

# Host identity sources

These topics provide information on host identity sources.


- Host data collection overview, on page 1
- Requirements and prerequisites for host identity sources, on page 2
- Determine which host operating systems the system can detect, on page 2
- Identifying host operating systems, on page 3
- Custom fingerprinting, on page 3
- Host input data, on page 11
- Nmap scanning, on page 19
- History for host identity sources, on page 36


# Host data collection overview

Host data collection is a passive monitoring mechanism that

- compares specific packet header values and other unique data from network traffic against established definitions called *fingerprints*,
- determines information about the hosts on your network, and
- identifies network topology and system characteristics through traffic analysis.

### Host information collected

The system determines this information about hosts on your network:

- The number and types of hosts (including network devices such as bridges, routers, load balancers, and NAT devices).
- Basic network topology data, including the number of hops from the discovery point on the network to the hosts.
- The operating systems running on the hosts.
- Applications on the hosts and users associated with these applications.

If the system cannot identify a host's operating system, you can create custom client or server fingerprints. The system uses these fingerprints to identify new hosts. You can map fingerprints to systems in the

vulnerability database (VDB) to allow the appropriate vulnerability information to be displayed whenever a host is identified using the custom fingerprint.

**Note** In addition to collecting host data from monitored network traffic, the system can collect host data from exported NetFlow records, and you can actively add host data using Nmap scans and the host input feature.

# Requirements and prerequisites for host identity sources

This topic provides the necessary requirements and prerequisites to manage host identity sources:

| Requirement | Details |
|---|---|
| Model support | Any. |
| Supported domains | Any, with the exception of custom fingerprinting, which is Leaf only. |
| User roles | • Administrator<br>• Discovery Admin, except for third-party data and custom mappings. |

# Determine which host operating systems the system can detect

To verify the exact operating systems that the system can fingerprint, you can view the list of available fingerprints during the process of creating a custom operating system fingerprint. This helps you understand which operating systems the system is capable of identifying.

### Procedure

**Step 1** Choose **Policies** > **+ Show more** > **Advanced** > **Network Discovery**.

**Step 2** Click **Custom Operating Systems**.

**Step 3** Click **Create Custom Fingerprint**.

**Step 4** In the **OS Vulnerability Mappings** section, view the options available in the drop-down lists. These options represent the operating systems that the system can fingerprint.

### What to do next

For more information, refer to Identifying host operating systems, on page 3.

# Identifying host operating systems

If the system does not correctly identify a host operating system (for example, it shows in the Host Profile as Unknown or is incorrectly identified), try the strategies listed here.

**Procedure**

Try one of these strategies:

- Check the Network Discovery Identity Conflict Settings.
- Create a custom fingerprint for the host.
- Run an Nmap scan against the host.
- Import data into the network map, using the host input feature.
- Manually enter operating system information.

# Custom fingerprinting

The system includes operating system *fingerprints* that the system uses to identify the operating system on each host it detects. However, sometimes the system cannot identify a host operating system or misidentifies it because no fingerprints exist that match the operating system. To correct this problem, you can create a *custom fingerprint*. This fingerprint provides a pattern of operating system characteristics unique to the unknown or misidentified operating system and supplies the name of the operating system for identification purposes

### Operating system identification and vulnerability mapping

If the system cannot match the operating system of a host, it cannot identify the vulnerabilities for the host, because the system derives the list of vulnerabilities for each host from its operating system fingerprint. For example, if the system detects a host running Microsoft Windows, it adds a stored Microsoft Windows vulnerability list to the host's profile based on the detected operating system.

As an example, if you have several devices on your network running a new beta version of Microsoft Windows, the system cannot identify that operating system or map vulnerabilities to the hosts. However, knowing that the system has a list of vulnerabilities for Microsoft Windows, you may want to create a custom fingerprint for one of the hosts to help identify the other hosts running the same operating system. You can include a mapping of the vulnerability list for Microsoft Windows in the fingerprint to associate it with each host that matches the fingerprint.

When you create a custom fingerprint, the Firewall Management Center lists the set of vulnerabilities associated with that fingerprint for any hosts running the same operating system. If the custom fingerprint does not contain any vulnerability mappings, the system uses the fingerprint to assign the custom operating system information you provide. When the system sees new traffic from a previously detected host, it updates the

host with the new fingerprint information. The system also uses the new fingerprint to identify any new hosts with that operating system the first time they are detected.

Before you create a custom fingerprint, determine why the host is not being identified correctly to decide whether custom fingerprinting is a viable solution.

You can create two types of fingerprints with the system:

- Client fingerprints, which identify operating systems based on the SYN packet that the host sends when it connects to a TCP application running on another host on the network.
- Server fingerprints, which identify operating systems based on the SYN-ACK packet that the host uses to respond to an incoming connection to a running TCP application.

**Note** If both a client and server fingerprint match the same host, the client fingerprint is used.

After creating fingerprints, you must activate them before the system can associate them with hosts.

# Manage fingerprints

After a fingerprint is created and activated, you can edit a fingerprint to make changes or add vulnerability mappings.

### Procedure

**Step 1** Choose **Policies** > **+ Show more** > **Advanced** > **Network Discovery**.

**Step 2** Click **Custom Operating Systems**.

If the system is waiting for data to create a fingerprint, it refreshes the page every 10 seconds until the fingerprint is created.

**Step 3** Manage your custom fingerprints using these options:

- **Activate/Deactivate**: Activate or deactivate a fingerprint as described in Activate and deactivate fingerprints, on page 4.
- **Create**: Create fingerprints as described in Create a custom fingerprint for clients, on page 6 and Create a custom fingerprint for servers, on page 8.
- **Edit**: Edit a fingerprint as described in Edit an active fingerprint, on page 5 and Edit an inactive fingerprint, on page 6.
- **Delete**: Click **Delete** ( ) next to the fingerprint you want to delete, and click **OK** to confirm. You can only delete deactivated fingerprints.

## Activate and deactivate fingerprints

You must activate a custom fingerprint before the system can use it to identify hosts. After the new fingerprint is activated, the system uses it to re-identify previously discovered hosts and discover new hosts.

If you want to stop using a fingerprint, you can deactivate it. Deactivating a fingerprint prevents the system from using it, but the fingerprint remains on the system. When you deactivate a fingerprint, the operating system is marked as unknown for hosts that use the fingerprint. If these hosts are detected again and match a different active fingerprint, they are then identified by that active fingerprint.

Deleting a fingerprint removes it from the system completely. After deactivating a fingerprint, you can delete it.

**Procedure**

**Step 1** Choose **Policies** > **+ Show more** > **Advanced** > **Network Discovery**.

**Step 2** Click **Custom Operating Systems**.

**Step 3** Click the slider next to the fingerprint you want to activate or deactivate.

**Note** The activate option is only available if the fingerprint you created is valid. If the slider is not available, try creating the fingerprint again.

## Edit an active fingerprint

If a fingerprint is *active*, you can modify the fingerprint name, description, and custom operating system display. You can also map additional vulnerabilities to it.

You can modify the fingerprint name, description, custom operating system display, and map additional vulnerabilities to it.

**Procedure**

**Step 1** Choose **Policies** > **+ Show more** > **Advanced** > **Network Discovery**.

**Step 2** Click **Custom Operating Systems**.

**Step 3** Click **Edit** (✎) next to the fingerprint you want to edit.

**Step 4** Modify the fingerprint name, description, and custom OS display, if necessary.

**Step 5** If you want to delete a vulnerability mapping, click **Delete** next to the mapping in the **Pre-Defined OS Product Maps** section of the page.

**Step 6** If you want to add additional operating systems for vulnerability mapping, choose the **Product** and, if applicable, **Major Version**, **Minor Version**, **Revision Version**, **Build**, **Patch**, and **Extension** and then click **Add OS Definition**.

The vulnerability mapping is added to the **Pre-Defined OS Product Maps** list.

**Step 7** Click **Save**.

# Edit an inactive fingerprint

If a fingerprint is *inactive*, you can modify all elements of the fingerprint and resubmit it to the Secure Firewall Management Center. This includes all properties you specified when creating the fingerprint, such as fingerprint type, target IP addresses and ports, vulnerability mappings, and so on.

When you edit and submit an inactive fingerprint, the system resubmits it. If it is a client fingerprint, you must resend traffic to the appliance before activating it. Note that you can choose only a single vulnerability mapping for an inactive fingerprint. After you activate the fingerprint, you can map additional operating systems and versions to its vulnerabilities list.

