Tanium™ Network Quarantine User Guide

Version 1.3.0

February 23, 2021

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 to make interaction with Tanium software more intuitive and to accelerate the time to success. To ensure high accessibility standards, Tanium complies with the U.S. Federal regulations - specifically Section 508 of the Rehabilitation Act of 1998. We have conducted third-party accessibility assessments over the course of product development for many years, and most recently a comprehensive audit against the WCAG 2.1 / VPAT 2.3 standards for all major product modules was completed in September 2019. 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.

Table of contents

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.

NAC devices

With the Network Quarantine service, Tanium products can communicate with a NAC to isolate endpoints. The following NAC devices are supported:

Palo Alto Networks Layer 3 Firewall

Supports blocking of IP addresses with Dynamic Address Groups (DAG). Palo Alto Networks Panorama is not supported.

Cisco Identity Services Engine (ISE)

Supports blocking by MAC address.

For more information, see Configuring NACs on page 15.

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 25.

Product integration

Tanium™ Discover

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

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 29.

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 15.

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 29.

Step 4: Quarantine endpoints

Quarantine endpoints.

For more information, see Quarantining endpoints on page 25.

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.

Tanium dependencies

Network Quarantine is included with Tanium Connect. For information about licensing, contact Tanium Support. Make sure that your environment meets the following requirements.

Component	Requirement
Tanium™ Core Platform	Version 7.3.314.4250 or later
Tanium products	The following modules are optional, but Network Quarantine requires the specified minimum versions to work with them: • Tanium Connect 4.7.4 or later • Tanium Discover 2.7.0 or later

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 operating systems

Same as Tanium Client support. See Tanium Client User Guide: Host system requirements.

Third-party software

- Cisco Identity Services Engine (ISE) 2.2 or later with pxGrid installed
- Palo Alto Networks OS 7.1 or later
- Palo Alto Networks Panorama is 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.
	Palo Alto Networks firewall	443	TCP	Access to Palo Alto Networks firewall, unless specified otherwise.

Best Practice: Configure firewall policies to open ports for Tanium traffic with TCP-based rules instead of application identity-based rules. For example, on a Palo Alto Networks firewall, configure the rules with service objects or service groups instead of application objects or application groups.

User role requirements

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
Show Networkquarantine View Network Quarantine shared service	✓	✓	✓	✓	✓	✗
Network Quarantine Certificates Read View configured certificates	✓	✗	✗	✗	✗	✗
Network Quarantine Certificates Write Add or update configured certificates	✓	✗	✗	✗	✗	✗
Network Quarantine Nacs Read View configured NACs	✓	✓	✓	✓	✗	✗
Network Quarantine Nacs Write Add or update configured NACs	✓	✗	✗	✗	✗	✗
Network Quarantine Quarantines Read View quarantined endpoints	✓	✓	✓	✓	✓	✗

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 Quarantines Write Quarantine or unquarantine endpoints	✓	✗	✗	✓	✗	✗
Network Quarantine Rules Evaluate Use service account to evaluate rules	✗	✗	✗	✗	✗	✓
Network Quarantine Settings Read View service settings	✓	✓	✓	✓	✓	✗
Network Quarantine Settings Write Configure service settings	✓	✗	✓	✗	✗	✗
Network Quarantine Nacauditlog Read View audit log	✓	✓	✓	✓	✗	✗
Network Quarantine Rules Run Start rule evaluation process	✓	✗	✓	✗	✗	✗
Network Quarantine Rules Read View rules and targets	✓	✓	✓	✗	✗	✗
Network Quarantine Rules Write Edit rules and targets	✓	✗	✓	✗	✗	✗
Network Quarantine Requests Read View quarantine requests	✓	✓	✓	✗	✗	✗
Network Quarantine Requests Approve Approve quarantine requests	✓	✓	✓	✗	✗	✗

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 Requests Deny Deny quarantine requests	✓	✓	✓	✗	✗	✗
Network Quarantine Runs Read View rule evaluation runs	✓	✓	✓	✗	✗	✗

Provided Network Quarantine micro admin and advanced user role permissions

Permission	Role type	Content set for permission	Network Quarantine Administrator	Network Quarantine Approver	Network Quarantine Rule Author	Network Quarantine User	Network Quarantine Read Only User	Network Quarantine Service Account
Read User	Micro Admin		✓	✗	✓	✗	✗	✗
Read Computer Group	Micro Admin		✓	✓	✓	✗	✗	✓
Execute Plugin	Advanced	Network Quarantine Content Set	✓	✓	✓	✓	✓	✓
Read Plugin	Advanced	Network Quarantine Content Set	✓	✗	✓	✗	✗	✗
Read Saved Question	Advanced	Network Quarantine Content Set	✓	✗	✓	✗	✗	✓
Read Sensor	Advanced	Reserved, Default, Base, Network Quarantine Content Set	✓	✗	✓	✗	✗	✓
Write saved question	Advanced	Network Quarantine Content Set	✗	✗	✗	✗	✗	✓

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 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 and configure 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 and configure Network Quarantine with custom settings on page 13.

Before you begin

- Read the release notes.
- Review the Network Quarantine requirements on page 8.

