Cisco Secure Firewall Management Center Remediation Module for Cisco Secure Workload, Quick Start Guide

First Published: 2022-06-06

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

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

CHAPTER 1

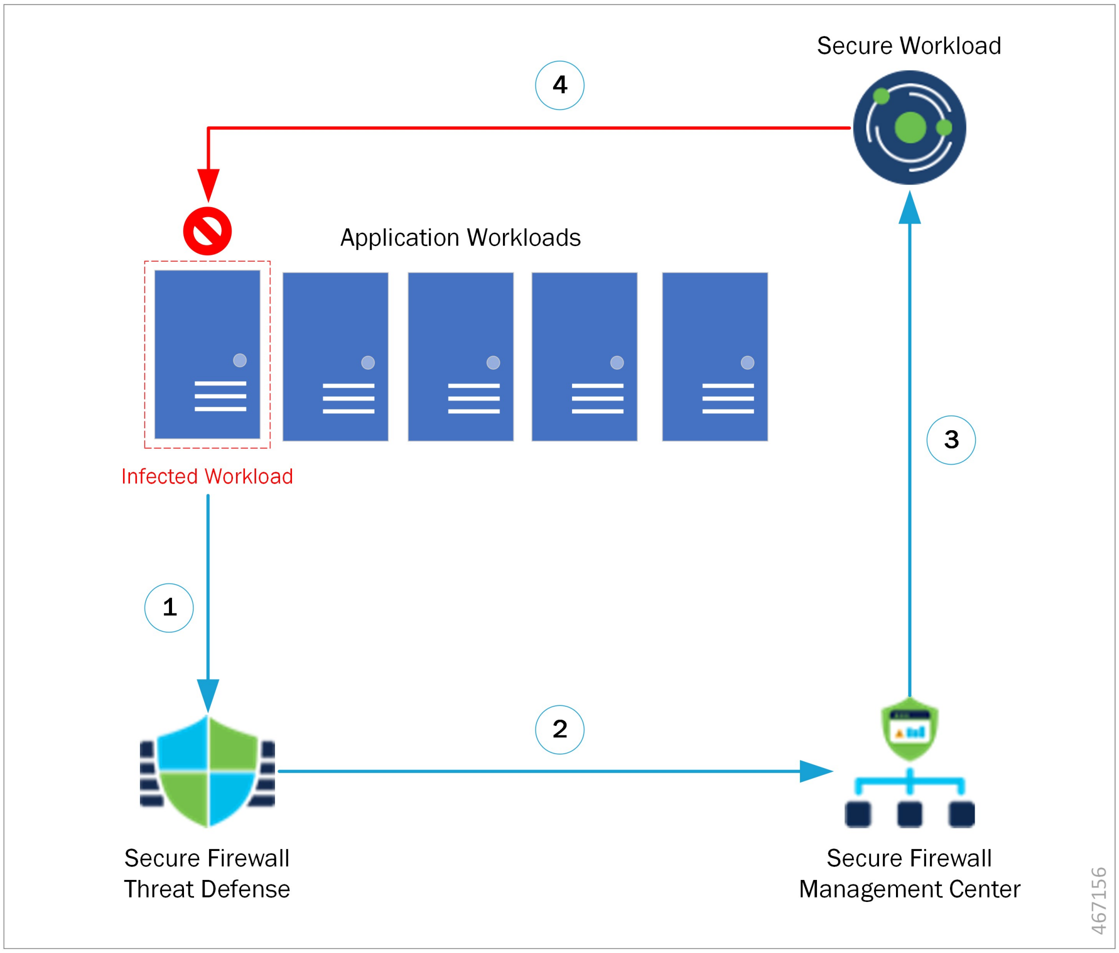
Introduction

The Cisco Secure Firewall Management Center remediation module for Cisco Secure Workload (formerly known as Tetration) helps to create remediations that your Secure Firewall Management Center can automatically launch when conditions on your network violate the associated correlation policy. For example, to assess the host status, and quarantine an offending host with the Secure Workload enforcement agent, you can block traffic at a device on the source or destination IP address. If multiple rules in a policy trigger, the Secure Firewall Management Center can launch responses for each rule. A remediation module is the package of files you install on the Secure Firewall Management Center to perform the response.

