Cisco Firepower Management Center Remediation Module for Tetration, Version 1.0.1 Quick Start Guide

First Published: 2018-08-01

Last Modified: 2018-09-20

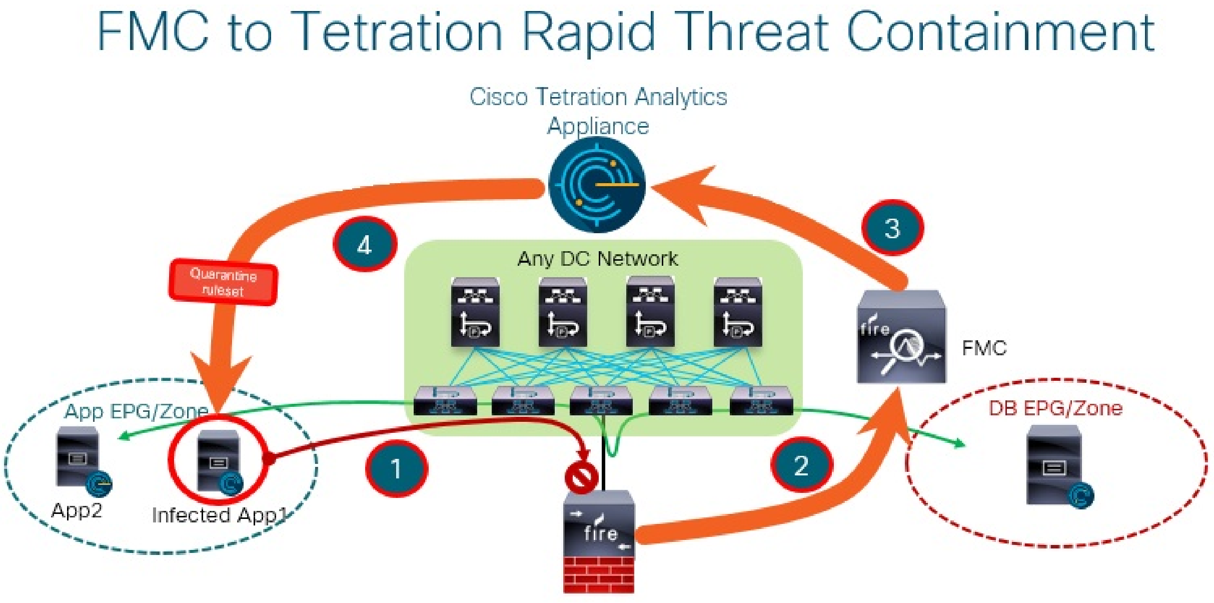
Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CHAPTER 1

Introduction

Overview

With the Cisco Firepower Management Center (FMC) Remediation Module for Tetration, when an attack on your network from an infected host is detected by the FMC, the offending host can be quarantined by a Tetration Analytics (TA) enforcement agent so that no further traffic is allowed to go in or out of that host. The following illustration shows the relationship between the FMC and Tetration when the remediation module is installed:



The illustration also shows the overall process of quarantining the network attack:

Step 1 A host with an infected application launches an attack on your network. The attack is blocked inline by Cisco Firepower Threat Defense (FTD) running on a Firepower device (physical or virtual).

Step 2 An intrusion event that includes information about the infection is generated and reported to the FMC managing the FTD.

Step 3 The attack triggers the remediation module on the FMC to use the Northbound API to request that Tetration quarantine the infected host.

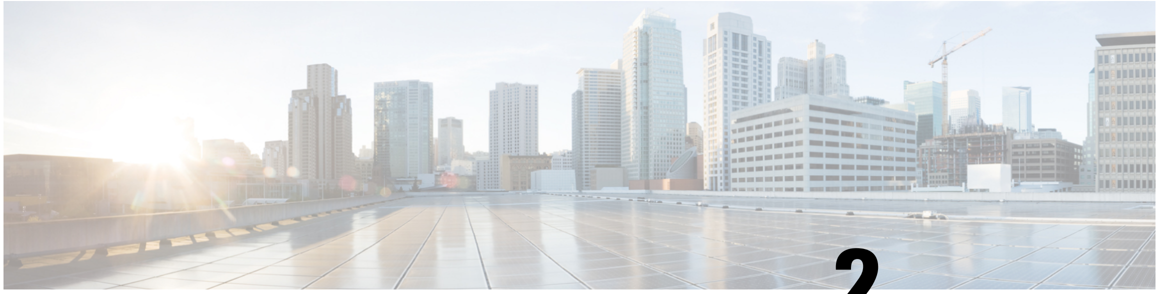
Step 4 Tetration quickly contains the infected application workload by sending a quarantine request to the enforcement agent on the infected host.

Prerequisites

- Pre-define absolute policies in TA to drop all traffic from and to any host annotated with 'quarantine.' If a partial quarantine is what you want, customize the policy in TA to deny only some, but not all, types of traffic. For more information, see the User Guide in the TA GUI.
- Tetration agents are software that runs within a host operating system, such as Linux or Windows. As enforcement agents, they have the capability to set firewall rules on installed hosts. Install enforcement agents on network hosts you want to protect. For more information, see Cisco Tetration Analytics for the Software Agent Installation Guide.

Related Documentation

- Firepower Management Center Configuration Guides
- Cisco Tetration Analytics



CHAPTER 2

Install

Install

To download and install the Cisco Firepower Management Center Remediation Module for Tetration, complete the following procedure:

Step 1 Use a web browser to download the remediation module:

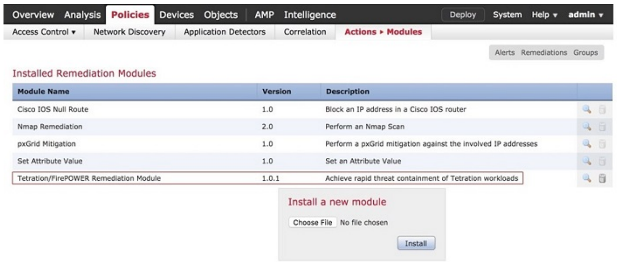
https://software.cisco.com/download/home/286259687/type

Step 2 Install the remediation module onto the FMC:

1. In the FMC GUI, navigate to **Policies** > **Actions** > **Modules**.
2. In the **Install a new module** dialog box, click **Choose File** as shown below.
3. Select the file for the remediation module that was downloaded in Step 1.
4. Click **Install**.

