Compliance White Lists

The following topics describe how to configure compliance white lists before you add them to correlation policies.

- Introduction to Compliance White Lists, on page 1
- Requirements and Prerequisites for Compliance, on page 6
- Creating a Compliance White List, on page 6
- Managing Compliance White Lists, on page 12
- Managing Shared Host Profiles, on page 14

Introduction to Compliance White Lists

A *compliance white list*, sometimes abbreviated as a *white list*, is a set of criteria that specifies which operating systems, applications (web and client), and protocols are allowed on hosts on your network. The system generates an event (violation) if a host is not on this list.

A compliance white list has two main components:

- *Targets* are the hosts you select for compliance evaluation. You can evaluate all or some monitored hosts, constraining by subnet, VLAN, and host attribute. In a multidomain deployment, you can target domains and subnets within or across domains.
- *Host profiles* specify the compliance criteria for the targets. The global host profile is operating system agnostic. You can also configure operating-system specific host profiles, either unique to one white list or shared across multiple white lists.

The Cisco Talos Intelligence Group (Talos) provides a default white list with recommended settings. You can also create custom white lists. A simple custom list might allow only hosts running a certain operating system. A more complex list might allow all operating systems, but specify which operating system a host must use to run a certain application protocol on a specific port.

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. This limitation may affect the way you build compliance white lists.

Implementing Compliance White Lists

To implement white lists, add the list to an active correlation policy. The system evaluates the targets and assigns every host a corresponding attribute:

- Compliant — The host does not violate the list.
- Non-Compliant — The host violates the list.
- Not Evaluated — The host is not a target of the list, the host is currently being evaluated, or the system has insufficient information to determine whether the host is in compliance.

Note To delete the host attribute, delete its corresponding white list. Deactivating, deleting, or removing a white list from a correlation policy does **not** delete the host attribute, nor does it change the attribute's value for each host.

After its initial evaluation, the system generates a *white list event* whenever a monitored host goes out of compliance with an active white list; it also records a *white list violation*.

You can use workflows, dashboards, and network maps to monitor system-wide compliance activity and determine when and how an individual host violates your white lists. You can also automatically respond to such violations with remediations and alerts.

Example: Restricting HTTP to Web Servers

Your security policy states that only web servers may run HTTP. You create a white list that evaluates your entire network, excluding your web farm, to determine which hosts are running HTTP.

Using the network map and the dashboard, you can obtain an at-a-glance summary of the compliance of your network. In just a few seconds, you can determine exactly which hosts in your organization are running HTTP in violation of your policy, and take appropriate action.

Then, using the correlation feature, you can configure the system to alert you whenever a host that is not in your web farm starts running HTTP.

Related Topics

Configuring Correlation Policies

Compliance White List Target Networks

A *target network* specifies the hosts you want to evaluate for compliance. A white list can have more than one target network, and it evaluates hosts that meet the criteria of any of its targets.

Initially, you constrain a target network by IP address or range. In multidomain deployments, the initial constraints also include a domain.

The system-provided default white list targets all monitored hosts: 0.0.0.0/0 and ::/0. In a multidomain deployment, the default white list is constrained to (and only available in) the Global domain.

If you modify a target network or a host so that the host is no longer a valid target for the white list, the host is no longer evaluated by the list and is considered neither compliant nor non-compliant.

Surveying and Refining Target Networks

When you add a target network to a white list, the system prompts you to survey the network map to help you characterize compliant hosts. The survey adds a target to the white list that represents the hosts you surveyed.

You can survey a subnet or individual host. In a multidomain deployment, you can survey an entire domain, or you can survey across domains. Surveying an ancestor domain causes the system to survey that domain's descendants.

In addition to the added target, the survey also populates the white list with one host profile for each operating system detected in the survey. These host profiles allow all the clients, application protocols, web applications, and protocols that the system has detected on the applicable operating systems.

After you survey a target network (or skip the survey), refine the target. You can exclude hosts by IP address, or constrain target networks by host attribute or VLAN.

