Tanium™ Certificate Manager User Guide

Version 1.9.18

March 14, 2023

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://docs.tanium.com for the most current Tanium product documentation.

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

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

Tanium is committed to the highest accessibility standards for our products. To date, Tanium has focused on compliance with U.S. Federal regulations - specifically Section 508 of the Rehabilitation Act of 1998. Tanium has conducted 3rd party accessibility assessments over the course of product development for many years and has most recently completed certification against the WCAG 2.1 / VPAT 2.3 standards for all major product modules in summer 2021. In the recent testing the Tanium Console UI achieved supports or partially supports for all applicable WCAG 2.1 criteria. Tanium can make available any VPAT reports on a module-by-module basis as part of a larger solution planning process for any customer or prospect.

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

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

Table of contents

Certificate Manager overview **7**

Certificate Manager dashboard 7

Certificate Manager reports 8

Certificate Manager packages 9

Certificate sources 9

Certificate Details sensor 10

Integration with other Tanium products 10

Reporting 10

Getting started with Certificate Manager **11**

Step 1: Install and configure Certificate Manager 11

Step 2: Manage certificates 11

Step 3: Deploy certificate audits 11

Certificate Manager requirements **12**

Core platform dependencies 12

Solution dependencies 12

Tanium recommended installation 12

Import specific solutions 12

Required dependencies 12

Feature-specific dependencies 13

Endpoints 13

Supported operating systems 13

Host and network security requirements 13

Security exclusions 13

User role requirements 14

Installing Certificate Manager **16**

Before you begin 16

Import Certificate Manager 16

Manage solution dependencies ... 16
Verify Certificate Manager version ... 16
Configuring Certificate Manager ... **17**
Install and configure Tanium Endpoint Configuration ... 17
Manage solution configurations with Tanium Endpoint Configuration ... 17
Configure Certificate Manager ... 17
Configure the Certificate Manager action group ... 17
Set up Certificate Manager users ... 18
Create scheduled actions for Certificate Manager ... 18
Configure authorized certificate authorities ... 19
Managing certificates ... **20**
View the Certificate Manager dashboard in Tanium Reporting ... 20
View expired certificates ... 20
View expiring certificates ... 20
View listening service certificates that are expiring in 30 days ... 20
View all certificates that are expiring in 30 days ... 21
Email a report of expiring certificates with Tanium Connect ... 21
Before you begin ... 21
Create a connection ... 21
View short keys ... 22
View listening service certificates that use short keys ... 22
View all certificates that use short keys ... 22
View weak signatures ... 22
View listening service certificates that use weak signatures ... 22
View all certificates that use weak signatures ... 22
View wildcard certificates ... 22
View listening service certificates that use a wildcard subject ... 22
View all certificates that use a wildcard subject ... 22
View self-signed certificates ... 23
View unauthorized certificates ... 23

Prepare for post-quantum cryptography ... 23
View listening service certificates by cipher suite strength ... 23
View all certificates by cipher suite strength ... 23
Deploying certificate audits ... **24**
Deploy a certificate audit package ... 24
Verify that a certificate audit completed successfully ... 24
Configure certificate port exceptions ... 24
Add port exclusions ... 25
Delete port exclusions ... 25
Configure authorized certificate authorities ... 25
Obtain the certificate chain for your external CA using OpenSSL ... 26
Obtain your internal CA certificates ... 27
Add the files to the packages in Tanium ... 28
Update and reissue scheduled actions ... 28
Add certificate exceptions ... 29
Maintaining Certificate Manager ... **30**
Perform monthly maintenance ... 30
Perform as-needed maintenance ... 30
Check scheduled Connect connections ... 30
Monitor and troubleshoot Certificate Manager Coverage ... 30
Troubleshooting Certificate Manager ... **32**
Collect logs ... 32
Cannot view all chart panels in the dashboard ... 32
Issue ... 32
Solution ... 33
Unexpected certificate audit results ... 33
Issue ... 33
Solution ... 33
ERROR - lsof was not found ... 33
Issue ... 33

Solution 33
Contact Tanium Support 33

Certificate Manager overview

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

With weak encryption and expired certificates, endpoint communications are at risk of interception critical business service outages. You can use Certificate Manager to find and alert on expired or expiring certificates and for visibility into certificate encryption strength.

