

# Host Profiles

The following topics describe how to use host profiles:


- Requirements and prerequisites for host profiles, on page 1
- Host profiles, on page 2
- Basic host information in the host profile, on page 4
- Operating systems in the host profile, on page 6
- Servers in the host profile, on page 10
- Web applications in the host profile, on page 14
- Host protocols in the host profile, on page 16
- Indications of compromise in the host profile, on page 16
- VLAN tags in the host profile, on page 17
- User history in host profiles, on page 17
- Host attributes in the host profile, on page 18
- Allow list violations in the host profile, on page 22
- Malware detections in the host profile, on page 23
- Vulnerabilities in the host profile, on page 24
- Scan results in the host profile, on page 26
- History for host profiles, on page 27


# Requirements and prerequisites for host profiles

This reference provides the requirements and prerequisites necessary for configuring and managing host profiles in the system.

### Model support

Any.

### Supported domains

Any

### User roles

- Administrator

- Security Analyst

# Host profiles

A host profile is a system view that provides a complete view of all the information the system has gathered about a single host.

### Host profile access and information

To access a host profile:

- navigate from any network map view.
- navigate from any event view that includes the IP addresses of hosts on monitored networks.

Host profiles provide basic information about detected hosts or devices, such as the host name or MAC addresses. Depending on your licenses and system configuration, host profiles can also provide you with this information:

Device and application insights

- the operating system running on a host
- the servers running on a host
- the clients and web applications running on a host
- the protocols running on a host

Security and network insights

- the indications of compromise (IOC) tags on a host
- the VLAN tags on a host
- the last twenty-four hours of user activity on your network
- the compliance allow violations associated with a host
- the most recent malware events for a host
- the vulnerabilities associated with a host
- the Nmap scan results for a host

*Host attributes* are also listed in the profile. You can use host attributes to classify hosts in ways that are important to your network environment. For example, you can:

- assign a host attribute that indicates the building where the host is located
- use the *host criticality* attribute to designate the business criticality of a given host and tailor correlation policies and alerts based on host criticality

From a host profile, you can view the existing host attributes applied to that host and modify the host attribute values.

If you use adaptive profile updates as part of a passive intrusion prevention deployment, you can tailor the way the system processes traffic so it best fits the type of operating system on the host and the servers and clients the host is running.

Optionally, you can perform an Nmap scan from the host profile to augment the server and operating system information in your host profile. The Nmap scanner actively probes the host to obtain information about the operating system and servers running on the host. The results of the scan are added to the list of operating system and server identities for the host.

# Host profile limitations

This reference describes limitations that may affect host profile availability and the completeness of information displayed in host profiles. Understanding these limitations helps explain why some hosts may not have profiles or why information may vary between different host types.

**Unavailable Hosts**

A host profile may not be available for every host on your network. Possible reasons include:

- The host was deleted from the network map because it timed out.
- You have reached your host limit.
- The host resides in a network segment that is not monitored by the network discovery policy.

**Unavailable Information**

The information displayed in a host profile may vary according to the type of host and the information available about the host.

For example:

- If your system detects a host using a non-IP-based protocol like STP, SNAP, or IPX, the host is added to the network map as a MAC host and much less information is available than for an IP host.
- The system can add hosts to the network map from exported NetFlow records, but the available information for these hosts is limited; see Differences between NetFlow and managed device data.

**(Deployments Running VRF) A Single IP Address May Represent Multiple Hosts**

If a host was reported by a device running VRF, a single IP address may actually represent multiple hosts. VRF can monitor multiple networks that have overlapping IP addresses, so the same IP address can exist on different networks.

# View host profiles

Host profiles provide detailed information about devices and their status on your network. Accessing this information helps identify compromised hosts and assess network security events.

### Procedure

You have two choices:

- On any network map, drill down to the IP address of the host whose profile you want to view.

- On any event view, click **Host Profile** or **Compromised Host** next to the IP address of the host whose profile you want to view.

# Basic host information in the host profile

Each host profile provides basic information about a detected host or other device. Descriptions of each of the basic host profile fields follow.

### Domain

The domain associated with the host.

### IP addresses

All IP addresses (both IPv4 and IPv6) associated with the host. The system detects IP addresses associated with hosts and, where supported, groups multiple IP addresses used by the same host. IPv6 hosts often have at least two IPv6 addresses (local-only and globally routable), and may also have IPv4 addresses. IPv4-only hosts may have multiple IPv4 addresses.

The host profile lists all detected IP addresses associated with that host. Where available, routable host IP addresses also include a flag icon and country code indicating the geolocation data associated with that address.

Note that only the first three addresses are shown by default. Click **show all** to show all addresses for a host.

### Hostname

The fully qualified domain name of the host, if known.

### NetBIOS name

The NetBIOS name of the host, if available. Microsoft Windows hosts, as well as Macintosh, Linux, or other platforms configured to use NetBIOS, can have a NetBIOS name. For example, Linux hosts configured as Samba servers have NetBIOS names.

### Device (hops)

Either:

- the reporting device for the network where the host resides, as defined in the network discovery policy, or
- the device that processed the NetFlow data that added the host to the network map

The number of network hops between the device that detected the host and the host itself follows the device name, in parentheses. If multiple devices can see the host, the reporting device is displayed in bold.

If this field is blank, either:

- the host was added to the network map by a device that is not explicitly monitoring the network where the host resides, as defined in the network discovery policy, or
- the host was added using the host input feature and has not also been detected by the system.