Import and configure Network Quarantine with default settings

When you import Network Quarantine with automatic configuration, the Network Quarantine service account is set to the account that you used to import the module.

To import Network Quarantine and configure default settings, be sure to select the **Apply Tanium recommended configurations** check box while performing the steps in Tanium Console User Guide: Manage Tanium modules. After the import, verify that the correct version is installed: see Verify Network Quarantine version on page 14.

Import and configure Network Quarantine with custom settings

To import Network Quarantine without automatically configuring default settings, follow the steps in Tanium Console User Guide: Manage Tanium content packs. After the import, verify that the correct version is installed: see Verify Network Quarantine version on page 14.

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.

1. From the Main menu, go to **Administration > Shared Services > Network Quarantine** to open the Network Quarantine **Overview** page.
2. Click Settings ⚙ and open the **Service Account** tab.
3. Update the service account settings and click **Submit**.

Upgrade Network Quarantine

For the steps to upgrade Network Quarantine, see Tanium Console User Guide: Manage Tanium modules. 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 ℹ.

What to do next

See Getting started on page 7 for more information about using Network Quarantine.

Configuring NACs

Configure Palo Alto Networks Layer 3 Firewall DAG NAC or 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.

Palo Alto Networks Layer 3 Firewall DAG NAC

If you have Palo Alto Networks Dynamic Address Group (DAG), Network Quarantine can send a request to Palo Alto to block network access for an IP address.

IMPORTANT: Palo Alto Networks Panorama is not supported.

Before you begin

Before you configure the Palo Alto DAG NAC in Network Quarantine, you must have:

- The host name, user name, and password for the firewall.
- The tags that you want to apply to the quarantined endpoints configured on the firewall.
- The necessary certificates configured. You must have the server certificate for the firewall to add to the Network Quarantine configuration. See PAN documentation: Certificate Management.

Configure Palo Alto Networks Firewall API access

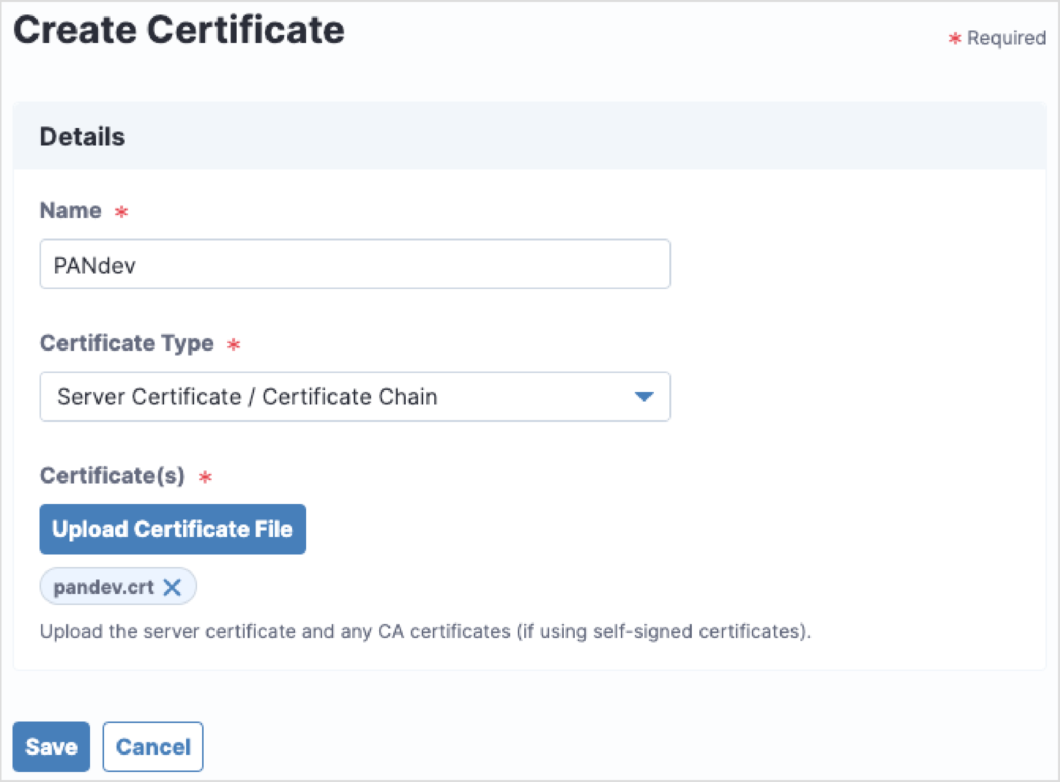
Create a user in the PAN Firewall that has Administrator user with API access. Specify this user when you configure NAC settings in Network Quarantine.

1. Log in to the PAN Firewall as an Administrator.
2. Create an Admin role with no WebUI permissions. For XML API permissions, select only **Operational Requests** and **UserID-Agent**.
3. Add a new Administrator user and password. Set the **Profile** to the admin role that you created to the new user.
4. Click **Commit** to save the changes.
5. Get an API key for the user. See PAN documentation: Get Your API Key.

Configure certificates in Network Quarantine

1. Download the firewall certificate.
2. From the Network Quarantine menu, go to **Configuration > Certificates > Create Certificate**.
3. Specify a name for the certificate.

