



## **Cisco APIC/FirePOWER Remediation Module Quick Start Guide 2.0.1**

**First Published:** 2022-06-07

**Last Modified:** 2022-06-07

### **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



# CONTENTS

**Full Cisco Trademarks with Software License ?**

---

**CHAPTER 1**

**About the Remediation Module 1**

About the Remediation Module 1

Supported Features 2

---

**CHAPTER 2**

**Deploy the Remediation Module 5**

Download and Install the Cisco Firepower Management Center Remediation Module for ACI 5

The Remediation and Quarantine Process 6

Optionally Create a Management Contract and Contract EPG 6

Create a Remediation Module Instance and Type 8

Configure an Access Control Rule for the Remediation 10

Configure a Correlation Rule for the Remediation 11

Associate the Correlation Rule with the Remediation Module Instance 12

Verify the Remediation in the FMC 13

Verify the Quarantine in APIC 13

Manually Quarantine an IP Address 15

---

**CHAPTER 3**

**Related Documentation 19**

Related Documentation 19

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO 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 MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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](http://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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.





# CHAPTER 1

## About the Remediation Module

---

- [About the Remediation Module, on page 1](#)
- [Supported Features, on page 2](#)

### About the Remediation Module

With the Cisco Firepower Management Center Remediation Module for ACI, when an attack on your network is detected by the FMC, the offending endpoint can be completely quarantined in the Application Policy Infrastructure Controller (APIC) so that no further traffic is allowed to go in or out of that endpoint. The following figure shows the relationship between the FMC and the APIC when the remediation module is installed.

#### Compatibility

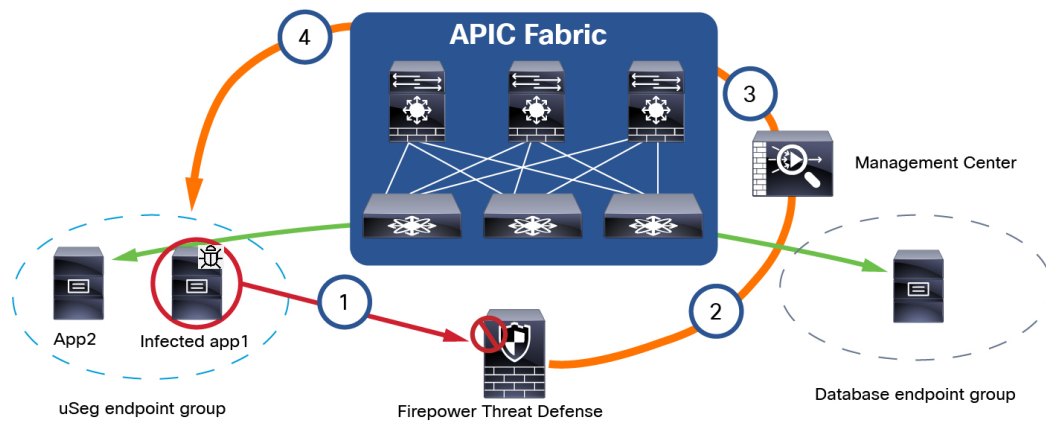
The following table shows the compatibility between the Cisco Firepower Management Center Remediation Module for ACI, FMC, and APIC.

**Table 1: Compatibility with the remediation module, FMC and APIC**

Remediation module version compatible with....	FMC version	APIC version
2.0.1	6.7 and later	5.1(1h)

#### Infected endpoint

The following figure shows how the Cisco Firepower Management Center Remediation Module for ACI reacts when an infected endpoint is detected.



The process is as follows:

1. An endpoint with an infected application in an endpoint group (endpoint group on the left) launches an attack on another endpoint in Database EPG. The attack is blocked inline by a managed device (such as a physical or virtual device running Firepower Threat Defense).
2. An attack event is generated and sent to the FMC. The attack event includes information about the infected endpoint.
3. The attack event triggers the remediation module for APIC, which used the APIC northbound (NB) API to contain the infected endpoint in the ACI fabric.
4. The APIC quickly contains or quarantines the infected application workload into an isolated microsegment (uSeg) EPG.

