crt` must contain the `SOAPServer.crt` of both Tanium Servers. Tanium Servers also verify the Module Server identity by checking that their `trusted-module-servers.crt` file contains the `ssl.crt` that the Module Server presented. The Module Server registration process generates `trusted.crt` on the Module Server and `trusted-module-servers.crt` on the Tanium Server. The Module Server installation process generates `ssl.crt`.

The Module Server opens a single HTTPS listener to route requests from the Tanium Server to Tanium module services, which listen only on localhost. TLS termination occurs on the Module Server, which forwards the requests locally over non-TLS connections from the HTTPS listener to the appropriate module service.

Module services connect to the Tanium Server over TLS and verify that the certificate that the Tanium Server presented during the TLS handshake is included in the `trusted.crt` file on the Module Server. Because module services use the same API as Tanium Console users, Client certificate validation is not enforced.

If you replace the `SOAPServer.crt` certificate on the Tanium Server, you must re-register the Module Server with the Tanium Server to regenerate the `trusted.crt` and `trusted-module-servers.crt` files.

The following table summarizes the certificates and keys that the Tanium Core Platform uses for connections to the Module Server:

Certificates and keys for Module Server connections

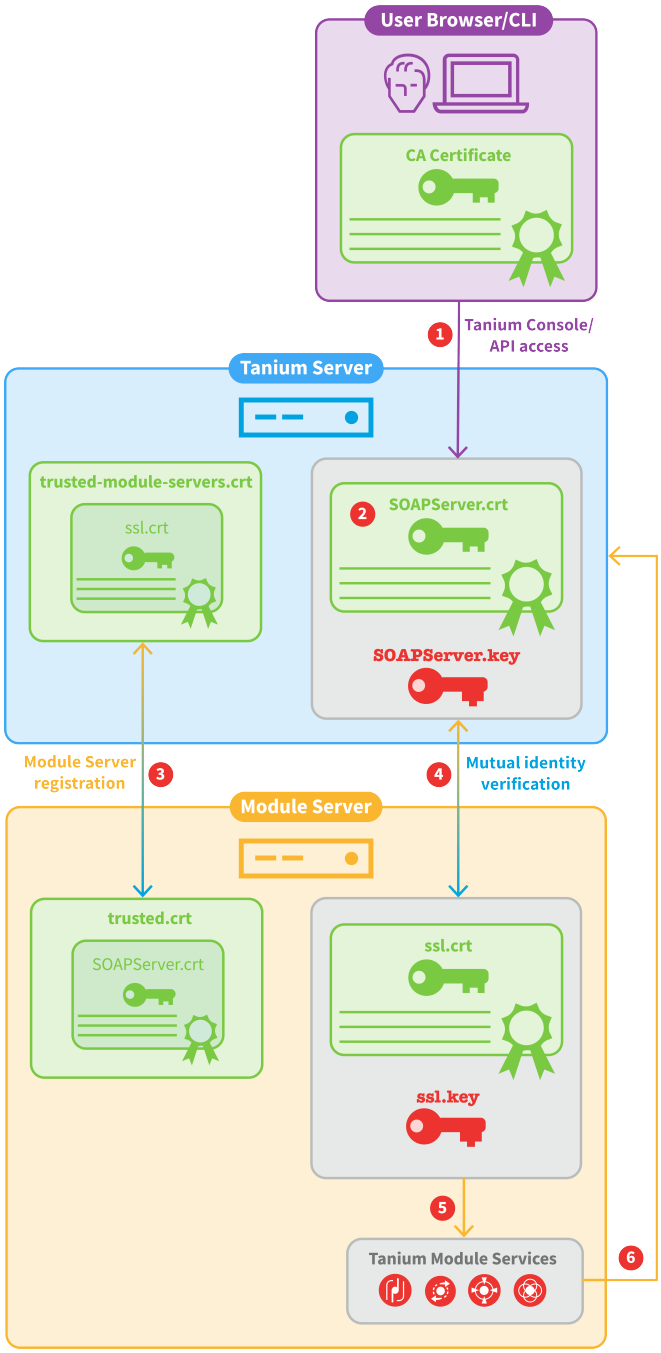
Location	File Name	Purpose
Module Server	`ssl.crt` `ssl.key`	HTTPS certificate and private key that the Module Server presents to secure incoming connections from the Tanium Server or outgoing connections to Tanium services.
	`trusted.crt`	Contains the `SOAPServer.crt` of the Tanium Servers with which the Module Server has registered. The Module Server uses `trusted.crt` to validate Tanium Server certificates.
Tanium Server	`SOAPServer.crt` `SOAPServer.key`	HTTPS certificate and private key that the Tanium Server presents to secure outgoing connections to the Module Server or incoming connections from the systems of Tanium Console users or Tanium API users.
	`trusted-module-servers.crt`	Contains the `ssl.crt` of the Module Server that has registered with the Tanium Server. The Tanium Server uses `trusted-module-servers.crt` to validate the Module Server certificate.

© 2026 Tanium Inc. All Rights Reserved

SSL/TLS connection processes and setup tasks

The following figure illustrates the components, processes, and setup tasks involved in securing connections to the Tanium Server (Tanium Console or API) and Module Server.

Figure 3: SSL/TLS connections



The following processes correspond to the numbers in Figure 3.

© 2026 Tanium Inc. All Rights Reserved

1 **Tanium Console/API access**

When a user system connects to Tanium Console or the Tanium API, the Tanium Server presents its `SOAPServer.crt` certificate to prove its identity to the user system. In Figure 3, the Server uses a CA-issued version of `SOAPServer.crt` (number 2) instead of a self-signed version. Therefore, the user system uses a CA certificate to validate `SOAPServer.crt`.

2 **Replace self-signed certificate with CA-issued certificate**

Generate a certificate signing request (CSR) and associated private key `SOAPServer.key` for the Tanium Server. You submit the CSR to your CA, which uses a CA certificate and associated private key to digitally sign the requested certificate (`SOAPServer.crt`). The CA signing certificate must also be present on the systems from which users access Tanium Console or the Tanium API (number 1). The Tanium Server can then use the requested CA-issued certificate instead of a self-signed certificate.

3 **Module Server registration**

During a fresh installation of the Module Server, you must manually enable trust between it and the Tanium Server before registration. The Module Server then registers with the Tanium Server and the Servers generate the `trusted-module-servers.crt` and `trusted.crt` files. For subsequent communication between the Servers, including during version upgrades, trust is already established, and the Servers automatically check `trusted-module-servers.crt` and `trusted.crt` during their mutual identity verification (number 4).

For information about manually enabling trust for the server certificates by verifying or entering certificate *fingerprints* (hash digests of certificate public keys) during installation on Windows, see Trust Tanium Server certificate.

4 **Mutual identity verification**

To establish a secure TLS connection, the Tanium Server and Module Server prove their identities to each other. During the TLS handshake, the Tanium Server presents its `SOAPServer.crt` certificate to the Module Server, which verifies that its `trusted.crt` file contains `SOAPServer.crt`. Also during the handshake, the Module Server presents its `ssl.crt` certificate to the Tanium Server, which verifies that its `trusted-module-servers.crt` file contains `ssl.crt`.

5 **Module Server to Tanium module services**

The Module Server opens a single HTTPS listener to route requests from the Tanium Server to Tanium module services, which listen only on localhost. The Module Server forwards the requests locally over non-TLS connections from the HTTPS listener to the appropriate module service.

6 **Module services to the Tanium Server**

Module services connect to the Tanium Server over TLS and verify that the certificate that the Tanium Server presented during the TLS handshake is included in the `trusted.crt` file on the Module Server. Because module services use the same API as Tanium Console users, Client certificate validation is not enforced for this connection (in contrast with the connection described in number 4).

© 2026 Tanium Inc. All Rights Reserved

CA-issued Tanium Server SOAP certificates

If your organization prefers to use CA-issued certificates to secure connections to systems, you can replace the self-signed certificates that the Tanium Server (`SOAPServer.crt`) generated during installation. In an active-active deployment, you can use the same CA-issued `SOAPServer.crt` (and associated private key) for both Tanium Servers as long as the Subject Alternative Name in the certificate specifies both Server names. Alternatively, you can use a distinct CA-issued certificate for each Tanium Server.

Obtaining a CA-issued certificate involves submitting a CSR to the CA and generating an associated private key. Use Tanium Console to create a CSR and replace the `SOAPServer.crt` certificate for the Tanium Server. For more information, see Tanium Console User Guide: Managing SSL/TLS certificates.

The CA uses a CA certificate and its associated private key to digitally sign the certificate that you requested. If a CA-issued certificate replaces `SOAPServer.crt` on the Tanium Server, then the CA signing certificate must also be present on the systems from which users access Tanium Console or the Tanium API. For Console users, the CA signing certificate must be in the trusted certificates store of their browsers. For API users, the CA signing certificate must be in the location specified in API calls, as shown in the `--cacert <file path>` option in the following example:

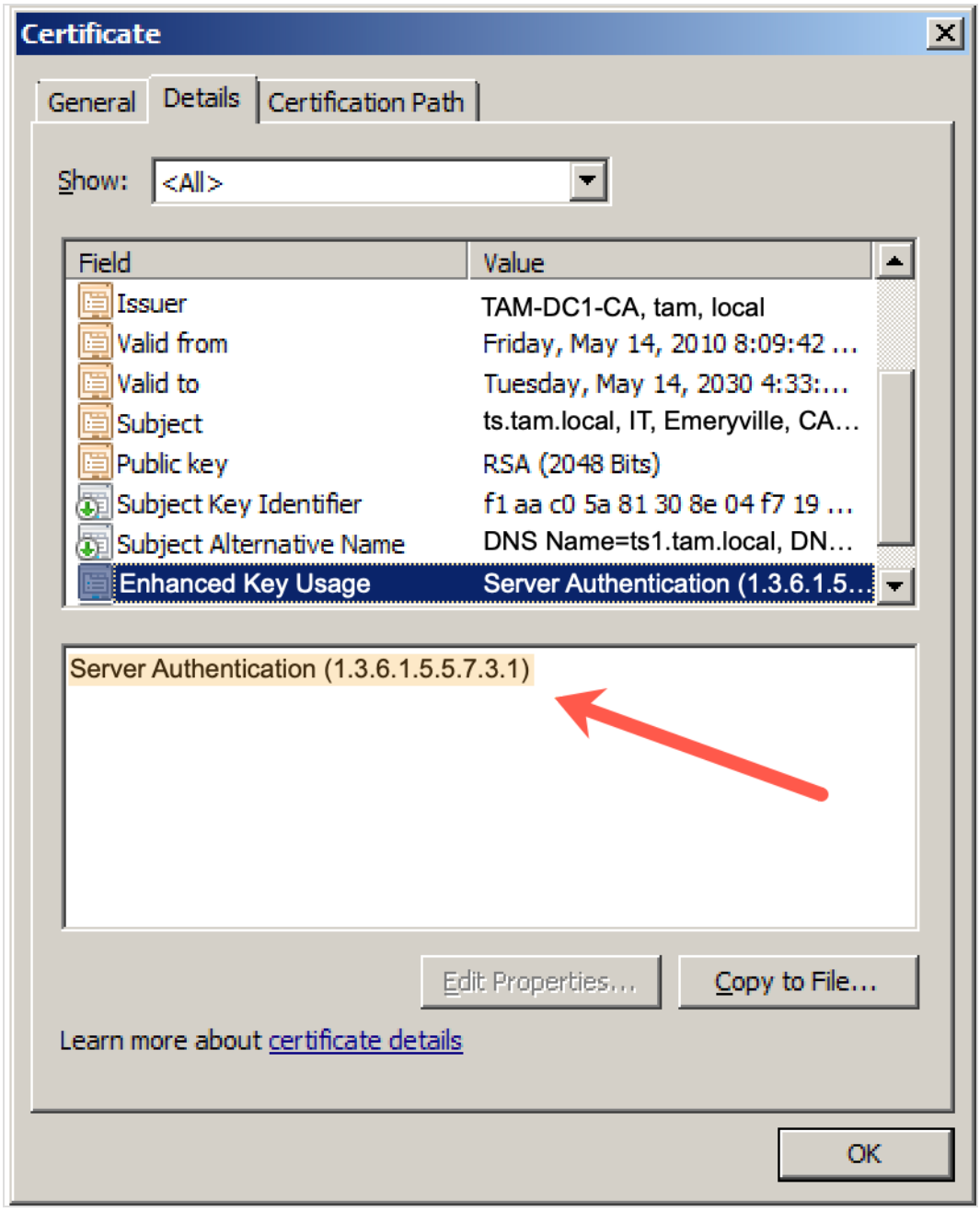
```
$ curl -s --cacert <file path> -X POST --data-binary @<sign in>.json
https://localhost/api/v2/session/login
```

Certificate requirements

Work with your CA to obtain a certificate with the following specifications for the Tanium Server SOAP certificate:

© 2026 Tanium Inc. All Rights Reserved

- X.509 certificate with TLS Web Server Authentication extended key usage



- Separate certificate and private key files.

> IMPORTANT
> You must remove the passphrase from the key file.

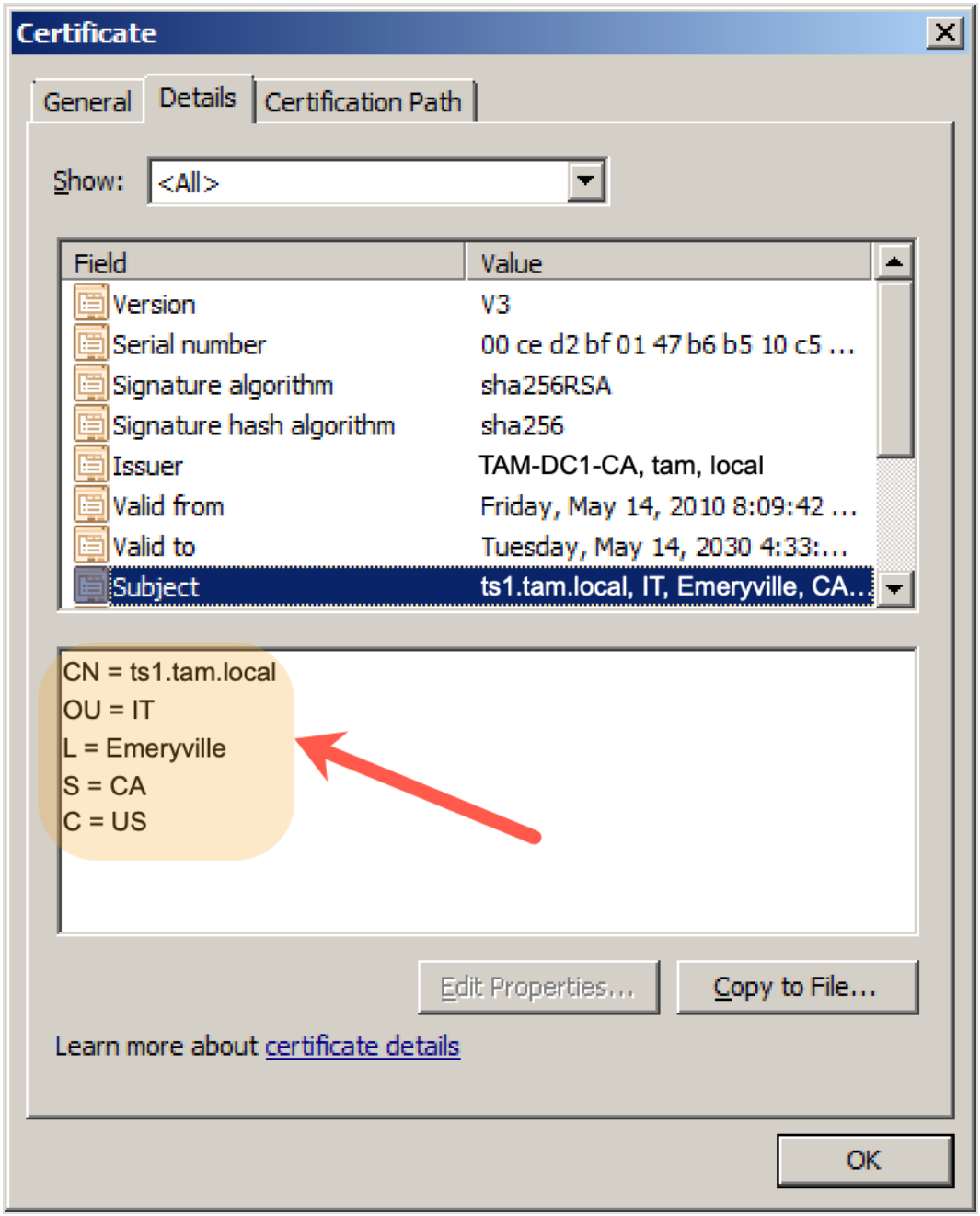
- PEM format (Base64 encoded)
- Certificate signed with a SHA-256 hashing algorithm

© 2026 Tanium Inc. All Rights Reserved

- RSA encryption with a key length of at least 2048 bits

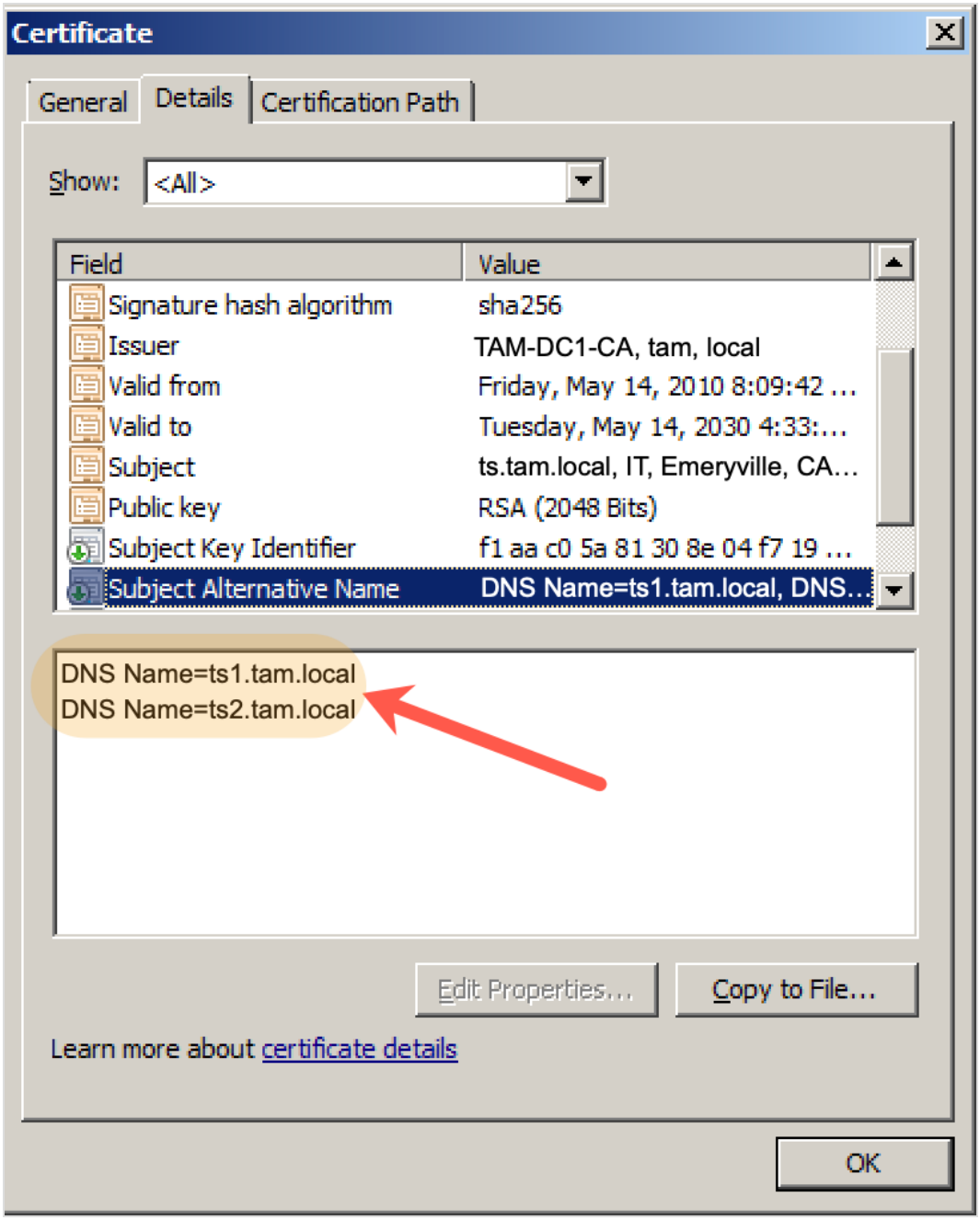
> TIP
>
> Secure certificates for server and client systems are required. To check key sizes, use OpenSSL from a CLI. If your Tanium license includes Tanium Certificate Manager, see Tanium Certificate Manager User Guide: View short keys for the steps to check the key sizes in your environment.

- Common Name (CN) that specifies the fully qualified domain name (FQDN) or IP address of the Tanium Server.



© 2026 Tanium Inc. All Rights Reserved

- Subject Alternative Name that also specifies the FQDN or IP address of the Server, as well as that of the secondary Tanium Server in an active-active deployment where both Servers use the same certificate. Web browsers typically require the Subject Alternative Name to be present, regardless of whether the certificate applies to multiple Servers.



© 2026 Tanium Inc. All Rights Reserved

- If the certificate is part of a chain that includes an intermediate certificate, the certificate file must include the entire chain. If you receive the certificates as individual files, build a single file for the chain:

  1. Use a text editor to create a new text file.
  2. Paste the entire body of each certificate into the text file in the following order:

     a. Server certificate (`SSL.crt` or `SOAPServer.crt`)

     b. Intermediate certificate

     c. CA certificate

     Be sure to include the beginning tag (`-----BEGIN CERTIFICATE----`) and ending tag (`-----END CERTIFICATE----`) of each certificate.

  3. Save the text file with the file name of the original server certificate (`SSL.crt` or `SOAPServer.crt`).

(Optional) Enable HTTP Strict Transport Security for Tanium Console access

If you have installed a valid CA-issued certificate, you can optionally enable HTTP Strict Transport Security (HSTS) on the Tanium Server. To do so, you add the `Strict-Transport-Security` HTTP header, which notifies browsers to always use HTTPS to connect to Tanium Console after a user accesses the Console using HTTPS the first time. In an active-active deployment, you must perform this procedure on both Tanium Servers.



Do not enable HSTS if you have not installed a CA-issued certificate. Doing so disables access to Tanium Console.

1. From the Tanium Console Main menu, go to **Administration > Configuration > Settings > Advanced Settings** and click **Add Setting**.
2. Configure the following properties and then click **Save.**

   - **Setting Type**: Local
   - **Platform Setting Name**: `DefaultHeaders`
   - **Value Type**: Text
   - **Value**: `Strict-Transport-Security: max-age=31536000; includeSubDomains`

     You can use any value that your organization policies recommend for `max-age`, which is the value that instructs the browser on how long, in seconds, to use HSTS for the Tanium Server address. The recommended minimum value is `31536000` (one year).

© 2026 Tanium Inc. All Rights Reserved

Securing Tanium Server, Zone Server, and Tanium Client access in a Windows deployment

Overview of TLS in the Tanium Core Platform

Communication protocols

All supported versions of the Tanium Core Platform use the following protocols for communication among platform components:

- **Tanium™ Protocol**: This application protocol is proprietary to Tanium and uses TLS 1.3 to encrypt communication.

  IMPORTANT

  You cannot use network devices such as firewalls to decrypt and inspect Tanium Protocol traffic.

- **Hypertext Transfer Protocol Secure (HTTPS)**: The Tanium Core Platform uses TLS 1.3 to encrypt HTTPS communication among platform components. The components negotiate the TLS version for HTTPS connections with external servers but enforce TLS 1.2 as the minimum version.

The following table lists the connections among Tanium Core Platform components and the protocol that each connection uses. The numbers correspond to the connections in Figure 4.