### MAC addresses (TTL)

The host's detected MAC address or addresses and associated NIC vendors, with the NIC's hardware vendor and current time-to-live (TTL) value in parentheses.

If multiple devices detected the host, the Firewall Management Center displays all MAC addresses and TTL values associated with the host, regardless of which device reported them.

If the MAC address is displayed in bold font, the MAC address is the actual/true/primary MAC address of the host, definitively tied to the IP address by detection through ARP and DHCP traffic.

MAC addresses that are not displayed in bold font are secondary addresses, which cannot be definitively associated with the IP address of the host. For example, since the firewall device can obtain MAC addresses only for hosts on its own network segments, if traffic originates from a network segment to which the firewall device is not directly connected, the observed MAC address (i.e. the router MAC address) will be displayed as a secondary MAC address for the host.

### Host type

The type of device that the system detected: host, mobile device, jailbroken mobile device, router, bridge, NAT device, or load balancer.

The methods the system uses to distinguish network devices include:

- the analysis of Cisco Discovery Protocol (CDP) messages, which can identify network devices and their type (Cisco devices only)
- the detection of the Spanning Tree Protocol (STP), which identifies a device as a switch or bridge
- the detection of multiple hosts using the same MAC address, which identifies the MAC address as belonging to a router
- the detection of TTL value changes from the client side, or TTL values that change more frequently than a typical boot time, which identify NAT devices and load balancers
- The methods the system uses to distinguish mobile devices include:
- analysis of User-Agent strings in HTTP traffic from the mobile device's mobile browser
- monitoring of HTTP traffic of specific mobile applications

If a device is not identified as a network device or a mobile device, it is categorized as a host.

### Last seen

The date and time that any of a host's IP addresses was last detected.

### Current user

The user most recently logged into this host.

Note that a non-authoritative user logging into a host only registers as the current user on the host if the existing current user is not an authoritative user.

### View

Links to views of connection, discovery, malware, and intrusion event data, using the default workflow for that event type and constrained to show events related to the host; where possible, these events include all IP addresses associated with the host.

# Operating systems in the host profile

The system passively detects the identity of the operating system running on a host by analyzing the network and application stack in traffic generated by the host or by analyzing host data reported by the User Agent. The system also collates operating system information from other sources, such as the Nmap scanner or application data imported through the host input feature. The system considers the priority assigned to each identity source when determining which identity to use. By default, user input has the highest priority, followed by application or scanner sources, followed by the discovered identity.

Sometimes the system supplies a general operating system definition rather than a specific one because the traffic and other identity sources do not provide sufficient information for a more focused identity. The system collates information from the sources to use the most detailed definition possible.

Because the operating system affects the vulnerabilities list for the host and the event impact correlation for events targeting the host, you may want to manually supply more specific operating system information. In addition, you can indicate that fixes have been applied to the operating system, such as service packs and updates, and invalidate any vulnerabilities addressed by the fixes.

For example, if the system identifies a host's operating system as Microsoft Windows 2003, but you know that the host is actually running Microsoft Windows XP Professional with Service Pack 2, you can set the operating system identity accordingly. Setting a more specific operating system identity refines the list of vulnerabilities for the host, so your impact correlation for that host is more focused and accurate.

If the system detects operating system information for a host and that information conflicts with a current operating system identity that was supplied by an active source, an identity conflict occurs. When an identity conflict is in effect, the system uses both identities for vulnerabilities and impact correlation.

You can configure the network discovery policy to add discovery data to the network map for hosts monitored by NetFlow exporters. However, there is no operating system data available for these hosts, unless you set the use the host input feature to set the operating system identity.

If a host is running an operating system that violates a compliance allow list in an activated network discovery policy, the Firewall Management Center marks the operating system information with the allow list **Violation**. In addition, if a jailbroken mobile device violates an active allow list, the icon appears next to the operating system for the device.

You can set a custom display string for the host's operating system identity. That display string is then used in the host profile.

**Note** Changing the operating system information for a host may change its compliance with a compliance allow list.

In the host profile for a network device, the label for the Operating Systems section changes to Systems and an additional Hardware column appears. If a value for a hardware platform is listed under Systems, that system represents a mobile device or devices detected behind the network device. Note that mobile devices may or

may not have hardware platform information, but hardware platform information is never detected for systems that are not mobile devices.

Descriptions of the operating system information fields displayed in the host profile follow.

#### Hardware

The hardware platform for a mobile device.

#### OS Vendor/Vendor

The operating system vendor.

#### OS Product/Product

One of these values:

- the operating system determined most likely to be running on the host, based on the identity data collected from all sources
- `Pending` if the system has not yet identified an operating system and no other identity data is available
- `unknown` if the system cannot identify the operating system and no other identity data is available for the operating system



**Note** If the host's operating system is not one the system is capable of detecting, see .

#### OS Version/Version

The operating system version. If a host is a jailbroken mobile device, `Jailbroken` is indicated in parentheses after the version.

#### Source

One of these values:

- User: user_name
- Application: app_name
- Scanner: scanner_type (Nmap or other scanner)
- Firepower

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

# View operating system identities

You can view the specific operating system identities discovered or added for a host. The system uses source prioritization to determine the current identity for the host. In the list of identities, the current identity is highlighted by boldface text.

Note that the **View** is only available if multiple operating system identities exist for the host.