Because App2 is not infected, it can still communicate on the network.

You can quarantine a source endpoint, a destination endpoint, or both, as the next section shows.

## Supported Features

This release enables you to quarantine offending endpoints that are detected by the Cisco Firepower Management Center Remediation Module for ACI, using APIC version 5.1(1h). For version 2.0.1 of the remediation module, the supported behavior when endpoints are quarantined is described in the following table:

	VMware Distributed Virtual Switch (DVS)	Bare metal
Verified in IPS inline mode	Yes	Yes
EPG bridge mode	Yes	Yes
EPG routed mode	No	No
Multiple IP to one MAC checking	Yes	Yes
Create only an IP address filter uSeg attribute	No	No

	<b>VMware Distributed Virtual Switch (DVS)</b>	<b>Bare metal</b>
Create both an IP address filter and a MAC address filter uSeg attribute	Yes	Yes
Quarantine source and destination endpoints	Yes	Yes
Apply a predefined management contract to source and destination endpoints	Yes	Yes
Always allow traffic to critical servers	Yes	Yes







## CHAPTER 2

# Deploy the Remediation Module

- [Download and Install the Cisco Firepower Management Center Remediation Module for ACI, on page 5](#)
- [The Remediation and Quarantine Process, on page 6](#)
- [Verify the Remediation in the FMC, on page 13](#)
- [Verify the Quarantine in APIC, on page 13](#)
- [Manually Quarantine an IP Address, on page 15](#)

## Download and Install the Cisco Firepower Management Center Remediation Module for ACI

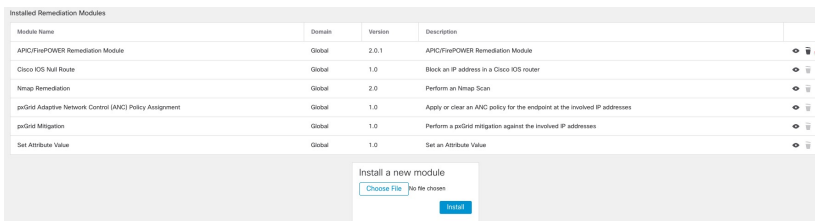
### Before you begin

Make sure you're using compatible versions as shown in the following table.

*Table 2: Compatibility with the remediation module, FMC and APIC*

Remediation module version compatible with....	FMC version	APIC version
2.0.1	6.7 and later	5.1(1h)

- Step 1** Download the Cisco Firepower Management Center Remediation Module for ACI ([link to download](#)) to a machine on which you'll connect to the FMC.
- Step 2** If you haven't done so already, log in to the FMC.
- Step 3** Click **Policies > Actions > Modules**.
- Step 4** In the Install a New Module section, click **Browse**.
- Step 5** Follow the prompts to upload the remediation module.
- Step 6** Click **Install**.
- Step 7** When successfully installed, the Cisco Firepower Management Center Remediation Module for ACI is displayed in the list of installed remediation modules:



Module Name	Domain	Version	Description
APIC/FirePOWER Remediation Module	Global	2.0.1	APIC/FirePOWER Remediation Module
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
psGrid Adaptive Network Control (ANC) Policy Assignment	Global	1.0	Apply or clear an ANC policy for the endpoint at the involved IP addresses
psGrid Mitigation	Global	1.0	Perform a psGrid mitigation against the involved IP addresses
Set Attribute Value	Global	1.0	Set an Attribute Value

## The Remediation and Quarantine Process

The following topics discuss the process of creating a remediation and quarantining an endpoint.

