

Tanium™ Certificate Manager User Guide

Autonomous IT. Unstoppable Business.

2026H1 Semiannual Release

Version 1.22

August 19, 2026

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

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

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

This documentation may provide access to or information about content, products (including hardware and software), and 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

Certificate Manager overview **10**

Supported certificates and Java KeyStores 10

Supported extensions for audit 10

Supported certificates for replacement 11

Certificate discovery methods 11

Certificate sources 12

Certificate Manager dashboard 13

Certificate Manager reports 15

Certificate Manager packages 15

Certificate Details sensor 16

Tanium Autonomous IT Platform in Certificate Manager 17

Interoperability with other Tanium products 17

Direct Connect 17

Tanium™ Guide 17

Endpoint Configuration 17

Reporting 17

Getting started with Certificate Manager **18**

Endpoints with Toolset 2.20.86 or later 18

Step 1: Install and configure Certificate Manager 18

Step 2: Add locations for at-rest certificates and Java KeyStores 18

Step 3: Configure certificate audits 18

Step 4: View and manage certificates 18

Endpoints with Toolset versions earlier than 2.20.86 18

Step 1: Install and configure Certificate Manager 18

Step 2: View and manage certificates 18

Step 3: Deploy certificate audits 18

Certificate Manager requirements **19**

© 2026 Tanium Inc. All Rights Reserved

Core platform dependencies ... 19
Solution dependencies ... 19
Tanium recommended installation ... 19
Import specific solutions ... 19
Required dependencies ... 19
Feature-specific dependencies ... 20
Client extensions and endpoint tools ... 20
Endpoints ... 20
Supported operating systems ... 20
Host and network security requirements ... 21
Security exclusions ... 21
User role requirements ... 22
Installing Certificate Manager ... 27
Before you begin ... 27
Import Certificate Manager with default settings ... 27
Import Certificate Manager with custom settings ... 28
Manage solution dependencies ... 28
Upgrade Certificate Manager ... 28
Verify Certificate Manager version ... 28
Configuring Certificate Manager ... 30
Install and configure Tanium Endpoint Configuration ... 30
Manage solution configurations with Tanium Endpoint Configuration ... 30
Configure Certificate Manager ... 31
Configure the Certificate Manager action group ... 31
Set up Certificate Manager users ... 31
Configure audit settings ... 33
Configure exclusion list ... 34
Configure certificate authorities ... 35
Obtain the certificate chain for your external CA using OpenSSL ... 35
Obtain your internal CA certificates ... 37

© 2026 Tanium Inc. All Rights Reserved

Configure and manage authorized CAs ... 38
Configure approved ciphers ... 39
Configure certificate replacement settings ... 40
Configure certificate port exceptions ... 41
Add port exclusions ... 41
Delete port exclusions ... 42
Deploy a certificate audit package ... 42
Customize Guide observations ... 43
Before you begin ... 43
Customize criteria for Certificate Manager-specific observations ... 44
Managing certificates ... 45
View the Certificate Manager dashboard in Tanium Reporting ... 45
View expired certificates ... 45
View expiring certificates ... 45
View listening service certificates that are expiring in 30 days ... 45
View all certificates that are expiring in 30 days ... 46
Email a report of expiring certificates with Tanium Connect ... 46
Before you begin ... 46
Create a connection ... 46
View short keys ... 47
View listening service certificates that use short keys ... 47
View all certificates that use short keys ... 47
View weak signatures ... 47
View listening service certificates that use weak signatures ... 47
View all certificates that use weak signatures ... 47
View wildcard certificates ... 47
View listening service certificates that use a wildcard subject ... 47
View all certificates that use a wildcard subject ... 48
View self-signed certificates ... 48
View unauthorized certificates ... 48

© 2026 Tanium Inc. All Rights Reserved

Prepare for post-quantum cryptography ... 48
View listening services accepting unapproved ciphers ... 49
View listening service certificates by approval status ... 49
View certificate inventory ... 49
View certificate details ... 52
Download certificate ... 53
Replace certificate ... 53
Before you begin ... 54
Generate certificate signing request ... 54
Download the certificate request and upload the new certificate ... 56
Create configuration packages ... 57
Deploy configuration packages ... 59
Verify package deployment ... 61
(Optional) Finalize certificate replacement ... 61
Configuring certificate locations ... **63**
Review certificate locations ... 63
Disable certificate location ... 64
Next steps ... 64
Add custom certificate location ... 64
Next steps ... 64
Deploy locations ... 64
Manage certificate locations ... 65
Edit custom certificate location ... 65
Next steps ... 65
Delete custom certificate location ... 65
Next steps ... 65
Deploying certificate audits ... **66**
Before you begin ... 66
Create a profile ... 66
Next steps ... 68

© 2026 Tanium Inc. All Rights Reserved

Cipher suites approved by default ... 68
Set the priority of profiles ... 69
Next steps ... 69
Review profiles ... 69
Enable or disable profiles ... 70
Next steps ... 70
Deploy profiles ... 71
Manage profiles ... 71
Edit profile ... 71
Next steps ... 71
Import profiles ... 71
Next steps ... 72
Export profiles ... 72
Delete profile ... 72
Next steps ... 72
Maintaining Certificate Manager ... 73
Perform monthly maintenance ... 73
Perform as-needed maintenance ... 73
Monitor and troubleshoot Certificate Manager Coverage ... 73
Troubleshooting Certificate Manager ... 75
Collect logs ... 75
Collect troubleshooting packages ... 75
Collect action logs ... 75
Endpoints with Toolset 2.20.86 or later ... 75
Endpoints with Toolset versions earlier than 2.20.86 ... 75
Review the activity log ... 76
Cannot view all chart panels in the dashboard ... 78
Issue ... 78
Solution ... 78
Endpoint does not have Toolset 2.20.86 or later ... 78

© 2026 Tanium Inc. All Rights Reserved

Endpoint with profile needs attention ... 79
Endpoint continues to run certificate audits after uninstalling or blocking Certificate Manager tools ... 79
Issue ... 79
Solution ... 79
Unexpected certificate audit results ... 79
Issue ... 80
Solution ... 80
Unable to view expected computer groups ... 80
Issue ... 80
Solution ... 80
Error: EC_KEY_new_by_curve_name ... 80
Issue ... 80
Solution ... 80
ERROR - lsof was not found ... 81
Issue ... 81
Solution ... 81
ERROR - No SSL Scan is being performed, limited data available ... 81
Issue ... 81
Solution ... 82
Verify that a certificate audit completed successfully ... 82
Verify endpoint tools ... 82
Uninstall Certificate Manager ... 83
Contact Tanium Support ... 83
Reference: Certificate Manager endpoint tools ... 84
Reference: Sensor usage ... 85

© 2026 Tanium Inc. All Rights Reserved

Certificate Manager overview

With Tanium Certificate Manager, gain complete visibility into the digital certificates across your Windows, macOS, and Linux endpoints managed by Tanium Client.

With weak endpoint encryption, communications are at risk of interception, and certificates that expire can cause critical business service outages. Use Certificate Manager to find and alert on expired or expiring certificates and to provide visibility into certificate and cipher encryption strength.

Certificate Manager provides dashboards, reports, sensors, and packages that you can use to:

- Find expired or expiring certificates
- Replace expired or expiring certificates
- Identify weak cryptographic algorithms and key lengths
- View self-signed and unauthorized CA certificates
- Inventory TLS ciphers for listening services
- Send reports with certificate details through Tanium™ Connect

Supported certificates and Java KeyStores

Certificate Manager supports the following certificates and Java KeyStores.

Supported extensions for audit

During a certificate audit, Certificate Manager gathers data on X.509 certificates and Java KeyStores with the following extensions.

Endpoint operating system	Supported extensions
Windows	• CRT • CER • PEM • Any certificate located in Windows certificate stores • JCEKS • JKS (only from Sun)

© 2026 Tanium Inc. All Rights Reserved

Endpoint operating system	Supported extensions
Linux	• CRT • CER • PEM • JCEKS • JKS (only from Sun)
macOS	• CRT • CER • PEM • JCEKS • JKS (only from Sun) NOTE Certificate Manager does not support any certificate stored in the keychain.

Certificate Manager finds these certificates and Java KeyStores in certain locations. For more information, see Certificate sources on page 12.

Supported certificates for replacement

Certificate Manager supports certificate replacement for any certificate identified during a certificate audit and for which Certificate Manager can locate and export its corresponding private key. You can identify these certificates on the **Certificate Inventory** page by using the **Private Key Available** filter. For more information, see Replace certificate on page 53.

NOTE For Windows certificates, Certificate Manager currently determines if the private key is exportable only after you start the certificate replacement process.

Certificate discovery methods

Certificate Manager uses three discovery methods to find certificates and Java KeyStores. For endpoints with Toolset versions earlier than 2.20.86, you configure these methods in the module settings. For more information, see Configuring Certificate Manager on page 30. For endpoints with Toolset 2.20.86 or later, you configure these methods in a profile. For more information, see Deploying certificate audits on page 66.

© 2026 Tanium Inc. All Rights Reserved

- A listening port certificate scan looks for certificates included in active port traffic. Certificate Manager performs this scan.

  To use this discovery method, you must enable the listening port scan.

- An at-rest certificate (or file) scan looks for certificates not being used by SSL/TLS services. For endpoints with Toolset versions earlier than 2.20.86, Certificate Manager performs this scan. For endpoints with Toolset 2.20.86 or later, an at-rest certificate scan also looks for Java KeyStores. Tanium Client Index Extension performs this scan. For more information, see Tanium Client Index Extension User Guide.
- A Windows Store certificate scan looks for certificates on Windows computers. Certificate Manager performs this scan.

Certificate sources

A *certificate source* is where Certificate Manager finds the certificates and Java KeyStores on the endpoint. The **Certificate Sources** chart panel in the **Certificate Manager** dashboard shows the top 10 certificate locations.

The following table describes where and how Certificate Manager finds certificates and Java KeyStores on each of the supported OS platforms.

Tanium Certificate Manager certificate discovery method

Certificate discovery method	Platforms	Locations	Unique capabilities	Customization
Listen ports*	• Windows • Linux • macOS	• Endpoints with Toolset versions earlier than 2.20.86: All ports except for some of the Tanium™ Client and Tanium Client API ports • Endpoints with Toolset 2.20.86 or later: All ports, including the option to include or exclude the Tanium Client and Tanium Client API ports	• Quantum Computer Vulnerable Ciphers • Authorized Certificate Authority (CA) • Cipher Strength • Owning Process	• Certificate Audit Add Port Exclusions • Certificate Audit Delete Port Exclusions

© 2026 Tanium Inc. All Rights Reserved

Tanium Certificate Manager certificate discovery method (continued)

Certificate discovery method	Platforms	Locations	Unique capabilities	Customization
File	• Linux • Windows • macOS	• Linux ◦ `/etc/pki/*` ◦ `/etc/ssl/*` ◦ Endpoints with Toolset 2.20.86 or later: ▪ `/usr/lib/jvm` ▪ `/usr/lib64/jvm` ▪ `/usr/share/ca-certificates` • Windows ◦ `Program Files` • macOS ◦ `/Library/Java/JavaVirtualMachines`	NOTE Certificate Manager does not inspect Java Keystores formatted with PKCS #12.	• Endpoints with Toolset versions earlier than 2.20.86: **Exclusion List** in **Certificate Manager Settings** • Endpoints with Toolset 2.20.86 or later: Certificate Manager **Configuration > Certificate Locations** page
Windows Certificate Store	Windows	• User certificate store for signed-in users NOTE Certificate Manager only finds user store certificates for users signed in during the audit. • Local machine certificate store	None	Exclusion List in Certificate Manager Settings

* Only one certificate is audited for each port.

Certificate Manager dashboard

The **Certificate Manager** dashboard in Tanium™ Reporting and the Certificate Manager **Overview** page includes the **Overview**, **Listening SSL/TLS Services Certificate and Cipher Inventory**, **All Certificates**, and **Health** sections, with the following chart panels:

© 2026 Tanium Inc. All Rights Reserved

- Overview
    - Total Certificates Inventoried
    - Total Endpoints Inventoried
    - Total Listening Service Certificates Inventoried
    - Total Root Certificates Inventoried
- Listening SSL/TLS Services Certificate and Cipher Inventory
    - Listening Service Certificates Expiring in 30 Days
    - Listening Service Short Keys
    - Listening Service Weak Signature Hash Algorithms
    - Listening Services with Wildcard Certificates
    - Listening Service Certificate Authorized CA Status
    - Certificate Expiration on Listening Services
    - Listening Services Accepting Unapproved Ciphers
    - Listening Services Accepting Unapproved Ciphers Over Time
    - Listening Service Cipher Inventory
- All Certificates
    - Expired Certificates
    - Wildcard Certificates
    - Weak Signature Hash Algorithms
    - Total Short Keys
    - Expiring within 30 Days
    - Certificate Expiration
    - Certificate Sources
    - Certificate Issuers
- Health
    - Endpoints Using Profiles
    - Endpoints Not Using Profiles
    - Endpoints with Profiles Needing Attention
    - Endpoints with Profiles and No Certificates

For more information, see View the Certificate Manager dashboard in Tanium Reporting on page 45.

© 2026 Tanium Inc. All Rights Reserved

Certificate Manager reports

Review Certificate Manager reports to gain insights about certificates and view report details. The following Certificate Manager reports are available in Tanium Reporting and the Certificate Manager **Overview** page:

- Certificate Manager - Current Coverage Status Details

  This report only applies to endpoints with Toolset versions earlier than 2.20.86.

- Certificate Manager - CX Endpoints
- Certificate Manager - CX Endpoints Needing Attention
- Certificate Manager - CX Errors
- Certificate Manager - Endpoints Not Using Profiles
- Certificate Manager - Expired Certificates
- Certificate Manager - Inventoried Endpoints
- Certificate Manager - Listening Service Certificate Details
- Certificate Manager - Listening Service Certificates Expiring within 30 Days
- Certificate Manager - Listening Service Cipher Suite Details
- Certificate Manager - Listening Services Accepting Unapproved Ciphers
- Certificate Manager - Listening Service Short Keys
- Certificate Manager - Listening Service SSL Certificate Details
- Certificate Manager - Listening Service Weak Signatures
- Certificate Manager - Listening Service Wildcard Certificates
- Certificate Manager - Root Certificate Details

For more information, see Managing certificates on page 45.

Certificate Manager packages

For endpoints with Toolset versions earlier than 2.20.86, Certificate Manager provides the following packages that you can deploy to gather certificate data from your endpoints:

- Certificate Audit [Non-Windows]
- Certificate Audit [Windows]
- Certificate Audit Add Port Exclusions [Non-Windows]

© 2026 Tanium Inc. All Rights Reserved

- Certificate Audit Add Port Exclusions [Windows]
- Certificate Audit Delete Port Exclusions [Non-Windows]
- Certificate Audit Delete Port Exclusions [Windows]

For more information, see Deploy a certificate audit package on page 42.

For endpoints with Toolset 2.20.86 or later, you do not need to deploy packages to gather certificate data from your endpoints. The Certificate Manager endpoint tools automatically deploy necessary content to gather certificate data from your endpoints.

Certificate Details sensor

The **Certificate Details** sensor includes the following columns:

Certificate Details columns

Column name	Description
Source	Certificate sources on page 12 of the certificate that is captured by the Certificate Audit action
Location	Specific location of the certificate within the certificate source
Subject	Full subject of the captured certificate
Issuer	The Certificate Authority that issued the certificate
Not Before	Start date of the certificate validity
Not After	Expiration date of the certificate
Expiration Status	Length of time until the certificate expires
Public Key Algorithm	Type of public key algorithm that the certificate uses
Public Key Bit Size	Public key length of the certificate
Signature Algorithm	Type of signature algorithm that the certificate uses
Signature Hash Algorithm	Signature hashing algorithm strength of the certificate
Subject Alternative Name	Additional host names for the certificate
Common Name	Common name of the certificate
Is Wildcard	Boolean value that indicates whether the certificate common name includes a wildcard character (*)
SHA256 Thumbprint	String of 64 hexadecimal digits that identifies the specific certificate in a certificate store
SHA1 Thumbprint	String of 40 hexadecimal digits that identifies the specific certificate in a certificate store
MD5 Thumbprint	String of 32 hexadecimal digits that identifies the specific certificate in a certificate store

© 2026 Tanium Inc. All Rights Reserved

Tanium Autonomous IT Platform in Certificate Manager

- **Guide notifications**: Certificate Manager can generate Guide observations related to certificate expiration. Tanium operators that receive these observations can view the affected certificates and replace certificates for which the private keys are available. For more information, see Customize Guide observations on page 43 and Tanium Guide User Guide: Viewing and managing notifications.

