Tanium™ Network Quarantine User Guide

Version 1.3.1

January 21, 2022

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

Network Quarantine overview **6**

NAC devices 6

Automated rules 6

Product integration 6

Tanium™ Connect 6

Tanium Discover 6

Getting started **7**

Step 1: Install Network Quarantine 7

Step 2: Configure a NAC 7

Step 3: (Optional) Configure notifications 7

Step 4: Quarantine endpoints 7

Network Quarantine requirements **8**

Core platform dependencies 8

Solution dependencies 8

Tanium recommended installation 8

Import specific solutions 8

Feature-specific dependencies 8

Tanium Module Server 9

Endpoints 9

Supported internet protocols 9

Supported operating systems 9

Third-party software 9

Host and network security requirements 9

Ports 9

User role requirements 9

Installing Network Quarantine **13**

Before you begin 13

Import Network Quarantine with default settings ... 13
Import Network Quarantine with custom settings ... 13
Manage solution dependencies ... 14
Upgrade Network Quarantine ... 14
Verify Network Quarantine version ... 14
Configuring Network Quarantine ... **15**
Configure Network Quarantine ... 15
Configure service account ... 15
Set up Network Quarantine users ... 15
Configuring NACs ... **18**
Cisco Identity Services Engine (ISE) pxGrid NAC ... 18
Create server and client self-signed certificates ... 18
Generate a signed certificate ... 18
Configure certificates in Network Quarantine ... 18
Configure pxGrid NAC ... 20
What to do next ... 23
Quarantining endpoints ... **24**
Quarantine with automated rules ... 24
Add saved questions to Network Quarantine content set ... 24
Create an automated rule ... 25
View and act on violations ... 25
Configure global rule settings ... 26
Quarantine an individual MAC address ... 26
Quarantine in Discover ... 26
Configuring notifications ... **27**
Prerequisites ... 27
Configure notifications in Connect ... 27
Troubleshooting Network Quarantine ... **29**
Collect logs ... 29
Configure log levels ... 29

View audit log 29
Fix SASLError not-authorized error 29
Problem 29
Solution 30
Uninstall Network Quarantine 30
Contact Tanium Support 30

Network Quarantine overview

With Network Quarantine, you can use your existing Network Access control (NAC) solution to control the communication of both managed and unmanaged endpoints (controlling unmanaged endpoints requires Tanium™ Discover).

NAC devices

With the Network Quarantine service, Tanium products can communicate with a NAC to isolate endpoints. Network Quarantine is supported for use with Cisco Identity Services Engine (ISE) to block by MAC address.

For more information, see Configuring NACs on page 18.

Automated rules

If you are using ISE, you can create automated rules to find endpoints that need to be quarantined. Automated rules use saved questions to identify endpoints that are causing violations. You can then quarantine these endpoints. For more information, see Quarantine with automated rules on page 24.

Product integration

Tanium™ Connect

Network Quarantine generates events when the NAC starts or stops, or when an endpoint is quarantined. You can send notifications about these events to destinations such as email, security information and event management (SIEM) software, or a file by creating a connection in Connect. For more information, see Configuring notifications on page 27.

Tanium Discover

When the Network Quarantine service is configured with Tanium Discover, you can also quarantine a MAC address directly from the Discover **Interfaces** pages. For more information, see the Tanium Discover User Guide.

Getting started

Step 1: Install Network Quarantine

Install Network Quarantine.

For more information, see Installing Network Quarantine on page 13.

Step 2: Configure a NAC

Configure a network access control (NAC) solution.

For more information, see Configuring NACs on page 18.

Step 3: (Optional) Configure notifications

You can optionally configure notifications about NAC start and stop events or quarantine events.

For more information, see Configuring notifications on page 27.

Step 4: Quarantine endpoints

Quarantine endpoints.

For more information, see Quarantining endpoints on page 24.

If you set up integration with Tanium™ Discover, you can also quarantine endpoints from the Discover workbench.

Network Quarantine requirements

Review the requirements before you install and use Network Quarantine.

Core platform dependencies

Make sure that your environment meets the following requirements:

- **Tanium™ Core Platform servers:**
  - 7.3.314.4250 or later
  - 7.4.1.1939 or later

  Network Quarantine is not supported for use with Tanium Core Platform 7.5.x or later.

Solution dependencies

Other Tanium solutions are required for specific Network Quarantine 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 Network Quarantine dependencies have their own dependencies, which you can see by clicking the links in the list of Feature-specific dependencies on page 8. Note that the links open the user guides for the latest version of each solution, not necessarily the minimum version that Network Quarantine requires.

Tanium recommended installation

If you select **Tanium Recommended Installation** when you import Network Quarantine, 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 Network Quarantine to import, you must manually import dependencies. See Tanium Console User Guide: Import, re-import, or update specific solutions.

Feature-specific dependencies

Network Quarantine has the following feature-specific dependencies at the specified minimum versions:

- Tanium Connect 4.7.4 or later to send notifications about NAC events to destinations.
- Tanium Discover 2.7.0 or later to quarantine a MAC address directly from the Discover **Interfaces** pages.

Tanium Module Server

Network Quarantine is installed and runs as a service on the Module Server host computer. The impact on Module Server is minimal and depends on usage.

Endpoints

Supported internet protocols

Network Quarantine supports only IPv4 addresses.

