



# Configuring the Remediation Module

---

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

- [Configure, on page 1](#)

## Configure

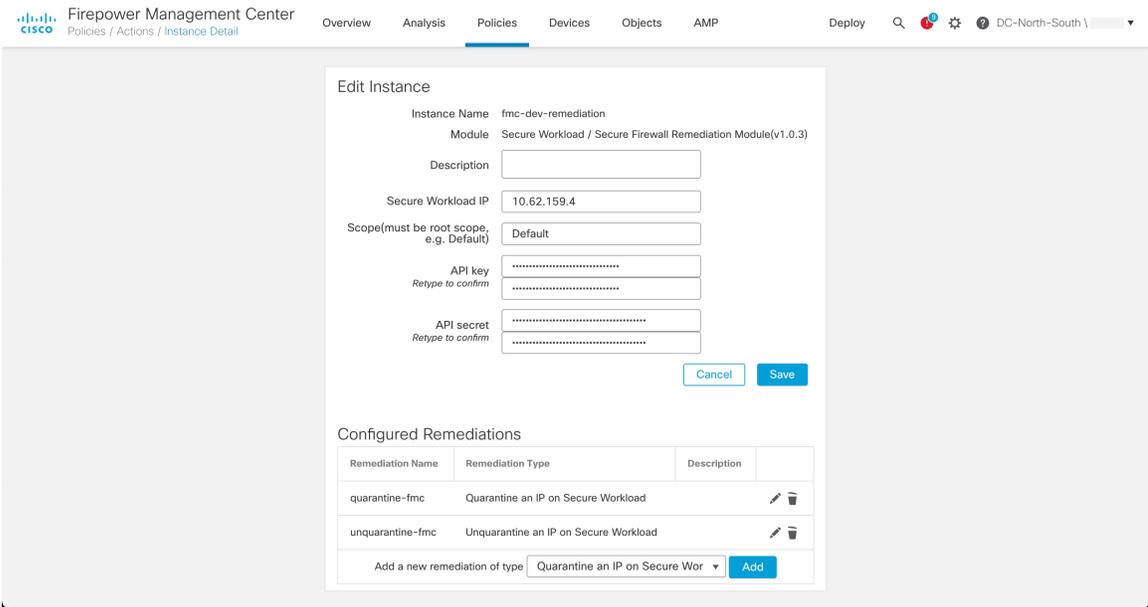
To configure the remediation module installed on the FMC, complete the following procedure:

---

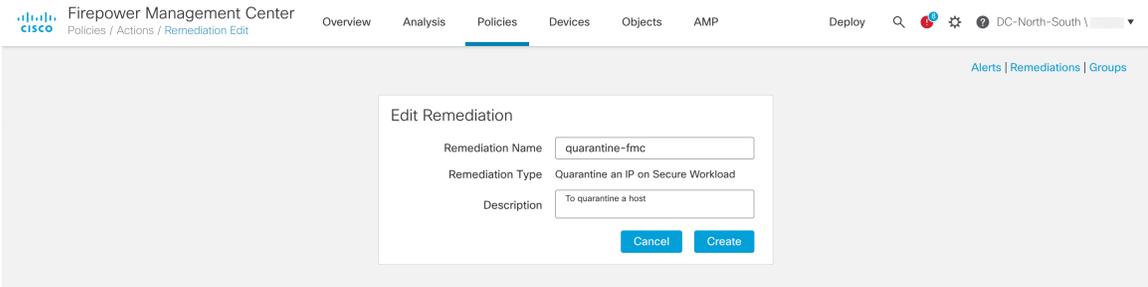
**Step 1** In FMC, create an instance of the remediation module for each Secure Workload cluster in your network:

- Navigate to **Policies > Actions > Instances**.
- Select the remediation module in the drop-down list, and click **Add**.
- Enter an **Instance Name** (in this example, **fmc-dev-remediation**).
- 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](#).



- 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**.



- 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**.

**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**).

Firepower Management Center  
Policies / Correlation / Rule Management

Overview Analysis Policies Devices Objects AMP Intelligence Deploy

Alerts | Remediations | Groups

Policy Management Rule Management Allow List Traffic Profiles

Rule Information Add Connection Tracker Add User Qualification Add Host Profile Qualification

Rule Name:   
 Rule Description:   
 Rule Group:

Select the type of event for this rule

If  at  and it meets the following conditions:

Add condition Add complex condition

Rule Options Add Inactive Period

Snooze: If this rule generates an event, snooze for

Inactive Periods: There are no defined inactive periods. To add an inactive period, click "Add Inactive Period".

Cancel 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**.

Firepower Management Center  
Policies / Correlation / Policy Management

Overview Analysis Policies Devices Objects AMP Intelligence Deploy

Alerts | Remediations | Groups

Policy Management Rule Management Allow List Traffic Profiles

Correlation Policy Information Cancel Save

Policy Name:   
 Policy Description:   
 Default Priority:

Policy Rules Add Rules

Rule	Responses	Priority
<a href="#">quaran-rule1</a>	test_rem (Remediation)	<input type="text" value="Default"/>

g. Click **Save**.