Overview

With the Cisco Secure Firewall Management Center (FMC) Remediation Module for Cisco Secure Workload (formerly known as Tetration), when an attack on your network from an infected host is detected by the FMC, the offending host can be quarantined by a Secure Workload 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 Secure Workload when the remediation module is installed:

Figure 1: Secure Firewall Management Center to Secure Workload Rapid Threat Containment



1	Threat Defense detects malicious traffic from infected workload.
2	Threat Defense sends an event with malicious traffic details to the Management Center.
3	Remediation module is triggered to quarantine infected workload.
4	Secure Workload sends quarantine request to the enforcement agent on workload.

The process of quarantining the network attack is as follows:

Step 1 An infected workload sends malicious traffic within the network. The malicious traffic is detected by Secure Firewall Threat Defense (FTD) running on a Secure Firewall device (physical or virtual).

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

Step 3 The action triggers the remediation module on the FMC to use the Secure Workload REST API to request that Secure Workload quarantine the infected workload.

Step 4 Secure Workload quickly contains the infected workload by sending a quarantine request to the enforcement agent on the infected workload.

Prerequisites

- Pre-define absolute policies in Secure Workload to drop all traffic from and to any host annotated with 'quarantine.' If a partial quarantine is what you want, customize the policy in Secure Workload to deny only some, but not all, types of traffic. For more information, see Related Documentation, on page 3.
- Secure Workload 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 Related Documentation, on page 3.

Related Documentation

- Secure Firewall Management Center Configuration Guides
- The user guide available from the Secure Workload web interface.
- Cisco Secure Workload Documentation

CHAPTER 2

Downloading and Installing the Remediation Module

The following section provides the steps to download and install the FMC remediation module for Secure Workload (formerly Tetration).

Install the Remediation Module

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:

a. In the FMC web interface, navigate to **Policies** > **Actions** > **Modules**.

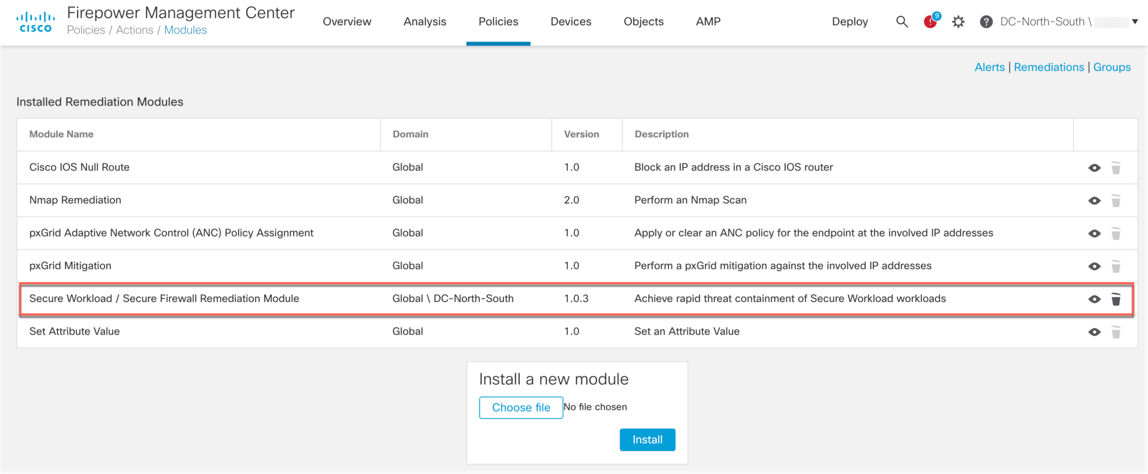
b. In the **Install a new module** dialog box, click **Choose File**.

c. Select the file for the remediation module that was downloaded in Step 1.

d. Click **Install**.

