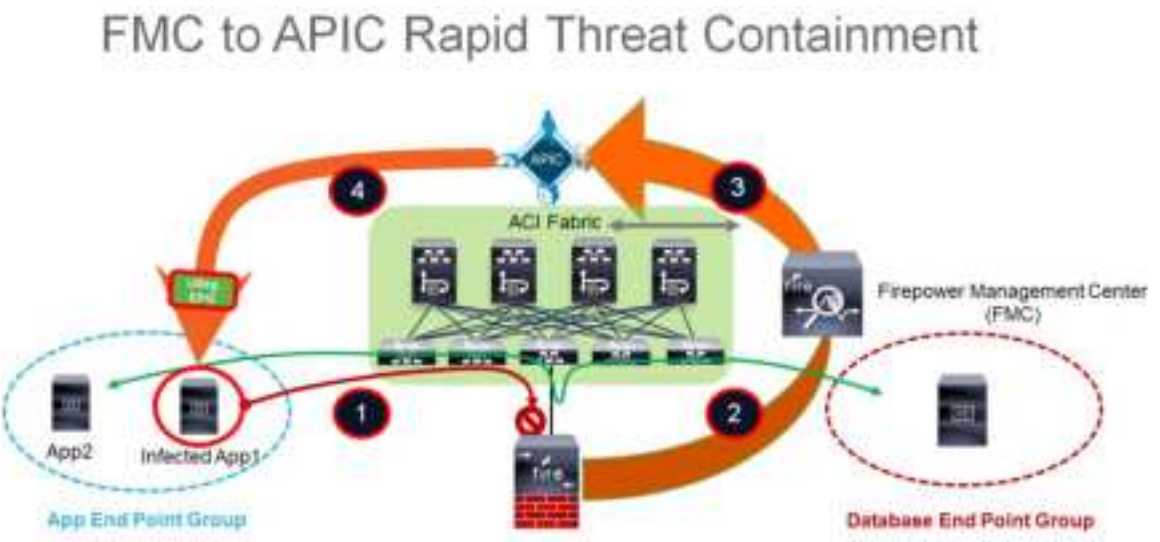
Cisco Firepower Management Center Remediation Module for ACI, Version 1.0.2 Quick Start Guide

Created: December 2, 2021

1 About the Cisco Firepower Management Center Remediation Module for ACI

With the Cisco Firepower Management Center Remediation Module for ACI, when an attack on your network is detected by the Firepower Management Center, 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 illustration shows the relationship between the Firepower Management Center (FMC) and the APIC when the Remediation Module is installed:



The illustration above shows the following process of quarantining a network attack in the APIC:

Step 1 An endpoint with an infected application in an endpoint group (EPG) launches an attack on your network. The attack is blocked inline by either a Cisco Firepower Next-Generation Firewall (physical or virtual), a Cisco ASA with FirePOWER Services, or a Cisco FirePOWER Appliance (physical or virtual).

Step 2 An attack event is generated and sent to the FMC. The attack event includes information about the infected endpoint.

Step 3 The attack event is configured to trigger the remediation module for APIC, which used the APIC northbound (NB) API to contain the infected endpoint in the ACI fabric.

Step 4 The APIC quickly contains or quarantines the infected application workload into an isolated microsegment (uSeg) EPG.

Note Currently, this only works with east-west traffic, where the attacking host is deployed in the ACI and learned on the APIC. An attack from an external, outside source connected to the fabric by L3Out and its north-south traffic is not blocked.

Behavior Supported in Version 1.0.2

Note In VMware Distributed Virtual Switch (DVS) and Bare Metal deployments, not all switches can support uSeg quarantine functionality on the APIC. Contact your Cisco representative to determine which model(s) of the Cisco Nexus 9000 Series switches to order if you plan to use the uSeg quarantine feature in DVS and Bare Metal deployments.