Interoperability with other Tanium products

Direct Connect

Certificate Manager uses Tanium™ Direct Connect to view certificate details and to download certificates from individual endpoints. For information, see View certificate details on page 52 and Download certificate on page 53.

Tanium™ Guide

Tanium Guide can generate Certificate Manager-related notifications for Tanium operators, which provide insight into certificate expiration.

For more information, see Tanium Guide User Guide: Overview.

Endpoint Configuration

Enable approvals for endpoint configuration changes with Tanium™ Endpoint Configuration. For more information, see Tanium Endpoint Configuration User Guide.

Reporting

View the Certificate Manager dashboard and reports in Reporting. For more information, see Tanium Reporting User Guide: Reporting overview.

You can also use the **Tanium Reporting (Source Data)** source in Tanium Connect to send Certificate Manager data to multiple destinations. For more information, see Email a report of expiring certificates with Tanium Connect on page 46.

© 2026 Tanium Inc. All Rights Reserved

Getting started with Certificate Manager

Follow these steps to configure and use Certificate Manager.

Endpoints with Toolset 2.20.86 or later

Step 1: Install and configure Certificate Manager

See Installing Certificate Manager on page 27 and Configuring Certificate Manager on page 30.

Step 2: Add locations for at-rest certificates and Java KeyStores

For more information, see Configuring certificate locations on page 63.

Step 3: Configure certificate audits

For more information, see Deploying certificate audits on page 66.

Step 4: View and manage certificates

For more information, see Managing certificates on page 45.

Endpoints with Toolset versions earlier than 2.20.86

Step 1: Install and configure Certificate Manager

For more information, see Installing Certificate Manager on page 27 and Configuring Certificate Manager on page 30.

Step 2: View and manage certificates

For more information, see Managing certificates on page 45.

Step 3: Deploy certificate audits

For more information, see Deploy a certificate audit package on page 42.

© 2026 Tanium Inc. All Rights Reserved

Certificate Manager requirements

Review the requirements before you install and use Certificate Manager.

Core platform dependencies

Make sure that your environment meets the following requirements:

- Tanium license that includes the Core Plus bundle. For more information about how to get a bundle, see Tanium Solutions & Bundles.
- **Tanium™ Core Platform servers**
- **Tanium Client**

Solution dependencies

Certificate Manager requires other Tanium solutions to function (required dependencies) or for specific Certificate Manager features to work (feature-specific dependencies). The installation method that you select determines if the Tanium Server automatically imports dependencies or if you must manually import them.

NOTE

Some Certificate Manager dependencies have their own dependencies, which you can see by clicking the links in the lists of Required dependencies on page 19 and Feature-specific dependencies on page 20. Note that the links open the user guides for the latest version of each solution, not necessarily the minimum version that Certificate Manager requires.

Tanium recommended installation

If you select **Tanium Recommended Installation** when you import Certificate Manager, the Tanium Server automatically imports all your licensed solutions at the same time. For more information, see Tanium Console User Guide: Import all modules and services.

Import specific solutions

If you select only Certificate Manager to import, you must manually import dependencies. For more information, see Tanium Console User Guide: Import or update specific solutions.

Required dependencies

Certificate Manager has the following required dependencies:

© 2026 Tanium Inc. All Rights Reserved

- Tanium™ Endpoint Configuration
- Tanium™ Interact
- Tanium™ Data Service (TDS)
- Tanium Reporting
- Tanium™ RDB Service
- Tanium Direct Connect

Feature-specific dependencies

Certificate Manager has the following feature-specific dependencies:

- Tanium Connect 5.9.65 or later to create connections with reports as the data source

Client extensions and endpoint tools

Tanium Endpoint Configuration installs Client Extensions and other tools for Certificate Manager on endpoints. Client extensions perform tasks that are common to certain Tanium solutions. Each Client Extension and tool might have recommended security exclusions to allow them to run without interference. For more information, see Security exclusions. For a list of Certificate Manager tools, see Reference: Certificate Manager endpoint tools on page 84.For a list of Certificate Manager tools, see Reference: Endpoint Management for Operational Technology endpoint tools. For a list of all Client Extensions and tools, see Tanium Client Management User Guide: Reference: Client extensions and endpoint tools used for Tanium solutions.

Endpoints

Supported operating systems

The following Tanium Client managed endpoint operating systems are supported with Certificate Manager.

Endpoint operating systems supported with Tanium Certificate Manager

Operating System	Version	Notes
Windows	Same as Tanium Client support. For more information, see Tanium Client Management User Guide: Client version and operating system requirements.	Endpoints with Toolset 1.16 or earlier: Listen port scans are not supported on endpoints with Windows Server 2008 R2 or earlier, and Windows 7 or earlier. For more information, see Deploy a certificate audit package on page 42.
macOS	Same as Tanium Client support. For more information, see Tanium Client Management User Guide: Client version and operating system requirements.	SSL Audit only

© 2026 Tanium Inc. All Rights Reserved

Endpoint operating systems supported with Tanium Certificate Manager (continued)

Operating System	Version	Notes
Linux	Same as Tanium Client support. For more information, see Tanium Client Management User Guide: Client version and operating system requirements.	Endpoints with Toolset 1.16 or earlier: • Requires OpenSSL 1.0.1 or later. For more information, see Error: EC_KEY_new_by_curve_name on page 80. NOTE: Note: Certificate Manager attempts to use the OpenSSL library that is included with TPython. If successful, the endpoint does not need a separate version of OpenSSL installed. • Requires lsof to capture owning process data. For more information, see ERROR - lsof was not found on page 81.

Host and network security requirements

Specific processes are needed to run Certificate Manager.

Security exclusions

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

NOTE

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

© 2026 Tanium Inc. All Rights Reserved

Certificate Manager security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows		Folder	<*Tanium Client*>\python312
		File	<*Tanium Client*>\TPython\TPython.bat
		Folder	<*Tanium Client*>\TPython312
		Process	<*Tanium Client*>\python312\TPython.exe
		Process	<*Tanium Client*>\TaniumCX.exe
		Process	<*Tanium Client*>\Tools\StdUtils\TaniumExecWrapper.exe
		Folder	<*Tanium Client*>\Tools\CertificateManager
Linux		Process	<*Tanium Client*>/TPython/TPython
		Folder	<*Tanium Client*>/TPython312
		Process	<*Tanium Client*>/python312/python
		Process	<*Tanium Client*>/python312/bin/pybin
		Process	<*Tanium Client*>/TaniumCX
		Process	<*Tanium Client*>/Tools/StdUtils/TaniumExecWrapper
		Folder	<*Tanium Client*>/Tools/CertificateManager
macOS		Process	<*Tanium Client*>/TPython/TPython
		Folder	<*Tanium Client*>/TPython312
		Folder	<*Tanium Client*>/python312
		Process	<*Tanium Client*>/python312/python
		Process	<*Tanium Client*>/python312/bin/pybin
		Process	<*Tanium Client*>/TaniumCX
		Process	<*Tanium Client*>/Tools/StdUtils/TaniumExecWrapper
		Folder	<*Tanium Client*>/Tools/CertificateManager

User role requirements

Predefined roles grant the following permissions, which are required to use Certificate Manager functionality:

© 2026 Tanium Inc. All Rights Reserved

- Certificate Manager solution permissions on page 23
- Certificate Manager administration and platform content permissions on page 25: The solution permissions automatically provide some of these permissions.

To review a summary of the predefined roles, see Set up Certificate Manager users on page 31.

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

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



Do not assign the **Certificate Manager Service Account** role to users. This role is for internal purposes only.

Certificate Manager solution permissions

Permission	Certificate Manager Operator[1]	Certificate Manager User[1]	Certificate Manager Read Only User[1]	Certificate Manager Package Author	Certificate Manager Configuration Manager[1]	Certificate Manager Configuration Approver[1]
Certificate Manager SHOW: View the Certificate Manager workbench USER: User access to Certificate Manager	✓ SHOW USER	✓ SHOW USER	✓ SHOW	✗	✓ SHOW	✗
Certificate Manager API Use the Certificate Manager API	✓ USER	✓ USER	✓ USER	✗	✓ SHOW	✗

© 2026 Tanium Inc. All Rights Reserved

Certificate Manager solution permissions (continued)

Permission	Certificate Manager Operator[1]	Certificate Manager User[1]	Certificate Manager Read Only User[1]	Certificate Manager Package Author	Certificate Manager Configuration Manager[1]	Certificate Manager Configuration Approver[1]
Certificate Manager Audit Read the audit log available through the Certificate Manager API	✓ READ	✗	✗	✗	✗	✗
Certificate Manager Certificate View or manage the certificate inventory	✓ READ WRITE	✓ READ	✓ READ	✗	✗	✗
Certificate Manager Certificate Operation View or manage certificate operations and details	✓ READ WRITE	✓ READ	✓ READ	✗	✗	✗
Certificate Manager Certificate Replacement View or manage certificate replacements	✓ READ WRITE	✓ READ	✓ READ	✗	✗	✗
Certificate Manager Config View, update, or distribute the Certificate Manager configuration, and manage profiles APPROVE: approve proposed Endpoint Configuration changes for Certificate Manager	✓ READ WRITE EXECUTE	✓ READ	✓ READ	✗	✓ READ WRITE EXECUTE	✓ APPROVE

© 2026 Tanium Inc. All Rights Reserved

Certificate Manager solution permissions (continued)

Permission	Certificate Manager Operator[1]	Certificate Manager User[1]	Certificate Manager Read Only User[1]	Certificate Manager Package Author	Certificate Manager Configuration Manager[1]	Certificate Manager Configuration Approver[1]
Certificate Manager Package Author packages to unpack and configure replacement certificates on endpoints	✗	✗	✗	✓ AUTHOR	✗	✗
Certificate Manager Read Only Read-only access to the Certificate Manager module	✓ USER	✓ USER	✓ USER	✗	✗	✗

[1] The permissions for this role provide solution permissions for other solutions. To view the provided permissions, see Tanium Console User Guide: View effective role permissions.

Certificate Manager administration and platform content permissions

Permission	Permission Type	Certificate Manager Operator	Certificate Manager User	Certificate Manager Read Only User	Certificate Manager Package Author	Certificate Manager Configuration Manager	Certificate Manager Configuration Approver
Action	Platform Content	✓ READ WRITE	✓ READ WRITE	✗	✗	✗	✗
Action Group	Administration	✓ READ	✓ READ	✓ READ	✗	✓ READ	✗
Dashboard	Platform Content	✓ READ	✓ READ	✓ READ	✗	✗	✗
Filter Group	Platform Content	✓ READ	✓ READ	✓ READ	✗	✓ READ	✗
Own Action	Platform Content	✓ READ	✓ READ	✗	✗	✗	✗

© 2026 Tanium Inc. All Rights Reserved

Certificate Manager administration and platform content permissions (continued)

Permission	Permission Type	Certificate Manager Operator	Certificate Manager User	Certificate Manager Read Only User	Certificate Manager Package Author	Certificate Manager Configuration Manager	Certificate Manager Configuration Approver
Package	Platform Content	✓ READ	✓ READ	✓ READ	✓ READ WRITE	✗	✗
Plugin	Platform Content	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✗	✓ READ EXECUTE	✓ READ EXECUTE
Saved Question	Platform Content	✓ READ	✓ READ	✓ READ	✗	✗	✗
Sensor	Platform Content	✓ READ	✓ READ	✓ READ	✗	✓ READ	✗

To view the content sets to which the platform content permissions apply, see Tanium Console User Guide: View effective role permissions.

© 2026 Tanium Inc. All Rights Reserved

Installing Certificate Manager

Before you begin

- Read the release notes.
- Review the Certificate Manager requirements on page 19.
- Assign the correct roles to users for Certificate Manager. Review the User role requirements on page 22.
    - To import the Certificate Manager solution, you must be assigned the Administrator reserved role.
    - To configure the Certificate Manager action group, you must be assigned the Administrator reserved role, Content Administrator reserved role, or a role that has the **Action Group write** permission.

Import Certificate Manager with default settings

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

When you import Certificate Manager, the following default settings are configured:

Tanium Certificate Manager default settings

Setting	Default value
Action group	• Restricted targeting disabled (default): `All Computers` computer group • Restricted targeting enabled: `No Computers` computer group NOTE If the action group was already created in a previous version of Certificate Manager, the action group is not updated.
Scheduled action for default audit settings	• Maximum Audit Age: 1 Day • Port Scan: enabled • Log Verbosity: Info • Distribute over time: 15 Minutes

To import Certificate Manager and configure default settings, see Tanium Console User Guide: Import all modules and services. After the import, verify that the correct version is installed. For more information, see Verify Certificate Manager version on page 28.

© 2026 Tanium Inc. All Rights Reserved

Import Certificate Manager with custom settings

To import Certificate Manager without automatically configuring default settings, be sure to clear the **Apply All Tanium recommended configurations** checkbox while performing the steps in Tanium Console User Guide: Import or update specific solutions. After the import, verify that the correct version is installed: see Verify Certificate Manager version on page 28.

To configure the Certificate Manager action group, see Configure the Certificate Manager action group on page 31.

To configure the Certificate Manager audit settings, see Configure audit settings on page 33.

Manage solution dependencies

Other Tanium solutions are required for Certificate Manager to function (required dependencies) or for specific Certificate Manager features to work (feature-specific dependencies). For more information, see Solution dependencies on page 19.

Upgrade Certificate Manager

For the steps to upgrade Certificate Manager, see Tanium Console User Guide: Managing Tanium solutions. After the upgrade, verify that the correct version is installed. For more information, see Verify Certificate Manager version on page 28.

IMPORTANT

In Certificate Manager 1.17 and later, port scanning is disabled by default. Prior to this release, the default setting was to enable port scanning. If you disabled port scanning and then re-enabled port scanning prior to this release, port scanning remains enabled after upgrade. If you never changed port scanning options and used the default option of enabled port scans, the default changes to disabled port scans upon upgrade and a **Port scanning is disabled** warning banner appears on the Certificate Manager **Overview** page. To enable port scanning, either follow the link that appears in the warning banner or see Configure audit settings on page 33.

IMPORTANT

If you are upgrading from Certificate Manager 1.10 or earlier, the following customizations are not migrated when you upgrade to Certificate Manager 1.11 or later:

- Certificate exclusions: To reconfigure any custom certificate exclusions, see Configure exclusion list on page 34.
- Authorized certificate authorities (CAs): To reconfigure any custom CAs, see Configure certificate authorities on page 35.
- Scheduled actions: Certificate Manager 1.11 now manages scheduled actions through the service. To prevent Certificate Manager audits from running more often than intended, delete any previously created schedule actions after you upgrade Certificate Manager.

Verify Certificate Manager version

After you import Certificate Manager, verify that the correct version is installed:

© 2026 Tanium Inc. All Rights Reserved

1. Refresh your browser.
2. From the Main menu, go to **Administration > Configuration > Solutions**.
3. In the **Modules** section, verify that the **Certificate Manager <*version*>** reflects the version that you installed.

© 2026 Tanium Inc. All Rights Reserved

Configuring Certificate Manager

Configure Tanium Certificate Manager settings to specify your administrative and security needs. Configurations include assigning user roles, modifying certificate replacement settings, and designating certificate authorities.

You must enable and configure certain features.

Install and configure Tanium Endpoint Configuration

Manage solution configurations with Tanium Endpoint Configuration

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

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



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

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



For information about how to install Endpoint Configuration, see Tanium Endpoint Configuration User Guide: Installing Endpoint Configuration.

Optionally, you can use Endpoint Configuration to require approval of configuration changes. When configuration approvals are enabled, Endpoint Configuration does not deploy a configuration change to endpoints until a user with approval permission

© 2026 Tanium Inc. All Rights Reserved

approves the change. For information about the roles and permissions that are required to approve configuration changes for Certificate Manager, see User role requirements on page 22. For more information about how to enable and use configuration approvals in Endpoint Configuration, see Tanium Endpoint Configuration User Guide: Managing approvals.