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

When successfully installed, the Secure Firewall Management Center Remediation Module for Secure Workload is displayed in the list of installed remediation modules:


Firepower Management Center
Policies / Actions / Modules
Overview
Analysis
Policies
Devices
Objects
AMP
Deploy
DC-North-South \
Alerts | Remediations | Groups

Installed Remediation Modules

Module Name	Domain	Version	Description
Cisco IOS Null Route	Global	1.0	Block an IP address in a Cisco IOS router
Nmap Remediation	Global	2.0	Perform an Nmap Scan
pxGrid Adaptive Network Control (ANC) Policy Assignment	Global	1.0	Apply or clear an ANC policy for the endpoint at the involved IP addresses
pxGrid Mitigation	Global	1.0	Perform a pxGrid mitigation against the involved IP addresses
Secure Workload / Secure Firewall Remediation Module	Global \ DC-North-South	1.0.3	Achieve rapid threat containment of Secure Workload workloads
Set Attribute Value	Global	1.0	Set an Attribute Value

Install a new module

Choose file No file chosen

Install

CHAPTER 3

Configuring the Remediation Module

The following section provides the steps for configuring the remediation module.

Configure

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

Step 1 In FMC, create an instance of the remediation module for each Secure Workload cluster in your network:

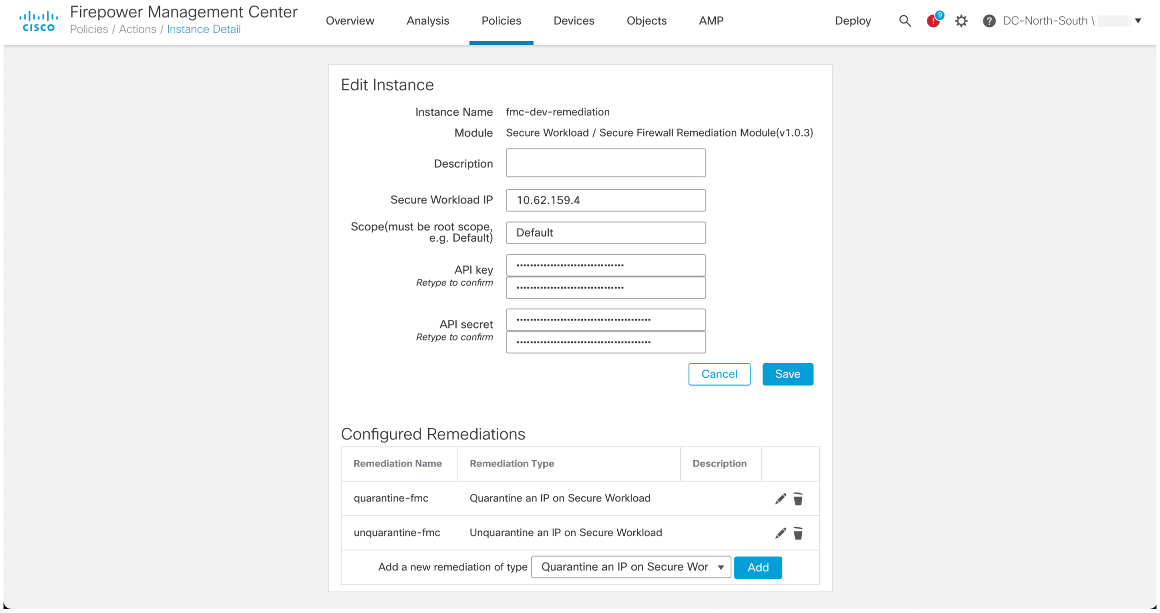
a. Navigate to **Policies** > **Actions** > **Instances**.

b. Select the remediation module in the drop-down list, and click **Add**.

c. Enter an **Instance Name** (in this example, **`fmc-dev-remediation`**).

d. Enter the Secure Workload 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 Secure Workload server at this point. The API key and secret must first be created in Secure Workload by a site admin, customer support, or a root scope owner role. Copy that information for use here. For more details, see Related Documentation, on page 3.



