



Remediation and Quarantine

This chapter discusses tasks you must perform in APIC and in the Secure Firewall Management Center to create rules to remediate and quarantine an endpoint.

- [The Remediation and Quarantine Process, on page 1](#)
- [Create an Optional Management Contract and Contract EPG, on page 3](#)
- [Create a Remediation Module Instance and Type, on page 5](#)
- [Configure an Access Control Rule for the Remediation, on page 8](#)
- [Configure a Correlation Rule for the Remediation, on page 10](#)
- [Associate the Correlation Rule with the Remediation Module Instance, on page 11](#)
- [Verify the Remediation in the Management Center, on page 11](#)
- [Verify the Quarantine in APIC, on page 12](#)

The Remediation and Quarantine Process

Remediation (defining the circumstances under which an endpoint should be quarantined) and *quarantine* (isolating an endpoint so it cannot communicate on the network) is a multi-step process summarized in the next section, [How to Remediate and Quarantine, on page 1](#).

How to Remediate and Quarantine

The following summarizes the tasks required to remediate and quarantine an endpoint. You perform some tasks in APIC and some in the management center.

Before you begin

Consult a reference such as the [Endpoint Groups \(EPG\) Usage and Design](#) whitepaper or the [Cisco APIC Basic Configuration Guide](#) to understand APIC-related concepts.

SUMMARY STEPS

1. Optionally create a management contract and management contract endpoint group (EPG).
2. Create a remediation module instance and type.
3. Configure an access control rule that determines the conditions under which an endpoint should be quarantined.
4. Associate the correlation rule with the remediation policy.

5. Verify the quarantine and remediation.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Optionally create a management contract and management contract endpoint group (EPG).	<p>Perform this task in APIC.</p> <p>APIC uses an allow-list model where we explicitly define what traffic should be permitted. A <i>contract</i> is a policy construct used to define communication between EPGs.</p> <p>This optional configuration enables you to initiate a connection to the quarantined uSeg EPG. For more information, see Optionally Create a Management Contract and Contract EPG, on page 4.</p>
Step 2	Create a remediation module instance and type.	<p>Perform this task in the management center.</p> <p>The remediation module creates, on APIC, the EPG that enables you to view and work with quarantined endpoints. The remediation module can:</p> <ul style="list-style-type: none"> • Quarantine source endpoint, destination endpoint, or both • Reference a management EPG • Audit remediation activity only without triggering remediation or affecting production traffic <p>For more information, see Create a Remediation Module Instance and Type, on page 5.</p>
Step 3	Configure an access control rule that determines the conditions under which an endpoint should be quarantined.	<p>Perform this task in the management center.</p> <p>Determine the conditions under which you want an endpoint quarantined; for example, passing unsecure traffic. Set up an access control rule that in turn triggers the remediation policy you set up previously.</p> <p>For more information, see Configure an Access Control Rule for the Remediation, on page 8.</p>
Step 4	Associate the correlation rule with the remediation policy.	<p>Perform this task in the management center.</p> <p>This triggers the quarantine on APIC. For more information, see Associate the Correlation Rule with the Remediation Module Instance, on page 11.</p>
Step 5	Verify the quarantine and remediation.	<p>Verify the <i>quarantine</i> in APIC and verify the <i>remediation</i> in the management center.</p> <p>For more information, see Verify the Quarantine in APIC, on page 12 and Verify the Remediation in the Management Center, on page 11.</p>

What to do next

[Create an Optional Management Contract and Contract EPG, on page 3](#)

Create an Optional 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](#).

What To Do Next

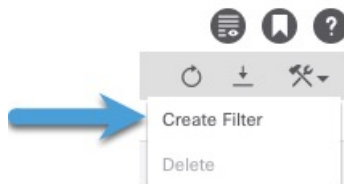
[Prerequisites for Creating an Optional Management Contract and Contract EPG, on page 3.](#)

Prerequisites for Creating an Optional Management Contract and Contract EPG

This task discusses how to do the following before you configure an optional management contract and contract EPG:

- Create an application ESG.
- Create a filter for the quarantine you wish to perform; in this example, the filter is for SSH2 traffic.