This release enables you to quarantine offending endpoints that are detected by the Firepower Management Center, using the APIC version 1.2(7). For version 1.0.2 of the Cisco Firepower Management Center Remediation Module for ACI, the supported behavior when endpoints are quarantined is described in the following table:

	Cisco Application Virtual Switch (AVS)	VMware Distributed Virtual Switch (DVS)	Bare Metal
Verified in IPS inline mode	Yes	Yes	Yes
EPG bridge mode	Yes	Yes	Yes
EPG routed mode	Yes	No	No
Multiple IP to one MAC checking	No	Yes	Yes
Create only an IP address filter uSeg attribute	Yes	No	No
Create both an IP address filter and a MAC address filter uSeg attribute	No	Yes	Yes

2 Deploy the Cisco Firepower Management Center Remediation Module for ACI

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

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

Step 1 Download the remediation module.

a. Go to the software download page:
https://software.cisco.com/download/home/286259687/type/286311510/release/ACI

b. Download the Cisco Firepower Management Center Remediation Module for ACI.

Step 2 Install the remediation module.

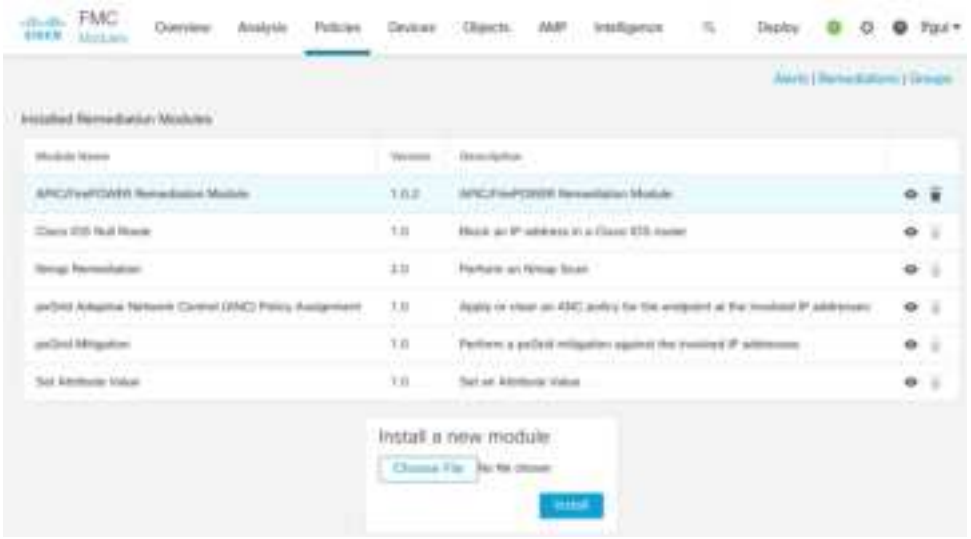
a. On the **Policies** tab of the FMC GUI, select the **Actions > Modules** sub-tab.

b. In the Install a New Module dialog box, click **Choose File** as shown below.

c. Select the file for the APIC/FMC Remediation Module.

d. Click **Install**.