Firepower Management Center
Policies / Actions / Instance Detail
Overview
Analysis
Policies
Devices
Objects
AMP
Deploy
DC-North-South \

Edit Instance

Instance Name	fmc-dev-remediation
Module	Secure Workload / Secure Firewall Remediation Module(v1.0.3)
Description	
Secure Workload IP	10.62.159.4
Scope(must be root scope, e.g. Default)	Default
API key	••••••••••••••••••••••••••••••
Retype to confirm	••••••••••••••••••••••••••••••
API secret	••••••••••••••••••••••••••••••••••••••
Retype to confirm	••••••••••••••••••••••••••••••••••••••

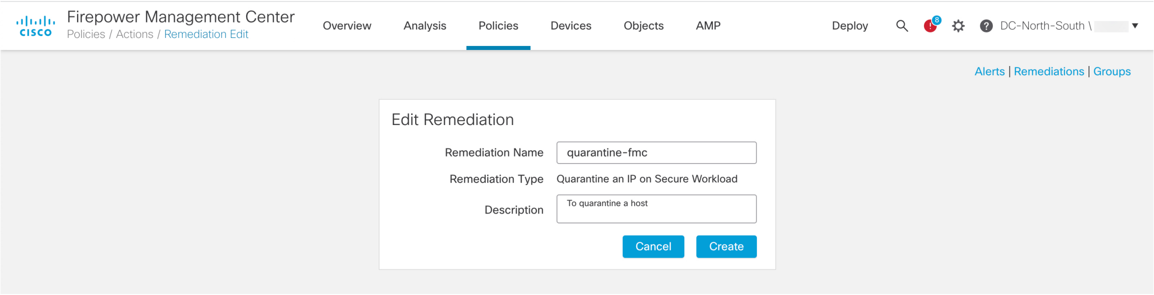
Configured Remediations

Remediation Name	Remediation Type	Description	
quarantine-fmc	Quarantine an IP on Secure Workload		
unquarantine-fmc	Unquarantine an IP on Secure Workload		

Add a new remediation of type Quarantine an IP on Secure Wor ▾ Add

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

f. Enter a **Remediation Name** (in this example, **`quarantine-fmc`**), and click **Create**.



Firepower Management Center
Policies / Actions / Remediation Edit
Overview
Analysis
Policies
Devices
Objects
AMP
Deploy
DC-North-South \
Alerts | Remediations | Groups

Edit Remediation

Remediation Name	quarantine-fmc
Remediation Type	Quarantine an IP on Secure Workload
Description	To quarantine a host

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

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

a. Navigate to **Policies** > **Access Control** and click the **Edit** icon of the access control policy to add rules.

b. Click **Add Rule** and enter a name (for example, **`block-ssh-add-tag`**).