TLS communication in the Tanium Core Platform

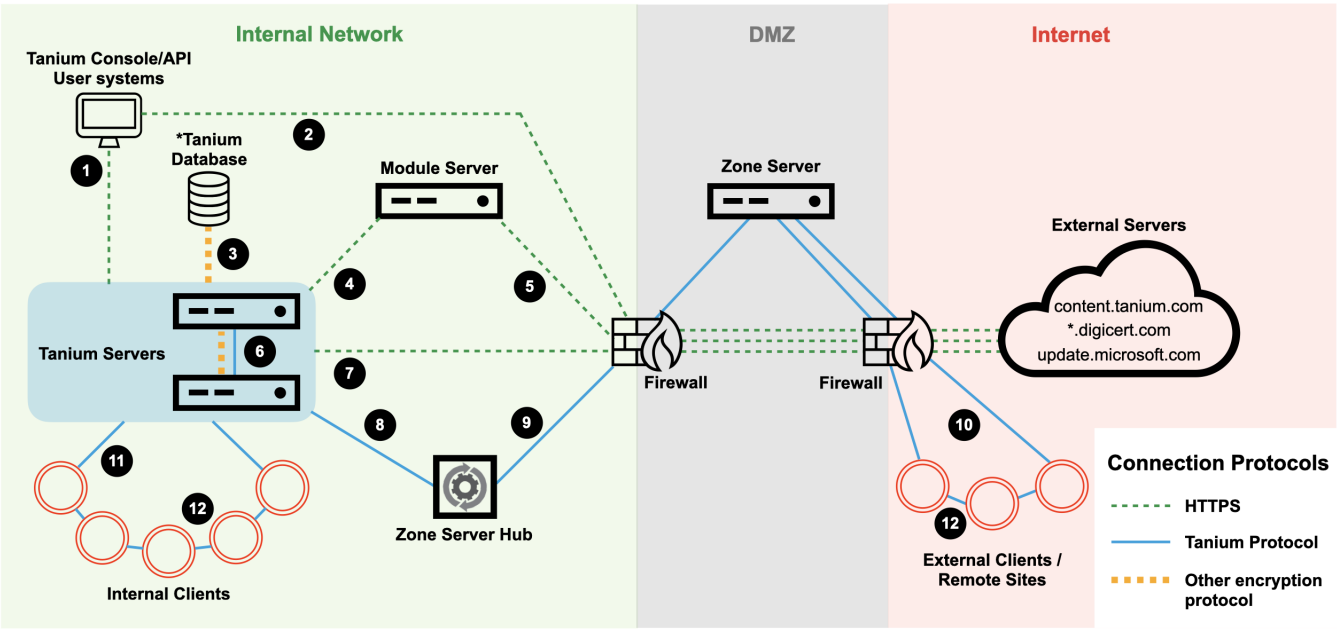
Connection		Protocol
1	Tanium Console or API user systems to Tanium Servers	HTTPS
2	Tanium Console or API user systems to external servers, such as `content.tanium.com`	HTTPS
3	(Windows only) Tanium Servers to Tanium database in deployments where the database is not on the Tanium Server host	By default, communication is over TCP/IP without encryption, but configuring encryption is a best practice. Consult your database administrator.
4	Tanium Servers to Tanium Module Server	HTTPS
5	Module Server to external servers	HTTPS
6	Tanium Server to Tanium Server in an active-active deployment	Tanium Protocol
7	Tanium Servers to external servers	HTTPS

© 2026 Tanium Inc. All Rights Reserved

TLS communication in the Tanium Core Platform (continued)

Connection		Protocol
8	Tanium Servers to Zone Server Hub Figure 4 shows the Zone Server Hub installed on a host that is separate from the Tanium Server hosts to illustrate that the connection is encrypted. However, in most deployments, you install the hubs on the same hosts as the Tanium Servers.	Tanium Protocol
9	Zone Server Hub to Zone Server	Tanium Protocol
10	Tanium Clients (external) to Zone Server	Tanium Protocol
11	Tanium Clients (internal) to Tanium Servers	Tanium Protocol
12	Tanium Client to Tanium Client (external and internal)	Tanium Protocol

Figure 4: TLS communication in the Tanium Core Platform



NOTE

To manage the certificates and keys that the Tanium Core Platform uses for HTTPS traffic, see Securing Tanium Console, API, and Module Server access.

To manage the certificates and credentials for securing connections between Tanium Core Platform Servers and remote sources of content (such as packages), see Tanium Console User Guide: Managing remote authentication.

For additional details and procedures related to the digital keys for Tanium Protocol traffic, see Tanium Console User Guide: Managing Tanium keys.

© 2026 Tanium Inc. All Rights Reserved

NOTE

The Tanium Core Platform supports TLS for additional connections that various Tanium modules and shared services require. For more information, see the User Guides for your Tanium products.

To troubleshoot TLS communication issues, see PKI TLS logs.

TLS communication process

TLS communication starts when a TLS client initiates a TLS handshake to establish a secure connection with a server. The following are examples in the context of the Tanium Core Platform:

- The Zone Server acts as a client when registering with the Tanium Server.
- The Tanium Client acts as a client when registering with the Zone Server or Tanium Server.
- A Tanium Server acts as a client when performing active-active synchronization with another Tanium Server.

During the TLS handshake, the client and server generate a shared, unique session key, which they use to secure communication for the duration of their session. You can configure TLS as optional for Tanium Clients. If the handshake fails and TLS is optional, the client and server attempt a non-TLS (unencrypted) connection instead. If the handshake fails and TLS is configured as required, the client and server cannot connect.

Supported cipher suites

The Tanium Core Platform supports the following cipher suites for creating keys and encrypting information in TLS communication:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-RSA-CHACHA20-POLY1305

TLS options, and defaults

After a fresh installation or upgrade, TLS is required for the Tanium Server (including between Tanium Servers in an active-active deployment), Zone Server, and Zone Server Hub, and you cannot disable it. The Tanium Server installer generates the TLS public and private keys that are used to set up TLS for connections with the Tanium Server.

After a fresh installation or upgrade, TLS is required by default for endpoints. You can optionally configure this requirement.

© 2026 Tanium Inc. All Rights Reserved

Contact Tanium Support and consult your network security team before modifying the TLS configuration. Whether TLS is available and required depends on the Tanium Core Platform version, components, and infrastructure:

HSM integration

If your organization uses a hardware security module (HSM) to store and manage keys, you can configure the Tanium Server to integrate with the HSM. For more information, see Securing keys with an HSM.

(Optional) Configure the TLS requirement for Tanium Client connections

The Tanium Core Platform also requires TLS for incoming connections from endpoints by default. You can configure the TLS requirement for Tanium Client.

From the Tanium Console Main menu, go to **Administration > Configuration > Settings > Advanced Settings**, and configure the **require_client_tls_315_flag** setting for connections from Tanium Clients to the Tanium Server:

- `1` (default): The Tanium Server allows connections from endpoints with Tanium Client only if TLS is used. Tanium strongly recommends that you leave the value at `1`.
- `0`: The Tanium Server allows both TLS and non-TLS connections from endpoints. Contact Tanium Support before setting the value to `0`.



These settings also apply to connections from Tanium Clients to the Zone Server if you deploy one.

Configure TLS on Tanium Clients

After a fresh installation or upgrade, TLS is enabled and required by default. Tanium strongly recommends that you use these default settings.

Perform the following steps to enable or disable TLS on Tanium Clients:

1. From the Main menu, go to **Administration > Configuration > Client Status**.
2. In the **Filter by Registration** section, select **Registered using TLS** and **Registered unencrypted** if they are not already enabled.
   The **Using TLS** column indicates which Tanium Clients have TLS enabled or disabled.
3. From the Main menu, go to **Administration > Configuration > Settings > Advanced Settings** and configure the **TLSMode** setting for the Tanium Clients:
   - `0` (TLS not used): TLS is disabled.
   - `1` (TLS required): If a TLS handshake fails, the Tanium Client cannot communicate with other Clients or the Servers. This is the default value.

© 2026 Tanium Inc. All Rights Reserved

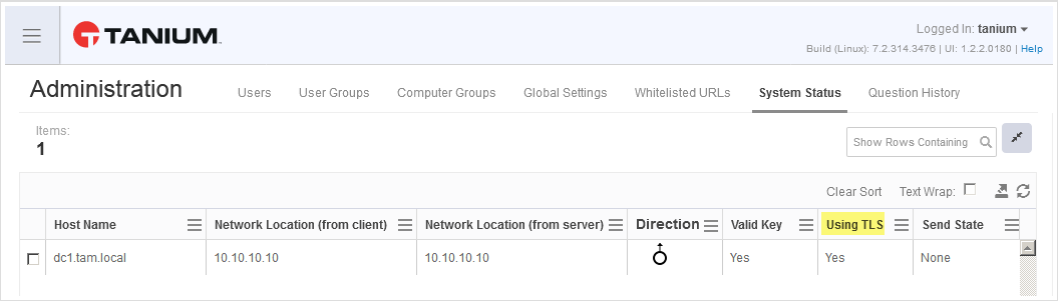
On the Tanium Client endpoint, the setting name is **Server_TLSMode**, with the **Server_** prefix indicating that the Tanium Client received the settings from platform settings on the Tanium Server during registration, and future registration updates might change the settings. In some cases, you might want a Tanium Client to use a setting that differs from the Tanium Server platform setting. To override the Tanium Server platform settings, add the **TLSMode** setting (without the **Server_** prefix) to the Tanium Client settings on the Client endpoints.



It takes two to six hours (the randomized client-reset interval) for Clients to register and receive the updated settings.

Verify the TLS connections

Verify whether Tanium Clients used TLS to connect with the Tanium Server or Zone Server when the Clients last registered: from the Main menu, go to **Administration > Configuration > Client Status** and check the **Using TLS** column.



Update the TLS configuration when you make changes to key pair

When you add or revoke Tanium root keys, the Tanium Server automatically propagates the changes to all subordinate keys on the platform Servers and Tanium Clients (see Tanium Console User Guide: Managing Tanium keys).

© 2026 Tanium Inc. All Rights Reserved

Verifying the deployment to your Windows environment

After you install the Tanium Server (standalone or high availability (HA) cluster), Tanium Module Server, and optional Tanium Zone Server, verify that the Servers are installed correctly and can communicate with all the necessary components of the Tanium Core Platform. If any verification step fails, see Troubleshoot Server installation and upgrade issues on page 128.

1. Sign in to Tanium Console of each Tanium Server as described in Tanium Console User Guide: Sign in through the Tanium Server. If the sign-in page shows both single sign-on (SSO) and password authentication options, click **Sign In with Password**. Enter the administrator **Username** and **Password** that you set when running the Tanium Server installation wizard: see Set Administrator Account on page 41.

2. Verify that each Tanium Server connects to a remote Module Server: Go to the Tanium Console info page (`https://<Tanium Server FQDN>/info` and search for `Module Count`. If the entry lists `127.0.0.1`, the Tanium Server is using the local Module Server, and you must revisit the steps you performed to install the Tanium Server and remote Module Server.

Module Cache	
Local Module Count	6
Module Definition Count	21
tms1.tam.local:17477 Certificate	{ "CertificateDetails" : { "ExtensionCount" : 0, "Extensions" : [], "Fingerprint" : "88b94e8f82a5f52cc13499d859cba821a0a1d5eb", "Issuer" : "/CN=tms2.tam.local", "SerialNumber" : "-07650118", "Subject" : "/CN=tms2.tam.local" } }
tms1.tam.local:17477 Connected	Success
tms1.tam.local:17477 Module Count	15

3. Import Tanium modules and shared services: see Tanium Console User Guide: Manage Tanium solutions. Successful imports indicate that all the Tanium Servers can connect to `content.tanium.com`.

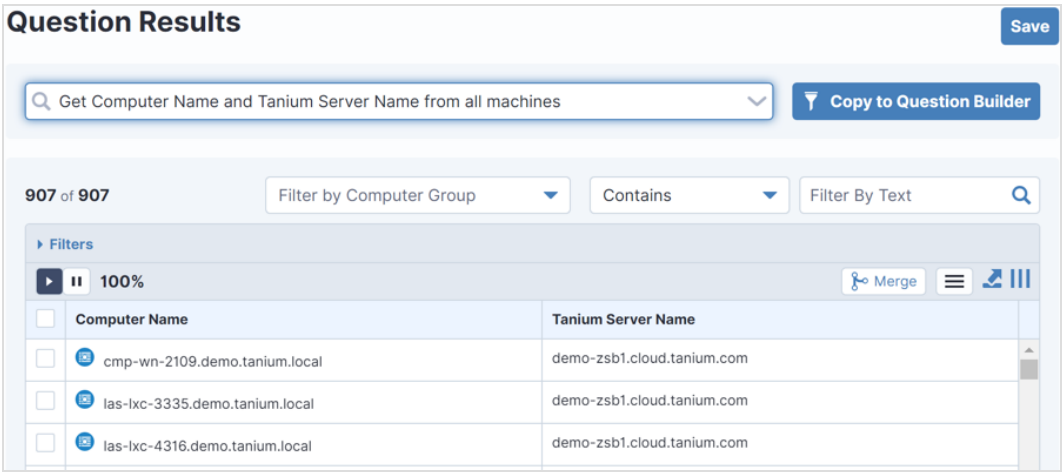
> **NOTE** The import process installs the actual solutions onto the Module Server that all Tanium Servers share, but installs the solution workbenches on the Tanium Servers.

© 2026 Tanium Inc. All Rights Reserved

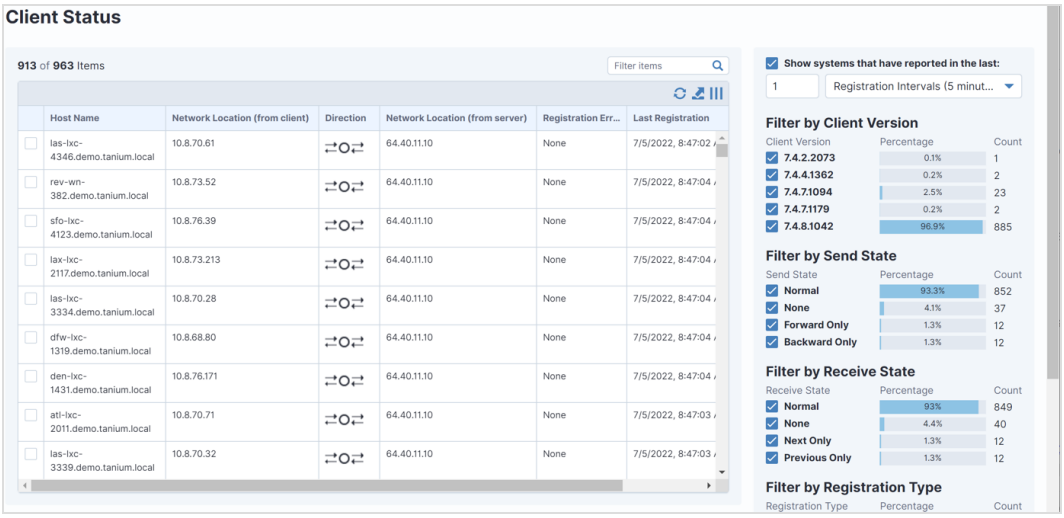
4. Verify that Tanium Clients register with the Tanium Servers or Tanium Zone Servers and reply to questions.

   a. Deploy Tanium Clients to endpoints. For more information, see Tanium Client Management User Guide.

   b. Use Interact to issue the question `Get Computer Name and Tanium Server Name from all machines`.
   Verify that the **Question Results** grid shows that Tanium Clients have registered with the correct Tanium Server or Zone Server, as specified in the **Tanium Server Name** column.



   c. Review recent Tanium Client registration details at **Administration > Management > Client Status**.
   Successful registration indicates the Tanium Clients installed correctly and can communicate with the Tanium Server or Zone Server.



© 2026 Tanium Inc. All Rights Reserved

5. (HA deployments only) Verify that both Tanium Servers in the HA cluster can download packages with URL-specified files when such a package is created or imported. The following sub-steps use **Distribute Application Management Tools** as an example of a package with URL-specified files.

   If authentication is required for Tanium Servers to download files from remote source, configure authentication before proceeding. For more information, see Tanium Console User Guide: Managing remote authentication.

© 2026 Tanium Inc. All Rights Reserved

a. From the Main menu, go to **Administration > Content > Packages**.

© 2026 Tanium Inc. All Rights Reserved

b. Select **Distribute Application Management Tools**, click **Status**, and verify that the **Cached on** value appears for both Servers.

© 2026 Tanium Inc. All Rights Reserved

© 2026 Tanium Inc. All Rights Reserved

6. (HA deployments only) Create a new package and specify a locally uploaded file: see Tanium Console User Guide: Create a package. After you save the package, wait a moment for HA synchronization to occur, and then repeat the previous step to verify that all the Tanium Servers in the HA cluster downloaded and cached the files.

BEST PRACTICE

After verifying that your deployment is in a functional state, consider planning regular backups as part of your disaster recovery plan. For more information, see Back up Tanium Core Platform Servers and databases on page 124.

© 2026 Tanium Inc. All Rights Reserved

Configuring smart card authentication in a Windows deployment

The Tanium™ Console supports *smart card authentication*. A smart card is physical credential that has a microchip and data, such as secure certificates and keys. Smart cards are also known as common access cards (CAC) and personal identity verification (PIV) cards. Endpoint systems are set up with smart card readers, and end users use their smart card to authenticate and gain access.

Requirements

When smart card authentication is enabled, the Tanium Server and Tanium Module Server must reside on separate hosts. All authentication to Tanium Console requires smart cards unless the authentication request is from one of the following sources:

- The system hosting the Tanium Server through the local loopback address (127.0.0.1 for IPv4 or [::1] for IPv6).
- The Module Server connection to the Tanium Server.

Consequently, any additional integrations that you want to automate must reside on one of the two hosts. The following are some examples:

- SSRS plugin
- Microsoft Excel plugin (unless using the version that supports smart card authentication)
- Tanium™ Connect for Lightweight Directory Access Protocol (LDAP) synchronization
- PyTan
- Thrid-party security operations center (SOC) websites that query Tanium for data

IMPORTANT

An air gap deployment with smart card authentication has additional caveats:

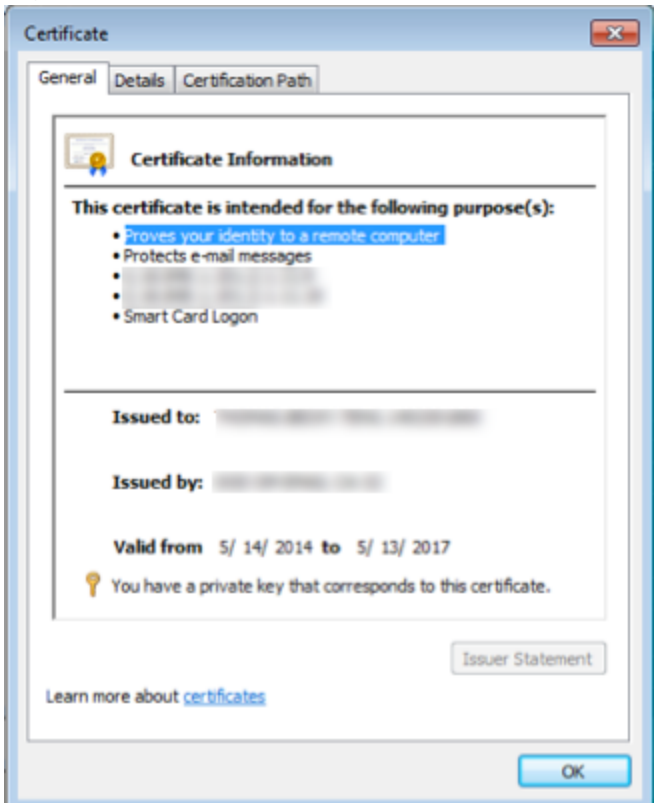
- Links to content that is hosted on the Tanium Server must use the local loopback address. This is because the TDownloader service that downloads content to the Tanium Server cannot present a certificate.
- Links to Tanium module or shared service imports use both the local loopback address (for the workbench) and the Tanium Module Server fully qualified domain name (FQDN) for the portion of the solution installed on the Module Server.

Create a certificate

Smart card authentication for Tanium Console access depends on the public key infrastructure (PKI) of your organization. You can get started if you have a Client certificate that is signed by the root certificate authority (CA) certificate for the domain where the Tanium Server is deployed. Make sure the certificate has the **Proves your identity to a remote computer** attribute.

© 2026 Tanium Inc. All Rights Reserved

Figure 5: Proves your identity to a remote computer



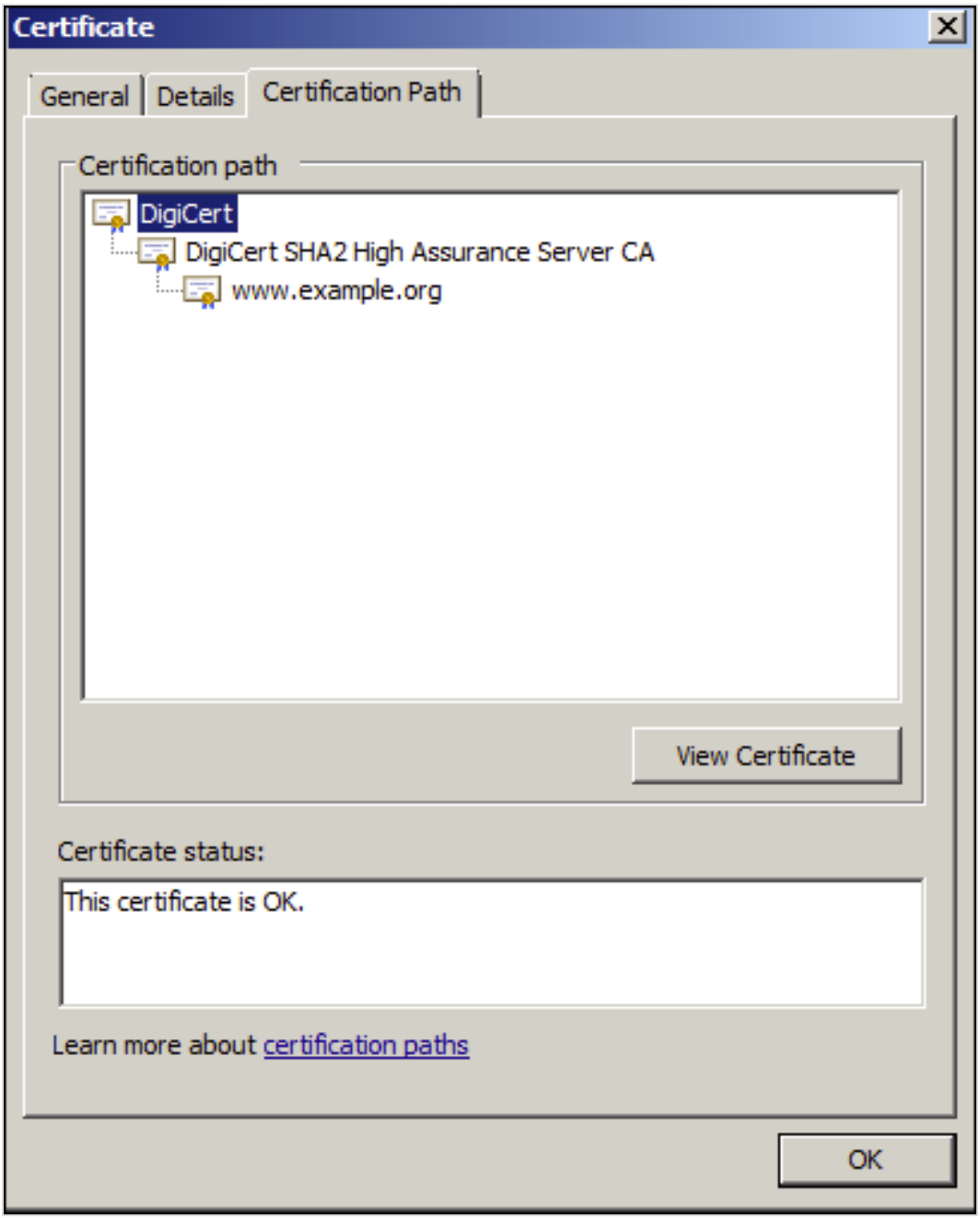
Create a new certificate file from certificates that you extract from the Client certificate. Usually, you need to extract only the root certificate. If this does not work, you might also need to add intermediate certificates to the certificate chain.

Extract the certificates

1. Get a copy of a Client certificate file that is signed by the root CA certificate for the domain. For more information, see Figure 5.
2. On a Windows endpoint, double-click the certificate file to open it in the Windows Certificate Snap-In.

© 2026 Tanium Inc. All Rights Reserved

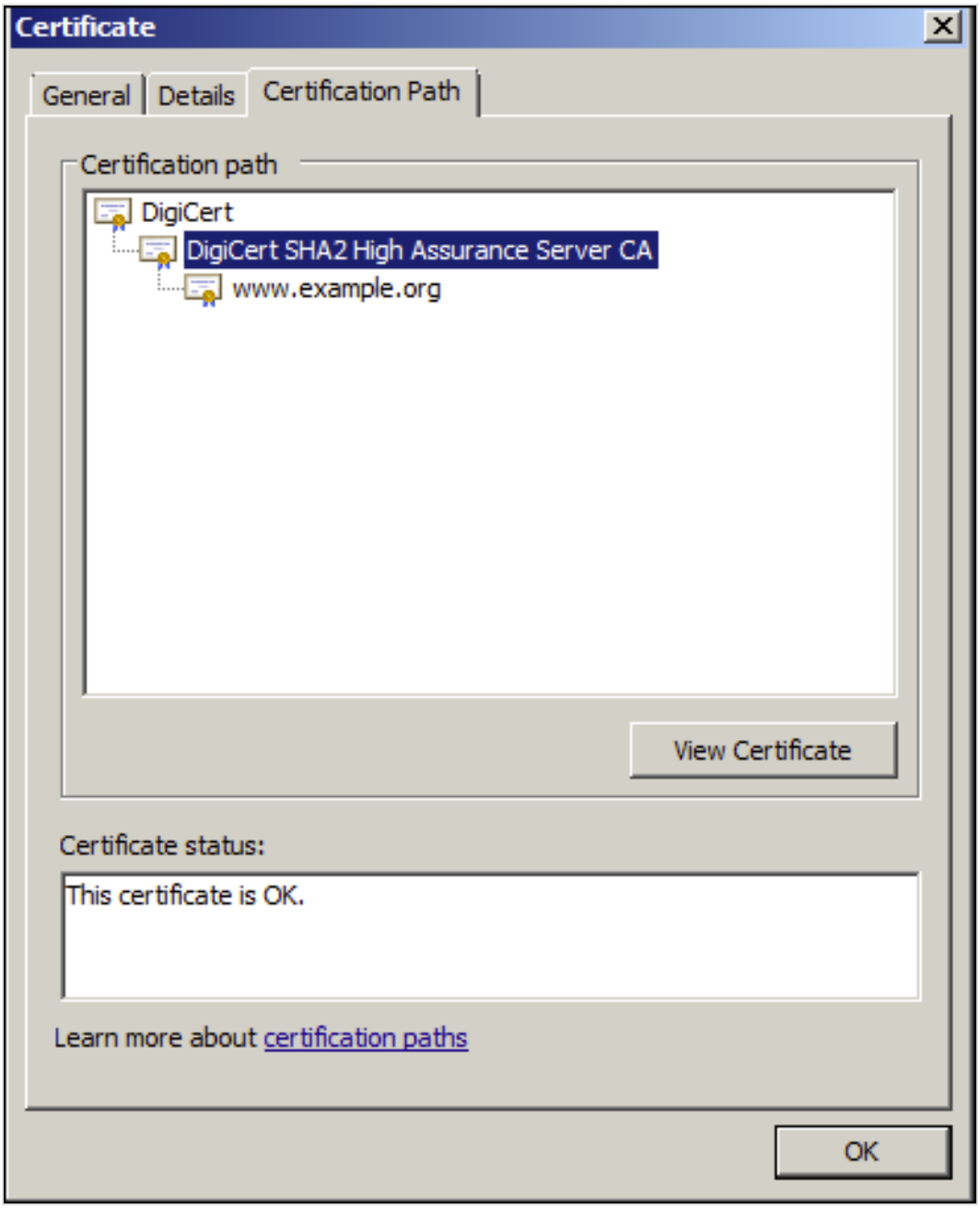
3. On the **Certification Path** tab, select the root certificate. In this example, DigiCert is the root certificate.