### Procedure

**Step 1** Choose **Policies** > **+ Show more** > **Advanced** > **Network Discovery**.

**Step 2** Click **Custom Operating Systems**.

**Step 3** Click **Edit** (✎) next to the fingerprint you want to edit.

**Step 4** Make changes to the fingerprint as necessary:

- If you are modifying a client fingerprint, refer to Create a custom fingerprint for clients, on page 6.
- If you are modifying a server fingerprint, refer to Create a custom fingerprint for servers, on page 8.

**Step 5** Click **Save**.

### What to do next

If you modified a client fingerprint, remember to send traffic from the host to the appliance gathering the fingerprint.

# Create a custom fingerprint for clients

Client fingerprints identify the operating system by analyzing the SYN packet a host sends when it connects to a TCP application on another network host.

If the Firewall Management Center does not have direct contact with monitored hosts, you can specify a device that is managed by the Firewall Management Center and is closest to the host you intend to fingerprint when specifying client fingerprint properties.

### Before you begin

Before you begin the fingerprinting process, obtain these details about the host you want to fingerprint:

- The number of network hops between the host and the Firewall Management Center or the device you use to obtain the fingerprint. (Cisco strongly recommends that you directly connect the Firewall Management Center or the device to the same subnet that the host is connected to.)
- The network interface (on the Firewall Management Center or the device) that is connected to the network where the host resides.
- The actual operating system vendor, product, and version of the host.
- Access to the host in order to generate client traffic.

### Procedure

**Step 1** Choose **Policies** > **+ Show more** > **Advanced** > **Network Discovery**.

**Step 2** Click **Custom Operating Systems**, and then click **Create Custom Fingerprint**.

**Step 3** Enter these details:

**a.** From the **Device** drop-down list, choose the Firewall Management Center or the device that you want to use to collect the fingerprint.

**b.** Enter a **Fingerprint Name**, **Fingerprint Description**, and from the **Fingerprint Type** list, choose **Client**.

**c.** In the **Target IP Address** field, enter an IP address of the host you want to fingerprint.

**Note** The fingerprint is based exclusively on traffic to and from the specified host IP address. Traffic from other IP addresses assigned to the host is not included.

**d.** In the **Target Distance** field, enter the number of network hops between the host and the device that you chose earlier to collect the fingerprint.

**Caution** This must be the actual number of physical network hops to the host, which may or may not be the same as the number of hops detected by the system.

**e.** From the **Interface** list, choose the network interface that is connected to the network segment where the host resides.

**Note** Use the management interface or any other available network interfaces that is configured as the sensing interface on your device to perform fingerprint collection. If you do not know which interface is the sensing interface on your device, refer to the *Installation Guide* for the specific model you are using to fingerprint.

**f.** If you want to display custom information in the host profile for fingerprinted hosts (or if the host you want to fingerprint does not reside in the **OS Vulnerability Mappings** section), choose **Use Custom OS Display** and provide the values you want to display for these fields:

- In the **Vendor String** field, enter the operating system's vendor name. For example, the vendor for Microsoft Windows would be Microsoft.
- In the **Product String** field, enter the operating system's product name. For example, the product name for Microsoft Windows 2000 would be Windows.
- In the **Version String** field, enter the operating system's version number. For example, the version number for Microsoft Windows 2000 would be 2000.

**g.** In the OS Vulnerability Mappings section, choose the operating system, product, and versions you want to use for vulnerability mapping.

You must specify **Vendor** and **Product** values in this section if you want to use the fingerprint to identify vulnerabilities for matching hosts or if you do not assign custom operating system display information.

To map vulnerabilities for all versions of an operating system, specify only the **Vendor** and **Product** values.



**Note** Not all options in the **Major Version**, **Minor Version**, **Revision Version**, **Build**, **Patch**, and **Extension** drop-down lists may apply to the operating system you choose. In addition, if no definition appears in a list that matches the operating system you want to fingerprint, you can leave these values empty. Be aware that if you do not create any OS vulnerability mappings in a fingerprint, the system cannot use the fingerprint to assign a vulnerabilities list with hosts identified by the fingerprint.

**Example:**

If you want your custom fingerprint to assign the list of vulnerabilities from Redhat Linux 9 to matching hosts, choose **Redhat, Inc.** as the vendor, **Redhat Linux** as the product, and **9** as the major version.

**Example:**

To add all versions of the Palm OS, you would choose **PalmSource, Inc.** from the **Vendor** list, **Palm OS** from the **Product** list, and leave all other lists at their default settings.

**Step 4** Click **Create**.

The status briefly shows `New`, then switches to `Pending`, where it remains until traffic is seen for the fingerprint. Once traffic is seen, it switches to `Ready`.

The Custom Fingerprint status page refreshes every ten seconds until it receives data from the host in question.

**Step 5** Using the IP address you specified as the target IP address, access the host you are trying to fingerprint and initiate a TCP connection to the appliance.

To create an accurate fingerprint, traffic **must** be seen by the appliance collecting the fingerprint. If you are connected through a switch, traffic to a system other than the appliance may not be seen by the system.

**Example:**

Access the web interface of the Firewall Management Center from the host you want to fingerprint or SSH into the Firewall Management Center from the host. If you are using SSH, use the command below, where localIPv6address is the IPv6 address specified in step 7 that is currently assigned to the host and DCmanagementIPv6address is the management IPv6 address of the Firewall Management Center. The Custom Fingerprint page should then reload with a “Ready” status.

```
ssh -b localIPv6address DCmanagementIPv6address
```

## Create a custom fingerprint for servers

Server fingerprints identify operating systems based on the SYN-ACK packet that the host uses to respond to an incoming connection to a running TCP application.

Before you begin, you should obtain this information about the host you want to fingerprint:

- The number of network hops between the host and the appliance you use to obtain the fingerprint. Cisco strongly recommends that you directly connect an unused interface on the appliance to the same subnet that the host is connected to.
- The network interface (on the appliance) that is connected to the network where the host resides.
- The actual operating system vendor, product, and version of the host.
- An IP address that is not currently in use and is authorized on the network where the host is located.

**Tip** If the Firewall Management Center does not have direct contact with monitored hosts, you can specify a managed device that is closest to the host you intend to fingerprint when specifying server fingerprint properties.

## Procedure

**Step 1** Choose **Policies** > **+ Show more** > **Advanced** > **Network Discovery**.

**Step 2** Click **Custom Operating Systems** and then, click **Create Custom Fingerprint**.

**Step 3**

**a.** From the **Device** list, choose the Firewall Management Center or the managed device that you want to use to collect the fingerprint and enter a **Fingerprint Name**.

**b.** Enter a **Fingerprint Description** and from the **Fingerprint Type** list, choose **Server** to display the server fingerprinting options. In the **Target IP Address** field, enter an IP address of the host you want to fingerprint.

Note that the fingerprint will only be based on traffic to and from the host IP address you specify, not any of the host's other IP addresses (if it has any).

**Caution** You can capture IPv6 fingerprints only with appliances running Version 5.2 and later.

**c.** In the **Target Distance** field, enter the number of network hops between the host and the device that you chose earlier to collect the fingerprint.

**Caution** This must be the actual number of physical network hops to the host, which may or may not be the same as the number of hops detected by the system.

**d.** From the **Interface** list, choose the network interface that is connected to the network segment where the host resides.

**Caution** Cisco recommends that you do **not** use the sensing interface on a managed device for fingerprinting for several reasons. First, fingerprinting does not work if the sensing interface is on a span port. Also, if you use the sensing interface on a device, the device stops monitoring the network for the amount of time it takes to collect the fingerprint. You can, however, use the management interface or any other available network interfaces to perform fingerprint collection. If you do not know which interface is the sensing interface on your device, refer to the *Installation Guide* for the specific model you are using to fingerprint.

**e.** Click **Get Active Ports**. In the **Server Port** field, enter the port that you want the device chose to collect the fingerprint to initiate contact with, or choose a port from the **Get Active Ports** drop-down list.

You can use any server port that you know is open on the host (for instance, 80 if the host is running a web server).

**f.** In the **Source IP Address** field, enter an IP address that should be used to attempt to communicate with the host.

You should use a source IP address that is authorized for use on the network but is not currently being used, for example, a DHCP pool address that is currently not in use. This prevents you from temporarily knocking another host offline while you create the fingerprint.

You should exclude that IP address from monitoring in your network discovery policy while you create the fingerprint. Otherwise, the network map and discovery event views will be cluttered with inaccurate information about the host represented by that IP address.