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

- Find 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 using Tanium™ Connect

Certificate Manager dashboard

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

- Overview
    - Total Certificates Inventoried
    - Total Endpoints Inventoried
    - Total Service Certificates Inventoried
    - Total Root Certificates Inventoried
    - Certificate Manager Coverage
- Listening SSL/TLS Services Certificate and Cipher Inventory
    - Listening Service Certificates Expiring in 30 Days
    - Listening Service Short Keys
    - Listening Service Signature Hash Algorithms
    - Listening Services with Wildcard Certificates
    - Listening Service Certificate Authorized CA Status
    - Certificate Expiration on Listening Services

    - Lowest Cipher Strength by Listening Service Port
    - Number of Ciphers by Listening Service Port
    - Cipher Inventory by Cipher Suite Strength
- All Certificates
    - Expired Certificates
    - Wildcard Certificates
    - Weak Signature Hash Algorithms
    - Total Short Keys
    - Expiring within 30 Days
    - Certificate Expiration
    - Certificate Sources
    - Certificate Issuers

For more information, see View the Certificate Manager dashboard in Tanium Reporting on page 20.

Certificate Manager reports

The following Certificate Manager reports are available in Tanium Reporting:

- Certificate Manager - Certificate Details
- Certificate Manager - Certificates Expiring within 30 Days
- Certificate Manager - Cipher Inventory
- Certificate Manager - Cipher Suite Strength
- Certificate Manager - Coverage Status Details
- Certificate Manager - Expired Certificates
- Certificate Manager - Listening Service Certificate Details
- Certificate Manager - Listening Service Certificates Expiring within 30 Days
- Certificate Manager - Listening Service Cipher Suite Strength
- 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 - Minimum Cipher Suite Strength by Port

- Certificate Manager - Root Certificate Details
- Certificate Manager - Short Keys
- Certificate Manager - SSL Certificate Details
- Certificate Manager - Weak Signatures
- Certificate Manager - Wildcard Certificates

For more information, see Managing certificates on page 20.

Certificate Manager packages

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

For more information, see Deploying certificate audits on page 24.

Certificate sources

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

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

Certificate discovery method	Platforms	Locations	Unique capabilities	Customization
Listen ports*	• Windows • Linux • macOS	All ports except for 17472	• Quantum Computer Vulnerable Ciphers • Authorized Certificate Authority (CA) • Cipher Strength • Owning Process	• Certificate Audit Add Port Exclusions • Certificate Audit Delete Port Exclusions
File	Linux	• `/etc/pki/*` • `/etc/ssl/*`	None	`exceptions.csv` in Certificate Audit packages

Certificate discovery method	Platforms	Locations	Unique capabilities	Customization
Windows Certificate Store	Windows	User Store for signed-in users	None	`exceptions.csv` in Certificate Audit packages

* Only one certificate is audited for each port.

Certificate Details sensor

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

Column name	Description
Source	Certificate sources on page 9 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	Certificate issuing authority
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

Integration with other Tanium products

Certificate Manager integrates with Tanium Reporting to provide reporting of related data.

Reporting

View Certificate Manager reports and dashboards in Tanium 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 21.

Getting started with Certificate Manager

Follow these steps to configure and use Certificate Manager.

Step 1: Install and configure Certificate Manager

See Installing Certificate Manager on page 16 and Configuring Certificate Manager on page 17.

Step 2: Manage certificates

See Managing certificates on page 20.

Step 3: Deploy certificate audits

See Deploying certificate audits on page 24.

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 Certificate Manager
- **Tanium™ Core Platform servers**: 7.5.5.1140 or later
- **Tanium™ Client**: 7.4 or later

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). The installation method that you select determines if the Tanium Server automatically imports dependencies or if you must manually import them.

Some Certificate Manager dependencies have their own dependencies, which you can see by clicking the links in the lists of Required dependencies on page 12 and Feature-specific dependencies on page 13. 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. 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. See Tanium Console User Guide: Import, re-import, or update specific solutions.

Required dependencies

Certificate Manager has the following required dependencies at the specified minimum versions:

- Tanium™ Client Management 1.12.77 or later
- Tanium Reporting 1.13.76 or later

Feature-specific dependencies

Certificate Manager has the following feature-specific dependencies at the specified minimum versions:

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

Endpoints

Supported operating systems

The following endpoint operating systems are supported with Certificate Manager.