Supported operating systems

Same as Tanium Client support. See Tanium Client Management User Guide: Client version and host system requirements.

Third-party software

Network Quarantine is supported for use with Cisco Identity Services Engine (ISE) 2.2 - 2.7 with Cisco Platform Exchange Grid (pxGrid) installed.

Cisco ISE 3.x or later and pxGrid 2.0 or later are not supported.

Host and network security requirements

Specific ports and processes are needed to run Network Quarantine.

Ports

The following ports are required for Network Quarantine communication.

Source	Destination	Port	Protocol	Purpose
Module Server	Module Server (loopback)	17467	TCP	Internal purposes; not externally accessible.
	Cisco ISE	5222	TCP	Access to Cisco ISE, unless specified otherwise.

User role requirements

The following tables list the role permissions required to use Network Quarantine. To review a summary of the predefined roles, see Set up Network Quarantine users on page 15.

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

Network Quarantine user role permissions

Permission	Network Quarantine Administrator	Network Quarantine Approver	Network Quarantine Rule Author	Network Quarantine User	Network Quarantine Read Only User	Network Quarantine Service Account
Network Quarantine Certificates View, add or update configured certificates	✓ READ WRITE	✗	✗	✗	✗	✗
Network Quarantine Nacauditlog View audit log	✓ READ	✓ READ	✓ READ	✓ READ	✗	✗
Network Quarantine NACs View, add or update configured NACs	✓ READ WRITE	✓ READ	✓ READ	✓ READ	✗	✗
Network Quarantine Quarantines View, quarantine or unquarantine quarantined endpoints	✓ READ WRITE	✓ READ	✓ READ	✓ READ WRITE	✓ READ	✗
Network Quarantine Requests View, approve and deny quarantine requests	✓ APPROVE READ DENY	✓ APPROVE READ DENY	✓ APPROVE READ DENY	✗	✗	✗
Network Quarantine Rules View and edit rules and targets; use service account to evaluate rules; start rule evaluation process	✓ READ WRITE RUN	✓ READ	✓ READ WRITE RUN	✗	✗	✓ EVALUATE
Network Quarantine Runs View rule evaluation runs	✓ READ	✓ READ	✓ READ	✗	✗	✗

Network Quarantine user role permissions (continued)

Permission	Network Quarantine Administrator	Network Quarantine Approver	Network Quarantine Rule Author	Network Quarantine User	Network Quarantine Read Only User	Network Quarantine Service Account
Network Quarantine Settings View and configure service settings	✓ READ WRITE	✓ READ	✓ READ WRITE	✓ READ	✓ READ	✗
Networkquarantine View Network Quarantine shared service	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW	✗

Provided Network Quarantine administration and platform content user role permissions

Permission	Role type	Network Quarantine Administrator	Network Quarantine Approver	Network Quarantine Rule Author	Network Quarantine User	Network Quarantine Read Only User	Network Quarantine Service Account
Computer Group	Administration	✓ READ	✓ READ	✓ READ	✗	✗	✓ READ
User	Administration	✓ READ	✗	✓ READ	✗	✗	✗
Plugin	Platform content	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE
Saved Question	Platform content	✓ READ	✗	✓ READ	✗	✗	✓ READ WRITE
Sensor	Platform content	✓ READ	✗	✓ READ	✗	✗	✓ READ

Optional roles for Network Quarantine

Role	Enables
Connect User	For signed in user: • Configure connections for Network Quarantine event notifications For service account: • Send Network Quarantine event notifications

For more information and descriptions of content sets and permissions, see the Tanium Core Platform User Guide: Users and user groups.

Installing Network Quarantine

Use the Tanium Console **Solutions** page to install Network Quarantine and choose either automatic or manual configuration:

- **Automatic configuration with default settings** (Tanium Core Platform 7.4.2 or later only): Network Quarantine is installed with any required dependencies and other selected products. After installation, the Tanium Server automatically configures the recommended default settings. This option is the best practice for most deployments. For more information about the automatic configuration for Network Quarantine, see Import Network Quarantine with default settings on page 13.
- **Manual configuration with custom settings**: After installing Network Quarantine, you must manually configure required settings. Select this option only if Network Quarantine requires settings that differ from the recommended default settings. For more information, see Import Network Quarantine with custom settings on page 13.

Before you begin

- Read the release notes.
- Review the Network Quarantine requirements on page 8.
    - To import the Network Quarantine solution, you must be assigned the Administrator reserved role or a role that has the **Import Signed Content** permission.
    - To configure the Network Quarantine action group, you must be assigned the Administrator reserved role, Content Administrator reserved role, or a role that has the **Write Action Group** permission.

Import Network Quarantine with default settings

When you import Network Quarantine with automatic configuration, the following default setting is configured:

Setting	Default value
Service account	The service account is set to the account that you used to import the shared service. Configuring a unique service account for each Tanium solution is an extra security measure to consider in consultation with the security team of your organization. See Configure service account on page 15.

To import Network Quarantine 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 Network Quarantine version on page 14.

Import Network Quarantine with custom settings

To import Network Quarantine 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 Network Quarantine version on page 14.

To configure the service account, see Configure service account on page 15.