### Related Topics

[Create a Remediation Module Instance and Type](#), on page 8

[Configure an Access Control Rule for the Remediation](#), on page 10

[Configure a Correlation Rule for the Remediation](#), on page 11

[Associate the Correlation Rule with the Remediation Module Instance](#), on page 12

[Optionally Create a Management Contract and Contract EPG](#), on page 6

## Optionally Create a Management Contract and Contract EPG

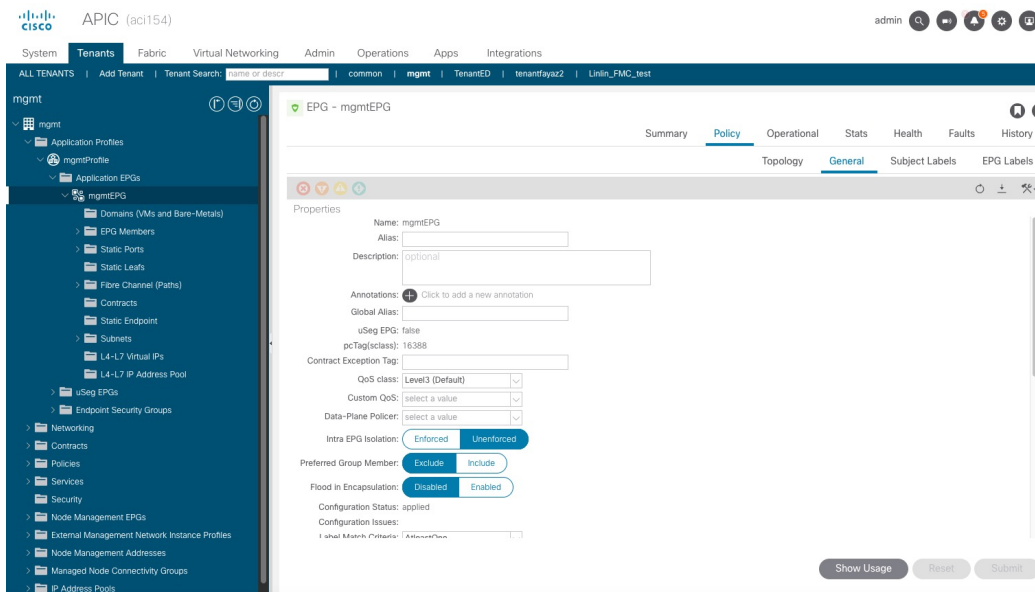
You can optionally predefine an APIC traffic filtering contract in the common tenant and a management EPG in the mgmt tenant to initiate a connection to the quarantined uSeg EPG. To use this optional configuration, you *must* define a management EPG in APIC in its **mgmt** tenant, and you *must* define a contract in the **common** tenant.

For more information, see the *Cisco APIC Basic Configuration Guide*.

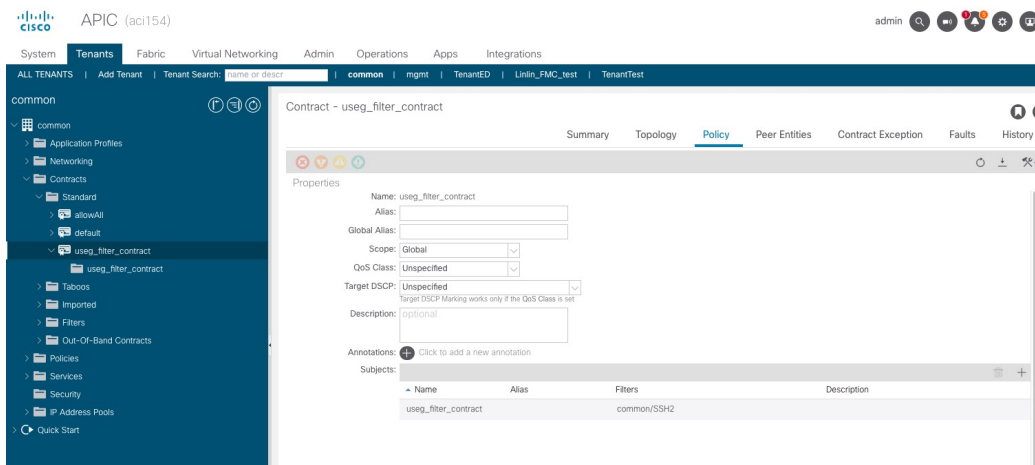
If you do not wish to create contracts, skip this section and continue with [Create a Remediation Module Instance and Type](#), on page 8.