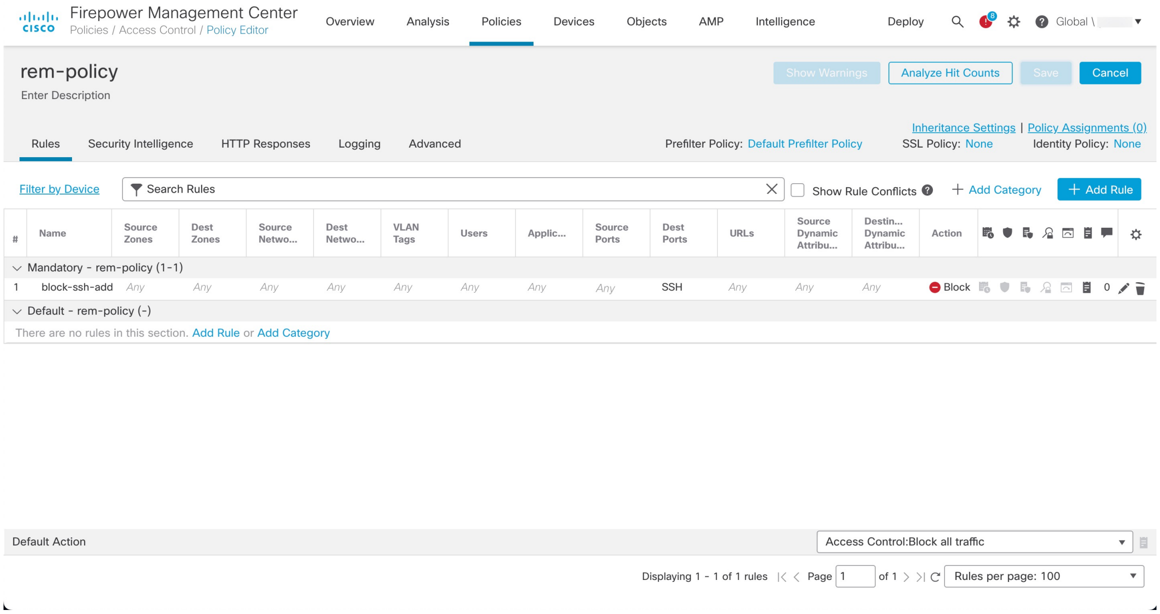
c. Select **Block** for the **Action**.

d. On the **Ports** tab, select **SSH** from the list of protocols for the destination port.

e. 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, and click **Add**

f. Click **Save**.



rem-policy

Enter Description

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

#	Name	Source Zones	Dest Zones	Source Netwo...	Dest Netwo...	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source Dynamic Attribu...	Destin... Dynamic Attribu...	Action
Mandatory - rem-policy (1-1)														
1	block-ssh-add	Any	Any	Any	Any	Any	Any	Any	Any	SSH	Any	Any	Any	Block
Default - rem-policy (-)														

There are no rules in this section. Add Rule or Add Category

Default Action: Access Control:Block all traffic

Displaying 1 - 1 of 1 rules Page 1 of 1 Rules per page: 100

Step 3 Configure a correlation rule:

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

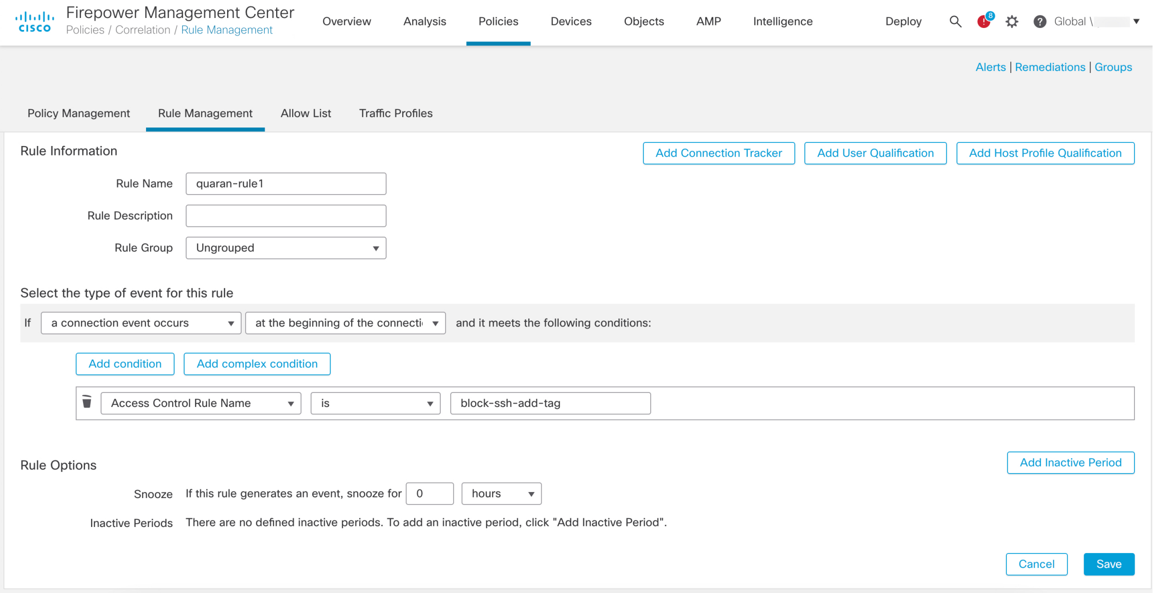
b. Click **Create Rule**.