Note If you receive an access error message, clear the error message and repeat Step 2.

When successfully installed, the Cisco Firepower Management Center Remediation Module for Tetration is displayed in the list of installed remediation modules:



Installed Remediation Modules

Module Name	Version	Description
Cisco IOS Null Route	1.0	Block an IP address in a Cisco IOS router
Nmap Remediation	2.0	Perform an Nmap Scan
pxGrid Mitigation	1.0	Perform a pxGrid mitigation against the involved IP addresses
Set Attribute Value	1.0	Set an Attribute Value
Tetration/FirePOWER Remediation Module	1.0.1	Achieve rapid threat containment of Tetration workloads

Install a new module

Choose File No file chosen

CHAPTER 3

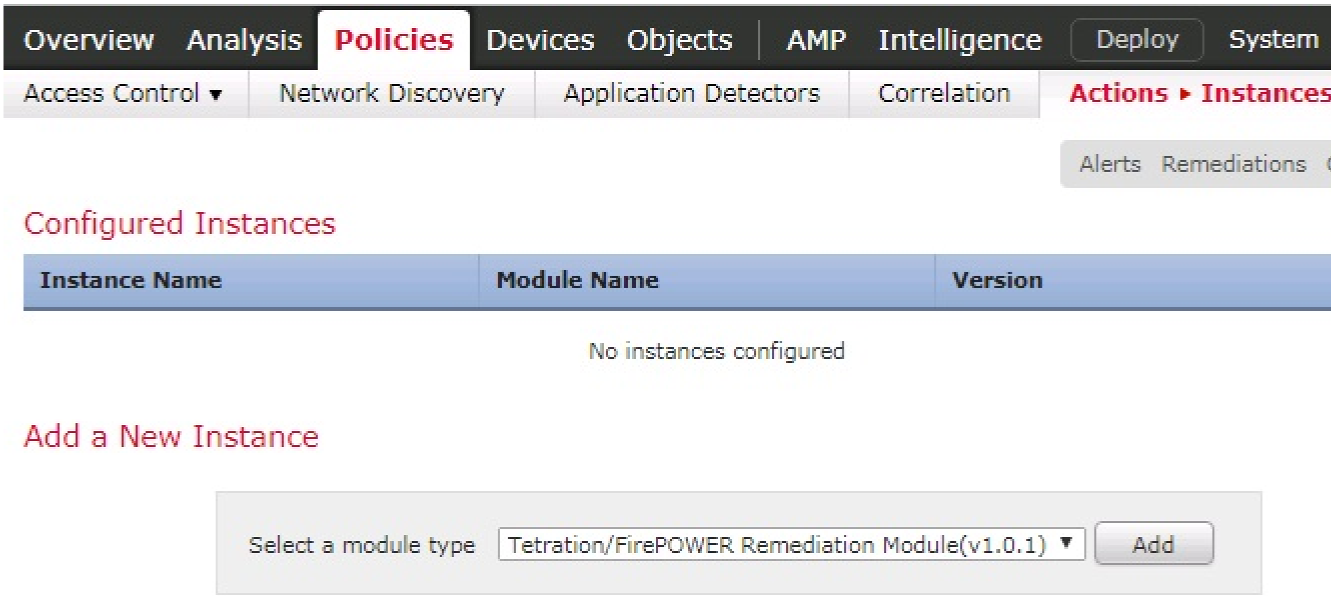
Configure

Configure

To configure the remediation module installed on the FMC, complete the following procedure in the FMC GUI:

Step 1 Create an instance of the remediation module for each Tetration Analytics (TA) server in your network:

1. Navigate to **Policies > Actions > Instances**.
2. Select the remediation module in the drop-down list, and click **Add**.