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



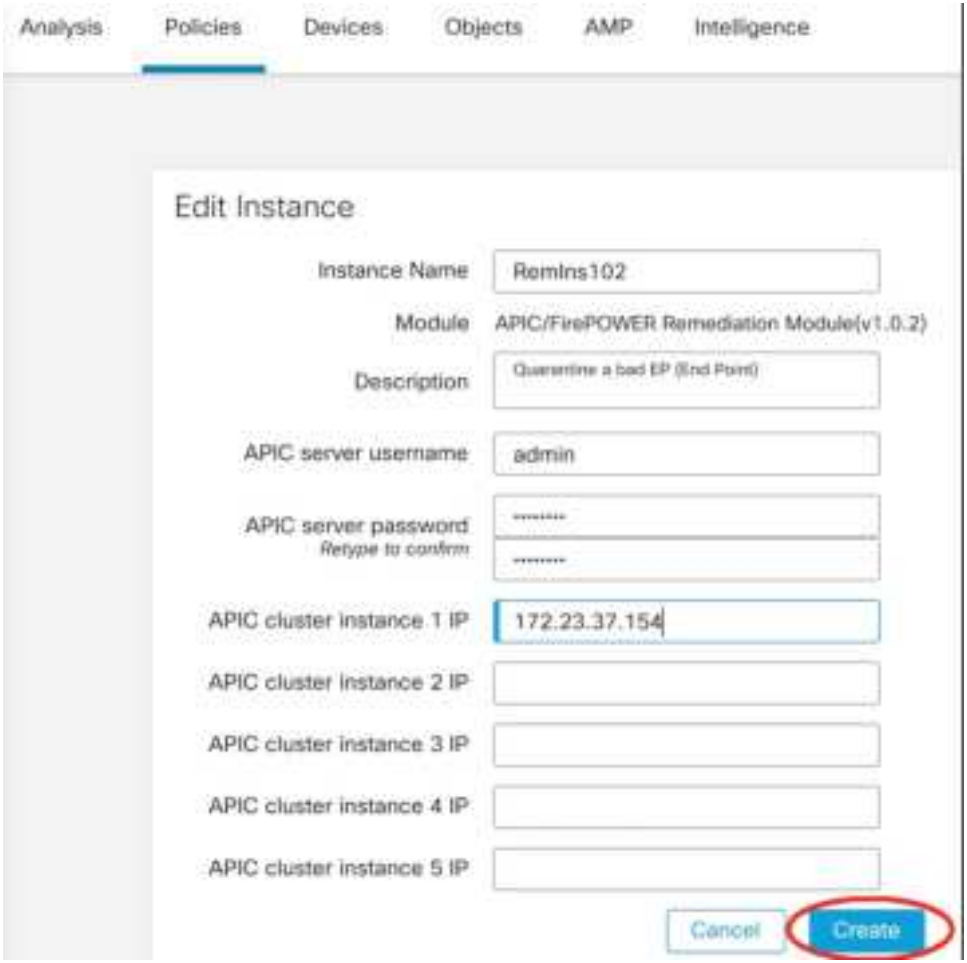
Step 3 Create an instance of the remediation module for each APIC server in your network.

a. Click the edit icon for the remediation module in the list of installed remediation modules (on the **Policies** tab and **Actions > Modules** sub-tab, as shown above).

b. Enter an **Instance Name** and optional **Description**.

c. Enter the IP address, username, and password for the APIC server.

d. Click **Create.**



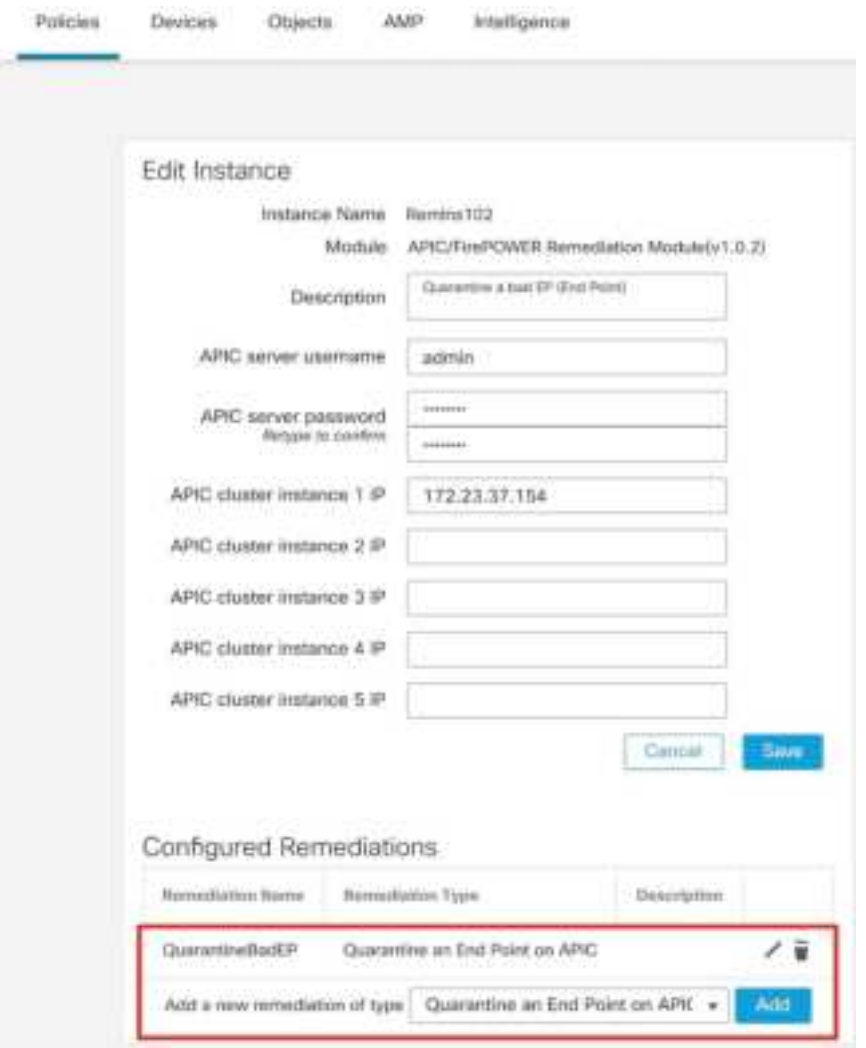
Step 4 Create a Remediation Type for each instance of the APIC/FMC Remediation Module.