### Procedure

**Step 1** Click **View** in the **Operating System** or **Operating System Conflicts** section of the host profile.

**Step 2** Review the list of operating system identities. The current identity is shown in bold text, determined by source prioritization.

For detailed information about identity sources and prioritization, refer to Operating systems in the host profile, on page 6.

**Step 3** Optionally, click **Delete** ( ) next to any operating system identity to remove it.

**Note** You cannot delete Cisco-detected operating system identities.

This system removes the identity from the Operating System Identity Information pop-up window and, if applicable, updates the current identity for the operating system in the host profile.

# Set the current operating system identity

You can set the current operating system identity for a host using the web interface. Setting the identity through the web interface overrides all other identity sources so that identity is used for vulnerability assessment and impact correlation. However, if the system detects a conflicting operating system identity for the host after you edit the operating system, an operating system conflict occurs. Both operating systems are then considered current until you resolve the conflict.

### Procedure

**Step 1** Click **Edit** in the **Operating System** section of a host profile.

**Step 2** You have several options:

- Choose **Current Definition** from the **OS Definition** drop-down list to confirm the current operating system identity through host input, then skip to step 6.
- Choose a variation on the current operating system identity from the **OS Definition** drop-down list, then skip to step 6.
- Choose **User-Defined** from the **OS Definition** drop-down list, then continue with step 3.

**Step 3** Optionally, choose **Use Custom Display String** and modify the custom strings you want to display in the **Vendor String**, **Product String**, and **Version String** fields.

**Step 4** Optionally, to change to an operating system from a different vendor, choose from the **Vendor** and **Product** drop-down lists.

**Step 5** Optionally, to configure the operating system product release level, choose from the **Major**, **Minor**, **Revision**, **Build**, **Patch**, and **Extension** drop-down lists.

**Step 6** Optionally, if you want to indicate that fixes for the operating system have been applied, click **Configure Fixes**.

**Step 7** Choose the applicable fixes in the drop-down list, and click **Add**.

**Step 8** Optionally, add the relevant patches and extensions using the **Patch** and **Extension** drop-down lists.

**Step 9** Click **Finish**.

# Operating system identity conflicts

An operating system identity conflict is a host profile condition that

- occurs when the system detects a new operating system identity that conflicts with a current identity from an active source,
- highlights conflicting identities in bold within the host profile, and
- can be resolved by manually setting the operating system identity through the system web interface, overriding other sources for vulnerability assessment and impact correlation.

### Identity conflict resolution

You can resolve an identity conflict and set the current operating system identity for a host through the system web interface. Setting the identity through the web interface overrides all other identity sources so that identity is used for vulnerability assessment and impact correlation.

## Make a conflicting operating system identity current

When a host has multiple operating system identities that conflict with each other, you need to specify which identity should be considered the current operating system for that host.

### Procedure

**Step 1** Navigate to the **Operating System** section of a host profile.

**Step 2** Choose one of the following options:

- Click **Make Current** next to the operating system identity you want to set as the operating system for the host.
- If the identity that you *do not* want as the current identity came from an active source, delete the unwanted identity.

## Resolving an operating system identity conflict

Operating system conflicts arise when there are discrepancies between the detected operating system and the configured identity in the host profile. This task allows you to select the correct operating system definition or create a custom one.

### Procedure

**Step 1** Click **Resolve** in the **Operating System Conflicts** section of a host profile.

**Step 2** You have the following choices:

- Choose **Current Definition** from the **OS Definition** drop-down list to confirm the current operating system identity through host input, then skip to step 6.
- Choose a variation on one of the conflicting operating system identities from the **OS Definition** drop-down list, then skip to step 6.
- Choose **User-Defined** from the **OS Definition** drop-down list, then continue with step 3.

**Step 3** Optionally, choose **Use Custom Display String** and enter the custom strings you want to display in the **Vendor String**, **Product String**, and **Version String** fields.

**Step 4** Optionally, to change to an operating system from a different vendor, choose from the **Vendor** and **Product** drop-down lists.

**Step 5** Optionally, to configure the operating system product release level, choose from the **Major**, **Minor**, **Revision**, **Build, Patch,** and **Extension** drop-down lists.

**Step 6** Optionally, if you want to indicate that fixes for the operating system have been applied, click **Configure Fixes**.

**Step 7** Add the fixes you have applied to the fixes list.

**Step 8** Click **Finish**.

# Servers in the host profile

The Servers Section of the host profile lists servers either detected on hosts on your monitored network, added from exported NetFlow records, or added through an active source like a scanner or the host input feature.

The list can include up to 100 servers per host. After that limit is reached, new server information from any source, whether active or passive, is discarded until you delete a server from the host or a server times out.

If you scan a host using Nmap, Nmap adds the results of previously undetected servers running on open TCP ports to the Servers list. If you perform an Nmap scan or import Nmap results, an expandable Scan Results section also appears in the host profile, listing the server information detected on the host by the Nmap scan. In addition, if the host is deleted from the network map, the Nmap scan results for that server for the host are discarded.

**Note** The system can add hosts to the network map from exported NetFlow records, but the available information for these hosts is limited; see Differences between NetFlow and managed device data.

The process for working with servers in the host profile differs depending on how you access the profile:

- If you access the host profile by drilling down through the network map, the details for that server appear with the server name highlighted in bold. If you want to view the details for any other server on the host, click **View** ( ) next to that server name.

- If you access the host profile in any other way, expand the Servers section and click **View** ( ) next to the server whose details you want to see.