Configured Instances

Instance Name	Module Name	Version

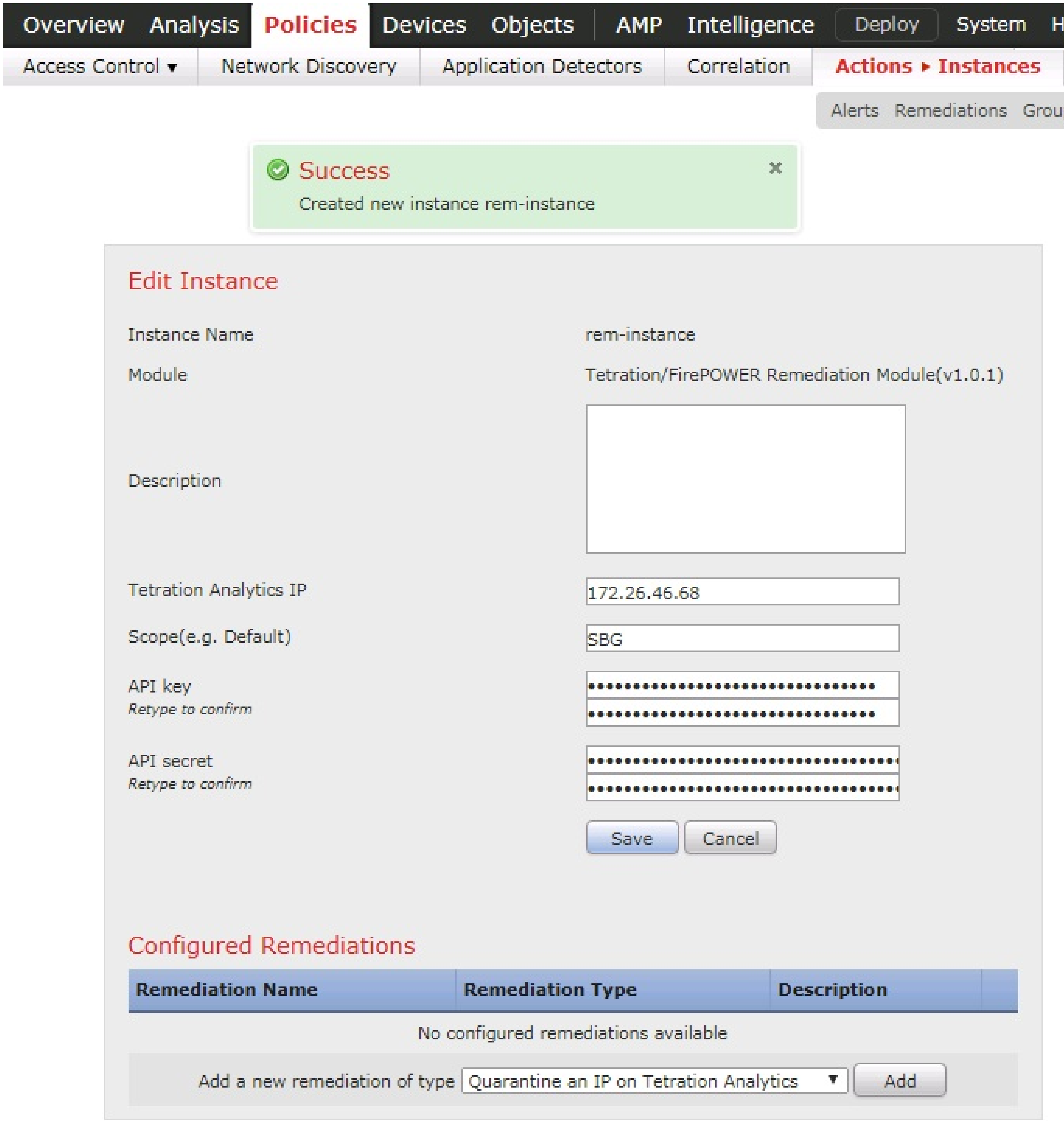
No instances configured

Add a New Instance

Select a module type: Tetration/FirePOWER Remediation Module(v1.0.1) ▾ Add

3. Enter an **Instance Name** (in this example, **`rem-instance`**).
4. Enter the TA server's IP address, API key, API secret, and scope containing the potentially offending host. Click **Create**.

Note The API key and secret are not validated against the TA server at this point. The API key and secret must first be created in TA by a site admin, customer support, or a root scope owner role. Copy that information for use here. For more details, see the TA API Configuration Guide.



Success ✕

Created new instance rem-instance

Edit Instance

Instance Name	rem-instance
Module	Tetration/FirePOWER Remediation Module(v1.0.1)
Description	
Tetration Analytics IP	172.26.46.68
Scope(e.g. Default)	SBG
API key *Retype to confirm*	•••••••••••••••••••••••••••••••••• ••••••••••••••••••••••••••••••••••
API secret *Retype to confirm*	•••••••••••••••••••••••••••••••••••• ••••••••••••••••••••••••••••••••••••

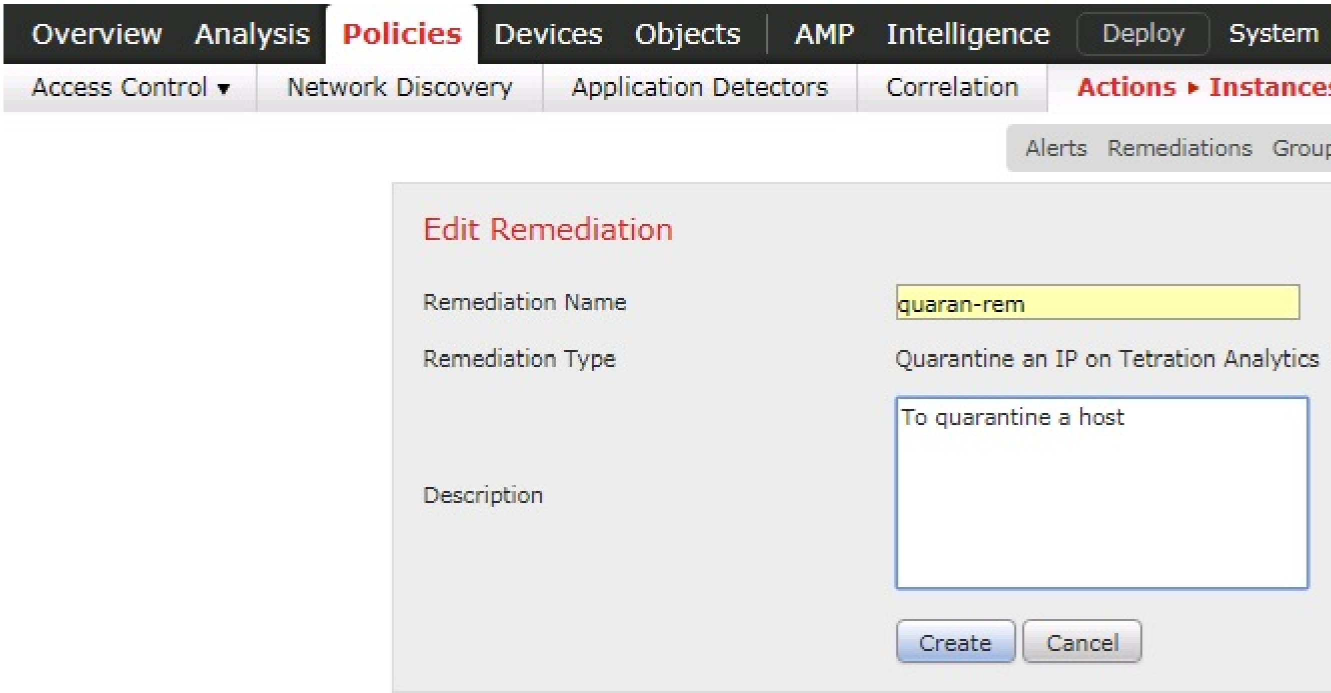
Configured Remediations

Remediation Name	Remediation Type	Description
No configured remediations available		

Add a new remediation of type Quarantine an IP on Tetration Analytics ▾

5. Under **Configured Remediations**, select a type of remediation (in this example, **`Quarantine an IP on Tetration Analytics`**), and click **Add** to add a new remediation.