a. On the **Policies** tab and **Actions > Instances** sub-tab, click the edit icon for the instance of the APIC/FMC Remediation Module that you just created.

b. Select **Quarantine an End Point on APIC.**

c. Click **Add.**

d. Click **Save.**



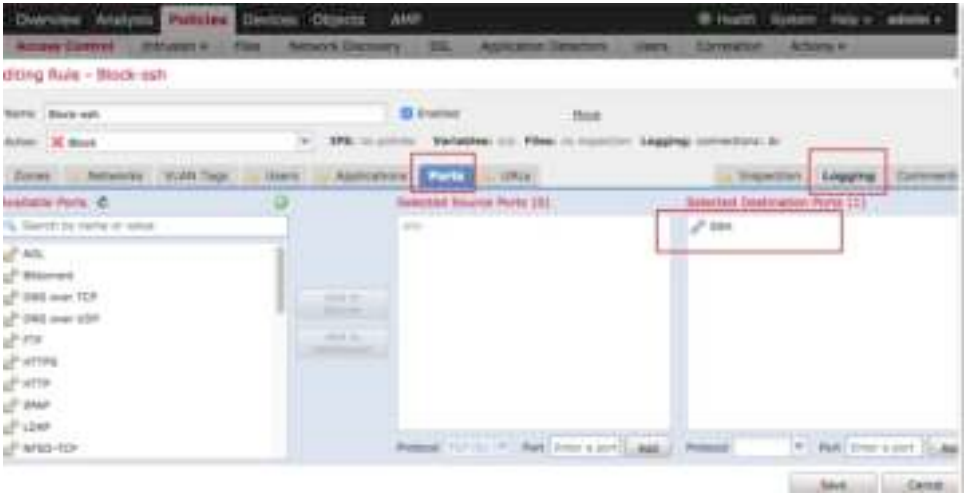
Step 5 Configure an access control policy.

a. Navigate to **Policies > Access Control > Rules** to add a rule (for example, a Block-ssh rule).

b. Click the Edit icon for the Standard Rules to configure a rule to block SSH.

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

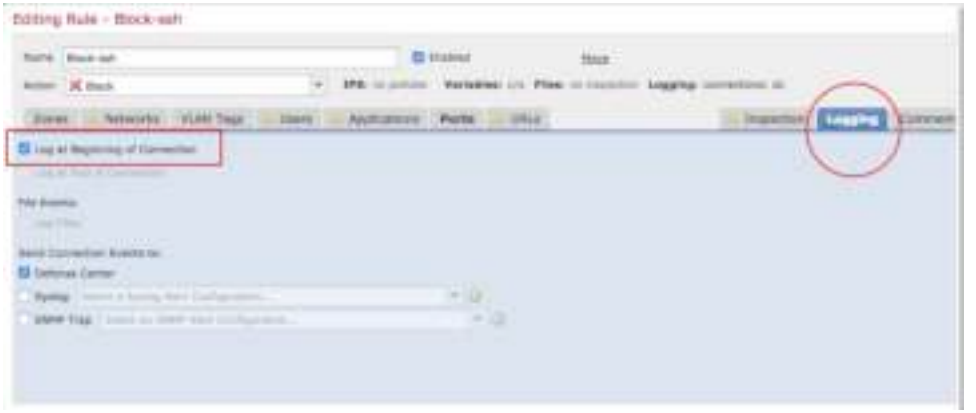
d. On the **Ports** tab, select **SSH** from the list of protocols for the Destination Port and click **Add.**



e. Click **Save**.