Manage solution dependencies

When you start the Network Quarantine workbench for the first time, the Tanium Server checks whether all the Tanium modules and shared services (solutions) that are required for Network Quarantine are installed at the required versions. The Network Quarantine workbench cannot load unless all required dependencies are installed. If you selected **Tanium Recommended Installation** when you imported Network Quarantine, the Tanium Server automatically imported all your licensed solutions at the same time. Otherwise, if you manually imported Network Quarantine and did not import all its dependencies, the Tanium Console displays a banner that lists the dependencies and the required versions. See Solution dependencies.

Perform the following steps if a banner indicates any Network Quarantine dependencies are not installed:

1. Install the dependencies as described in Tanium Console User Guide: Import, re-import, or update specific solutions.
2. From the Main menu, go to **Modules > Network Quarantine** to open the Network Quarantine **Overview** page and verify that the Console no longer displays a banner to list missing dependencies.

Upgrade Network Quarantine

For the steps to upgrade Network Quarantine, see Tanium Console User Guide: Import, re-import, or update specific solutions. After the upgrade, verify that the correct version is installed: see Verify Network Quarantine version on page 14.

Verify Network Quarantine version

After you import or upgrade Network Quarantine, verify that the correct version is installed:

1. Refresh your browser.
2. From the Main menu, go to **Administration > Shared Services > Network Quarantine** to open the Network Quarantine **Overview** page.
3. To display version information, click Info  .

Configuring Network Quarantine

If you did not install Network Quarantine with the **Apply All Tanium recommended configurations**, you must enable and configure certain features.

Configure Network Quarantine

Configure service account

The service account is a user that runs several background processes for Network Quarantine. This user requires the following roles and access:

- **Network Quarantine Service Account** role
- **Connect User** role, to send notifications with Connect
- Access to the saved questions that are used for the automated rules

For more information about Network Quarantine permissions, see User role requirements on page 9.

> NOTE If you imported Network Quarantine with default settings, the service account is set to the account that you used to perform the import. Configuring a unique service account for each Tanium solution is an extra security measure to consider in consultation with the security team of your organization.

1. On the Network Quarantine **Overview** page, click Settings and then click **Service Account** if needed.
2. Provide a user name and password, and then click **Save**.

Set up Network Quarantine users

You can use the following set of predefined user roles to set up Network Quarantine users.

To review specific permissions for each role, see User role requirements on page 9.

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

Network Quarantine Administrator

Assign the **Network Quarantine Administrator** role to users who manage the configuration and deployment of Network Quarantine functionality, including configuration of certificates and NACs.
This role can perform the following tasks:

- Configure Network Quarantine service settings, including viewing, adding and updating configured certificates
- View, add and update NACs
- View, quarantine or unquarantine quarantined endpoints
- View, approve and deny quarantine requests

- View and edit automated rules and targets
- Start the rule evaluation process
- View the audit log

Network Quarantine Approver

Assign the **Network Quarantine Approver** role to users who manage the configuration and deployment of Network Quarantine functionality but do not need to configure certificates or NACs.
This role can perform the following tasks:

- View Network Quarantine service settings, except for configured certificates
- View configured NACs
- View quarantined endpoints
- View, approve and deny quarantine requests
- View automated rules and targets
- View rule evaluation runs
- View the audit log

Network Quarantine Rule Author

Assign the **Network Quarantine Rule Author** role to users who manage automated rules for and quarantine requests for Network Quarantine.
This role can perform the following tasks:

- View Network Quarantine service settings, except for configured certificates
- View configured NACs
- View quarantined endpoints
- View, approve and deny quarantine requests
- View and edit automated rules and targets
- Start the rule evaluation process and view rule evaluation runs
- View the audit log

Network Quarantine User

Assign the **Network Quarantine User** role to users who need to view Network Quarantine details and quarantine or unquarantine endpoints.
This role can perform the following tasks:

- View Network Quarantine service settings, except for configured certificates
- View configured NACs
- View, quarantine or unquarantine quarantined endpoints
- View, approve and deny quarantine requests
- View the audit log

Network Quarantine Read Only User

Assign the **Network Quarantine Read Only User** role to users who need to view quarantined endpoints.
This role can perform the following tasks:

- View Network Quarantine service settings, except for configured certificates and NACs
- View configured NACs
- View quarantined endpoints

Network Quarantine Service Account

Assign the **Network Quarantine Service Account** role to the account that configures system settings for Network Quarantine.
This role can perform several background processes for Network Quarantine, including evaluating rules.

Configuring NACs

Configure Cisco Identity Services Engine (ISE) pxGrid NAC. After a NAC is configured, you can begin to quarantine endpoints.

To create or edit NAC configurations, you must have the Network Quarantine Administrator role. See User role requirements on page 9.

Cisco Identity Services Engine (ISE) pxGrid NAC

To configure a Cisco ISE pxGrid NAC, you can either use self-signed or server-signed certificates. After you configure the NAC, you can quarantine specific MAC addresses with the Adaptive Network Control (ANC) policies that are configured in ISE.

You can sign in to ISE with the user interface or with SSH.

Create server and client self-signed certificates

ISE can work with self-signed certificates for both server authentication and client authentication.

1. Get a self-signed certificate from the server. In the ISE UI, go to **Administration > Certificates > System Certificates**. If you need the certificate, export the public certificate from the UI.
2. Generate a self-signed certificate for the client.
    a. See Cisco Communities: Deploying Certificates with pxGrid.
    b. In the ISE UI, go to **Administration > Certificates > System Certificates** and upload the certificate into the **Trusted Certificates** section.
3. If you changed pxGrid certificates, restart the ISE server. See Cisco ISE Client Commands: Start/stop commands.
4. Make sure that you have the server certificate, client certificate, and client key to create the certificate configuration in Network Quarantine.

