



Deploy the Remediation Module

- [Download and Install the APIC/Secure Firewall Remediation Module, on page 1](#)
- [The Remediation and Quarantine Process, on page 2](#)
- [Verify the Remediation in the Management Center, on page 9](#)
- [Verify the Quarantine in APIC, on page 9](#)
- [Manually Quarantine an IP Address, on page 11](#)

Download and Install the APIC/Secure Firewall Remediation Module













Before you begin

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

Table 1: Compatibility with the remediation module, Management Center and APIC

Remediation module version compatible with....	Management Center version	APIC version
2.0.2	7.0 and later	5.1(1h)

- Step 1** Download the APIC/Secure Firewall Remediation Module ([link to download](#)) to a machine on which you'll connect to the management center.
- Step 2** If you haven't done so already, log in to the management center.
- 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 APIC/Secure Firewall Remediation Module is displayed in the list of installed remediation modules:

Module Name	Version	Description	
APIC/Secure Firewall Remediation Module	2.0.2	APIC/Secure Firewall Remediation Module	 
Cisco IOS Null Route	1.0	Block an IP address in a Cisco IOS router	 
Nmap Remediation	2.0	Perform an Nmap Scan	 
pxGrid Adaptive Network Control (ANC) Policy Assignment	1.0	Apply or clear an ANC policy for the endpoint at the involved IP addresses	 
pxGrid Mitigation	1.0	Perform a pxGrid mitigation against the involved IP addresses	 
Set Attribute Value	1.0	Set an Attribute Value	 

Install a new module

No file selected.

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 4
- [Configure an Access Control Rule for the Remediation](#), on page 6
- [Configure a Correlation Rule for the Remediation](#), on page 7
- [Associate the Correlation Rule with the Remediation Module Instance](#), on page 8
- [Optionally Create a Management Contract and Contract EPG](#), on page 2

Optionally Create a Management Contract and Contract EPG

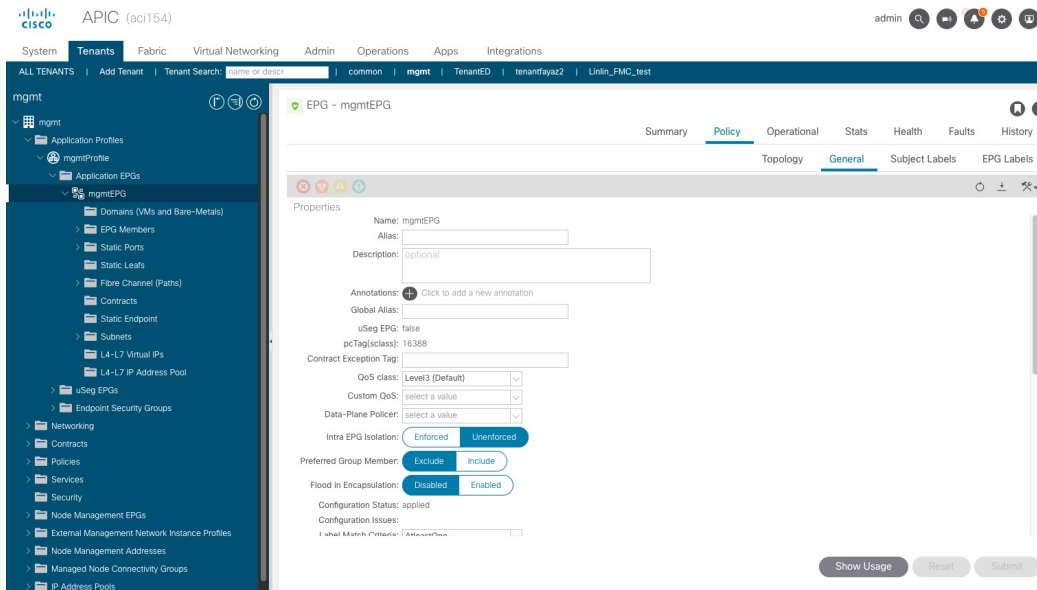
You can optionally predefine an APIC traffic filtering contract in the common tenant and a management EPG in the mgmt tenant to initiate a connection to the quarantined uSeg EPG. To use this optional configuration, you *must* define a management EPG in APIC in its **mgmt** tenant, and you *must* define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

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

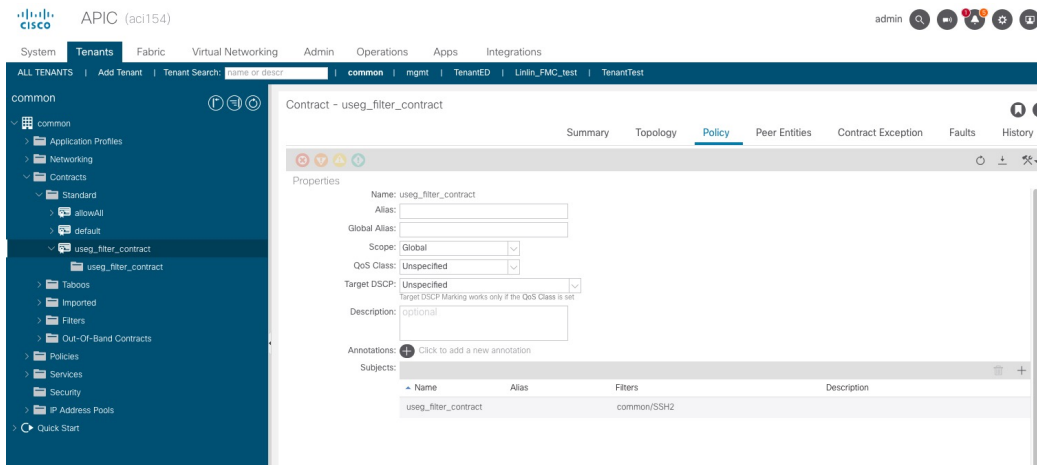
If you do not wish to create contracts, skip this section and continue with [Create a Remediation Module Instance and Type](#), on page 4.

