

Remediations

The following topics contain information on configuring remediations:

- Requirements and Prerequisites for Remediations, on page 1
- Introduction to Remediations, on page 1
- Managing Remediation Modules, on page 11
- Managing Remediation Instances, on page 12
- Managing Instances for a Single Remediation Module, on page 12

Requirements and Prerequisites for Remediations

Model Support

Any

Supported Domains

Any

User Roles

- Admin
- Discovery Admin

Introduction to Remediations

A *remediation* is a program that the Firepower System launches in response to a correlation policy violation.

When a remediation runs, the system generates a *remediation status event*. Remediation status events include details such as the remediation name, the correlation policy and rule that triggered it, and the exit status message.

The system supports several remediation modules:

- Cisco ISE Endpoint Protection Services (EPS) — quarantines, unquarantines, or shuts down traffic sent to a host or network involved in a correlation policy violation

- Cisco IOS Null Route — blocks traffic sent to a host or network involved in a correlation policy violation (requires Cisco IOS Version 12.0 or higher)
- Nmap Scanning — scans hosts to determine running operating systems and servers
- Set Attribute Value — sets a host attribute on a host involved in a correlation policy violation

Tip You can install custom modules that perform other tasks; see the *Firepower System Remediation API Guide*.

Implementing Remediations

To implement a remediation, first create at least one *instance* for the module you choose. You can create multiple instances per module, where each instance is configured differently. For example, to communicate with multiple routers using the Cisco IOS Null Route remediation module, configure multiples instances of that module.

You can then add multiple *remediations* to each instance that describe the actions you want to perform when a policy is violated.

Finally, associate remediations with rules in correlation policies, so that the system launches the remediations in response to correlation policy violations.

Remediations and Multitenancy

In a multidomain deployment, you can install custom remediation modules at any domain level. The system-provided modules belong to the Global domain.

Though you cannot add a remediation to an instance created in an ancestor domain, you can create a similarly configured instance in the current domain and add remediations to that instance. You can also use remediations created in ancestor domains as correlation responses.

Related Topics

Firepower Management Center Alert Responses
Nmap Scanning
Adding Responses to Rules and White Lists

Cisco ISE EPS Remediations

If you have Endpoint Protection Service (EPS) enabled and configured in your ISE deployment, you can configure your Firepower Management Center to launch remediations using ISE. When fully configured, ISE EPS remediations run the following **Mitigation Actions** on the source or destination host involved in a correlation policy violation:

- **`quarantine`**—Limits or denies an endpoint's access the network
- **`unquarantine`**—Reverses an endpoint's quarantine status and allows full access to the network
- **`shutdown`**—Deactivates an endpoint's network attached system (NAS) port to disconnect it from the network

You can also exempt specific IP addresses from ISE EPS remediation.

Note Your ISE version and configuration impact how you can use ISE in the Firepower System. For more information, see The ISE Identity Source for more information.

For more information about ISE EPS actions, see the *Cisco Identity Services Engine User Guide*.

Configuring ISE EPS Remediations

You can respond to correlation policy violations by running ISE EPS remediations on the source or destination host.

Before you begin

- Configure EPS operations on your ISE server.
- Configure a connection to ISE as described in Configure ISE for User Control.

Procedure

Step 1 Choose **Policies** > **Actions** > **Instances**.

Step 2 Add a pxGrid mitigation instance as described in Adding an ISE EPS Instance, on page 3.

Step 3 Add one or more ISE EPS remediations as described in Adding ISE EPS Remediations, on page 4.

What to do next

- Assign remediations as responses to correlation policy violations as described in Adding Responses to Rules and White Lists.

Adding an ISE EPS Instance

Create ISE EPS instances to group individual remediations by logging type.

Procedure

Step 1 Choose **Policies** > **Actions** > **Instances**.

Step 2 From the **Add a New Instance** list, choose **pxGrid Mitigation(v1.0)** as the module type and click **Add**.

Step 3 Enter an **Instance Name** and **Description**.

Step 4 Set **Enable Logging** option to enable or disable system logging.

Step 5 Click **Create**.

What to do next

- Create an ISE EPS remediation as described in Adding Set Attribute Value Remediations, on page 10.

Related Topics

Firepower System IP Address Conventions

Adding ISE EPS Remediations

Create one or more ISE EPS remediations within an instance to run **Mitigation Actions** on the source or destination host involved in a correlation policy violation.

In a multidomain deployment, you cannot add a remediation to an instance created in an ancestor domain.

Before you begin

- Create an ISE EPS instance as described in Adding an ISE EPS Instance, on page 3.

Procedure

Step 1 Choose **Policies** > **Actions** > **Instances**.

Step 2 Next to the instance where you want to add the remediation, click **View** ( ).