Operating System	Version	Notes
Windows	Same as Tanium Client support. See Tanium Client Management User Guide: Client version and host system requirements.	
macOS	Same as Tanium Client support. See Tanium Client Management User Guide: Client version and host system requirements.	SSL Audit only
Linux	Same as Tanium Client support. See Tanium Client Management User Guide: Client version and host system requirements.	Requires lsof to capture owning process data. For more information, see ERROR - lsof was not found on page 33.

Host and network security requirements

Specific processes are needed to run Certificate Manager.

Security exclusions

If security software is in use in the environment to monitor and block unknown host system processes, Tanium recommends that a security administrator create exclusions to allow the Tanium processes to run without interference. The configuration of these exclusions varies depending on AV software. For a list of all security exclusions to define across Tanium, see Tanium Core Platform Deployment Reference Guide: Host system security exclusions.

Certificate Manager security exclusions

Target Device	Notes	Exclusion Type	Exclusion
Windows endpoints		Process	`<Tanium Client>\Python38\TPython.exe`
		Folder	`<Tanium Client>\Python38`
		Process	`<Tanium Client>\TaniumCX.exe`
		Process	`<Tanium Client>\Tools\StdUtils\TaniumExecWrapper.exe`
		Folder	`<Tanium Client>\Tools\CertificateManager`
Linux endpoints		Process	`<Tanium Client>/python38/python`
		Process	`<Tanium Client>/TaniumCX`
		Process	`<Tanium Client>/Tools/StdUtils/TaniumExecWrapper`
		Folder	`<Tanium Client>/Tools/CertificateManager`
macOS endpoints		Process	`<Tanium Client>/python38/python`
		Process	`<Tanium Client>/TaniumCX`
		Process	`<Tanium Client>/Tools/StdUtils/TaniumExecWrapper`
		Folder	`<Tanium Client>/Tools/CertificateManager`

User role requirements

The following table lists the role permissions required to use Certificate Manager. To review a summary of the predefined roles, see Set up Certificate Manager users on page 18.

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

Certificate Manager user role permissions

Permission	Certificate Manager User[1,2]	Certificate Manager Read Only User[1,2]
Certificate Manager SHOW: View the Certificate Manager workbench USER: User access to Certificate Manager	✓ SHOW USER	✓ SHOW

Certificate Manager user role permissions (continued)

Permission	Certificate Manager User[1,2]	Certificate Manager Read Only User[1,2]
Certificate Manager Read Only Read-only access to the Certificate Manager module	✅ USER	✅ USER

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

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

Provided Certificate Manager platform content permissions

Permission	Certificate Manager user	Certificate Manager Read Only User
Action	✅ WRITE	❌
Dashboard	✅ READ	✅ READ
Filter Group	✅ READ	✅ READ
Own Action	✅ READ	❌
Package	✅ READ	✅ READ
Plugin	✅ READ EXECUTE	✅ READ EXECUTE
Saved Question	✅ READ	✅ READ
Sensor	✅ READ	✅ READ

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

Installing Certificate Manager

Before you begin

- Read the release notes.
- Review the Certificate Manager requirements on page 12.
- Assign the correct roles to users for Certificate Manager. Review the User role requirements on page 14.
    - 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

Use the Tanium Console **Solutions** page to install Certificate Manager.

When you import Certificate Manager, the following default setting is configured:

Setting	Default value
Action group	`No Computers` computer group

After the import, verify that the correct version is installed: see Verify Certificate Manager version on page 16.

To configure the Certificate Manager action group, see Configure the Certificate Manager action group on page 17.

To create scheduled actions for Certificate Manager, see Create scheduled actions for Certificate Manager on page 18.

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). See Solution dependencies.

Verify Certificate Manager version

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

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.

Configuring Certificate Manager

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.

NOTE Endpoint Configuration is installed as a part of Tanium Client Management. For more information, see the Tanium Client Management User Guide: Installing Client Management.

Optionally, you can use Endpoint Configuration to require approval of configuration changes. When configuration approvals are enabled, Endpoint Configuration does not deploy a configuration change to endpoints until a user with approval permission approves the change. For information about the roles and permissions that are required to approve configuration changes for Certificate Manager, see User role requirements on page 14. For more information about enabling and using 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.

Configure Certificate Manager

Configure the Certificate Manager action group

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.

Select the **All Windows**, **All Linux**, and **All Mac** computer groups and choose the **OR** operator.

Set up Certificate Manager users

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

To review specific permissions for each role, see User role requirements on page 14.

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

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 Certificate Manager reports and dashboard in Tanium Reporting.
- Deploy Certificate Manager packages.