4. For **Certificate Type**, select **Server Certificate / Certificate Chain**.
5. Upload the certificate. Click **Save**.



Create Certificate

* Required

Details

Name *

PANdev

Certificate Type *

Server Certificate / Certificate Chain

Certificate(s) *

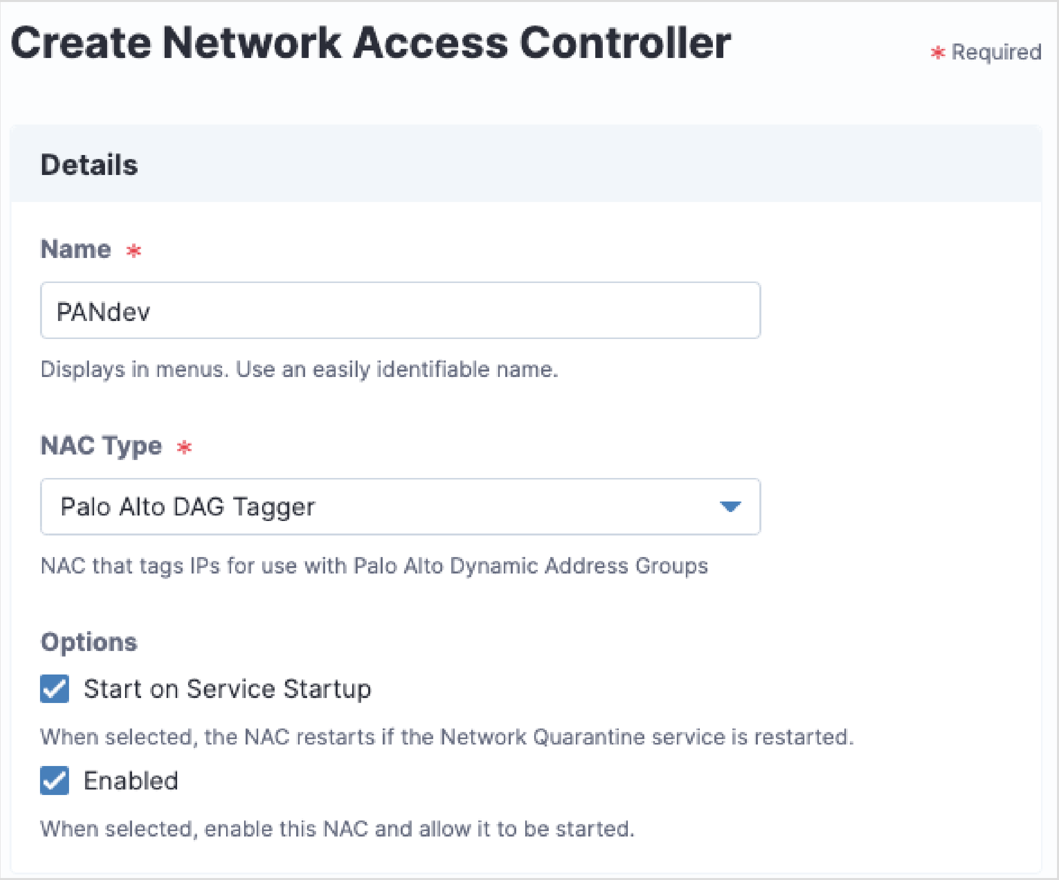
pandev.crt

Upload the server certificate and any CA certificates (if using self-signed certificates).

Configure Palo Alto DAG tagger

1. From the Network Quarantine menu, go to **Configuration > NACs > Create NAC**.
2. Specify a display name.
3. For the **NAC Type**, select **Palo Alto DAG Tagger**.

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.



Create Network Access Controller

* Required

Details

Name *

PANdev

Displays in menus. Use an easily identifiable name.