Step 3 In the **Configured Remediations** section, choose the **Mitigate Destination** or **Mitigate Source** and click **Add**.

If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 4 Enter a **Remediation Name** and **Description**.

Step 5 Choose a **Mitigation Action**: **`quarantine`**, **`unquarantine`**, or **`shutdown`**.

Step 6 (Optional) To exempt IP addresses or ranges from remediation, enter them into the **Whitelist** box.

Step 7 Click **Create**, then click **Done**.

What to do next

- Assign remediations as responses to correlation policy violations; see Adding Responses to Rules and White Lists.

Cisco IOS Null Route Remediations

The Cisco IOS Null Route remediation module allows you to block an IP address or range of addresses using Cisco's "null route" command. This drops all traffic sent to a host or network by routing it to the router's NULL interface. This does not block traffic sent from the violating host or network.

Note Do not use a destination-based remediation as a response to a correlation rule that is based on a discovery or host input event. These events are associated with source hosts.

Caution When a Cisco IOS remediation is activated, there is no timeout period. To unblock the IP address or network, you must manually clear the routing change from the router.

Configuring Remediations for Cisco IOS Routers

Note Do not use a destination-based remediation as a response to a correlation rule that is based on a discovery or host input event. These events are associated with source hosts.

Caution When a Cisco IOS remediation is activated, there is no timeout period. To unblock the IP address or network, you must manually clear the routing change from the router.

Before you begin

- Confirm that your Cisco router is running Cisco IOS 12.0 or higher.
- Confirm that you have level 15 administrative access to the router.

Procedure

Step 1 Enable Telnet on the Cisco router as described in the documentation provided with your Cisco router or IOS software.

Step 2 On the Firepower Management Center, add a Cisco IOS Null Route instance for each Cisco IOS router you plan to use; see Adding a Cisco IOS Instance, on page 5.

Step 3 Create remediations for each instance, based on the type of response you want to elicit on the router when correlation policies are violated:

- Adding Cisco IOS Block Destination Remediations, on page 6
- Adding Cisco IOS Block Destination Network Remediations, on page 7
- Adding Cisco IOS Block Source Remediations, on page 8
- Adding Cisco IOS Block Source Network Remediations, on page 8

What to do next

- Assign remediations as responses to correlation policy violations; see Adding Responses to Rules and White Lists.

Adding a Cisco IOS Instance

If you have multiple routers where you want to send remediations, create a separate instance for each router.

Before you begin

- Configure Telnet access on the Cisco IOS router as described in the documentation provided with the router or IOS software.

Procedure

Step 1 Choose **Policies** > **Actions** > **Instances**.

Step 2 From the **Add a New Instance** list, choose **Cisco IOS Null Route** and click **Add**.

Step 3 Enter an **Instance Name** and **Description**.

Step 4 In the **Router IP** field, enter the IP address of the Cisco IOS router you want to use for the remediation.

Step 5 In the **Username** field, enter the Telnet user name for the router. This user must have level 15 administrative access on the router.

Step 6 In the **Connection Password** fields, enter the Telnet user's user password.

Step 7 In the **Enable Password** fields, enter the Telnet user's enable password. This is the password used to enter privileged mode on the router.

Step 8 In the **White List** field, enter IP addresses or ranges that you want to exempt from the remediation, one per line.

Note The system builds a separate network map for each leaf domain. In a multidomain deployment, using literal IP addresses to constrain this configuration can have unexpected results.

Step 9 Click **Create**.

What to do next

- Add specific remediations to be used by correlation policies as described in Adding Cisco IOS Block Destination Remediations, on page 6, Adding Cisco IOS Block Destination Network Remediations, on page 7, Adding Cisco IOS Block Source Remediations, on page 8, and Adding Cisco IOS Block Source Network Remediations, on page 8.

Related Topics

Firepower System IP Address Conventions

Adding Cisco IOS Block Destination Remediations

The Cisco IOS Block Destination remediation blocks traffic sent from the router to the destination host involved in a correlation policy violation. Do not use this remediation as a response to a correlation rule that is based on a discovery or host input event. These events are associated with source hosts.

In a multidomain deployment, you cannot add a remediation to an instance created in an ancestor domain.

Before you begin

- Add a Cisco IOS instance as described in Adding a Cisco IOS Instance, on page 5.

Procedure

Step 1 Choose **Policies** > **Actions** > **Instances**.

Step 2 Next to the instance where you want to add the remediation, click **View** ( ).

Step 3 In the **Configured Remediations** section, choose **Block Destination** and click **Add**.

If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 4 Enter a **Remediation Name** and **Description**.

Step 5 Click **Create**, then click **Done**.

What to do next

- Assign remediations as responses to correlation policy violations; see Adding Responses to Rules and White Lists.