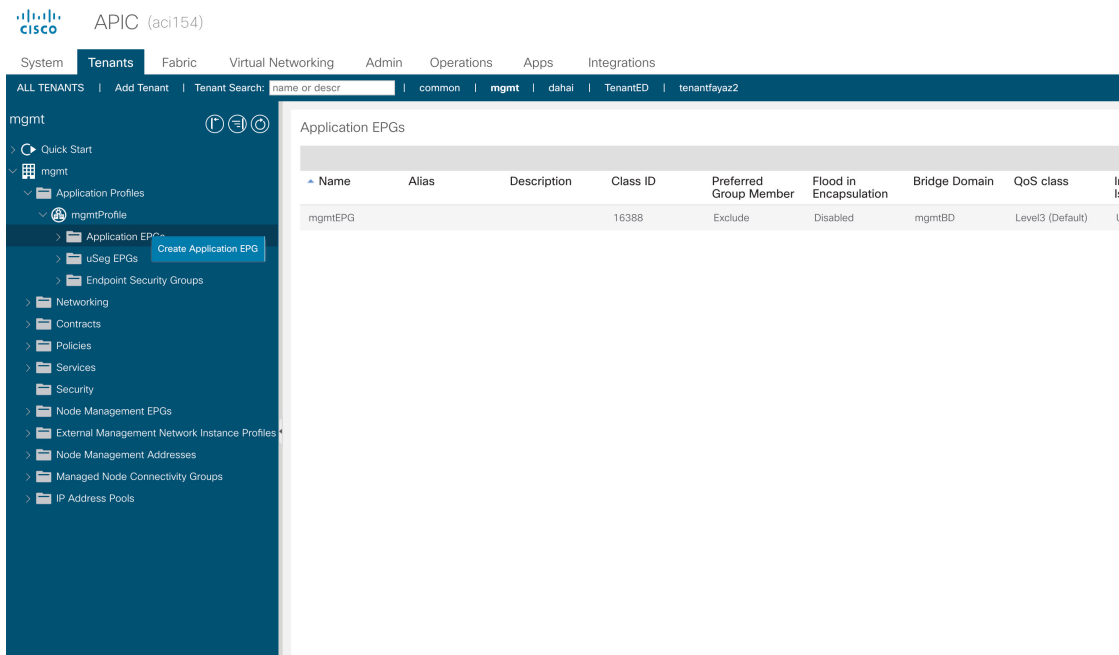
-
- Step 1** Log in to APIC.
- Step 2** Click **Tenants**.
- Step 3** Double-click **common**.
- Step 4** In the left pane, expand **Contracts > Filters**.
- Step 5** In the right pane, click **Create Filter**.



- Step 6** Give the filter a **Name** like SSHv2.
- Step 7** Click **Submit**.
- Step 8** In the left pane, click **Tenants > ALL TENANTS**.
- Step 9** Click **mgmt**.
- Step 10** Expand **Application Profiles > mgmt profile**.
- Step 11** Right-click **Application EPGs** and click **Create Application EPG**.

The following figure shows an example.

Optionally Create a Management Contract and Contract EPG



- Step 12** Give the EPG a **Name**.
- Step 13** From the **Bridge Domain** list, click **WHICH BRIDGE DOMAIN**.
- Step 14** Click **Finish**.