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 view Certificate Manager reports and dashboard in Tanium Reporting.

In addition to the Certificate Manager roles, users must also include the following requirements:

- be assigned a basic Interact role, such as **Interact Read-Only User**
- have sufficient management rights, such as **All Computers**

Create scheduled actions for Certificate Manager

1. From the Main menu, go to **Administration > Content > Packages** and search for **Certificate**.
2. For each of the following packages, select the package and then click **Deploy Action**.
   - Certificate Audit [Non-Windows]
   - Certificate Audit [Windows]

3. In the **Deployment Schedule** section, configure the following schedule.
    - **Schedule Type**: **Recurring Deployment**
    - **Re-issue every**: 1 Days
    - **Distribute Over**: 10 Minutes

    Schedule the action to run daily.
4. In the **Targeting Criteria** section, select the **All non-Windows** or **All Windows** action group depending on which package you previously selected and then click **Show Preview To Continue**.
5. When the preview completes, click **Deploy Action** and confirm.

Configure authorized certificate authorities

To configure authorized certificate authorities, see Configure authorized certificate authorities on page 25.

Managing certificates

Certificate Manager data is visible through the Certificate Manager dashboard and reports in Tanium Reporting. Use Tanium Reporting to:

- Find expired or expiring certificates
- Identify weak cryptographic algorithms and key lengths
- View self-signed and unauthorized CA certificates
- Send certificate data using 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 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 > Dashboard** and select the **Certificate Manager** label.
2. To view the dashboard, click **Certificate Manager**.

You can also go to **Modules > Certificate Manager > Overview** to view the dashboard in Tanium Reporting.

Click on 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 about dashboards, see Tanium Reporting User Guide: Working with dashboards.

View expired certificates

1. From the Main menu, go to **Data > Reports** and select the **Certificate Manager** label.
2. To view the list of expired certificates, click **Certificate Manager - Expired Certificates**.

You can also click the **Expired Certificates** panel in the **All Certificates** section of the Certificate Manager dashboard.

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.

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 21 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 **Data > Reports** and select the **Certificate Manager** label.
2. To view the list of expiring certificates, click **Certificate Manager - Certificates Expiring within 30 Days**.

You can also click the **Expiring within 30 Days** panel in the **All Certificates** section of the Certificate Manager dashboard.

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 21 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 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**.

   BEST PRACTICE

   Schedule this connection to run at least weekly.

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

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 certificates that use a **Public Key Bit Size** less than 256.

View all certificates that use short keys

1. From the Main menu, go to **Data > Reports** and select the **Certificate Manager** label.
2. Click **Certificate Manager - Short Keys** to view the certificates that use a **Public Key Bit Size** less than 256.

You can also click the **Total Short Keys** panel in the **All Certificates** section of the Certificate Manager dashboard.

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 Signature Hash Algorithms** to view the certificates that use the sha1 or md5 **Signature Hash Algorithm**.

View all certificates that use weak signatures

1. From the Main menu, go to **Data > Reports** and select the **Certificate Manager** label.
2. Click **Certificate Manager - Weak Signatures** to view the certificates that use the sha1 or md5 **Signature Hash Algorithm**.

You can also click the **Weak Signature Hash Algorithms** panel in the **All Certificates** section of the Certificate Manager dashboard.

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.

View all certificates that use a wildcard subject

1. From the Main menu, go to **Data > Reports** and select the **Certificate Manager** label.
2. Click **Certificate Manager - Wildcard Certificates** to view the certificates that use a wildcard subject.

You can also click the **Wildcard Certificates** panel in the **All Certificates** section of the Certificate Manager dashboard.

View self-signed certificates

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

View unauthorized certificates

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

After you review the list of unauthorized certificates, you can Configure authorized certificate authorities on page 25 or Add certificate exceptions on page 29.

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 Strength** report includes a **Cipher Suite** column that shows the algorithm and key length. This information is used by Certificate Manager to provide the **Cipher Suite Strength** ratings. The strength ratings are **Vulnerable**, **Acceptable**, or **Strong**.

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

View listening service certificates by cipher suite strength

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

View all certificates by cipher suite strength

1. From the Main menu, go to **Data > Reports** and select the **Certificate Manager** label.
2. Click **Certificate Manager - Cipher Inventory**.
3. Click the **Cipher Suite Strength** column to view the certificates by cipher suite strength.