NAC Type *

Palo Alto DAG Tagger ▾

NAC that tags IPs for use with Palo Alto Dynamic Address Groups

Options

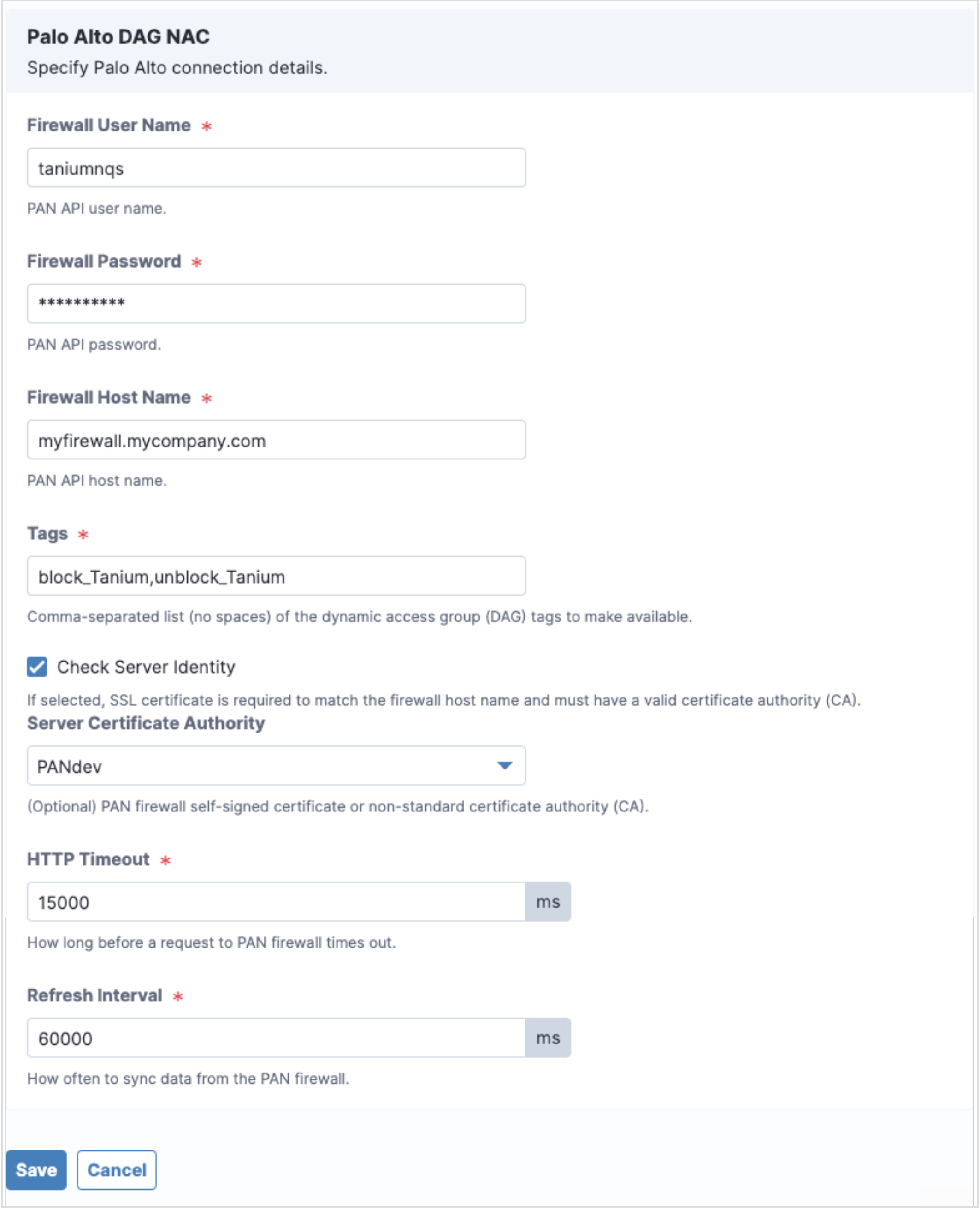
☑ Start on Service Startup

When selected, the NAC restarts if the Network Quarantine service is restarted.

☑ Enabled

When selected, enable this NAC and allow it to be started.

5. Specify the Palo Alto DAG NAC connection details.
   a. Enter the PAN API user name and password that you configured.
   b. Specify the host name for the firewall.
   c. Specify the list of tags that you want to send to the NAC.
   d. If you are using a self-signed certificate, clear **Check Server Identity**.
   e. (Optional) Select the certificate that you uploaded to Network Quarantine.
   f. (Optional) Update the **HTTP Timeout** and **Refresh Interval** settings.
   g. Click **Save**.



Palo Alto DAG NAC

Specify Palo Alto connection details.

Firewall User Name *

taniumnqs

PAN API user name.

Firewall Password *

****

PAN API password.

Firewall Host Name *

myfirewall.mycompany.com

PAN API host name.

Tags *

block_Tanium,unblock_Tanium

Comma-separated list (no spaces) of the dynamic access group (DAG) tags to make available.

☑ Check Server Identity

If selected, SSL certificate is required to match the firewall host name and must have a valid certificate authority (CA).

Server Certificate Authority

PANdev

(Optional) PAN firewall self-signed certificate or non-standard certificate authority (CA).

HTTP Timeout *

15000 ms

How long before a request to PAN firewall times out.

Refresh Interval *

60000 ms

How often to sync data from the PAN firewall.

6. Start the NAC. Select the NAC from the list and click **Start**.

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

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 log 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

