Tanium™ Certificate Manager User Guide

Version 1.11.230

August 15, 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.

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.

© 2023 Tanium Inc. All rights reserved.

Table of contents

© 2023 Tanium Inc. All Rights Reserved

© 2023 Tanium Inc. All Rights Reserved

© 2023 Tanium Inc. All Rights Reserved

© 2023 Tanium Inc. All Rights Reserved

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 and the Certificate Manager **Overview** page 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 Endpoint Coverage
- 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

© 2023 Tanium Inc. All Rights Reserved

    - Lowest Cipher Strength by Listening Service Port
    - Number of Ciphers by Listening Service Port
    - Approved 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

For more information, see View the Certificate Manager dashboard in Tanium Reporting on page 27.

Certificate Manager reports

The following Certificate Manager reports are available in Tanium Reporting and the Certificate Manager **Overview** page:

- Certificate Manager - Certificate Details
- Certificate Manager - Certificates Expiring within 30 Days
- Certificate Manager - Cipher Inventory
- Certificate Manager - Current Coverage Status Details
- Certificate Manager - Expired Certificates
- Certificate Manager - Inventoried Certificates
- Certificate Manager - Listening Service Certificate Details
- Certificate Manager - Listening Service Certificates Expiring within 30 Days
- Certificate Manager - Listening Service Cipher Suite Approval
- 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

© 2023 Tanium Inc. All Rights Reserved

- 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 27.

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 32.

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 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 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

© 2023 Tanium Inc. All Rights Reserved

Certificate discovery method	Platforms	Locations	Unique capabilities	Customization
File	Linux	• `/etc/pki/*` • `/etc/ssl/*`	None	Exclusion List in Certificate Manager Settings
Windows Certificate Store	Windows	User Store for signed-in users	None	Exclusion List in Certificate Manager Settings

* 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
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 location of the certificate in a certificate store

Interoperability with other Tanium products

Certificate Manager works with Tanium Endpoint Configuration and Tanium Reporting to provide reporting of related data.

© 2023 Tanium Inc. All Rights Reserved

Endpoint Configuration

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

Reporting

View the Certificate Manager dashboard and reports 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 28.

© 2023 Tanium Inc. All Rights Reserved

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 18 and Configuring Certificate Manager on page 20.

Step 2: Manage certificates

See Managing certificates on page 27.

Step 3: Deploy certificate audits

See Deploying certificate audits on page 32.

© 2023 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 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 13 and Feature-specific dependencies on page 14. 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™ Endpoint Configuration 1.7.151 or later
- Tanium Reporting 1.13.76 or later
- Tanium™ RDB Service 1.2.211 or later

© 2023 Tanium Inc. All Rights Reserved

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 OpenSSL 1.0.1 or later. For more information, see Error: EC_KEY_new_by_curve_name on page 38. Requires lsof to capture owning process data. For more information, see ERROR - lsof was not found on page 38.

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.

© 2023 Tanium Inc. All Rights Reserved

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 21.

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

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

© 2023 Tanium Inc. All Rights Reserved

Certificate Manager user role permissions

Permission	Certificate Manager Operator[1,2,3]	Certificate Manager User[2,3]	Certificate Manager Read Only User[2,3]
Certificate Manager SHOW: View the Certificate Manager workbench USER: User access to Certificate Manager	✓ SHOW USER	✓ SHOW USER	✓ SHOW
Certificate Manager Config View, update, or distribute the Certificate Manager configuration	✓ READ WRITE EXECUTE	✓ READ	✓ READ
Certificate Manager Read Only Read-only access to the Certificate Manager module	✓ USER	✓ USER	✓ USER

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

[2] 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.

[3] 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 administration and platform content permissions

Permission	Permission Type	Certificate Manager Operator	Certificate Manager User	Certificate Manager Read Only User
Action Group	Administration	✓ READ	✓ READ	✓ READ
Action	Platform Content	✓ WRITE	✓ WRITE	✗

© 2023 Tanium Inc. All Rights Reserved

Provided Certificate Manager administration and platform content permissions (continued)

Permission	Permission Type	Certificate Manager Operator	Certificate Manager User	Certificate Manager Read Only User
Dashboard	Platform Content	READ	READ	READ
Filter Group	Platform Content	READ	READ	READ
Own Action	Platform Content	READ	READ	
Package	Platform Content	READ	READ	READ
Plugin	Platform Content	READ EXECUTE	READ EXECUTE	READ EXECUTE
Saved Question	Platform Content	READ	READ	READ
Sensor	Platform Content	READ	READ	READ

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

© 2023 Tanium Inc. All Rights Reserved

Installing Certificate Manager

Before you begin

- Read the release notes.
- Review the Certificate Manager requirements on page 13.
- Assign the correct roles to users for Certificate Manager. Review the User role requirements on page 15.
    - 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

(Tanium Core Platform 7.4.5 or later only) 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: Dependencies, default settings, and tools deployment.

