Verifying Remediation

The following section provides the steps to verify if the remediation process is successful.

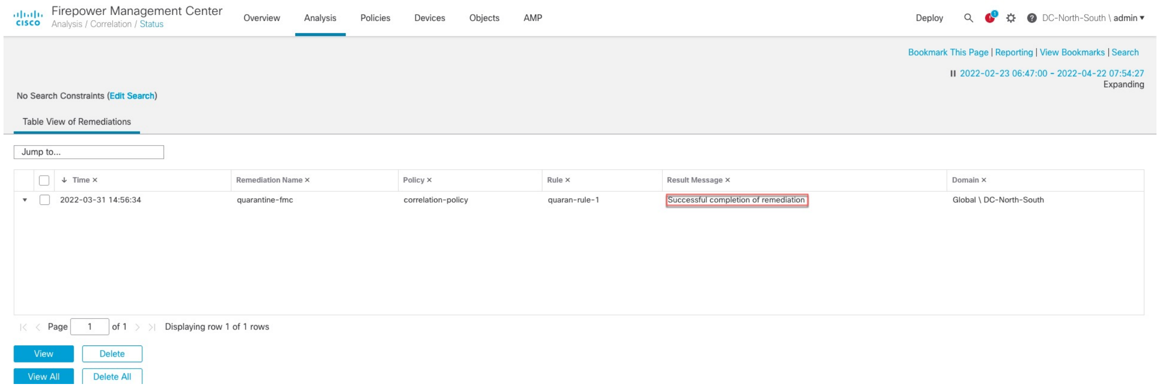
- Verify Remediation, on page 1

Verify Remediation

Because remediations can fail for various reasons, perform the following steps to verify that a remediation is successful.

Step 1 After the remediation module is triggered by an associated correlation rule, check the status of the remediation execution. In the FMC web interface, navigate to **Analysis** > **Correlation** > **Status**.

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



Firepower Management Center
Analysis / Correlation / Status
Overview
Analysis
Policies
Devices
Objects
AMP
Deploy
DC-North-South \ admin ▾
Bookmark This Page | Reporting | View Bookmarks | Search

II 2022-02-23 06:47:00 - 2022-04-22 07:54:27
Expanding

No Search Constraints (Edit Search)

Table View of Remediations

Jump to...

	□	↓ Time ×	Remediation Name ×	Policy ×	Rule ×	Result Message ×	Domain ×
▾	□	2022-03-31 14:56:34	quarantine-fmc	correlation-policy	quaran-rule-1	Successful completion of remediation	Global \ DC-North-South

|< < Page 1 of 1 > >| Displaying row 1 of 1 rows

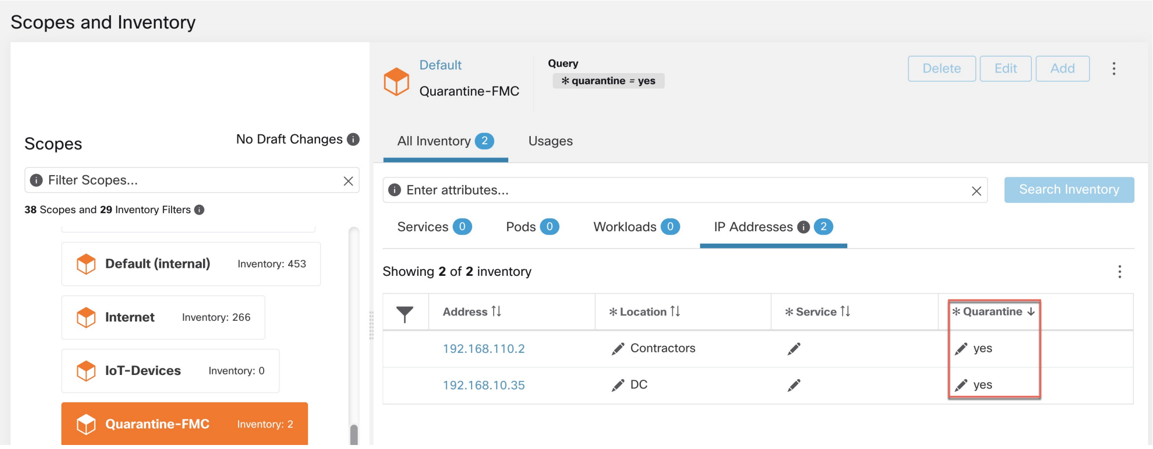
View
Delete
View All
Delete All

Step 3 Once the remediation is complete, perform the following steps:

a. In the Secure Workload user interface, navigate to **Visibility** > **Inventory Search**.

b. Enter the IP address of the infected hosts, and click **Search**.

c. In User Annotations, you should see `quarantine = yes` annotated to the IP address of the infected hosts.