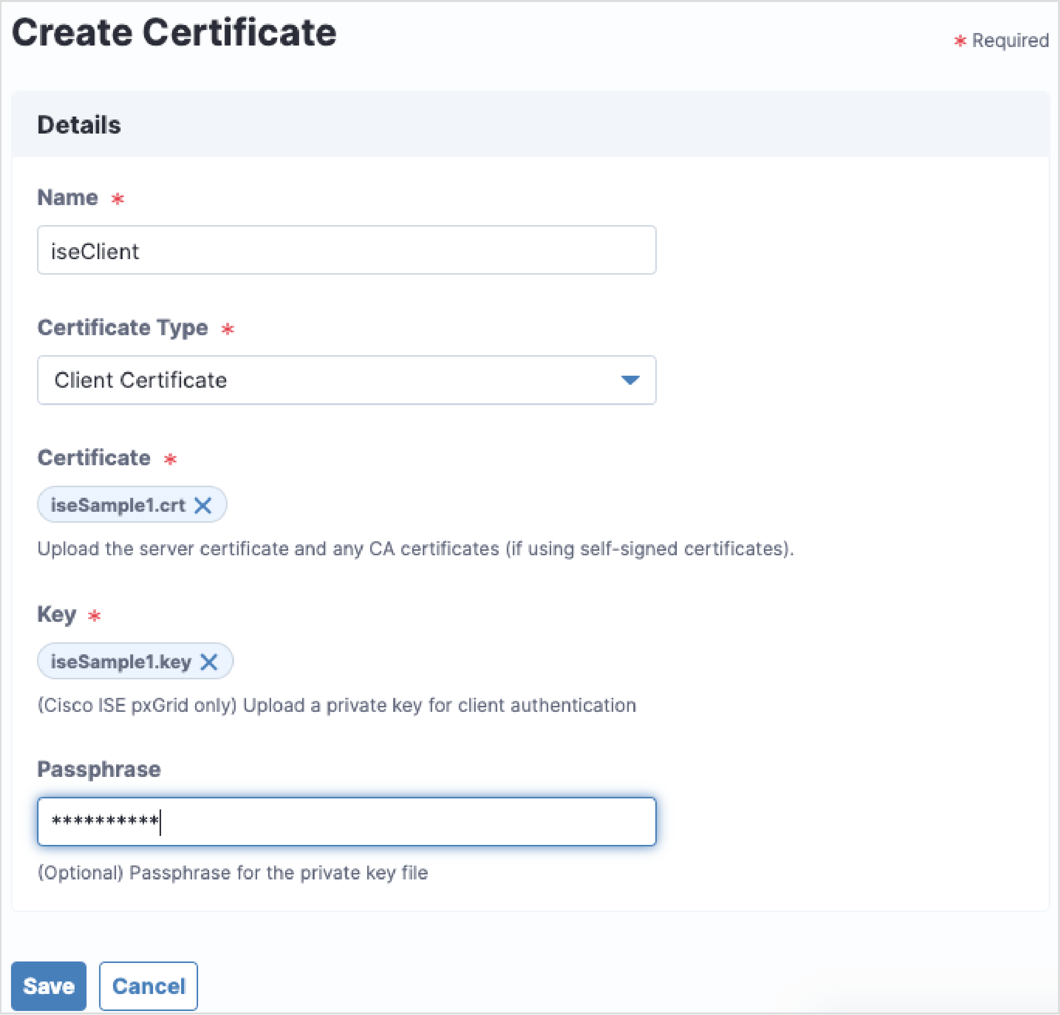
Create the client and server certificates in Network Quarantine.

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**.



Create Certificate

* Required

Details

Name *

iseClient

Certificate Type *

Client Certificate

Certificate *

iseSample1.crt

Upload the server certificate and any CA certificates (if using self-signed certificates).

Key *

iseSample1.key

(Cisco ISE pxGrid only) Upload a private key for client authentication

Passphrase

****

(Optional) Passphrase for the private key file

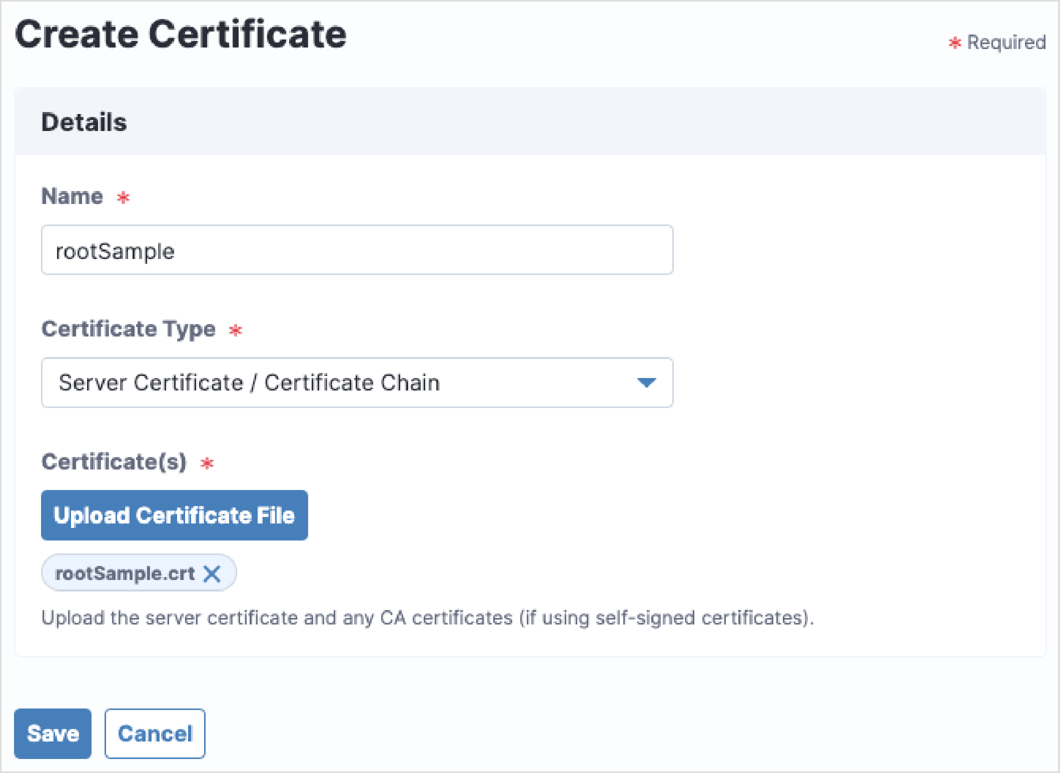
3. Create the server certificate.