- 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**.

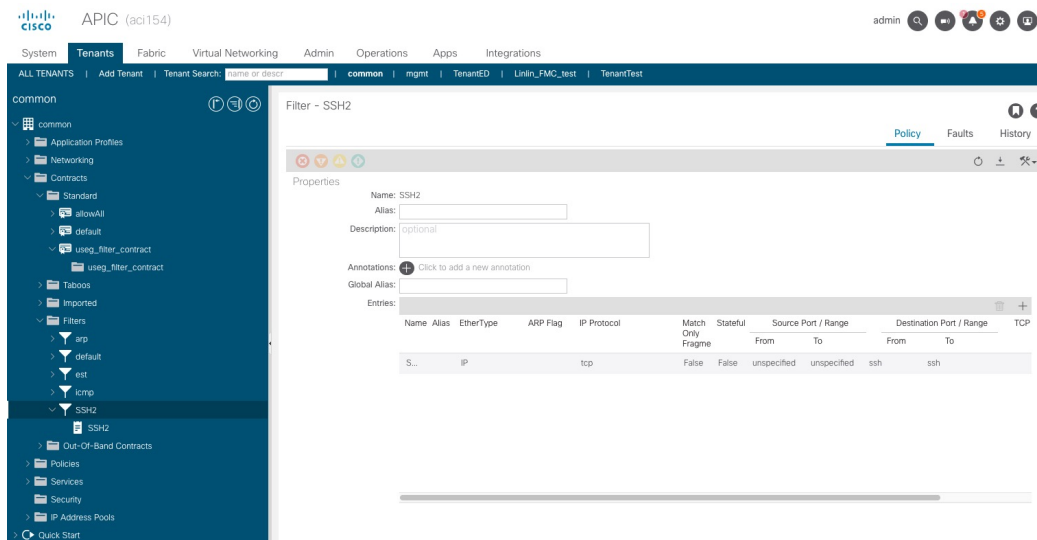
The following figure shows an example.



- 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 4.

Create a Remediation Module Instance and Type

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

- Step 1** If you haven't done so already, log in to the management center.
- Step 2** Click **Policies > Actions > Instances**.
- Step 3** From the **Select a module type** list, click **APIC/Secure Firewall Remediation Module (2.0.2)**.
- 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
Instance name	Enter a name to identify this instance. (Spaces are not allowed in the name.)
Description	(Optional.) Enter a description.
APIC server username	Enter the user name of an APIC user with admin privileges.
APIC server password	Enter and re-enter the user's password
APIC cluster instance 1 IP	Enter the IP address of the APIC server or of the first server in the cluster.

Item	Description
APIC cluster instance x IP	(Optional.) If your APIC cluster has more than one server, enter additional IP addresses in the provided fields.
IP addresses NOT to quarantine	(Optional.) Enter a list of IP addresses to always exclude from the quarantine. Separate IP addresses with Enter.
Management Contract Name	(Optional.) Enter the name of the management contract you created in APIC. For more information, see the <i>Cisco APIC Basic Configuration Guide</i> .
Management EPG Name	(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 6](#).

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 management center.

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.

The screenshot shows the 'Add Rule' configuration interface. The rule name is 'Block SSH', it is enabled, and the action is 'Block'. The 'Ports' tab is selected, showing 'any' in the 'Selected Source Ports (0)' field and 'SSH' in the 'Selected Destination Ports (1)' field. The 'Available Ports' list on the left includes RIP, SIP, SMTP, SMTPS, SNMP, SSH (highlighted), SYSLOG, and TCP_high_ports. The 'Add' button is located at the bottom right of the configuration area.

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

For more information about access control rules, see the [Cisco Secure Firewall 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 7](#).

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 [Cisco Secure Firewall Management Center Administration Guide](#).

- Step 1** If you haven't done so already, log in to the management center.
- 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' interface with the following configuration:

- Rule Information:**
 - Rule Name: MyCorrelationRule
 - Rule Description: (empty)
 - Rule Group: Ungrouped
- Event Selection:**
 - If a connection event occurs at any point of the connection and it meets the following conditions:
- Conditions:**
 - 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 8](#).

Associate the Correlation Rule with the Remediation Module Instance

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

- Step 1** If you haven't done so already, log in to the management center.
- 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 Management Center

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 management center.

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

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 9](#).
- 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 9](#) 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 9](#).

Verify the Quarantine in APIC

Before you begin

Complete the tasks discussed in [Verify the Remediation in the Management Center, on page 9](#).

- 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 quarantine. The left navigation pane shows the hierarchy: Tenant ed > Application Profiles > app2 > uSeg EPGs > EPG quarantine-epg11. The main content area shows the configuration for 'EPG - 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 (selected) / Unenforced
- Preferred Group Member: Exclude (selected) / Include
- Configuration Status: applied
- Configuration Issues:
- Label Match Criteria: AtleastOne
- Bridge Domain: ed/bd-ext (highlighted with a red box)
- Resolved Bridge Domain: ed/bd-ext
- Monitoring Policy: select a value
- uSeg Attributes table (highlighted with a red box):

Name	Value
192.168.103.21	IP Address: 192.168.103.21

The figure shows that a device at IP address 192.168.100.21 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 11](#).
-

What to do next

See [Verify the Remediation in the Management Center, on page 9](#).

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 management center.
 - 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. 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	uni/tn-ed/ap-app2/epg-quarantine-epg11/cep-00:50:56:81:7F:A9	
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.