Targeting Domains with Compliance White Lists

In a multidomain deployment, domains and target networks are closely linked.

- Leaf-domain administrators can create white lists that evaluate hosts within their leaf domains.
- Higher-level domain administrators can create white lists that evaluate hosts across domains. You can target different subnets in different domains in the same white list.

Consider a scenario where you are a Global domain administrator, and you want to apply the same compliance criteria to web servers across the entire deployment. You can create one white list in the Global domain that defines the compliance criteria. Then, constrain the white list with target networks that specify the IP space (or individual IP addresses) of the web servers in each leaf domain.

Note In addition to targeting IP addresses and ranges in leaf domains, you can also constrain a target network using a higher-level domain. Targeting a subnet in a higher-level domain targets the **same** subnet in **each** of the descendant leaf domains. The system builds a separate network map for each leaf domain. In a multidomain deployment, using literal IP addresses to constrain this configuration can have unexpected results.

Compliance White List Host Profiles

In a compliance white list, host profiles specify which operating systems, clients, application protocols, web applications, and protocols are allowed to run on the target hosts. There are three types of host profile you can use in a compliance white list; each type appears differently in the compliance list editor.

Table 1: Compliance White List Host Profile Types

Host Profile Type	Appearance	Description
global	Any Operating System	specifies what is allowed to run on target hosts, regardless of operating system
operating-system specific	is listed in plain text	specifies what is allowed to run on target hosts of a particular operating system

Host Profile Type	Appearance	Description
shared	is listed in italics	specifies operating-system criteria that can be used in multiple white lists

Operating System-Specific Host Profiles

In a compliance white list, *operating-system specific host profiles* indicate not only which operating systems are allowed to run on your network, but also the application protocols, clients, web applications, and protocols that are allowed to run on those operating systems.

For example, you could require that compliant hosts run a particular version of Microsoft Windows. As another example, you could allow SSH to run on Linux hosts on port 22, and further restrict the vendor and version of the SSH client.

Create one host profile for each operating system you want to allow on your network. To disallow an operating system on your network, do not create a host profile for that operating system. For example, to make sure that all the hosts on your network are running Windows, configure the white list to only contain host profiles for that operating system.

Note Unidentified hosts remain in compliance with all white lists until they are identified. You can, however, create a white list host profile for unknown hosts. *Unidentified* hosts are hosts about which the system has not yet gathered enough information to identify their operating systems. *Unknown* hosts are hosts whose operating systems do not match known fingerprints.

Shared Host Profiles

In a compliance white list, *shared host profiles* are tied to specific operating systems, but you can use each shared host profile in more than one white list.

For example, you might have offices worldwide with a separate white list for each location, but you want to use the same profile for all hosts running Apple Mac OS X. You can create a shared profile for that operating system and use it in all your white lists.

The default white list uses a special category of shared host profiles, called *built-in host profiles*. These profiles use built-in application protocols, web applications, protocols, and clients. In the compliance white list editor, the system marks these profiles with the **Built-In Host Profile icon**.

In a multidomain deployment, the system displays shared host profiles created in the current domain, which you can edit. It also displays shared host profiles from ancestor domains, which you cannot edit. To view and edit shared host profiles created in a lower domain, switch to that domain.

Note If you modify a shared host profile (including built-ins), or modify a built-in application protocol, protocol, or client, your change affects every white list that uses it. If you make unintended changes to or delete these built-in elements, you can reset to factory defaults.