IMPORTANT

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

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

If you enabled configuration approvals, the following configuration changes must be approved in Endpoint Configuration before they deploy to Tanium Client managed endpoints:

- Deploying Certificate Manager tools to endpoints
- User-initiated actions, such as updating Certificate Manager audit settings, certificate exclusions, certificate authorities, and approved ciphers, and uninstalling Certificate Manager

Configure Certificate Manager

Configure the Certificate Manager action group

Importing the Certificate Manager module automatically creates an action group to target specific endpoints. If you did not use automatic configuration or you enabled restricted targeting when you imported Certificate Manager, the action group targets **No Computers**.

If you used automatic configuration and restricted targeting was disabled when you imported Certificate Manager, configuring the Certificate Manager action group is optional.

Select the computer groups to include in the Certificate Manager action group.

BEST PRACTICE

Clear the selection for **No Computers** and make sure that all operating systems that are supported by Certificate Manager are included in the Certificate Manager action group.

1. From the Main menu, go to **Administration > Actions > Action Groups**.
2. Click **Tanium Certificate Manager**.
3. Select the computer groups that you want to include in the action group and click **Save**.
   If you select multiple computer groups, choose an operator (AND or OR) to combine the groups.

Set up Certificate Manager users

You can use the following set of predefined user roles to set up Certificate Manager users.

© 2026 Tanium Inc. All Rights Reserved

For more information about assigning specific permissions for each role, see User role requirements on page 22.

For more information about assigning user roles, see Tanium Core Platform User Guide: Manage role assignments for a user.

Certificate Manager Operator

Assign the **Certificate Manager Operator** role to users who manage the deployment of Certificate Manager functionality to endpoints.
This role can perform the following tasks:

- Update and distribute the Certificate Manager configuration.
- View Certificate Manager reports and dashboard in Tanium Reporting.
- View and manage the certificate inventory.
- Deploy Certificate Manager packages.

Certificate Manager Configuration Manager

Assign the **Certificate Manager Configuration Manager** role to users who manage the deployment of Certificate Manager functionality to endpoints.
This role can perform the following tasks:

- View the Certificate Manager configuration.
- Create, manage, and deploy Certificate Manager profiles.

Certificate Manager User

Assign the **Certificate Manager User** role to users who manage the deployment of Certificate Manager functionality to endpoints .
This role can perform the following tasks:

- View the Certificate Manager configuration.
- View Certificate Manager reports and dashboard in Tanium Reporting.
- Deploy Certificate Manager packages.
- View the certificate inventory.

Certificate Manager Read Only User

Assign the **Certificate Manager Read Only User** role to users who need visibility into Certificate Manager data.
This role can perform the following tasks:

- View Certificate Manager reports and dashboard in Tanium Reporting.
- View the certificate inventory.

© 2026 Tanium Inc. All Rights Reserved

Certificate Manager Package Author

Assign the **Certificate Manager Package Author** role to users who need to create packages to configure replacement certificates on endpoints.

Certificate Manager Configuration Approver

Assign the **Certificate Manager Configuration Approver** role to users who need to approve Certificate Manager configuration changes in Tanium Endpoint Configuration.
This role can view and approve the proposed Certificate Manager configuration changes in Tanium Endpoint Configuration.

In addition to the Certificate Manager roles, users must also have sufficient management rights, such as **All Computers**. Otherwise, saved configurations are deployed only to the specific management rights group for the user.



Do not assign the **Certificate Manager Service Account** role to users. This role is for internal purposes only.

Configure audit settings



If you have endpoints with Toolset versions earlier than 2.20.86, complete the following steps. If you have endpoints with Toolset 2.20.86 or later, you configure audit settings when you add a profile. For more information, see Create a profile on page 66.

You can configure certificate audit settings for all endpoints.

1. From the Main menu, go to **Modules > Certificate Manager > Overview** and then click Settings.
2. Enter a **Maximum Audit Age** value. The default is 1 day.
3. (Optional) If you want increased details around listening ports and ciphers, select the **Enable Listening Port Scan** option.
4. Select a **Log Verbosity**. The available options are **Info**, **Warning**, **Error**, and **Fatal**.
5. (Optional) If you do not need to prevent spikes in network traffic or other resource consumption, clear the **Distribute over time** option and then click **Save**. The default is set to distribute over 15 minutes.

© 2026 Tanium Inc. All Rights Reserved

Configure exclusion list

IMPORTANT

If you have endpoints with Toolset versions earlier than 2.20.86, complete the following steps. If you have endpoints with Toolset 2.20.86 or later, you configure exclusions when you add a profile. For more information, see Create a profile on page 66.

You can specify a list of certificates that you want to exclude from auditing in Certificate Manager.

NOTE

Certificates that are found on listening ports cannot be excluded by the exclusion list. Only certificates that are found by file or certificate store are excluded by the exclusion list. For more information about certificate discovery methods, see Certificate sources on page 12.

1. From the Main menu, go to **Modules > Certificate Manager > Overview**, click Settings, and then click the **Exclusion List** tab.
2. Enter a certificate by name or fingerprint, or select one from the list, click **Add Exclusion**, enter an optional note, and then click **Submit**.

   TIP

   You can select more than one certificate to exclude. If you select more than one certificate, the name of the button changes to **Add Exclusions**.
3. To sort the list, click on any of the column names. The available options are **Exclusion**, **Common Name**, **Subject**, **Issuer**, **Expiration**, and **SHA-256 Fingerprint**.
4. To filter the list by status, select the corresponding toggle.

Exclusion status

Status	Description
All	All statuses.
Deployed	Exclusion has been deployed to endpoints.
Never Deployed	Exclusion has not been deployed to endpoints.
Changed	Exclusion has been previously deployed to endpoints but now has changes that need to be deployed to endpoints.
Pending Approval	(Only on-premises) Exclusion will not be deployed to endpoints until a user with approval permission approves the change. For more information about enabling and using configuration approvals in Endpoint Configuration, see Tanium Endpoint Configuration User Guide: Managing approvals.

© 2026 Tanium Inc. All Rights Reserved

5. To view all active and inactive certificate exclusions, select **All** from the **Exclusion** options. The available options are **All**, **Active**, and **Inactive**.

   a. To deactivate an active exclusion, select it and then click **Deactivate Exclusion**.

   > TIP You can also select multiple active exclusions and then click **Deactivate Exclusions**.

   b. To activate an inactive exclusion, select it and then click **Activate Exclusion**.

   > TIP You can also select multiple inactive exclusions and then click **Activate Exclusions**.

   c. To add or edit a note for a certificate, select it and then click **Edit Note**.

   d. If you no longer need to exclude a specific certificate, select it and then click Delete .

   > TIP You can also select multiple certificates and then click Delete .

Configure certificate authorities

If your organization requires that you use a particular set of certificate authorities (CAs), such as one approved external provider and one or more internal public key infrastructures (PKIs), you can use Certificate Manager to designate these certificates as authorized certificates.

> NOTE The full certificate chain, which includes the root and all intermediate certificates, must be imported in the Certificate Authorities tab of the Certificate Manager settings. Certificate Manager does not evaluate the chain for at-rest certificates.

Obtain the certificate chain for your external CA using OpenSSL

1. Use OpenSSL to get the certificate chain that is used by a known good site.

```
openssl s_client -connect tanium.com:443 -showcerts
```

2. Review the response to locate the root and intermediate certificates.

   Click here to view an example response.

   > NOTE The example response was shortened to not display the entire certificate contents.

© 2026 Tanium Inc. All Rights Reserved

```
CONNECTED(00000003)
depth=2 C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root CA
verify return:1
depth=1 C = US, O = DigiCert Inc, CN = DigiCert TLS RSA SHA256 2020 CA1
verify return:1
depth=0 C = US, ST = California, L = Emeryville, O = Tanium Inc., CN = *.tanium.com
verify return:1
write W BLOCK
---
Certificate chain
0 s:/C=US/ST=California/L=Emeryville/O=Tanium Inc./CN=*.tanium.com
i:/C=US/O=DigiCert Inc/CN=DigiCert TLS RSA SHA256 2020 CA1
-----BEGIN CERTIFICATE-----
MIIGtzCCBZ+gAwIBAgIQCEq/Uf85v78s/1CqKhKjqjANBgkqhkiG9w0BAQsFADBP
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMSkwJwYDVQQDEyBE
...
rij6WpCEkEin0yZBaxYmqpv18XKzoiaY9AhrO0p0QorbQrGKH87zkR+n6Cn8lCKC
ry4i8sJRuzV7hTWyjylr19b/iHu79bGIpsDrG3Huikm0of076bSzSWEpUQ0tH7XY
XnShELTAhXGlxPgJX4clpMrG5SKlr0S0FVHU7nZ6GMN47Kd3GuvIfX7NnQ==
-----END CERTIFICATE-----
1 s:/C=US/O=DigiCert Inc/CN=DigiCert TLS RSA SHA256 2020 CA1
i:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root CA
-----BEGIN CERTIFICATE-----
MIIEvjCCA6agAwIBAgIQBtjZBNVYQ0b2ii+nVCJ+xDANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
...
EXffPgK2fPOre3qGNm+499iTcc+G33Mw+nur7SpZyEKEOxEXGlLzyQ4UfaJbcme6
ce1XR2bFuAJKZTRei9AqPCCcUZlM51Ke92sRKw2Sfh3oius2FkOH6ipjv3U/697E
A7sKPPcw7+uvTPyLNhBzPvOk
-----END CERTIFICATE-----
---
Server certificate
subject=/C=US/ST=California/L=Emeryville/O=Tanium Inc./CN=*.tanium.com
issuer=/C=US/O=DigiCert Inc/CN=DigiCert TLS RSA SHA256 2020 CA1
---
No client certificate CA names sent
Server Temp Key: ECDH, X25519, 253 bits
---
SSL handshake has read 3436 bytes and written 367 bytes
---
New, TLSv1/SSLv3, Cipher is AEAD-AES256-GCM-SHA384
```

© 2026 Tanium Inc. All Rights Reserved

```
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
       Protocol  : TLSv1.3
       Cipher    : AEAD-AES256-GCM-SHA384
       Session-ID:
       Session-ID-ctx:
       Master-Key:
       Start Time: 1675375403
       Timeout   : 7200 (sec)
       Verify return code: 0 (ok)
---
closed
```

3. Copy the first certificate, including the BEGIN/END markers and save the contents to a file that is named `trusted_intermediate_certificate_authorities.pem`.
4. Copy the second certificate, including the BEGIN/END markers and save the contents to a file that is named `trusted_root_certificate_authorities.pem`.

Repeat these steps if you have multiple approved CAs and append each certificate to the two PEM files.

Obtain your internal CA certificates

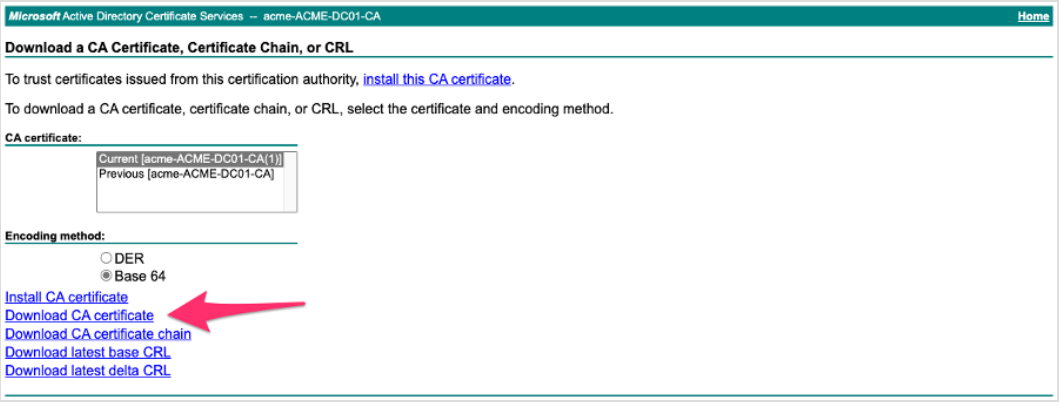
In many organizations, any internal PKI is implemented using Microsoft's AD-integrated CA, but other solutions are also available.

1. Sign in to your CA.

For Microsoft, the CA is likely on a domain controller at a URL that is similar to `https://acme-dc01.acme.lab/CertSrv`.

© 2026 Tanium Inc. All Rights Reserved

2. Click **Download CA certificate**.



A `certnew.crt` file downloads to your computer.

3. Append the contents of the `certnew.crt` file to your `trusted_root_certificate_authorities.pem` file.

> NOTE
>
> If you did not create the two PEM files as described in Obtain the certificate chain for your external CA using OpenSSL on page 35, you can rename the `certnew.crt` file to `trusted_root_certificate_authorities.pem` and create a blank `trusted_intermediate_certificate_authorities.pem` file.

Configure and manage authorized CAs

> IMPORTANT
>
> If you have endpoints with Toolset versions earlier than 2.20.86, complete the following steps. If you have endpoints with Toolset 2.20.86 or later, you add certificate authorities when you add a profile. For more information, see Create a profile on page 66.

Designate certificate authorities as authorized on the **Certificate Authorities** page. Also, confirm that you have enabled the listening port scan on the Settings **Audit Settings** page, so that Certificate Manager can find the certificate authorities during a listening service scan. For more information, see Configure audit settings on page 33.

On the **Certificate Inventory** page, you can review the authorized certificate authorities found by Certificate Manager. For more information, see View certificate inventory on page 49.

1. From the Main menu, go to **Modules > Certificate Manager > Overview**, click Settings, and then click the **Certificate Authorities** tab.
2. To manually add a CA, click **Add**, enter a PEM-encoded certificate and an optional description, and then click **Submit**.
3. To import a CA, click **Import**, click **Browse for Files** to select a PEM or DER encoded certificate file, and then click **Submit**.

© 2026 Tanium Inc. All Rights Reserved

4. To view all active and inactive CAs, select **All** from the **Authority** options. The available options are **All**, **Active**, and **Inactive**.

   a. To deactivate an active CA, select the CA and then click **Deactivate Authority**.

   > TIP You can also select multiple active CAs and then click **Deactivate Authorities**.

   b. To activate an inactive CA, select the CA and then click **Activate Authority**.

   > TIP You can also select multiple inactive CAs and then click **Activate Authorities**.

   c. To edit the certificate type or description for a CA, select the CA and then click **Edit Authority**.

   d. To delete a CA, select the CA and then click Delete .

   > TIP You can also select multiple CAs and then click Delete .

Configure approved ciphers

> IMPORTANT If you have endpoints with Toolset versions earlier than 2.20.86, complete the following steps. If you have endpoints with Toolset 2.20.86 or later, you add configure ciphers when you add a profile. For more information, see Create a profile on page 66.

Certificate Manager pre-populates the approved cipher suites based on Internet Assigned Numbers Authority (IANA) recommendations. Approval status appears in Certificate Manager dashboards and reports.

The following ciphers are approved by default in Certificate Manager:

- TLS_DHE_PSK_WITH_AES_128_CCM
- TLS_DHE_PSK_WITH_AES_256_CCM
- TLS_DHE_PSK_WITH_AES_128_GCM_SHA256
- TLS_DHE_PSK_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_CCM
- TLS_DHE_RSA_WITH_AES_256_CCM
- TLS_ECDHE_PSK_WITH_AES_128_CCM_SHA256
- TLS_ECDHE_PSK_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_PSK_WITH_AES_256_GCM_SHA384

If your organization has a policy for acceptable cipher suites, you can add or remove approvals based on your organization policy.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules > Certificate Manager > Overview**, click Settings, and then click the **Approved Ciphers** tab.
2. To filter the list by status, select the corresponding toggle.

   Cipher suite status

Status	Description
All	All statuses.
Deployed	Cipher suite has been deployed to endpoints.
Never Deployed	Cipher suite has not been deployed to endpoints.
Changed	Cipher suite has been previously deployed to endpoints but now has changes that need to be deployed to endpoints.
Pending Approval	(Only on-premises) Cipher suite will not be deployed to endpoints until a user with approval permission approves the change. For more information about enabling and using configuration approvals in Endpoint Configuration, see Tanium Endpoint Configuration User Guide: Managing approvals.