   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**.



Create Certificate

Details

Name *

rootSample

Certificate Type *

Server Certificate / Certificate Chain

Certificate(s) *

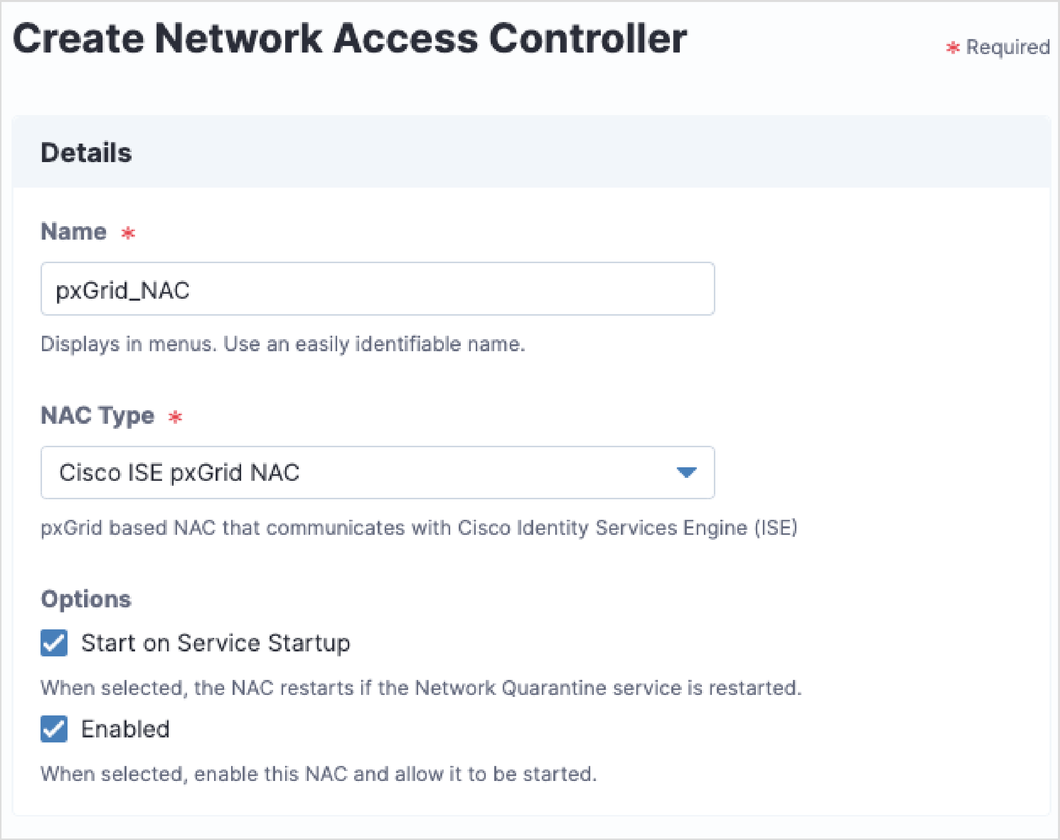
rootSample.crt

Upload the server certificate and any CA certificates (if using self-signed certificates).

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.



Create Network Access Controller

* Required

Details

Name *

pxGrid_NAC

Displays in menus. Use an easily identifiable name.

NAC Type *

Cisco ISE pxGrid NAC

pxGrid based NAC that communicates with Cisco Identity Services Engine (ISE)

Options

☑ Start on Service Startup

When selected, the NAC restarts if the Network Quarantine service is restarted.

☑ Enabled

When selected, enable this NAC and allow it to be started.

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 25.

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 IP or 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.

> **IMPORTANT:** With automated rules, you can block by MAC Address using an ISE NAC. You cannot use automated rules with Palo Alto Networks Layer 3 Firewall blocking by IP 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.