Generate a signed certificate

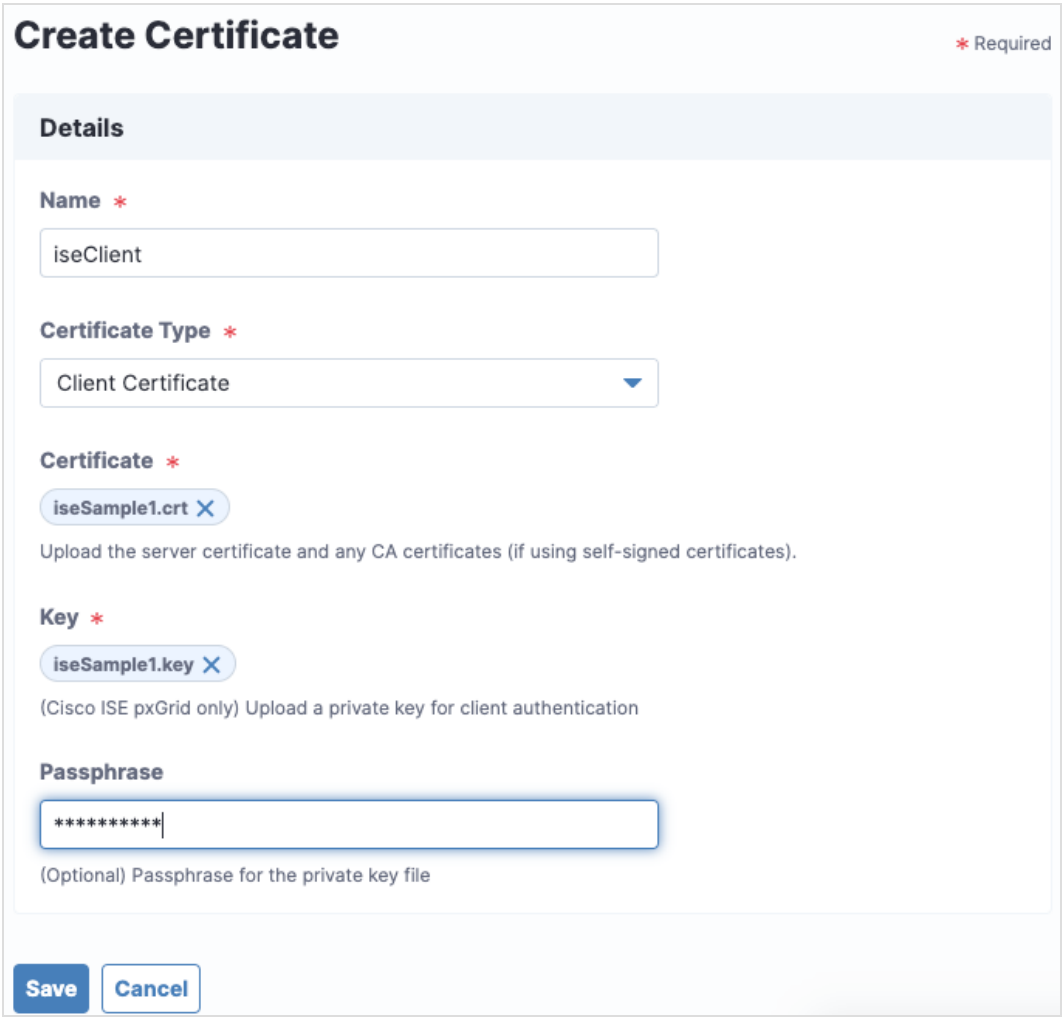
Generate a pxGrid certificate to provide as the certificate authority (CA) when you configure the NAC in Network Quarantine.

1. In the pxGrid UI, go to **Administration > pxGrid Services > Certificates**. Generate a single certificate (without a certificate signing request). For the Common Name (CN), use any identifying value, such as IP address. Choose the PEM download format. Enter a password for the certificate.
2. Click **Create** to download a ZIP file that contains the server certificate. Extract this ZIP file to get the server certificate that you need to configure in Network Quarantine.