3. To view the list by approval status, select **Approved** or **Not Approved** from the **Approval Status** options. The available options are **All**, **Approved**, and **Not Approved**.
   a. To add an approval for a cipher suite, select one with a **Not Approved** status and then click **Add Approval**.

   TIP You can also select multiple cipher suites with a **Not Approved** status and then click **Add Approvals**.

   b. To remove an approval for a cipher suite, select one with an **Approved** status and then click **Remove Approval**.

   TIP You can also select multiple cipher suites with an **Approved** status and then click **Remove Approvals**.

Configure certificate replacement settings

You can modify settings that apply to all certificate replacement requests. For more information, see Replace certificate on page 53.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules > Certificate Manager > Overview**, click Settings, and then click the **Replacement Settings** tab.
2. Edit any of the following settings:

Certificate replacement settings

Setting	Default Value	Description
Finalize after	14 days	The amount of time after the renewed certificates has been uploaded before the certificate deployment is automatically finalized. Finalizing a deployment removes the enciphered private key from secure storage and prevents further deployments of the certificate replacement. You can also manually finalize the deployment during the process to replace a certificate.
Remove staged jobs after	14 days	The amount of time after the replacement certificate and enciphered private key have been staged on an endpoint before they are removed. For best results, this value should greater than or equal to the **Finalize after** value.

3. When finished, click **Save**.

Certificate Manager uses the new finalization timeframe for future replacement requests. Any existing requests continue to use the timeframe that was in effect when the certificate replacement workflow was initiated for automatic finalization.

Configure certificate port exceptions

IMPORTANT

The following instructions only apply to endpoints with Toolset versions earlier than 2.20.86. If you have endpoints with Toolset 2.20.86 or later, you add configure certificate port exceptions when you add a profile. For more information, see Create a profile on page 66.

You can configure port exclusions if you want Certificate Manager to ignore server certificates on a specific listening port.

You can add or delete port exclusions by deploying the following packages:

- **Certificate Audit Add Port Exclusions [Non-Windows]**
- **Certificate Audit Add Port Exclusions [Windows]**
- **Certificate Audit Delete Port Exclusions [Non-Windows]**
- **Certificate Audit Delete Port Exclusions [Windows]**

Add port exclusions

1. From the Main menu, go to **Administration > Content > Packages** and search for `Certificate Audit`.
2. Select the checkbox for **Certificate Audit Add Port Exclusions [Non-Windows]** or **Certificate Audit Add Port Exclusions [Windows]** and then click **Deploy Action**.
3. In the **Deployment Package** section, enter the **Ports to Exclude**.

© 2026 Tanium Inc. All Rights Reserved

4. In the **Targeting Criteria** section, choose an option to target one or more endpoints and then click **Show Preview to Continue**.

   TIP

   To add the port exclusion for all endpoints, select **Tanium Certificate Manager** for **Action Group**. For more information, see Configure the Certificate Manager action group on page 31.

5. Verify the list of targeted endpoints and then click **Deploy Action**.

Delete port exclusions

1. From the Main menu, go to **Administration > Content > Packages** and search for `Certificate Audit`.
2. Select the checkbox for **Certificate Audit Delete Port Exclusions [Non-Windows]** or **Certificate Audit Delete Port Exclusions [Windows]** and then click **Deploy Action**.
3. In the **Deployment Package** section, enter the **Ports to no longer exclude**.
4. In the **Targeting Criteria** section, choose an option to target one or more endpoints and then click **Show Preview to Continue**.

   TIP

   To delete the port exclusion for all endpoints, select **Tanium Certificate Manager** for **Action Group**. For more information, see Configure the Certificate Manager action group on page 31.

5. Verify the list of targeted endpoints and then click **Deploy Action**.

NOTE

Although the **Certificate Audit Port Exclusions** sensor displays the updated exclusions, the port exclusions do not take effect until after the next certificate audit runs. You can either Deploy a certificate audit package on page 42 manually, or wait until the next **Certificate Audit [Non-Windows]** and **Certificate Audit [Windows]** scheduled actions run.

Deploy a certificate audit package

IMPORTANT

The following instructions only apply to endpoints with Toolset versions earlier than 2.20.86. If you have endpoints with Toolset 2.20.86 or later, you deploy a certificate audit when you add and deploy a profile. For more information, see Create a profile on page 66.

By default, certificate audits are scheduled to run daily. If you need to refresh a certificate audit on one or more endpoints, you can deploy a certificate audit package.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration > Content > Packages** and search for `Certificate Audit`.
2. Select the checkbox for **Certificate Audit [Non-Windows]** or **Certificate Audit [Windows]** and then click **Deploy Action**.
3. In the **Deployment Package** section, configure the following details.
   a. (Optional) If you do not need increased details around listening ports and ciphers, clear the **Enable Listen Port Scan** option.

   > NOTE
   > Listen port scans are not supported on endpoints with Windows Server 2008 R2 or earlier, and Windows 7 or earlier. If you have endpoints with these operating systems, either clear the **Enable Listen Port Scan** option or remove those endpoints from the Certificate Manager action group. For information about how to configure the Certificate Manager action group, see Configure the Certificate Manager action group on page 31.

   b. Select a **Log Level**.
4. In the **Targeting Criteria** section, choose an option to target one or more endpoints and then click **Show Preview to Continue**.

   > TIP
   > To run the certificate audit on all endpoints, select **Tanium Certificate Manager** for **Action Group**. For more information, see Configure the Certificate Manager action group on page 31.
5. Verify the list of targeted endpoints and then click **Deploy Action**.

Customize Guide observations

By default, you can view Guide observations (alerts) for certificates that are about to expire or have expired on endpoints using profiles. You can customize these observations to be more specific to your organizational needs and to include endpoints not using profiles.

> NOTE
> Observations are a Guide notification category. Observations provide an opportunity to review data and determine the root cause of a situation.

Before you begin

- Ensure that you have the permissions needed to view observations. For more information, see User role requirements on page 22
- Ensure that you have the permissions needed to edit notifications. For more information, see Tanium Guide User Guide: User role requirements.

© 2026 Tanium Inc. All Rights Reserved

Customize criteria for Certificate Manager-specific observations

On the Guide **Administration** page, customize the parameters for the Certificate Manager-specific observations. For general instructions on customizing a notification, see Tanium Guide User Guide: Configure notification display.

Consider the following:

- To view observations only for certificates that you can replace with Certificate Manager, select **Yes** for **Filter by Private Key Available**.
- To reduce the frequency of **Review Certificates Expiring Soon** observations, increase the **Filter by Minimum Lifetime** days. You might not need to review certificates with short lifetimes because they might be automatically managed by another tool.
- To view **Review Certificates Expiring Soon** observations for endpoints not using profiles, set the **Filter by Minimum Lifetime** days to `0`.

© 2026 Tanium Inc. All Rights Reserved

Managing certificates

Certificate Manager uses reports from Tanium Reporting. From the Certificate Manager **Overview** page, you can use Certificate Manager data to:

- Find expired or expiring certificates
- Identify weak cryptographic algorithms and key lengths
- View self-signed and unauthorized CA certificates
- Send certificate data using the **Tanium Reporting (Source Data)** source in Tanium Connect

View the Certificate Manager dashboard in Tanium Reporting

The Certificate Manager dashboard in Tanium Reporting includes three sections. The **Overview** section shows a high-level view of the number of certificates across your Tanium Client managed endpoints. The **Listening SSL/TLS Services Certificate and Cipher Inventory** section shows certificates that are currently being served, while the **All Certificates** section shows all certificates that are being referenced.

1. From the Main menu, go to **Data > Dashboards** and select the **Certificate Manager** label.
2. To view the dashboard, click **Certificate Manager**.

Click the name of a chart panel to open the report that supplies the data to that chart, or click any data point on a chart to view the data in the report. For more information, see Tanium Reporting User Guide: Working with dashboards.

You can also go to **Modules > Certificate Manager > Overview** to view the dashboard and reports.

View expired certificates

1. From the Main menu, go to **Modules > Certificate Manager > Overview**.
2. In the **All Certificates** section, click **Expired Certificates**.

This data comes from the **Certificate Manager - Expired Certificates** report in Tanium Reporting.

View expiring certificates

View listening service certificates that are expiring in 30 days

1. From the Main menu, go to **Modules > Certificate Manager > Overview**.
2. In the **Listening SSL/TLS Services Certificate and Cipher Inventory** section, click **Listening Service Certificates Expiring in 30 Days** to view the list of expiring certificates.

© 2026 Tanium Inc. All Rights Reserved

This data comes from the **Certificate Manager - Certificates Expiring within 30 Days** report in Tanium Reporting.

To send a recurring email with the list of listening service certificates that are expiring in 30 days, Email a report of expiring certificates with Tanium Connect on page 46 using the **Certificate Manager - Listening Service Certificates Expiring within 30 Days** report.

View all certificates that are expiring in 30 days

1. From the Main menu, go to **Modules > Certificate Manager > Overview**.
2. In the **All Certificates** section, click **Expiring within 30 Days** to view the list of expiring certificates.

This data comes from the **Certificate Manager - Certificates Expiring within 30 Days** report in Tanium Reporting.

To send a recurring email with the list of all certificates that are expiring in 30 days, Email a report of expiring certificates with Tanium Connect on page 46 using the **Certificate Manager - Certificates Expiring within 30 Days** report.

Email a report of expiring certificates with Tanium Connect

Before you begin

Ensure that you have Tanium Connect 5.9.65 or later installed.

Create a connection

1. From the Main menu, go to **Modules > Connect > Connections** and then click **Create Connection**.
2. In the **General Information** section, provide a name and optional description for the connection.
3. In the **Configuration** section, configure the source and destination.
   a. For **Source**, select **Tanium Reporting (Source Data)**.
   b. For **Report**, select one of the following reports:
      - **Certificate Manager - Listening Service Certificates Expiring within 30 Days**
      - **Certificate Manager - Certificates Expiring within 30 Days**
   c. For **Destination**, select **Email** and then provide the required information. For more information about configuring email destinations, see Tanium Connect User Guide: Configuring SMTP email destinations.
4. In the **Configure Output** section, select the **Format**.
5. In the **Schedule** section, select **Enable Schedule** to configure schedule preferences, and then click **Save**.



Schedule this connection to run at least weekly.

For more information, see Tanium Reporting User Guide: Export reports through Tanium Connect.

© 2026 Tanium Inc. All Rights Reserved

View short keys

View listening service certificates that use short keys

1. From the Main menu, go to **Modules > Certificate Manager > Overview**.
2. In the **Listening SSL/TLS Services Certificate and Cipher Inventory** section, click **Listening Service Short Keys** to view the EC certificates that use a **Public Key Bit Size** less than 256 or RSA certificates that use a **Public Key Bit Size** less than 2048.

This data comes from the **Certificate Manager - Listening Service Short Keys** report in Tanium Reporting.

View all certificates that use short keys

1. From the Main menu, go to **Modules > Certificate Manager > Overview**.
2. In the **All Certificates** section, click **Total Short Keys** to view the EC certificates that use a **Public Key Bit Size** less than 256 or RSA certificates that use a **Public Key Bit Size** less than 2048.

This data comes from the **Certificate Manager - Short Keys** report in Tanium Reporting.

View weak signatures

View listening service certificates that use weak signatures

1. From the Main menu, go to **Modules > Certificate Manager > Overview**.
2. In the **Listening SSL/TLS Services Certificate and Cipher Inventory** section, click **Listening Service Weak Signature Hash Algorithms** to view the certificates that use the sha1 or md5 **Signature Hash Algorithm**.

This data comes from the **Certificate Manager - Listening Service Weak Signatures** report in Tanium Reporting.

View all certificates that use weak signatures

1. From the Main menu, go to **Modules > Certificate Manager > Overview**.
2. In the **All Certificates** section, click **Certificate Manager - Weak Signatures Hash Algorithms** to view the certificates that use the sha1 or md5 **Signature Hash Algorithm**.

This data comes from the **Certificate Manager - Weak Signatures** report in Tanium Reporting.

View wildcard certificates

View listening service certificates that use a wildcard subject

1. From the Main menu, go to **Modules > Certificate Manager > Overview**.
2. In the **Listening SSL/TLS Services Certificate and Cipher Inventory** section, click **Listening Service with Wildcard Certificates** to view the certificates that use a wildcard subject.

© 2026 Tanium Inc. All Rights Reserved

View all certificates that use a wildcard subject

1. From the Main menu, go to **Modules > Certificate Manager > Overview**.
2. In the **All Certificates** section, click **Wildcard Certificates** to view the certificates that use a wildcard subject.

This data comes from the **Certificate Manager - Wildcard Certificates** report in Tanium Reporting.

View self-signed certificates

1. From the Main menu, go to **Modules > Certificate Manager > Overview**.
2. In the **Listening SSL/TLS Services Certificate and Cipher Inventory** section, click **Self Signed** in the **Listening Service Certificate Authorized CA Status** panel.

This data comes from the **Certificate Manager - Listening Service SSL Certificate Details** report in Tanium Reporting.

View unauthorized certificates

Any certificates that are not configured as authorized certificates appear as **Unauthorized**.

Tip: To add authorized certificates, see Configure and manage authorized CAs on page 38.

1. From the Main menu, go to **Modules > Certificate Manager > Overview**.
2. In the **Listening SSL/TLS Services Certificate and Cipher Inventory** section, click **False** in the **Listening Service Certificate Authorized CA Status** panel.

This data comes from the **Certificate Manager - Listening Service SSL Certificate Details** report in Tanium Reporting.

After you review the list of unauthorized certificates, you can Configure certificate authorities on page 35 or Configure exclusion list on page 34.

Prepare for post-quantum cryptography

Certificates that use certain encryption algorithms are more likely to be compromised by future advances in quantum computer capabilities. Certificate Manager does not specifically scan for post-quantum cryptographic algorithms, but the **Certificate Manager - Listening Service Cipher Suite Details** report includes a **Cipher Suite** column that shows the algorithm and key length. This information is used by Certificate Manager to provide the **Cipher Approval Status** ratings of **Approved** or **Not Approved**.

For more information, see The White House: Memo on Migrating to Post-Quantum Cryptography.

As suggested in the White House memo, analyzing quantum computer vulnerability exposure starts with building a comprehensive, real-time inventory of all cryptographic algorithms and ciphers in use within the environment.

© 2026 Tanium Inc. All Rights Reserved

View listening services accepting unapproved ciphers

1. From the Main menu, go to **Modules > Certificate Manager > Overview**.
2. In the **Listening SSL/TLS Services Certificate and Cipher Inventory** section, click **Listening Services Accepting Unapproved Ciphers** to view the ports that are accepting unapproved ciphers.

This data comes from the **Certificate Manager - Listening Services Accepting Unapproved Ciphers** report in Tanium Reporting.

View listening service certificates by approval status

1. From the Main menu, go to **Modules > Certificate Manager > Overview**.
2. In the **Listening SSL/TLS Services Certificate and Cipher Inventory** section, click **Listening Service Cipher Inventory** to view the certificates by cipher approval status.

This data comes from the **Certificate Manager - Listening Service Cipher Suite Details** report in Tanium Reporting.

View certificate inventory

View all certificates found on endpoints by Certificate Manager.

To identify the certificates from endpoints that are not using profiles, ask the following question in Interact: `Get Certificate Details from all machines with Certificate Manager - Client Extension for Certificate Audits contains No`

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules > Certificate Manager > Certificate Inventory**.
2. View the certificates. The table contains the following columns.

Certificate Inventory columns

Column	Description
SHA-256 Fingerprint	Unique string of digits that identifies the certificate, generated with the SHA-256 algorithm
SHA-1 Fingerprint	Unique string of digits that identifies the certificate, generated with the SHA-1 algorithm
Serial Number	Serial number of certificate
Subject	Entity identified by the certificate
Issuer	Entity that issued the certificate
Authorized	A certificate is authorized when the following conditions are met: • You enable the listening port scan on the Settings > **Audit Settings** page or in a profile. • Certificate Manager finds the certificate during a listening service scan. • You add the certificate as an authorized certificate on the Settings > **Certificate Authorities** page or in a profile.
Expiration (UTC)	Expiration date and time (UTC) of the certificate
Days to Expiration	Number of days before expiration
Lifetime	Length of time that the certificate is valid
Service Instances	Number of listening service ports presenting the certificate Each internet protocol is considered a port. For example, if a certificate is found on port 443 for both IPv4 and IPv6, the service instances are 2.
Private Key Available	Yes or No, depending on if Certificate Manager can locate the private key

3. (Optional) Use any filter options to help find a specific certificate if the grid is long. The grid shows only the certificates that match all the filters that you specify.