**Note** If the host is running a server that violates a compliance allow list in an activated correlation policy, the Firewall Management Center marks the non-compliant server with the allow list **Violation**.

Descriptions of the columns in the Servers list follow.

#### Protocol

The name of the protocol the server uses.

#### Port

The port where the server runs.

#### Application protocol

One of:

- the name of the application protocol
- `pending` if the system cannot positively or negatively identify the application protocol for one of several reasons
- `unknown` if the system cannot identify the application protocol based on known application protocol fingerprints, or if the server was added through host input by adding a vulnerability with port information without adding a corresponding server

When you hover the mouse on an application protocol name, the tags display.

#### Vendor and version

The vendor and version identified by the system, Nmap, or another active source, or acquired via the host input feature. The field is blank if none of the available sources provides an identification.

# Server details in the host profile

The Firewall Management Center lists up to 16 passively detected identities per server. Passive detection sources include network discovery data and NetFlow records. A server can have multiple passive identities if the system detects multiple vendors or versions of that server. For example, a load balancer between your managed device and your web server farm may cause your system to identify multiple passive identities for HTTP if your web servers are not running the same version of the server software. Note that the Firewall Management Center does not limit the number of server identities from active sources such as user input, scanners, or other applications.

The Firewall Management Center displays the current identity in bold. The system uses the current identity of a server for multiple purposes, including assigning vulnerabilities to a host, impact assessment, evaluating correlation rules written against host profile qualifications and compliance allow lists, and so on.

The server detail may also display updated sub-server information known about the selected server.

The server detail may also display the server banner, which appears below the server details when you view a server from the host profile. Server banners provide additional information about a server that may help you identify the server. The system cannot identify or detect a misidentified server when an attacker purposely alters the server banner string. The server banner displays the first 256 bytes of the first packet detected for the server. It is collected only once, the first time the server is detected by the system. Banner content is listed in two columns, with a hexadecimal representation on the left and a corresponding ASCII representation on the right.



**Note** To view server banners, you must enable the **Capture Banners** check box in the network discovery policy. This option is disabled by default.

The server details section of the host profile includes the following information:

**Protocol**

The name of the protocol the server uses.

**Port**

The port where the server runs.

**Hits**

The number of times the server was detected by a managed device or an Nmap scanner. The number of hits is 0 for servers imported through host input, unless the system detects traffic for that server.

**Last Used**

The time and date the server was last detected. The last used time for host input data reflects the initial data import time unless the system detects new traffic for that server. Scanner and application data imported through the host input feature times out according to settings in the Firewall Management Center configuration, but user input through the Firewall Management Center web interface does not time out.

**Application Protocol**

The name of the application protocol used by the server, if known.

**Vendor**

The server vendor. This field does not appear if the vendor is unknown.

**Version**

The server version. This field does not appear if the version is unknown.

**Source**

One of these values:

- User: user_name
- Application: app_name
- Scanner: scanner_type (Nmap or other scanner)
- `Firepower`, `Firepower Port Match`, or `Firepower Pattern Match` for applications detected by the system

- `NetFlow` for servers added to the network map from NetFlow records

The system may reconcile data from multiple sources to determine the identity of a server.

# View server details

Use this task to investigate server-specific data, such as configuration settings or operational status, for troubleshooting or validating setups.

**Before you begin**

Ensure you have a host profile open in the user interface.

**Procedure**

In a host profile, click **View** ( ) next to a server in the **Servers** section.

# Editing server identities

You can manually update the identity settings for a server on a host and configure any fixes that you have applied to the host to remove the vulnerabilities addressed by the fixes. You can also delete server identities.

Deleting an identity does not delete the server, even if you delete the only identity. Deleting an identity does remove the identity from the Server Detail pop-up window and, if applicable, updates the current identity for the server in the host profile.

You cannot edit or delete server identities added by a Cisco-managed device.

**Procedure**

**Step 1** Navigate to the **Servers** section of a host profile.

**Step 2** Click **View** to open the Server Detail pop-up window.

**Step 3** To delete a server identity, click **Delete** ( ) next to the server identity you want to remove.

**Step 4** To modify a server identity, click **Edit** ( ) next to the server in the servers list.

You have two choices:

- Choose the current definition from the **Select Server Type** drop-down list.
- Choose the type of server from the **Select Server Type** drop-down list.

**Step 5** Optionally, to only list vendors and products for that server type, choose the **Restrict by Server Type** check box.

**Step 6** Optionally, to customize the name and version of the server, choose the **Use Custom Display String**, and enter a **Vendor String** and **Version String**.

**Step 7** In the **Product Mappings** section, choose the operating system, product, and versions you want to use.

**Example:**

For example, if you want the server to map to Red Hat Linux 9, choose **Redhat, Inc.** as the vendor, **Redhat Linux** as the product, and **9** as the version.

**Step 8** If you want to indicate that fixes for the server have been applied, click **Configure Fixes**, and add the patches you want to apply for that server to the fixes list.

**Step 9** Click **Finish**.

# Resolving server identity conflicts

A server identity conflict occurs when an active source, such as an application or scanner, adds identity data for a server to a host, after which the system detects traffic for that port that indicates a conflicting server identity.

**Procedure**

**Step 1** In a host profile, navigate to the **Servers** section.

**Step 2** Click resolve next to a server.

**Step 3** Choose the type of server from the **Select Server Type** drop-down list.

**Step 4** Optionally, to only list vendors and products for that server type, choose the **Restrict by Server Type** check box.