**g.** In the **Source Subnet Mask** field, enter the subnet mask for the IP address you are using. If the **Source Gateway** field appears, enter the default gateway IP address that should be used to establish a route to the host. If you want to display custom information in the host profile for fingerprinted hosts or if the fingerprint name you want to use does not exist in the OS Definition section, choose **Use Custom OS Display** in the Custom OS Display section.

Provide the values you want to appear in host profiles for these fields:

- In the **Vendor String** field, enter the operating system's vendor name. For example, the vendor for Microsoft Windows would be Microsoft.
- In the **Product String** field, enter the operating system's product name. For example, the product name for Microsoft Windows 2000 would be Windows.
- In the **Version String** field, enter the operating system's version number. For example, the version number for Microsoft Windows 2000 would be 2000.

**h.**

**Step 4** In the OS Vulnerability Mappings section, choose the operating system, product, and versions you want to use for vulnerability mapping.

You must specify a Vendor and Product name in this section if you want to use the fingerprint to identify vulnerabilities for matching hosts or if you do not assign custom operating system display information.

To map vulnerabilities for all versions of an operating system, specify only the vendor and product name.

**Note** Not all options in the **Major Version**, **Minor Version**, **Revision Version**, **Build**, **Patch**, and **Extension** drop-down lists may apply to the operating system you choose. In addition, if no definition appears in a list that matches the operating system you want to fingerprint, you can leave these values empty. Be aware that if you do not create any OS vulnerability mappings in a fingerprint, the system cannot use the fingerprint to assign a vulnerabilities list with hosts identified by the fingerprint.

**Example:**

If you want your custom fingerprint to assign the list of vulnerabilities from Redhat Linux 9 to matching hosts, choose **Redhat, Inc.** as the vendor, **Redhat Linux** as the product, and **9** as the version.

**Example:**

To add all versions of the Palm OS, you would choose **PalmSource, Inc.** from the **Vendor** list, **Palm OS** from the **Product** list, and leave all other lists at their default settings.

**Step 5** Click **Create**.
The Custom Fingerprint status page refreshes every ten seconds and should reload with a "Ready" status.

**Note** If the target system stops responding during the fingerprinting process, the status shows an `ERROR: No Response` message. If you see this message, submit the fingerprint again. Wait three to five minutes (the time period may vary depending on the target system), click **Edit** (✎) to access the Custom Fingerprint page, and then click **Create**.

### What to do next

Activate the fingerprint as described in Activate and deactivate fingerprints, on page 4.

# Host input data

You can augment the network map by importing network map data from third parties. You can also use the host input feature by modifying operating system or application identities or deleting application protocols, protocols, host attributes, or clients using the web interface.

The system may reconcile data from multiple sources to determine the current identity of an operating system or application.

All data except third-party vulnerabilities is discarded when the affected host is removed from the network map. For more information on setting up scripts or import files, see the *Firepower System Host Input API Guide*.

To include imported data in impact correlations, you must map the data to the operating system and application definitions in the database.

# Requirements for using third-party data

You can import discovery data from third-party systems on your network. However, to enable features where intrusion and discovery data are used together, such as Cisco recommendations, adaptive profile updates, or impact assessment, you should map as many elements of it as possible to corresponding definitions. Consider the following requirements for using third-party data:

- If you have a third-party system that has specific data on your network assets, you can import that data using the host input feature. However, because third parties may name the products differently, you must map the third-party vendor, product, and versions to the corresponding Cisco product definition. After you map the products, you must enable vulnerability mappings for impact assessment in the Firewall Management Center configuration to allow impact correlation. For versionless or vendorless application protocols, you need to map vulnerabilities for the application protocols in the Firewall Management Center configuration.
- If you import patch information from a third party and you want to mark all vulnerabilities fixed by that patch as invalid, you must map the third-party fix name to a fix definition in the database. All vulnerabilities addressed by the fix will then be removed from hosts where you add that fix.
- If you import operating system and application protocol vulnerabilities from a third party and you want to use them for impact correlation, you must map the third-party vulnerability identification string to vulnerabilities in the database. Note that although many clients have associated vulnerabilities, and clients are used for impact assessment, you cannot import and map third-party client vulnerabilities. After the vulnerabilities are mapped, you must enable third-party vulnerability mappings for impact assessment in the Firewall Management Center configuration. To cause application protocols without vendor or version information to map to vulnerabilities, an administrative user must also map vulnerabilities for the applications in the Firewall Management Center configuration.
- If you import application data and you want to use that data for impact correlation, you must map the vendor string for each application protocol to the corresponding Cisco application protocol definition.

# Third-party product mappings

When you add data from third parties to the network map through the user input feature, you must map the vendor, product, and version names used by the third party to the Cisco product definitions. Mapping the products to Cisco definitions assigns vulnerabilities based on those definitions.

Similarly, if you are importing patch information from a third party, such as a patch management product, you must map the name for the fix to the appropriate vendor and product and the corresponding fix in the database.

## Map third-party products

If you import data from a third party, you must map the Cisco product to the third-party name to assign vulnerabilities and perform impact correlation using that data. Mapping the product associates Cisco vulnerability information with the third-party product name, which allows the system to perform impact correlation using that data.

If you import data using the host input import feature, you can also use the AddScanResult function to map third-party products to operating system and application vulnerabilities during the import.

For example, if you import data from a third party that lists Apache Tomcat as an application and you know it is version 6 of that product, you could add a third-party map where:

- **Vendor Name** is set to `Apache`.
- **Product Name** is set to `Tomcat`.
- **Apache** is chosen from the **Vendor** drop-down list.
- **Tomcat** is chosen from the **Product** drop-down list.
- **6** is chosen from the **Version** drop-down list

This mapping would cause any vulnerabilities for Apache Tomcat 6 to be assigned to hosts with an application listing for Apache Tomcat.

Note that for versionless or vendorless applications, you must map vulnerabilities for the application types in the Secure Firewall Management Center configuration. Although many clients have associated vulnerabilities, and clients are used for impact assessment, you cannot import and map third-party client vulnerabilities.

**Tip** If you have already created a third-party mapping on another Secure Firewall Management Center, you can export it and then import it onto this Firewall Management Center. You can then edit the imported mapping to suit your needs.

Follow these steps to map third-party products:

**Procedure**

**Step 1** Choose **Policies** > **+ Show more** > **Advanced** > **Applications**.

**Step 2** Click **User Third-Party Mappings**. You have two choices:

- **Create**: To create a new map set, click **Create Product Map Set**.
- **Edit**: To edit an existing map set, click **Edit** (✎) next to the map set you want to modify. If **View** (👁) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

**Step 3** Enter a **Mapping Set Name**.

**Step 4** Enter a **Description**.

**Step 5** You have two choices:

- **Create**: To map a third-party product, click **Add Product Map**.
- **Edit**: To edit an existing third-party product map, **Edit** (✎) next to the map set you want to modify. If **View** (👁) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

**Step 6** Enter the **Vendor String**, **Product String**, and **Version String** used by the third-party product.

**Step 7** In the Product Mappings section, choose the operating system, product, and versions you want to use for vulnerability mapping from the **Vendor**, **Product**, **Major Version**, **Minor Version**, **Revision Version**, **Build**, **Patch**, and **Extension** fields.

**Example:**

If you want a host running a product whose name consists of third-party strings to use the vulnerabilities from Red Hat Linux 9, choose **Redhat, Inc.** as the vendor, **Redhat Linux** as the product, and **9** as the version.

**Step 8** Click **Save**.

## Map third-party product fixes

Mapping a fix name to a set of fixes in the database allows you to import data from a third-party patch management application and apply the fix to specified hosts. When the fix name is imported to a host, the system marks all vulnerabilities addressed by the fix as invalid for that host.

### Procedure

**Step 1** Choose **Policies** > **+ Show more** > **Advanced** > **Applications**.

**Step 2** Click **User Third-Party Mappings**. You have two choices:

- Create — To create a new map set, click **Create Product Map Set**.
- Edit — To edit an existing map set, click **Edit** (✎) next to the map set you want to modify. If **View** (👁) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

**Step 3** Enter a **Mapping Set Name**.

**Step 4** Enter a **Description**.

**Step 5** You have two choices:

- Create — To map a third-party product, click **Add Fix Map.**
- Edit — To edit an existing third-party product map, click **Edit** (✎) next to it. If **View** (👁) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

**Step 6** Enter the name of the fix you want to map in the **Third-Party Fix Name** field.

**Step 7** In the **Product Mappings** section, choose the operating system, product, and versions you want to use for fix mapping from these fields:

- **Vendor**
- **Product**
- **Major Version**
- **Minor Version**
- **Revision Version**
- **Build**
- **Patch**
- **Extension**

**Example:**

If you want your mapping to assign the fixes from Red Hat Linux 9 to hosts where the patch is applied, choose **Redhat, Inc.** as the vendor, **Redhat Linux** as the product, and **9** as the version.