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

g. Click **Save**.



Step 6 Configure a correlation rule.

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

b. Enter a Rule Name.

c. 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**.

d. Click the drop-down icon and select **Access Control Policy** and the name of the access control policy that you previously configured in Step 5.

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

f. Select **Access Control Rule Name**, select **Is**, and select the rule you created (such as **Block-ssh** in this example).

g. Click **Save**.


Overview
Analysis
Policies
Devices
Objects
AMP
Rule Information
Select the type of event for this rule
Rule Options

Step 7 Associate the instance of the remediation module with a correlation rule as a response.

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

b. Enter a Policy Name and optional Policy Description and Default Priority.

c. Click **Add Rules** and select **BlockSSHRule.**

d. Click **Add** and click on the red-colored Responses icon.

e. Select **QuarantineBadEP** (**Remediation**) from the **Unassigned Responses** box to **Assigned Responses** box.

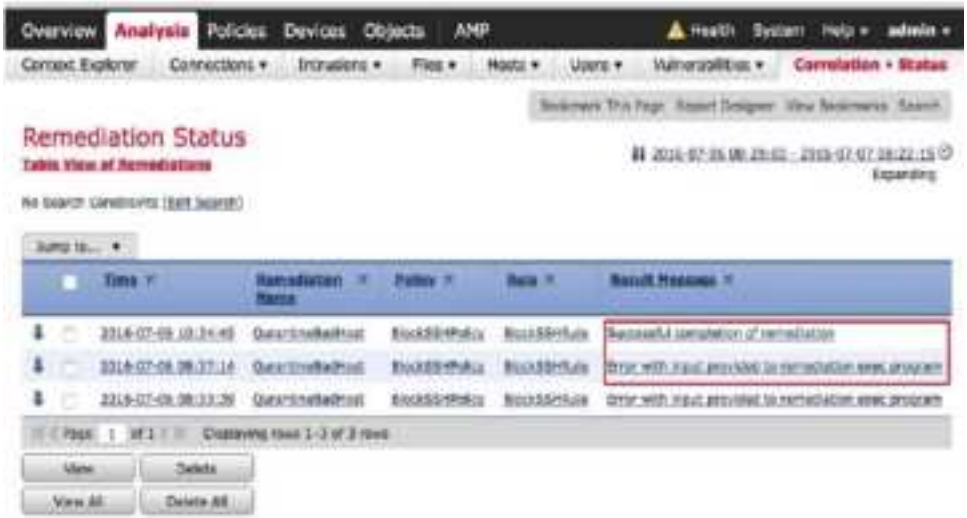
f. Click **Update** and **Save.**

Verify that the Remediation Executed Properly

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 Cisco FMC.

Step 1 On the **Analysis** tab of the FMC GUI, select the **Correlation > Status** tab.

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



Step 3 If the remediation was successful, continue to the next section.

Step 4 If an error is shown, the end point may still be quarantined if subsequent remediation events are successful. When you see an error, go the next section to verify that the quarantine happened.

If the quarantine of the end point was eventually successful, you can ignore all of its error messages.