4. Go to the **Details** tab and click **Copy to File** to display the Certificate Export Wizard.
5. Select **Base-64 encoded X.509 (.CER)**.
6. Select a folder and specify a file name such as `example1.cer`.
7. Review the settings and click **Finish** to save the certificate.

© 2026 Tanium Inc. All Rights Reserved

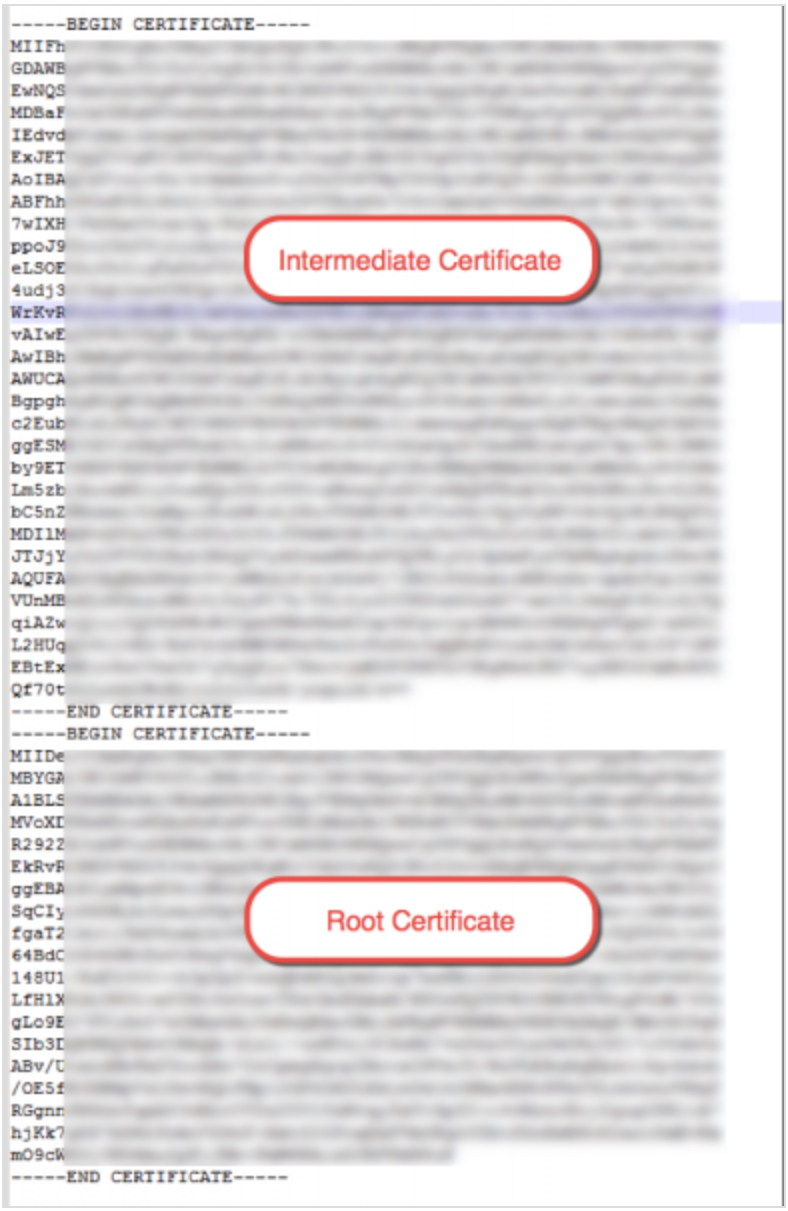
8. If your deployment has intermediate CA certificates, repeat these steps to extract them. Go to the **Certification Path** tab and select the next certificate in the chain. In the following example, DigiCert SHA2 High Assurance Server CA is the next certificate. Export this certificate with a name such as `example2.cer`.



© 2026 Tanium Inc. All Rights Reserved

Create a new certificate file

1. Create a file named `cac.pem`.
2. Copy and paste in the contents of each certificate in the chain into the file.



IMPORTANT

- Each section of the certificate file must start with `-----BEGIN CERTIFICATE-----` and end with `-----END CERTIFICATE-----`.
- There must be only one carriage return between each certificate in the chain.

© 2026 Tanium Inc. All Rights Reserved

IMPORTANT

- There must be no extra white spaces or carriage returns at the beginning or end of the file.
- The preceding example shows the root certificate last, which is a convention that Tanium Support uses.

3. Save the file.

Configure CAC

Step 1: Copy the certificate to the Tanium Server installation directory

Copy the file to the Tanium Server installation directory, which by default is `\Program Files\Tanium\Tanium Server`.

Step 2: Add Windows registry keys on Tanium Server host

1. Add Windows registry key entries as described in the following tables.
2. Open the Windows **Services** program, right-click the **Tanium Server** service, and select **Restart**.

Enable smart card authentication

Location	HKLM\Software\Wow6432Node\Tanium\Tanium Server
Value	ForceSOAPSSLClientCert
Value Type	REG_DWORD
Valid Range	`0` or `1`
Default Value	1
Guidelines	Optional. If the registry value does not exist (but other CAC/PIV registry values do exist), or is set to a value of `1`, CAC/PIV authentication becomes mandatory. NOTE: The design supports the value `0` to turn off Client certificate authentication and use the Tanium Console sign in credentials instead. However, the current implementation to support the value `0` is not finished. At this time, set the value only to `1`.

Certificate attribute to be matched

Location	HKLM\Software\Wow6432Node\Tanium\Tanium Server
Value	ClientCertificateAuthField
Value Type	REG_SZ

© 2026 Tanium Inc. All Rights Reserved

Certificate attribute to be matched (continued)

Valid Range	Any valid certificate field.
Default Value	Subject
Guidelines	Optional. If it is not defined, certificate authentication matches on the Subject field. Specify a value for this key if you want to match on a different attribute. Many organizations use `X509v3 Subject Alternative Name`. **Note**: X509v3 is typically hidden when displayed in Windows. Note that the string `X509v3` is case sensitive.

Regular expression to match

Location	HKLM\Software\Wow6432Node\Tanium\Tanium Server
Value	ClientCertificateAuthRegex
Value Type	REG_SZ
Valid Range	Any valid regular expression.
Default Value	.*CN=(.*)$
Guidelines	Optional. If it is not defined, the default regular expression is used to match the user's identifier.  BEST PRACTICE Use the following expression to match any Subject Alternative Name entry: `.*:\s(\d+\.?\w?)@.*`

Location of the smart card certificate file

Location	HKLM\Software\Wow6432Node\Tanium\Tanium Server
Value	ClientCertificateAuth
Value Type	REG_SZ
Valid Range	Any valid certificate file.
Default Value	None
Guidelines	Defines the location of the certificate file to use for authentication, such as `D:\Program Files\Tanium\Tanium Server\cac.pem`.  NOTE The path name is case sensitive.

© 2026 Tanium Inc. All Rights Reserved

Define trusted systems and components

Location	HKLM\Software\Wow6432Node\Tanium\Tanium Server
Value	CACTrustedAddresses
Value Type	REG_SZ
Valid Range	A comma-separated list of FQDNs.
Default Value	None
Guidelines	Defines which endpoints to exempt from CAC authentication requirements. These systems do not require a CAC/PIV certificate to authenticate and work for all Tanium assets. Specify the Tanium Server and Module Server. In an active-active deployment, configure this setting on both Tanium Servers to prevent TDownloader errors. Specify additional addresses to exempt any other trusted systems and components.

(Optional) LDAP server

Location	HKLM\Software\Wow6432Node\Tanium\Tanium Server
Value	cac_ldap_server_url
Value Type	REG_SZ
Valid Range	A valid LDAP server.
Default Value	None
Guidelines	Optional. If it is defined, requires that Tanium validate every CAC/PIV authentication attempt with LDAP to determine the state of the account that is signing in. Because this does not use the Windows authentication subsystem, the service account running Tanium must have the permissions to look up accounts through a direct LDAP query. Use the following syntax, where `LDAP` must be uppercase: `LDAP://<LDAP FQDN>` If multiple domains are in use, specify a global catalog. It must use the syntax `GC://<domain>`.  Also configure LDAP integration in Tanium Console, and assign roles, computer groups, and personas to user groups and users that are imported from the LDAP server. For more information, see Tanium Console User Guide: Integrating with LDAP servers.

(Optional) LDAP query

Location	HKLM\Software\Wow6432Node\Tanium\Tanium Server
Value	CertLDAPQueryField

© 2026 Tanium Inc. All Rights Reserved

(Optional) LDAP query (continued)

Value Type	REG_SZ
Valid Range	`userPrincipalName` or `sAMAccountName`
Default Value	userPrincipalName
Guidelines	Optional. If it is defined, it specifies an LDAP user naming attribute. If it is not defined, the default attribute is used. The valid values are: • `userPrincipalName` — The sign in name for the user. • `sAMAccountName` — A sign in name that supports previous version of Windows.

(Optional) LDAP secondary lookup

Location	HKLM\Software\Wow6432Node\Tanium\Tanium Server
Value	CertLDAPCertField
Value Type	REG_SZ
Valid Range	
Default Value	Subject
Guidelines	Optional. Add this setting in conjunction with the **cac_ldap_server_url** setting. This setting specifies a secondary attribute to query within the X509 certificate. Usually, this value is expected to match **ClientCertificateAuthField** with a value of `X509v3 Subject Alternative Name`. If it is not defined, certificate authentication matches on the Subject attribute.  NOTE X509v3 is typically hidden when displayed in Windows. The string `X509v3` is case sensitive.

(Optional) LDAP regex

Location	HKLM\Software\Wow6432Node\Tanium\Tanium Server
Value	CertLDAPCertFieldRegex
Value Type	REG_SZ
Valid Range	Any valid regular expression.
Default Value	None

© 2026 Tanium Inc. All Rights Reserved

(Optional) LDAP regex (continued)

Guidelines	Optional. Add this attribute in conjunction with the **cac_ldap_server_url** setting. This setting specifies a regular expression that accounts for the UPN Suffix when a secondary LDAP lookup occurs. This is necessary because LDAP synchronization matches UPN without the UPN Suffix.
	If it is not defined, whatever is returned in the user naming attribute would be used.
	The following example is most commonly used. It returns the full UPN:
	`.*\:\s*([^@]+@.*)$`
	The following example returns just the numeric value from the UPN:
	`([^@]+)@.*$`

Troubleshoot smart card authentication

- Check the configuration for typos, such as extra spaces or letter case errors.
- Test whether the system works with just the required registry keys. Then enable and test optional settings, such as the LDAP integration settings.
- In an active-active deployment, configure the **CACTrustedAddresses** value with entries for each Tanium Server and the Module Server to avoid errors by the Tanium Downloader (TDownloader) service during package synchronization.
- Set the logging level to 41 or higher on the Tanium Server and Module Server to record the following events. For more information, see Tanium Console User Guide: Configure Server logging levels. If you Create a custom log that records only these events, use `.*Client Certificate auth.*` as the filter regex. After generating logs at level 41, search for the following log entries:
  - If **ClientCertificateMatchField** is set and does not match:
    - No regex match:

      ```
      Client Certificate auth logon denied, match failed
      ```

    - Field used for regex not found in the CA certificate:

      ```
      Client Certificate auth logon denied, match property not present
      ```

  - If **ClientCertificateMatchField** passes or is empty, the user is extracted using the **ClientCertificateAuthField** and **ClientCertificateAuthRegex**:
    - If **ClientCertificateAuthRegex** is not matched:

      ```
      Client Certificate auth logon denied, regex not matched
      ```

    - If **ClientCertificateAuthField** is not found:

      ```
      Client Certificate auth logon denied, field not found
      ```

© 2026 Tanium Inc. All Rights Reserved

        - If the the regex matches and the field is found but the name is not valid:

          ```
          Client Certificate auth logon denied, unknown user
          ```

    - Any other error or information message also starts with:

      ```
      Client Certificate auth
      ```

© 2026 Tanium Inc. All Rights Reserved

Securing keys with an HSM in a Windows deployment

HSM integration overview

A hardware security module (HSM) is a hardened, tamper-resistant device that organizations use to store and generate digital keys and to perform cryptographic operations with those keys, such as encryption and decryption for Transport Layer Security (TLS) communication. During these operations, the keys never leave the HSM and are therefore more secure than if you store them in a file system, such as the installation directories of Tanium Core Platform Servers. You can use any HSM that supports the standard PKCS #11 API (Cryptoki) to manage the Tanium root keys and message-signing keys. For more information about how the Tanium Core Platform uses these keys, see Tanium Console User Guide: Managing Tanium keys.

NOTE

You require the **Administrator** reserved role to configure and manage an HSM integration.

To troubleshoot issues related to Tanium keys, see PKI log on page 146.

Integrate with an HSM

Before you begin

Perform the following tasks before configuring the Tanium deployment to use an HSM.

1. Set up the HSM. For more information, see the HSM documentation.
2. Determine the PKCS #11 module that the HSM vendor provides to support Cryptoki. The module enables communication between the Tanium Server and HSM. For example, Thales HSM provides the library `cknfast.dll` as the PKCS #11 module for 32-bit Windows systems.
3. Work with an HSM Security Officer (SO) to initialize tokens on the HSM to contain Tanium keys. Initialization involves assigning a token name (or ID) and personal identification number (PIN) for each token. You must know the PINs and the token names or IDs to configure the Tanium Server to authenticate to the tokens. The Server authenticates when performing operations that involve the keys in those tokens.

   NOTE

   In HSM terminology, a *token* is a logical view of a cryptographic device that contains keys.

© 2026 Tanium Inc. All Rights Reserved

4. (Optional, best practice) Back up the Tanium deployment. For more information, see Back up Tanium Core Platform Servers and databases on page 124.

   If you need to back up keys after integrating with an HSM, see the HSM documentation.

5. Determine a maintenance window to perform the HSM integration. You must restart the Tanium Server during the process of configuring it to use an HSM, and the restart interrupts any operations that the Server is performing.

Integrate the Tanium deployment with an HSM

In an active-active deployment, Tanium Servers do not synchronize local settings, which include HSM settings. Therefore, perform the steps for adding settings and restarting the Tanium Server service on each Server.

1. From the Main menu, go to **Administration > Configuration > Settings > Advanced Settings**.
2. Click **Add Setting**, configure the `HSMModulePath` setting as follows, and click **Save**:
   - **Setting Type**: **Local**
   - **Name**: `HSMModulePath`
   - **Value Type**: **Text**
   - **Value**: Directory path of the HSM vendor-specific PKCS #11 module, such as `C:\Program Files\nCipher\nfast\toolkits\pkcs11\cknfast.dll`

   In the following steps, replace the `<key>` variable with the Tanium key that the HSM will manage: `Root` or `MessageSigning`.
3. For each key, click **Add Setting**, configure the `UseHSM` setting as follows, and click **Save**. `UseHSM` forces the Tanium Server to generate the key on the HSM instead of locally.
   - **Setting Type**: **Local**
   - **Name**: `Keys.<key>.UseHSM`
   - **Value Type**: **Numeric**
   - **Value**: `1`
4. For each key, click **Add Setting**, configure the `HSMPassword` setting as follows, and click **Save**. When the Tanium Server performs key operations, it uses the `HSMPassword` to authenticate to the token that contains the key.
   - **Setting Type**: **Local**
   - **Name**: `Keys.<key>.HSMPassword`
   - **Value Type**: **Protected**
   - **Value**: The PIN that is associated with the token that contains the key

© 2026 Tanium Inc. All Rights Reserved

5. For each key, click **Add Setting**, configure the `HSMTokenName` or `HSMTokenID` setting as follows, and click **Save**. The Tanium Server uses `HSMTokenName` or `HSMTokenID` to identify the token that contains the key.
    - **Setting Type**: **Local**
    - **Name**: `Keys.<key>.HSMTokenName` or `Keys.<key>.HSMTokenID`
    - **Value Type**: **Text** for `HSMTokenName` or **Numeric** for `HSMTokenID`
    - **Value**: The token name or ID
6. (Optional) Review the settings to ensure you entered them correctly. To display only the HSM settings on the **Advanced Settings** page, enter `HSM` in the **Filter items** field.
7. Sign in to the Tanium Server host, open the Windows **Services** program, right-click the **Tanium Server** service, and select **All Tasks > Restart**.

    Wait for the **Tanium Server** service to finish restarting before continuing. In an active-active deployment, restart the service on both Servers before continuing.
8. Rotate the root keys by generating new keys and revoking the old keys. For more information, see Tanium Console User Guide: Managing Tanium keys.

    When you rotate the root keys, the Tanium Server automatically rotates the subordinate keys. The new keys are stored on the HSM instead of on the Tanium Server.

    BEST PRACTICE

    After generating new keys, wait one week before revoking the old root keys to ensure that the process of generating new keys finishes for all Tanium Core Platform components. When you revoke, any components that did not finish this process expend more processing resources and network traffic to generate new keys.
9. Verify that the new keys on the HSM work. For more information, see Verify an HSM integration on page 112.

Verify an HSM integration

After you generate new keys on an HSM, verify that the Tanium Core Platform can use the keys for communication among platform components:

1. Sign in to Tanium Console as a user who is assigned a role that allows issuing questions.
2. Verify that the **Environment Status** section on the Tanium **Home** page shows Tanium Clients are connected to the Tanium Server. Connectivity indicates that the root keys work properly.
3. Issue any question to any number of Tanium Clients. If the Clients return results, the message-signing key works properly. For more information, see Tanium Console User Guide: Asking questions.

If any verification steps fail, see Troubleshoot an HSM integration on page 114.

© 2026 Tanium Inc. All Rights Reserved

Disable an HSM integration

You might want to temporarily disable an HSM integration if, for example, you plan to migrate to a new HSM appliance. After completing the migration, you would configure the HSM settings with the values of the new appliance and re-enable the integration. If you do not want to use any HSM for managing keys, you can remove the integration.

1. From the Main menu, go to **Administration > Configuration > Settings > Advanced Settings**.
2. Perform one of the following sub-tasks based on whether you want to temporarily disable the HSM integration or remove it entirely. In an active-active deployment, perform the sub-task on each Tanium Server.
   - **Disable the integration temporarily**: Perform the following sub-steps for each Tanium key that the HSM manages.
     a. In the **Name** column, click **Keys.*<key>*.UseHSM**, where ***<key>*** is **Root** or **MessageSigning**.
     b. Set the **Value** to `0` and click **Save**.
   - **Remove the integration**:
     a. Enter `HSM` in the **Filter items** field to display only the HSM settings.
     b. Select all the HSM settings and click Delete Selected Settings.
3. Rotate the root keys by generating new keys and revoking the old keys. For more information, see Tanium Console User Guide: Managing Tanium keys.
   When you rotate the root keys, the Tanium Server automatically rotates the subordinate keys. The new keys are stored on the Tanium Server (`pki.db` file) instead of on the HSM.

   BEST PRACTICE

   After generating new keys, wait one week before revoking the old root keys to ensure that the process of generating new keys finishes for all Tanium Core Platform components. When you revoke, any components that did not finish this process expend more processing resources and network traffic to generate new keys.
4. Verify that the new keys on the Tanium Server work. The verification steps are the same as when you enable an HSM integration. For more information, see Verify an HSM integration on page 112.

Update token PINS, names, or IDs

IMPORTANT

If possible, avoid changing the PIN, name, or ID for a token that stores Tanium keys. If updating these token credentials becomes necessary, update the key settings as described in the following steps. Additionally, for a new token name or ID, you must contact Tanium Support for help performing configuration steps that are not available through Tanium Console. For more information, see Contact Tanium Support on page 137.

1. From the Main menu, go to **Administration > Configuration > Settings > Advanced Settings**.
   In the remaining steps, replace the `<key>` variable with the Tanium key that the HSM manages: `Root` or `MessageSigning`.
2. To change a token PIN, click **Keys.*<key>*.HSMPassword** in the **Name** column, set the **Value** to the new PIN, and click **Save**.

© 2026 Tanium Inc. All Rights Reserved

3. To change a token name, click **Keys.*<key>*.HSMTokenName** in the **Name** column, set the **Value** to the new name, and click **Save**.
4. To change a token ID, click **Keys.*<key>*.HSMTokenID** in the **Name** column, set the **Value** to the new ID, and click **Save**.

Troubleshoot an HSM integration

If issues occur when you configure or verify an HSM integration:

1. Review the PKI logs for error messages. All Tanium Core Platform Servers and Tanium Clients generate PKI logs.
   - **Platform Servers on Windows**: For more information, see PKI log on page 146.
   - **Tanium Client**: The PKI logs are in the `<Client installation directory>/Logs` directory.
2. Verify that Tanium Clients are using the correct keys. For more information, see Tanium Client Management User Guide: Review or reset the public key to troubleshoot connection issues.
3. Resolve the issues. Contact Tanium Support on page 137 if necessary.
4. Perform the task Verify an HSM integration on page 112 to confirm the resolution works.

© 2026 Tanium Inc. All Rights Reserved

Upgrading Tanium Core Platform Servers in a Windows deployment

Upgrading to a new semiannual release or maintenance release

Tanium™ Semiannual Release 2025H2

Tanium™ Semiannual Release 2025H2 includes new versions of the following components:

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

For version and support information, see 2025H2 release notes.

For more information about Tanium releases, see Tanium Console User Guide: Tanium releases.

Maintenance releases

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

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



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

Upgrade process

UPGRADING TANIUM CORE PLATFORM AND TANIUM SOLUTIONS

You must use the versions of Tanium Core Platform and Tanium solutions that are provided in a semiannual release together, or the later versions of each component that are provided in maintenance releases that upgrade the semiannual release. When upgrading to a new semiannual release, you must upgrade these components at the same time, beginning with Tanium Core Platform. For

© 2026 Tanium Inc. All Rights Reserved

specific upgrade steps, see Upgrading Tanium Core Platform Servers in a Windows deployment on page 115.

IMPORTANT

- After you start the upgrade process for a new semiannual release, you cannot access Tanium solutions until you finish upgrading both the platform and solutions. Make sure to plan a maintenance window with enough time to complete all upgrades.
- As a best practice, upgrade to the latest maintenance release available for semiannual release 2025H2. Do not upgrade to a maintenance release that has an earlier release date than the currently installed maintenance release. For example, if you have a maintenance release from Februrary 1 currently installed, install a maintenance release of the 2025H2 semiannual release from February 1 or later.

UPGRADING THE TANIUM ENDPOINT CONFIGURATION TOOLSET AND TANIUM CLIENT

You deploy the Tanium Endpoint Configuration Toolset and, optionally, the Tanium Client to endpoints using the change management feature of Tanium Endpoint Configuration. For more information, see Tanium Endpoint Configuration User Guide: Managing endpoint tool upgrade rollouts. If you do not enable Client upgrades in the change management feature, or if you need to upgrade the Tanium Client in upgrade rings for which Client upgrades are not yet enabled, you must upgrade the Tanium Client on endpoints using Client Management or other means to maintain a supported configuration. For more information, see Tanium Client Management User Guide: Upgrading Tanium Clients. Tanium Semiannual Release 2025H2 supports all Tanium Client versions that the Tanium Core Platform supports. Each semiannual release supports the current endpoint configuration toolset and the two previous toolset releases.

BEST PRACTICE

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

TIP

In Tanium Console, the **Solutions** page (**Administration > Configuration > Solutions**) indicates at the top-right if Tanium Core Platform Servers are up-to-date or if an update is available.

Server upgrade overview

The maintenance window for upgrading Tanium Core Platform Servers is usually under an hour, but make sure to allow enough time to upgrade solutions as well.

To avoid unexpected issues, all Servers must run the same software version. As a best practice, complete the upgrade for all the Servers in the same maintenance window. If you have a high availability (HA) cluster, complete the upgrade for both Tanium Servers in the same window.