Deploying certificate audits

Refresh a certificate audit on one or more endpoints by deploying a certificate audit package.

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

Deploy a certificate audit package

1. From the Main menu, go to **Administration > Content > Packages** and search for `Certificate Audit`.
2. Select **Certificate Audit [Non-Windows]** or **Certificate Audit [Windows]** and then click **Deploy Action**.
3. In the **Targeting Criteria** section, choose an option to target one or more endpoints and then click **Show Preview to Continue**.

   To run the certificate audit on all endpoints, select **All non-Windows** or **All Windows** for **Action Group**.
4. Verify the list of targeted endpoints and then click **Deploy Action**.

Verify that a certificate audit completed successfully

1. From the Main menu, go to **Administration > Actions > Action History** and search for `Certificate Audit`.
2. Select 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 33.

Configure certificate port exceptions

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 **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**.
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 **All non-Windows** or **All Windows** for **Action Group**.
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 **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 **All non-Windows** or **All Windows** for **Action Group**.
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 24 manually, or wait until the next **Certificate Audit [Non-Windows]** and **Certificate Audit [Windows]** scheduled actions run.

Configure authorized 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 to the audit package.

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.

```
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
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.

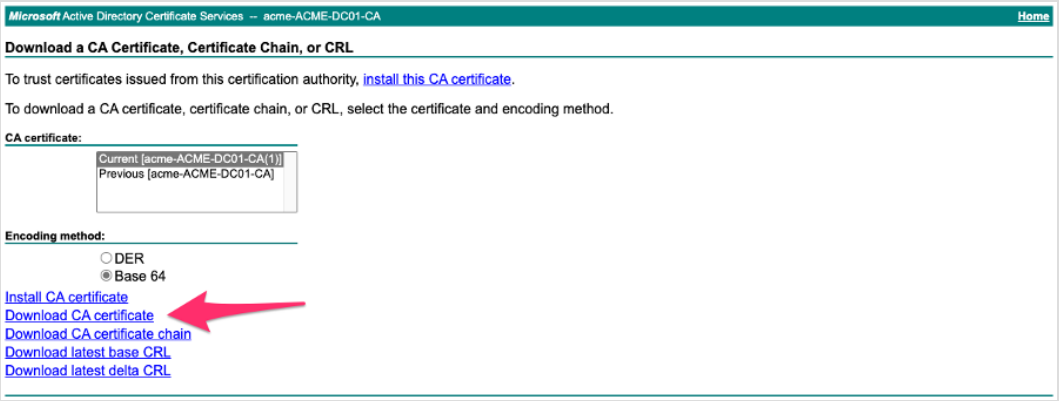
Obtain your internal CA certificates

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`.

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 26, you can rename the `certnew.crt` file to `trusted_root_certificate_authorities.pem` and create a blank `trusted_intermediate_certificate_authorities.pem` file.

Add the files to the packages in Tanium

1. From the Main menu, go to **Administration > Content > Packages** and search for `Certificate Audit`.
2. For each of the following packages, select the package and then click **Edit**.
   - Certificate Audit [Non-Windows]
   - Certificate Audit [Windows]
3. In the **Files** section, click **Add File > Local Files** to add the `trusted_root_certificate_authorities.pem` and `trusted_intermediate_certificate_authorities.pem` files and then click **Save**.

> IMPORTANT If you upgrade Certificate Manager, you must Add the files to the packages in Tanium on page 28 and Update and reissue scheduled actions on page 28 again.

Update and reissue scheduled actions

After you add the two PEM files to the packages, you must update the source packages. You can then either reissue the scheduled actions manually or wait for the next scheduled actions to run.

1. From the Main menu, go to **Administration > Actions > Scheduled Actions** and search for **Certificate**.
2. For each of the following scheduled actions, click Update source package to get the latest source package.
    - Certificate Audit [Non-Windows]
    - Certificate Audit [Windows]
3. For each of the following scheduled actions, select the package and then click **Reissue**.
    - Certificate Audit [Non-Windows]
    - Certificate Audit [Windows]
4. In the **Targeting Criteria** section, click **Show Preview To Continue** and then click **Reissue Action**.
5. View unauthorized certificates on page 23 to verify that there are fewer unauthorized certificates.

Add certificate exceptions