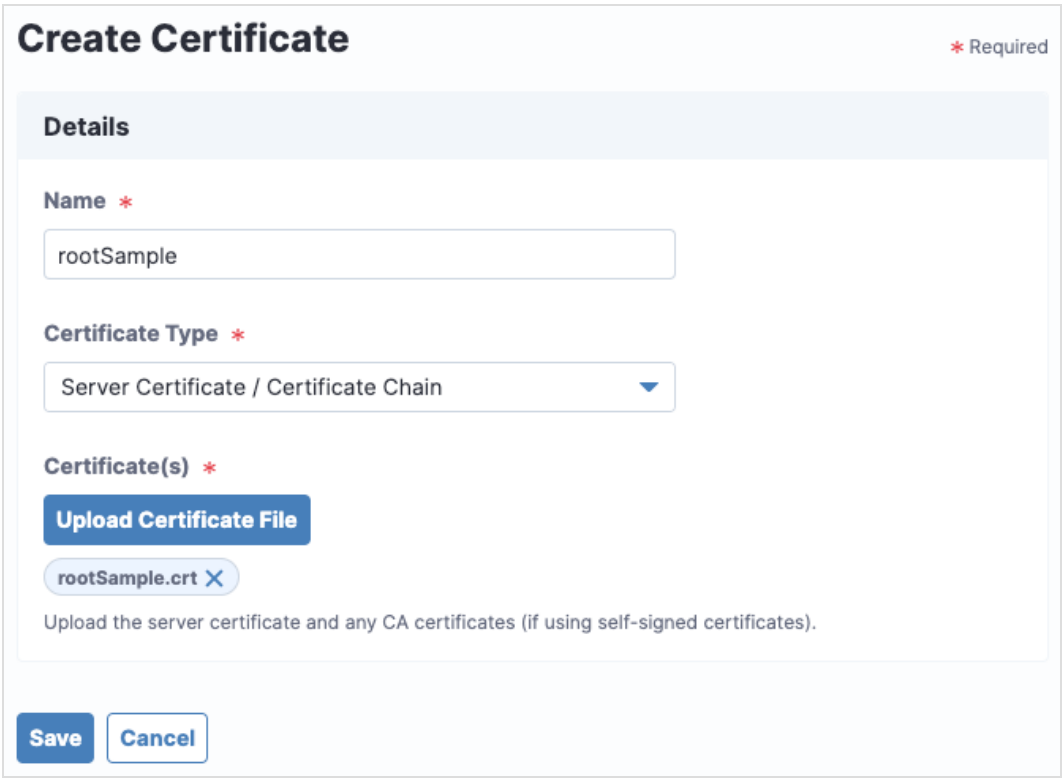
Configure certificates in Network Quarantine

Create the client and server certificates in Network Quarantine.

1. From the Network Quarantine menu, go to **Configuration > Certificates**.
2. Create the client certificate.
    a. Click **Create Certificate**.
    b. Specify a name for the certificate.
    c. For **Certificate Type**, select **Client Certificate**.
    d. Upload the client certificate and key files.
    e. If required, provide the passphrase for the private key file.
    f. Click **Save**.



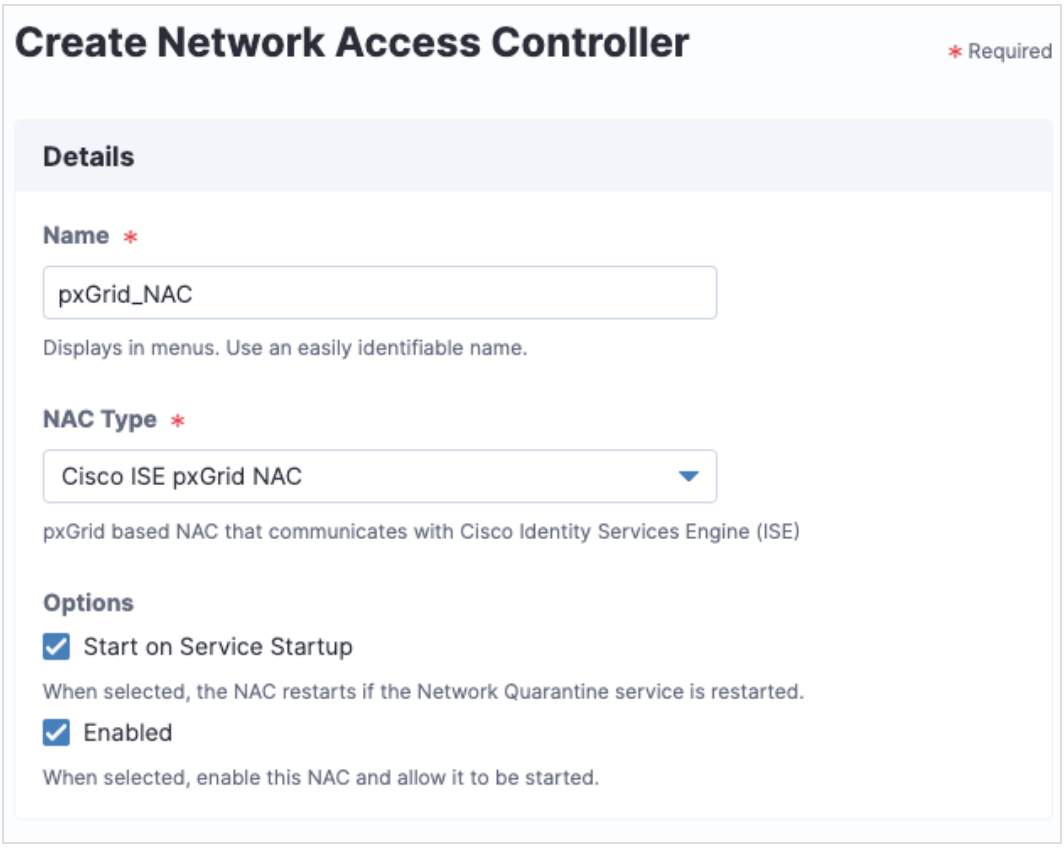
3. Create the server certificate.
    a. Click **Create Certificate**.
    b. Specify a name for the certificate.
    c. For **Certificate Type**, select **Server Certificate / Certificate Chain**.
    d. Upload the pxGrid certificate that you created in the pxGrid web admin UI. Click **Save**.