**Step 5** Optionally, to customize the name and version of the server, choose **Use Custom Display String**, and enter a **Vendor String** and **Version String**.

**Step 6** In the **Product Mappings** section, choose the operating system, product, and versions you want to use.

**Example:**

For example, if you want the server to map to Red Hat Linux 9, choose **Redhat, Inc.** as the vendor, **Redhat Linux** as the product, and **9** as the version.

**Step 7** If you want to indicate that fixes for the server have been applied, click **Configure Fixes**, and add the patches you want to apply for that server to the fixes list.

**Step 8** Click **Finish**.

# Web applications in the host profile

The Web Application section of the host profile displays the clients and web applications that the system identifies as running on the hosts on your network. The system can identify client and web application information from both passive and active detection sources, although the information for hosts added from NetFlow records is limited.

Details in this section include the product and version of the detected applications on a host, any available client or web application information, and the time that the application was last detected in use.

The section lists up to 16 clients running on the host. After that limit is reached, new client information from any source, whether active or passive, is discarded until you delete a client application from the host or the system deletes the client from the host profile due to inactivity (the client times out).

Additionally, for each detected web browser, the system displays the first 100 web applications accessed. After that limit is reached, new web applications associated with that browser from any source, whether active or passive, are discarded until either:

- the web browser client application times out, or
- you delete application information associated with a web application from the host profile

If the host is running an application that violates a compliance allow list in an activated correlation policy, the Firewall Management Center marks the non-compliant application with the allow list **Violation**.

**Tip** To analyze the connection events associated with a particular application on the host, click **Logging** ( ) next to the application. The first page of your preferred workflow for connection events appears, showing connection events constrained by the type, product, and version of the application, as well as the IP address(es) of the host. If you do not have a preferred workflow for connection events, you must select one.

Descriptions of the application information that appears in a host profile follow.

#### Application protocol

Displays the application protocol used by the application (HTTP browser, DNS client, and so on).

#### Client

Client information derived from payload if identified by the system, captured by Nmap, or acquired via the host input feature. The field is blank if none of the available sources provides an identification.

#### Version

Displays the version of the client.

#### Web application

For web browsers, the content detected by the system in the HTTP traffic. Web application information indicates the specific type of content (for example, WMV or QuickTime) identified by the system, captured by Nmap, or acquired via the host input feature. The field is blank if none of the available sources provides an identification.

# Delete web applications from the host profile

If the system detects the application again, it re-adds it to the network map and the host profile.

### Procedure

**Step 1** In a host profile, navigate to the **Applications** section.

**Step 2** Click **Delete** ( ) next to the application you want to delete.

# Host protocols in the host profile

Each host profile contains details about the protocols detected in network traffic associated with the host. The recorded protocol information includes:

- **Protocol**: The name of a protocol used by the host.
- **Layer**: The network layer where the protocol runs (**Network** or **Transport**).

If a protocol displaying in the host profile violates a compliance allow list in an activated correlation policy, the Firewall Management Center marks the non-compliant protocol with the allow list **violation**.

If the host profile lists protocols that you know are not running on the host, you can delete those protocols. Deleting a protocol from a host may bring the host into compliance with a compliance allow list.

**Note** If the system detects the protocol again, it automatically re-adds the protocol to the network map and the host profile.

## Delete a protocol from the host profile

You can remove protocols from host profiles when they are no longer required for your network configuration or security policies.

**Procedure**

**Step 1** Navigate to the **Protocols** section of a host profile.

**Step 2** Click **Delete** ( ) next to the protocol you want to delete.

# Indications of compromise in the host profile

The system correlates various types of data (intrusion events, Security Intelligence, connection events, and file or malware events) to determine whether a host on your monitored network is likely to be compromised by malicious means. Certain combinations and frequencies of event data trigger indications of compromise (IOC) tags on affected hosts. The Indications of Compromise section of the host profile displays all indication of compromise tags for a host.

To configure the system to tag indications of compromise, see *Enabling Indications of Compromise Rules* in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

For more information about working with indications of compromise, see Indications of compromise data and the subtopics under that topic.

# VLAN tags in the host profile

The VLAN Tag section of the host profile appears if the host is a member of a Virtual LAN (VLAN).

Physical network equipment often uses VLANs to create logical network segments from different network blocks. The system detects 802.1q VLAN tags and displays the information for each.

- **VLAN ID** identifies the VLAN where the host is a member. This can be any integer between zero and 4095 for 802.1q VLANs.
- **Type** identifies the encapsulated packet containing the VLAN tag, which can be either Ethernet or Token Ring.
- **Priority** identifies the priority in the VLAN tag, which can be any integer from zero to 7, where 7 is the highest priority.

If VLAN tags are nested within the packet, the system processes and the Firewall Management Center displays the innermost VLAN tag. The system collects and displays VLAN tag information only for MAC addresses that it identifies through ARP and DHCP traffic.

VLAN tag information can be useful, for example, if you have a VLAN composed entirely of printers and the system detects a Microsoft Windows 2000 operating system in that VLAN. VLAN information also helps the system generate more accurate network maps.

# User history in host profiles

User history in the host profile is a network monitoring feature that

- provides a graphic representation of the last twenty-four hours of user activity,
- displays user identities with bar graphs to indicate when user logins are detected, and
- associates user logins with host IP addresses for tracking purposes.