IMPORTANT

If you enter a number greater than 0 in the **Minimum Lifetime** filter, only certificates found on endpoints using profiles appear on the **Certificate Inventory** page.

© 2026 Tanium Inc. All Rights Reserved

Certificate Inventory search and filter options

Option	Description
Search by text	Enter an alphanumeric string in the **Filter items** field to match text in the **Subject**, **Issuer**, **Authorized**, and **Expiration (UTC)** columns.
Filter by authorization status	For the **Authorized** option, select **All** to show authorized and unauthorized certificates. Select **Yes** to show only authorized certificates, or select **No** to show only unauthorized certificates. Default value is **All**.
Filter by private key available	For the **Private Key Available** filter, select **Yes** to show only certificates for which Certificate Manager can locate its corresponding private key. Select **No** to show only certificates for which Certificate Manager cannot locate its corresponding private key. Default value is **All**.
Filter by listening service	For the **Listening Services** filter, select **Yes** to show only certificates that are used by one or more listening services. Select **No** to only show certificates that are not used by any listening services.
Filter by expiring date	To show active certificates that expire soon, select an option for **Expiring in (Days)**. Available options include **All**, **14** days, **30** days, **60** days, **90** days, and **180** days. Default value is **All**, which shows all expiring certificates regardless of expiration date.
Filter by expired date	To show recently expired certificates, select an option for **Expired (Days)**. Available options include **All**, **14** days, **30** days, **60** days, and **60+** days. Default value is **All**, which shows all expired certificates regardless of expiration date.

4. The following actions are available:

Certificate Inventory actions

Option	Description
View certificate details	In the row of the certificate that you want to view, click Certificate Details. For more information, see View certificate details on page 52.
Export to CSV	To download a copy of Certificate Inventory table as a CSV file, apply any filters, click **Export**, and then select **Export to CSV**. The CSV file includes the table headers and table data. IMPORTANT For certificates that are found on endpoints not using profiles, the `Certificate Manager Inventory - Certificates:Lifetime` value is empty in the CSV file. To view the accurate lifetime values for these certificates, look at the **Certificate Inventory** page.
Download certificate	In the **Actions** column of the row of the certificate that you want to download, select Actions and then click **Download certificate**. For more information, see Download certificate on page 53.
Manage columns	In the header, click Customize Columns. To remove a column, clear the checkbox for the column. To adjust the column order, click and drag the column names.

© 2026 Tanium Inc. All Rights Reserved

Certificate Inventory actions (continued)

Option	Description
Refresh table data	Click Refresh . Any filters that you added apply to the updated results.

View certificate details

To view details for certificates, you must have a role with the **Certificate Manager Certificate read** permission.

1. From the Main menu, go to **Modules > Certificate Manager > Certificate Inventory**.
2. (Optional) Use any search and filter options to help find a specific certificate if the grid is long. For search and filter options, see View certificate inventory on page 49.
3. In the row of the certificate that you want to view, click Certificate Details .
4. The **Details** slide-out panel that appears contains the following sections:

Certificate Details sections

Option	Description
Details	Shows details for the certificate. Details include expiration, issue date, authorization status, fingerprint, subject, and the issuer.
Certificate PEM	Shows the PEM file for the certificate.
On Endpoints By Service	Shows where the certificate is currently in use and the listening services that use the certificate.

5. The following actions are available:

Available actions on the certificate details panel

Option	Description
Copy fingerprint	In the **Details** section, click the **Fingerprint** value to copy the fingerprint to your clipboard.
Initiate certificate replacement	Click **Actions** and then click **Start replacement**. For more information, see Replace certificate on page 53.
Download certificate	Click **Actions** and then click **Download certificate**. For more information, see Download certificate on page 53.

© 2026 Tanium Inc. All Rights Reserved

Available actions on the certificate details panel (continued)

Option	Description
View details for other certificates	Choose from the following: • Use the View Previous Certificate and View Next Certificate controls in the upper right of the **Details** panel to navigate through the details of certificates that appear on the **Certificate Inventory** page. • Close the **Details** panel to return to the **Certificate Inventory** page. From there, click Certificate Details in the row of the certificate that you want to view.
View endpoint details	You can view details for an endpoint in the **On Endpoints By Service** section. Click Endpoint Details to view basic details for the endpoint and then click **View Details** to open the Endpoint Details page in Tanium Reporting. For information about the Endpoint Details page, see Tanium Reporting User Guide: View endpoint details.

Download certificate

To download certificates, you must have a role with the **Certificate Manager Certificate read** permission. If you do not have this permission, the option to download a certificate does not appear.

1. From the Main menu, go to **Modules > Certificate Manager > Certificate Inventory**.
2. (Optional) Use any search and filter options to help find a specific certificate if the grid is long. The grid shows only the certificates that match all the filters that you specify. For more information, see View certificate inventory on page 49.
3. In the **Actions** column of the row of the certificate that you want to download, select Actions and then click **Download certificate**.
4. After the certificate details loads, click **Download**.

The downloaded certificate becomes available for selection in the **Certificate Authorities** section when you create or edit a profile. For more information, see Create a profile on page 66.

Replace certificate

Use Certificate Manager to replace expiring certificates, including wildcard certificates, on endpoints in your environment. Certificates contain a public key that corresponds to a matching private key. Both keys are required for cryptographic operations, such as when a listening service establishes a TLS connection with a client. The private key must be exportable.

NOTE

For Windows certificates, Certificate Manager currently determines if the private key is exportable only after you start the certificate replacement process.

IMPORTANT

Certificate Manager is intended to replace certificates, not to create certificates.

© 2026 Tanium Inc. All Rights Reserved

When you start the process to replace a certificate and you select an endpoint on which to generate a new Certificate Request (CSR), the client extension generates a new private key using the algorithm and key length that you specify. The client extension enciphers the new private key using the old private key. The enciphered private key is stored in Tanium Secrets Service for a customer-defined length of time. The default period is 14 days. When you upload the new certificate issued by the Certificate Authority (CA), Certificate Manager queries all endpoints (to which you have management rights) that have the old certificate and sends the enciphered private key and corresponding certificate to the client extension. Then, you deploy one or more configuration packages to instruct the client extension to unpack the files to disk and to attempt to decipher the private key. If an endpoint cannot decipher the private key, such as if the private key is no longer available on the endpoint, you need to manually resolve the issue. If the private key is no longer available on the endpoint, you can manually copy the replacement private key from an endpoint that was able to decipher the private key and then deploy a new audit. For information about how to deploy audits, see Deploying certificate audits on page 66.

Certificate Manager does not manage the private keys. Instead, Certificate Manager generates a new private key on a workstation and then manually copies the key to each endpoint that needs the key to use the new certificate. This process reduces the attack surface to ensure that the only places where the plaintext private key exists are endpoints that need to have the key.

Before you begin

- You must have a role with the **Certificate Manager Certificate write** permission and the Platform Content **Package write** permission. Users assigned the Certificate Manager Operator or Certificate Manager Administrator reserved roles have these permissions.
- You can replace certificates only on endpoints in computer groups to which you have access. For information about managing computer group assignments, see Tanium Console User Guide: Manage computer group assignments for a user.
- The replacement steps require you to edit a script file to unpack the replacement certificate and private key on endpoints and then to deploy a Tanium package to endpoints. You must have software to edit script files, you should have experience writing and testing scripts that are written in shell script (non-Windows endpoints) or PowerShell, and you should have experience editing and deploying packages to endpoints. For information about packages, see Tanium Console User Guide: Managing packages.

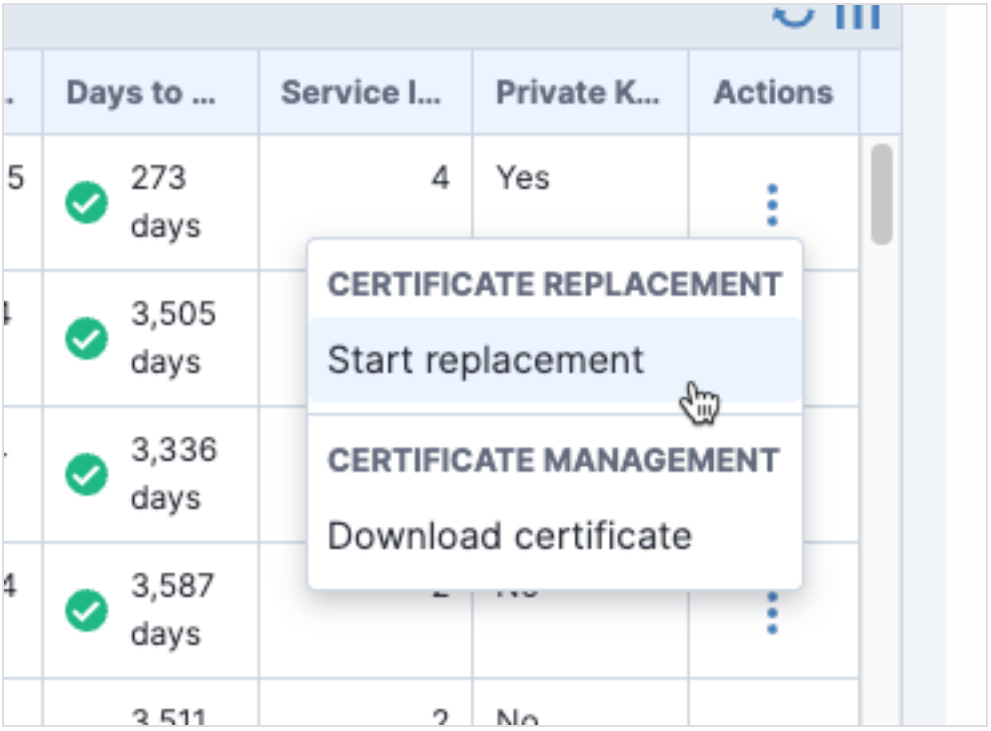
Generate certificate signing request

To replace a certificate, find a trusted endpoint with the expiring certificate. Certificate Manager uses the private key on that endpoint to generate a new certificate. Then deploy one or more packages to apply the new certificate to endpoints with the old certificate.

1. From the Main menu, go to **Modules > Certificate Manager > Certificate Inventory**.
2. (Optional) Use any search and filter options to help find a specific certificate if the grid is long. The grid shows only the certificates that match all the filters and search text that you specify. For descriptions of search and filter options, see View certificate inventory on page 49.

© 2026 Tanium Inc. All Rights Reserved

3. In the **Actions** column of the row of the certificate that you want to replace, click Actions, and then click **Start replacement**.



If the **Start replacement** option is disabled, no endpoints contain the minimum required version of swmgr-cx, or the audit was unable to locate the private key for the certificate. For a list of endpoint tools required by Certificate Manager, see Reference: Certificate Manager endpoint tools on page 84.

> TIP
> Alternatively, you can begin the certificate replacement process when you view details for a certificate. For information, see View certificate details on page 52.

4. From the **Generate Certificate Signing Request (CSR)** page, review and edit certificate details. The **Certificate Details** section shows configured details to apply to the new certificate request. To edit or add additional details, click Edit.

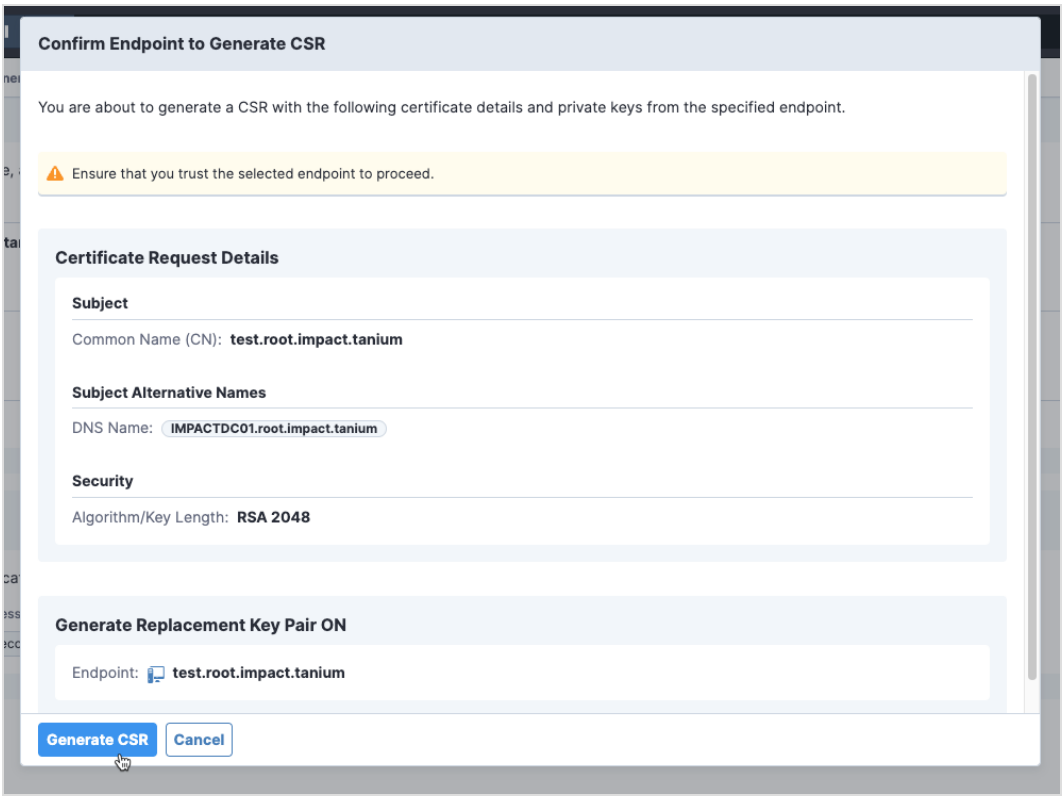
5. In the **Source Endpoint** section, review the trusted endpoint. To change which endpoint from which to retrieve the existing certificate (and private key), click Edit and select another endpoint, if available.

> NOTE
> If an endpoint is missing any required tools or does not have the private key, you cannot select the endpoint for the source.

6. Click **Submit** and then review all certificate details for correctness. Once the certificate replacement process starts, you cannot edit any of the details.

© 2026 Tanium Inc. All Rights Reserved

7. Click **Generate CSR**.



Certificate Manager opens a Direct Connect connection to the source endpoint, generates a new private key and CSR from the provided details, and then retrieves the new private key from the endpoint for distribution to other endpoints.

Download the certificate request and upload the new certificate

Download the CSR, send the request to your CA, and then upload the new certificate.

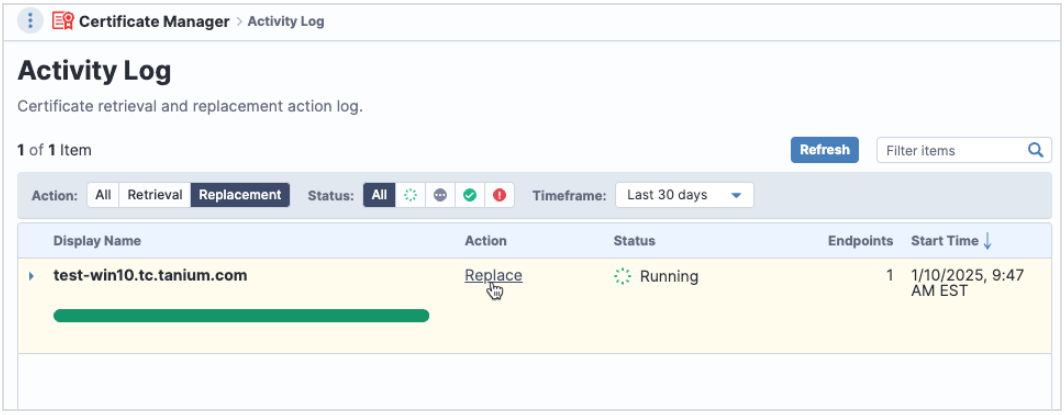
© 2026 Tanium Inc. All Rights Reserved

1. Open the **Certificate Replacement** page from the **Activity Log**. Note that this page is already open if you just clicked **Generate CSR** from Generate certificate signing request on page 54.

   a. From the Main menu, go to **Modules > Certificate Manager > Activity Log**.

   b. Set the **Action** filter to **Replacement** and adjust the **Timeframe** filter if necessary.

   c. Find the entry for the certificate replacement and click **Replace** in the **Action** column to open the log entry.