If you do not need to change the Server host names, SSL/TLS certificates, or key files, you can simply run the Tanium Core Platform installers to replace the existing installation with updated files, and upload the new license file (if applicable) to the installation directory on the Tanium Servers (see Managing the Tanium license).

© 2026 Tanium Inc. All Rights Reserved

In some cases, you might want to take the opportunity to change Server host names or install new SSL/TLS certificates and keys (for example, if the existing ones are due to expire). If so, the upgrade experience is similar to the initial installation and has similar prerequisite steps. If you change the Server host names, you must reconfigure the Tanium Client on endpoints so they can communicate with the Servers.

The upgrade procedures in this guide assume your host and network environment meets the initial installation requirements (see Tanium Core Platform requirements in a Windows environment on page 20).

The settings that you manage through Tanium Console are saved to the Tanium database. Therefore, any customizations that you saved in your existing deployment persist through the upgrade.

Before you begin

Perform the following tasks before upgrading:

- Read the release notes for all of the Tanium Core Platform software versions that were released after your current version to stay informed about expected behavior.
- Make sure the current deployment is working as expected, including all Tanium Core Platform Servers and solutions.
- If you plan to change the Tanium Server hostname, Contact Tanium Support on page 137 to provide the updated hostname to obtain a new new Tanium license file for the new hostname. You must have this updated license file during the upgrade process if it includes a hostname change.
- Download the installation package from the **Artifacts** section of your Tanium Account. For more information, see Tanium Account User Guide: View Tanium artifacts.
- A normal upgrade does not require you to restore from backups, but backups can save you work if you encounter issues and want to restore the system to a known functional state. For more information, see Back up Tanium Core Platform Servers and databases on page 124.
- Under ordinary circumstances, the installer for each Tanium Core Platform Server stops the associated Tanium service, updates the software, and restarts the service. In deployments with an exceptionally large amount of data, stopping a service might take an exceptionally long time, and the installer might abort the installation before the service properly shuts down. As a best practice to avoid this, use the Windows Services program to stop the Tanium Core Platform services in the following order before starting the upgrade:
    - Tanium Zone Server
    - Tanium Zone Server Hub
    - Tanium Module Server
    - (HA deployment only) Non-primary Tanium Server
    - Primary (HA) or standalone (non-HA) Tanium Server

Order of Tanium Core Platform Server upgrades

You must upgrade Tanium Core Platform Servers in the following order:

© 2026 Tanium Inc. All Rights Reserved

1. Tanium Servers (primary and non-primary Servers in HA deployments)
2. Module Server
3. Zone Server Hub
4. Zone Server

Upgrade the Tanium Server

When you upgrade, the Tanium™ Server installer takes the following actions:

- Stops the Tanium Server service.
- Installs Tanium Server software and Tanium Console UI components.
- Updates the Windows registry with the values you specify in the interactive installation wizard.
- Updates the Tanium databases on the remote database server and re-initializes the database tables in those databases.
- Opens required ports in the local host computer Windows Firewall.
- Starts the Tanium Server service.



The Windows Secondary Logon service (seclogon) on the host computer for the Tanium Server must have its **Startup type** set to **Automatic** or **Manual** (not **Disabled**) during an upgrade of the Tanium Server . If the Secondary Logon service is disabled, the installation cannot connect to the database server (even if it is installed locally), and the upgrade of the Tanium database fails. The Secondary Logon service is required only during installation and upgrades.



In an upgrade of a production deployment, the installer detects from the Windows Registry that the Tanium Module Server is not installed locally, so it does not attempt to upgrade it or start the Tanium Module Server service.

Upgrade a standalone (non-HA) or primary (HA) Tanium Server

1. Sign in to the host system as a local administrator or domain user with administrator permissions.
2. Copy the installer (`SetupServer.exe`) and, if needed, license files to a temporary location on the host computer.
3. If you have new SSL/TLS certificate and key files, copy them to the host computer so you can select them when you run the installer.
4. Right-click `SetupServer.exe` and select **Run as administrator**.

© 2026 Tanium Inc. All Rights Reserved

5. Complete the installation wizard. Consider the following:
    - Select **Custom Install**, not **Express Install**. When you select **Custom Install**, the installer prompts you for each setting and populates the wizard form with the values extant in the present installation. This gives you a chance to review the current installation and replace the certificate and license files, if necessary, or change other installation settings. When you select **Express Install**, the installer uses the existing values but does not give you an opportunity to review or change them.
    - On the **License Configuration** page, select the new license file if applicable.
    - If the Server has new SSL/TLS certificate and key files, use the **Certificate Path** and **Key Path** to select them; otherwise, use the values that the installer populates.

Upgrade a secondary (HA) Tanium Server

1. Sign in to the host system as a local administrator or domain user with administrator permissions.
2. Copy the installer (`SetupServer.exe`) and license files to a temporary location on the host computer.
3. If you updated the SSL/TLS certificate and key files, copy the following files from the Tanium Server installation directory on the primary host to the installation directory on the non-primary host:
    - `SOAPServer.crt`
    - `SOAPServer.key`
    - `tanium.license`

    Always follow your organization's best practices for securely copying sensitive files, such as the Tanium Server `SOAPServer.key` file. For example, use GNU Privacy Guard (GPG) to encrypt the files before copying and then decrypt when they are in place on the target Server.
4. Right-click `SetupServer.exe` and select **Run as administrator**.
5. Complete the installation wizard. Consider the following:
    - Select the **Custom** installation type, not **Express**. When you select **Custom**, the installer prompts you for each setting and populates the wizard form with the values extant in the present installation. This gives you a chance to review the current installation and replace the certificate and license files, if necessary, or change other installation settings. When you select **Express**, the installer uses the existing values but does not give you an opportunity to review or change them.
    - On the **License Configuration** page, be sure to select the new license file if appropriate.
    - If the Server has new SSL/TLS certificate and key files, use the **SSL Certificate and Key** controls to select them; otherwise, retain the values that the installer populated.
    - After upgrading the Tanium Module Server, you must manually register it with the non-primary Tanium Server (see the last step under Upgrade the Tanium Module Server on page 120).

© 2026 Tanium Inc. All Rights Reserved

Upgrade the Tanium Module Server

When you upgrade, the Tanium™ Module Server installer takes the following actions:

- Stops the Tanium Module Server service.
- Updates Tanium Module Server software.
- Updates the Windows registry with the values you specify in the interactive installation wizard.
- Initiates registration with the primary (HA) or standalone Tanium Server (if selected).
- Opens required ports in the local host computer Windows Firewall.
- Starts the Tanium Module Server service.

Before you begin

Ensure that your network security administrator has configured network firewall rules to allow communication between the Tanium Server and Module Server on TCP ports 17477 and 443. For more information, see Internet access, network connectivity, and firewalls on page 26.



When you first upgrade to the latest release, automatically register the Module Server with the primary (HA) or standalone Tanium Server instead of manually registering.



The Windows Secondary Logon service (seclogon) on the host computer for the Tanium Module Server must have its **Startup type** set to **Automatic** or **Manual** (not **Disabled**) during an upgrade of the Tanium Module Server . If the Secondary Logon service is disabled, the installation cannot connect to the database server (even if it is installed locally), and the upgrade of the Tanium database fails. The Secondary Logon service is required only during installation and upgrades.

Upgrade the Tanium Module Server

1. Sign in to the Tanium Module Server host system as an administrator user.
2. Copy the installer (`SetupModuleServer.exe`) to a temporary location on the host computer.
3. If the Tanium Module Server has new certificate and public key files, copy them to a temporary location on the Tanium Module Server host computer so you can select them when you run the installer.
4. Right-click `SetupModuleServer.exe` and select **Run as administrator**.

© 2026 Tanium Inc. All Rights Reserved

5. Complete the installation wizard. Consider these points:
    - If the Tanium Module Server has a new certificate and key, use the **Use Existing Certificate and Key** controls to select them.
    - If the Tanium Server has a new certificate, use the **Register with the Tanium Server** or **Manually specify Tanium Server certificate** controls to select it. In an HA deployment, register with the primary Tanium Server.
    - If you do not use automatic registration, or if registration fails, see Install and manually register the Module Server on page 47 for steps you must perform after completing the wizard to finish registration.
6. (HA only) Access the CLI of the Module Server host and run the following commands to register with the non-primary Tanium Server.

```
cmd-prompt>cd <Module Server>
cmd-prompt>TaniumModuleServer register <Tanium_Server_FQDN>
Enter administrator username: <username>
Enter password for user '<username>':
Successfully completed registration.
```

For more information about using the CLI, see Reference: Tanium Core Platform Command-line interface in a Windows deployment on page 176.

> **NOTE** You typically only need to perform registration one time when you first upgrade to the latest release. You only need to re-register if you change the Tanium Server or Module Server certificates.

7. Sign in to the Tanium Server host system as an administrator user, open the Windows **Registry Editor**, navigate to the `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Tanium\Tanium Server` key, and ensure that the **ModuleServer** value specifies the IP address of the Module Server.

> **NOTE** The IP address `127.0.0.1` applies only to a local Module Server that is installed on the same system as the Tanium Server.

Upgrade the Tanium Zone Server

Tanium™ Zone Server software is installed on the Zone Server Hub (a host computer in the internal network, typically the Tanium Server host computer) and on one or more dedicated Zone Server host computers in the DMZ. Upgrade both types of Servers.

When you upgrade, the Tanium Zone Server installer takes the following actions:

- Stops the Tanium Zone Server service.
- Updates Tanium Zone Server software.

© 2026 Tanium Inc. All Rights Reserved

- Updates the Windows registry with the values you specify in the interactive installation wizard.
- Opens required ports in the local host computer Windows Firewall.
- Starts the Tanium Zone Server service.

Upgrade the Zone Server Hub

1. Sign in to the Tanium Server host system as an administrator user.
2. Copy the installer (`SetupZoneServer.exe`) to a temporary location.
3. Right-click `SetupZoneServer.exe` and select **Run as administrator**.
4. Complete the installation wizard.

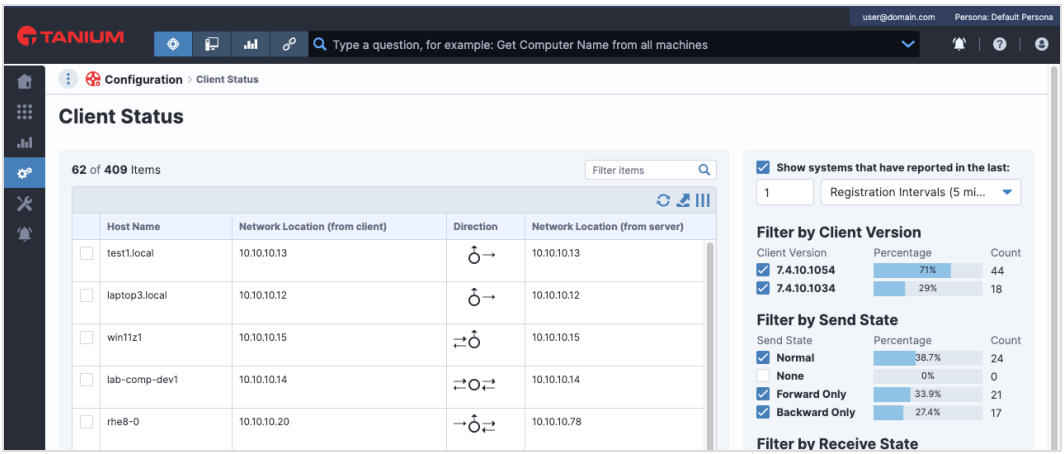
Upgrade the dedicated Zone Server

1. Sign in to the Tanium Zone Server host system as an administrator user.
2. Copy the installer (`SetupZoneServer.exe`) to a temporary location.
3. Right-click `SetupZoneServer.exe` and select **Run as administrator**.
4. Complete the installation wizard.

Upgrade solutions and verify the Servers upgrade

If errors occur when you verify the upgrade, see Troubleshoot Server installation and upgrade issues on page 128.

1. Sign in to Tanium Console as a user with the **Administrator** role.
   You are redirected to the **Solutions** page, where each installed solution upgrades to the version included in the semiannual release bundle.
2. From the Main menu, go to **Administration > Configuration > Client Status** to review recent Tanium Client registration details and verify that Clients are registering as expected.



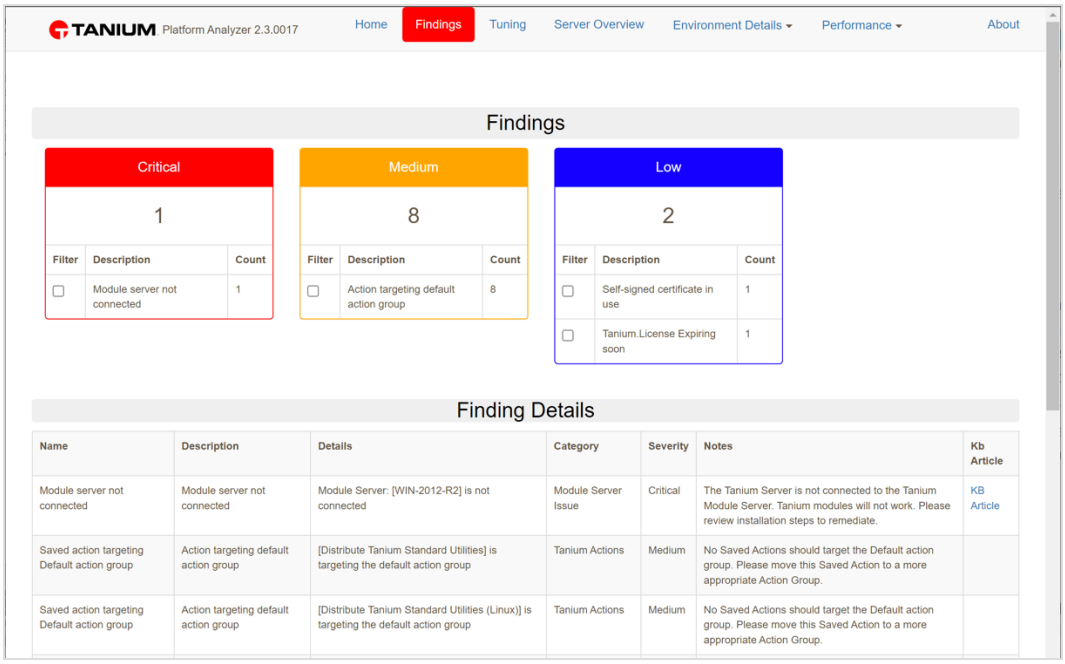
© 2026 Tanium Inc. All Rights Reserved

Troubleshooting installation and upgrade in a Windows environment

This chapter covers procedures, settings, and logs that you can use to troubleshoot issues relating to the installation or upgrade of Tanium Core Platform Servers.

Basic troubleshooting tips

- Regularly run and review Tanium™ Health Check reports, such as the Tanium Platform Analyzer (TPAN) report, regardless of whether you currently have issues to troubleshoot. If necessary, you can share these reports with Tanium Support for troubleshooting assistance. For more information, see Troubleshooting workflow on page 139.



- Ensure that all Tanium Core Platform servers are the same version. For example, if you are installing Tanium Core Platform 7.8.2.2345 on one server, you must install 7.8.2.2345 on all servers; you cannot install 7.8.2.1234 on a different Tanium Core Platform server. To update the versions, see Upgrading Tanium Core Platform Servers in a Windows deployment on page 115.
- Ensure that your environment meets the host system and network requirements. For more information, see Tanium Core Platform requirements in a Windows environment on page 20.
- Verify the deployment after you finish installing all the Servers. For more information, see Verifying the deployment to your Windows environment on page 92.

© 2026 Tanium Inc. All Rights Reserved

- Review any error messages in the:
  - Tanium Console. For more information, see Tanium Console User Guide: Work with the Tanium Console error log.
  - Installation log files. For more information, see Reviewing logs and troubleshooting Tanium Core Platform in a Windows deployment on page 138.



If the browser that you use to access Tanium Console displays an HTTP response status code in the 500 to 599 range, this indicates a server error. The responsible server might or might not be a Tanium Core Platform Server.

Back up Tanium Core Platform Servers and databases

Back up the Tanium Core Platform Servers and Tanium databases so that you can restore your deployment to a known functional state in case of issues. For example, a system failure might make the host system of the Tanium Server unrecoverable.

Best practices for backups

The following are standard guidelines for backups. Your backup strategy might differ based on the specific needs of your organization.

- Define a disaster recovery (DR) plan early during the initial deployment phase. Define specific restore time objectives (RTO) and restore point objectives (RPO), which affect how frequently you back up your deployment.
  - **RPO**: The expected point of recovery. For example, an RPO of 1 day means recovery point within 24 hours of the time of failure.
  - **RTO**: The amount of downtime that is acceptable to recover the system.

  Tanium data, such as question result strings, change frequently. Therefore, back up your deployment daily to ensure that you do not lose the latest state that critical operations require.
- Back up your deployment before any major changes, including upgrades to Tanium Core Platform Servers or migrations to new servers.
- If you rotate the Tanium root keys, back up your deployment immediately after revoking the old keys. For more information about managing the root keys, see Tanium Console User Guide: Managing Tanium keys.

  If you configure the Tanium Server to integrate with an HSM, you cannot use a backup of the `pki.db` file containing the root keys to install a cryptographically identical duplicate of the Server.
- Archive, secure, and manage copies of the SSL/TLS certificate and key files according to the security policies of your organization as you would any other system-level security and credential files. For more information, see Securing Tanium Console, API, and Module Server access in a Windows deployment on page 77.

© 2026 Tanium Inc. All Rights Reserved

Back up the Servers and database

1. Copy the installation directories for Tanium Core Platform Servers and their associated databases to a secure location. Ensure that you can access the backup location in the event that a disaster makes the Server hosts inaccessible.

   The following are the default installation directories for Tanium Core Platform Servers:

   Default installation directories for Tanium Core Platform Servers

Target Server	Installation directory
[1]Tanium Server	`\Program Files\Tanium\Tanium Server`
Tanium Module Server	`\Program Files\Tanium\Tanium Module Server` `\Program Files\Tanium\Tanium Module Postgres`
[2]Tanium Zone Server	`\Program Files (x86)\Tanium\Tanium ZoneServer`
[3]Tanium Zone Server Hub	`\Program Files (x86)\Tanium\Tanium ZoneServer`

[1] Back up this directory on each Tanium Server in an active-active deployment. You might also have to copy the Tanium Server `Downloads` directory if it was moved out of the installation directory using the instructions in the KB article Relocate Downloads Directory.

[2]Backing up the Zone Server and hub is not essential because their data comes from the Tanium Server. After restoring from backups, you would have to re-establish trust between a Tanium Server and Zone Server anyway. To recreate the Zone Server and hub, you can also reinstall them.

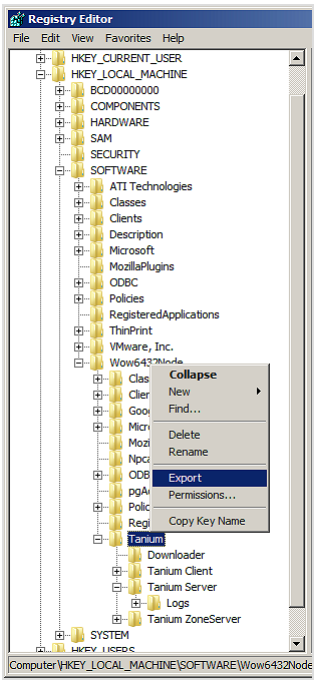
[3] The Zone Server Hub can be on the same host as the Tanium Server or on a dedicated host.

© 2026 Tanium Inc. All Rights Reserved

2. Back up the Windows registry keys for the Tanium Core Platform.

   a. Open the Windows **Registry Editor**.

   b. Navigate to the `Tanium` registry key, right click the `Tanium` registry key, and select **Export**.



   c. Set the **Save in** field to the backup location, enter a backup **File name**, and click **Save**.

3. Back up the **tanium** and **tanium_archive** databases.

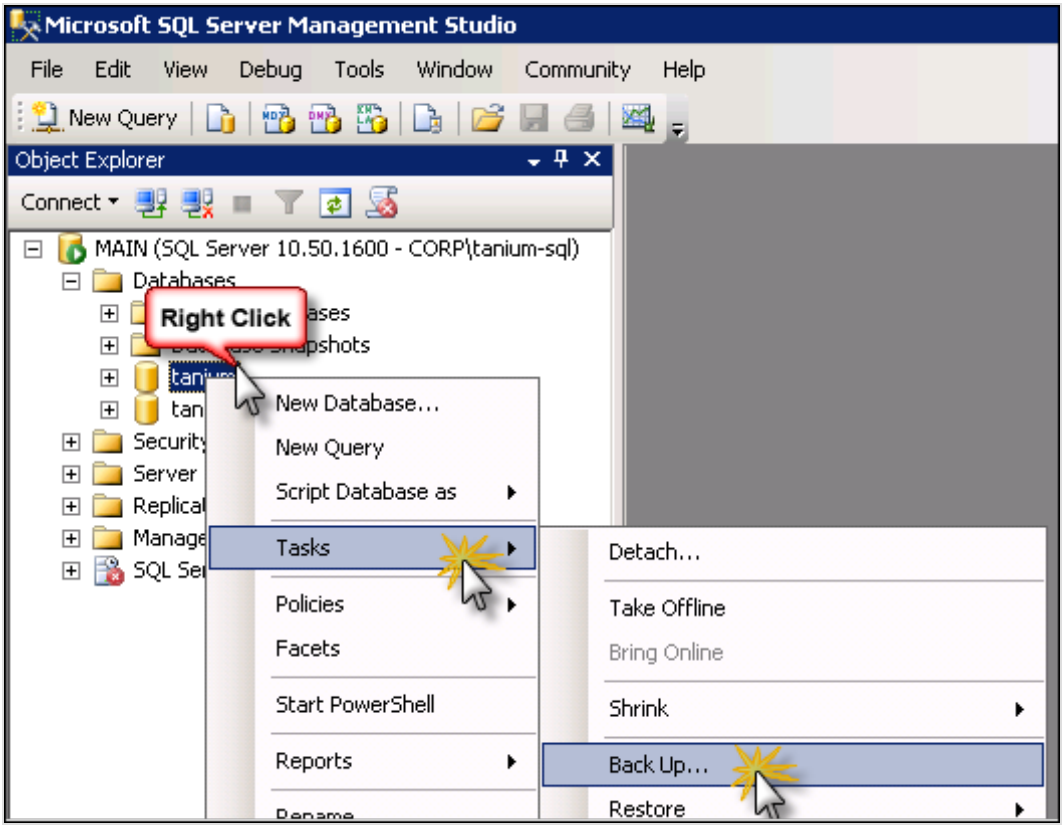
   To automate Microsoft SQL (MSSQL) database backups, see the Microsoft SQL documentation.

   To manually back up an MSSQL database through Microsoft SQL Server Management Studio:

© 2026 Tanium Inc. All Rights Reserved

a. Navigate to the database in the **Object Explorer**.

b. Right-click the database name, select **Tasks > Back Up**, and follow the prompts.



[Contact Tanium Support on page 137](#) for the steps to back up Tanium databases on a PostgreSQL server.

Common issues and solutions

The following table lists issues that you might encounter when installing or upgrading Tanium Core Platform Servers, as well as recommended troubleshooting steps:

Common deployment issues and solutions

Issue	Troubleshooting steps
Failed access messages	If you encounter failed access messages when running an installer, examine the permissions for your user account. For more information, see [Administrator account permissions on page 31](#).
Service account lockouts	If passwords change for the service accounts that Tanium Core Platform Servers use, lockout errors might occur until you update the passwords in the Windows **Services** program. For more information, see [Tanium Console User Guide: Windows service accounts](#).

© 2026 Tanium Inc. All Rights Reserved

Common deployment issues and solutions (continued)

Issue	Troubleshooting steps
Failed connections	For more information, see Troubleshoot connectivity among core platform Servers on page 132.
Tanium Console is unavailable	For more information, see Tanium Console User Guide: Troubleshoot Console access.
Disk space depletion	To monitor and free disk space in the directories where the Tanium Server stores files that it deploys to Tanium Clients, see: • Tanium Console User Guide: Manage the package file repository • Download catalog cleaner log on page 143
Installation verification fails	If you encounter verification failures while performing the steps under Verifying the deployment to your Windows environment on page 92, see Troubleshoot Server installation and upgrade issues on page 128.
Installer files or other Tanium executables do not behave as expected	If a Tanium executable file that you manually downloaded does not behave as expected, you can verify the file hash as an integrity check. For more information, see Verify file integrity on page 129.

Troubleshoot Server installation and upgrade issues

Perform the following tasks to troubleshoot installation and upgrade issues for Tanium Core Platform Servers. The tasks are listed in the order that issues might occur during the installation or upgrade and in the order that you perform subsequent diagnostics and remediation.

1. If a Server installer file that you manually downloaded does not behave as expected, verify its file hash to ensure that it has not been compromised. For more information, see Verify file integrity on page 129.
2. If you encounter failed access messages when running a Server installer, examine your Administrator account permissions on page 31. To change accounts or update their passwords, see Tanium Console User Guide: Windows service accounts. After updating account permissions or passwords, re-run the Server installer.
3. If other issues occur when you run a Server installer, review the following logs:
    - **All Servers**:
        - Reviewing logs and troubleshooting Tanium Core Platform in a Windows deployment on page 138: Record events that Server installers perform during installations and upgrades.
        - Database upgrade log on page 143: Records actions that the Tanium Server installer performs on Tanium database schemas when you upgrade the Tanium Core Platform.
        - Server logs on page 147: Record events that the other log types do not capture.
    - **Module Server**: The PostgreSQL installation log on page 146 records events that relate to the local PostgreSQL instance that the Module Server installer automatically creates.