Adding Cisco IOS Block Destination Network Remediations

The Cisco IOS Block Destination Network remediation blocks traffic sent from the router to the network of the destination host involved in a correlation policy violation. Do not use this remediation as a response to a correlation rule that is based on a discovery or host input event. These events are associated with source hosts.

In a multidomain deployment, you cannot add a remediation to an instance created in an ancestor domain.

Before you begin

- Add a Cisco IOS instance as described in Adding a Cisco IOS Instance, on page 5.

Procedure

Step 1 Choose **Policies** > **Actions** > **Instances**.

Step 2 Next to the instance where you want to add the remediation, click **View** ( ).

Step 3 In the **Configured Remediations** section, choose **Block Destination Network** and click **Add**.

If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 4 Enter a **Remediation Name** and **Description**.

Step 5 In the **Netmask** field, enter the subnet mask or use CIDR notation to describe the network that you want to block traffic to.

For example, to block traffic to an entire Class C network when a single host triggered a rule (this is not recommended), use `255.255.255.0` or `24` as the netmask.

As another example, to block traffic to 30 addresses that include the triggering IP address, specify `255.255.255.224` or `27` as the netmask. In this case, if the IP address `10.1.1.15` triggers the remediation, all IP addresses between `10.1.1.1` and `10.1.1.30` are blocked. To block only the triggering IP address, leave the field blank, enter `32`, or enter `255.255.255.255`.

Step 6 Click **Create**, then click **Done**.

What to do next

- Assign remediations as responses to correlation policy violations; see Adding Responses to Rules and White Lists.

Related Topics

Firepower System IP Address Conventions

Adding Cisco IOS Block Source Remediations

The Cisco IOS Block Source remediation blocks traffic sent from the router to the source host involved in a correlation policy violation.

In a multidomain deployment, you cannot add a remediation to an instance created in an ancestor domain.

Before you begin

- Add a Cisco IOS instance as described in Adding a Cisco IOS Instance, on page 5.

Procedure

Step 1 Choose **Policies** > **Actions** > **Instances**.

Step 2 Next to the instance where you want to add the remediation, click **View** ( ).

Step 3 In the **Configured Remediations** section, choose **Block Source** and click **Add**.

If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 4 Enter a **Remediation Name** and **Description**.

Step 5 Click **Create**, then click **Done**.

What to do next

- Assign remediations as responses to correlation policy violations; see Adding Responses to Rules and White Lists.

Adding Cisco IOS Block Source Network Remediations

The Cisco IOS Block Source Network remediation blocks traffic sent from the router to the network of the source host involved in a correlation policy violation.

In a multidomain deployment, you cannot add a remediation to an instance created in an ancestor domain.

Before you begin

- Add a Cisco IOS instance as described in Adding a Cisco IOS Instance, on page 5.

Procedure

Step 1 Choose **Policies** > **Actions** > **Instances**.

Step 2 Next to the instance where you want to add the remediation, click **View** ( ).

Step 3 In the **Configured Remediations** section, choose **Block Source Network** and click **Add**.

If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 4 Enter a **Remediation Name** and **Description**.

Step 5 In the **Netmask** field, enter the subnet mask or CIDR notation that describes the network that you want to block traffic to.

For example, to block traffic to an entire Class C network when a single host triggered a rule (this is not recommended), use `255.255.255.0` or `24` as the netmask.

As another example, to block traffic to 30 addresses that include the triggering IP address, specify `255.255.255.224` or `27` as the netmask. In this case, if the IP address `10.1.1.15` triggers the remediation, all IP addresses between `10.1.1.1` and `10.1.1.30` are blocked. To block only the triggering IP address, leave the field blank, enter `32`, or enter `255.255.255.255`.

Step 6 Click **Create**, then click **Done**.

What to do next

- Assign remediations as responses to correlation policy violations; see Adding Responses to Rules and White Lists.

Related Topics

Firepower System IP Address Conventions

Nmap Scan Remediations

The Firepower System integrates with Nmap™, an open source active scanner for network exploration and security auditing. You can respond to a correlation policy violation using an Nmap remediation, which triggers an Nmap scan remediation.

For more information about Nmap scanning, see Nmap Scanning.

Set Attribute Value Remediations

You can respond to a correlation policy violation by setting a host attribute value on the host where the triggering event occurred. For text host attributes, you can use the description from the event as the attribute value.

Configuring Set Attribute Remediations

Procedure

Step 1 Choose **Policies** > **Actions** > **Instances**.

Step 2 Create a set attribute instance as described in Adding a Set Attribute Value Instance, on page 10.

Step 3 Add a set attribute remediation as described in Adding Set Attribute Value Remediations, on page 10.

What to do next

- Assign remediations as responses to correlation policy violations; see Adding Responses to Rules and White Lists.

Related Topics

Predefined Host Attributes
User-Defined Host Attributes

Adding a Set Attribute Value Instance

Procedure

Step 1 Choose **Policies** > **Actions** > **Instances**.