2. In the **Certificate Request** section, click Download CSR to download the certificate request to a local PEM file.

   TIP Alternatively, you can copy the certificate request to the clipboard.

3. Send the CSR to your CA.

4. After your CA processes the CSR and returns a new certificate, review the new certificate to ensure that the certificate meets the requirements of the endpoints to which you plan to distribute the certificate.

5. Return to the **Certificate Replacement** page from the **Activity Log**.

6. In the **Replacement Certificate** section, click **Upload Replacement**.

7. Drag and drop the replacement certificate to the **Drag and drop files** field or click **Browse for Files** and select the certificate. Click **Upload** after you select the file.

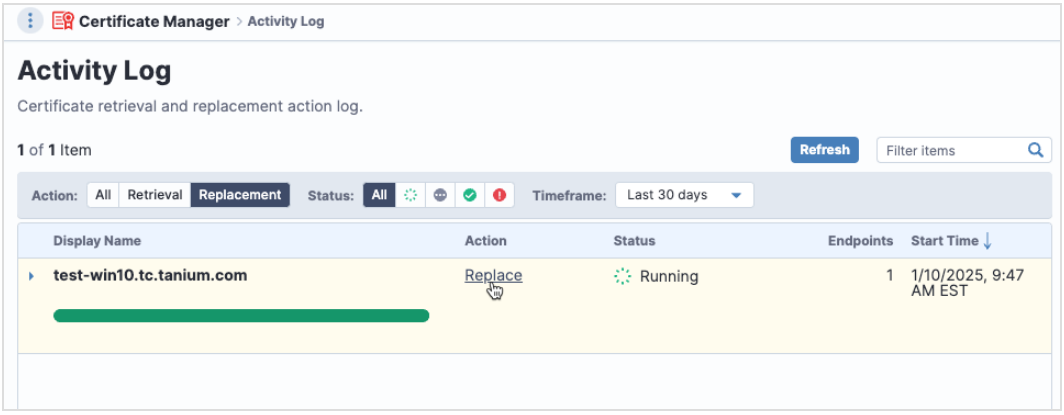
Certificate Manager begins to distribute the certificate to endpoints that use the previous certificate. In the **Target Endpoints** section, you can view the status of certificate replacements for affected endpoints. Only computer groups to which you have access appear as options.

Create configuration packages

Create packages to deploy the replacement certificate to target endpoints and to configure services to use the new certificate.

© 2026 Tanium Inc. All Rights Reserved

1. Open the **Certificate Replacement** page from the **Activity Log**. Note that this page is already open if you just uploaded the signed certificate.
   a. From the Main menu, go to **Modules > Certificate Manager > Activity Log**.
   b. Set the **Action** filter to **Replacement** and adjust the **Timeframe** filter if necessary.
   c. Find the entry for the certificate replacement and click **Replace** in the **Action** column to open the log entry.



2. In the **Configuration Package** section, click a template option to clone a configuration package from the template. Certificate Manager includes templates for Windows endpoints and non-Windows endpoints.
3. (Optional) Edit the **Package Name** and **Display Name** to be more unique or descriptive.
4. Make sure the package is assigned to the **Certificate Manager Replacement Configuration Packages** content set. Only packages assigned to the **Certificate Manager Replacement Configuration Packages** content set appear on the **Certificate Replacement page**.
5. Do not edit any other fields in the package at this time.
6. Click **Save**, and then click **Yes** to confirm that you want to save the new package.
   The **Packages** page opens, and a notification appears if the package is successfully saved.
7. Find the package on the **Packages** page and click the **Display Name** to open the package.
8. From the **Preview Package** page, click **Edit Mode**. The title of the page changes to **Edit Package**.
   The **Files** section contains two scripts based on endpoint operating systems: `configure-replacement` and `custom-script`. The `configure-replacement` file unpacks the replacement certificate and private key on endpoints. The `custom-script` file contains instructions for rotating the certificate.
9. Edit the `custom-script` file to add code to rotate the certificate.

> **NOTE**
>
> You can also edit the `configure-replacement` file to add code to rotate the certificate. However, for best results, make the changes in `custom-script` to simplify future certificate replacements. As part of normal product maintenance, Tanium might update `configure-replacement` and you will need to merge the Tanium updates into your version of `configure-replacement`.

© 2026 Tanium Inc. All Rights Reserved

a. Click Download next to `custom-script`.

b. Open the file in your preferred editor and navigate to the **USER CONFIGURATION** section.

c. Follow the instructions in that section to edit the commands to back up the previous keys and rotate in the replacement keys. You might need to add additional commands to change file ownership or permissions, and to restart services.

d. When finished, save the script file.

> IMPORTANT
>
> If you use PowerShell cmdlets that are only available with 64-bit PowerShell, you need to use a utility such as TPowershell in the package command to run the script. TPowerShell is a wrapper provided by Tanium that allows a package to run a PowerShell script in the 64-bit version of PowerShell. The template package includes `TPowerShell.exe`, and the template package command uses `TPowerShell.exe` by default.

10. Return to the **Edit Package** page.

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

    b. Find the package on the **Packages** page and click the **Display Name** to open the package.

    c. From the **Preview Package** page, click **Edit Mode**. The title of the page changes to **Edit Package**.

11. In the **Files** section, click Delete next to the existing script file.

12. Click **Add File** and select **Local Files**.

13. Select the updated script file and click **Open**.

14. Verify that the name of the script file matches the name specified in the **Command** field of the **Details** section, and then click **Save**.

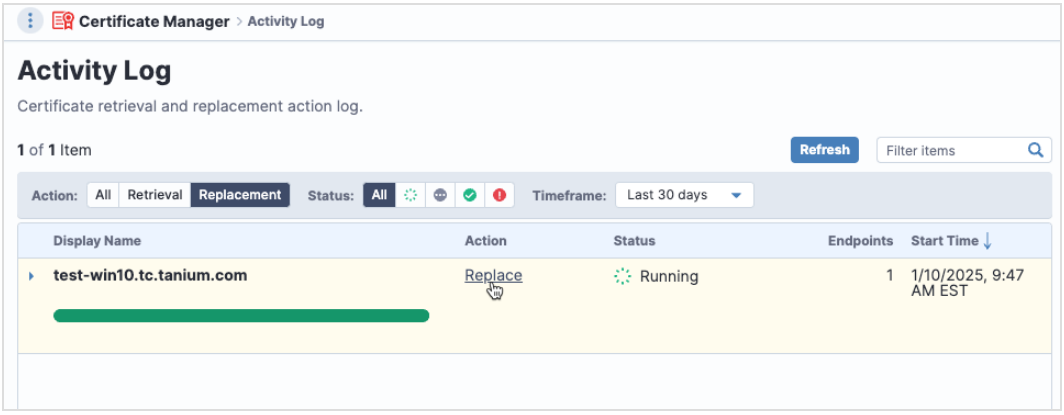
Repeat the steps to create more configuration packages if you need different packages to target additional endpoints.

Deploy configuration packages

Deploy the configuration packages that you created to replace certificates on target endpoints.

© 2026 Tanium Inc. All Rights Reserved

1. Return to the **Certificate Replacement** page from the **Activity Log**.
   a. From the Main menu, go to **Modules > Certificate Manager > Activity Log**.
   b. Set the **Action** filter to **Replacement** and adjust the **Timeframe** filter if necessary.
   c. Find the entry for the certificate replacement and click **Replace** in the **Action** column to open the log entry.



2. In the **Configuration Package** section, verify that any configuration packages you created appear in this section. If needed, view the action log to troubleshoot.
3. Deploy each package.
   a. Click **Run** next to the package.
   The **Run Configuration Package** page opens with prepopulated fields.
   b. Click **Select Computer Groups**, select the computer groups to target, and click **Save**.

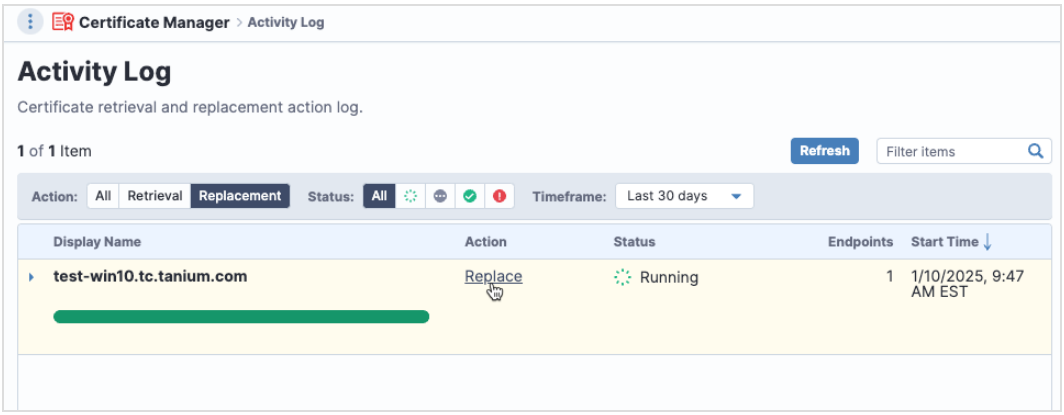
> NOTE
> Certificate Manager only deploys the package to endpoints which have the previous certificate in the selected computer groups.

   c. Click **Show Preview to Continue**, review the list of targeted endpoints, click **Run**, and then click **Confirm**.
   d. Repeat these steps for all packages that you want to run.

© 2026 Tanium Inc. All Rights Reserved

Verify package deployment

1. Return to the **Certificate Replacement** page from the **Activity Log**.
   a. From the Main menu, go to **Modules > Certificate Manager > Activity Log**.
   b. Set the **Action** filter to **Replacement** and adjust the **Timeframe** filter if necessary.
   c. Find the entry for the certificate replacement and click **Replace** in the **Action** column to open the log entry.



2. In the **Configuration Results** section, verify that the packages have been deployed.

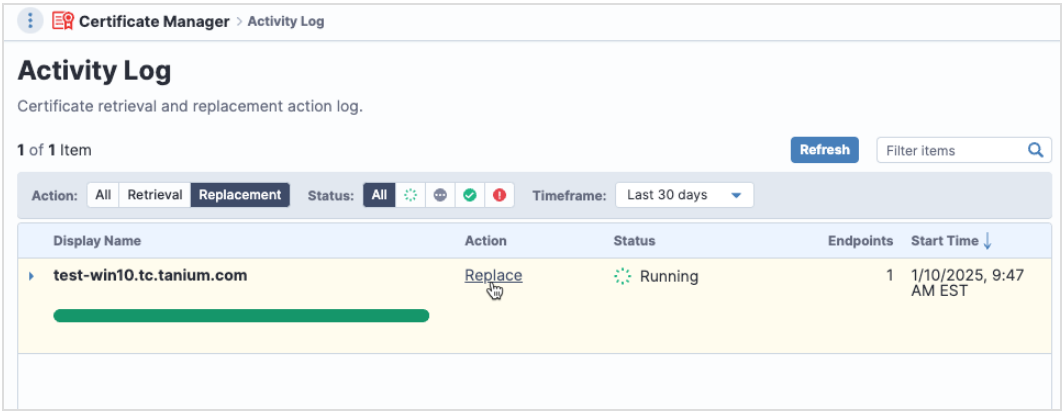
(Optional) Finalize certificate replacement

The finalization process removes the enciphered private key from secure storage on the endpoints and in Tanium Secrets Service. By default, finalization occurs automatically 14 days after you upload the replacement certificate in Certificate Manager. To remove the enciphered private key from secure storage sooner, perform the following steps.

> TIP
>
> This process only removes the enciphered private key of the new certificate. You must manually remove the previous certificate and private keys from endpoints.

© 2026 Tanium Inc. All Rights Reserved

1. Return to the **Certificate Replacement** page from the **Activity Log**.
    a. From the Main menu, go to **Modules > Certificate Manager > Activity Log**.
    b. Set the **Action** filter to **Replacement** and adjust the **Timeframe** filter if necessary.
    c. Find the entry for the certificate replacement and click **Replace** in the **Action** column to open the log entry.



2. In the **Replacement Steps** section, click **Finalize Replacement**.

NOTE

You can customize the timeframe of the automatic finalization from the default of 14 days. For more information, see Configure certificate replacement settings on page 40.

© 2026 Tanium Inc. All Rights Reserved

Configuring certificate locations

IMPORTANT

The following instructions only apply to endpoints with Toolset 2.20.86 or later. For endpoints with Toolset versions earlier than 2.20.86, the certificate locations are not configurable.

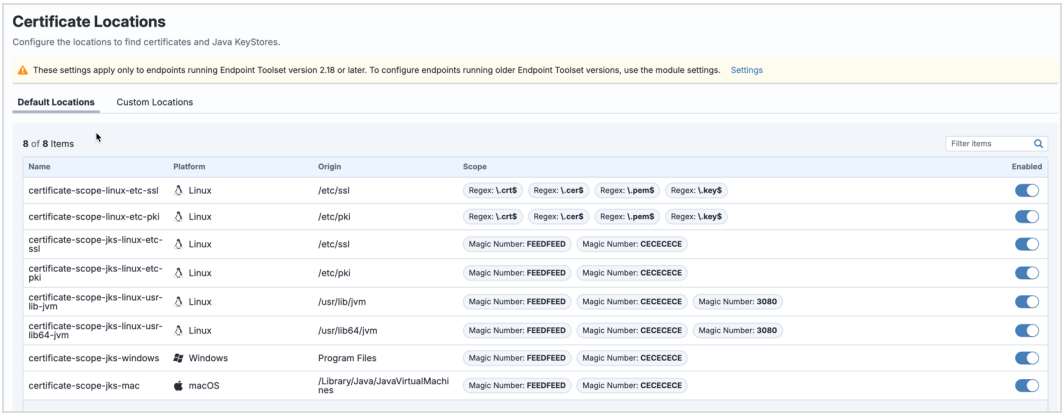
You can configure the locations where Certificate Manager looks for at-rest certificates and Java KeyStores during a certificate audit.

Review certificate locations

By default, Certificate Manager audits default and custom locations for certificates and Java KeyStores. You cannot edit or delete default locations. However, you can add custom locations.

To disable audits in the default locations, see Disable certificate location on page 64.

1. From the Main menu, go to **Modules > Certificate Manager > Configuration > Certificate Locations**.
2. Review the certificate locations.



The table contains the following columns.

- **Name**: Unique name to identify the location
- **Platform**: Linux or Windows
- **Origin**: Directory path of certificates or Java KeyStores
- **Scope**: Regular expressions or magic numbers used to identify certificates and Java KeyStores
- **Enabled**: Whether or not to include the location in certificate audits

© 2026 Tanium Inc. All Rights Reserved

Disable certificate location

You might disable a certificate location if you do not want Certificate Manager to audit a certain directory. For example, you might disable a location with old operating system certificates that are not updated by the vendor.

1. From the Main menu, go to **Modules > Certificate Manager > Configuration > Certificate Locations**.
2. In the **Default Locations** or **Custom Locations** tab, toggle off the location.

Next steps

Deploy locations on page 64.

Add custom certificate location

Add a custom certificate location if your endpoints store certificates and Java KeyStores at locations other than the default locations.

1. From the Main menu, go to **Modules > Certificate Manager > Configuration > Certificate Locations**.
2. In the **Custom Locations** tab, click **Add Certificate Location**.
3. Enter a name.
4. Select the platform.
5. In **Origin**, select **Path** and enter the directory path, or select **Predefined Origin** and select the location.
6. In **Include By**, select to include certificates by regular expression or magic number. Enter the regular expressions or magic numbers in the field and click **Save**.
   Regular expressions match file names and hexadecimal numbers match file magic numbers. Add one entry per line.