- Step 1** Log in to APIC.
- Step 2** Click **Tenants**.
- Step 3** Double-click **mgmt**.
- Step 4** Expand **Application Profiles** > **mgmt Profile** > **Application EPGs**.
- Step 5** Click **mgmtEPG**.
- Step 6** In the right pane, click **Policy** > **General**.

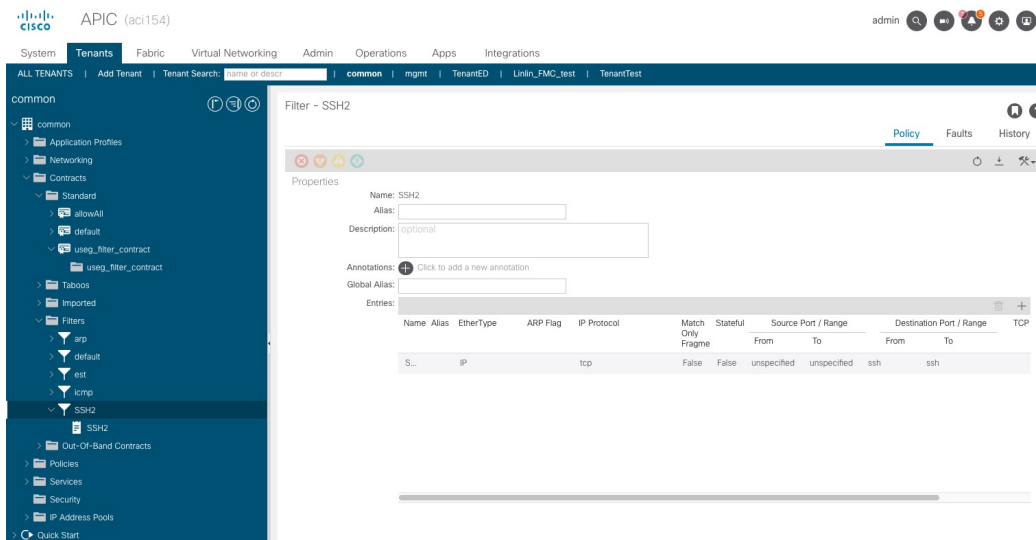
The following figure shows an example.



- Step 7** Click **ALL TENANTS**.
- Step 8** Double-click **common**.
- Step 9** Expand **Contracts > Standard**.
- Step 10** Click **useg\_filter\_contract**.
- Step 11** In the right pane, click the **Policy** tab.
- The following figure shows an example.



- Step 12** Under the common tenant, expand the name of your filter; for example, **Filters > SSH2**.
- The following figure shows an example



### What to do next

See [Create a Remediation Module Instance and Type](#), on page 8.

## Create a Remediation Module Instance and Type

For the Firepower Management Center to be able to detect and quarantine threats, you must configure on the Firepower Management Center a remediation module instance and type. For more information about remediations, see the [Firepower Management Center Administration Guide](#).

- Step 1** If you haven't done so already, log in to the FMC.
- Step 2** Click **Policies > Actions > Instances**.
- Step 3** From the **Select a module type** list, click **APIC/FirePOWER Remediation Module (2.0.1)**.
- Step 4** Click **Add**.  
The Edit Instance page is displayed as follows.

### Edit Instance

Instance Name

Module APIC/Secure Firewall Remediation Module(v2.0.2)

Description

APIC server username\*

APIC server password\*   
*Retype to confirm*

APIC cluster instance 1 IP\*

APIC cluster instance 2 IP

APIC cluster instance 3 IP

APIC cluster instance 4 IP

APIC cluster instance 5 IP

IP addresses NOT to quarantine  
(a list of strings )

Management Contract Name

Management EPG Name

**Step 5**

Enter the following information:

Item	Description
<b>Instance name</b>	Enter a name to identify this instance. (Spaces are not allowed in the name.)
<b>Description</b>	(Optional.) Enter a description.
<b>APIC server username</b>	Enter the user name of an APIC user with admin privileges.
<b>APIC server password</b>	Enter and re-enter the user's password
<b>APIC cluster instance 1 IP</b>	Enter the IP address of the APIC server or of the first server in the cluster.