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

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: see Verify Certificate Manager version on page 19.

© 2023 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** check box while performing the steps in Tanium Console User Guide: Import, re-import, or update specific solutions. After the import, verify that the correct version is installed: see Verify Certificate Manager version on page 19.

To configure the Certificate Manager action group, see Configure the Certificate Manager action group on page 21.

To configure the Certificate Manager audit settings, see Configure audit settings on page 22.

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.

Upgrade Certificate Manager

For the steps to upgrade Certificate Manager, see Tanium Console User Guide: Import, re-import, or update specific solutions. After the upgrade, verify that the correct version is installed: see Verify Certificate Manager version on page 19.

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 22.
- Authorized certificate authorities (CAs): To reconfigure any custom CAs, see Configure certificate authorities on page 23.
- 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:

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.

© 2023 Tanium Inc. All Rights Reserved

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 For information about installing Endpoint Configuration, see Tanium Endpoint Configuration User Guide: Installing Endpoint Configuration.

Optionally, you can use Endpoint Configuration to require approval of configuration changes. When configuration approvals are enabled, Endpoint Configuration does not deploy a configuration change to endpoints until a user with approval permission approves the change. For information about the roles and permissions that are required to approve configuration changes for Certificate Manager, see User role requirements on page 15. 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.

If you enabled configuration approvals, the following configuration changes must be approved in Endpoint Configuration before they deploy to 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

© 2023 Tanium Inc. All Rights Reserved

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.

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.

To review specific permissions for each role, see User role requirements on page 15.

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.
- Deploy Certificate Manager packages.

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:

© 2023 Tanium Inc. All Rights Reserved

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

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

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

Configure audit settings

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 do not need increased details around listening ports and ciphers, clear the **Enable Listen 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.

Configure exclusion list

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 9.

© 2023 Tanium Inc. All Rights Reserved

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, select it from the dropdown list, click **Add Exclusion**, enter an optional note, and then click **Submit**.

   TIP You can continue entering additional certificates before you click **Add Exclusion**.
3. 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**.
   b. To activate an inactive exclusion, select it and then click **Activate Exclusion**.
   c. To add or edit a note for a certificate, select it, click **Edit Note**.
   d. If you no longer need to exclude a specific certificate, select one or more exclusions 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.

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
```

© 2023 Tanium Inc. All Rights Reserved

```
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
```

© 2023 Tanium Inc. All Rights Reserved

```
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.

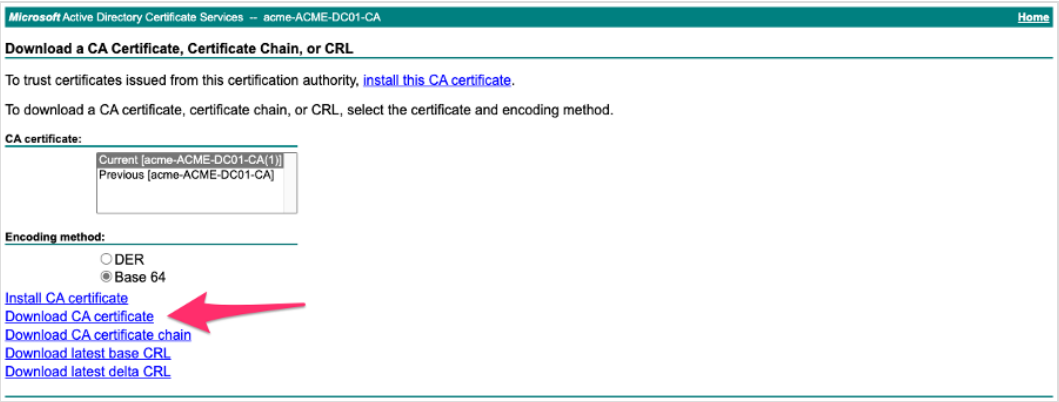
Obtain your internal CA certificates

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.

   TIP 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.

© 2023 Tanium Inc. All Rights Reserved

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 23, 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

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**.
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 it, click **Edit Authority**, clear the **Enabled** option, and then click **Submit**.
   b. To activate an inactive exclusion, select it, click **Edit Authority**, select the **Enabled** option, and then click **Submit**.
   c. To delete a CA, select one or more CAs and then click Delete.

Configure approved ciphers

Certificate Manager pre-populates the approved cipher suites based on National Institute of Standards and Technology (NIST) guidelines. Approval status appears in Certificate Manager dashboards and reports. If your organization has a policy for acceptable cipher suites, you can add or remove approvals based on your organization policy.