**Step 8** Click **Save** to save the fix map.

# Map third-party vulnerabilities

To add vulnerability information from a third party to the VDB, you must map the third-party identification string for each imported vulnerability to any existing SVID, Bugtraq, or SID. After you create a mapping for the vulnerability, the mapping works for all vulnerabilities imported to hosts in the network map and allows impact correlation for those vulnerabilities.

You must enable impact correlation for third-party vulnerabilities to allow correlation to occur. For versionless or vendorless applications, you must also map vulnerabilities for the application types in the Secure Firewall Management Center configuration.

Although many clients have associated vulnerabilities, and clients are used for impact assessment, you cannot use third-party client vulnerabilities for impact assessment.

**Tip** If you have already created a third-party mapping on another Secure Firewall Management Center, you can export it and then import it onto this Firewall Management Center. You can then edit the imported mapping to suit your needs.

**Procedure**

**Step 1** Choose **Policies** > **+ Show more** > **Advanced** > **Applications**.

**Step 2** Click **User Third-Party Mappings**.

**Step 3** You have two choices:

- Create — To create a new vulnerability set, click **Create Vulnerability Map Set**.
- Edit — To edit an existing vulnerability set, click **Edit** ( ) next to the vulnerability set. If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

**Step 4** Click **Add Vulnerability Map**.

**Step 5** Enter the third-party identification for the vulnerability in the **Vulnerability ID** field.

**Step 6** Enter a **Vulnerability Description**.

**Step 7** Optionally:

- Enter a Snort ID in the **Snort Vulnerability ID Mappings** field.
- Enter a legacy vulnerability ID in the **SVID Mappings** field.
- Enter a Bugtraq identification number in the **Bugtraq Vulnerability ID Mappings** field.

**Step 8** Click **Add**.

# Custom product mappings

A custom product mapping is a network configuration feature that - ensures servers input by a third party are associated with the appropriate Cisco definitions - applies to all servers or clients on monitored hosts that

have the mapped vendor strings, and - enables mapping vulnerabilities for all servers in the network map with a particular vendor string instead of explicitly setting the vendor, product, and version for the server.

## Create custom product mappings

Custom product mappings allow you to manually create mappings when the system cannot automatically map a server to a vendor and product in the VDB. When you activate a custom product mapping, the system maps vulnerabilities for the specified vendor and product to all servers in the network map where that vendor string occurs.

**Note** Custom product mappings apply to all occurrences of an application protocol, regardless of the source of the application data (such as Nmap, the host input feature, or the system itself). However, if third-party vulnerability mappings for data imported using the host input feature conflicts with the mappings you set through a custom product mapping, the third-party vulnerability mapping overrides the custom product mapping and uses the third-party vulnerability mapping settings when the input occurs.

You create lists of product mappings and then enable or disable use of several mappings at once by activating or deactivating each list. When you specify a vendor to map to, the system updates the list of products to include only those made by that vendor.

After you create a custom product mapping, you must activate the custom product mapping list. After you activate a list of custom product mappings, the system updates all servers with occurrences of the specified vendor strings. For data imported through the host input feature, vulnerabilities update unless you have already explicitly set the product mappings for this server.

If, for example, your company modifies the banner for your Apache Tomcat web servers to read `Internal Web Server`, you can map the vendor string `Internal Web Server` to the vendor **Apache** and the product **Tomcat**, then activate the list containing that mapping, all hosts where a server labeled `Internal Web Server` occurs have the vulnerabilities for Apache Tomcat in the database.

**Tip** You can use this feature to map vulnerabilities to local intrusion rules by mapping the SID for the rule to another vulnerability.

### Procedure

**Step 1** Choose **Policies** > **+ Show more** > **Advanced** > **Applications**.

**Step 2** Click **Custom Product Mappings**, and then **Create Custom Product Mapping List**.

**Step 3** Enter a **Custom Product Mapping List Name**.

**Step 4** Click **Add Vendor String**.

**Step 5** In the **Vendor String** field, enter the vendor string that identifies the applications that should map to the chosen vendor and product values.

**Step 6** Choose the vendor you want to map to from the **Vendor** drop-down list. Choose the product you want to map to from the **Product** drop-down list.

**Step 7** Click **Add** to add the mapped vendor string to the list.

Optionally, repeat steps 4 to 8 as needed to add additional vendor string mappings to the list.

**Step 8** Click **Save**.

### What to do next

- Activate the custom product mapping list. For more information, see Activate and deactivate custom product mappings, on page 17.

## Edit custom product mapping lists

You can modify existing custom product mapping lists by adding or removing vendor strings or changing the list name.

### Procedure

**Step 1** Choose **Policies** > **+ Show more** > **Advanced** > **Applications**.

**Step 2** Click **Custom Product Mappings**.

**Step 3** Click **Edit** (✎) next to the product mapping list you want to edit.

If **View** (👁) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

**Step 4** Make changes to the list as described in Create custom product mappings, on page 16.

**Step 5** When you finish, click **Save**.

## Activate and deactivate custom product mappings

Activating custom product mappings allows you to enable or disable use of an entire list of custom product mappings at once, providing centralized control over application detection across your network.

After you activate a custom product mapping list, each mapping on that list applies to all applications with the specified vendor string, whether detected by managed devices or imported through the host input feature.

### Procedure

**Step 1** Choose **Policies** > **+ Show more** > **Advanced** > **Applications**.

**Step 2** Click **Custom Product Mappings**.

**Step 3** Click the slider next to the custom product mapping list to activate or deactivate it.

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

# Configure the host input client

The host input feature allows you to update the Firewall Management Center's network map from a client program running on another appliance. For example, you can add or delete hosts from the network map, or update the host OS and service information. For more information, see the *Firepower System Host Input API Guide*.

Before you can run a remote client, you must add the client to the Firewall Management Center's peers database from the Host Input Client page. You must also copy the authentication certificate generated by the Firewall Management Center to the client. After completing these steps the client can connect to the Firewall Management Center.

In a multidomain deployment, you can create a client in any domain. The authentication certificate allows the client to submit network map updates for any leaf domains associated with the client certificate's domain. If you create a certificate for an ancestor domain (or if your certificate domain later becomes an ancestor domain after adding descendant domains), any clients using that certificate must specify a target leaf domain with every transaction, as described in the *Firepower System Host Input API Guide*.

The Host Input Client shows only clients associated the current domain, so if you want to download or revoke a certificate, switch to the domain where the client was created.

This connection uses TLS 1.2.

**Before you begin**

Follow these steps to configure the host input client:

**Procedure**

**Step 1** Choose **Integrations** > **+ Show more** > **Host Input Client**

**Step 2** Click **Create Client**.

**Step 3** In the **Hostname** field, enter the host name or IP address of the host running the host input client.

**Note** If you have not configured DNS resolution, use an IP address.

**Step 4** If you want to encrypt the certificate file, enter a password in the **Password** field.

**Step 5** Click **Save**.
The host input service allows the host to access port 8307 on the Firewall Management Center and creates an authentication certificate to use during client-server authentication.

**Step 6** Click **Download** ( ) next to the certificate file.

**Step 7** Save the certificate file to the directory used by your client for SSL/TLS authentication.

**Step 8** To revoke access for a client, click **Delete** ( ) next to the host you want to remove.

# Nmap scanning

The system builds network maps through passive analysis of traffic on your network. Information obtained through this passive analysis can occasionally be incomplete, depending on system conditions. However, you can actively scan a host to obtain complete information.

If a host has a server running on an open port but the server has not received or sent traffic during the time that the system has been monitoring your network, the system does not add information about that server to the network map. If you scan the host using an active scanner, you can detect the server.

You can use Nmap, an open source active scanner, to explore your network and audit its security.

When you scan a host using Nmap, the system:

- Adds servers found on previously undetected open ports are added to the Servers list in the host profile. The host profile lists any servers detected on filtered or closed TCP ports or on UDP ports in the **Scan Results** section. By default, Nmap scans more than 1660 TCP ports.

  If the system recognizes a server identified in an Nmap scan and has a corresponding server definition, the system maps the names Nmap uses for servers to the corresponding Cisco server definitions.