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

d. 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**.

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

f. 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:

Rule Group: Ungrouped

Select the type of event for this rule

If a connection event occurs at the beginning of the connecti and it meets the following conditions:

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".

g. Click **Save**.

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

a. Navigate to **Policies** > **Correlation** > **Policy Management**.

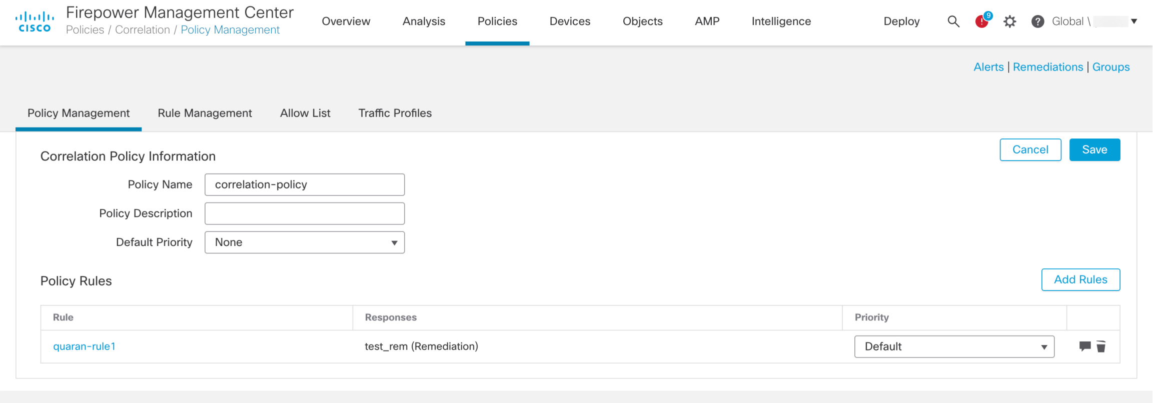
b. Click **Create Policy**.

c. Enter a **Policy Name** (in this example, **`correlation-policy`**) and description (optional).

d. From the **Default Priority** drop-down list, select a priority for the policy. Select **None** to use rule priorities only.

e. Click **Add Rules**, select the correlation rule you previously configured in Step 3 (in this example, **`quaran-rule1`**), and click **Add**.

f. Click the **Responses** icon next to the rule and assign a response (in this example, **`test_rem`**) to the rule. Click **Update**.



Correlation Policy Information

Policy Name: correlation-policy

Policy Description:

Default Priority: None

Policy Rules

Rule	Responses	Priority
quaran-rule1	test_rem (Remediation)	Default

g. Click **Save**.