What to do next

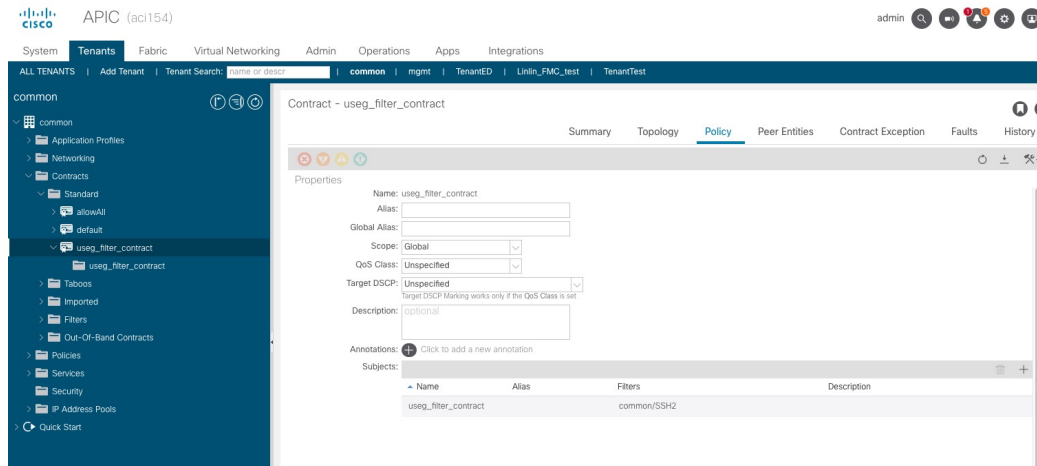
[Optionally Create a Management Contract and Contract EPG, on page 4](#)

Optionally Create a Management Contract and Contract EPG

If you do not wish to create contracts, skip this section and continue with [Create a Remediation Module Instance and Type, on page 5](#).

- Step 1** Log in to APIC.
- Step 2** Click **ALL TENANTS**.
- Step 3** Double-click **common**.
- Step 4** Expand **Contracts > Standard**.
- Step 5** Right-click **Standard** and then click **Create Contract**.
- Step 6** In the **Name** field, enter **useg_filter_contract**.
- Step 7** From the **Scope** list, click **Global**.
- Step 8** Make other selections as desired.
- Step 9** Click **Submit**.
- Step 10** Click **useg_filter_contract**.
- Step 11** In the right pane, click the **Policy** tab.

The following figure shows an example.



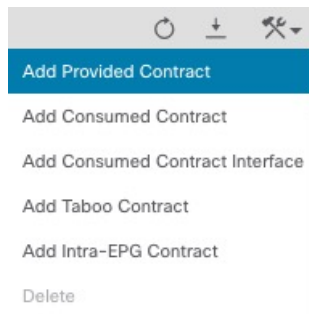
Step 12 Click **ALL TENANTS**.

Step 13 Double-click **mgmt**.

Step 14 Expand **mgmt** > **Application Profiles** > **mgmtProfile** > **Application EPGs** > **mgmtEPG** > .

Step 15 Click **Contracts**.

Step 16 Click **Add Provided Contract**.



Step 17 From the **Contract** list, click **useg_filter_contract**.

Step 18 Click **Submit**.

What to do next

See [Create a Remediation Module Instance and Type, on page 5](#).

Create a Remediation Module Instance and Type

For the Secure Firewall Management Center to be able to detect threats and inform APIC to quarantine them, 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](#). You can optionally choose to quarantine the source endpoint, the destination endpoint, or both.

You can also choose to only audit endpoints without quarantining them.

- 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 (3.0.1)**.
- Step 4** Click **Add**.
The Edit Instance page is displayed as follows.

Edit Instance

Instance Name

Module APIC/Secure Firewall Remediation Module(v3.0.1)

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

L3Out Name

L3Out 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.
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 individual IP addresses to always exclude from the quarantine. Separate IP addresses with Enter. You cannot specify subnet masks.
Management Contract Name	(Optional.) Enter the name of the management contract you created in APIC. For more information, see Create an Optional Management Contract and Contract EPG, on page 3 .
Management EPG Name	(Optional.) Enter the name of the EPG with which the management contract is associated. For more information, see Create an Optional Management Contract and Contract EPG, on page 3 .
L3Out Name	(Optional.) The name of an L3Out target configured on APIC. If you enter a value in L3Out Name , you must also enter a value in L3Out EPG Name . Drops traffic between a quarantined endpoint in an L3Out target and the source endpoint group while allowing traffic from the quarantined endpoint for forensic analysis purposes.
L3Out EPG Name	(Optional.) The name of an L3Out endpoint group (EPG) configured on APIC. If you enter a value in L3Out EPG Name , you must also enter a value in L3Out Name .
Audit-only	Off (default): Quarantines an infected endpoint and sends correlation status messages to the management center. On : Does not quarantine an infected endpoint; instead, sends correlation status messages to the management center (Analysis > Correlation > Correlation Events).