- Compares the results of the scan to over 1500 known operating system fingerprints to determine the operating system and assigns scores to each. The operating system assigned to the host is the operating system fingerprint with the highest score.

  The system maps Nmap operating system names to Cisco operating system definitions.

- Vulnerabilities are assigned to the host for any added servers and operating systems.



**Note**

- A host must exist in the network map before Nmap can append its results to the host profile.
- If the host is deleted from the network map, any Nmap scan results for that host are discarded.



**Tip** Scanning options like port scans can put a heavy load on networks with low bandwidth. Run these scans when your network traffic is low.

For more information on the underlying Nmap technology used to scan, refer to the Nmap documentation at http://insecure.org/.

# Nmap remediation options

You define the settings for an Nmap scan by creating an Nmap remediation. An Nmap remediation can be used in a correlation policy, initiated on demand, or scheduled for a specific time.

**Note** Nmap-supplied server and operating system data remain static until you run another Nmap scan. If you plan to scan a host for operating system and server data using Nmap, schedule regular scans to keep Nmap-supplied data and server data up-to-date.

***Table 1: Nmap remediation options***

| Option | Description | Corresponding Nmap option |
|---|---|---|
| Scan which addresses from the event? | When you use an Nmap scan as a response to a correlation rule, select one of the following options to control which address in the event is scanned: that of the source host, the destination host, or both:<br>• **Scan Source and Destination Addresses** scans the hosts represented by the source IP address and the destination IP address in the event.<br>• **Scan Source Address Only** scans the host represented by the event's source IP address.<br>• **Scan Destination Address Only** scans the host represented by the event's destination IP address. | N/A |
| Scan types | Select how Nmap scans ports:<br>• The **TCP Syn** scan connects quickly to thousands of ports without using a complete TCP handshake. This option allows you to scan quickly in stealth mode on hosts where the `admin` account has raw packet access or where IPv6 is not running, by initiating TCP connections but not completing them. If a host acknowledges the Syn packet sent in a TCP Syn scan, Nmap resets the connection.<br>• The **TCP Connect** scan uses the `connect()` system call to open connections through the operating system on the host. You can use the TCP Connect scan if the `admin` user on the Firewall Management Center or managed device does not have raw packet privileges on a host or you are scanning IPv6 networks. In other words, use this option in situations where the TCP SYN scan cannot be used.<br>• The **TCP ACK** scan sends an ACK packet to check whether ports are filtered or unfiltered.<br>• The **TCP Window** scan works in the same way as a TCP ACK scan but can also determine whether a port is open or closed.<br>• The **TCP Maimon** scan identifies BSD-derived systems using a FIN/ACK probe. | **TCP Syn**: `-sS`<br>**TCP Connect**: `-sT`<br>**TCP ACK**: `-sA`<br>**TCP Window**: `-sW`<br>**TCP Maimon**: `-sM` |
| Scan for UDP ports | Enable this option to scan UDP ports as well as TCP ports. Scanning UDP ports may be time consuming, so avoid using this option if you want to scan quickly. | `-sU` |

| Option | Description | Corresponding Nmap option |
|---|---|---|
| Use port from event | If you plan to use the remediation as a response in a correlation policy, enable to cause the remediation to scan only the port specified in the event that triggers the correlation response.<br>• Select **On** to scan the port in the correlation event, rather than the ports you specify during Nmap remediation configuration. If you scan the port in the correlation event, note that the remediation scans the port on the IP addresses that you specify during Nmap remediation configuration. These ports are also added to the remediation's dynamic scan target.<br>• Select **Off** to scan only the ports you specify Nmap remediation configuration.<br>You can also control whether Nmap collects information about operating system and server information. Enable the **Use Port From Event** option to scan the port associated with the new server. | N/A |
| Scan from reporting detection engine | Enable this option to scan a host from the appliance where the detection engine that reported the host resides.<br>• To scan from the appliance running the reporting detection engine, select **On**.<br>• To scan from the appliance configured in the remediation, select **Off**. | N/A |
| Fast port scan | Enable this option to scan only the TCP ports listed in the `nmap-services` file located in the `/var/sf/nmap/share/nmap/nmap-services` directory on the device that does the scanning, ignoring other port settings. You cannot use this option with the **Port Ranges and Scan Order** option.<br>• To scan only the ports listed in the `nmap-services` file located in the `/var/sf/nmap/share/nmap/nmap-services` directory on the device that does the scanning, ignoring other port settings, select **On**.<br>• To scan all TCP ports, select **Off**. | `-F` |
| Port ranges and scan order | Set the specific ports you want to scan and the order in which you want to scan them using Nmap port specification syntax. Note that you cannot use this option with the **Fast Port Scan** option. | `-p` |
| Probe open ports for vendor and version information | Enable to detect server vendor and version information. If you probe open ports for server vendor and version information, Nmap obtains server data that it uses to identify servers. Nmap then replaces the Cisco server data for that server.<br>• Select **On** to scan open ports on the host for server information to identify server vendors and versions.<br>• Select **Off** to continue using Cisco server information for the host. | `-sV` |

| Option | Description | Corresponding Nmap option |
|---|---|---|
| Service version intensity | Select the intensity of Nmap probes for service versions.<br>• To use more probes for higher accuracy with a longer scan, select a higher number.<br>• To use fewer probes for less accuracy with a faster scan, select a lower number. | `--version-intensity` <intensity> |
| Detect operating system | Enable to detect operating system information for the host.<br>If you configure detection of the operating system for a host, Nmap scans the host and uses the results to create a rating for each operating system that reflects the likelihood that the operating system is running on the host.<br>• Select **On** to scan the host for information to identify the operating system.<br>• Select **Off** to continue using Cisco operating system information for the host. | `-O` |
| Treat all hosts as online | Enable to skip the host discovery process and run a port scan on every host in the target range. Note that when you enable this option, Nmap ignores settings for **Host Discovery Method** and **Host Discovery Port List**.<br>• To skip the host discovery process and run a port scan on every host in the target range, select **On**.<br>• To perform host discovery using the settings for **Host Discovery Method** and **Host Discovery Port List** and skip the port scan on any host that is not available, select **Off**. | `-PN` |
| Host discovery method | Select to perform host discovery for all hosts in the target range, over the ports listed in the **Host Discovery Port List**, or if no ports are listed, over the default ports for that host discovery method.<br>Note that if you also enabled **Treat All Hosts As Online**, however, the **Host Discovery Method** option has no effect and host discovery is not performed.<br>Select the method to be used when Nmap tests to see if a host is present and available:<br>• The **TCP SYN** option sends an empty TCP packet with the SYN flag set and recognizes the host as available if a response is received. TCP SYN scans port 80 by default. Note that TCP SYN scans are less likely to be blocked by a firewall with stateful firewall rules.<br>• The **TCP ACK** option sends an empty TCP packet with the ACK flag set and recognizes the host as available if a response is received. TCP ACK also scans port 80 by default. Note that TCP ACK scans are less likely to be blocked by a firewall with stateless firewall rules.<br>• The **UDP** option sends a UDP packet and assumes host availability if a port unreachable response comes back from a closed port. UDP scans port 40125 by default. | **TCP SYN**: `-PS`<br>**TCP ACK**: `-PA`<br>**UDP**: `-PU` |

| Option | Description | Corresponding Nmap option |
|---|---|---|
| Host discovery port list | Specify a customized list of ports, separated by commas, that you want to scan when doing host discovery. | port list for host discovery method |
| Default NSE scripts | Enable to run the default set of Nmap scripts for host discovery and server and operating system and vulnerability detection. or a list of default scripts, refer to https://nmap.org/nsedoc/categories/default.html.<br>• To run the default set of Nmap scripts, select **On**.<br>• To skip the default set of Nmap scripts, select **Off**. | `-sC` |
| Timing template | Select the timing of the scan process; the higher the number you select, the faster and less comprehensive the scan. | **0**: `T0` (paranoid)<br>**1**: `T1` (sneaky)<br>**2**: `T2` (polite)<br>**3**: `T3` (normal)<br>**4**: `T4` (aggressive)<br>**5**: `T5` (insane) |

# Nmap scanning guidelines

While active scanning can obtain valuable information, overuse of a tool such as Nmap may overload your network resources or even crash important hosts. When you use any active scanner, create a scanning strategy to scan only the hosts and ports you need.

## Selecting appropriate scan targets

When you configure Nmap, you can create scan targets that identify which hosts you want to scan. A scan target includes a single IP address, a CIDR block, an octet range of IP addresses, an IP address range, or a list of IP addresses or ranges to scan. You can also select the ports on the host or hosts.