© 2026 Tanium Inc. All Rights Reserved

4. After you install or upgrade all the Tanium Core Platform Servers, verify that the operation succeeded:

   - **Installation**: Verifying the deployment to your Windows environment on page 92
   - **Upgrade**: Upgrade solutions and verify the Servers upgrade on page 122

   If a verification step fails, perform the appropriate troubleshooting task:

   - If you cannot access the Console, see Tanium Console User Guide: Troubleshoot Console access.
   - If Tanium Servers do not connect with a remote Module Server, or Tanium Clients do not register with Tanium Servers or Zone Servers, check the status of the corresponding Windows services and start any services that are not started. For more information, see Manage Windows services for core platform Servers on page 130.
   - If Tanium Clients do not register even though Tanium Server and Zone Server services are running, see Tanium Client Management User Guide: Troubleshoot issues with connection and registration.

5. Access the CLI of a platform Server to review and, if necessary, correct Server settings. For more information, see Review and update Server settings on page 131.
6. Troubleshoot connectivity among core platform Servers on page 132.
7. If the preceding steps do not resolve the issue, generate logs at logging level 41 and then contact Tanium Support for help analyzing the logs. For more information, see Generate and review logs on page 133 and Contact Tanium Support on page 137.

Verify file integrity

If a Tanium executable file that you manually downloaded does not behave as expected, you can use the Tanium™ **KeyUtility** program to verify the file hash as an integrity check. For example, if you use a token to download the Tanium Server installer (`SetupServer.exe`), you can calculate the SHA-256 digest of the installer and compare it to the digest that the tokens site provides for that file. **KeyUtility** and its associated files reside in the top-level installation directory of the Tanium Server. You can run the program from the installation directory or copy the files to a working directory on another system and run the program from that working directory.

1. (Optional) To run **KeyUtility** from a working directory instead of the installation directory:

   a. Copy the following files from the Tanium Server installation directory or from the location where you unzipped the `KeyUtility-<release>.zip` file that Tanium Support provided:

      - `KeyUtility.exe`
      - `libeay32.dll`
      - `ssleay32.dll`

   b. Paste the files into the working directory.

2. Open the Windows **Command Prompt** (`cmd.exe`) and go to the directory where the **KeyUtility** and key files reside.

© 2026 Tanium Inc. All Rights Reserved

3. Run the following command, where `<algorithm>` is the hash algorithm. The supported algorithms are `SHA-1`, `SHA-256`, and `SHA-512`.

   ```
   KeyUtility.exe calchash <algorithm> <file>
   ```

   The following is an example of the command:

   ```
   KeyUtility.exe calchash SHA-256 SetupServer.exe
   ```

   The following digest is an example of the output:

   ```
   214d00fc4c3d5d52fe0f7a58df566385bd6ad39f5457829e73ead26778e79caf
   ```

Manage Windows services for core platform Servers

The Tanium Server, Tanium Module Server, Tanium Zone Server, and Tanium Zone Server Hub all have Windows services that must be started for the Servers to function and for Tanium Clients to register. To check the status of the services and to stop, start, or restart them:

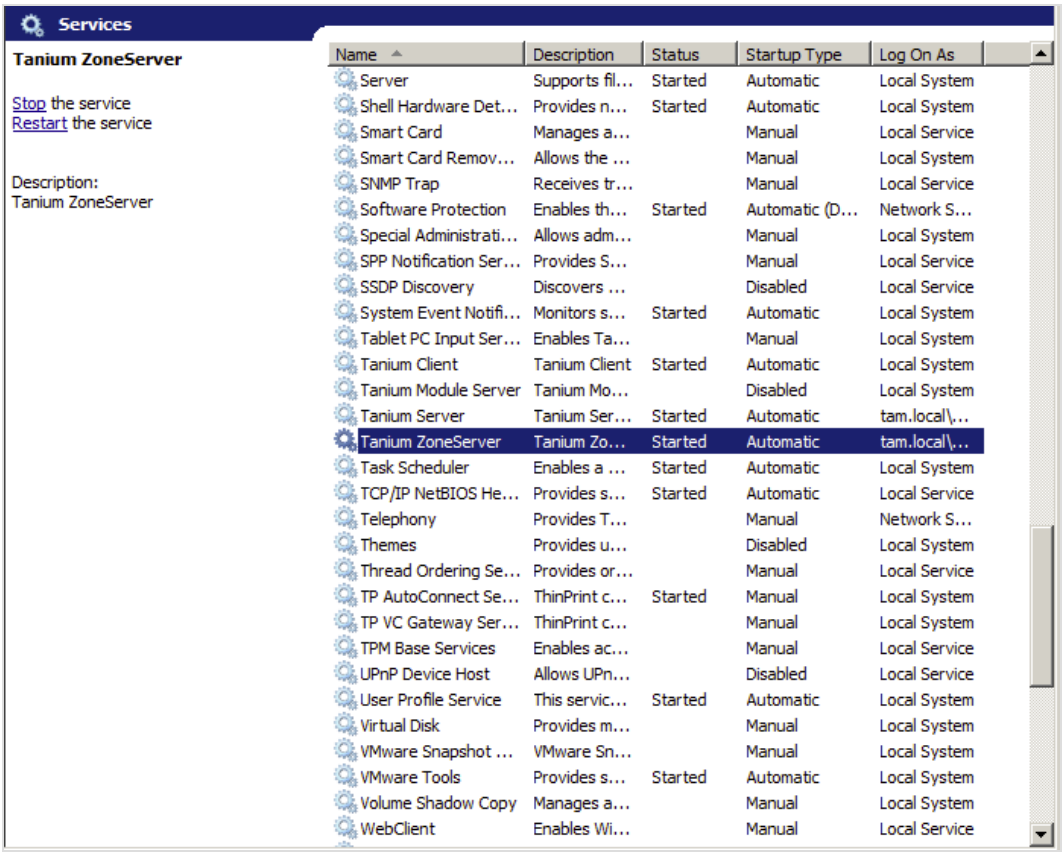
1. Sign in to the server for which you want to manage the Windows service.

   Typically, the Zone Server Hub service runs on the Tanium Server, but it can also be on a dedicated machine. Wherever the hub is installed, its service name (**Tanium ZoneServer**) is the same as for the Zone Server.

© 2026 Tanium Inc. All Rights Reserved

2. Open the Windows **Services** program, locate the service **Name**, and check its **Status**.



3. Click the **Stop**, **Start**, or **Restart** link to perform the corresponding operation.

Review and update Server settings

Many settings for Tanium Core Platform Servers are added to the Windows Registry when you install the Servers. If you encounter issues when installing a Server, use the CLI to review the Server settings for incorrect values and update them as necessary:

1. Access the Server CLI. For more information, see Reference: Tanium Core Platform Command-line interface in a Windows deployment on page 176.
2. List the Server settings:
   - **Tanium Server**: `TaniumReceiver config list`
   - **Module Server**: `TaniumModuleServer config list`
   - **Zone Server**: `TaniumZoneServer config list`
   - **Zone Server Hub**: `TaniumZoneServer config list`

© 2026 Tanium Inc. All Rights Reserved

> **NOTE** If you configured a proxy server, its settings are listed with the Tanium Server and Module Server settings.

3. Verify that the values are correct based on the setting descriptions in Reference: Deployment-related Tanium Core Platform settings in a Windows deployment on page 182.
4. Update the settings as necessary. The specific command varies by Server type and setting. For examples, see CLI examples on page 177.

Troubleshoot connectivity among core platform Servers

1. Use any appropriate utility to test connectivity from the Zone Server Hub to the Zone Server and from the Module Server to the Tanium Server. The following example shows how to use Portqry at the CLI of the Zone Server Hub host to verify whether the Zone Server is listening on a specified port.

```
c:\> portqry -n zs1.example.com -p tcp -e 17472
Querying target system called:
zs1.example.com
Attempting to resolve name to IP address...
Name resolved to 10.10.10.15
querying...
TCP port 17472 (unknown service): LISTENING
```

   If you can reach the Server and get an answer (`LISTENING`), then basic connectivity is not the issue. If you cannot reach the Server, you might need to work with your network and security administrators to resolve the issue.

2. Verify that the Server FQDNs resolve to an IP address through Domain Name System (DNS). The preceding step uses Portqry as an example to show DNS resolution. You can also use **nslookup** at the CLI:

```
c:\> nslookup ts1.example.com
Server: Unknown
Address: 10.10.10.10
Name: ts1.example.com
Address: 10.10.10.15
```

   If DNS resolution fails, work with your network administrator to resolve it. If DNS resolution is not possible, you can reconfigure the connection settings using IP addresses instead of FQDNs.

3. Verify that your deployment meets the Internet access, network connectivity, and firewalls on page 26 requirements.
4. Review the PKI TLS logs for messages that relate to Transport Layer Security (TLS) connections among Tanium Core Platform components. For more information, see PKI TLS log on page 146.

© 2026 Tanium Inc. All Rights Reserved

Generate and review logs

The default logging level is 1 on Tanium Core Platform Servers and Tanium Clients. However, because the Servers and Clients record certain events only at higher logging levels, you can raise the levels during troubleshooting to generate more detailed logs. If you cannot resolve deployment issues through other troubleshooting steps, perform the following steps to generate and review logs.



For more information about logging levels, see Logging levels on page 138.

If you want to review only specific information in predefined Tanium logs, you can configure a Tanium Core Platform Server or Tanium Client to filter the logs based on a regular expression and to copy the matching content to a custom log. Custom logs are especially useful if you set a high logging level for the predefined logs such that they roll over too quickly and record too much information for you to easily find specific issues. For more information, see Reviewing logs and troubleshooting Tanium Core Platform in a Windows deployment on page 138.

Contact Tanium Support on page 137 for help in analyzing the logs.

The following steps describe how to generate logs at logging level 41, which is the best practice when performing temporary troubleshooting for specific issue.

1. Set the logging level to 41 on:
   - **Tanium Clients**: see Tanium Client Management User Guide: Tanium Client settings.
   - **Tanium Core Platform Servers**: You can set the logging level for the Tanium Server and Module Server through Tanium Console: see Tanium Console User Guide: Configure Server logging levels. To set the logging level for other platform components (such as the Zone Server or Tanium Downloader service), see Reference: Deployment-related Tanium Core Platform settings in a Windows deployment on page 182.
2. Sign in to Tanium Console and repeat the activity that produced the issue that you are troubleshooting.
   For example, import a solution if the previous attempt to import it failed.

© 2026 Tanium Inc. All Rights Reserved

3. Review the logs that pertain to the deployment issue that you are troubleshooting:

Logs for troubleshooting Tanium Core Platform deployment issues

Issue	Logs
Trust among Tanium Servers, Zone Servers, and Zone Server Hubs	PKI log on page 146
TLS communication among Tanium Core Platform Servers and Tanium Clients	PKI TLS log on page 146
Zone Server or Tanium Client registration	• HTTP connection log on page 144 • Tanium Client logs
Package downloads	• Package download log on page 145 • TDownloader log on page 149
Solution imports	• TDownloader log on page 149 • Workbenches manager log on page 150
Other deployment issues	Server logs on page 147



After you finish troubleshooting, set the logging level to 11 or lower.

Uninstall Tanium

Uninstall the Tanium Core Platform

If you no longer want to use the Tanium Core Platform, or you want to clean up completely before reinstalling:

1. Uninstall the Tanium Core Platform Servers: Tanium Server, Tanium Module Server, Tanium Zone Server, and Tanium Zone Server Hub. The order in which you uninstall the Servers does not matter.
2. Remove the Tanium databases (**tanium** and **tanium_archive**) from the Tanium database server. For the specific steps, see your database server documentation.

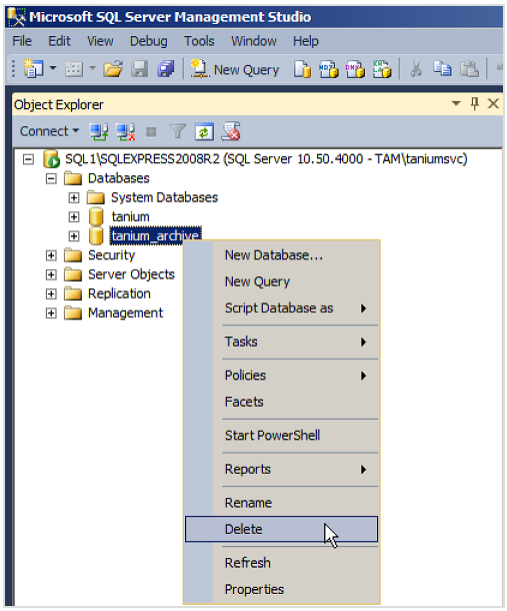
Uninstall a Tanium Core Platform Server

1. Open the Windows Control Panel and use the **Uninstall a program** feature to uninstall a Tanium Core Platform Server.
   The Windows program invokes the Tanium uninstaller, which stops and removes the Tanium service associated with the Server and deletes Windows Registry entries (except the top entry for Tanium). Completely wiping the installation requires the following manual tasks that the installer does not perform.
2. In the Windows Registry, go to `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\` and delete `Tanium`.
3. In Windows Explorer, go to the Tanium installation location and delete the `Tanium` directory.
4. Empty the Windows Recycle Bin.

© 2026 Tanium Inc. All Rights Reserved

Remove Tanium databases

Sign in to the database server as a database administrator and delete the **tanium** and **tanium.archive** databases.



Uninstall a Tanium solution or Tanium Client

For information about uninstalling a Tanium solution or Tanium Client, see the User Guide for that product:

- Tanium Client:
  - Tanium Client on Windows
  - Tanium Client on macOS
  - Tanium Client on Linux
  - Tanium Client on Solaris
  - Tanium Client on AIX
- Asset
- Automate
- Benchmark
- Certificate Manager
- Client Management
- Comply

© 2026 Tanium Inc. All Rights Reserved

- Connect
- Criticality
- Deploy
- Direct Connect
- Directory Query
- Discover
- Endpoint Configuration
- End-User Notifications
- Enforce
- Engage
- Gateway
- Guide
- Health Check
- Impact
- Integrations Gallery
- Integrity Monitor
- Interact
- Investigate
- Patch
- Performance
- Provision: Contact Tanium Support for the steps to uninstall Provision.
- Reporting
- Reputation
- Reveal
- Threat Response
- Trends
- Zero Trust

© 2026 Tanium Inc. All Rights Reserved

Contact Tanium Support

Tanium Support is your first contact for assistance with preparing for and performing an installation or upgrade, as well as verifying and troubleshooting the initial deployment. If you require further assistance from Tanium Support, please be sure to include version information for Tanium Core Platform components and specific details on dependencies, such as the host system hardware and OS details and database server version.

To contact Tanium Support for help, sign in to the Tanium Customer Community.

For more information about how to submit a support case, see Case Submission Form.

© 2026 Tanium Inc. All Rights Reserved

Reviewing logs and troubleshooting Tanium Core Platform in a Windows deployment

Tanium Core Platform Servers generate several predefined logs that you can use to diagnose issues and unexpected behavior. You can also configure custom logs that copy specific content from the predefined logs based on filters.

NOTE

For information about Tanium Client logs, see Tanium Client Management User Guide: Troubleshooting.

Contact Tanium Support if you need help to analyze logs.

Logging levels

The logging level determines how much detail Tanium Core Platform Servers and Tanium Clients record in logs, from 0 (no logging) to 99 (the highest level of detail). Select a level that provides just enough detail for you to understand what happened during an event. If you set the level too high, logs might contain so much detail that finding a particular event becomes difficult, especially if the logs roll over quickly and you must search across multiple files. Furthermore, when the number of log files reaches the maximum, the oldest files are deleted and you lose their record of events. For more information, see Log rollover on page 151.

The following logging levels are best practices for specific scenarios with all Tanium components except TDownloader:

- **1**: Normal (default) logging level. At this level, logs typically record error conditions (such as failed operations) but few informational messages (such as successful operations).
- **11**: Best practice value for long-term troubleshooting. At this level, logs generally record enough information to help you understand the history of issues that occur. You can leave the level at 11 indefinitely without the logs being cluttered with less useful information or rolling over too quickly.
- **41**: Best practice value for temporary troubleshooting. At this level, logs record details that are useful for diagnosing specific issues. When you finish troubleshooting the issue, the best practice is to revert to a lower logging level.
- **91** or higher: Most detailed logging level for advanced debugging. Because this level causes logs to roll over quickly and include details that are excessive for most scenarios, use it only for short periods and then revert to a lower logging level.

NOTE

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

In the case of TDownloader, which typically records fewer log messages than other components, it is a best practice to set the logging level at **41** for typical use.

The logging level that you set on a platform Server or Tanium Client applies to all the log types on that Server or Client, except for custom logs. You can also set the TDownloader log on page 149 to a different level than other logs on the same Tanium Server or Module Server. You have the following options for changing the logging level:

© 2026 Tanium Inc. All Rights Reserved

- **Tanium Server and Tanium Module Server**: Change the logging level through Tanium Console. For more information, see Tanium Console User Guide: Configure Server logging levels.
- **All Tanium Core Platform Servers**: Configure the **LogVerbosityLevel** settings through the Console (see Reference: Deployment-related settings) or the CLI (see Reference: Command-line interface).
- **TDownloader**: Configure the **LogVerbosityLevel** setting through the CLI (see Reference: Command-line interface).
- **Custom logs**: For more information about the logging level impact on custom logs, or to change the level, see CLI command executables and options for custom logs on page 153.
- **Tanium Client**: Configure the **LogVerbosityLevel** setting on the Tanium Client. For more information, see Tanium Client Management User Guide: LogVerbosityLevel and Tanium Client Management User Guide: Modify Client settings.

Troubleshooting workflow

Before you begin

As a best practice, configure the Tanium Platform Analyzer (TPAN) report with the following settings. The report can facilitate future troubleshooting regardless of whether your deployment currently has issues. For the specific steps, see Tanium Health Check User Guide: Configuring Health Check.

- **Number of reports to keep on disk**: Enter `12`.
- **Metrics collection schedule**: Select **Every 15 minutes**.

  NOTE

  To see the current metrics, use your browser to navigate to `https://<Tanium Server URL>/metrics` and sign in as a user with the **Administrator** reserved role.

- **Enable Collection**: Select **Enabled**.
- **Set Collection Schedule**: Run the report at least once per week.
- **Log Level**: Select **Debug**.
- **VDI in use**: Select **Yes** if any Tanium Clients run on virtual desktop infrastructure (VDI) endpoints.
- **Active-Active 50/50?**: Select **Yes** if the Tanium Servers have an active-active configuration.

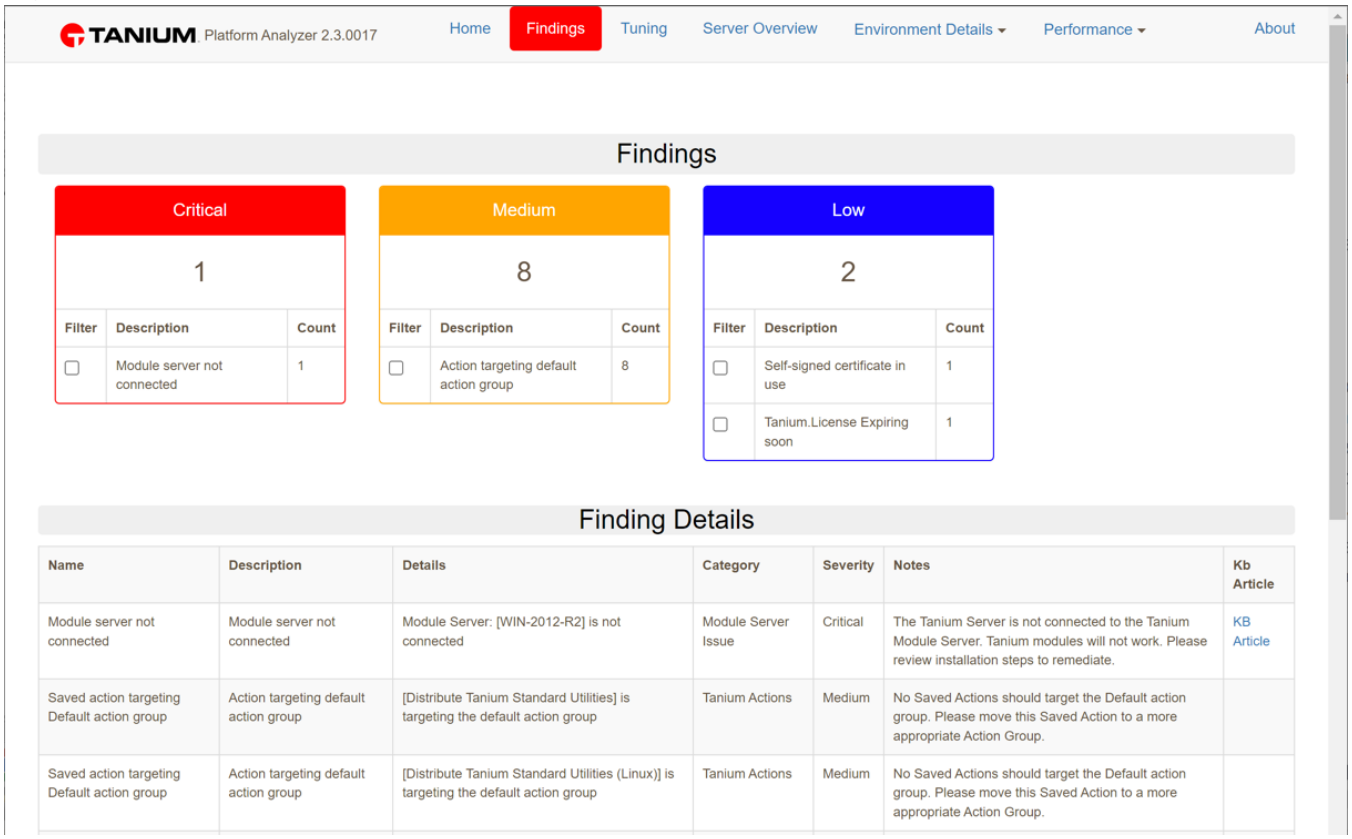
NOTE

You can use the default values for other settings.

Tanium Support might ask you to send TPAN reports if you request troubleshooting assistance. You can manually download the reports and manually or automatically share them with Tanium. For more information, see Tanium Health Check User Guide: Generating reports.

© 2026 Tanium Inc. All Rights Reserved

Figure 6: TPAN report



Troubleshoot issues during Server deployment or solution operations

The following steps represent an overview of the tasks to perform if issues occur during the installation or upgrade of Tanium Core Platform Servers, or during the regular operation of Tanium solutions:

1. Perform troubleshooting tasks that are specific to the activity during which the issue occurred, as described in the following guides. First perform the tasks that do not require reviewing logs. If those initial tasks do not resolve the issue, perform the remaining tasks in this workflow to review reports and logs.

Activity	User Guide
Installing or upgrading Tanium Core Platform Servers on Windows infrastructure	Troubleshooting installation and upgrade
Deploying and managing Tanium Clients	Tanium Client Management User Guide: Troubleshooting
Performing regular operations in Tanium Console or Interact	Tanium Console User Guide: Troubleshooting
Performing regular operations in other Tanium modules or shared services	Tanium Console User Guide: Troubleshoot solution-specific issues

2. Run and review the TPAN report on page 150 for a comprehensive view of the issues, risks, and performance of your Tanium environment.

© 2026 Tanium Inc. All Rights Reserved

3. If Tanium Console displays error messages, review them in the Console local error log on page 143.
4. Review the Tanium Core Platform Server logs on page 147. These are the most comprehensive logs in terms of recording the broadest range of events.
5. Review any other log types based on the activity during which the issue occurred. For example, if users encounter role permission errors during Console operations, review the RBAC log. For more information, see Reviewing logs and troubleshooting Tanium Core Platform in a Windows deployment on page 138.
6. (Optional) If the logs do not have enough detail for you to understand an issue, raise the logging level to 41 (see Logging levels on page 138) and repeat the operation that triggered the issue. For example, import a solution if the previous attempt to import it failed.

   After you finish troubleshooting, set the logging level to 11 or lower.
7. If analyzing logs on your own is insufficient to diagnose the issue, create a support package to send to Tanium Support and then Contact Tanium Support for additional help. The issue that you are troubleshooting determines which support package to send:
   - **Issues with specific Tanium solutions**: For more information, see Solution logs and support packages on page 148.
   - **Issues with Tanium Core Platform Servers in a Windows deployment**: Send the latest TPAN report.

Log and report types

You can view the **Local Error Log** through Tanium Console. The requirements for viewing other log types vary by infrastructure:

- **Platform Server logs**: You require access to the platform Server hosts.
- **Tanium Client logs**: You require access to the endpoint hosts.

  In addition to viewing action logs directly on individual endpoints, you can use the Console to view the action logs of up to 50 endpoints. For more information, see Tanium Console User Guide: Investigate action-related issues.

The following Tanium Core Platform Server logs are available.



For log types that are available on Tanium Clients, see Tanium Client Management User Guide: Troubleshooting.