Item	Description
<b>APIC cluster instance x IP</b>	(Optional.) If your APIC cluster has more than one server, enter additional IP addresses in the provided fields.
<b>IP addresses NOT to quarantine</b>	(Optional.) Enter a list of IP addresses to always exclude from the quarantine. Separate IP addresses with Enter.
<b>Management Contract Name</b>	(Optional.) Enter the name of the management contract you created in APIC. For more information, see the <i>Cisco APIC Basic Configuration Guide</i> .
<b>Management EPG Name</b>	(Optional.) Enter the name of the EPG with which the management contract is associated.

**Step 6** In the Configured Remediation section at the bottom of the page, click one of the following then click **Add**:

- **Quarantine the destination End Point on APIC**
- **Quarantine the source End Point on APIC**

**Step 7** On the Edit Remediation page, enter the following information:

- **Remediation Name:** Enter a name to identify the remediation instance.
- (Optional.) **Description:** Enter a description of the remediation instance.

**Step 8** Click **Create**.

**Step 9** Click **Done**.

**Step 10** On the Edit Instance page, optionally configure another remediation.

---

### What to do next

See [Configure an Access Control Rule for the Remediation, on page 10](#).

## Configure an Access Control Rule for the Remediation

This example shows how to create an access control rule that blocks the SSH protocol. After creating this rule, any endpoint that attempts to SSH to another endpoint in an monitored EPG, the offending node or nodes are quarantined.

**Step 1** If you haven't done so already, log in to the FMC.

**Step 2** Click **Policies > Access Control**.

**Step 3** Create a new access control policy or click **Add Rule** to add a rule to an existing policy.

Enter the following information.

Item	Description
<b>Name</b> field	Enter a name to identify this rule. <i>Write down</i> the name because you'll need it later.
<b>Action</b> list	Click <b>Block</b> .
<b>Ports</b> tab page	From the <b>Available Ports</b> list, scroll to SSH and click <b>Add to Destination</b> .
<b>Logging</b> tab page	Select the <b>Log at Beginning of Connection</b> check box.

For more information about access control rules, see the [Firepower Management Center Device Configuration Guide](#).

**Step 4** Click **Add**.

**Step 5** At the top of the page, click **Save**.

### What to do next

See [Configure a Correlation Rule for the Remediation](#), on page 11.

## Configure a Correlation Rule for the Remediation

A correlation rule provides conditions in which the system responds to threats. The following task discusses how to set up a correlation rule that is triggered at any point in the connection when your access control rule conditions are met. In particular, the sample access control policy and rule are triggered when SSH traffic is passed between a source and destination endpoint.

For more information about correlation policies and rules, see the [Firepower Management Center Administration Guide](#).

- Step 1** If you haven't done so already, log in to the FMC.
- Step 2** Click **Policies > Correlation**.
- Step 3** Click the **Rule Management** tab.
- Step 4** Click **Create Rule**.
- Step 5** Enter a name to identify the rule and an optional description.
- Step 6** In the Select the type of event for this rule section, click **a connection event occurs** and **at any point of the connection**.
- Step 7** Set up the rest of the rule as shown in the following figure.

The screenshot shows the 'Rule Management' tab in the FMC interface. The 'Rule Information' section includes fields for 'Rule Name' (MyCorrelationRule), 'Rule Description', and 'Rule Group' (Ungrouped). There are buttons for 'Add Connection Tracker', 'Add User Qualification', and 'Add Host Profile Qualification'. Below this, the 'Select the type of event for this rule' section is configured with 'If a connection event occurs at any point of the connection and it meets the following conditions:'. There are buttons for 'Add condition' and 'Add complex condition'. The conditions are listed in a table:

AND	Access Control Policy	is	SampleAC
	Access Control Rule Name	is	Block SSH

Substitute the name of your access control policy and rule name for those shown in the preceding figure.

- Step 8** Set other options as desired and click **Save**.