You can specify targets in various ways:

- For IPv6 hosts: An exact IP address (for example, `2001:DB8:1::178:ABCD`).
- For IPv4 hosts:
  - An exact IP address (for example, `192.168.x.x`) or a list of IP addresses separated by commas or spaces.
  - An IP address block using CIDR notation (for example, `192.168.1.0/24` scans the 254 hosts between 192.168.x.x and 192.168.x.x, inclusive).
  - An IP address range using octet range addressing (for example, `198.51.0-255.1-254` scans all addresses in the 198.51.x.x range, except those that end in .0 and or .255).
  - An IP address range using hyphenation (for example, `192.168.x.x-192.168.x.x` scans the six hosts between 192.168.x.x and 192.168.x.x, inclusive).

- A list of addresses or ranges separated by commas or spaces (for example, `192.168.1.0/24, 194.168.1.0/24` scans the 254 hosts between 192.168.x.x and 192.168.x.x, inclusive and the 254 hosts between 194.168.x.x and 194.168.x.x, inclusive).

Ideal scan targets for Nmap scans include hosts with operating systems that the system is unable to identify, hosts with unidentified servers, or hosts recently detected on your network. Remember that Nmap results cannot be added to the network map for hosts that do not already exist in the network map.

**Caution**

- Nmap-supplied server and operating system data remains static until you run another Nmap scan. If you plan to scan a host using Nmap, regularly schedule scans.
- If a host is deleted from the network map, any Nmap scan results are discarded.
- Make sure you have permission to scan your targets. Scanning Nmap hosts not owned by you or your company may be illegal.

### Selecting appropriate ports to scan

For each scan target you configure, you can select the ports you want to scan. You can designate individual port numbers, port ranges, or a series of port numbers and port ranges to identify the exact set of ports that should be scanned on each target.

By default, Nmap scans TCP ports 1 through 1024. If you plan to use the remediation as a response in a correlation policy, you can configure the remediation to scan only the port specified in the event that triggers the correlation response. If you run remediation on demand, or as a scheduled task, or if you do not use the port from the event, you can use other port options to determine which ports are scanned. You can choose to scan only the TCP ports listed in the `nmap-services` file, ignoring other port settings. You can also scan UDP ports in addition to TCP ports. Scanning for UDP ports may take longer. Use this option only if you do not require a quick scan. To select the specific ports or range of ports to scan, use Nmap port specification syntax to identify ports.

### Setting host discovery options

You can decide whether to perform host discovery before starting a port scan for a host, or you can assume that all the hosts you plan to scan are online. If you choose not to treat all hosts as online, you can choose what method of host discovery to use and, if needed, customize the list of ports scanned during host discovery. Host discovery does not probe the ports listed for operating system or server information; it uses the response over a particular port only to determine whether a host is active and available. If you perform host discovery and a host is not available, Nmap does not scan ports on that host.

## Example: Use Nmap to resolve unknown operating systems

This example walks through an Nmap configuration designed to resolve unknown operating systems. For a complete look at Nmap configuration, see Manage Nmap scanning, on page 26.

If the system cannot determine the operating system on a host on your network, you can use Nmap to actively scan the host. Nmap uses the information it obtains from the scan to rate the possible operating systems. It then uses the operating system that has the highest rating as the host operating system identification.

Using Nmap to challenge new hosts for operating system and server information deactivates the system's monitoring of that data for scanned hosts. If you use Nmap to discover the host and server operating system

for hosts marked as unknown by the systems, you may identify groups of similar hosts. You can then create a custom fingerprint using one of these hosts to associate the fingerprint with the operating system you identified through Nmap scan. Whenever possible, create a custom fingerprint rather than inputting static data through a third-party source like Nmap because the custom fingerprint allows the system to continue to monitor the host operating system and update it as needed.

### Procedure

**Step 1** Configure a scan instance as described in Add an Nmap scan instance, on page 27.

**Step 2** Create an Nmap remediation using the following settings:

- Enable **Use Port From Event** to scan the port associated with the new server.
- Enable **Detect Operating System** to detect operating system information for the host.
- Enable **Probe open ports for vendor and version information** to detect server vendor and version information.
- Enable **Treat All Hosts as Online**, because you know the host exists.

**Step 3** Create a correlation rule that triggers when the system detects a host with an unknown operating system.

The rule should trigger when **a discovery event occurs** and **the OS information for a host has changed** and it meets the following conditions: **OS Name is unknown**.

**Step 4** Create a correlation policy that contains the correlation rule.

**Step 5** In the correlation policy, add the Nmap remediation you created in step 2 as a response to the rule you created in step 3.

**Step 6** Activate the correlation policy.

**Step 7** Purge the hosts on the network map to force network discovery to restart and rebuild the network map.

**Step 8** After a day or two, search for events generated by the correlation policy.

Analyze the Nmap results for the operating systems detected on the hosts to see if there is a particular host configuration on your network that the system does not recognize.

**Step 9** If you find hosts with unknown operating systems whose Nmap results are identical, create a custom fingerprint for one of those hosts and use it to identify similar hosts in the future.

## Example: Using Nmap to respond to new hosts

This example walks through an Nmap configuration designed to respond to new hosts. For a complete look at Nmap configuration, see Manage Nmap scanning, on page 26.

When the system detects a new host in a subnet where intrusions may be likely, you may want to scan that host to make sure you have accurate vulnerability information for it.

You can accomplish this by creating and activating a correlation policy that detects when a new host appears in this subnet, and that launches a remediation that performs an Nmap scan on the host.

**Procedure**

**Step 1** Configure a scan instance as described in Add an Nmap scan instance, on page 27.

**Step 2** Create an Nmap remediation using the following settings:

- Enable **Use Port From Event** to scan the port associated with the new server.
- Enable **Detect Operating System** to detect operating system information for the host.
- Enable **Probe open ports for vendor and version information** to detect server vendor and version information.
- Enable **Treat All Hosts as Online**, because you know the host exists.

**Step 3** Create a correlation rule that triggers when the system detects a new host on a specific subnet.

The rule should trigger when **a discovery event occurs** and **a new host is detected**.

**Step 4** Create a correlation policy that contains the correlation rule.

**Step 5** In the correlation policy, add the Nmap remediation you created in step 2 as a response to the rule you created in step 3.

**Step 6** Activate the correlation policy.

**Step 7** When you are notified of a new host, check the host profile to see the results of the Nmap scan and address any vulnerabilities that apply to the host.

After you activate the policy, you can periodically check the remediation status view (**Events & Logs** > **+ Show more** > **Correlation** > **Status**) to see when the remediation launched. The remediation's dynamic scan target should include the IP addresses of the hosts it scanned as a result of the server detection. Check the host profile for those hosts to see if there are vulnerabilities that need to be addressed for the host, based on the operating system and servers detected by Nmap.



**Caution** If you have a large or dynamic network, detection of a new host may be too frequent an occurrence to respond to using a scan. To prevent resource overload, avoid using Nmap scans as a response to events that occur frequently. In addition, note that using Nmap to challenge new hosts for operating system and server information deactivates Cisco monitoring of that data for scanned hosts.

# Manage Nmap scanning

To use Nmap scanning, you must, at minimum, configure an Nmap scan instance and an Nmap remediation. Configuring an Nmap scan target is optional.

**Procedure**

**Step 1** Configure the Nmap scan:

- Add an Nmap scan instance as described in Add an Nmap scan instance, on page 27.
- Create an Nmap remediation as described in Create an Nmap remediation, on page 30.
- Optionally, add an Nmap scan target as described in Add an Nmap scan target, on page 29.

**Step 2** Run the Nmap scan:

- Run an on-demand Nmap scan as described in Run an on-demand Nmap scan, on page 33.
- Configure automatic Nmap scans as described in *Nmap Scan Automation* in the *Cisco Secure Firewall Management Center Administration Guide*.
- Schedule automatic Nmap scans as described in *Scheduling an Nmap Scan* in the *Cisco Secure Firewall Management Center Administration Guide*.

### What to do next

- Monitor the Nmap scan in progress by viewing the related task; see *Viewing Task Messages* in the *Cisco Secure Firewall Management Center Administration Guide*.
- Optionally, refine the scan:
  - Edit an Nmap scan instance as described in Edit an Nmap scan instance, on page 28.
  - Edit an Nmap scan target as described in Edit an Nmap scan target, on page 30.
  - Edit an Nmap remediation as described in Edit an Nmap remediation, on page 32.