CHAPTER 4

Verifying Remediation

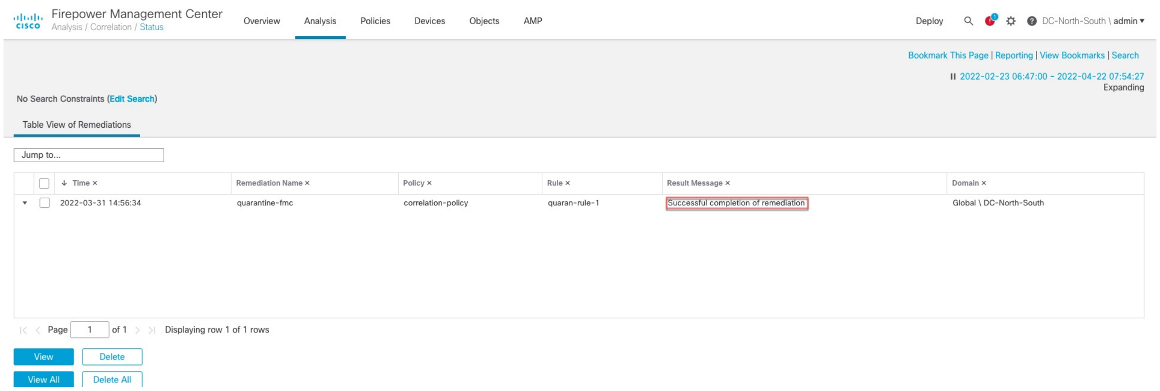
The following section provides the steps to verify if the remediation process is successful.

Verify Remediation

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

Step 1 After the remediation module is triggered by an associated correlation rule, check the status of the remediation execution. In the FMC web interface, navigate to **Analysis** > **Correlation** > **Status**.

Step 2 In the Remediation Status table, find the row for your policy and view the result message.


Firepower Management Center
Analysis / Correlation / Status
Overview
Analysis
Policies
Devices
Objects
AMP
Deploy
DC-North-South \ admin ▾
Bookmark This Page | Reporting | View Bookmarks | Search
Jump to...
View
Delete
View All
Delete All

⏸ 2022-02-23 06:47:00 - 2022-04-22 07:54:27
Expanding

No Search Constraints (Edit Search)

Table View of Remediations

	□	↓ Time ×	Remediation Name ×	Policy ×	Rule ×	Result Message ×	Domain ×
▾	□	2022-03-31 14:56:34	quarantine-fmc	correlation-policy	quaran-rule-1	Successful completion of remediation	Global \ DC-North-South

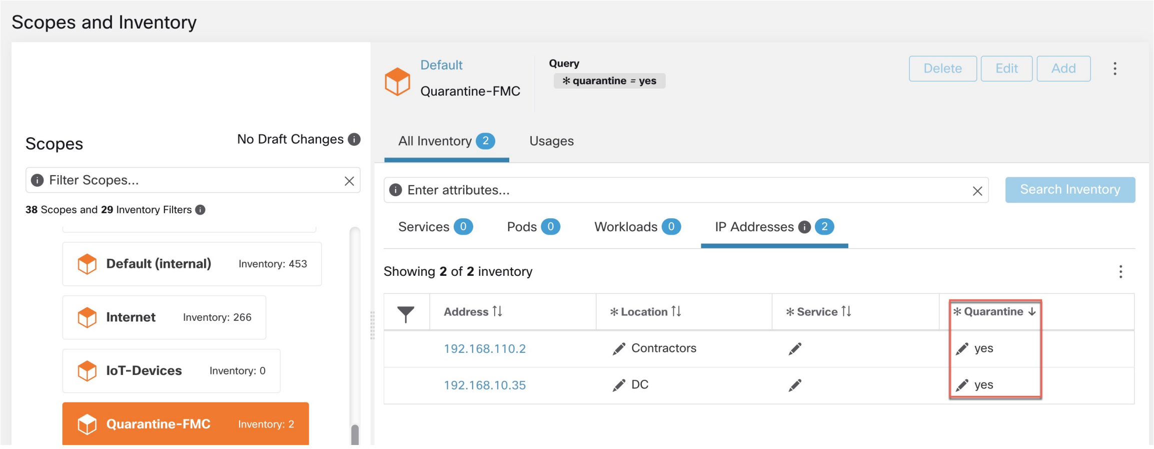
Page 1 of 1 Displaying row 1 of 1 rows

Step 3 Once the remediation is complete, perform the following steps:

a. In the Secure Workload user interface, navigate to **Visibility** > **Inventory Search**.

b. Enter the IP address of the infected hosts, and click **Search**.

c. In User Annotations, you should see **`quarantine = yes`** annotated to the IP address of the infected hosts.