6. Enter a **Remediation Name** (in this example, **`quaran-rem`**), and click **Create**.



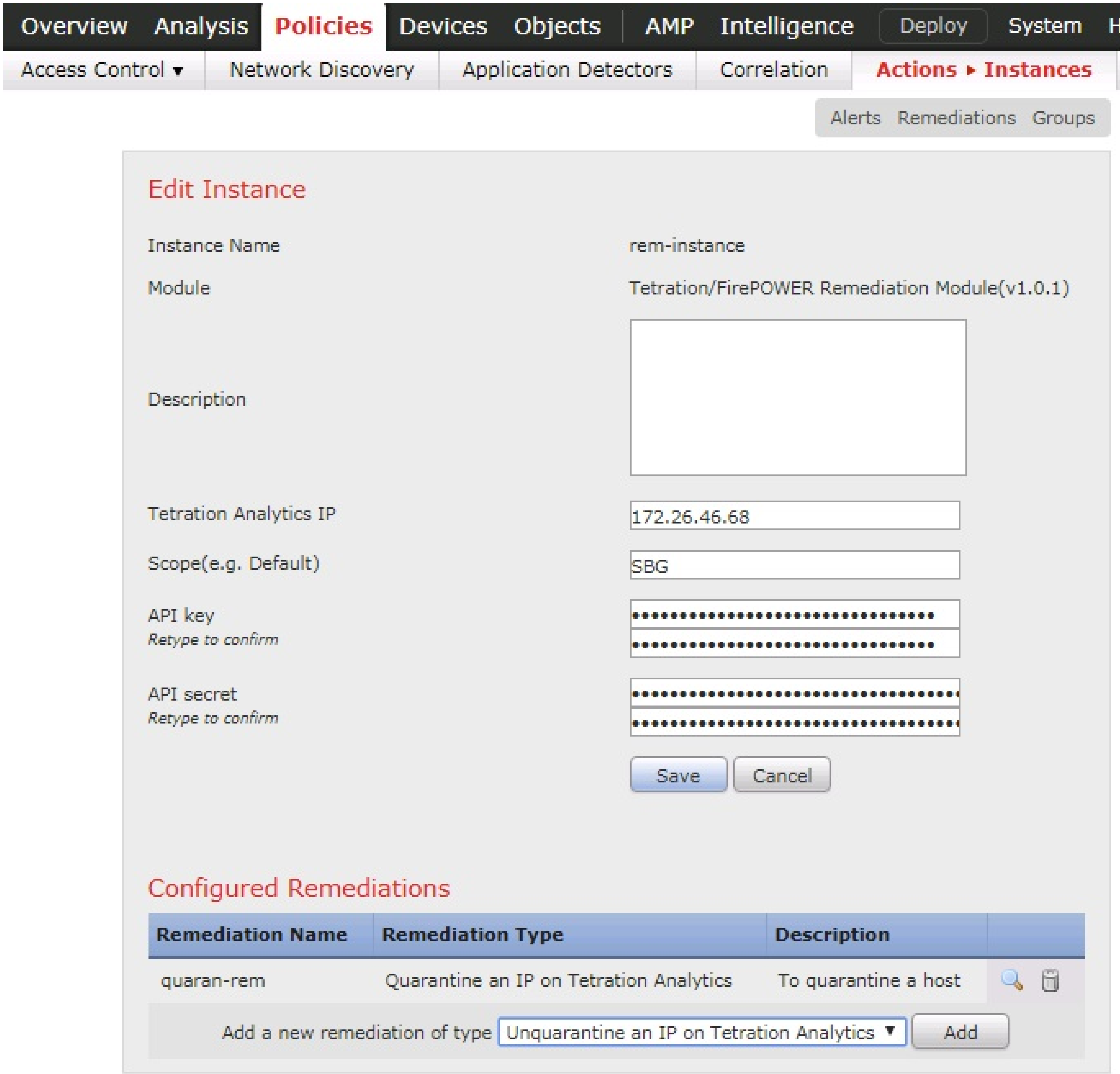
Edit Remediation

Remediation Name: quaran-rem

Remediation Type: Quarantine an IP on Tetration Analytics

Description: To quarantine a host

7. The remediation you just configured then shows up in the table. Click **Save**.



Edit Instance

Instance Name	rem-instance
Module	Tetration/FirePOWER Remediation Module(v1.0.1)
Description	
Tetration Analytics IP	172.26.46.68
Scope(e.g. Default)	SBG
API key *Retype to confirm*	•••••••••••••••••••••••••••••••••• ••••••••••••••••••••••••••••••••••
API secret *Retype to confirm*	•••••••••••••••••••••••••••••••••••• ••••••••••••••••••••••••••••••••••••

Configured Remediations

Remediation Name	Remediation Type	Description	
quaran-rem	Quarantine an IP on Tetration Analytics	To quarantine a host	

Add a new remediation of type Unquarantine an IP on Tetration Analytics ▾ Add

Step 2 Configure an access control policy (in this example, **`rem-policy`**):

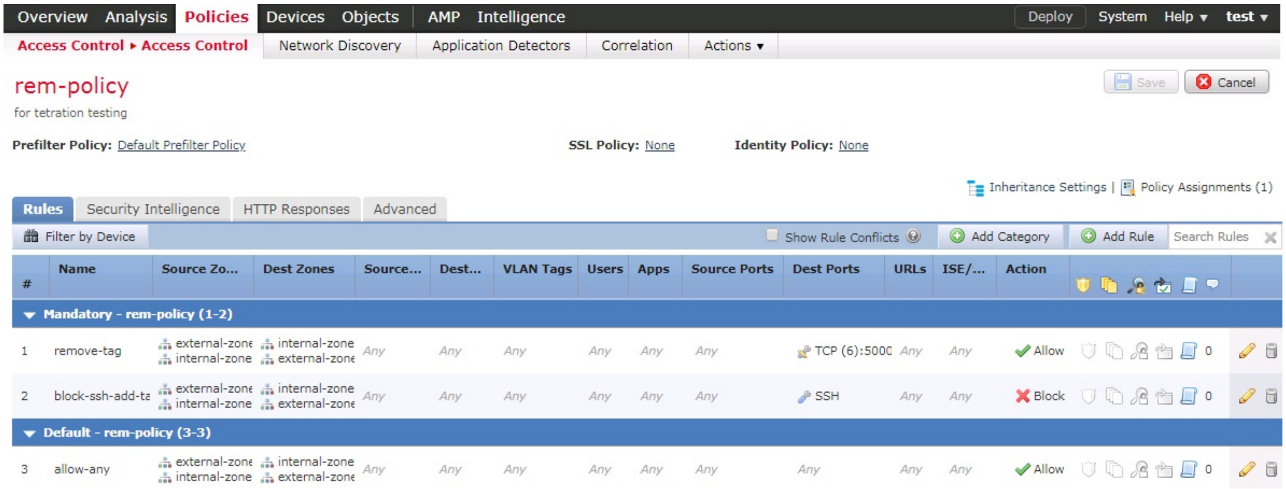
1. Navigate to **Policies** > **Access Control** > **Rules**.
2. Click **Add Rule** (for example, **`block-ssh-add-tag`**).
3. Select **Block** for the **Action**.
4. On the **Ports** tab, select **SSH** from the list of protocols for the destination port, and click **Add**.