## Add an Nmap scan instance

You can set up a separate scan instance for each Nmap module that you want to use to scan your network for vulnerabilities. You can set up scan instances for the local Nmap module on the Secure Firewall Management Center and for any devices you want to use to run scans remotely. The results of each scan are always stored on the Firewall Management Center where you configure the scan, even if you run the scan from a remote device. To prevent accidental or malicious scanning of mission-critical hosts, you can create a blacklist for the instance to indicate the hosts that should never be scanned with the instance.

You cannot add a scan instance with the same name as any existing scan instance.

### Procedure

**Step 1** Access the list of Nmap scan instances using either of the following methods:

- Choose **Policies** > **+ Show more** > **Correlation** > **Instances**.
- Choose **Policies** > **+ Show more** > **Correlation** > **Scanners**.

**Step 2** Add the remediation:

- If you accessed the list via the first method above, locate the Add a New Instance section, choose the Nmap Remediation module from the drop-down list, and click **Add**.
- If you accessed the list via the second method above, click **Add Nmap Instance**.

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

**Step 4** Enter a **Description**.

**Step 5** Optionally, in the **Exempted hosts** field, specify any hosts or networks that should *never* be scanned with this scan instance, using the following syntax:

- For IPv6 hosts, an exact IP address (for example, `2001:DB8::fedd:eeff`)
- For IPv4 hosts, an exact IP address (for example, `192.168.1.101`) or an IP address block using CIDR notation (for example, `192.168.1.0/24` scans the 254 hosts between `192.168.1.1` and `192.168.1.254`, inclusive)
- Note that you cannot use an exclamation mark (!) to negate an address value.

**Note** If you specifically target a scan to a host that is in a blacklisted network, that scan will not run.

**Step 6** Optionally, to run the scan from a remote device instead of the Firewall Management Center, specify the IP address or name of the device as it appears in the Information page for the device in the Firewall Management Center web interface, in the **Remote Device Name** field.

**Step 7** Click **Create**.
When the system is done creating the instance, it displays it in edit mode.

**Step 8** Optionally, add an Nmap remediation to the instance. To do so, locate the Configured Remediations section of the instance, click **Add**, and create a remediation as described in Create an Nmap remediation, on page 30.

**Step 9** Click **Cancel** to return to the list of instances.

**Note** If you accessed the list of Nmap scan instances via the **Scanners** option, the system does not display the instance you added unless you also added a remediation to the instance. To view any instances to which you have not yet added remedations, use the **Instances** menu option to access the list.

## Edit an Nmap scan instance

When you edit a scan instance, you can view, add, and delete remediations associated with the instance. If you no longer need the Nmap module in this scan instance, delete the Nmap scan instance. When you delete a scan instance, you also remove any remediations that use this instance.

### Procedure

**Step 1** To access the list of Nmap scan instances, use one of these methods:

- Choose **Policies** > **+ Show more** > **Correlation** > **Instances**.
- Choose **Policies** > **+ Show more** > **Correlation** > **Scanners**.

**Step 2** Click **View** ( ) next to the instance you want to edit.

**Step 3** Make changes to the scan instance settings as described in Add an Nmap scan instance, on page 27.

**Step 4** Click **Save**.

**Step 5** Click **Done**.

### What to do next

- To add a new remediation to the scan instance; refer to Create an Nmap remediation, on page 30.
- To edit a remediation associated with the instance; refer to Edit an Nmap remediation, on page 32.
- To delete a remediation associated with the instance; refer to Run an on-demand Nmap scan, on page 33.
- You can delete the scan instance by clicking **Delete** ( ) next to it.

## Add an Nmap scan target

Create and save scan targets that identify the hosts and ports you want to target when you perform an on-demand or a scheduled scan, so that you do not have to construct a new scan target every time.

A scan target includes a single IP address or a block of IP addresses. It also specifies the ports on the host or hosts. For Nmap targets, you can also use Nmap octet range addressing or IP address ranges. For more information on Nmap octet range addressing, see the Nmap documentation at https://insecure.org/.

**Note**

- Scans for targets containing a large number of hosts can take a long time. As a workaround, scan fewer hosts at a time.
- Nmap-supplied server and operating system data remains static until you run another Nmap scan. If you plan to scan a host using Nmap, regularly schedule scans. If a host is deleted from the network map, any Nmap scan results are discarded.

### Procedure

**Step 1** Choose **Policies** > **+ Show more** > **Correlation** > **Scanners**.

**Step 2** On the toolbar, click **Targets**.

**Step 3** Click **Create Scan Target**.

**Step 4** In the **Name** field, enter the name you want to use for this scan target.

**Step 5** In the **IP Range** text box, specify the host or hosts you want to scan using the syntax described in Nmap scanning guidelines, on page 23.

**Note** If you use a comma in a list of IP addresses or ranges in a scan target, the comma converts to a space when you save the target.

**Step 6** In the **Ports** field, specify the ports you want to scan.

You can enter any of these values from 1 to 65535:

- A port number.
- A list of ports separated by commas.
- A range of port numbers separated by a dash.
- Range of port numbers separated by dashes, and commas.

**Step 7** Click **Save**.

## Edit an Nmap scan target

Edit a remediation's dynamic scan target to exclude a specific IP address, but the IP address was added to the target because the host was involved in a correlation policy violation that launched the remediation.

Delete a scan target if you no longer want to scan the hosts listed in it.

### Procedure

**Step 1** Choose **Policies** > **+ Show more** > **Correlation** > **Scanners**.

**Step 2** On the toolbar, click **Targets**.

**Step 3** Click **Edit** (✎) next to the scan target you want to edit.

If **View** (👁) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

**Step 4** Make modifications as necessary. For more information, see Add an Nmap scan target, on page 29.

**Step 5** Click **Save**.

**Step 6** Delete the scan target by clicking **Delete** (🗑) next to it.

## Create an Nmap remediation

An Nmap remediation can only be created by adding it to an existing Nmap scan instance. You can use the remediation as a response in a correlation policy, run it on demand, or schedule it to run at a specific time.

Nmap-supplied server and operating system data remains static until another Nmap scan is run. To keep data updated, regularly schedule scans if you plan to scan a host using Nmap. If a host is deleted from the network map, any existing Nmap scan results are discarded.

For general information about Nmap functionality, refer to the Nmap documentation at https://insecure.org.

**Before you begin**

Add an Nmap scan instanceas described in Add an Nmap scan instance, on page 27 .

### Procedure

**Step 1** Choose **Policies** > **+ Show more** > **Correlation** > **Instances**.

**Step 2** Click **View** ( ) next to the instance to which you want to add the remediation.

**Step 3** In the Configured Remediations section, click **Add**.

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

**Step 5** Enter a **Description**.

**Step 6** If you plan to use this remediation in response to a correlation rule that triggers on an intrusion event, a connection event, or a user event, configure the **Scan Which Address(es) From Event?** option.

**Tip** If you plan to use this remediation in response to a correlation rule that triggers on a discovery event or a host input event, by default the remediation scans the IP address of the host involved in the event; you do not need to configure this option.

**Note** Do **not** assign an Nmap remediation as a response to a correlation rule that triggers on a traffic profile change.

**Step 7** Configure the **Scan Type** option.

**Step 8** To scan UDP ports in addition to TCP ports, choose **On** for the **Scan for UDP ports** option.

**Tip** A UDP portscan takes more time than a TCP portscan. To speed up your scans, leave this option disabled.

**Step 9** If you plan to use this remediation in response to correlation policy violations, configure the **Use Port From Event** option.

**Step 10** If you plan to use this remediation in response to correlation policy violations and want to run the scan using the appliance running the detection engine that detected the event, configure the **Scan from reporting detection engine** option.

**Step 11** Configure the **Fast Port Scan** option.

**Step 12** In the **Port Ranges and Scan Order** field, enter the ports you want to scan by default, using Nmap port specification syntax, in the order you want to scan those ports.

Use this format:

- Specify values from 1 to 65535.
- Separate ports using commas or spaces.
- Use a hyphen to indicate a port range.
- When scanning for both TCP and UDP ports, preface the list of TCP ports you want to scan with a T and the list of UDP ports with a U.

**Note** The **Use Port From Event** option overrides this setting when the remediation is launched in response to a correlation policy violation, as described in step 8.

**Example:**

To scan ports 53 and 111 for UDP traffic, then scan ports 21-25 for TCP traffic, enter **U:53,111,T:21-25**.

**Step 13** To probe open ports for server vendor and version information, configure **Probe open ports for vendor and version information**.

**Step 14** If you choose to probe open ports, set the number of probes used by choosing a number from the **Service Version Intensity** drop-down list.