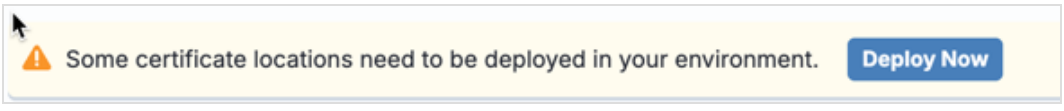
Next steps

Deploy locations on page 64.

Deploy locations

After you create or make a change to a location, you must deploy the locations to endpoints. Endpoint Configuration distributes the location changes to the **All Computers** group.

1. From the Main menu, go to **Modules > Certificate Manager > Configuration > Certificate Locations**.
2. In the banner at the top of the page, click **Deploy Now**.



3. Review the location changes and click **Confirm**.

© 2026 Tanium Inc. All Rights Reserved

Manage certificate locations

You can edit or delete custom certificate locations.

Edit custom certificate location

You can edit a custom certificate location, for example, to update the path or add an additional regular expression.

1. From the Main menu, go to **Modules > Certificate Manager > Configuration > Certificate Locations**.
2. In the **Custom Locations** tab, select the location and click  Edit.

Next steps

Deploy locations on page 64.

Delete custom certificate location

You might delete a custom certificate location that does not need to be audited.

1. From the Main menu, go to **Modules > Certificate Manager > Configuration > Certificate Locations**.
2. In the **Custom Locations** tab, select the location and click  Delete.

Next steps

Deploy locations on page 64.

© 2026 Tanium Inc. All Rights Reserved

Deploying certificate audits

IMPORTANT

The following instructions only apply to endpoints with Toolset 2.20.86 or later. If you have endpoints with Toolset versions earlier than 2.20.86, you configure and deploy certificate audits in the **Settings** page. For more information, see Configuring Certificate Manager on page 30.

Use profiles to configure and deploy certificate audits at the computer-group level.

Before you begin

- Confirm the locations that are scanned for at-rest certificates. For more information, see Review certificate locations on page 63.
- Keep in mind that Certificate Manager only finds user store certificates for users signed in during the audit. For more information, see Certificate sources on page 12.

Create a profile

Create a profile to configure a certificate audit on endpoints.

1. From the Main menu, go to **Modules > Certificate Manager > Configuration > Profiles**.
2. Click **Create Profile**.
3. Enter a name and optional description for the profile.
4. Specify an **Audit Frequency**, which is the amount of time before the listening port and Windows Certificate Store scans run again on the endpoint. Specify the number of days between 1-30. The default value is `1`.

   NOTE

   The at-rest certificate scan frequency is managed by Index. For more information, see Tanium Client Index Extension User Guide.
5. To mitigate resource consumption, enable **Distribute Over Time** and select an amount of time. **Distribute Over Time** randomizes the audit start time on each endpoint by an amount of time up to the value configured. The value you indicate for **Distribute Over Time** must be less than the **Audit Frequency**.

© 2026 Tanium Inc. All Rights Reserved

6. In the **Target Endpoints** section, click **Select Computer Groups** and select one or more computer groups to target.

   IMPORTANT

   After you deploy the profile, to stop audits on an endpoint that the profile targets, remove the endpoint from the target computer groups. (For more information, see Tanium Console User Guide: Controlling endpoint management rights through computer groups). Then save and re-deploy the profile.

7. (Optional) In the **At-Rest Certificates** section, specify the certificates to exclude from auditing in Certificate Manager.

   a. Select **SHA-256 Fingerprint**.

   b. Select one or more certificates and then click **Select Certificates**.
   The fingerprint for each certificate is added to the **Fingerprint** list.

   c. To add another fingerprint, click **Add Fingerprint** and enter the fingerprint.

   d. Click  to remove fingerprints.

8. (Optional) In the **Listening Service Certificates** section, add any exclusion criteria.

   a. Select **Enable Listening Port Scan**.

   b. (Optional) If you want to see all certificates used in your environment, unselect the **Tanium Client Ports** checkbox.

      NOTE

      By default, Tanium Client and Tanium Client API ports are excluded because Tanium Client certificates are managed by Tanium.

   c. Select the types of exclusions to add: **Port**, **Port Range**, **Address**, and **Process Name**. For each exclusion type, enter any criteria. Multiple exclusion criteria and types are joined by OR.

   d. In the **Cipher Suites** section, enable the approved ciphers for your organization.
   You can filter the ciphers based on IANA Recommendation and ciphers already approved in the profile. To review the ciphers approved by default, see Cipher suites approved by default on page 68.

9. In the **Certificate Authorities** section, select certificate authorities to designate as authorized certificates. Select a certificate authority that was previously added in the **Settings** page. Or import a PEM or DER x.509 certificate or PKCS #7 certificate bundle.
   You can add certificate authorities that Certificate Manager will find during a listening port certificate scan. Be sure that you have enabled the listening port scan in step 8. Certificate Manager does not evaluate the chain for at-rest certificates.

   NOTE

   If you want to authorize all certificates issued by a certain root CA, add all the intermediate certificates that form the links in the chain down to a given leaf certificate.

   As part of the certificate audit, Certificate Manager identifies authorized and non-authorized certificates and includes the results in dashboards and reports.

© 2026 Tanium Inc. All Rights Reserved

If you previously downloaded a certificate from the **Certificate Inventory** page (using the **Actions** > **Download certificate** option), that certificate is automatically added to this section when you create or edit a profile.

10. Click **Create**.

Next steps

Deploy profiles on page 71.

Cipher suites approved by default

Certificate Manager pre-populates the approved cipher suites based on Internet Assigned Numbers Authority (IANA) recommendations. Approval status appears in Certificate Manager dashboards and reports.

The following ciphers are approved by default in Certificate Manager:

- TLS_AES_128_CCM_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_DHE_PSK_WITH_AES_128_CCM
- TLS_DHE_PSK_WITH_AES_128_GCM_SHA256
- TLS_DHE_PSK_WITH_AES_256_CCM
- TLS_DHE_PSK_WITH_AES_256_GCM_SHA384
- TLS_DHE_PSK_WITH_CHACHA20_POLY1305_SHA256
- TLS_DHE_RSA_WITH_AES_128_CCM
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_CCM
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_PSK_WITH_AES_128_CCM_SHA256
- TLS_ECDHE_PSK_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_PSK_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_PSK_WITH_CHACHA20_POLY1305_SHA256

© 2026 Tanium Inc. All Rights Reserved

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

Set the priority of profiles

Set the priority of profiles. If more than one profile is on an endpoint, Endpoint Configuration uses the top priority profile during a certificate audit.

1. From the Main menu, go to **Modules > Certificate Manager > Configuration > Profiles**.
2. Click **Prioritize**.
3. Drag the profiles in the order that you want and then click **Prioritize**.

The profile with a priority of **1** is the highest priority profile.

Next steps

Deploy profiles on page 71.

Review profiles

You can review the status and other details of profiles.

By default, Certificate Manager includes the **Default Config** profile, which contains the current certificate audit configuration settings specified in the Settings pages and is targeted at the **All Computers** group. To review the settings on these pages, see Configuring Certificate Manager on page 30. Note that most of the Settings pages are now used only for endpoints with Toolset versions earlier than 2.20.86.

To simplify profile deployment in your environment, the **Default Config** profile is enabled by default. Review the profile for accuracy before deploying it. If you do not want to keep the same settings, disable the profile, so that it is not deployed when you deploy other profile updates.

1. From the Main menu, go to **Modules > Certificate Manager > Configuration > Profiles**.
2. View the profiles.
   To filter the rules based on enablement or status, click the corresponding toggle. The table contains the following columns:
   - **Priority**: Priority number of the profile. If more than one profile is on an endpoint during a certificate audit, Endpoint Configuration uses the highest priority profile.
   - **Enabled**: Enablement status of the profile

© 2026 Tanium Inc. All Rights Reserved

- **Status**: Status of the profile

  Certificate Manager profile status

Status	Description
Never Deployed	Profile has not been deployed to endpoints
Deployed	Profile has been deployed to endpoints
Pending Approval	Profile will not be deployed to endpoints until a user with approval permission approves the change. For more information about enabling and using configuration approvals in Endpoint Configuration, see Tanium Endpoint Configuration User Guide: Managing approvals.
Changed	Profile has been previously deployed to endpoints but now has changes that need to be deployed to endpoints

- **Name**: Name of the profile
- **Computer Groups**: Computer groups targeted by the profile
- **Audit Frequency**: Amount of time between the start of certificate audits

3. To review a profile, expand the row.

Enable or disable profiles

You must enable a profile in the Certificate Manager workbench to activate it. After you enable a profile, you then need to deploy it. For more information, see Deploy profiles on page 71.

If you want to temporarily deactivate a profile in the Certificate Manager workbench, disable it. For example, you might disable a profile that excludes certain ports because you want a profile with a less restrictive port strategy to run certificate audits on the targeted endpoints for a period of time. If you disable a profile that has already been deployed, Endpoint Configuration deletes the profile from endpoints. Disabled profiles are not deleted from the **Profiles** page. (If you want to permanently remove a profile, delete it. For more information, see Delete profile on page 72.)

1. From the Main menu, go to **Modules > Disabled profiles are deleted from the targeted endpoints. Disabled profiles are not deleted from the Profiles page. > Configuration > Profiles**.
2. Toggle a profile in the **Enabled** column to enable or disable.

Next steps

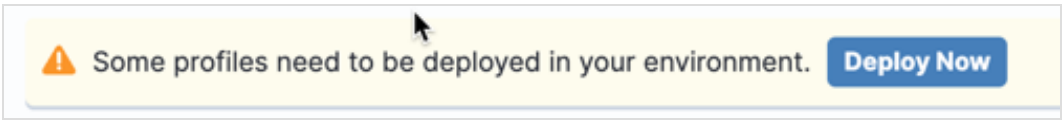
Deploy profiles on page 71.

© 2026 Tanium Inc. All Rights Reserved

Deploy profiles

After you create or edit profiles, you must deploy the profiles to endpoints. Endpoint Configuration distributes the profiles to the endpoints targeted in the profiles.

1. From the Main menu, go to **Modules > Certificate Manager > Configuration > Profiles**.
2. In the banner at the top of the page, click **Deploy Now**.



3. Review the profiles changes and click **Deploy**.

> NOTE
>
> After a profile has been deployed to endpoints, the profile status is updated to **Deployed**.

Manage profiles

Edit profile

You can edit a profile to make necessary changes. For example, you might edit a profile to modify the ports to exclude.

1. From the Main menu, go to **Modules > Certificate Manager > Profiles**.
2. Select the checkbox next to the profile that you want to edit and click Edit.

   If you select more than one profile, the option to edit is disabled.
3. Update any fields and then click **Save**. For information on specific fields, see Create a profile on page 66.

Next steps

Deploy profiles on page 71.

Import profiles

You can import profiles from a JSON file to quickly add profiles to Certificate Manager. For example, you might import profiles from a staging environment to a production environment.

1. From the Main menu, go to **Modules > Certificate Manager > Configuration > Profiles**.
2. Click **Import Profiles**.
3. Click **Browse for File** and select a JSON file.

© 2026 Tanium Inc. All Rights Reserved

4. Select the import type.
    - **Replace All** replaces all current profiles with the profiles in the imported file. If an existing profile is not in the imported file, Certificate Manager deletes the existing profile.
    - **Merge** combines the current profiles and the profiles in the imported file. If an existing profile name matches a profile name in the imported file, Certificate Manager uses the profile details in the imported file.
5. Click **Preview to Continue > Import**.

Next steps

Deploy profiles on page 71.

Export profiles

You can download profile definitions as a JSON file to your local machine. For example, you might export profiles from a staging environment to later import into a production environment.

1. From the Main menu, go to **Modules > Certificate Manager > Configuration > Profiles**.
2. Select the profiles that you want to export and click **Export**.

Delete profile

Delete a profile that you no longer need. For example, you might delete a proifle that has been disabled for an extended period of time and you no longer need. Deleting a profile deletes the profile from the targeted endpoints and from the **Profiles** page.



Use caution when deleting a profile because you can delete an active profile on an endpoint.

1. From the Main menu, go to **Modules > Certificate Manager > Configuration > Profiles**.
2. Select the profiles that you want to delete and click Delete.

Next steps

Deploy profiles on page 71.

© 2026 Tanium Inc. All Rights Reserved

Maintaining Certificate Manager

Perform regular maintenance tasks to ensure that Certificate Manager successfully performs scheduled activities on all the targeted Tanium Client managed endpoints and does not overuse endpoint or network resources. If Certificate Manager is not performing as expected, you might need to troubleshoot issues or change settings.

Perform monthly maintenance

Identify and resolve errors that might prevent Certificate Manager from completing certificate audits.

1. From the Main menu, go to **Modules > Certificate Manager > Overview**.
2. In the **Overview** section, review the **Certificate Manager Endpoint Coverage** panel for endpoints with the **Needs Attention** status.
3. To investigate issues, see Monitor and troubleshoot Certificate Manager Coverage on page 73.
4. To troubleshoot other Certificate Manager issues, see Troubleshooting Certificate Manager on page 75.

Perform as-needed maintenance

Verify that any recurring connections in Tanium Connect are running as expected.

1. From the Main menu, go to **Modules > Connect > Connections**.
2. Click on each of your connections to check the **Run Status** and **Next Run** details.
3. If the **Owner** is no longer an active user, click **Actions > Edit Ownership** to take ownership of the connection. For more information, see Tanium Connect User Guide: Scheduled connection owned by a deleted user no longer runs.
4. To troubleshoot other connection issues, see Tanium Connect User Guide: Troubleshoot issues.

Monitor and troubleshoot Certificate Manager Coverage



The following instructions only apply to endpoints with Toolset versions earlier than 2.20.86.

The following table lists contributing factors into why the Certificate Manager coverage metric might report endpoints as **Needs Attention**, and corrective actions you can make.

© 2026 Tanium Inc. All Rights Reserved

Troubleshooting for Tanium Certificate Manager coverage metric Needs Attention reports

Contributing factor	Corrective action
Audit scan age over 30 days	• Verify that the certificate audit packages are scheduled to run daily. For more information, see Configuring Certificate Manager on page 30. • Deploy a certificate audit package on page 42.
Audit scan timed out	Contact Tanium Support on page 83 to determine why the audit scan timed out before completing successfully and if increasing the **Certificate Audit [Windows]** or **Certificate Audit [Non-Windows]** package parameterized timeout is needed.
Certificate Audit has not been run	• Verify that a certificate audit completed successfully on page 82. • Deploy a certificate audit package on page 42 if needed.
Certificate Manager Tools missing	• Verify that all endpoints have the latest version of the Certificate Manager Tools installed using the following sensor: `Get Endpoint Configuration - Tools Status having Endpoint Configuration - Tools Status:Tool Name contains Certificate Manager from all machines` • Ensure that the **Tanium Certificate Manager** action group is configured to the targeted endpoints.
Error parsing the Audit Database	Contact Tanium Support on page 83 to determine why the audit database could not be parsed and next steps to take.
Missing lsof command	Verify that lsof is installed on all Linux endpoints. For more information, see ERROR - lsof was not found on page 81.
• TPython missing • Tanium Python 3.8 missing	• Verify that all endpoints have the latest version of the Tanium Python Tools installed using the following sensor: `Get Python - Tools Version from all machines` • Deploy the **Python - Tools [Linux]** package to any endpoints that return **Linux Package Required**. • Deploy the **Python - Tools [Mac]** package to any endpoints that return **Mac Package Required**. • Deploy the **Python - Tools [Windows]** package to any endpoints that return **Windows Package Required**.

© 2026 Tanium Inc. All Rights Reserved

Troubleshooting Certificate Manager

If Certificate Manager is not performing as expected, you might need to troubleshoot issues or change settings.

Collect logs

Collect troubleshooting packages

The information is saved as ZIP files that you can download with your browser. The zip files are also known as a support bundle.

To download logs:

1. From the Certificate Manager **Overview** page, click Help .
2. From the **Troubleshooting** tab, select the solutions for which to gather troubleshooting packages and click **Create Packages**. By default, all solutions are selected.
3. When the packages are ready, click **Download Packages**.
   ZIP files of all the selected packages download to the local download directory.