### User login types and associations

The system handles different types of user logins and their associations with host resources:

- **Authoritative logins:** Display as colored bar graphs and take precedence in host associations
- **Non-authoritative logins:** Display as gray bar graphs and do not disrupt existing authoritative user associations
- **Failed logins:** Appear in the user list when capture of failed logins is configured in the network discovery policy

Periodic login requests, such as those made to check email, appear as short regular bars. When an authoritative user login is detected for a host, that user takes over the association with the host IP address, and subsequent non-authoritative user logins do not disrupt the association.

### Typical user activity patterns

A typical user logs off in the evening and may share the host resource with another user. The user history displays this pattern through bar graph representations showing login duration and frequency throughout the twenty-four hour period.

# Host attributes in the host profile

A host attribute is a classification criterion that

- organizes hosts into categories relevant to network management,
- provides both predefined and user-defined attribute options, and
- enables assignment of values to hosts for more granular control.

### Host attribute types

Three types of attributes are present in the system:

- *predefined host attributes*
- *compliance allow list host attributes*
- *user-defined host attributes*

After an attribute is set, whether predefined or user-defined, a value must be assigned to the associated host.



**Note** Host attributes can be defined at any domain level. You can assign host attributes created in current and ancestor domains.

# Predefined Host Attributes

The Firewall Management Center provides two predefined host attributes:

**Host Criticality**

Use this attribute to designate the business criticality of a given host and to tailor correlation responses to host criticality. For example, if you consider your organization's mail servers more critical to your business than a typical user workstation, you can assign a value of High to your mail servers and other business-critical devices and Medium or Low to other hosts. You can then create a correlation policy that launches different alerts based on the criticality of an affected host.

**Notes**

Use this host-specific attribute to record information about the host that you want other analysts to view. For example, if you have a computer on the network that has an older, unpatched version of an operating system that you use for testing, you can use the Notes feature to indicate that the system is intentionally unpatched.

# Allow list host attributes

Allow list host attributes are automatically generated attributes that

- are created with the same name as the compliance allow list,
- identify the compliance status of hosts against the allow list, and
- cannot be edited or deleted by users.

### Host attribute values

Possible values for allow list host attributes are:

- Compliant: Identifies hosts that are compliant with the allow list.
- Non-Compliant: Identifies hosts that violate the allow list.
- Not Evaluated: Identifies hosts that are not valid targets of the allow list or have not been evaluated for any reason.

You cannot edit the value of an allow list host attribute or delete an allow list host attribute.

# User-Defined Host Attributes

If you want to identify hosts using criteria that differs from those used in the predefined host attributes or compliance allow list host attributes, you can create user-defined host attributes. For example, you can:

- Assign physical location identifiers to hosts, such as a facility code, city, or room number.
- Assign a Responsible Party Identifier that indicates which system administrator is responsible for a given host. You can then craft correlation rules and policies to send alerts to the correct system administrator when problems related to a host are detected.
- Automatically assign values to hosts from a predefined list based on the hosts' IP addresses. This feature can be useful to assign values to new hosts when they appear on your network for the first time.

User-defined host attributes appear in the host profile page, where you can assign values on a per-host basis. You can also:

- Use the attributes in correlation policies and searches.
- View the attributes on the host attribute table view of events and generate reports based on them.

User-defined host attributes can be one of the following types:

**Text**

Allows you to manually assign a text string to a host.

**Integer**

Allows you to specify the first and last number of a range of positive integers, then manually assign one of these numbers to a host.

**List**

Allows you to create a list of string values, then manually assign one of the values to a host. You can also automatically assign values to hosts based on the host's IP addresses.

If you auto-assign values based on one IP address of a host with multiple IP addresses, those values will apply across all addresses associated with that host. Keep this in mind when you view the Host Attributes table.

When automatically assigning list values, consider using network objects rather than literal IP addresses. This approach can improve maintainability, particularly in a multidomain deployment where using override-enabled objects allows descendant domain administrators to tailor ancestor configurations to their local environments. In a multidomain deployment, be careful when defining auto-assigned lists at ancestor domain levels to avoid matching unintended hosts when the descendant domains use overlapping IP addresses.

**URL**

Allows you to manually assign a URL value to a host.

Deleting a user-defined host attribute removes it from every host profile where it is used.

# Create text- or URL-based host attributes

Host attributes provide a way to classify and group hosts in your network based on custom criteria. This allows for more granular security policies and improved network management.

### Procedure

**Step 1** Choose **Analysis** > **Hosts heading** > **Host Attributes**.

**Step 2** Click **Host Attribute Management**.

**Step 3** Click **Create Attribute**.

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

**Step 5** Choose the **Type** of attribute that you want to create as described in User-Defined Host Attributes, on page 19.

**Step 6** Click **Save**.

# Create integer-based host attributes

When you define an integer-based host attribute, you must specify the range of numbers that the attribute accepts.

### Procedure

**Step 1** Choose **Analysis** > **Hosts heading** > **Host Attributes**.

**Step 2** Click **Host Attribute Management**.

**Step 3** Click **Create Attribute**.

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

**Step 5** Choose the **Type** of attribute that you want to create as described in User-Defined Host Attributes, on page 19.

**Step 6** In the **Min** field, enter the minimum integer value that can be assigned to a host.

**Step 7** In the **Max** field, enter the maximum integer value that can be assigned to a host.

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

# Create list-based host attributes

When you define a list-based host attribute, you must supply each of the values for the list. These values can contain alphanumeric characters, spaces, and symbols.