### What to do next

See [Associate the Correlation Rule with the Remediation Module Instance, on page 12](#).

## Associate the Correlation Rule with the Remediation Module Instance

The final step in configuring the FMC for remediation and quarantine is to associate your correlation rule with your remediation policy. After you do this, when the FMC detects a threat, the offending endpoints are quarantined in APIC.

- Step 1** If you haven't done so already, log in to the FMC.
- Step 2** Click **Policies > Correlation**.
- Step 3** Click the **Policy Management** tab.
- Step 4** Click **Create Policy**.
- Step 5** Enter a policy name and optional policy description.
- Step 6** Do not change **Default Priority**.
- Step 7** Click **Add Rules**.
- Step 8** Select the check box next to the name of the correlation rule you created earlier.
- Step 9** Click **Add**.



- Step 10** Click **Responses** (🗨️).
- Step 11** From the **Unassigned Responses** list, double-click the name of your remediation policy to move it to **Assigned Responses**.
- Step 12** Click **Update**.
- Step 13** At the top of the page, click **Save**.
- Step 14** Move the slider for the remediation policy to **Slider enabled** (🔘).

## Verify the Remediation in the FMC

Because remediations can fail for various reasons, complete the following steps to verify that no error messages are listed for the remediation status on the FMC.

- Step 1** If you haven't done so already, log in to the FMC.
- Step 2** Click **Analysis > Correlation > Status**.
- Step 3** In the Remediation Status table, find the row for your policy and view the result message. The following figure shows an example

The screenshot shows the FMC interface with the 'Analysis / Correlation / Status' page. The 'Table View of Remediations' section contains a table with the following data:

Time	Remediation Name	Policy	Rule	Result Message
2022-01-24 17:12:15	quarantine_src	http_policy	cr_1	Successful completion of remediation

- Step 4** If the remediation was successful, see [Verify the Quarantine in APIC, on page 13](#).
- Step 5** If an error is displayed, the endpoint might still be quarantined if subsequent remediation events are successful.
- Step 6** If you see an error, see [Verify the Quarantine in APIC, on page 13](#) to verify whether or not the quarantine was successful. If the quarantine was eventually successful, you can ignore all of its error messages.

### What to do next

See [Verify the Quarantine in APIC, on page 13](#).

## Verify the Quarantine in APIC

### Before you begin

Complete the tasks discussed in [Verify the Remediation in the FMC, on page 13](#).

- Step 1** Log in to APIC.
- Step 2** Click the **Tenants** tab page.
- Step 3** Click **ALL TENANTS**.
- Step 4** Double-click the name of the tenant that is infected.
- Step 5** Expand the infected application in the left pane.
- Step 6** Click **uSeg EPGs**
- Step 7** Click the EPG quarantine for the quarantined endpoint.
- Step 8** In the right panel, click **Policies > General**.
- Step 9** Verify that one or more uSeg attributes were created on the APIC server.  
The following figure shows an example.

The screenshot displays the Cisco APIC interface for configuring an EPG. The left navigation pane shows the hierarchy: Tenant ed > uSeg EPGs > EPG quarantine-epg11. The main content area shows the configuration for 'quarantine-epg11' under the 'General' tab. Key configuration details include:

- Name: quarantine-epg11
- Description: optional
- Tags: enter tags separated by comma
- Alias:
- uSeg EPG: true
- pcTag(class): 32772
- QoS class: Unspecified
- Custom QoS: select a value
- Intra EPG Isolation: Enforced
- Preferred Group Member: Exclude
- Configuration Status: applied
- Label Match Criteria: AtleastOne
- Bridge Domain: ed/bd-ext
- Resolved Bridge Domain: ed/bd-ext
- Monitoring Policy: select a value

The 'uSeg Attributes' table lists the quarantined device:

Name	Value
192.168.103.21	IP Address: 192.168.103.21

The figure shows that a device at IP address 192.168.103.21 has been quarantined.

**Note** For VMware DVS and Bare Metal (in bridged mode), two attributes (filters) are automatically created when an endpoint is quarantined, one attribute for the IP address and one attribute for the MAC address. Therefore, to remove the quarantine, you must delete both attributes.