- Action scheduler log on page 142
- Authentication log on page 143
- Console local error log on page 143
- Database upgrade log on page 143

© 2026 Tanium Inc. All Rights Reserved

- Download catalog cleaner log on page 143
- HTTP connection log on page 144
- Installation logs on page 144
- LDAP log on page 144
- Module plugin history log on page 144
- Module-provided privileges log on page 145
- Package cache cleaner log on page 145
- Package download log on page 145
- PKI log on page 146
- PKI TLS log on page 146
- PostgreSQL installation log on page 146
- RBAC log on page 147
- Server logs on page 147
- Solution logs and support packages on page 148
- TDownloader log on page 149
- TPAN report on page 150
- Workbenches manager log on page 150



Platform Servers do not generate certain log types unless errors occur or you raise the logging level beyond a specific threshold.

In the following sections, variables such as <*Tanium Server*> represent Server installation directories.

To find specific events in a log, you can open it in a text editor or use CLI commands to search for keywords. For examples of useful search strings, see Filter regex on page 154.

Action scheduler log

- **Access**: View the log `<Tanium Server>\Logs\action-scheduler<#>.txt`.
- **Content**: This log records events that relate to scheduled actions, such as why the Tanium Server did or did not deploy actions. For example, the log records Tanium Client connection failures. At logging levels between 1 (default) and 41, the Server generates the log only if errors occurred, such as actions failing to deploy. To record additional details for normal (successful) operations of scheduled actions, set the logging level to 91.

© 2026 Tanium Inc. All Rights Reserved

Authentication log

- **Access**: View the log `<Tanium Server>\Logs\auth<#>.txt`.
- **Content**: This log records user and service account access to Tanium Console or the Tanium API through all authentication methods, including SAML SSO, Lightweight Directory Access Protocol (LDAP), Active Directory (AD), Windows authentication, and API tokens.

Console local error log

- **Access**: Sign in to Tanium Console, click expand the ***<user name>*** drop-down menu in the Main menu (header), and select **Local Error Log**.
- **Content**: Tanium Console maintains an error log on the local host computer for your web browser. It includes details on the last 100 errors that were returned to the Console in response to actions that you performed through the browser. For example, the log records errors that are associated with attempting to save a configuration or import a content file. The Console maintains a separate log for each browser that you use. For more information, see Tanium Console User Guide: Work with the Console error log.

Database upgrade log

- **Access**: View the log `<Tanium Server>\Logs\database-upgrade<#>.txt`.
- **Content**: This log records actions that the Tanium Server installer performs on Tanium database schemas when you upgrade the Tanium Core Platform.

Download catalog cleaner log

- **Access**: View the log `<Tanium Server>\Logs\download-catalog-cleaner<#>.txt`.
- **Content**: This log records events that relate to the periodic removal of files from the Tanium Server downloads directory. These are files that Tanium Clients request from Internet URLs upon executing certain content, such as action packages or sensors that require the files. The downloads cleaning process removes files only if they are associated with an allowed URL that has an expiration configured (default is seven days) and the files have expired. For more information about allowed URL settings, see Tanium Console User Guide: Managing allowed URLs.

  Review the following logs for similar issues:

  - Package download log on page 145: This log records events that relate to the downloads queue for package files.
  - Package cache cleaner log on page 145: This log records events that relate to the removal of package files from the Tanium Server chunk cache (a sub-directory of the downloads directory).
  - TDownloader log on page 149: This log records download events on the Tanium Server.

© 2026 Tanium Inc. All Rights Reserved

HTTP connection log

- **Access**: View the log `<Tanium Server>\Logs\http-access<#>.txt`.
- **Content**: This log records all HTTP requests that are sent to port 443 on the Tanium Server. For example, the log records registration attempts by Tanium Clients or the Zone Server and Tanium API access attempts. The log includes timing information for the requests, such as date-time and duration.

Installation logs

- **Access**: View the log on each Server:
  - Tanium Server: `<Tanium Server>\Install.log`
  - Module Server: `<Module Server>\Install.log`
  - Zone Server: `<Zone Server>\Install.log`
- **Content**: This log records actions that the installer for a Tanium Core Platform Server performs during installations and upgrades in a Windows deployment. If you encounter issues with your installation, examine the logs to see which actions completed successfully and which failed. Each time you run the installer, it appends the actions for that execution to the end of the file instead of rolling over the file.

LDAP log

- **Access**: View the log `<Tanium Server>\Logs\ldap<#>.txt`.
- **Content**: This log records LDAP synchronization and authentication events for interactions between the Tanium Server and LDAP servers.



At any given time in an active-active deployment, only one Tanium Server performs synchronization and records synchronization events in its LDAP log.

The Authentication log on page 143 can also help you troubleshoot LDAP authentication issues.

Module plugin history log

- **Access**: View the log on each Server:
  - **Tanium Server**: `<Tanium Server>\Logs\module-history<#>.txt`
  - **Module Server**: `<Module Server>\Logs\module-history<#>.txt`
- **Content**: This log records all HTTP requests from the Tanium Server to any solution on the Module Server. For example, if a Tanium Console user tries to access the **Endpoints by Compliance Rule Failures** chart, the user browser sends the request to the Tanium Server, which forwards the request to the Module Server, which forwards the request to the Tanium™ Risk

© 2026 Tanium Inc. All Rights Reserved

service. The log also records *plugin* executions. A plugin is an extension to a Tanium Core Platform component or solution. Plugin operations are usually transparent to users. However, Tanium Support might instruct you to review plugin details when troubleshooting unexpected behavior.

Module-provided privileges log

- **Access**: View the log `<Tanium Server>\Logs\module-provided-privileges<#>.txt`.
- **Content**: This log records events that relate to dependencies among Tanium solutions with respect to implicitly provided permissions. For example, if Tanium™ Deploy references a content set in Tanium™ Trends, an error occurs if you import Deploy but not Trends. As another example, the log records an error if you delete a content set that is associated with role permissions that are assigned to users. The Tanium Server generates this log only if the logging level is at least 40.

Package cache cleaner log

- **Access**: View the log `<Tanium Server>\Logs\package-cleaner<#>.txt`.
- **Content**: The Tanium Server uses cache storage for packages and associated files that actions reference. To conserve disk space, the Server periodically removes packages and files that are no longer referenced by an action that has an issue date-time in the future. Before removing the package and files, the Server waits until they have aged past the expiration interval (default 120 days) since the last issue date-time.

Review the following logs for similar issues:

- Download catalog cleaner log on page 143: This log records events that relate to the removal of files that the Tanium Server downloads to serve Tanium Client requests.
- Package download log on page 145: This log records events that relate to the downloads queue for package files.
- TDownloader log on page 149: This log records all download events on the Tanium Server.

Package download log

- **Access**: View the log `<Tanium Server>\Logs\package-download<#>.txt`.
- **Content**: This log records events that relate to the download queue for package files that the Tanium Server downloads and deploys to Tanium Clients through actions. For example, the log might indicate why certain packages are not in the download queue. The Server generates this log only if the logging level is at least 20.

© 2026 Tanium Inc. All Rights Reserved

Review the following logs for similar issues:

- Download catalog cleaner log on page 143: This log records events that relate to the removal of files that the Tanium Server downloads to serve Tanium Client requests.
- Package cache cleaner log on page 145: This log records events that relate to the removal of package files from the Tanium Server chunk cache.
- TDownloader log on page 149: This log records all download events on the Tanium Server.

PKI log

- **Access**: View the log on each Server:
  - **Tanium Server**: `<Tanium Server>\Logs\pki<#>.txt`
  - **Module Server**: `<Module Server>\Logs\pki<#>.txt`
  - **Zone Server**: `<Zone Server>\Logs\pki<#>.txt`
  - **Zone Server Hub** (if the hub is not on the Tanium Server): `<Zone Server Hub>\Logs\pki<#>.txt`
- **Content**: This log records events that relate to changes in the set of digital keys that Tanium Core Platform components use to prove their identity to each other. For example, the log records key generation and revocation events. The log also records events that relate to trust approvals and denials among Tanium Servers, Zone Server Hubs, and Zone Servers.

PKI TLS log

- **Access**: View the log on each Server:
  - **Tanium Server**: `<Tanium Server>\Logs\pki-tls<#>.txt`
  - **Module Server**: `<Module Server>\Logs\pki-tls<#>.txt`
  - **Zone Server**: `<Zone Server>\Logs\pki-tls<#>.txt`
  - **Zone Server Hub** (if the hub is not on the Tanium Server): `<Zone Server Hub>\Logs\pki-tls<#>.txt`
- **Content**: This log records events that relate to Transport Layer Security (TLS) connections among Tanium Core Platform Servers and Tanium Clients. For example, the log records TLS handshake failures that occur due to expired certificates.

PostgreSQL installation log

- **Access**: View the log `<Tanium installation directory>\Tanium Module Postgres\Install_postgres.log`.
- **Content**: This log records events that relate to the PostgreSQL database that the Module Server installer creates locally as the storage system for Tanium solutions.

© 2026 Tanium Inc. All Rights Reserved

RBAC log

- **Access**: View the log `<Tanium Server>\Logs\rbac<#>.txt`.
- **Content**: This log records events that relate to Tanium role-based access control (RBAC). If users attempt operations that their assigned roles do not allow, the log indicates which permissions are missing. These operations include viewing, editing, reassigning, creating, or deleting configuration objects that are associated with permissions. Some examples are viewing persona configurations, editing sensors, reassigning computer groups for a user, moving filter groups to other content sets, or deleting platform settings.

Tanium Console displays an alert when you attempt an operation that fails due to missing permissions. You can then view the Console error log to find the reference number (`Ref# <hash>`) for that error. To see more details for the error, use the same reference number to find the corresponding entry in the RBAC log. The following entry is an example from the Console error log:

```
ERROR: 400 Bad Request RBAC Exception (Ref# 1f14e8215610cf72):
RBACInsufficientPrivilege
```

The corresponding entry in the RBAC log might resemble the following record:

```
2020-10-02T19:22:24.076Z[00:001652:] RBAC Exception (Ref#
1f14e8215610cf72) thrown during SOAP request processing:
RBACInsufficientPrivilege - Operation: add question -
Privileges: Any of these privileges ('administrator', 'write
sensor', 'write action', 'write action for saved question',
'approve action', 'content administrator', 'write package',
'define question')
```

For more information, see Tanium Console User Guide: Work with the Console error log.

Server logs

- **Access**:
  - **Tanium Server**: `<Tanium Server>\Logs\log<#>.txt`
  - **Module Server**: `<Module Server>\Logs\log<#>.txt`
  - **Zone Server**: `<Zone Server>\Logs\log<#>.txt`
  - **Zone Server Hub** (if the hub is not on the Tanium Server): `<Zone Server Hub>\Logs\log<#>.txt`
- **Content**: Each Tanium Core Platform Server has a main log that is the most comprehensive in terms of which events it records. The Server log includes all the events that other log types do not record. For example, the Tanium Server log records Tanium database access errors that result from incorrect credentials or permissions.

© 2026 Tanium Inc. All Rights Reserved

Solution logs and support packages

- **Log access**: View the log `<Module Server>\services\<solution>-files\logs\<solution>.log`.
- **Log content**: Each Tanium solution generates a log that records events that relate to the activities of that solution. Solutions include modules (such as Comply), shared services (such as Client Management), and platform services (such as Tanium Data Service).
- **Support packages**: Tanium solutions enable you to create packages that collect all the logs and files that are relevant for troubleshooting. Tanium Support might request that you provide these packages to help you troubleshoot. See:
  - Asset
  - Automate
  - Benchmark
  - Certificate Manager
  - Client Management
  - Comply
  - Connect
  - Console
  - Criticality
  - Deploy
  - Direct Connect
  - Directory Query
  - Discover
  - Endpoint Configuration
  - End-User Notifications
  - Enforce
  - Engage
  - Gateway
  - Guide
  - Health Check
  - Impact
  - Integrations Gallery
  - Integrity Monitor
  - Interact

© 2026 Tanium Inc. All Rights Reserved

- Investigate
- Patch
- Performance
- Provision
- Reporting
- Reputation
- Reveal
- Threat Response
- Trends
- Zero Trust

TDownloader log

- **Access**: View the log on each Server:
  - **Tanium Server**: `<Tanium Server>\TDL_Logs\log<#>.txt`
  - **Module Server**: `<Module Server>\TDL_Logs\log<#>.txt`
- **Content**: This log records a history of the actions that the TDownloader service performs when it downloads files from Tanium and other Internet locations. If your deployment includes a proxy server, the log records connection status events on the proxy. The log might help you troubleshoot when importing or updating Tanium modules, shared services, content packs, and content configurations (such as package definitions).



The TDownloader log has its own logging level setting that you can configure independently of other logs on the same Server. The default logging level is **1**. However, because TDownloader typically records fewer log messages than other components, you can set it to **41** indefinitely for improved troubleshooting without the TDownloader log becoming cluttered with less useful information or rolling over too quickly. Configure the **LogVerbosityLevel** setting for TDownloader through the CLI (see Reference: Command-line interface).

If the TDownloader log indicates certificate errors, you might resolve the errors by updating the certificates that the service uses for downloads authentication. For more information, see Tanium Console User Guide: Managing remote authentication.

Review the following logs for similar issues:

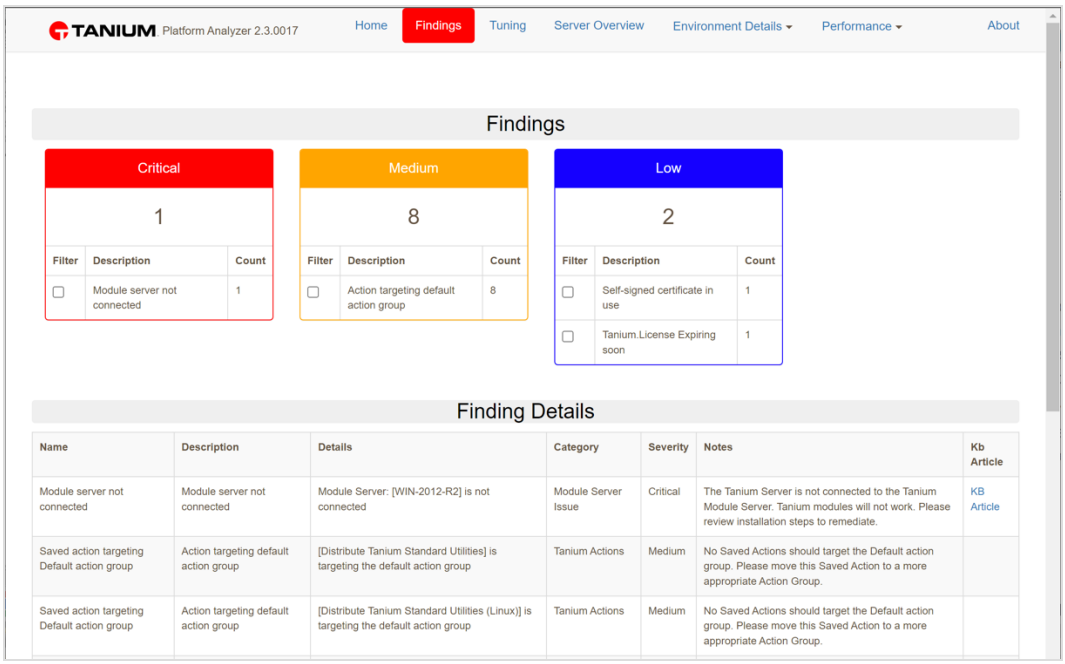
© 2026 Tanium Inc. All Rights Reserved

TIP

- Download catalog cleaner log on page 143: This log records events that relate to the removal of files that the Tanium Server downloads to serve Tanium Client requests.
- Package cache cleaner log on page 145: This log records events that relate to the removal of package files from the Tanium Server chunk cache.
- Package download log on page 145: This log records events that relate to the downloads queue for package files.

TPAN report

- **Access**: Generate TPAN reports through Tanium Health Check. For more information, see Tanium Health Check User Guide: Generating reports.
- **Content**: Provides a comprehensive view of the issues, risks, and performance of your Tanium environment. You can download reports locally to share with Tanium Support. Regularly collecting and sharing these reports can help Tanium provide you with the best support.



Workbenches manager log

- **Access**: View the log `<Tanium Server>\plugins\console\WorkbenchesManager\workbenches_manager.log`
- **Content**: This log records events that relate to the installation and uninstallation of workbenches for Tanium solutions (modules and shared services). A *workbench* is the user interface that you use to perform solution operations.

© 2026 Tanium Inc. All Rights Reserved

Log rollover

To clear space for new logs, Tanium Core Platform Servers roll over and compress existing logs when they exceed the maximum log size (10 MB) and maximum number of logs. The maximum number of log files varies by log type and format. By default, custom log types have a maximum of 10 plain text logs and 10 ZIP logs.

Number of log files

Log File Name	Plain Text	ZIP
`action-scheduler<#>.txt`	10	10
`auth<#>.txt`	10	10
`database-upgrade<#>.txt`	10	10
`download-catalog-cleaner<#>.txt`	10	10
`http-access<#>.txt`	2	3
`Install_postgres.log`	1	0
`ldap<#>.txt`	10	10
`log<#>.txt` (main Server log for each Tanium Core Platform Server)	10	10
`log<#>.txt` (TDownloader log)	10	0
`module-history<#>.txt`	2	3
`module-provided-privileges<#>.txt`	10	10
`package-cleaner<#>.txt`	10	10
`package-download<#>.txt`	10	10
`pki<#>.txt`	10	10
`pki-tls<#>.txt`	10	10
`rbac<#>.txt`	10	10
`tanium-data.log<#>.txt`	10	10
`workbenches_manager.log`	1	0

The following sections describe the rollover process. The variable *<log_type#>*`.txt` represents a log file name (such as `log0.txt`):

© 2026 Tanium Inc. All Rights Reserved

Rollover for plain text logs

When the first log file `<log_type>0.txt` reaches 10 MB in size, it is renamed `<log_type>1.txt` and a new `<log_type>0.txt` is created. When `<log_type>0.txt` again reaches 10 MB, `<log_type>1.txt` is renamed `<log_type>2.txt`, `<log_type>0.txt` is again renamed `<log_type>1.txt`, and `<log_type>0.txt` is again recreated. The process of rolling logs whenever `<log_type>0.txt` reaches 10 MB continues until the maximum number of plain-text logs exist. For example, each Tanium Core Platform Server log has a maximum of 10 plain-text logs: `log0.txt` to `log9.txt`.

Rollover for ZIP logs

After recording the maximum number of plain-text logs, the oldest log is compressed. For example, `log9.txt` is saved as `log10.zip`. When `<log_type>0.txt` again reaches 10 MB, the file name of the first ZIP log is incremented (for example, `log10.zip` becomes `log11.zip` and the oldest plain-text log is again compressed and replaces the first ZIP log. The ZIP file rollover process continues until the maximum number of ZIP files exist. For example, each Tanium Core Platform Server log has a maximum of 10 ZIP files: `log10.zip` to `log19.zip`. When `<log_type>0.txt` reaches 10 MB again after that, the first ZIP log is created again (such as `log10.zip`) but the oldest ZIP log (such as `log19.zip`) is not renamed and is effectively dropped because the second oldest ZIP file replaces it (for example, `log18.zip` becomes the new `log19.zip`).

Create a custom log for Tanium Core Platform Servers

If you want to troubleshoot only specific information in predefined Tanium logs, you can configure a Tanium Core Platform Server to filter the logs based on a regular expression and to copy the matching content to a custom log. Custom logs are especially useful if you set a high logging level for the predefined logs such that they roll over too quickly and record too much information for you to easily find specific issues. You can create as many custom logs as necessary and base each one on a different filter. After you configure a new log type, the Tanium Core Platform Server creates a custom log file upon recording an event in a predefined log that matches the regular expression. Thereafter, whenever the predefined logs record additional events that match the filter, the server copies those records to the custom log.



Log filtering can consume significant resources on a server, especially if you set a high logging level. Therefore, the best practice is to remove custom logs after you finish a troubleshooting session. For more information, see the logging level setting in the CLI command executables and options for custom logs on page 153 table.

You can also configure custom logs on a Tanium Client. For more information, see Tanium Client Management User Guide: Create a custom log for a Tanium Client.

Perform the following procedure with the options listed in the CLI command executables and options for custom logs table, using the CLI executable for the applicable Server.

1. Sign in to the host system of the platform Server or Tanium Client.
2. Open the **Command Prompt** and navigate (**cd**) to the server installation directory.
3. Configure a regular expression for the custom log.
   `<executable> config set Logs.<log prefix>.FilterRegex "<filter regex>"`

© 2026 Tanium Inc. All Rights Reserved

4. (Optional) Set the logging level of the custom log. If you skip this step, the default level is 1.
   `<executable> config set Logs.<log prefix>.LogVerbosityLevel <logging level>`

CLI command executables and options for custom logs

Executable/Option	Description
Executable	The Tanium Client and Tanium Core Platform Servers use the following executables for running CLI commands. The executables reside in the server or client installation directory. • **Tanium Server**: `TaniumReceiver` • **Module Server**: `TaniumModuleServer` • **Zone Server or Zone Serve Hub**: `TaniumZoneServer`
Log prefix	The log file prefix. The server automatically appends a number to the prefix and adds the suffix (.txt) upon generating the log. For example, if you enter `CertificateAuthentication` as the prefix for a custom server log, the first file that the Client generates for that log type is `CertificateAuthentication0.txt`.

© 2026 Tanium Inc. All Rights Reserved

CLI command executables and options for custom logs (continued)

Executable/Option	Description
Filter regex	The regular expression to use for filtering the predefined logs. The Server or Client copies log entries that match the filter to the custom log. NOTE: The filter applies only to log messages, not to thread names, thread IDs, or timestamps. The following are examples of useful filter expressions for the Tanium Server `Install.txt` log: • `.*Begin MiniDumper.*` records messages about application crashes. • `.*Failing to sync sensors.*` identifies sensor synchronization failures. • `.*msg=NoMaxAgeFound.*` records instances where the Tanium Server issues a question that uses deleted sensors. • `.*Client Certificate auth.*` records authentication messages relating to Tanium Client certificates. This is useful for troubleshooting smart card (common access card) authentication issues. For more information, see Troubleshoot smart card authentication. The following are examples of useful filter expressions for Tanium Server or Zone Server `Install.txt` logs: • `.*Begin registration.*` identifies Tanium Clients that are trying to register. • `.*Registration complete.*` identifies Clients that successfully registered.

© 2026 Tanium Inc. All Rights Reserved

CLI command executables and options for custom logs (continued)

Executable/Option	Description
Logging level	The logging level of the custom log. For more information, see Logging levels on page 138. IMPORTANT Higher logging levels consume more resources on the server. If different custom log types have different levels, the server generates all log types at the highest level that is set for any custom log type. This ensures that filter matching applies to all log messages at the highest configured level. However, in this case, each log file still contains only the level of detail that corresponds to the level you set for its log type. For example, you might set the logging level to 1 for predefined logs on the Tanium Server and set the level to 91 for a custom log. In this case, the server generates log messages at level 91 for all log types and the custom log contains messages at level 91, but the predefined logs contain messages only at level 1.

© 2026 Tanium Inc. All Rights Reserved

Reference: Host system resource guidelines

You can use the following guidelines to estimate host system requirements for Tanium Core Platform Servers. Exact requirements vary based on dynamic usage factors, such as the Tanium solutions that you use and the number of managed endpoints. Because usage differs among customers, the requirements listed in the following tables are based on representative data from numerous deployments ranging in size from under 1,000 to over 500,000 managed endpoints.

Tanium Core Platform Server host systems

Operating system support

The Tanium Server, Module Server, and Zone Server support the Standard, Enterprise, and Datacenter editions of the following Windows Server platforms. The Servers do not support the Server Core or Nano Server options.

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

Resource requirements

Use the following table to determine the device type (physical or virtual) and resources that the Tanium Core Platform Server hosts require. The columns indicate the total number of endpoints that are deployed.

In a Tanium Server high availability (HA) deployment, both Servers must meet or exceed the requirements for the total number of endpoints that your deployment targets. That means each Server must be able to independently handle load from the full deployment in the event of failure.

In a Zone Server HA deployment, provision each Zone Server to independently handle load for the cluster in case one HA peer fails.

Certain Tanium modules and shared services have additional server resource requirements. For more information, see Solution-specific requirements for Tanium Core Platform Servers on page 21.



The following table lists the minimum requirements. Tanium Support might recommend more resources based on factors that are specific to your deployment. Contact Tanium Support on page 137 for details.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform Server resource requirements

Server[1]	Specification	Up to 10,000	Up to 35,000	Up to 75,000	Up to 150,000	Up to 500,000[2]
Tanium Server	Server device type	Physical or virtual[3]	Physical or virtual[3]	Physical[4]	Physical[4]	Physical[4]
	CPU cores[5]	8	16	24	40	80
	Memory	32 GB	48 GB	96 GB	256 GB	512 GB
	Disk Space[6]	250 GB	400 GB	750 GB	1.5 TB	3 TB
Module Server	Server device type	Physical or virtual[3]	Physical or virtual[3]	Physical[4]	Physical[4]	Physical[4]
	CPU cores[5]	8	16	24	40	80
	Memory	32 GB	48 GB	96 GB	256 GB	512 GB
	Disk Space	150 GB	150 GB	150 GB	200 GB	300 GB
Zone Server	Server device type	Physical or virtual[3]	Physical or virtual[3]	Physical[4]	Physical[4]	Physical[4]
	CPU cores[5]	8	16	24	40	80
	Memory	16 GB	24 GB	48 GB	128 GB	256 GB
	Disk Space[6]	250 GB	400 GB	750 GB	1.5 TB	3 TB

[1] To ensure that the response times of Tanium Core Platform Servers do not adversely affect the user experience, the Servers must be able to sustain I/O loads of at least 30 MBps at 2,500 IOPS and maintain disk utilization below 15 percent under such workloads. Sustaining 2,500 IOPS ensures that disk latency stays below 15 milliseconds (ms) on the drive where the Servers and modules are stored.