**Step 15** To scan for operating system information, configure **Detect Operating System** settings.

**Step 16** To determine whether host discovery occurs and whether port scans are only run against available hosts, configure **Treat All Hosts As Online**.

**Step 17** To set the method you want Nmap to use when it tests for host availability, choose a method from the **Host Discovery Method** drop-down list.

**Step 18** If you want to scan a custom list of ports during host discovery, enter a list of ports appropriate for the host discovery method you chose, separated by commas, in the **Host Discovery Port List** field.

**Step 19** Configure the **Default NSE Scripts** option to control whether to use the default set of Nmap scripts for host discovery and server, operating system, and vulnerability discovery.

**Tip** See https://nmap.org/nsedoc/categories/default.html for the list of default scripts.

**Step 20** To set the timing of the scan process, choose a timing template number from the **Timing Template** drop-down list.

Choose a higher number for a faster, less comprehensive scan and a lower number for a slower, more comprehensive scan.

**Step 21** Click **Create**.
When the system is done creating the remediation, it displays it in edit mode.

**Step 22** Click **Done** to return to the related instance.

**Step 23** Click **Cancel** to return to the instance list.

## Edit an Nmap remediation

Edit an Nmap remediation to modify scan settings or remove it when it is no longer required.

Modifications you make to Nmap remediations do not affect scans in progress. The new settings take effect when the next scan starts. Delete an Nmap remediation if you no longer need it.

### Procedure

**Step 1** Access the list of Nmap scan instances using one of these methods:

- Choose **Policies** > **+ Show more** > **Correlation** > **Instances**.
- Choose **Policies** > **+ Show more** > **Correlation** > **Scanners**.

**Step 2** Access the remediation you want to edit by performing one of these actions:

- If you accessed the list via the first method above, click **View** ( ) next to the relevant instance, and then click it again next to the remediation you want to edit in the Configured Remediations section.
- If you accessed the list via the second method above, click **View** ( ) next to the remediation you want to edit.

**Step 3** Make any necessary modifications as described in Create an Nmap remediation, on page 30.

**Step 4** Click **Save** if you want to save your changes, or click **Done** to exit without saving.

**Step 5** Delete the remediation by clicking **Delete** ( ) next to it.

# Run an on-demand Nmap scan

You can launch on-demand Nmap scans whenever needed. You can specify the target for an on-demand scan by entering the IP addresses and ports you want to scan or by choosing an existing scan target.

Nmap-supplied server and operating system data remains static until you run another Nmap scan. If you plan to scan a host using Nmap, regularly schedule scans. If a host is deleted from the network map, any Nmap scan results are discarded.

**Before you begin**

Optionally, add an Nmap scan target; for more information, refer to Add an Nmap scan target, on page 29 section.

**Procedure**

**Step 1** Choose **Policies** > **+ Show more** > **Correlation** > **Scanners**.

**Step 2** Next to the Nmap remediation you want to use to perform the scan, click **Scan** ( ).

**Step 3** To scan using a saved scan target, choose a target from the **Saved Targets** drop-down list, and click **Load**.

**Step 4** In the **IP Range(s)** field, specify the IP address for hosts you want to scan or modify the loaded list.

**Note**

- For hosts with IPv4 addresses, you can specify multiple IP addresses separated by commas or use CIDR notation. You can also negate IP addresses by preceding them with an exclamation point (!).
- For hosts with IPv6 addresses, use an exact IP address. Ranges are not supported.

**Step 5** In the **Ports** field, specify the ports you want to scan or modify the loaded list.

You can enter a port number, a list of ports separated by commas, or a range of port numbers separated by a dash.

**Step 6** Click **Scan Now**.

### What to do next

- Monitor the task status; see *Viewing Task Messages* in the *Cisco Secure Firewall Management Center Administration Guide*.

# Nmap scan results

You can manage, monitor, and analyze Nmap scan data to gain insights into your network configuration.

### Nmap scan result viewing options

You can monitor Nmap scans in progress. You can import results from scans previously performed through the system, or import results performed outside the system. You can also view and analyze scan results.

You can view scan results that you create using the local Nmap module as a rendered page in a pop-up window. You can also download the Nmap results file in raw XML format.

You can also view operating system and server information detected by Nmap in host profiles and in the network map. If a scan of a host produces server information for servers on filtered or closed ports, or if a scan collects information that cannot be included in the operating system information or the servers section, the host profile includes those results in an Nmap Scan Results section.

## View Nmap scan results

You can view the scan results in tabular format after the Nmap scan is completed and use the results view to find specific information.

When an Nmap scan is complete, you can view a table of scan results.

You can customize the results view depending on the information you are looking for. The page you see when you access scan results differs, based on the workflow. The predefined workflow includes a table view of scan results. You can also create a custom workflow that displays only the information that matches your specific needs.

You can download and view the Nmap results using the Nmap Version 1.01 DTD, available at http://insecure.org.

You can also clear scan results.

### Procedure

**Step 1** Choose **Policies** > **+ Show more** > **Correlation** > **Scanners**.

**Step 2** On the toolbar, click **Scan Results**.

**Step 3** You have the following choices:

- Adjust the time range as described in *Event Time Constraints* in the *Cisco Secure Firewall Management Center Administration Guide*.

- To use a different workflow, including a custom workflow, click **(switch workflows)** by the workflow title.
- To view the scan results as a rendered page in a pop-up window, click **View** next to the scan job.
- To save a copy of the scan results file so that you can view the raw XML code in any text editor, click **Download** next to the scan job.
- To sort scan results, click the column title. Click the column title again to reverse the sort order.
- To constrain the columns that appear, click **Close** (✕) in the column heading that you want to hide. In the pop-up window that appears, click **Apply**.

**Tip** To hide or show other columns, check or clear the appropriate check boxes before you click **Apply**. To add a disabled column back to the view, Click the expand arrow to expand the search constraints, then click the column name under **Disabled Columns**.

- To drill down to the next page in the workflow, see *Using Drill-Down Pages* in the *Cisco Secure Firewall Management Center Administration Guide*.
- To configure scan instances and remediations, click **Scanners** in the toolbar and see Manage Nmap scanning, on page 26.
- To navigate within and between workflow pages, see *Workflow Page Navigation Tools* in the *Cisco Secure Firewall Management Center Administration Guide*.
- To navigate to other event views to view associated events, choose the name of the event view you want to see from the **Jump to** drop-down list.
- To search for scan results, enter your search criteria in the appropriate fields.

## Nmap scan results fields

When you run an Nmap scan, the Firewall Management Center collects the scan results in a database. The following table describes the fields in the scan results table that can be viewed and searched.

***Table 2: Scan results fields***

| Field | Description |
|---|---|
| Start Time | The date and time that the scan that produced the results started. |
| End Time | The date and time that the scan that produced the results ended. |
| Target | The IP address (or host name, if DNS resolution is enabled) of the scan target for the scan that produced the results. |
| Scan Type | Either `Nmap` or the name of the third-party scanner to indicate the type of the scan that produced the results. |

| Field | Description |
|---|---|
| Scan Mode | The mode of the scan that produced the results:<br>• `On Demand`: results from scans run on demand.<br>• `Imported`: results from scans on a different system and imported onto the Firewall Management Center.<br>• `Scheduled`: results from scans run as a scheduled task. |
| Results | The results of the scan. |
| Domain | The domain of the scan target. This field is only present in a multidomain deployment. |

## Import Nmap scan results

You can import XML results files created by an Nmap scan performed outside of the system. You can also import XML results files that you previously downloaded from the system. To import Nmap scan results, the results file must be in XML format and adhere to the Nmap Version 1.01 DTD. For more information on creating Nmap results and on the Nmap DTD, refer to the Nmap documentation at https://insecure.org.

A host must already exist in the network map before Nmap can append its results to the host profile.

### Procedure

**Step 1** Choose **Policies** > **+ Show more** > **Correlation** > **Scanners**.

**Step 2** On the toolbar, click **Import Results**.

**Step 3** Click **Browse** to navigate to the results file.

**Step 4** After you return to the Import Results page, click **Import** to import the results.

# History for host identity sources

This reference provides the version history for Host Identity Sources features, including security improvements and version compatibility information.

| Feature | Minimum Firewall Management Center | Minimum Firewall Threat Defense | Details |
|---|---|---|---|
| Security improvement to the host input data feature | 6.5 | Any | TLS 1.2 is now used for communication between your Firewall Management Center and the host input client. The topic Configure the host input client, on page 18has been updated with this information. |