White Violation Triggers

The white list compliance of a host can change when the system:

- detects a change in a host's operating system
- detects an identity conflict for a host's operating system or an application protocol on the host
- detects a new TCP server port (for example, a port used by SMTP or web servers) active on a host, or a new UDP server running on a host
- detects a change in a discovered TCP or UDP server running on a host, for example, a version change due to an upgrade
- detects a new client or web application running on a host
- drops a client or web application from its database due to inactivity
- detects that a host is communicating with a new network or transport protocol
- detects a new jailbroken mobile device
- detects that a TCP or UDP port has closed or timed out on a host

In addition, you can trigger a compliance change for a host by using the host input feature or the host profile to:

- add a client, protocol, or server to a host
- delete a client, protocol, or server from a host
- set the operating system definition for a host
- change a host attribute for a host so that the host is no longer a valid target

Note To avoid overwhelming you with events, the system does not generate white list events for non-compliant hosts on its initial evaluation, nor hosts made non-compliant as a result of you modifying an active white list or shared host profile. The violations, however, are still recorded. If you want to generate white list events for all non-compliant targets, purge discovery data. Rediscovering network assets may trigger white list events.

Operating System Compliance

If your white list specifies that only Microsoft Windows hosts are allowed on your network, and the system detects a host running Mac OS X, the system generates a white list event. In addition, the host attribute associated with the white list changes from Compliant to Non-Compliant for that host.

For the host in this example to come back into compliance, one of the following must occur:

- you edit the white list so that the Mac OS X operating system is allowed
- you manually change the operating system definition of the host to Microsoft Windows
- the system detects that the operating system has changed back to Microsoft Windows

Deleting a Non-Compliant Asset from the Network Map

If your white list disallows the use of FTP, and you then delete FTP from the application protocols network map or from an event view, hosts running FTP become compliant. However, if the system detects the application protocol again, the system generates a white list event and the hosts become non-compliant.

Triggering on Complete Information Only

If your white list allows only TCP FTP traffic on port 21, and the system detects indeterminate activity on port 21/TCP, the white list does not trigger. The white list triggers only when the system identifies the traffic as something other than FTP, or you use the host input feature to designate the traffic as non-FTP traffic. The system does not record a violation with only partial information.

Requirements and Prerequisites for Compliance

Model support

Any

Supported domains

Any

User roles

- Admin

Creating a Compliance White List

When you create a compliance white list, the system prompts you to survey your network to create an initial target and to help you characterize compliant hosts.

Procedure

Step 1 Choose **Policies** > **Correlation**, then click **White List**.

Step 2 Click **NewWhite List**.

Step 3 Optionally, enter the **IP Address** and **Netmask** for an initial target network. In a multidomain deployment, choose the **Domain** where the target network resides.

Tip
To survey the entire monitored network, use the default values of 0.0.0.0/0 and ::/0.

Note

After you choose a domain for the target network, you cannot change it. Targeting a subnet in a higher-level domain targets the **same** subnet in **each** of the descendant leaf domains. The system builds a separate network map for each leaf domain. In a multidomain deployment, using literal IP addresses to constrain this configuration can have unexpected results.

Step 4 Add the target network:

- Add—To add the target network without a survey, click **Add**.
- Add and Survey Network—To add and survey the target network, click **Add and Survey Network**.
- Skip—To create a white list without surveying your network, click **Skip**.

Step 5 Optionally, enter a new **Name** and **Description** for the white list.

Step 6 Optionally, **Allow Jailbroken Mobile Devices** on your network. Disabling this option causes jailbroken devices to generate white list violations.

Step 7 Add at least one **Target Network** to the white list, as described in Setting Target Networks for a Compliance White List, on page 7.

Step 8 Characterize compliant hosts using **Allowed Host Profiles**:

- Global Host Profile—To edit the white list's global host profile, click **Any Operating System** and proceed as described in Building White List Host Profiles, on page 8.
- Edit Surveyed Profiles—To edit an existing operating system-specific host profile created by a network survey, click its name and proceed as described in Building White List Host Profiles, on page 8.
- Create New Profiles—To create a new operating system-specific host profile for this white list, click **Add** ( ) next to **Allowed Host Profiles**, and proceed as described in Building White List Host Profiles, on page 8.
- Add Shared Host Profile—To add an existing shared host profile to the white list, click **Add Shared Host Profile**, select the shared host profile you want to add, then click **OK**. Shared host profiles appear in italics.

Step 9 Click **SaveWhite List**.