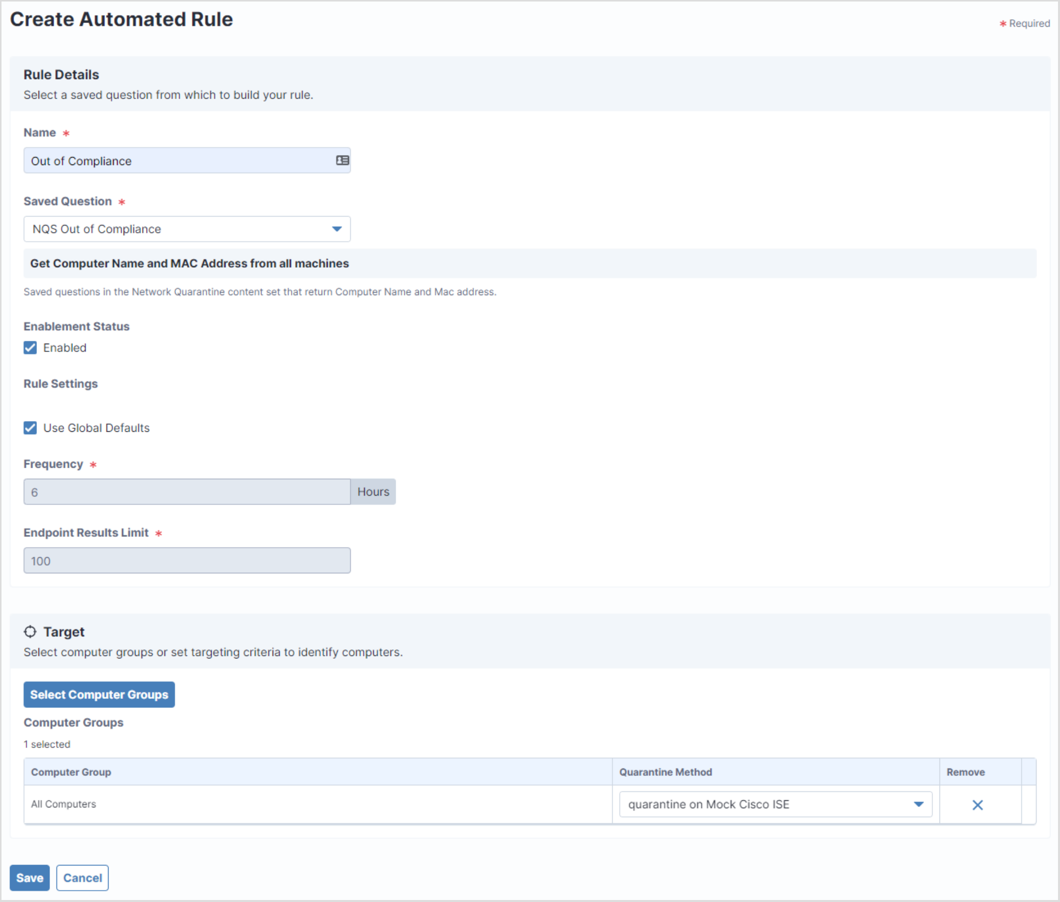
The saved question you use for a rule must meet the following requirements:

- 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. >



Create Automated Rule

* Required

Rule Details

Select a saved question from which to build your rule.

Name *

Out of Compliance

Saved Question *

NQS Out of Compliance

Get Computer Name and MAC Address from all machines

Saved questions in the Network Quarantine content set that return Computer Name and Mac address.

Enablement Status

☑ Enabled

Rule Settings

☑ Use Global Defaults

Frequency *

6 Hours

Endpoint Results Limit *

100

Target

Select computer groups or set targeting criteria to identify computers.

Select Computer Groups

Computer Groups

1 selected

Computer Group	Quarantine Method	Remove
All Computers	quarantine on Mock Cisco ISE	×

Save Cancel

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**.

Tip: 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 or IP address

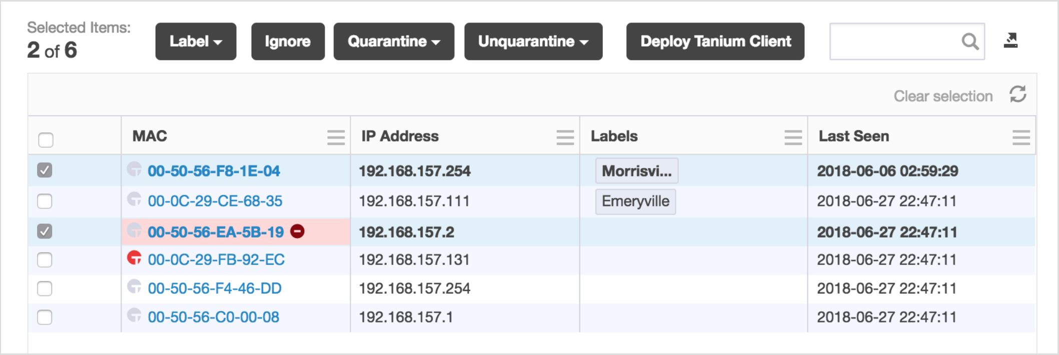
1. On the **Quarantine** tab in the **Issues** section of the Network Quarantine **Overview** page, click **Create Quarantine**.
2. Use the available options to quarantine endpoints:
    - To quarantine endpoints with a Palo Alto Dynamic Address Group (DAG) NAC, enter a list of IP addresses on which to apply the quarantine and choose the quarantine method that you want to use.
    - 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 IP or 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 IP or MAC address and click **Remove Quarantine**.

Quarantine in Discover

If you have Tanium Discover installed, you can also quarantine and remove quarantine for an IP or 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 or IP addresses are marked as blocked.

For more information, see Tanium Discover User Guide.