5. Click **Save**.

6. On the **Logging** tab, select **Log at Beginning of Connection**.

   Important Ensure that logging is enabled on the access rule, so that the FMC receives event notifications.

7. Click **Save**.



rem-policy

for tetration testing

Prefilter Policy: Default Prefilter Policy **SSL Policy:** None **Identity Policy:** None

#	Name	Source Zo...	Dest Zones	Source...	Dest...	VLAN Tags	Users	Apps	Source Ports	Dest Ports	URLs	ISE/...	Action		
▾ Mandatory - rem-policy (1-2)															
1	remove-tag	external-zone internal-zone	internal-zone external-zone	Any	Any	Any	Any	Any	Any	TCP (6):5000	Any	Any	✓ Allow	0	
2	block-ssh-add-ta	external-zone internal-zone	internal-zone external-zone	Any	Any	Any	Any	Any	Any	SSH	Any	Any	✗ Block	0	
▾ Default - rem-policy (3-3)															
3	allow-any	external-zone internal-zone	internal-zone external-zone	Any	Any	Any	Any	Any	Any	Any	Any	Any	✓ Allow	0	

Step 3 Configure a correlation rule:

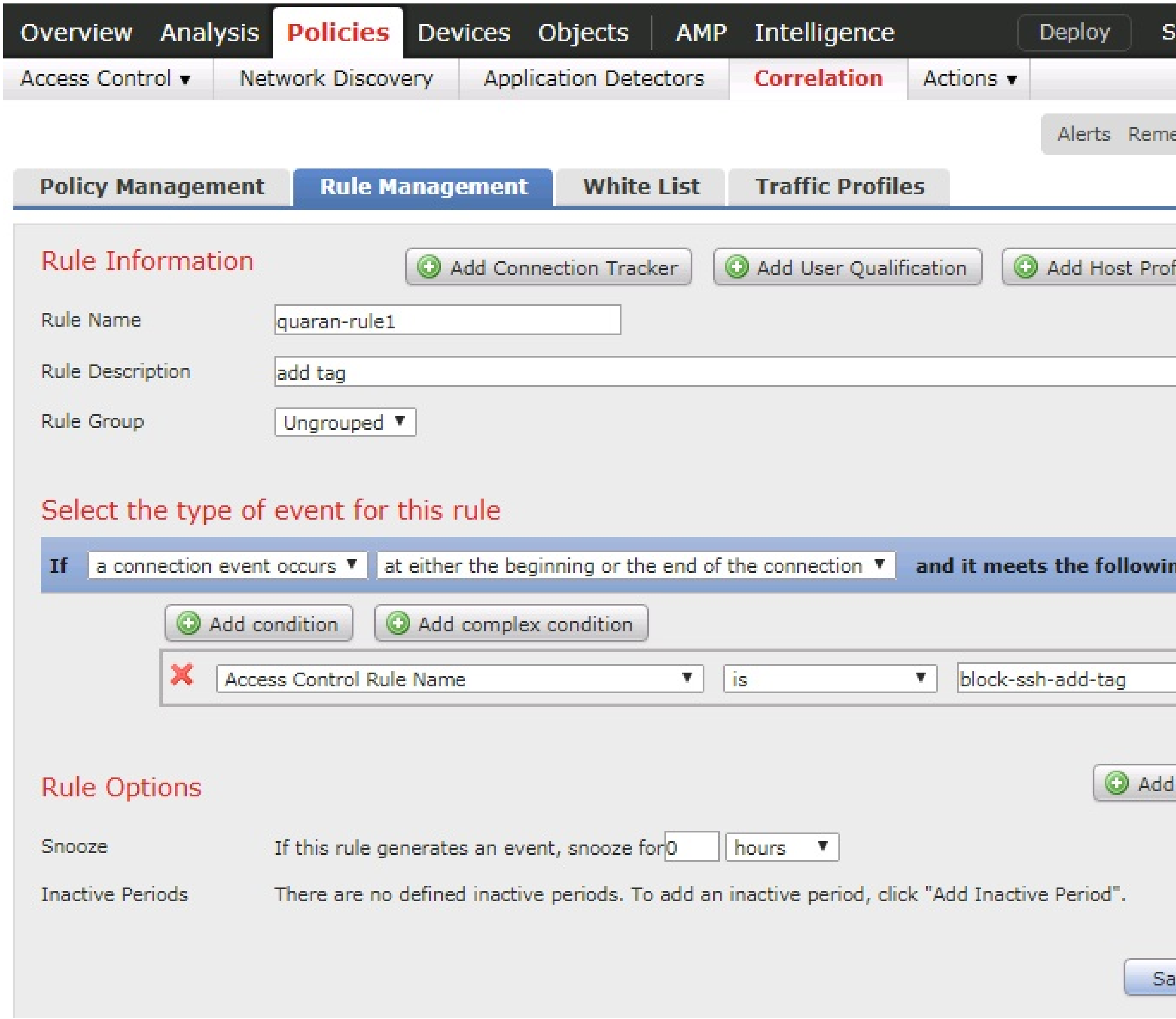
1. Navigate to **Policies > Correlation > Rule Management**.

2. Enter a **Rule Name** (in this example, `quaran-rule1`) and description (optional).

3. In the **Select the type of event for this rule** section, select **a connection event occurs** and **at either the beginning or the end of the connection**.

4. Click **Add condition**, and change the operator from **OR** to **AND**.

5. In the drop-down list, select **Access Control Rule Name**, **is**, and enter the name of the access control rule that you previously configured in Step 2 (in this example, `block-ssh-add-tag`).