Step 2 From the **Add a New Instance** list, choose **Set Attribute Value** and click **Add**.

Step 3 Enter an **Instance Name** and **Description**.

Step 4 Click **Create**.

What to do next

- Create a set attribute remediation as described in Adding Set Attribute Value Remediations, on page 10.

Adding Set Attribute Value Remediations

The Set Attribute Value remediation sets a host attribute on a host involved in a correlation policy violation. Create a remediation for each attribute value you want set. For text attributes, you can use the description from the triggering event as the attribute value.

In a multidomain deployment, you cannot add a remediation to an instance created in an ancestor domain.

Before you begin

- Create a set attribute instance as described in Adding a Set Attribute Value Instance, on page 10.

Procedure

Step 1 Choose **Policies** > **Actions** > **Instances**.

Step 2 Next to the instance where you want to add the remediation, click **View** ( ).

Step 3 In the **Configured Remediations** section, choose **Set Attribute Value** and click **Add**.

If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 4 Enter a **Remediation Name** and **Description**.

Step 5 To use this remediation in response to an event with source and destination data, choose an **Update Which Host(s) From Event** option.

Step 6 For text attributes, specify whether you want to **Use Description From Event For Attribute Value**:

- To use the description from the event as the attribute value, click **On** and enter the **Attribute Value** you want to set.
- To use the **Attribute Value** setting for the remediation as the attribute value, click **Off**.

Step 7 Click **Create**, then click **Done**.

What to do next

- Assign remediations as responses to correlation policy violations; see Adding Responses to Rules and White Lists.

Managing Remediation Modules

In a multidomain deployment, the system displays remediation modules installed in the current domain, which you can delete. It also displays modules installed in ancestor domains, which you cannot delete. To manage remediation modules in a lower domain, switch to that domain.

Procedure

Step 1 Choose **Policies** > **Actions** > **Modules**.

Step 2 Manage your remediation modules:

- Configure — To view the Module Detail page for a module and configure its instances and remediations, click **View** ( ). In a multidomain deployment, you cannot use the Module Detail page to add, delete, or edit instances in the current domain for a module installed in an ancestor domain. Instead, use the Instances page (**Policies** > **Actions** > **Instances**); see Managing Remediation Instances, on page 12.
- Delete — To delete a custom module that is not in use, click **Delete** ( ). You cannot delete system-provided modules.

- Install — To install a custom module, click **Choose File**, browse to the module, and click **Install**. For more information, see the *Firepower System Remediation API Guide*.

Managing Remediation Instances

The Instances page lists all configured instances for all remediation modules.

In a multidomain deployment, the system displays remediation instances created in the current domain, which you can edit. It also displays instances created in ancestor domains, which you cannot edit. To manage remediation instances in a lower domain, switch to that domain.

Though you cannot add a remediation to an instance created in an ancestor domain, you can create a similarly configured instance in the current domain and add remediations to that instance. You can also use remediations created in ancestor domains as correlation responses.

Procedure

Step 1 Choose **Policies** > **Actions** > **Instances**.

Step 2 Manage your remediation instances:

- Add—To add an instance, choose the remediation module for which you want to add an instance and click **Add**. For system-provided modules, see:
  - Adding an ISE EPS Instance, on page 3
  - Adding a Cisco IOS Instance, on page 5
  - Adding an Nmap Scan Instance
  - Adding a Set Attribute Value Instance, on page 10

  For help adding a custom module, see the documentation for that module, if available.
- Configure—To configure instance details and add remediations to the instance, click **View** ().
- Delete—To delete an instance that is not in use, click **Delete** ().

Managing Instances for a Single Remediation Module

The Module Detail page displays all of the instances and remediations configured for a particular remediation module.

In a multidomain deployment, you can access the Module Detail page for remediation modules installed in the current domain and in ancestor domains. However, you cannot use the Module Detail page to add, delete, or edit instances in the current domain for a module installed in an ancestor domain. Instead, use the Instances page (**Policies** > **Actions** > **Instances**); see Managing Remediation Instances, on page 12 .

Procedure

Step 1 Choose **Policies** > **Actions** > **Modules**.

Step 2 Next to the remediation module whose instances you want to manage, click **View** ().

Step 3 Manage your remediation instances:

- Add — To add an instance, click **Add**. For system-provided modules, see:
  - Adding an ISE EPS Instance, on page 3
  - Adding a Cisco IOS Instance, on page 5
  - Adding an Nmap Scan Instance
  - Adding a Set Attribute Value Instance, on page 10

  For help adding an instance for a custom module, see the documentation for that module, if available.
- Configure — To configure instance details and add remediations to the instance, click **View** ().
- Delete — To delete an instance that is not in use, click **Delete** ().