

Configuring the Remediation Module

The following section provides the steps for configuring the remediation module.

• Configure, on page 1

Configure

To configure the remediation module installed on the FMC, complete the following procedure:

Step 1 In FMC, create an instance of the remediation module for each Secure Workload cluster in your network:

- a. Navigate to Policies > Actions > Instances.
- b. Select the remediation module in the drop-down list, and click Add.
- c. Enter an Instance Name (in this example, fmc-dev-remediation).
- d. Enter the Secure Workload server's IP address, API key, API secret, and scope containing the potentially offending host. Click Create.
 - **Note** The API key and secret are not validated against the Secure Workload server at this point. The API key and secret must first be created in Secure Workload by a site admin, customer support, or a root scope owner role. Copy that information for use here. For more details, see Related Documentation.

Firepower Management Center Policies / Actions / Instance Detail	Overview Analysis Pol	icies Devices Objects	AMP	Deploy Q	🥵 🔅 😧 DC-North-South \ 🚬 🔻
	Edit Instance				
	Instance Name	fmc-dev-remediation			
	Module	Secure Workload / Secure Firewall I	Remediation Module(v1.0.3)		
	Description				
	Secure Workload IP	10.62.159.4			
	Scope(must be root scope, e.g. Default)	Default			
	API key				
	Retype to confirm				
	API secret				
	hetype to commit				
			Cancel Save		
	Configured Remediat	ions			
	Remediation Name Reme	diation Type	Description		
	quarantine-fmc Quara	antine an IP on Secure Workload	/1		
	unquarantine-fmc Unqua	arantine an IP on Secure Workload	/1		
	Add a new remediation of	of type Quarantine an IP on Secur	e Wor 🔻 🛛 Add		

- e. Under Configured Remediations, select a type of remediation (in this example, Quarantine an IP on Secure Workload), and click Add to add a new remediation.
- f. Enter a Remediation Name (in this example, quarantine-fmc), and click Create.

Firepower Management Center Policies / Actions / Remediation Edit	riew Analysis	Policies	Devices	Objects	AMP		Deploy	۹	¢	¢	DC-North-South \
											Alerts Remediations Groups
	Edit Rer	nediation									
	F	emediation Nam	ne quarant	ine-fmc							
		Remediation Typ	pe Quarantine	e an IP on Secu	re Workload						
		Descriptio	To quaran	tine a host							
				Cancel	Create	e					

- g. The remediation you just configured then shows up in the table. Click Save.
- **Step 2** Configure an access control policy (in this example, **rem-policy**):
 - a. Navigate to Policies > Access Control and click the Edit icon of the access control policy to add rules.
 - b. Click Add Rule and enter a name (for example, block-ssh-add-tag).
 - c. Select Block for the Action.
 - d. On the Ports tab, select SSH from the list of protocols for the destination port.
 - e. On the Logging tab, select Log at Beginning of Connection.

Important Ensure that logging is enabled on the access rule, so that the FMC receives event notifications, and click Add

f. Click Save.

1	Firepower Management Center Policies / Access Control / Policy Editor				Overview	Analysis	Policie	s Devic	es Obj	ects AN	IP Intelli	gence	Deploy	, Q	6 9 🌣	F (2)	Global	١.	•	
ľ	rem-policy Enter Description Show Warnings Analyze Hit Counts Save Cancel																			
	Rules Security Intelligence HTTP Responses Logging Advanced Prefilter Policy: Default Prefilter Policy SSL Policy: None Identity Policy: None																			
E	ilter by Dev	<u>/ice</u>	T Searc	h Rules								×	Show R	ule Conflicts	0 + /	Add Cate	gory	+ /	Add R	ule
#	Name		Source Zones	Dest Zones	Source Netwo	Dest Netwo	VLAN Tags	Users	Applic	Source Ports	Dest Ports	URLs	Source Dynamic Attribu	Destin Dynamic Attribu	Action	F6 🛡	B <i>S</i>) (¢
\sim	Mandatory	/ - rem	-policy (1-1)																
1	block-ss	sh-add	Any	Any	Any	Any	Any	Any	Any	Any	SSH	Any	Any	Any	Block	B 🛡	B 2		0	11
\sim	✓ Default - rem-policy (-)																			
T	There are no rules in this section. Add Rule or Add Category																			

Default Action	Access Control:Block all traffic	Ŧ	B
	Displaying 1 - 1 of 1 rules $ \langle \langle Page 1 $ of 1 $\rangle \rangle \subset \mathbb{C}$ Rules per page: 100	Ŧ]

Step 3 Configure a correlation rule:

- a. Navigate to Policies > Correlation > Rule Management.
- b. Click Create Rule.
- c. Enter a Rule Name (in this example, quaran-rule1) and description (optional).
- **d.** 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.
- e. Click Add condition, and change the operator from OR to AND.
- f. In the drop-down list, select Access Control Rule Name, is, and enter the name of the access control rule that you previously configured in Step 2 (in this example, block-ssh-add-tag).

CISCO Firepower Management Center Overview Policies / Correlation / Rule Management	Analysis Policies	Devices Ob	ects AMP	Intelligence	Deploy (ર 🔮 🌣	 Global \
						Alerts Re	emediations Groups
Policy Management Rule Management Allow List Traffic	Profiles						
Rule Information			Add Connection	n Tracker Add Use	er Qualification	Add Host F	Profile Qualification
Rule Name quaran-rule1							
Rule Description							
Rule Group Ungrouped 💌							
Select the type of event for this rule							
If a connection event occurs • at the beginning of the co	nnecti 💌 and it meets t	he following condition	s:				
Add condition Add complex condition							
Access Control Rule Name	▼ block-ssh-ac	ld-tag					
Rule Options						A	dd Inactive Period
Snooze If this rule generates an event, snooze	for 0 hours	•					
Inactive Periods There are no defined inactive periods.	To add an inactive period, o	click "Add Inactive Pe	iod".				
						С	ancel Save

g. Click Save.

Step 4 Associate the instance of the remediation module as a response with a correlation rule:

- a. Navigate to Policies > Correlation > Policy Management.
- b. Click Create Policy.
- c. Enter a Policy Name (in this example, correlation-policy) and description (optional).
- d. From the Default Priority drop-down list, select a priority for the policy. Select None to use rule priorities only.
- e. Click Add Rules, select the correlation rule you previously configured in Step 3 (in this example, quaran-rule1), and click Add.
- f. Click the Responses icon next to the rule and assign a response (in this example, test_rem) to the rule. Click Update.

c,	Firepower Management Center Policies / Correlation / Policy Management	iew Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy	Q	6 ¢	1 0 G	ilobal \	Ŧ
										Alerts F	temedia	tions Gr	oups
	Policy Management Rule Management Allow List Traffic Profiles												
	Correlation Policy Information										ancel	Save	9
	Policy Name correlation-policy												
	Policy Description												
	Default Priority None	¥											
	Policy Rules										A	Add Rules	s
	Rule	Responses						Priority					
	quaran-rule1	tion)					Default			•			

g. Click Save.