If you want to manually add known certificates for Certificate Manager to consider as authorized certificates, you can create a `customer-exceptions.csv` file to add to the certificate audit packages.

1. Create a comma-separated `customer-exceptions.csv` file with the following columns:
    - Thumbprint
    - Subject
    - Reason for exception
    - Date added
2. From the Main menu, go to **Administration > Content > Packages** and search for `Certificate Audit`.
3. For each of the following scheduled actions, select the package and then click **Edit**.
    - Certificate Audit [Non-Windows]
    - Certificate Audit [Windows]
4. In the **Files** section, click **Add File > Local Files**, click **Browse for Files** to select the `customer-exceptions.csv` file that you created, and then click **Save**.
5. From the Main menu, go to **Administration > Actions > Scheduled Actions** and search for **Certificate**.
6. For each of the following scheduled actions, click Update source package to get the latest source package.
    - Certificate Audit [Non-Windows]
    - Certificate Audit [Windows]
7. Deploy a certificate audit package on page 24 and View unauthorized certificates on page 23 to verify that there are fewer unauthorized certificates.

Maintaining Certificate Manager

Perform regular maintenance tasks to ensure that Certificate Manager successfully performs scheduled activities on all the targeted 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

1. From the Main menu, go to **Modules > Certificate Manager > Overview**.
2. In the Overview section, review the **Certificate Manager Coverage** panel for endpoints with the **Needs Attention** status.
3. To investigate issues, see Monitor and troubleshoot Certificate Manager Coverage on page 30.
4. To troubleshoot other Certificate Manager issues, see Troubleshooting Certificate Manager on page 32.

Perform as-needed maintenance

Check scheduled Connect connections

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

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 Create scheduled actions for Certificate Manager on page 18. • Deploy a certificate audit package on page 24.
Audit scan timed out	Contact Tanium Support on page 33 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.

Contributing factor	Corrective action
Certificate Audit has not been run	• Verify that a certificate audit completed successfully on page 24. • Deploy a certificate audit package on page 24 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 33 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 33.
• 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**.

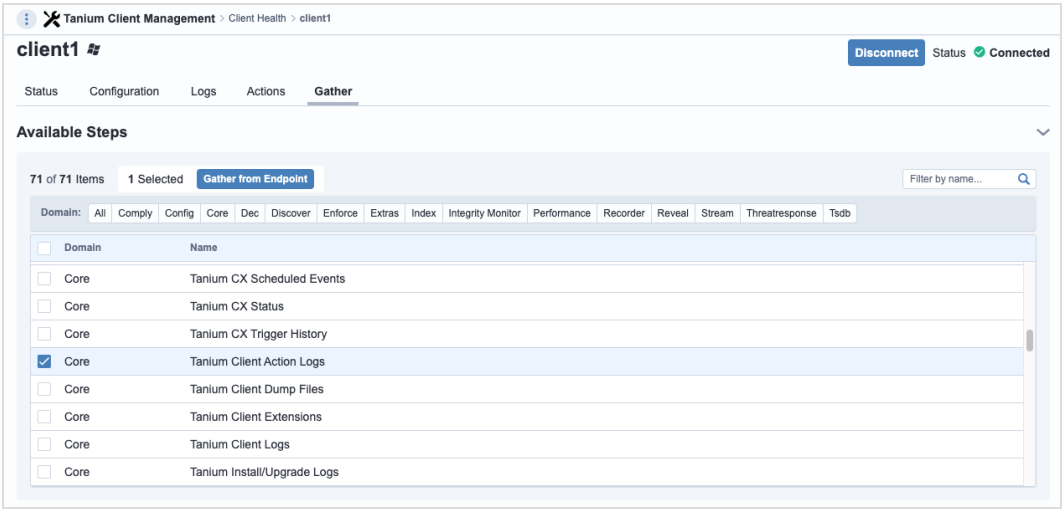
Troubleshooting Certificate Manager

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

Collect logs

Collect the action log and other tools files from the 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.



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 33.

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 include the following requirements:

- be assigned a basic Interact role, such as **Interact Read-Only User**
- have sufficient management rights, such as **All Computers**

For more information about Certificate Manager roles, see Set up Certificate Manager users on page 18.

Unexpected certificate audit results

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 on page 24.
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.

ERROR - lsof was not found

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 error is found in the action log: `ERROR - lsof was not found.`

Solution

Check the action log for the **Deploy Certificate Audit [Non-Windows]** action to confirm the error and then install lsof. For more information about how to view the action log, see Tanium Console User Guide: Investigate action-related issues.

Contact Tanium Support

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