Selected Items: 2 of 6

□	MAC	IP Address	Labels	Last Seen
☑	00-50-56-F8-1E-04	192.168.157.254	Morrisvi...	2018-06-06 02:59:29
□	00-0C-29-CE-68-35	192.168.157.111	Emeryville	2018-06-27 22:47:11
☑	00-50-56-EA-5B-19 ⊖	192.168.157.2		2018-06-27 22:47:11
□	00-0C-29-FB-92-EC	192.168.157.131		2018-06-27 22:47:11
□	00-50-56-F4-46-DD	192.168.157.254		2018-06-27 22:47:11
□	00-50-56-C0-00-08	192.168.157.1		2018-06-27 22:47:11

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.

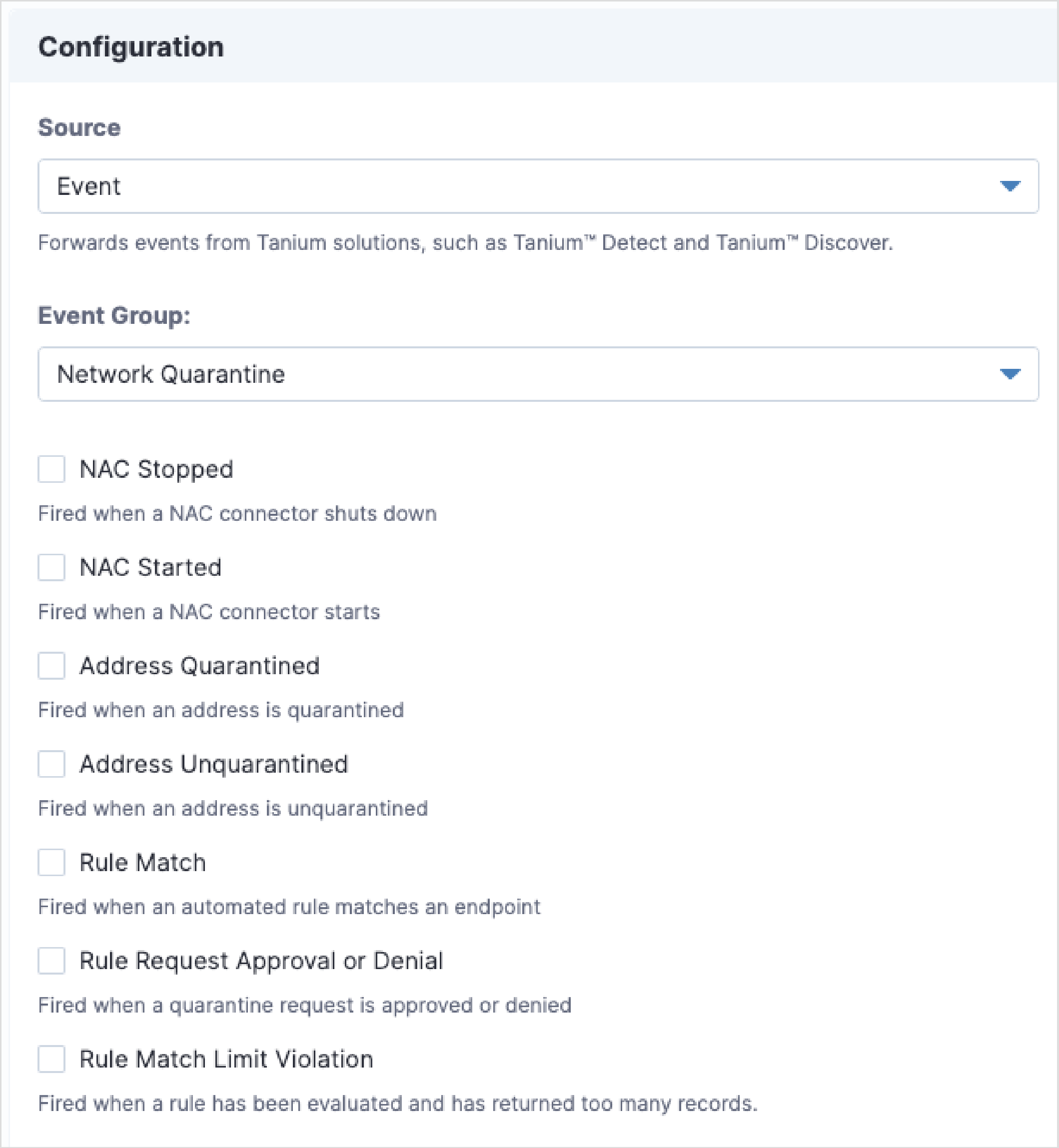
Prerequisites

- 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.



Configuration

Source

Event

Forwards events from Tanium solutions, such as Tanium™ Detect and Tanium™ Discover.

Event Group:

Network Quarantine

☐ NAC Stopped

Fired when a NAC connector shuts down

☐ NAC Started

Fired when a NAC connector starts

☐ Address Quarantined

Fired when an address is quarantined

☐ Address Unquarantined

Fired when an address is unquarantined

☐ Rule Match

Fired when an automated rule matches an endpoint

☐ Rule Request Approval or Denial

Fired when a quarantine request is approved or denied

☐ Rule Match Limit Violation

Fired when a rule has been evaluated and has returned too many records.

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 32.

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 specific IP or 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 into https://support.tanium.com.