**Before you begin**

Follow these steps to create list-based host attributes:

**Procedure**

**Step 1** Choose **Analysis** > **Hosts heading** > **Host Attributes**.

**Step 2** Click **Host Attribute Management**.

**Step 3** Click **Create Attribute**.

**Step 4** Enter a **Name**, and choose the **Type** of attribute that you want to create as described in User-Defined Host Attributes, on page 19.

**Step 5** To add a value to the list, click **Add Value**.

**Step 6** In the **Name** field, enter the first value you want to add.

Optionally, to auto-assign the attribute value you just added to your hosts, click **Add Networks**.

**Step 7** Choose the value you added from the **Value** drop-down list.

**Step 8** In the **IP Address** and **Netmask** fields, enter the IP address and network mask (IPv4) that represent the IP address block where you want to auto-assign this value. Note that you must enter the **IP Address** and **Netmask** in CIDR notation, for example, *198.51.100.0/24*.

Repeat steps 6 through 10 to add additional values to the list and assign them automatically to new hosts that fall within an IP address block.

**Step 9** Click **Save**.

# Set host attribute values

You can set values for predefined and user-defined host attributes. You cannot set values for compliance allow list host attributes generated by the system.

**Procedure**

**Step 1** Open the host profile you want to modify.

**Step 2** In the **Attributes** section, click **Edit Attributes**.

**Step 3** Update attribute as desired.

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

# Allow list violations in the host profile

A *compliance allow list* (or *allow list*) is a set of criteria that allows you to specify the operating systems, application protocols, clients, web applications, and protocols that are allowed to run on a specific subnet.

If you add an allow list to an active correlation policy, when the system detects that a host is violating the allow list, the Firewall Management Center logs an allow list event—which is a special kind of correlation event— to the database. Each of these allow list events is associated with an *allow list violation*, which indicates how and why a particular host is violating the allow list. If a host violates one or more allow lists, you can view these violations in its host profile in two ways.

First, the host profile lists all of the individual allow list violations associated with the host.

Second, in the sections associated with operating systems, applications, protocols, and servers, the Firewall Management Center marks non-compliant elements with the allow list **Violation**. For example, for an allow list that allows only Microsoft Windows hosts, the host profile displays the allow list violation icon next to the operating system information for that host.

Descriptions of the allow list violation information in the host profile follow.

**Type**

The type of the violation, that is, whether the violation occurred as a result of a non-compliant operating system, application, server, or protocol.

**Reason**

The specific reason for the violation. For example, if you have an allow list that allows only Microsoft Windows hosts, the host profile displays the current operating system running on the host (such as `Linux Linux 2.4, 2.6`)

**Allow List**

The name of the allow list associated with the violation.

**Note** You can use a host's profile to create a shared host profile for compliance allow lists.

# Create Shared Allow List Host Profiles

Shared host profiles for compliance allow lists specify which operating systems, application protocols, clients, web applications, and protocols are allowed to run on target hosts across multiple allow lists. That is, if you create multiple allow lists but want to use the same host profile to evaluate hosts running a particular operating system across the allow lists, use a shared host profile.

You can use a host profile of any host with a known IP address to create a shared host profile that your compliance allow lists can use. However, note that you cannot create a shared host profile based on an individual host's host profile if the system has not yet identified the operating system of the host.

**Procedure**

**Step 1** In a host profile, click **Generate Allow List Profile**.

**Step 2** Modify and save the shared host profile according to your specific needs.

# Malware detections in the host profile

The most recent malware detections section lists the most recent malware events where the host sent or received a malware file, up to 100 events. The host profile lists both network-based malware events (those generated by malware defense) and endpoint-based malware events (those generated by Secure Endpoint).

If the host is involved in a file event where the file is then retrospectively identified as malware, the original events where the file was transmitted appear in the malware detections list after the malware identification occurs. When a file identified as malware is retrospectively determined not to be malware, the malware events related to that file no longer appear in the list. For example, if a file has a disposition of `Malware` and that disposition changes to `Clean`, the event for that file is removed from the malware detections list on the host profile.

When viewing malware detections in the host profile, you can view malware events for that host by clicking the **Malware**.

Description of the columns in the Most Recent Malware Detections sections of the host profile follow.

The Most Recent Malware Detections section contains these columns:

- **Time**: The date and time the event was generated. For an event where the file was retrospectively identified as malware, note that this is the time of the original event, not the time when the malware was identified.
- **Host Role**: The host's role in the transmission of detected malware, either sender or receiver. Note that for malware events generated by Secure Endpoint ("endpoint-based malware events"), the host is always the receiver.
- **Threat Name**: The name of the detected malware.
- **File Name**: The name of the malware file.
- **File Type**: The type of file; for example, `PDF` or `MSEXE`.

# Vulnerabilities in the host profile

The Vulnerabilities sections of the host profile list the vulnerabilities that affect that host. These vulnerabilities are based on the operating system, servers, and applications that the system detected on the host.

If there is an identity conflict for either the identity of the host's operating system or one of the application protocols on the host, the system lists vulnerabilities for both identities until the conflict is resolved.

Because no operating system information is available for hosts added to the network map from NetFlow data, the system cannot assign Vulnerable (impact level 1: red) impact levels for intrusion events involving those hosts. In such cases, use the host input feature to manually set the operating system identity for the hosts.