Rule Information

Rule Name: quaran-rule1

Rule Description: add tag

Rule Group: Ungrouped ▾

Select the type of event for this rule

If a connection event occurs ▾ at either the beginning or the end of the connection ▾ and it meets the followin

Access Control Rule Name ▾ is ▾ block-ssh-add-tag

Rule Options

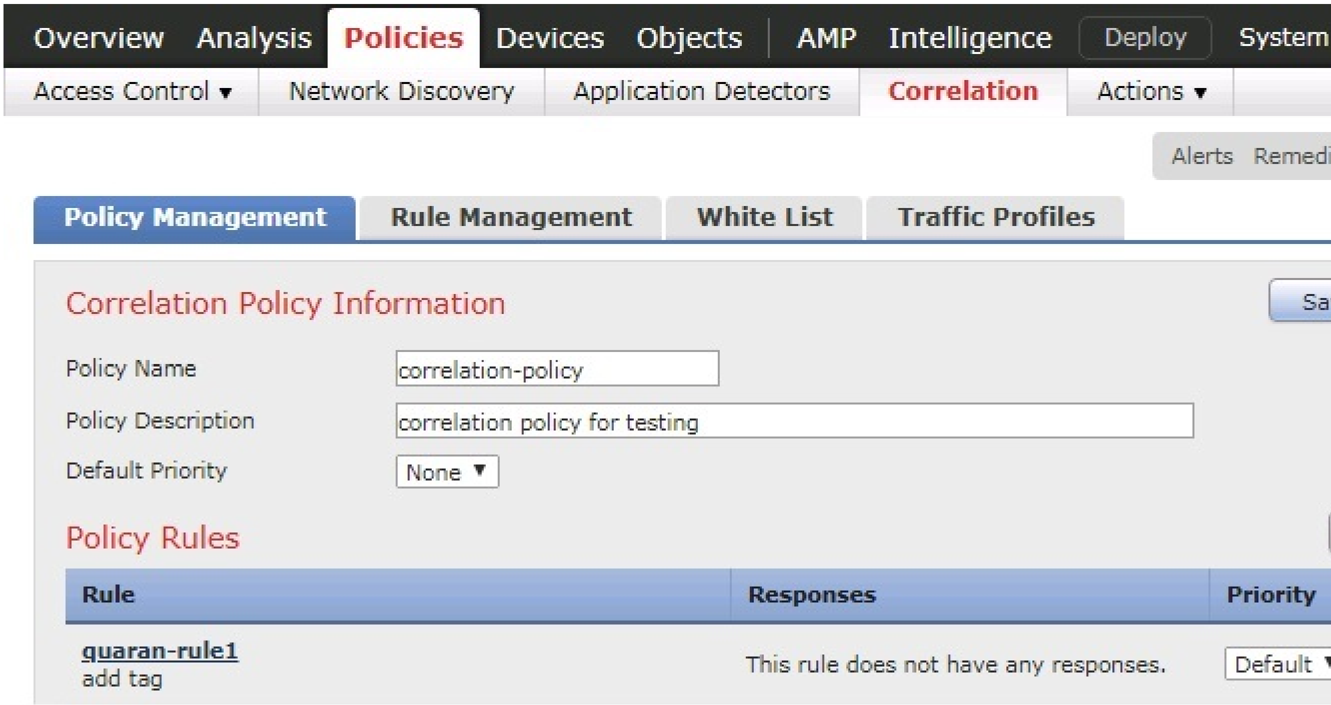
Snooze: If this rule generates an event, snooze for 0 hours ▾

Inactive Periods: There are no defined inactive periods. To add an inactive period, click "Add Inactive Period".

6. Click **Save**.

Step 4 Associate the instance of the remediation module as a response with a correlation rule:

1. Navigate to **Policies** > **Correlation** > **Policy Management**.
2. Click **Create Policy**.
3. Enter a **Policy Name** (in this example, **`correlation-policy`**) and description (optional).
4. From the **Default Priority** drop-down list, select a priority for the policy. Select **None** to use rule priorities only.
5. Click **Add Rules**, select the correlation rule you previously configured in Step 3 (in this example, **`quaran-rule1`**), and click **Add**.



Correlation Policy Information

Policy Name: correlation-policy

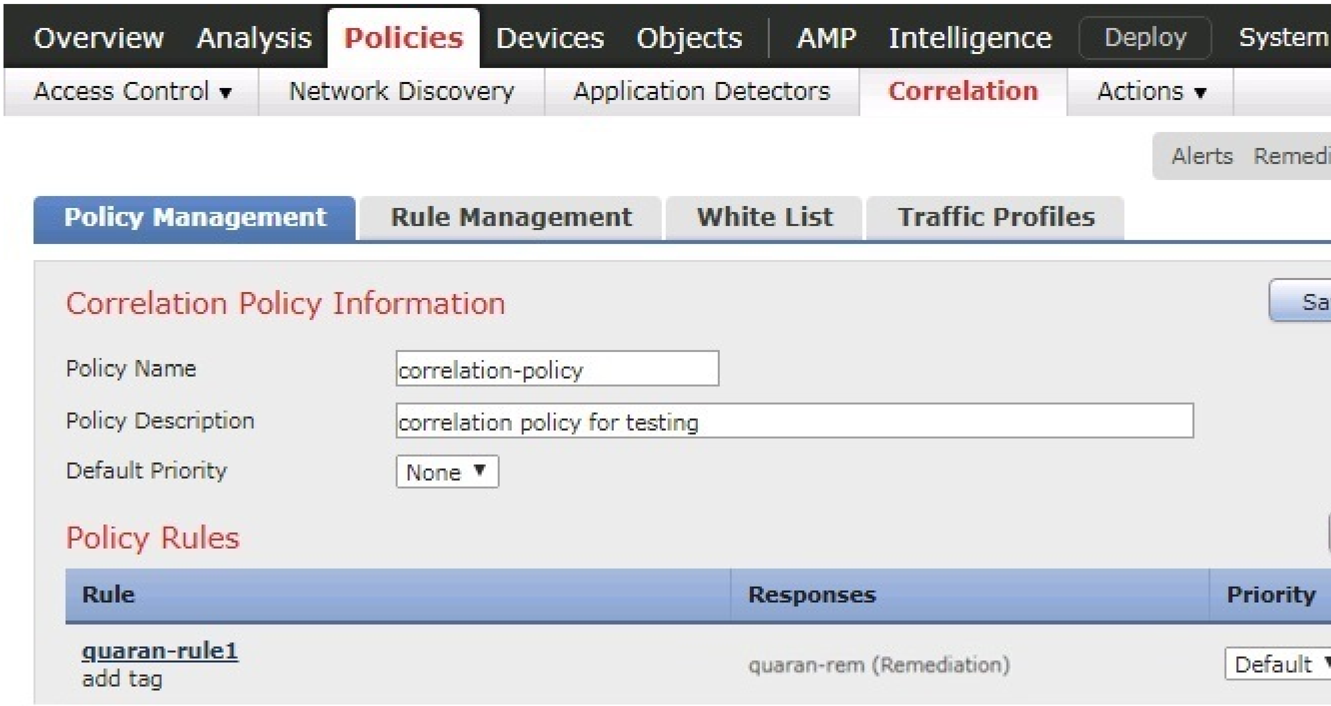
Policy Description: correlation policy for testing

Default Priority: None ▾

Policy Rules

Rule	Responses	Priority
quaran-rule1 add tag	This rule does not have any responses.	Default ▾

6. Click the **Responses** icon next to the rule and assign a response (in this example, `quaran-rem`) to the rule. Click **Update**.