Scopes and Inventory

Scopes — No Draft Changes

Filter Scopes...

38 Scopes and 29 Inventory Filters

Scope	Inventory
Default (internal)	Inventory: 453
Internet	Inventory: 266
IoT-Devices	Inventory: 0
Quarantine-FMC	Inventory: 2

Default
Quarantine-FMC — Query: quarantine = yes

All Inventory 2 — Usages

Enter attributes... — Search Inventory

Services 0 — Pods 0 — Workloads 0 — IP Addresses 2

Showing 2 of 2 inventory

Address	Location	Service	Quarantine
192.168.110.2	Contractors		yes
192.168.10.35	DC		yes

What to do next

Once you clean the quarantined host and it is no longer infected, you can perform either of the following actions to remove the quarantine annotation:

- (**Recommended**) Use Secure Workload to change the **`quarantine = yes`** annotation back to **`quarantine = no`**.

  1. 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:

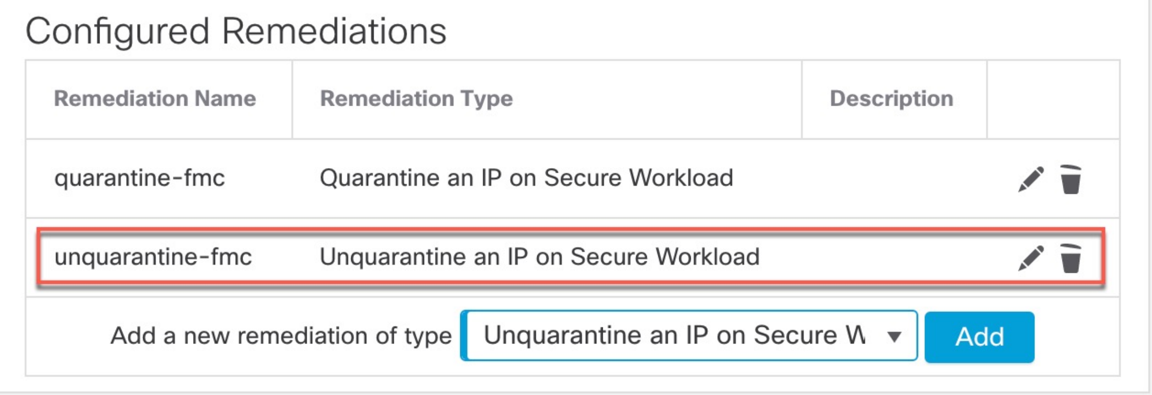
     ```
     IP,VRF,quarantine
     172.21.208.11,Default,no
     ```

  2. Navigate to **Applications** > **Inventory Upload**, and then upload the CSV file to Secure Workload. For more information on how to upload a CSV file to Secure Workload, see the Related Documentation, on page 3 section.

- Use FMC Remediation Module to remove the quarantine annotation.

  Important This method is not recommended in production networks due to security concerns.

  1. (In the Configure section, see 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, **`unquarantine-fmc`**).



Configured Remediations

Remediation Name	Remediation Type	Description	
quarantine-fmc	Quarantine an IP on Secure Workload		
unquarantine-fmc	Unquarantine an IP on Secure Workload		

Add a new remediation of type: Unquarantine an IP on Secure W ▼

2. (In the Configure section, see Step 2) Add an access control rule (For example, **`remove-tag`**) to the same policy (For example, **`rem-policy`**) which can be used to trigger the un-quarantine remediation.

3. (In the Configure section, see Step 3) Add a correlation rule (For example, **`unquaran-rule1`**) that uses the access control rule (in this example, **`remove-tag`**).

4. (In the Configure section, see Step 4ß) Assign the un-quarantine response (For example, **`un-quaran-rem`**) to the correlation rule (For example, **`unquaran-rule1`**).

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