What to do next

- Add the white list to an active correlation policy as described in Configuring Correlation Policies. The system immediately starts evaluating the white list and generating violations.

Related Topics

Compliance White List Target Networks, on page 2
Creating a Compliance White List Based on Selected Hosts
Firepower System IP Address Conventions

Setting Target Networks for a Compliance White List

When you add a target network, you can survey it to characterize compliant hosts. This survey populates the white list with one host profile for each operating system detected in the survey. These host profiles allow all the clients, application protocols, web applications, and protocols that the system has detected on the applicable operating systems.

Procedure

Step 1 In the compliance white list editor, click **Add Target Network**.

Step 2 Enter the **IP Address** and **Netmask** for the target network.

Step 3 In a multidomain deployment, choose the **Domain** where the target network resides.

Note
After you choose a domain for the target network, you cannot change it. Targeting a subnet in a higher-level domain targets the **same** subnet in **each** of the descendant leaf domains. The system builds a separate network map for each leaf domain. In a multidomain deployment, using literal IP addresses to constrain this configuration can have unexpected results.

Step 4 Add the target network:

- Add — To add the target network without a survey, click **Add**.
- Add and Survey Network — To add and survey the target network, click **Add and Survey Network**.

Step 5 Optionally, click the new target to configure it further:

- Name — Enter a new **Name**.
- Add Networks — To target additional hosts, click **Add** (), then enter the **IP Address** and **Netmask**. To exclude the network from white list compliance, select **Exclude**.
- Add Host Attributes — To target hosts with a specific host attribute, click **Add** (), then specify the **Attribute** and its **Value**.
- Add VLANs — To target a VLAN, click **Add** (), then type a VLAN number (for 802.1q VLANs).
- Delete — To remove a target restriction, click **Delete** ().

Step 6 To immediately implement all changes made since the last time you saved, click **SaveWhite List**.

Related Topics

Compliance White List Target Networks, on page 2
Firepower System IP Address Conventions

Building White List Host Profiles

Host profiles specify the white list's compliance criteria, that is, which operating systems, clients, application protocols, web applications, and protocols are allowed to run on the target hosts.

Every white list has a global host profile which is operating-system agnostic. For example, instead of editing multiple Microsoft Windows and Linux host profiles to allow Mozilla Firefox, you can configure the global host profile to allow Firefox regardless of the operating system where it was detected.

You can also configure operating-system specific host profiles, either unique to one white list or shared across white lists.

Note If you modify a shared host profile (including built-ins), or modify a built-in application protocol, protocol, or client, your change affects every white list that uses it. If you make unintended changes to or delete these built-in elements, you can reset to factory defaults.

Before you begin

- Create or edit a host profile within a white list as described in Editing a Compliance White List, on page 12, or create or edit a shared host profile as described in Managing Shared Host Profiles, on page 14.

Procedure

Step 1 In the compliance white list host profile editor, configure a host profile:

- Name — Type a **Name**.
- Operating System — To restrict the host profile to a specific operating system, use the **OS Vendor**, **OS Name**, and **Version** drop-down lists. Because its purpose is to apply to hosts running any operating system, you cannot restrict a global host profile.
- Application Protocol — To allow an application protocol, click **Add** ( ) and proceed as described in Adding an Application Protocol to a Compliance White List, on page 10.
- Client — To allow a client, click **Add** ( ) and proceed as described in Adding a Client to a Compliance White List, on page 10.
- Web Application — To allow a web application, click **Add** ( ) and proceed as described in Adding a Web Application to a Compliance White List, on page 11.
- Protocol — To allow a protocol, click **Add** ( ) and proceed as described in Adding a Protocol to a Compliance White List, on page 11.
- Delete — To disallow an item you previously allowed, click **Delete** ( ).
- Edit Properties — To edit the properties of an allowed application protocol, client, or protocol, click its name. The changes you make are reflected in every host profile that uses that element.

Tip
Select the appropriate **Allow all...** check box to allow all application protocols, clients, or web applications for hosts matching this profile.