Correlation Policy Information

Policy Name: correlation-policy

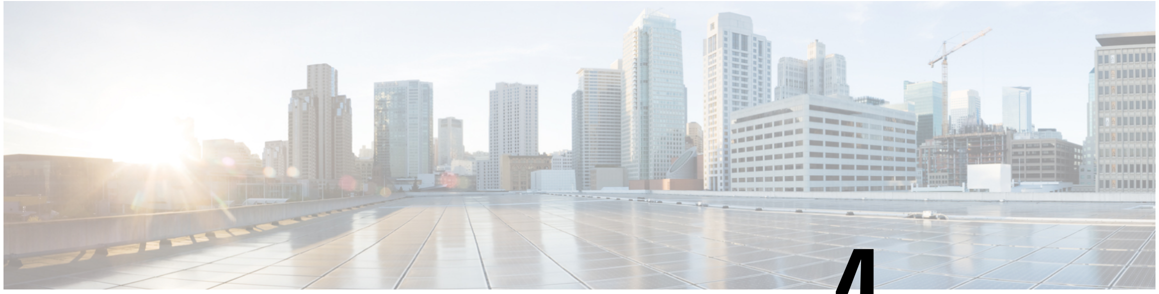
Policy Description: correlation policy for testing

Default Priority: None ▾

Policy Rules

Rule	Responses	Priority
quaran-rule1 add tag	quaran-rem (Remediation)	Default ▾

7. Click **Save**.



CHAPTER 4

Verify

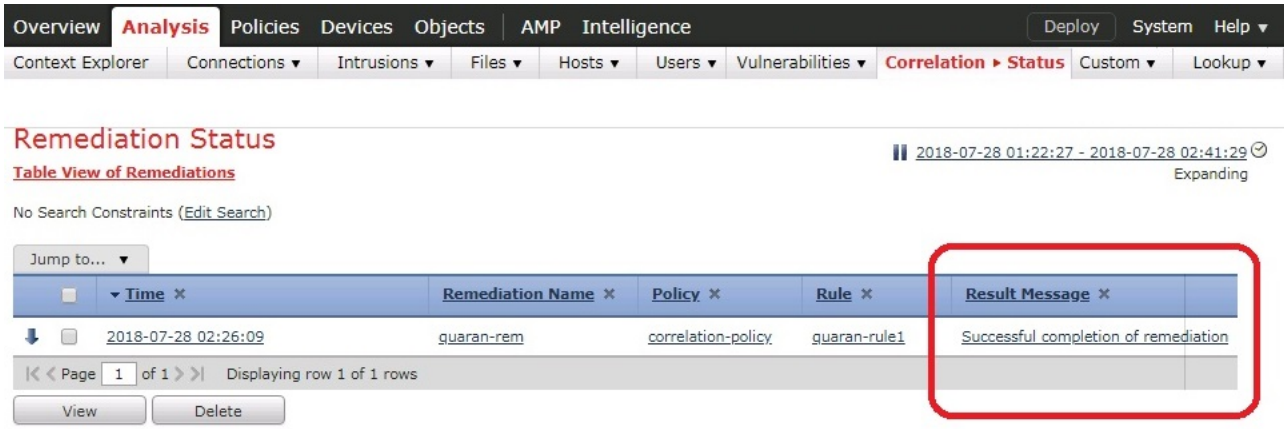
Verify

Because remediations can fail for various reasons, perform the following steps to verify that a remediation is successful:

Step 1 Once the remediation module is triggered by an associated correlation rule, check the status of the remediation execution in the FMC GUI.

Step 2 Navigate to **Analysis** > **Correlation** > **Status**.

Step 3 In the Remediation Status table, find the row for your policy and view the result message.



Remediation Status

Table View of Remediations

2018-07-28 01:22:27 - 2018-07-28 02:41:29

Expanding

No Search Constraints (Edit Search)

Jump to... ▾

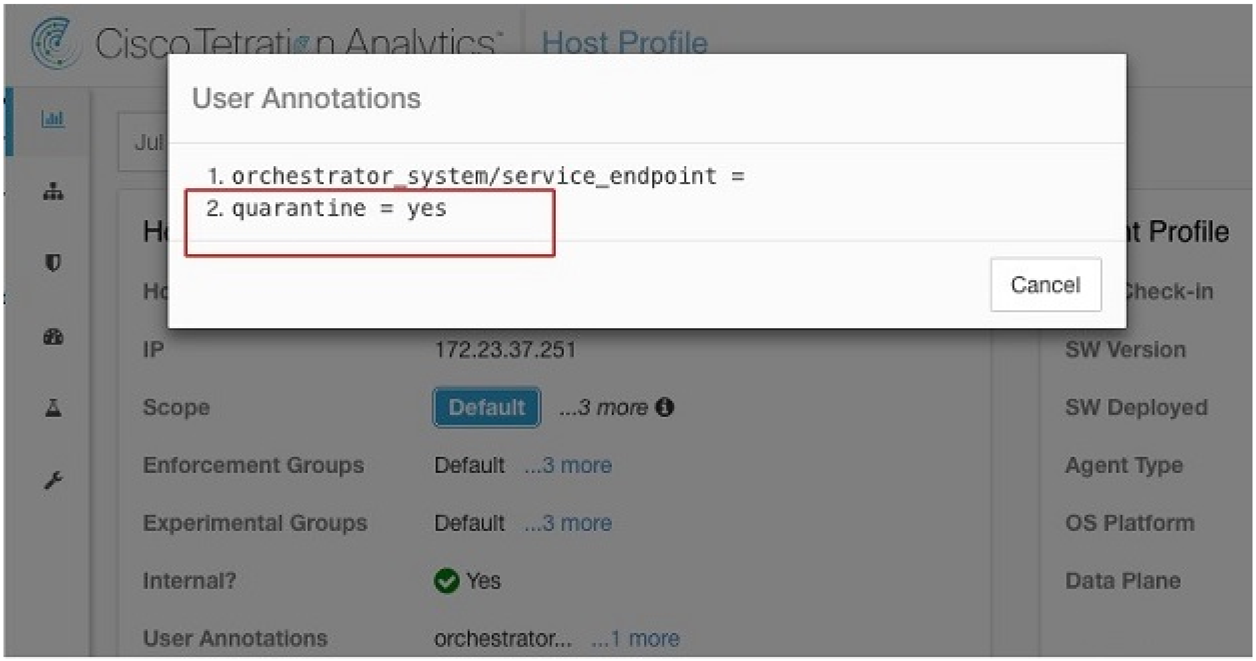
□	Time	Remediation Name	Policy	Rule	Result Message
□	2018-07-28 02:26:09	quaran-rem	correlation-policy	quaran-rule1	Successful completion of remediation