Configure pxGrid NAC

1. From the Network Quarantine menu, go to **Configuration > NACs > Create NAC**.
2. Specify a display name.
3. For the NAC Type, select **Cisco ISE pxGrid NAC**.

4. In the **Options** section, select **Start on Service Startup** to restart the NAC when the Network Quarantine service restarts. Select **Enabled** to enable and start the NAC.



5. Specify the Cisco ISE pxGrid NAC connection details.

   a. Specify the **pxGrid User Name** and **pxGrid URI**.
   Do not modify the default **pxGrid Bind Resource**, **pxGrid Domain**, or **pxGrid Capabilities** values without guidance from Tanium or Cisco Support.

   b. If you are using a self-signed certificate, clear **Check Server Identity**.

   c. For the **Client Certificate**, select the client certificate that you configured.

   d. For the **Server Certificate Chain**, select the server certificate that you configured.

6. (Optional) Update the **IQ Timeout** and **Refresh Interval** settings.
7. Start the NAC. Select the NAC from the list and click **Start**.

To edit NAC settings, you must stop the NAC first.

What to do next

After you configure a NAC in Network Quarantine, you can begin to quarantine endpoints. See Quarantining endpoints on page 24.

Quarantining endpoints

After you configure a NAC, you can configure how endpoints are quarantined. You can set up automated rules to quarantine based on the results of a saved question on a computer group, or you can select individual MAC addresses.

Quarantine with automated rules

Automated rules use saved questions to query a computer group for a set of conditions. If an endpoint meets the conditions, it is added to the list of violations. From the violations page, you can choose to quarantine the endpoint by MAC address.

Add saved questions to Network Quarantine content set

Before you configure automated rules, you must decide on a saved question with which you are going to select the endpoints to quarantine. For example, you might create a saved question that returns endpoints that do not have a certain patch installed.

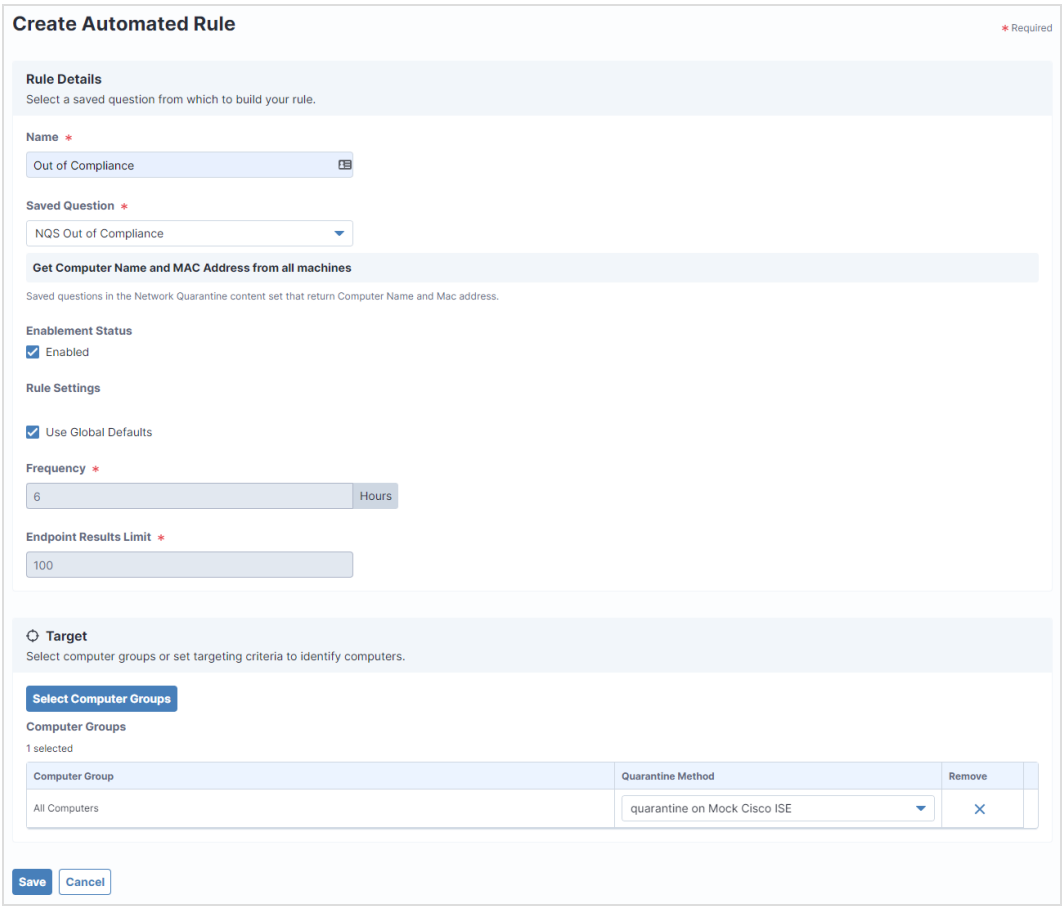
The saved question you use for a rule must meet the following requirements:

- Be in the Network Quarantine Content Set content set
- Return columns for the Computer Name and MAC Address sensors
- Be accessible by the service account user that you configured for the Network Quarantine service

To add saved question to the Network Quarantine Content Set, you can either choose the content set when you create the saved question, or you can edit a saved question to add it to the content set. For more information, see Tanium Core Platform User Guide: Edit a saved question.

