Cisco APIC/Secure Firewall Remediation Module, Version 2.0.2 Release Notes

First Published: 2022-04-01

Last Modified: 2022-05-31

Release Notes

Supported Features

This release enables you to quarantine offending endpoints that are detected by the APIC/Secure Firewall Remediation Module, using APIC version 5.1(1h). For version 2.0.2 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
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

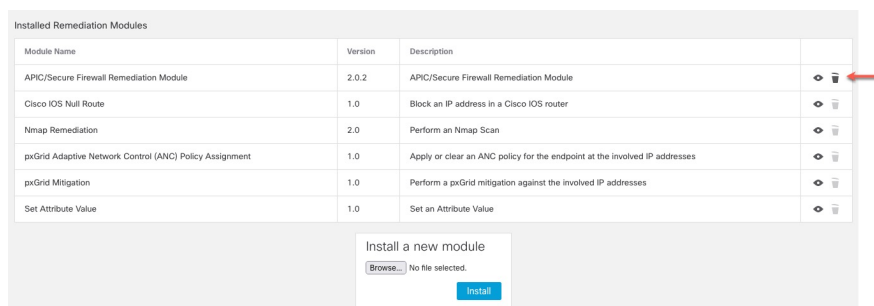## Download and Install the APIC/Secure Firewall Remediation Module

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)

Procedure

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:

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
Browse... No file selected.
Install

Resolved Caveats

Version 2.0.2

There are no resolved caveats in the APIC/Secure Firewall Remediation Module version 2.0.2.

Open Caveats

Version 2.0.2

There are no open caveats in the APIC/Secure Firewall Remediation Module version 2.0.2.

Resolved Enhancement Requests

Version 2.0.2

Link to issue	Description
CSCvz43553	Add quarantine destination type in APIC/FMC Remediation Module for FMC 7.0 or later
CSCvz66336	Avoid quarantining critical servers in APIC/FMC Remediation Module for FMC 7.0 or later
CSCwa18128	Rebranding ACI/FirePOPWER Remediation Module
CSCwa17749	Apply a predefined contract to allow an administrator to access a quarantined endpoint

Open Enhancement Requests

Version 2.0.2

There are no open enhancement requests in the APIC/Secure Firewall Remediation Module version 2.0.2.

Related Documentation

For additional information about the Cisco APIC/Secure Firewall Remediation Module, 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.