1. From the Main menu, go to **Modules > Certificate Manager > Overview**, click Settings, and then click the **Approved Ciphers** tab.
2. 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**.
   b. To remove an approval for a cipher suite, select one with an **Approved** status, and then click **Remove Approval**.

© 2023 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 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**.

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.

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.

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

© 2023 Tanium Inc. All Rights Reserved

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 28 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 28 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**.

Schedule this connection to run at least weekly.

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

© 2023 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.

© 2023 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

1. From the Main menu, go to **Modules > Certificate Manager > Overview**.
2. In the **Listening SSL/TLS Services Certificate and Cipher Inventory** section, click **Unauthorized** 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 23 or Configure exclusion list on page 22.

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 **Lowest Cipher Strength by Listening Service Port** to view the certificates by cipher suite strength.

This data comes from the**Certificate Manager - Minimum Cipher Suite Strength by Port**report in Tanium Reporting.

© 2023 Tanium Inc. All Rights Reserved

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.

© 2023 Tanium Inc. All Rights Reserved

Deploying certificate audits

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.

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 **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.
    b. Update the **Listen Port Scan Timeout** if needed.
    c. 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**.

    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 21.
5. 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 37.

Configure certificate port exceptions

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

© 2023 Tanium Inc. All Rights Reserved

- **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**.

   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 21.
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**.

   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 21.
5. Verify the list of targeted endpoints and then click **Deploy Action**.

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 32 manually, or wait until the next **Certificate Audit [Non-Windows]** and **Certificate Audit [Windows]** scheduled actions run.

© 2023 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 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 Endpoint Coverage** panel for endpoints with the **Needs Attention** status.
3. To investigate issues, see Monitor and troubleshoot Certificate Manager Coverage on page 34.
4. To troubleshoot other Certificate Manager issues, see Troubleshooting Certificate Manager on page 36.

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 Configuring Certificate Manager on page 20. • Deploy a certificate audit package on page 32.

© 2023 Tanium Inc. All Rights Reserved

Contributing factor	Corrective action
Audit scan timed out	Contact Tanium Support on page 38 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 32. • Deploy a certificate audit package on page 32 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 38 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 38.
• 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**.

© 2023 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.

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 38.

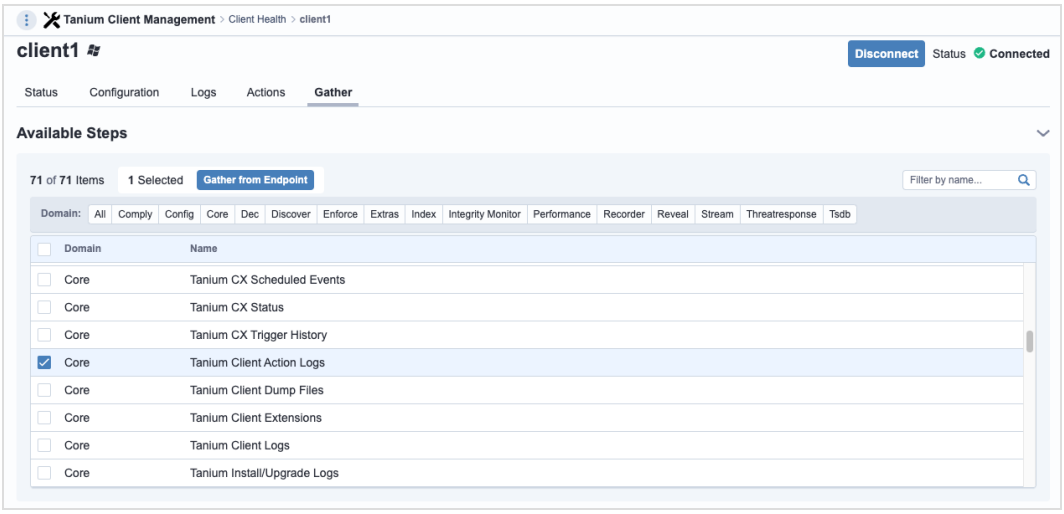
Tanium Certificate Manager maintains logging information in the `Certificate Manager.log` file in the `\Program Files\Tanium\Tanium Module Server\services\Certificate Manager` directory.

Collect action 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.

© 2023 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 38.

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 21.

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.

© 2023 Tanium Inc. All Rights Reserved

Solution

1. Verify that a certificate audit completed successfully on page 32.
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: EC_KEY_new_by_curve_name

Issue

Older Linux endpoints with OpenSSL versions earlier 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.

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.

Uninstall Certificate Manager

1. From the Main menu, go to **Administration > Configuration > Solutions**.
2. Select the check box 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 https://support.tanium.com.

© 2023 Tanium Inc. All Rights Reserved