- Step 10** If no uSeg attributes were created, but you know that the conditions set by a correlation rule were met, the quarantine failed. To manually quarantine the IP address, see [Manually Quarantine an IP Address, on page 15](#).
- 

**What to do next**

See [Verify the Remediation in the FMC, on page 13](#).

## Manually Quarantine an IP Address

You can try to manually quarantine an IP address if the quarantine discussed earlier in this chapter failed.

---

- Step 1** Find the IP address of the endpoint to quarantine.
- If you haven't done so already, log in to the FMC.
  - Click **Analysis > Correlation > Status**.
  - Find the timestamp of entry for the unsuccessful quarantine and make note of the source IP address.
  - On the Operations tab page, click **EP Tracker**, enter the IP address, and press Enter.
  - If no information is displayed, the endpoint cannot be quarantined. If more than one IP address is displayed, look for the one in the offending tenant.
- Step 2** If you can identify the EPG of the endpoint that you want to quarantine, create a uSeg EPG attribute corresponding to this endpoint.
- To find the MAC address of the IP address to quarantine, go to the APIC Object Store Browser at [https://apic\\_IP\\_address/visore.html](https://apic_IP_address/visore.html). Use the IP address of the endpoint to run a query and display the MAC address. The following figure shows an example.

## APIC Object Store Browser

Filter			
Class or DN:	fvCEp		
Property:	ip	Op: ==	Val1: 192.168.103.21
			Val2:
Run Query			

[Display URI of last query](#)

[Display last response](#)

fvCEp	
childAction	
contName	
dn	<a href="#">uni/tn-ed/ap-app2/epg-quarantine-epg11/cep-00:50:56:81:7F:A9</a>
encap	vlan-176
id	0
idepdn	
ip	192.168.103.21
lcC	learned,vmm
lcOwn	local
mac	00:50:56:81:7F:A9

- Right-click **Domains** (VMs and Bare Metals) under the newly created uSeg EPG, and add a domain association with the same name and domain type as the original EPG.
- For Bare Metal, right-click **Static Leafs**, and click **Statically Link With Node**.
- Log in to APIC.
- Click **Tenants > ALL TENANTS**.
- Double-click the tenant that contains the endpoint to be quarantined.
- Expand **Networking > Bridge Domains**.
- Make note of the EPG bridge domain.
- Expand **Application Profiles > profile-name > Application EPGs > epg-name** and make note of the domain profile name.
- Expand **Application Profiles** and right-click **uSeg EPG**.
- Click **Create uSeg EPG**.
- Enter a name for the uSeg EPG, in the format **uSegEPGendpoint-name**. (For example, **uSegEPG-EPG1**.)
- From the **Bridge Domain** list, click the EPG's bridge domain.
- Click **Next**.
- On the Domains page, click **Add (+)**.
- From the **Domain Profiles** list, click the domain profile.
- Set the **Deployment Immediacy** to **Immediate**.
- Set the **Resolution Immediacy** to **Immediate**.
- Add an IP filter attribute by clicking **Add (+)** on the lower right and entering the IP address for the name and filter.

t) Click **Update** and then click **Finish**.

If the uSeg EPG is not displayed, refresh your browser page.

u) Click **uSeg Attributes**.

v) Click **Add (+)**

w) Add attributes for the quarantined host's IP address and MAC address with an operator of **Match Any**.

For the IP filter, use the IP address as the name. For MAC filter, use the IP address plus an underscore and the last three octets of the MAC address as a name.

x) Click **Submit**.

### Step 3

Verify that no traffic can go into or out from the quarantined endpoint.

For example, after an IP address is quarantined, pinging it should fail.

---





## CHAPTER 3

# Related Documentation

---

- [Related Documentation](#), on page 19

## Related Documentation

For additional information about the Cisco Firepower Management Center Remediation Module for ACI, see the [appropriate guide](#).

For additional information about the Cisco APIC and ACI, see [APIC Documentation](#).

For information on using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see the [Support Case Manager](#).