Server vendor and version information is often not included in traffic. By default, the system does not map the associated vulnerabilities for the sending and receiving hosts of such traffic. However, you can configure the system to map vulnerabilities for specific application protocols that do not have vendor or version information.

If you use the host input feature to add third-party vulnerability information for the hosts on your network, additional Vulnerabilities sections appear. For example, if you import vulnerabilities from a QualysGuard Scanner, host profiles on your include a QualysGuard Vulnerabilities section. For third-party vulnerabilities, the information in the corresponding Vulnerabilities section in the host profile is limited to the information that you provided when you imported the vulnerability data using the host input feature.

You can associate third-party vulnerabilities with operating systems and application protocols, but not clients. For information on importing third-party vulnerabilities, refer to the *Firepower System Host Input API Guide*.

Descriptions of the columns in the Vulnerabilities sections of the host profile follow.

| Column | Description |
|---|---|
| Name | The name of the vulnerability. |
| Remote | Indicates whether the vulnerability can be remotely exploited. If this column is blank, the vulnerability definition does not include this information. |
| Component | The name of the operating system, application protocol, or client associated with the vulnerability. |
| Port | A port number, if the vulnerability is associated with an application protocol running on a specific port. |

# Download patches for vulnerabilities

You can download patches to mitigate the vulnerabilities discovered on the hosts on your network.

**Procedure**

**Step 1** Access the host profile of a host for which you want to download a patch.

**Step 2** Expand the **Vulnerabilities** section.

**Step 3** Click the name of the vulnerability you want to patch.

**Step 4** Expand the **Fixes** section to display the list of patches for the vulnerability.

**Step 5** Click **Download** next to the patch you want to download.

**Step 6** Download the patch and apply it to your affected systems.

# Deactivate vulnerabilities for individual hosts

You can use the host vulnerability editor to deactivate vulnerabilities on a host-by-host basis. When you deactivate a vulnerability for a host, it is still used for impact correlations for that host, but the impact level is automatically reduced one level.

### Procedure

**Step 1** Navigate to the **Vulnerabilities** section of a host profile.

**Step 2** Click **Edit Vulnerabilities**.

**Step 3** Choose the vulnerability from the **Valid Vulnerabilities** list, and click the down arrow to move it to the **Invalid Vulnerabilities** list.

**Tip** You can click and drag to choose multiple adjacent vulnerabilities; you can also double-click any vulnerability to move it from list to list.

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

### What to do next

- Optionally, activate the vulnerability for the host by moving it from the **Invalid Vulnerabilities** list to the **Valid Vulnerabilities** list.

# Deactivate individual vulnerabilities

If you deactivate a vulnerability in a host profile, it deactivates it for all hosts in your network map. However, you can reactivate it at any time.

In a multidomain deployment, deactivating a vulnerability in an ancestor domain deactivates it in all descendant domains. Leaf domains can activate or deactivate a vulnerability for their devices if the vulnerability is activated in the ancestor domain.

### Procedure

**Step 1** Access the vulnerability detail:

- In an affected host profile, expand the **Vulnerabilities** section, and click the name of the vulnerability you want to enable or disable.
- In the predefined workflow, choose **Analysis** > **Hosts heading** > **Vulnerabilities**, and click **View** ( ) next to the vulnerability you want to enable or disable.

**Step 2** Choose **Disabled** from the **Impact Qualification** drop-down list.

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

**Step 3** Confirm that you want to change the **Impact Qualification** value for all hosts on the network map.

**Step 4** Click **Done**.

### What to do next

Optionally, activate the vulnerability by choosing **Enabled** from the **Impact Qualification** drop-down list while performing the steps above.

# Scan results in the host profile

A scan result is a data record collected from network hosts that

- includes information about open and unfiltered ports,
- identifies the operating system and active servers running on those ports, and
- records additional details such as port state, server name, and detected vendor.

### Scan result information

Each result indicates the following information:

- Source of the information
- Number and type of the scanned port
- Name of the server running on the port
- Additional information detected by Nmap, such as the state of the port or the vendor name for the server

If you scan for UDP ports, servers detected on those ports only appear in the Scan Results section.

**Note**

- You can run an Nmap scan from the host profile.
- The scan must find open ports on the host for Scan Results section to appear in the profile.

# Scan a host from the host profile

You can perform a Nmap scan against a host from the host profile. After the scan completes, server and operating system information for that host are updated in the host profile. Any additional scan results are added to the Scan Results section of the host profile.

**Caution** Nmap-supplied server and operating system data remains static until you run another Nmap scan or override it with higher priority host input. If you plan to scan a host using Nmap, regularly schedule scans.

**Before you begin**

- Add an Nmap scan instance; see the *Host Identity Sources* chapter in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

**Procedure**

**Step 1** In the host profile, click **Scan Host**.

**Step 2** Click **Scan** next to the scan remediation you want to use to scan the host.

The system scans the host and adds the results to the host profile.

# History for host profiles

This reference provides the history of features and limitations for host profiles, specifically when virtual routing and forwarding (VRF) is used in the environment.

| Feature | Minimum Firewall Management Center | Minimum Firewall Threat Defense | Details |
|---|---|---|---|
| Limitation when using VRF | 6.6 | Any | If virtual routing and forwarding is used in your environment, a single IP address may represent multiple hosts because VRF may include overlapping network spaces.<br>Supported Platforms: Firewall Management Center |