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**

The remediation name cannot include a space.

Following is an example of the Configured Remediation section showing a remediation.

Configured Remediations

Remediation Name	Remediation Type	Description	
QuarDestSample	Quarantine the destination End Point on APIC		 
Add a new remediation of type <input type="text" value="Quarantine the destination End"/> <input type="button" value="Add"/>			


- 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 8](#).

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 **Edit** () to edit an existing policy.
- Step 4** If you're editing an existing policy, click **Add Rule** to add a rule.
- Enter the following information (management center version 7.2 and earlier).

Add Rule

Name: Block SSH Enabled Insert: into Mandatory

Action: Block Time Range: None

Zones Networks VLAN Tags Users Applications **Ports** URLs Dynamic Attributes Inspection Logging Comments

Available Ports

- RIP
- SIP
- SMTP
- SMTPS
- SNMP
- SSH**
- SYSLOG
- TCP_high_ports

Selected Source Ports (0) Selected Destination Ports (1)

any SSH

Protocol TCP (6) Port Enter a Add Protocol TCP (6) Port Enter a Add

Enter the following information (management center version 7.3 and later).

Create Rule

Name: Sample SSH block rule Action: Block Logging: ON Time Range: None Rule Enabled:

Insert: into Mandatory

All (1) Zones Networks **Ports (1)** Applications Users URLs Dynamic Attributes VLAN Tags

Clear Selections ssh Showing 1 out of 29 Selected 1 Selected Sources: 0 Selected Destinations and Applications: 0

SSH (Port Object) tcp (6)/22

Comments

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 5 Click **Add**.

Step 6 At the top of the page, click **Save**.

What to do next

See [Configure a Correlation Rule for the Remediation, on page 10](#).

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 displays the 'Rule Management' interface. At the top, there are tabs for 'Policy Management', 'Rule Management', 'Allow List', and 'Traffic Profiles'. Below the tabs, there are three buttons: 'Add Connection Tracker', 'Add User Qualification', and 'Add Host Profile Qualification'. The 'Rule Information' section contains three input fields: 'Rule Name' with the value 'MyCorrelationRule', 'Rule Description', and 'Rule Group' with a dropdown menu set to 'Ungrouped'. Below this, a section titled 'Select the type of event for this rule' shows a configuration where the event is 'a connection event occurs' and it occurs 'at any point of the connection'. Underneath, there are two conditions listed in a table-like structure. The first condition is 'Access Control Policy is SampleAC' and the second is 'Access Control Rule Name is Block SSH'. There are buttons for 'Add condition' and 'Add complex condition' above the conditions list.

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 11](#).

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**.

If the name of your remediation policy is not displayed, go back to the correlation rule and make sure the name of both the access control policy and access control rule are correct.
 - 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

The screenshot shows the Firewall Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Analysis' tab is active. The main content area displays a table of remediations. The table has columns for 'Time', 'Remediation Name', 'Policy', 'Rule', and 'Result Message'. A single row is visible 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 12](#).
- 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 12](#) 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 12](#).

Verify the Quarantine in APIC

Before you begin

Complete the tasks discussed in [Verify the Remediation in the Management Center, on page 11](#).

- 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 **Policy > General**.
- Step 9** Verify that one or more uSeg attributes were created on the APIC server. The following figure shows an example.

The screenshot shows the Cisco APIC interface for configuring an EPG. The left sidebar shows the navigation tree with 'EPG quarantine-epg11' selected. The main panel displays the 'Properties' section for this EPG, including fields for Name, Description, Tags, Alias, uSeg EPG (true), pcTag(sclass) (32772), QoS class (Unspecified), Custom QoS, 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), and Monitoring Policy. A table under 'uSeg Attributes' shows a single entry with Name '192.168.103.21' and Value '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 [Overview of Manually Quarantining an IP Address](#).