   Some browsers might block multiple downloads by default. Make sure to configure your browser to permit multiple downloads from the Tanium Console.
4. Contact Tanium Support to determine the best option to send the ZIP files. For information, see Contact Tanium Support on page 83.

Collect action logs

Collect the action log and other tools files from the endpoint to send to Tanium Support.

ENDPOINTS WITH TOOLSET 2.20.86 OR LATER

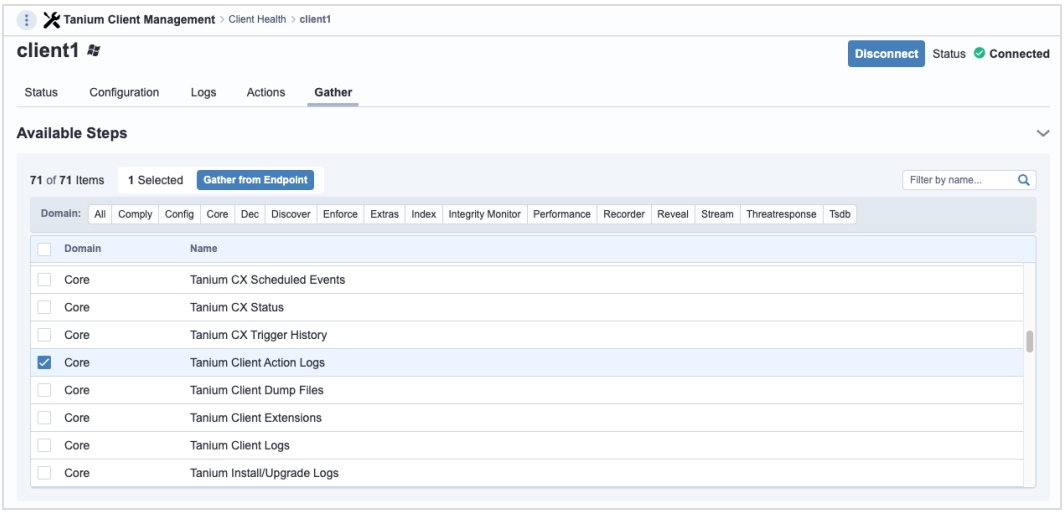
Use Client Management to generate an Endpoint Must Gather for all files in the **Software Manager** and **Core** domains. For more information, see Tanium Client Management User Guide: Collect troubleshooting information from endpoints.

ENDPOINTS WITH TOOLSET VERSIONS EARLIER THAN 2.20.86

Collect the action log and other tools files from the Tanium Client managed endpoint to send to Tanium Support.

1. To collect the action log for the **Deploy Certificate Audit [Windows]** or **Deploy Certificate Audit [Non-Windows]** actions, use Tanium Client Management to directly connect to an endpoint and collect the **Tanium Client Action Logs**. For more information, see Tanium Client Management User Guide: Collect troubleshooting information from endpoints.

© 2026 Tanium Inc. All Rights Reserved



2. Collect the following file and folder from the `<Tanium Client>\Tools\CertificateManager` folder:
    - `sslaudit.db`
    - `sensor_data`
3. Contact Tanium Support to determine the best option to send the files. For more information, see Contact Tanium Support on page 83.

Review the activity log

> **NOTE** You can view activity for endpoints for which you have management rights. For information about how to update management rights, see Tanium Console User Guide: Manage computer group assignments for a user or Tanium Console User Guide: Manage computer group assignments for a user group.

Certificate Manager includes an activity log for certificate retrievals and renewals. Review the activity log periodically to verify certificate retrievals and replacements.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules > Certificate Manager > Activity Log**.
2. The following actions are available:

Activity Log actions

Option	Description
View log entry	Click Expand  next to the log entry.
View certificate details	• To view basic certificate details, expand a log entry and then expand **Certificate Details**. • To retrieve additional certificate details, click the value in the **Action** column to open the **Certificate Retrieval** page. In addition to basic certificate details, the page shows extensions and contains a link to copy and download the certificate.
Search by text	Enter an alphanumeric string in the **Filter items** field to match text in the **Display Name** column.
Sort by start time	Click the **Start time** column header to toggle sorting by start time.
Filter by action	The **Action** filter includes the following options: • **All**: Show all entries for certificate retrievals and replacements. • **Retrieval**: Show only entries for certificate retrievals. • **Replacement**: Show only log entries for certificate replacements.
Filter by status	For the **Status** filter, select **All** to show only all entries regardless of status. Otherwise, select a status by which to filter the log entries: •  - Show only log entries that are active • - Show only log entries that are inactive •  - Show only log entries for actions that completed successfully •  - Show only log entries for actions that failed
Filter by timeframe	Select to filter log entries by timeframe. You can choose from the list of timeframes or select **Custom** to enter your own date range.

© 2026 Tanium Inc. All Rights Reserved

Activity Log actions (continued)

Option	Description

Filter endpoints	When you expand a log entry, you can apply filters to the **Found on Endpoints** section.
	• **Retrieval** filter options include:
	  ◦ **All**: Show all entries.
	  ◦ **Retrieved**: Show only endpoints where the certificate was successfully retrieved.
	  ◦ **Failed**: Show only endpoints from which Certificate Manager was unable to retrieve the certificate.
	  ◦ **Not Attempted**: Show only endpoints from which Certificate Manager did not attempt to retrieve a certificate.
	• Enter an alphanumeric string in the **Filter items** field to match text in any column of the endpoint table.

View endpoint details	You can view details for an endpoint in the **Found on Endpoints** section in any log entry. Click Endpoint Details to view basic details for the endpoint and then click **View Details** to open the Endpoint Details page in Tanium Reporting. For information about the Endpoint Details page, see Tanium Reporting User Guide: View endpoint details.
Refresh log	Click Refresh. Any filters that you added apply to the updated results.

Cannot view all chart panels in the dashboard

Issue

If users cannot view all chart panels in the Certificate Manager dashboard in Tanium Reporting, the user permissions might not have sufficient permissions.

Solution

In addition to the Certificate Manager roles, users must also have sufficient management rights, such as **All Computers**.

For more information about Certificate Manager roles, see Set up Certificate Manager users on page 31.

Endpoint does not have Toolset 2.20.86 or later

Endpoints must have Toolset 2.20.86 or later in order to use profiles. Identify and update endpoints with earlier toolset versions.

1. Confirm that Endpoint Toolset 2.20.86 or later is promoted to all rings in the ring deployment plan. For more information, see Tanium Endpoint Configuration User Guide: Manage and promote toolset versions in the upgrade rings.
2. To identify the remaining endpoints that do not have Toolset 2.20.86 or later, review the **Endpoints Not Scanning with**

© 2026 Tanium Inc. All Rights Reserved

Profiles chart on the **Overview** page.

3. Resolve the issues on these endpoints. For instructions, see Tanium Endpoint Configuration User Guide: Identify and resolve issues with endpoint tools or client extensions.

Endpoint with profile needs attention

The **Endpoints with Profiles Needing Attention** chart on the **Overview** page identifies endpoints with Toolset 2.20.86 or later that have scan errors. Use the following information to troubleshoot these errors.

1. Click the title or number of endpoints on the **Endpoints with Profiles Needing Attention** chart. The **Certificate Manager - CX Endpoints Needing Attention** report appears.
2. For each endpoint, in the **Client Health - Health Failures Error ID** column, identify the error ID.
3. In Knowledge Article: Health Check Messages (login required), filter by the error ID to quickly find the description and resolution.
4. If you cannot login to the Health Check Messages page or the error ID does not appear on that page, Contact Tanium Support on page 83.

Endpoint continues to run certificate audits after uninstalling or blocking Certificate Manager tools



The following instructions only apply to endpoints with Toolset 2.20.86 or later.

Issue

You uninstalled or blocked Certificate Manager tools on an endpoint to stop certificate audits, but the endpoint continues to run audits.

Solution

To stop audits on an endpoint, remove the endpoint from the profile's targeted computer groups. For more information, see Create a profile on page 66.

Unexpected certificate audit results



The following instructions only apply to endpoints with Toolset versions earlier than 2.20.86.

© 2026 Tanium Inc. All Rights Reserved

Issue

If an endpoint shows the following error in the **Protocol** column, you might have to refresh a certificate audit on that endpoint: `Error: Protocol and cipher suites do not exist. Run the Certificate Audit package.`

Certificate audit status shows **Failed** for some endpoints.

Solution

1. Verify that a certificate audit completed successfully.
2. If the **States of machines** section shows any **Failed** statuses, click **Show Client Status Details**.
3. Select one or more endpoints that show a **Failed** action status and click **Get action log for selected machines**.
4. Review the action log to determine the cause of the failure.

Unable to view expected computer groups

Issue

The **Computer Group** filter on the Certificate Manager **Overview** page does not contain all expected computer groups.

Solution

Enable data collection for the computer groups in Tanium Reporting. For information, see Tanium Reporting User Guide: Select computer groups for data collection.

Error: EC_KEY_new_by_curve_name



The following instructions only apply to endpoints with Toolset versions earlier than 2.20.86.

Issue

Older Linux endpoints with OpenSSL versions older than 1.0.1 cannot successfully run the **Deploy Certificate Audit [Non-Windows]** package. The following error is found in the action log: `undefined symbol: EC_KEY_new_by_curve_name`

Solution

Upgrade to OpenSSL 1.0.1 or later.

To view which version of OpenSSL is on an endpoint, use the **Certificate Audit Status** sensor.

© 2026 Tanium Inc. All Rights Reserved

ERROR - lsof was not found



The following instructions only apply to endpoints with Toolset versions earlier than 2.20.86.

Issue

To include the owning process data for Linux endpoints, the lsof command is required. If a Linux endpoint does not have lsof installed, the following errors are found:

- from the **Certificate Manager - Coverage Status Details** sensor: `Missing lsof command`
- in the action log : `ERROR – lsof was not found.`

Solution

Use either of the following options to confirm the error and then install lsof.

1. Check the **Certificate Manager - Current Coverage Status Details** report.
    a. From the Main menu, go to **Modules > Certificate Manager > Overview**.
    b. In the **Certificate Manager Endpoint Coverage** chart of the **Overview** section, click **Needs Attention**.
2. Check the action log for the **Deploy Certificate Audit [Non-Windows]** action. For more information, see Tanium Console User Guide: Investigate action-related issues.

ERROR - No SSL Scan is being performed, limited data available



The following instructions only apply to endpoints with Toolset versions earlier than 2.20.86.

Issue

When viewing an endpoint on the **Certificate Manager - Current Coverage Status Details** report, the **Issues** column contains **No SSL Scan is being performed, limited data available**.

This message appears when no certificate audit has run on the endpoint.

To view the **Certificate Manager - Current Coverage Status Details** report, choose one of the following:

© 2026 Tanium Inc. All Rights Reserved

TIP

- Go to the Certificate Manager **Overview** page. In the **Overview** section, click the title of the **Certificate Manager Endpoint Coverage** chart.
- From the Main menu, go to **Data > Reports**, and then search for **Certificate Manager - Current Coverage Status Details**. If there are multiple copies of the report, open the report with the **Tanium Internal** author.

Solution

1. Make sure port scanning is enabled in Certificate Manager. In Certificate Manager 1.7 and later, port scanning is disabled by default. If port scanning is disabled, a warning banner appears on Certificate Manager **Overview** page. For more information, see Configure audit settings on page 33
2. If port scanning is enabled, you can either deploy a certificate audit package manually or wait until the next **Certificate Audit [Non-Windows]** and **Certificate Audit [Windows]** scheduled actions run. By default, the scheduled actions run every two hours. For more information, see Deploying certificate audits.

Verify that a certificate audit completed successfully

IMPORTANT

The following instructions only apply to endpoints with Toolset versions earlier than 2.20.86.

1. From the Main menu, go to **Administration > Actions > Action History** and search for `Certificate Audit`.
2. Select the checkbox for one or more actions that correspond with the **Certificate Audit [Non-Windows]** or **Certificate Audit [Windows]** packages and click **Show Status**.
3. In the **States of machines** section, verify that the status is **Completed**.
   For more information about action states, see Tanium Console User Guide: View action status.

If you are not seeing expected results in the Certificate Manager reports, see Unexpected certificate audit results on page 79.

Verify endpoint tools

If you are experiencing issues such as a feature not working on an endpoint or seeing incorrect data in the workbench, confirm that your endpoints have the latest toolset version. For more information, see Tanium Endpoint Configuration User Guide: Identify and resolve issues with endpoint tools or Client Extensions. For more information about Certificate Manager tools, see Reference: Certificate Manager endpoint tools on page 84.

© 2026 Tanium Inc. All Rights Reserved

Uninstall Certificate Manager

1. From the Main menu, go to **Administration > Configuration > Solutions**.
2. Select the checkbox in the Certificate Manager section, and then click **Uninstall** and follow the process.
3. Return to the **Solutions** page and verify that the **Import** button is available for Certificate Manager.

Contact Tanium Support

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

Reference: Certificate Manager endpoint tools

Endpoint Configuration installs the following Certificate Manager tools on endpoints. Certificate Manager endpoint tools extend the functionality of Tanium Certificate Manager. You can check the status of these tools with the **Get Endpoint Configuration - Tools Status** sensor.



Each solution includes a tool with the same name as the solution that appears in the Endpoint Configuration Toolset manifest but that does not appear in the following table. This tool is not deployed to the endpoint itself, but it manages the endpoint tooling dependencies for the solution, as listed in the table.

Endpoint tools for Tanium Certificate Manager

Tool	Description
core-cx	Provides a management framework API for all other Client Extensions and exposes operating system metrics
cx-config	Provides installation and configuration of extensions on an endpoint
entity-cx	Provides management for entity providers and facilitates communication between the entity providers and Tanium Client
extras-cx	Provides a helper library that contains re-usable functions for various client extensions to use
index-cx	Provides the ability to index the local file systems on an endpoint
python312	Provides TPython binary and libraries
swmgr-cx	Provides a catalog of all installed software on an endpoint

© 2026 Tanium Inc. All Rights Reserved

Reference: Sensor usage

Use the following table to review Certificate Manager sensor usage. For more information, see Tanium Console User Guide: Managing sensors.

Tanium Certificate Manager sensors

Sensor name	Management/Metric	At Rest Certificates	Listen Port Certificates	Listen Port Protocols/Ciphers	Listen Port Service Information
Certificate Audit Age	✓				
Certificate Audit Status NOTE This sensor is only used for endpoints with Toolset versions earlier than 2.20.86.	✓				
Certificate Audit Port Exclusions NOTE This sensor is only used for endpoints with Toolset versions earlier than 2.20.86.	✓				
Certificate Details		✓	✓		
Certificate Duration		✓	✓		
Certificate Expiry		✓	✓		

© 2026 Tanium Inc. All Rights Reserved

Tanium Certificate Manager sensors (continued)

Sensor name	Management/Metric	At Rest Certificates	Listen Port Certificates	Listen Port Protocols/Ciphers	Listen Port Service Information
Certificates Asserting OID	✓				
Certificate Manager - Client Extension for Certificate Audits	✓				
Certificate Manager - Coverage Status Details	✓				
Certificate Manager - Profile Details	✓				
Certificate Manager - SSL Certificate CA Short Name			✓		
Certificate Manager - SSL Certificate Cipher Suite Details				✓	
Certificate Manager - SSL Certificate Details			✓		
Certificate Manager - SSL Certificate Expiration			✓		
Certificate Manager - SSL Certificate Process Details			✓		✓
Certificate Manager - SSL Certificate Subject			✓		
Certificate Manager - SSL Extended Key Usage			✓		
Certificate Manager - SSL Key Usage			✓		
Certificate Manager SSL Server Key Exchange				✓	
Certificate Manager - SSL Server Root CA			✓		
Certificate Manager - SSL Service Cipher Suite Approval				✓	✓

© 2026 Tanium Inc. All Rights Reserved

Tanium Certificate Manager sensors (continued)

Sensor name	Management/Metric	At Rest Certificates	Listen Port Certificates	Listen Port Protocols/Ciphers	Listen Port Service Information
Certificate Manager - Supported SSL/TLS Protocols				✓	
Certificate Thumbprints		✓			

© 2026 Tanium Inc. All Rights Reserved