Page 1 of 1 Displaying row 1 of 1 rows

View Delete

Step 4 Once the remediation is complete, go to the TA GUI:

1. Navigate to **Visibility** > **Inventory Search**.
2. Enter the IP address of the infected host, and click **Search**.
3. In User Annotations, you should see **`quarantine = yes`** annotated to the IP address of the infected host.



User Annotations

1. orchestrator_system/service_endpoint =
2. quarantine = yes

IP 172.23.37.251

Scope Default ...3 more

Enforcement Groups Default ...3 more

Experimental Groups Default ...3 more

Internal? ✓ Yes

User Annotations orchestrator... ...1 more

What to do next

Once you clean the quarantined host and it is no longer infected, you can either use Tetration (recommended) to change the **`quarantine = yes`** annotation back to **`quarantine = no`** as follows:

- For example, if the quarantined host that is no longer infected is 172.21.208.11 and within the **`Default`** scope, create a CSV file such as:

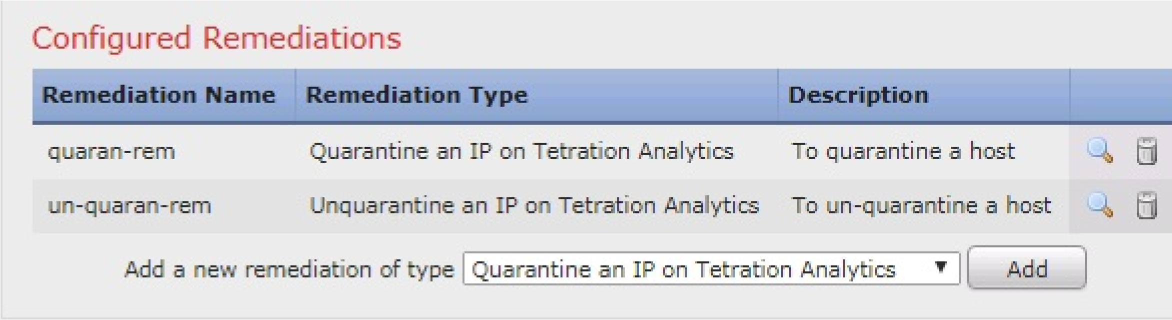
  ```
  IP,VRF,quarantine
  172.21.208.11,Default,no
  ```

- Navigate to **Applications** > **Inventory Upload**. For instructions on how to upload your CSV file to Tetration, see the online help user guide on your Tetration server:

  ```
  https://<your-Tetration-server-IP-address>/documentation/ui/inventory/user_annotations.html
  ```

Or, use the FMC remediation module to remove the quarantine (not recommended in production networks due to security concerns) as follows:

- (See Configure: Step 1) Add a new remediation that uses the un-quarantine type of remediation. Edit the same instance, and under **Configured Remediations**, select and add the un-quarantine type of remediation (in this example, **`un-quaran-rem`**).

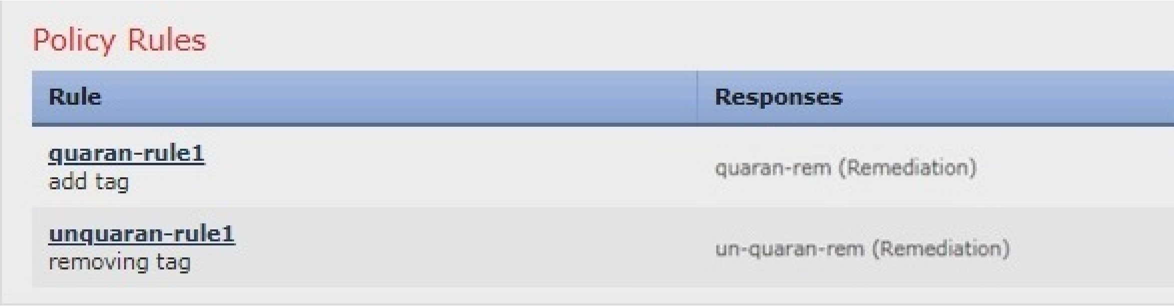


Configured Remediations

Remediation Name	Remediation Type	Description	
quaran-rem	Quarantine an IP on Tetration Analytics	To quarantine a host	🔍 🗑
un-quaran-rem	Unquarantine an IP on Tetration Analytics	To un-quarantine a host	🔍 🗑

Add a new remediation of type Quarantine an IP on Tetration Analytics ▼ Add

- (See Configure: Step 2) Add an access control rule (in this example, **`remove-tag`**) to the same policy (in this example, **`rem-policy`**) which can be used to trigger the un-quarantine remediation.
- (See Configure: Step 3) Add a correlation rule (in this example, **`unquaran-rule1`**) that uses the access control rule (in this example, **`remove-tag`**).
- (See Configure: Step 4) Assign the un-quarantine response (in this example, **`un-quaran-rem`**) to the correlation rule (in this example, **`unquaran-rule1`**).



Policy Rules

Rule	Responses
quaran-rule1 add tag	quaran-rem (Remediation)
unquaran-rule1 removing tag	un-quaran-rem (Remediation)

- Once that rule is matched, the un-quarantine remediation will be triggered to remove the quarantine annotation.