



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

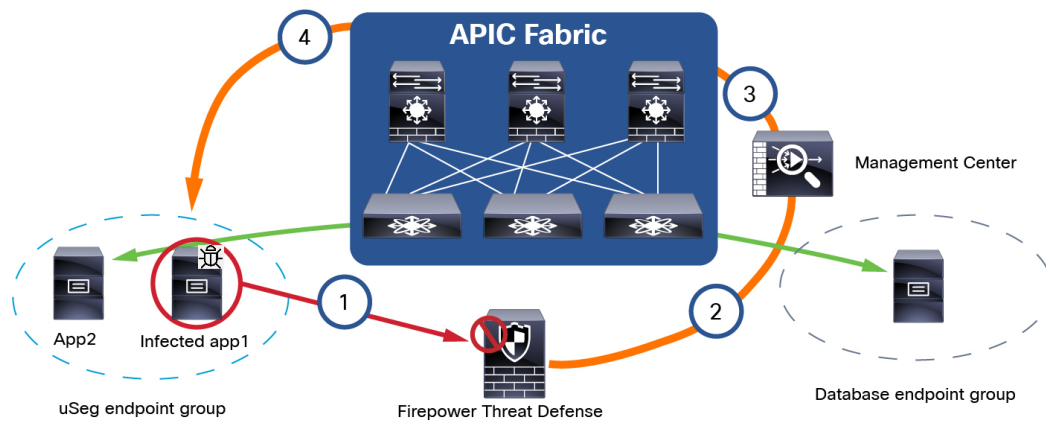
The following table shows the compatibility between the Cisco Firepower Management Center Remediation Module for ACI, FMC, and APIC.

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

	VMware Distributed Virtual Switch (DVS)	Bare metal
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