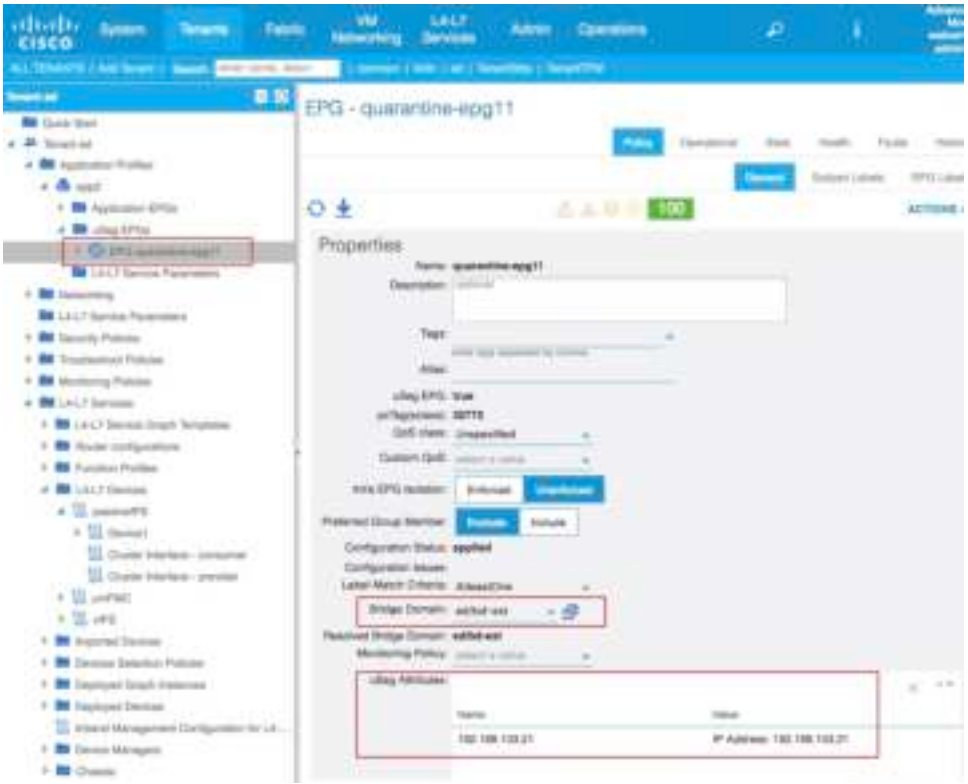
Check the Result of the Quarantine

Note In DVS and Bare Metal deployments, not all switches can support uSeg quarantine functionality on the APIC. If the quarantine fails, contact your Cisco representative to determine which model(s) of the Cisco Nexus 9000 Series switches you must use.

Step 1 On the **Tenants** tab of the APIC GUI, expand the infected application in the left panel, expand uSeg EPGs, and select the EPG quarantine for the offending end point.

Step 2 In the right panel, select the **Policies** tab and the **General** sub-tab.

Step 3 Verify that one or more uSeg attributes were created on the APIC server.



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 4 If the quarantine was not successful (no uSeg attributes were created), you can manually quarantine the IP address, as described in the next section.

Manually Quarantine an IP Address

If the quarantine was unsuccessful, optionally complete the following steps to manually quarantine the IP address.

Step 1 Identify the IP address of the end point that you want to quarantine.

- **a.** On the **Analysis** tab on the FMC GUI, select the **Correlation > Status** sub-tab.
- **b.** On the Remediation Status page, find the time stamp of entry for the unsuccessful quarantine and make note of the source IP address.
- **c.** On the **Operations** tab, select **EP Tracker,** enter the IP address, and press **Enter**.
- **d.** If no information is displayed, the end point 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 end point that you want to quarantine, create a uSeg EPG attribute corresponding to this end point.

- **a.** On the **Tenants** tab of the APIC GUI, use the information from Step 1 to find the EPG and make note of the bridge domain.
- **b.** Expand the EPG and make note of the domain profile name.
- **c.** On the **Tenants** tab, expand the **Application Profiles,** and right-click **uSeg EPG**.
- **d.** Enter a name for the uSeg EPG, in this format: "quarantine-*EPG_name_of_the_EP*."
- **e.** Select the bridge domain of the EPG from Step 2a.
- **f.** Add an IP filter attribute by clicking the plus sign on lower right and entering the IP address for the name and filter.
- **g.** Click **Next Step** and select the same domain profile from Step 2b.
- **h.** Set the **Deployment Immediacy** to **Immediate**.
- **i.** Click **Update** and then click **Finish**.

j. For DVS and Bare Metal, in addition to creating an IP address filter attribute, you must also create a MAC address filter attribute.

   For 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.

   To find the MAC address, go to the APIC Object Store Browser by navigating to: https://*apic_IP_address*/visore.html. Use the IP address of the endpoint to run a query and display the MAC address.

k. Right-click on **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.

l. For Bare Metal, right-click on **Static Leafs,** and select **Statically Link With Node**.

Step 3 Verify that no traffic can go into or out from this endpoint.

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

3 Related Documentation

For additional information about the Cisco Firepower Management Center, see the *Configuration Guide for the appropriate version*.

For additional information about the Cisco APIC and ACI, see APIC Documentation and Cisco Application Centric Infrastructure Security Solution.

4 Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.