Create an automated rule

1. From the Network Quarantine menu, click **Automated Rules > Add rule**.
2. Enter a name for the rule, and choose the saved question on which you want to base the rule.



3. Select **Enabled** to enable the rule to be run on the specified frequency.
4. To use custom settings for frequency and endpoint results limit, clear **Use Global Defaults**, and enter the custom values.
5. Choose targets for the rule. Configure one or more computer groups that you want to target. For each computer group, indicate which configured NAC you want to use for the quarantine method.
6. Click **Save**.
7. Rules are run on the configured frequency. To run all of the rules now, click **Run Now**.

View and act on violations

After the rules have been run, a list of computers that meet the conditions of the saved questions are returned. To view all violations, go to the **Violations** tab in the **Issues** section of the Network Quarantine **Overview** page.

- To approve the quarantine of a device that is violating a defined rule, select the endpoint and click **Approve**.
- To keep the endpoint connected, select the endpoint and click **Deny**.
- To generate a CSV list of endpoints, select the endpoints and click **Export**.

If you want to configure automated approval of quarantines, contact Tanium Support for more information.

Configure global rule settings

By default, rules are evaluated every 6 hours, and if more than 100 endpoints are returned for a rule, an event is generated. To change these global settings from the Network Quarantine **Overview** page, click Settings, then the **Automated Rules** tab.

Quarantine an individual MAC address

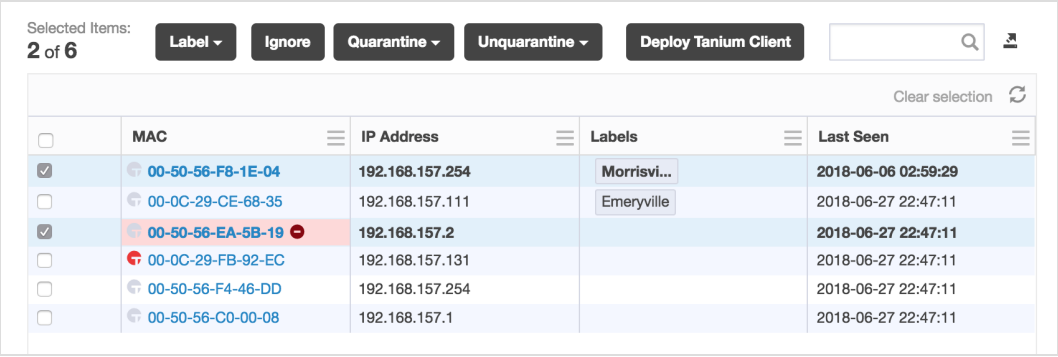
1. On the **Quarantine** tab in the **Issues** section of the Network Quarantine **Overview** page, click **Create Quarantine**.
2. Use the available options to quarantine endpoints:
    - To quarantine endpoints with a Cisco Identity Services Engine (ISE) pxGrid NAC, enter a list of MAC addresses on which to apply the quarantine and choose the quarantine method to use. The Adaptive Network Control (ANC) policies are configured in ISE.
3. Click **Save**.
4. The MAC addresses that you indicated are listed in the **Quarantine** section of the Network Quarantine **Overview** page. To disable the quarantine on the endpoint, select the MAC address and click **Remove Quarantine**.

Quarantine in Discover

If you have Tanium Discover installed, you can also quarantine and remove quarantine for a MAC address. Go to an **Interfaces** page and select the rows that relate to the endpoints that you want to quarantine, then click **Quarantine** and choose the NAC that you want to use to quarantine the endpoint.

Quarantined MAC addresses are marked as blocked.

For more information, see Tanium Discover User Guide.



Configuring notifications

You can create a connection in Tanium Connect to send a notification when the NAC starts or stops, when an endpoint is quarantined, when a rule match is returned for an endpoint, when a rule is approved or denied, and when rule match violation occurs. You can send these notifications to destinations such as email, SIEM, or Splunk.

Prerequisites

- You must have Connect installed. For more information, see Tanium Connect User Guide: Installing Tanium Connect.
- You must have the **Connect User** role to create a connection, and the Network Quarantine service account must have the **Connect User** role to send notifications. For more information about configuring user roles, see Tanium Core Platform User Guide: Assign roles to a user.