Query
* quarantine = yes

Showing 2 of 2 inventory

Address	* Location	* Service	* Quarantine
192.168.110.2	Contractors		yes
192.168.10.35	DC		yes

What to do next

Once you clean the quarantined host and it is no longer infected, you can perform either of the following actions to remove the quarantine annotation:

- (**Recommended**) Use Secure Workload to change the **`quarantine = yes`** annotation back to **`quarantine = no`**.

  1. For example, if the quarantined host that is no longer infected is 172.21.208.11 and within the **`Default`** scope, create a CSV file such as:

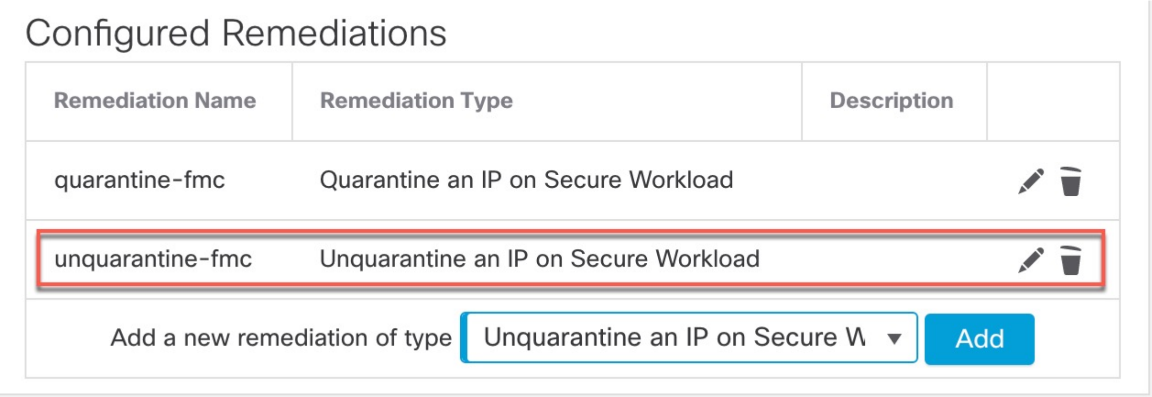
     ```
     IP,VRF,quarantine
     172.21.208.11,Default,no
     ```

  2. Navigate to **Applications** > **Inventory Upload**, and then upload the CSV file to Secure Workload. For more information on how to upload a CSV file to Secure Workload, see the Related Documentation section.

- Use FMC Remediation Module to remove the quarantine annotation.

Important This method is not recommended in production networks due to security concerns.

  1. (In the Configure section, see Step 1) Add a new remediation that uses the un-quarantine type of remediation. Edit the same instance, and under **Configured Remediations**, select and add the un-quarantine type of remediation (in this example, **`unquarantine-fmc`**).



Configured Remediations

Remediation Name	Remediation Type	Description	
quarantine-fmc	Quarantine an IP on Secure Workload		✎ 🗑
unquarantine-fmc	Unquarantine an IP on Secure Workload		✎ 🗑

Add a new remediation of type: Unquarantine an IP on Secure W ▾ Add

2. (In the Configure section, see Step 2) Add an access control rule (For example, **`remove-tag`**) to the same policy (For example, **`rem-policy`**) which can be used to trigger the un-quarantine remediation.

3. (In the Configure section, see Step 3) Add a correlation rule (For example, **`unquaran-rule1`**) that uses the access control rule (in this example, **`remove-tag`**).

4. (In the Configure section, see Step 4ß) Assign the un-quarantine response (For example, **`un-quaran-rem`**) to the correlation rule (For example, **`unquaran-rule1`**).

5. After the rule is matched, the un-quarantine remediation will be triggered to remove the quarantine annotation.