[2] The Tanium Core Platform supports over one million endpoints. Contact Tanium Support on page 137 for the resource specifications of deployments with over 500,000 endpoints.

[3] On virtual systems, allocate reserved resources whenever possible regardless of the number of endpoints.

[4] Tanium strongly recommends that the host system have 10Gb network cards with chipsets from Intel for deployments with over 70,000 endpoints.

[5] Calculate CPU cores based on only the physical cores from allocated CPUs.

[6] The disk space listed for the Tanium Server and Zone Server is the minimum space required for Microsoft Windows and the Tanium Core Platform Server software. If you use Tanium™ Patch, the Server needs an additional 500 GB of disk space to store and manage patches. If you use Tanium™ Deploy, the Server needs additional disk space greater than or equal to twice the Deploy software library storage.

PostgreSQL server host system

Contact Tanium Support on page 137 for guidance on host computer specifications and PostgreSQL server version specifications if you install the Tanium database on a PostgreSQL server.

© 2026 Tanium Inc. All Rights Reserved

SQL server host system

Operating system support

If you use an SQL server for the Tanium database, you can install the SQL server on Standard, Enterprise, and Datacenter editions of the following Windows Server platforms. The Server Core and Nano Server options are not supported.

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

The Tanium database server supports Microsoft SQL Server 2019 or later.

Use the following table to determine SQL server host and version specifications. The columns indicate the total number of endpoints that are deployed.

Database server operating system support

Edition	Up to 10,000	Up to 35,000	Up to 75,000	Up to 150,000	Up to 500,000[1]
Standard	✓	✓			
Business Intelligence	✓	✓			
Enterprise	✓	✓	✓	✓	✓

[1] The Tanium Core Platform supports over one million endpoints. Contact Tanium Support on page 137 for the resource specifications of deployments with over 500,000 endpoints.

Resource requirements

Use the following table to determine the device type (physical or virtual) and resources that the SQL server host requires. The columns indicate the total number of endpoints that are deployed.



The following table lists the minimum requirements. Tanium Support might recommend more resources based on factors that are specific to your deployment. Contact Tanium Support on page 137 for details.

SQL server resource requirements

Specification	Up to 10,000	Up to 35,000	Up to 75,000	Up to 150,000	Up to 500,000[1]
Server device type	Physical or virtual[2]	Physical or virtual[2]	Physical[3]	Physical[3]	Physical[3]
CPU cores[4]	4	8	10	16	32
Memory	8 GB	16 GB	24 GB	32 GB	48 GB
Disk space[5]	150 GB	200 GB	300 GB	500 GB	750 GB

© 2026 Tanium Inc. All Rights Reserved

SQL server resource requirements (continued)

Specification	Up to 10,000	Up to 35,000	Up to 75,000	Up to 150,000	Up to 500,000[1]
Database size	20 GB	75 GB	150 GB	300 GB	500 GB
Disk array IOPS[6]	2,000	2,000	2,000	2,000	2,000

[1] The Tanium Core Platform supports over one million endpoints. Contact Tanium Support on page 137 for the resource specifications of deployments with over 500,000 endpoints.

[2] On virtual systems, allocate reserved resources whenever possible regardless of the number of endpoints.

[3] Tanium strongly recommends that the host system have 10Gb network cards with chipsets from Intel for deployments with over 70,000 endpoints.

[4] Calculate CPU cores based on only the physical cores from allocated CPUs.

[5] Total space for Microsoft OS and SQL Server. Microsoft recommends that the disk space available for memory dumps be at least three times the amount of installed RAM. The required disk space for the OS and SQL Server accounts for the size of the OS, the size of the swap file, and the space required for memory dumps.

[6] To ensure that Server response times do not adversely affect the user experience, disk latency must be lower than 10 ms.

Most organizations achieve optimal performance using a single, internal RAID array when Microsoft SQL Server transaction logging is set to *Simple*. If you plan to enable *Full* transaction logging, you might have to provision an external RAID array to manage the transaction logs.

To determine the specific disk drive performance characteristics and RAID configuration necessary to support deployments of different sizes, see the SQL server resource requirements on page 158 table for the minimum input and output operations per second (IOPS) that the database server requires. Using IOPS as the performance measurement enables internal storage administrators or storage vendors the flexibility to recommend a final disk configuration to provide optimal performance at the least cost.

The results reported from each managed endpoint use an average of about 20 MB of data. However, storage requirements are directly related to platform usage patterns. Unless actual measurements confirm that the underlying disk infrastructure provides the minimum acceptable performance, the best practice is to not use a storage attached network (SAN) for the Tanium application server databases.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform Server 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 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 Tanium Core Platform Servers 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.



- Tanium Core Platform Servers require host system security exclusions only in a Windows deployment.
- In certain implementations, creating the security exclusions and optimizations described in the following sections might increase the attack vulnerability of a system and might expose devices to various security threats. Using advanced AV software that permits detailed exclusions potentially reduces risk while limiting Tanium performance impacts. Tanium recommends rigorously testing any exclusions or optimizations in a lab environment to thoroughly understand any impact on security and performance before implementation. Tanium also strongly recommends that you involve your AV vendor and security teams in reviewing these guidelines before applying them.
- If the required exclusions are not configured, or if Tanium suspects interference from AV or security software, Tanium might require you to remove or disable the AV or security software temporarily for the purposes of troubleshooting and restore it once troubleshooting is complete.



For the additional security exclusions that apply to the Tanium Client, see Tanium Client Management Guide: Reference: Endpoint security exclusions.

Tanium Core Platform folders

If you plan to implement exclusions on a folder-by-folder basis, the following table lists Tanium Core Platform 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.

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 Core Platform Server folders in a Windows deployment

Target Device	Installation folder
Tanium Server[1]	`C:\Program Files\Tanium\Tanium Server`

© 2026 Tanium Inc. All Rights Reserved

Security exclusions for Tanium Core Platform Server folders in a Windows deployment (continued)

Target Device	Installation folder
Module Server	`C:\Program Files\Tanium\Tanium Module Server`
	`C:\Program Files\Tanium\Tanium Module Postgres`
Zone Server, Zone Server Hub	`C:\Program Files (x86)\Tanium\Tanium ZoneServer`

[1] You might also choose to exclude the `<Tanium Server installation folder>/Downloads` subfolder if it was moved out of the installation folder. For more information, see Relocate the package file repository on page 41.

Tanium Core Platform system processes

The following table lists Tanium Core Platform system processes that Tanium requires allowing (not blocking, quarantining, or otherwise processing). The variables such as *<Module Server>* indicate the installation folder of the platform Servers.

Security exclusions for Tanium Core Platform Server processes in a Windows deployment

Target Device	Process
Tanium Server	`<Tanium Server>\TaniumReceiver.exe`
Module Server	`<Module Server>\services\comply-service\_new_\src\utils\7z\7za.exe`
	`<Module Server>\plugins\console\lib\7za.exe`
	`<Module Server>\TaniumModuleServer.exe`
	`<Module Server>\temp\content-management\ContentManagement.exe`
	`<Module Server>\services\tanium-data-service\TaniumDataService.exe`
Zone Server, Zone Server Hub	`<Zone Server>\TaniumZoneServer.exe`
	`<Zone Server Hub>\TaniumZoneServer.exe`

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 Core Platform Servers and Tanium solutions (modules and shared services).

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.
```

© 2026 Tanium Inc. All Rights Reserved

Module Server solution folders

Tanium solutions are installed in subfolders of the Tanium Module Server installation folder. This facilitates any exclusion rules that you create: simply exclude the Module Server installation folder and its subfolders. This applies only to a Module Server installed on Windows infrastructure.

Solution-specific exclusions

The following sections list additional processes, folders, and files on Tanium Core Platform Servers in Windows infrastructure that Tanium requires a security administrator to configure as exclusions in security software to enable the latest versions of Tanium modules and shared services to work. To view version-specific exclusions for any Tanium solution, see the PDF Archive.



- If the required exclusions are not configured, or if Tanium suspects interference from AV or security software, Tanium might require you to remove or disable the AV or security software temporarily for the purposes of troubleshooting and restore it once troubleshooting is complete.
- The following sections use variables (such as *<Module Server>*) to indicate the installation folder of a Tanium Core Platform Server.

- Asset on page 164
- Automate on page 164
- Benchmark on page 164
- Blob Service on page 165
- Certificate Manager on page 165
- Client Management on page 165
- Cloud Workloads on page 166
- Comply on page 166
- Connect on page 166
- Console: The host and network security requirements of the Tanium Core Platform apply to Tanium Console:
  - Tanium Core Platform folders on page 160
  - Tanium Core Platform system processes on page 161
- Criticality on page 167
- Deploy on page 167
- Direct Connect on page 167
- Directory Query on page 167
- Discover on page 168

© 2026 Tanium Inc. All Rights Reserved

- Endpoint Configuration on page 168
- End-User Notifications on page 168
- Enforce on page 169
- Engage on page 169
- Gateway on page 169
- Guide on page 169
- Health Check on page 170
- Impact on page 170
- Integrations Gallery on page 170
- Integrity Monitor on page 170
- Interact: The host and network security requirements of the Tanium Core Platform apply to Interact:
    - Tanium Core Platform folders on page 160
    - Tanium Core Platform system processes on page 161
- Investigate on page 171
- Patch on page 171
- Performance on page 171
- Provision on page 172
- RDB Service on page 172
- Reporting on page 172
- Reputation on page 172
- Reveal on page 173
- Screen Sharing on page 173
- Secrets Service on page 173
- System User Service on page 173
- Threat Response on page 174
- Trends on page 174
- Zero Trust on page 175

© 2026 Tanium Inc. All Rights Reserved

Asset

Asset security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`<Module Server>\services\asset-service\node.exe`
	Required only during upgrade from Asset 1.18 and earlier	Process	`<Module Server>\services\asset-service\node_modules\@tanium\postgresql\lib\win32\bin\postgres.exe`
	Required only during upgrade from Asset 1.18 and earlier	Process	`<Module Server>\services\asset-service\node_modules\@tanium\postgresql\lib\win32\bin\pg_ctl.exe`
		Process	`<Module Server>\services\endpoint-configuration-service\TaniumEndpointConfigService.exe`

Automate

Automate security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`<Module Server>\services\automate-service\TaniumAutomateService.exe`
		Process	`<Module Server>\services\automation-service\TaniumAutomationService.exe`

Benchmark

Benchmark security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Process
Tanium Module Server		Process	`<Module Server>\services\benchmark-service\TaniumBenchmarkService.exe`

© 2026 Tanium Inc. All Rights Reserved

Blob Service

Blob Service security exclusions for Tanium Core Platform Servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	*<Module Server>*\services\blob-service\TaniumBlobService.exe

Certificate Manager

No additional security exclusions are required.

Client Management

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

© 2026 Tanium Inc. All Rights Reserved

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

Target Device	Notes	Exclusion Type	Exclusion
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

Cloud Workloads

No additional security exclusions are required.

Comply

Comply security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	*<Module Server>*\services\comply-service\node.exe
		Process	*<Module Server>*\services\comply-service\node_modules\ovalindex\build\bin\ovalindex.exe
		Process	*<Module Server>*\services\endpoint-configuration-service\TaniumEndpointConfigService.exe
		Process	*<Module Server>*services\comply-service__new__\src\lib\bzip\platform-*\win-x64\TaniumExtractor.exe

Connect

Connect security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	*<Module Server>*\services\connect-service\node.exe
		Process	*<Module Server>*\services\email-service\TaniumEmailService.exe
		File	*<Module Server>*\extensions\TaniumSoftwareManager.dll
		File	*<Module Server>*\extensions\TaniumSoftwareManager.dll.sig

© 2026 Tanium Inc. All Rights Reserved

Criticality

No additional security exclusions are required.

Deploy

Deploy security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`<Module Server>\services\deploy-service\node.exe`
	Required when Endpoint Configuration is installed	Process	`<Module Server>\services\endpoint-configuration-service\TaniumEndpointConfigService.exe`

Direct Connect

Direct Connect security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`<Module Server>\services\direct-connect-service\TaniumDirectConnectService.exe`
		Process	`<Module Server>\services\endpoint-configuration-service\TaniumEndpointConfigService.exe`
Zone Server		Process	`<Tanium Installation Directory>\Tanium Direct Connect Zone Proxy\node.exe`
		Process	`<Tanium Installation Directory>\Tanium Direct Connect Zone Proxy\twsm.exe`

Directory Query

Directory Query security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`<Module Server>\services\directory-query-service\TaniumDirectoryQueryService.exe`

© 2026 Tanium Inc. All Rights Reserved

Discover

Discover security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`<Module Server>\services\discover-service\node.exe`
		Process	`<Module Server>\plugins\content\discover-proxy\proxyplugin.exe`
		Process	`<Module Server>\services\twsm-v1\twsm.exe`
		Process	`<Module Server>\services\endpoint-configuration-service\TaniumEndpointConfigService.exe`

Endpoint Configuration

Endpoint Configuration security exclusions for Tanium Core Platform Servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`<Module Server>\services\endpoint-configuration-service\TaniumEndpointConfigService.exe`

End-User Notifications

End-User Notifications security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server	Required when Endpoint Configuration is installed	Process	`<Module Server>\temp\endpoint-configuration-service\TaniumEndpointConfigService.exe`
		Process	`<Module Server>\services\end-user-notifications-service\node.exe`
		Process	`<Module Server>\services\twsm-v1\twsm.exe`

© 2026 Tanium Inc. All Rights Reserved

Enforce

Enforce security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`<Module Server>\services\enforce-service\node.exe`
Zone Server		Process	`<Tanium Installation Directory>\Tanium Direct Connect Zone Proxy\node.exe`
		Process	`<Tanium Installation Directory>\Tanium Direct Connect Zone Proxy\twsm.exe`

Engage

Engage security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`<Module Server>\services\engage-service\TaniumEngageService.exe`

Gateway

Gateway security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`<Module Server>\services\graphql-platform-service\TaniumGraphqlPlatformService.exe`
		Process	`<Module Server>\services\twsm-v1\twsm.exe`

Guide

Guide security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`<Module Server>\services\automation-service\TaniumAutomationService.exe`
Module Server		Process	`<Module Server>\services\feed-service\TaniumFeedService.exe`

© 2026 Tanium Inc. All Rights Reserved

Health Check

Health Check security exclusions for Tanium Core Platform Servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	<*Module Server*>\services\health-service\node.exe
		Process	<*Module Server*>\services\health-service\twsm.exe

Impact

Impact security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	<*Module Server*>\services\impact-service\TaniumImpactService.exe
		Process	<*Module Server*>\services\endpoint-configuration-service\TaniumEndpointConfigService.exe

Integrations Gallery

No additional security exclusions are required.

Integrity Monitor

Integrity Monitor security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Process
Tanium Module Server		Process	<*Module Server*>\services\integrity-monitor-service\node.exe
		Process	<*Module Server*>\services\endpoint-configuration-service\TaniumEndpointConfigService.exe

© 2026 Tanium Inc. All Rights Reserved

Investigate

Investigate security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Tanium Module Server		Process	`<Module Server>\services\endpoint-configuration-service\TaniumEndpointConfigService.exe`
		Process	`<Module Server>\services\investigate-service\TaniumInvestigateService.exe`
		Process	`<Module Server>\services\partner-integration-service\TaniumPartnerIntegrationService.exe`
Tanium Zone Server		Process	`<Tanium Installation Directory>\Tanium Direct Connect Zone Proxy\node.exe`
		Process	`<Tanium Installation Directory>\Tanium Direct Connect Zone Proxy\twsm.exe`

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

Patch

Patch security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`<Module Server>\services\patch-service\node.exe`
	Required when Endpoint Configuration is installed	Process	`<Module Server>\services\endpoint-configuration-service\TaniumEndpointConfigService.exe`

Performance

Performance security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`<Module Server>\services\performance-service\node.exe`
		Process	`<Module Server>\services\event-service\twsm.exe`
		Process	`<Module Server>\services\endpoint-configuration-service\TaniumEndpointConfigService.exe`

© 2026 Tanium Inc. All Rights Reserved

Provision

Provision security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`<Module Server>\services\provision-service\TaniumProvisionService.exe`
		Process	`<Module Server>\services\twsm-v1\twsm.exe`

RDB Service

RDB Service security exclusions for Tanium Core Platform Servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`<Module Server>\services\rdb-service\TaniumRdbService.exe`

Reporting

Reporting security exclusions for Tanium Core Platform servers (Windows deployment only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`<Module Server>\services\reporting-service\TaniumReportingService.exe`

Reputation

Reputation security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`<Module Server>\services\reputation-service\node.exe`

© 2026 Tanium Inc. All Rights Reserved

Reveal

Reveal security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	*<Module Server>*\services\reveal-service\node.exe
		Process	*<Module Server>*\services\endpoint-configuration-service\TaniumEndpointConfigService.exe

Screen Sharing

Screen Sharing security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	*<Module Server>*\services\screen-sharing-service\TaniumScreenSharingService.exe

Secrets Service

Secrets Service security exclusions for Tanium Core Platform Servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	*<Module Server>*\services\secrets-service\TaniumSecretsService.exe

System User Service

System User Service security exclusions for Tanium Core Platform Servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	*<Module Server>*\services\system-user-service\TaniumSystemUserService.exe

© 2026 Tanium Inc. All Rights Reserved

Threat Response

Threat Response security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Tanium Module Server		Process	*<Module Server>*\services\threat-response-service\node.exe
		Process	*<Module Server>*\services\twsm-v1\twsm.exe
		Process	*<Module Server>*\services\endpoint-configuration-service\TaniumEndpointConfigService.exe
Tanium Zone Server		Process	*<Tanium Installation Directory>*\Tanium Direct Connect Zone Proxy\node.exe
		Process	*<Tanium Installation Directory>*\Tanium Direct Connect Zone Proxy\twsm.exe

Trends

Trends security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	*<Module Server>*\services\twsm-v1\twsm.exe
	Required only during upgrade from Trends 3.8 and earlier	Process	*<Module Server>*\services\trends\node_modules\@tanium\postgresql\lib\win32\bin\postgres.exe
	Required only during upgrade from Trends 3.8 and earlier	Process	*<Module Server>*\services\trends\node_modules\@tanium\postgresql\lib\win32\bin\pg_ctl.exe

© 2026 Tanium Inc. All Rights Reserved

Zero Trust

Zero Trust security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`<Module Server>\services\zero-trust-service\TaniumZeroTrustService.exe`

© 2026 Tanium Inc. All Rights Reserved

Reference: Tanium Core Platform Command-line interface in a Windows deployment

You can use the command-line interface (CLI) to configure platform settings.

TIP

You can also change many platform settings through Tanium Console. For more information, see Tanium Console User Guide: Managing Tanium Core Platform settings.

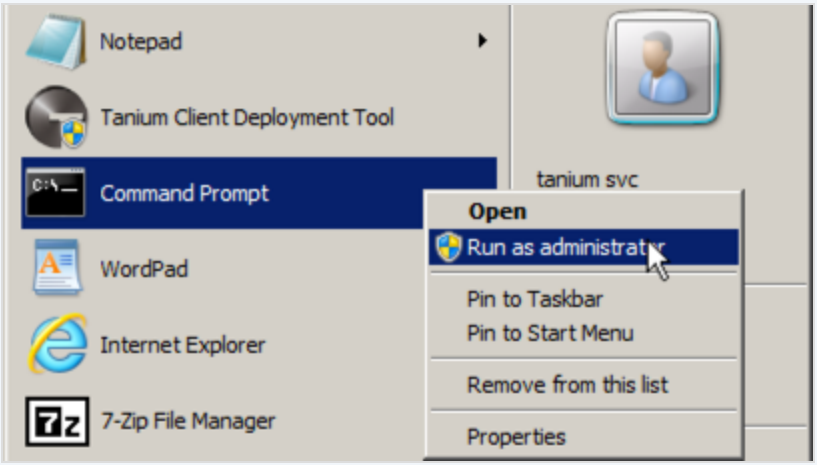
IMPORTANT

Contact Tanium Support on page 137 for guidance before you create, edit, or delete platform settings.

To access the CLI for a Tanium Core Platform component, open the **Command Prompt** and navigate to the directory where the component CLI program reside. The following table lists the directories. For descriptions of the settings that you can edit, see Deployment-related settings reference on page 183.

NOTE

To use the **Command Prompt** for commands that require administrator permissions, select the **Run as administrator** option to elevate permissions.



CLI directories for Windows deployment

Component	CLI program location
Tanium Server	`Program Files\Tanium\TaniumReceiver.exe`
Tanium Module Server	`Program Files\Tanium\TaniumModuleServer.exe`

© 2026 Tanium Inc. All Rights Reserved

CLI directories for Windows deployment (continued)

Component	CLI program location
Tanium Zone Server or Tanium Zone Server Hub	`Program Files (x86)\Tanium\Tanium Zone Server\TaniumZoneServer.exe`
TDownloader	`Program Files\Tanium\Tanium Server\TDownloader.exe`
	`Program Files\Tanium\Tanium Module Server\TDownloader.exe`

CLI examples

The following examples show how to use the CLI.

Display help

```
cmd-prompt>TaniumReceiver --help
Usage: TaniumReceiver [options] <command> [<args>]

General Options:
  -h [ --help ]         Print this help message
  -v [ --version ]      Print the version
  --verbose             Verbose output

Service Options:
  -i                    Install the service
  -u                    Uninstall the service
  -s                    Start the service
  -e                    Stop the service

Internal Tanium Options - DO NOT USE:
  -d                    Run without daemonizing

Commands:
  config                Manage configuration
  clean-downloads       Clean the downloads catalog
  database              Manages a database
  global-settings       Manages global settings
  license               Manages Deployment License
  pki                   Manages PKI
  registration-secret   Manages Client registration secrets
```

© 2026 Tanium Inc. All Rights Reserved

```
  server-registrations  Manages Server registration requests
  test-hsm              Test an HSM configuration
  trust-module-certs    Add trusted Module Server certificates

For help on a specific command run `TaniumReceiver COMMAND -h`
```

Display config help

```
cmd-prompt>TaniumReceiver config --help
Usage: TaniumReceiver config <action> [<key>] [<value>]

Actions:
  config list                         List all keys and non-protected values
  config list-protected               List all keys and values
  config get <key>                    Print non-protected config value
  config get-protected <key>          Print config value
  config set <key> <value>            Set config value and try to guess type
  config set-string <key> <value>     Set string value
  config set-protected <key> <value>  Set protected string value
  config set-number <key> <value>     Set numeric value (in decimal or hex notation)
  config remove <key>                 Remove config value
```

Example: List configuration settings

When displaying the current settings, note that the CLI output displays `(protected)` instead of the actual value for settings that are designated as protected, which means they are sensitive in the security sense.

```
cmd-prompt>TaniumReceiver config list
Keys:
  - AddressMask: 16777215
  - ConsoleSettingsJSON: C:\Program Files\Tanium\Tanium Server\http\config\console.json
  - DBUserDomain: tam.local
  - DBUserName: taniumsvc
  - LogPath: C:\Program Files\Tanium\Tanium Server\Logs
  - LogVerbosityLevel: 1
  - Logs:
    - Logs.MiniDumpMessages:
      - Logs.MiniDumpMessages.FilterRegex: .*Begin MiniDumper.*
      - Logs.MiniDumpMessages.LogVerbosityLevel: 1
```

© 2026 Tanium Inc. All Rights Reserved

```
- ModuleServer: tms1.tam.local,TMS1.tam.local:17477
- ModuleServerPort: 17477
- PGDLLPath: C:\Program Files\Tanium\Tanium Server\postgres\bin
- PKIDatabasePassword: (protected)
- PGRoot: C:\Program Files\Tanium\Tanium Server\postgres
- Path: C:\Program Files\Tanium\Tanium Server
- ProxyPassword: (protected)
- ProxyPort:
- ProxyServer:
- ProxyType: NONE
- ProxyUserid:
- SQLConnectionString: postgres:localhost@dbname=postgres port=5432
- ServerName: 0.0.0.0
- ServerPort: 17472
- ServerSOAPPort: 443
- TrustedCertPath: C:\Program Files\Tanium\Tanium Server\Certs\installedcacert.crt
- TrustedModuleServerCertsPath: C:\Program Files\Tanium\Tanium Server\trusted-module-servers.crt
- Version: 7.8.2.1234
```

Example: Set configuration values

```
cmd-prompt>TaniumReceiver config set BypassProxyHostList host1.example.com,192.168.0.1
cmd-prompt>TaniumReceiver config get BypassProxyHostList
host1.example.com,192.168.0.1
```

Example: Set configuration values

```
cmd-prompt>TDownloader config set ProxyServer 192.168.0.2
cmd-prompt>TDownloader config get ProxyServer
192.168.0.2
```

Example: Register the Module Server with the Tanium Server

On the Module Server host computer, use the CLI to register with a Tanium Server. Specify a Tanium Console administrator user name and password.

© 2026 Tanium Inc. All Rights Reserved

IMPORTANT

Registration involves copying files between the Module Server and the Tanium Server. Both Servers must be reachable when you issue the registration command or the command fails.

After registering the Module Server, you must restart the services for the **Tanium Module Server** and all Tanium modules and shared services. On the Module Server, open the Windows **Services** application and, for each service, right-click the service name and select **Restart**.