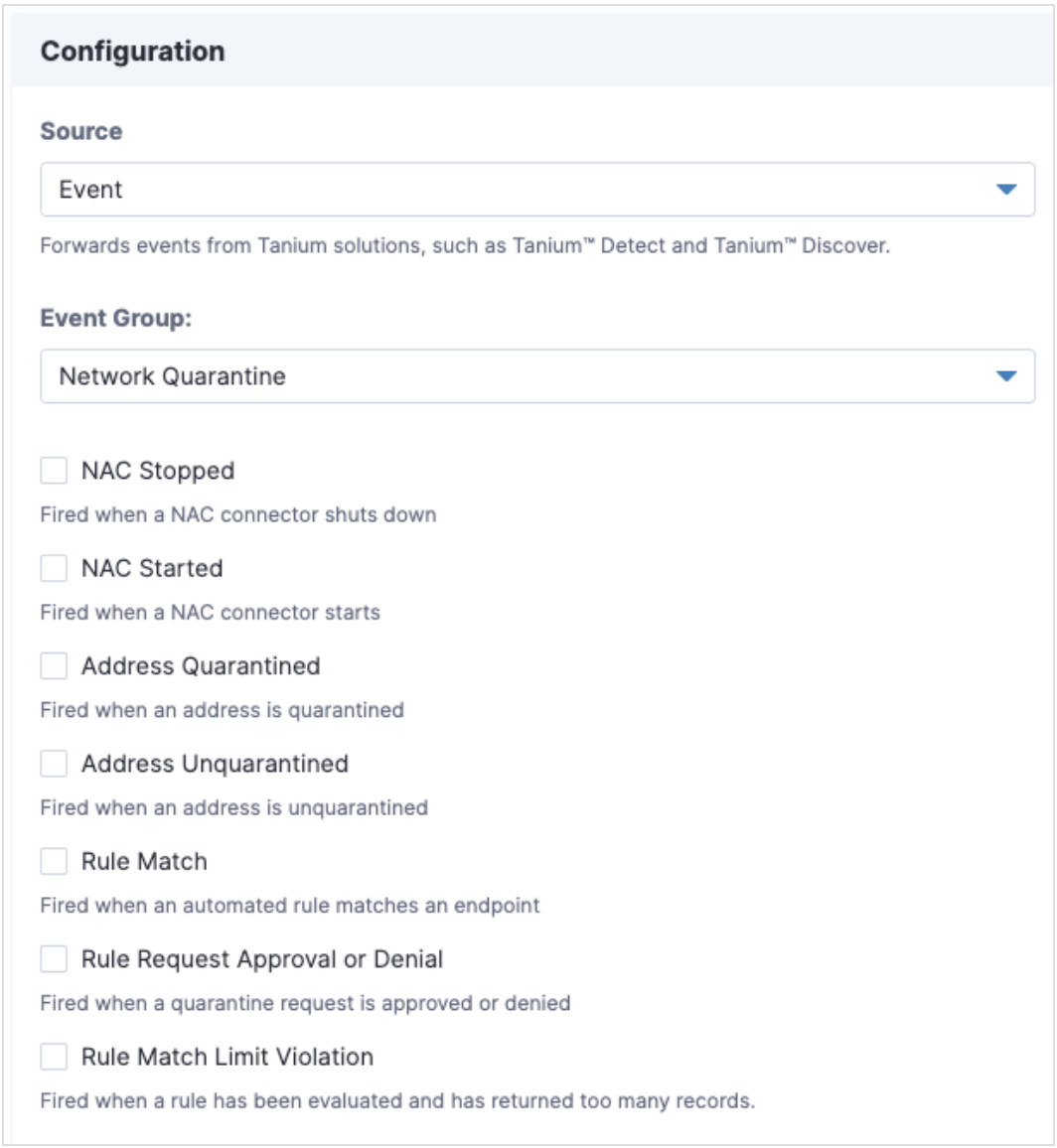
Configure notifications in Connect

1. Create the connection.
    a. From the Main menu, go to **Modules > Connect** to open the Connect **Overview** page. Click **Create Connection**.
    b. Specify a name and description for the connection.

2. Configure the data source.

   a. In the **Configuration** section, select the **Event** as the **Source**.

   b. Choose the **Network Quarantine** event group, then select the events for which you want to generate a notification.



3. Configure the connection destination.
   Select any of the connection destinations that are listed in the **Select Destination** menu. Common choices for notifications include Email, SIEM, and Splunk. However, you can use any of the available destinations. For more information, see the Tanium Connect User Guide. Complete the required fields and click **Create Connection**.

Troubleshooting Network Quarantine

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

Collect logs

The information is saved as a compressed ZIP file that you can download with your browser.

1. From the Network Quarantine **Overview** page, click Help, then click the **Troubleshooting** tab.
2. In the **Troubleshooting ZIP File** section, click **Download the File**.
   A `networkquarantine-support.zip` file downloads to the local download directory.
3. Contact Tanium Support to determine the best option to send the ZIP file. For more information, see Contact Tanium Support on page 30.

Tanium Network Quarantine maintains logging information in `networkquarantine`*`NN`*`.log` files in the `\Program Files\Tanium\Tanium Module Server\services\networkquarantine-files` directory. A new log file gets created each time the file size reaches 1 MB.

Configure log levels

1. From the Network Quarantine **Overview** page, click Help, then click the **Troubleshooting** tab.
2. In the **Logging Level** section, select the log level that you want to enable.

View audit log

The audit log contains all of the quarantine and unquarantine actions that occur on the configured NACs.

1. From the Network Quarantine menu, click **Audit log**.
2. You can filter the log by a specific MAC address, action, NAC name, and so on.
3. Click **Export** to save the current view of the audit log to a CSV file.

Fix SASLError not-authorized error

Problem

When a client connects to ISE with a certificate, ISE remembers that certificate and pins the certificate to the client. If that client then attempts to connect with a different client certificate, the connection is rejected with a `SASL:not-authorized` error.

Solution

1. In the ISE UI, go to **Administration > pxGrid Services > All Clients**.
2. Select the user and delete the session.
3. In Network Quarantine, start the NAC.

Uninstall Network Quarantine

1. From the Main menu, go to **Administration > Configuration > Solutions**.
2. In the **Content** section, select the **Network Quarantine** row.
3. Click Delete Selected  and then click **Uninstall** to complete the process.

Contact Tanium Support

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