```
cmd-prompt>TaniumModuleServer register -h
Usage: TaniumModuleServer register <server> [opts]

  --server arg                    Tanium Server hostname (optionally including
                                  port)
  --address arg (=TMS1.tam.local) DNS name or IP that the Tanium Server should
                                  use to connect to this Module Server
  --timeout arg (=120)            Registration timeout in seconds
  --user arg                      Administrator username
  --pass arg                      Administrator password (leave blank for
                                  interactive prompt)
  --pass-file arg                 Administrator password protected file
  --trusted-fingerprint arg       Trust the given server certificate
                                  fingerprint
  --json-out arg                  JSON file to output results to

cmd-prompt>TaniumModuleServer register ts2.tam.local
Enter administrator username: TaniumAdmin

Enter password for user 'TaniumAdmin':
Successfully completed registration.
```

If Tanium Console has been configured to use a non-standard port, you must specify the port number, as shown in the following example.

```
cmd-prompt>TaniumModuleServer register ts2.tam.local:8443
Enter administrator username: TaniumAdmin

Enter password for user 'TaniumAdmin':
Successfully completed registration.

cmd-prompt>
```

© 2026 Tanium Inc. All Rights Reserved

If Tanium Console is not listening on 443 and you do not specify the port in the registration command, the registration results in failure with the message:

```
Failed to register Module Server. Failed to authenticate for registration.
SSLClientConnection has failed to complete request.
```

Example: Configure global settings

```
cmd-prompt>TaniumReceiver global-settings -h
Usage: TaniumReceiver global-settings list|list-all|get|set|set-string|set-numbe
r|set-flags|unset-flags|remove

  -c [ --command ] arg  Command to run:
                          list
                          list-all
                          get <setting>
                          set <setting> <value>
                          set-string <setting> <value>
                          set-number <setting> <value>
                          set-flags <setting> [public|hidden|read-only|server...]
                          unset-flags <setting> [public|hidden|read-only|server ...]
                          remove <setting>

cmd-prompt>TaniumReceiver global-settings set ReportingTLSMode 0
```

Example: Add an administrator user

```
cmd-prompt>TaniumReceiverdatabase -h
Usage: TaniumReceiver database create|upgrade|create-admin-user

  -c [ --command ] arg  Command to run:
                          create
                          upgrade
                          create-admin-user [username] [domain]
                          sqlserver2postgre outputfile

cmd-prompt>TaniumReceiver database create-admin-user admin-recover tam.local
```

© 2026 Tanium Inc. All Rights Reserved

Reference: Deployment-related Tanium Core Platform settings in a Windows deployment

While you configure the most critical Tanium Core Platform Server settings during initial installation, you can configure additional deployment-related settings afterward.

This section lists many of the deployment-related settings that you might need to change for your environment.

You can change most Tanium Core Platform Server settings through Tanium Console. For more information, see Tanium Console User Guide: Managing Tanium Core Platform settings.

For a reference of all Tanium Core Platform settings Tanium Console User Guide: Reference: Tanium Core Platform settings.

To configure Tanium Client settings, see Tanium Client Management User Guide: Tanium Client CLI and Client settings.

Contact Tanium Support for help configuring settings for your deployment.

Configure settings using the command line

You can change most settings through Tanium Console (see Tanium Console User Guide: Managing Tanium Core Platform settings), but if the Console is unavailable, you can use the following commands on each Tanium Core Platform Server to configure these settings.

- **Tanium Server**
  - Display the current settings: `TaniumReceiver config list`
  - View the value configured for a setting: `TaniumReceiver config get *SettingName*`
  - Configure a setting: `TaniumReceiver config set *SettingNamevalue*`
- **Tanium Module Server**
  - Display the current settings: `TaniumModuleServer config list`
  - View the value configured for a setting: `TaniumModuleServer config get *SettingName*`
  - Configure a setting: `TaniumModuleServer config set *SettingNamevalue*`
- **TDownloader on the Tanium Server or Tanim Module Server**
  - Display the current settings: `TDownloader config list`
  - View the value configured for a setting: `TDownloader config get *SettingName*`
  - Configure a setting: `TDownloader config set *SettingNamevalue*`

© 2026 Tanium Inc. All Rights Reserved

- **Tanium Zone Server**
  - Display the current settings: `TaniumZoneServer config list`
  - View the value configured for a setting: `TaniumZoneServer config get SettingName`
  - Configure a setting: `TaniumZoneServer config set SettingNamevalue`

Deployment-related settings reference

Platform settings used during deployment

Settings	Platform components	Guidelines
AddressMask	Tanium Server (local)	Enter the hexadecimal value of a subnet CIDR that defines the boundaries of a Tanium linear chain of IPv4 Tanium Clients. Contact Tanium Support for guidance before configuring this setting. For more information about the setting, see Tanium Client Management User Guide: AddressMask.
AddressPrefixIPv6	Tanium Server (local)	Enter a decimal number from 0 to 128 to represent the IPv6 prefix that defines the boundaries of a linear chain of IPv6 Tanium Clients. By default, this setting is hidden and has a value of `0`, which specifies no peering. Contact Tanium Support to determine the optimum value for peering in IPv6 networks. Do not add or change the setting without direction from Support. For more information, see Tanium Client Management User Guide: AddressPrefixIPv6.
AllowedHubs	Tanium Server (local) Zone Server	Configure this setting based on the infrastructure and server type. • **Tanium Server**: Enter a comma-separated list of Zone Server Hubs that are authorized to communicate with the Tanium Server. Specify the hubs by FQDN or IP address. You must enter IPv6 addresses within square brackets (for example, `[2001:db8::1]`). Note that you can configure exceptions to the AllowedHubs list in the Tanium Console User Guide: AllowedLocalHubs setting. • **Zone Server**: Enter a comma-separated list of Zone Server Hubs that are authorized to communicate with the Zone Server. Specify the hubs by FQDN or IP address. You must enter IPv6 addresses within square brackets (for example, `[2001:db8::1]`). If the Zone Server Hub resides on a different host than the Tanium Server, see Install the Zone Server Hub.
AllowedLocalHubs	Tanium Server	By default, this setting is hidden and has a value of `1`, which enables any local Zone Server Hub to communicate with the Tanium Server regardless of the Tanium Console User Guide: AllowedHubs setting. Setting the value to `0` allows local Zone Server Hubs to communicate with the Tanium Server only if they are listed in AllowedHubs. You must add this setting manually if you need it. Contact Tanium Support for guidance before adding this setting (see Contact Tanium Support).

© 2026 Tanium Inc. All Rights Reserved

Platform settings used during deployment (continued)

Settings	Platform components	Guidelines
BypassCRLCheckHostList	Tanium Server Module Server TDownloader	List the servers that the Tanium Server or Module Server can trust without checking a certificate revocation list (CRL). The Tanium Server and Module Server perform a CRL check on all servers that are not in this list, and do not download files from a server that fails the check. Specify the servers by FQDN or IP address. You must enter IPv6 addresses within square brackets (for example, `[2001:db8::1]`). Configure this setting in the Tanium Server and Module Server configurations. If you configure the Tanium Server and Module Server to access Internet sites through a proxy server, you can configure BypassCRLCheckHostList through Tanium Core Platform. For more information, see Tanium Console User Guide: Configuring proxy server settings.
BypassProxyHostList	Tanium Server Module Server TDownloader	If you configure the Tanium Core Platform to access Internet sites through a proxy server, enter a comma-separated list of FQDNs or IP addresses for the hosts that do not go through the proxy server. You do not have to enter `127.0.0.1`, `localhost`, or the Module Server, but enter active-active Tanium Servers if necessary. You must enter IPv6 addresses within square brackets (for example, `[2001:db8::1]`). Specify literal values. All supported Tanium Core Platform versions allow wildcards. Configure this setting in the Tanium Server and Module Server configurations. For more information, see Tanium Console User Guide: Configuring proxy server settings.
ConsoleSettingsJSON	Tanium Server	Path to the Tanium Console settings file.
DBUserDomain	Tanium Server	This is the domain for the Tanium Server service account that connects to the Tanium database server. You configure DBUserDomain when completing the installation wizard for the Tanium Server. For more information, see Install the Tanium Server.
DBUserName	Tanium Server	This is the user name for the Tanium Server service account that connects to the Tanium database server. You configure DBUserName when completing the installation wizard for the Tanium Server. For more information, see Install the Tanium Server.
DefaultHeaders	Tanium Server	The HTTP headers returned when a browser accesses Tanium Console. You can use this setting to enable HTTP Strict Transport Security (HSTS). For more information, see (Optional) Enable HTTP Strict Transport Security for Tanium Console access. Otherwise, do not change this setting unless Tanium Support instructs you to do so. IMPORTANT: Do not enable HSTS if you have not installed a CA-issued certificate. Doing so disables access to Tanium Console.

© 2026 Tanium Inc. All Rights Reserved

Platform settings used during deployment (continued)

Settings	Platform components	Guidelines
EnableFileCache	Zone Server	If the Zone Server Hub is installed on a dedicated host instead of on the Tanium Server host, set the value to `1` to enable file caching. You must configure this setting through the hub CLI. For more information, see Manage caching on the Zone Server and Zone Server Hub.
EnforceAllowedHubs	Tanium Server (local) Zone Server	Configure this setting to enable (`1`) or disable (`0`) enforcement of the Tanium Console User Guide: AllowedHubs setting. EnforceAllowedHubs is a setting on the Tanium Server and Zone Server. If the Zone Server Hub resides on a different host than the Tanium Server, the best practice is to set the value to the default `1` on both Servers. • **Tanium Server**: The value `1` specifies that only hubs listed in AllowedHubs can communicate with the Tanium Server. The value `0` specifies that any hub can communicate with the Tanium Server regardless of the AllowedHubs setting. • **Zone Server**: The value `1` specifies that only hubs listed in AllowedHubs can communicate with the Zone Server. The value `0` specifies that any hub can communicate with the Zone Server regardless of the AllowedHubs setting. For more information, see Install the Zone Server Hub on page 55.
ForceIPV6	Tanium Server Module Server TDownloader	In deployments where traffic between Tanium Core Platform Servers and the Internet traverses a proxy server, TDownloader resolves the proxy address as an IPv4 address by default. If the proxy server has an IPv6 address, add ForceIPV6 with a value of `1`. ForceIPV6 is a TDownloader setting on the Tanium Server and Module Server in both Appliance and Windows deployments. The setting is hidden by default and its default value is `0`. Contact Tanium Support for guidance before adding this setting (see Contact Tanium Support). For more information about proxy server settings, see Configuring proxy server settings.
hub_hot_cache_limit_in_MB	Zone Server Hub	Specify the maximum storage space in megabytes for the Zone Server Hub cache. The default is 0 (20% of disk space). This setting applies only if the hub is installed on a dedicated host instead of on the Tanium Server host and you enabled file caching on the hub (set the EnableFileCache on page 185 setting value to `1`). On Tanium Core Platform for Windows Deployments, add this setting with the **Type** set to **Server**. For more information, see Manage Zone Server caching.

© 2026 Tanium Inc. All Rights Reserved

Platform settings used during deployment (continued)

Settings	Platform components	Guidelines
HubPriorityList	Zone Server	Add this setting on the Zone Server to specify the FQDN or IP address of the preferred Zone Server Hub for sending Tanium Client content (such as sensor definitions, configuration information, and action package files) to the Zone Server. As long as that hub is available, the Zone Server does not receive content from any other hub. If the preferred hub goes down, the Zone Server fails over to receiving content from any other available hub. Typically you use this setting for active-active deployments that have pairs of Zone Servers and hubs, where each hub connects to each Zone Server.  In active-active deployments, add HubPriorityList to ensure that each Zone Server receives content from its closest hub. Configuring this setting also optimizes hub usage by ensuring that each hub serves one Zone Server instead of one hub servicing both Servers. For more information, see Zone Server High Availability.
is_airgap	Tanium Server	Do not edit this setting, which indicates an air-gapped environment and is set automatically when you first import air gap content.
LogPath	Tanium Server Module Server Zone Server	The location for Tanium Server logs. The default is `/opt/Tanium/TaniumServer/Logs`.

© 2026 Tanium Inc. All Rights Reserved

Platform settings used during deployment (continued)

Settings	Platform components	Guidelines
LogVerbosityLevel	Tanium Server (local) Module Server Zone Server TDownloader	Specify the logging level as a decimal value on the Tanium Client, Tanium Server, Module Server, or Zone Server. On the Tanium Server and Module Server, you can configure the logging level separately for TDownloader. For best practices and configuration, see Logging levels. NOTE: By default, this setting is not present on Tanium Clients unless you set the logging level when deploying Clients. TIP: If you deploy an action to configure this setting on Tanium Clients, use the **Set Windows Tanium Client Logging Level** or **Set Tanium Client Logging Level [Non-Windows]** package. BEST PRACTICE: On Tanium Clients that run on virtual desktop infrastructure (VDI) endpoints or endpoints with limited resources, disable logging to reduce disk writes. Temporarily re-enable logging on individual endpoints for troubleshooting.
ModuleServer	Tanium Server (local)	This setting specifies the IP address or FQDN of the Module Server. It is set automatically when the Module Server registers with the Tanium Server during installation. Contact Tanium Support before editing this setting (see Contact Tanium Support).
ModuleServerPort	Tanium Server (local)	This setting specifies the Module Server port (default `17477`) for traffic from the Tanium Server. The port is set automatically when the Module Server registers with the Tanium Server during installation. Contact Tanium Support before editing this setting (see Contact Tanium Support).

© 2026 Tanium Inc. All Rights Reserved

Platform settings used during deployment (continued)

Settings	Platform components	Guidelines
Path	All Tanium Core Platform Servers	This setting indicates the installation directory of the platform Server orTanium Client: You configure the path when completing the Server installation wizard. TIP For Linux, Solaris, and AIX Clients, you can use symbolic links. For more information, see the following tasks in the Tanium Client Management User Guide: • Move an existing installation of the Tanium Client on Linux • Move an existing installation of the Tanium Client on Solaris • Move an existing installation of the Tanium Client on AIX
PGDLLPath	Tanium Server	This setting indicates the directory path of the PostgreSQL Server libraries. The path is set automatically during Tanium Server installation. Contact Tanium Support before editing this setting (see Contact Tanium Support).
PGRoot	Tanium Server	This setting indicates the directory path of the PostgreSQL installation. The path is set automatically during Tanium Server installation. Contact Tanium Support before editing this setting (see Contact Tanium Support).
PKIDatabasePassword	Tanium Server (local)	Specify a password to encrypt the root keys that the Tanium Server stores in the `pki.db` file. For more information, see Tanium Console User Guide: Encrypt the root keys databaseTanium Console User Guide: Encrypt the root keys database.
ProxyPassword	Tanium Server Module Server TDownloader	For a proxy server that requires authentication, enter the password of the Tanium Console User Guide: ProxyUserid user that establishes a connection with the proxy server. Configure this setting in the Tanium Server and Module Server configurations. For more information, see Tanium Console User Guide: Configuring proxy server settings.
ProxyPort	Tanium Server Module Server TDownloader	Specify the proxy server listening port. Configure this setting in the Tanium Server and Module Server configurations. For more information, see Tanium Console User Guide: Configuring proxy server settings.

© 2026 Tanium Inc. All Rights Reserved

Platform settings used during deployment (continued)

Settings	Platform components	Guidelines
ProxyServer	Tanium Server Module Server TDownloader	Specify the IP address of the proxy server. Configure this setting in the Tanium Server and Module Server configurations. For more information, see Tanium Console User Guide: Configuring proxy server settings. NOTE: By default, the proxy server address is resolved as an IPv4 address. If the proxy server has an IPv6 address, you must enter it within brackets (for example, `[2001:db8::1]`) and configure the TDownloader setting Tanium Console User Guide: ForceIPV6 to `1`.
ProxyType	Tanium Server Module Server TDownloader	Specify the type of proxy server authentication. Configure this setting in the Tanium Server and Module Server configurations. The possible values are `Basic` or `NTLM`. For more information, see Tanium Console User Guide: Configuring proxy server settings.
ProxyUserid	Tanium Server Module Server TDownloader	For a proxy server that requires authentication, specify the user ID of the account that establishes a connection with the proxy server. ProxyUserid is a Tanium Server and Module Server setting. For more information, see Tanium Console User Guide: Configuring proxy server settings.

© 2026 Tanium Inc. All Rights Reserved

Platform settings used during deployment (continued)

Settings	Platform components	Guidelines
ServerName	Tanium Server Module Server	On the Tanium Server or Module Server, specify the network adapter binding that the Server uses to listen for IPv4 Client registrations. By default, this setting is hidden and has a value of `0.0.0.0`, which specifies binding to all network adapters. Contact Tanium Support for guidance before changing this setting (see Contact Tanium Support). NOTE: Do not specify a value for this setting on the Zone Server, where the setting is deprecated. On the Tanium Client, specify the FQDN or IP address of the Tanium Server or Zone Server with which the Client tries to connect. For more information, see Tanium Client Management User Guide: ServerName. BEST PRACTICE: If you are manually configuring this setting, specify an FQDN. TIP: If you deploy an action to configure this setting on the Tanium Client, use the **Set Tanium Server Name** or **Set Tanium Server Name [Non-Windows]** package.
ServerNameIPv6	Tanium Server Module Server	By default, this setting is hidden and has a value of `[::]`, which specifies that the Server binds to all network adapters to listen for IPv6 Client registrations. To bind to a specific network adapter, add the setting and enter the IPv6 address of the adapter within square brackets (for example, `[2001:db8::1]`). Contact Tanium Support for guidance before adding this setting (see Contact Tanium Support).

© 2026 Tanium Inc. All Rights Reserved

Platform settings used during deployment (continued)

Settings	Platform components	Guidelines
ServerPort	Tanium Server (local) Module Server Zone Server	On Tanium Core Platform Servers, the ServerPort is set during Server installation. Update this setting if necessary according to the Tanium infrastructure and Server: • **Tanium Server**: This is the port on which the Server listens for Tanium Clients. The default is `17472`. You configure ServerPort when completing the Tanium Server installation wizard. For more information, see Install the Tanium Server. • **Module Server**: Specify the port for traffic from the Tanium Server. The default is `17477`. You configure ServerPort when completing the Module Server installation wizard. For more information, see Installing the Module Server. • **Zone Server Hub**: Specify the inbound port for traffic from the Tanium Server and Zone Server. The default is `17472`. You configure ServerPort when completing the hub installation wizard. For more information, see Installing the Zone Server. NOTE For information about port settings on the Zone Server, see ZoneServerPort on page 193 and ZoneServerPortForHub on page 193. On the Tanium Client, the ServerPort is set during Client installation. It specifies the port to use for communication between Clients and between Clients and Tanium Core Platform Servers. The default is 17472. If you need to update the port, see Tanium Client Management User Guide: ServerPort. NOTE If you configure the Reference: Deployment-related Tanium Core Platform settings in a Windows deployment on page 182 or Reference: Deployment-related Tanium Core Platform settings in a Windows deployment on page 182 setting, it overrides ServerPort for client-client communication. For more information, see Tanium Client Management User Guide: Customize listening ports.
ServerSOAPPort	Tanium Server (local)	Specify the port for Tanium Core Platform and the SOAP API. The default is `443`. You specify the port when completing the Tanium Server installation wizard. For more information, see Install the Tanium Server.
ServiceUserDomain	Zone Server Zone Server Hub	This is a setting on the Zone Server and Zone Server Hub. The Windows service for the Zone Server or hub runs in the context of a service account. You configure the domain when completing the installation wizard. For more information, see Installing the Zone Server.

© 2026 Tanium Inc. All Rights Reserved

Platform settings used during deployment (continued)

Settings	Platform components	Guidelines
ServiceUserName	Zone Server Zone Server Hub	This is a setting on the Zone Server and Zone Server Hub. The Windows service for the Zone Server or hub runs in the context of a service account. You configure the user name when completing the installation wizard. For more information, see Installing the Zone Server.
SQLConnectionString	Tanium Server (local)	Specify connection information for the Tanium database server, such as in the following examples: • **MSSQL**: `SQL1\SQLEXPRESS@tanium` • **PostgreSQL**: `postgres:<server IP address>@user=postgres dbname=tanium sslmode=require sslcert=/Program Files/Tanium/.postgresql/postgresql.crt sslkey=/Program Files/Tanium/.postgresql/postgresql.key sslcompression=1` For the supported PostgreSQL keywords, such as `dbname`, `port`, and `user`, see the PostgreSQL documentation . IMPORTANT If you change this setting, you must restart the Tanium Server: For more information, see .
SSLCipherSuite	Tanium Server (local)	Specify the cipher suites to use for TLS connections to the Tanium Server from the Module Server or the systems of Tanium Console users. The default is `TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384`. For more information, see Supported cipher suites.
SSLHonorCipherOrder	Tanium Server (local)	When the Tanium Server and Tanium Client determine a mutual set of supported ciphers, the Client normally selects which cipher to use. However, if you set SSLHonorCipherOrder to `1`, the Server selects a mutually supported cipher based on the SSLCipherSuite on page 192 setting. The Server applies an order of preference from left to right when selecting from the ciphers that SSLCipherSuite lists. For more information, see Supported cipher suites.
TrustedCertPath	Tanium Server TDownloader	Path to the certificate file used for secure connections to the Tanium Console port.

© 2026 Tanium Inc. All Rights Reserved

Platform settings used during deployment (continued)

Settings	Platform components	Guidelines
TrustedHostList	Tanium Server (local) Module Server TDownloader	By default, the Tanium Server and Module Server validate the SSL/TLS certificate of remote servers when establishing connections to them (such as for downloading files). To bypass certificate validation for specific servers, enter their FQDN or IP address. You do not have to enter 127.0.0.1, localhost, the Tanium Module Server, or Tanium Servers (standalone or active-active). Wildcards are supported. You must enter IPv6 addresses within square brackets (for example, `[2001:db8::1]`). TrustedHostList is a Tanium Server and Module Server setting. For more information, see Tanium Console User Guide: Configuring proxy server settings.
Version	Tanium Server (local) Module Server Zone Server Zone Server Hub	Do not edit this setting, which indicates the Server or Client version.
ZoneHubFlag	Zone Server Zone Server Hub	On the host where you install an instance of the Zone Server or Zone Server Hub, this setting indicates whether the current instance is (`1`) or is not (`0`) a hub. View the setting through the CLI. For more information, see Reference: Command-line interface.
zs_hot_cache_limit_in_MB	Zone Server	This setting applies only if the Zone Server Hub is installed on a dedicated host instead of on the Tanium Server host and file caching is enabled on the hub through the EnableFileCache on page 185 setting. You can configure zs_hot_cache_limit_in_MB to specify the maximum storage space in megabytes for the hub cache. By default, zs_hot_cache_limit_in_MB is hidden and has a value of `0` (20% of disk space). On Tanium Core Platform, manually add zs_hot_cache_limit_in_MB as a Server setting. For more information, see Manage caching on the Zone Server and Zone Server Hub.
ZoneServerPort	Zone Server	On the Zone Server, configure the incoming port (default `17472`) for traffic from Tanium Clients. For more information, see Configure ports for traffic from Zone Server Hubs and Tanium Clients.
ZoneServerPortForHub	Zone Server	On the Zone Server, configure the incoming port (default `17472`) for traffic from Zone Server Hubs. For more information, see Configure ports for traffic from Zone Server Hubs and Tanium Clients.

© 2026 Tanium Inc. All Rights Reserved

Reference: Default installation directories for Tanium Core Platform Servers

The following table lists the default installation paths for Tanium Core Platform Servers. If you troubleshoot issues for an installation that uses a non-default path, note this when you contact Tanium Support.

Target Server	Installation directory
Tanium Server	`\Program Files\Tanium\Tanium Server`
Tanium Module Server	`\Program Files\Tanium\Tanium Module Server` `\Program Files\Tanium\Tanium Module Postgres`
Tanium Zone Server	`\Program Files (x86)\Tanium\Tanium ZoneServer`
*Tanium Zone Server Hub	`\Program Files (x86)\Tanium\Tanium ZoneServer`

* The Zone Server Hub can be on the same host as the Tanium Server or on a dedicated host.

© 2026 Tanium Inc. All Rights Reserved

Reference: Default installation directory for the Tanium Client

The following table lists the default installation paths for the Tanium Client on each operating system (OS). If you troubleshoot issues for an installation that uses a non-default path, note this when you Contact Tanium Support.

OS	Installation Directory
Windows (64-bit OS versions)*	\Program Files (x86)\Tanium\Tanium Client\
Windows (32-bit OS versions)*	\Program Files\Tanium\Tanium Client\
macOS	/Library/Tanium/TaniumClient
Linux, UNIX	/opt/Tanium/TaniumClient

* On both 64-bit and 32-bit versions of Windows, Tanium Client is installed as a 32-bit application.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform and Tanium Client Export Commodity Classification (Windows deployments)

The Export Commodity Classification Automated Tracking System (CCATS) number for Tanium is G172792. The Export Control Classification Numbers (ECCNs) for Tanium 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
Tanium Server software	5D002.c.1	ENC/(b)(1)	All countries, except Embargoed Countries and the Crimea Region of Ukraine
Tanium Module Server software	5D002.c.1	ENC/(b)(1)	All countries, except Embargoed Countries and the Crimea Region of Ukraine



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.

© 2026 Tanium Inc. All Rights Reserved