Step 2 To immediately implement all changes made since the last time you saved, click **SaveWhite List** (or **Save All Profiles** if you are editing a shared host profile).

Adding an Application Protocol to a Compliance White List

Using white list host profiles, you can allow application protocols either globally or on specific operating systems. Optionally, you can restrict the application protocol by port, vendor, or version. For example, you could allow a particular version of OpenSSH to run on Linux hosts on port 22/TCP.

Procedure

Step 1 While you are creating or modifying a compliance white list host profile, click **Add** ( ) next to **Allowed Application Protocols** (or next to **Globally Allowed Application Protocols** if you are modifying the global host profile).

Step 2 You have two options:

- If the application protocols you want to allow are listed, select them. The web interface lists application protocols that have been allowed or are currently allowed by the white list.
- To allow an application protocol not in the list, select **<New Application Protocol>** and click **OK** to display the application protocol editor. Select the application protocol **Type** and **Protocol** you want to allow. Optionally, restrict the application protocol by **port**, **Vendor**, and **Version**.

  Note
  You must type the vendor and version exactly as they would appear in a table view of applications. If you do not specify a vendor or version, the white list allows all vendors and versions as long as the type and protocol match.

Step 3 Click **OK**.

Step 4 To immediately implement all changes made since the last time you saved, click **SaveWhite List**.

Adding a Client to a Compliance White List

Using white list host profiles, you can allow clients either globally or on specific operating systems. Optionally, you can require that the client be a specific version. For example, you could allow only Microsoft Internet Explorer 10 to run on Microsoft Windows hosts.

Procedure

Step 1 While you are creating or modifying a compliance white list host profile, click **Add** ( ) next to **Allowed Clients** (or next to **Globally Allowed Clients** if you are modifying the global host profile).

Step 2 You have two options:

- If the clients you want to allow are listed, select them. The web interface lists clients that have been allowed or are currently allowed by the white list.
- To allow a client not in the list, select **<New Client>** and click **OK** to display the client editor. Select the **Client** you want to allow from the drop-down list, and, optionally, restrict the client to an allowed **Version**.

  Note
  You must type the version exactly as it would appear in a table view of clients. If you do not specify a version, all versions are allowed.

Step 3 Click **OK**.

Step 4 To immediately implement all changes made since the last time you saved, click **SaveWhite List**.

Adding a Web Application to a Compliance White List

Using white list host profiles, you can allow web applications either globally or on specific operating systems.

Procedure

Step 1 While you are creating or modifying a compliance white list host profile, click **Add** ( ) next to **Allowed Web Applications** (or next to **Globally Allowed Web Applications** if you are modifying the global host profile).

Step 2 Select the web applications you want to allow.

Step 3 Click **OK**

Step 4 To immediately implement all changes made since the last time you saved, click **SaveWhite List**.

Adding a Protocol to a Compliance White List

Using white list host profiles, you can allow protocols either globally or on specific operating systems. ARP, IP, TCP, and UDP are always allowed to run on any host; you cannot disallow them.

Procedure

Step 1 While you are creating or modifying a compliance white list host profile, click **Add** ( ) next to **Allowed Protocols** (or next to **Globally Allowed Protocols** if you are modifying the global host profile).

Step 2 You have two options:

- If the protocols you want to allow are listed, select them. The web interface lists protocols that have been allowed or are currently allowed by the white list.
- To allow a protocol not in the list, select **<New Protocol>** and click **OK** to display the protocol editor. From the **Type** drop-down list, select the protocol type (**Network** or **Transport**), then select the **Protocol** from the drop-down list.

  Tip
  Select **Other (manual entry)** to specify a protocol that is not in the list. For network protocols, type the appropriate number as listed in http://www.iana.org/assignments/ethernet-numbers/. For transport protocols, type the appropriate number as listed in http://www.iana.org/assignments/protocol-numbers/.

Step 3 Click **OK**.

Step 4 To immediately implement all changes made since the last time you saved, click **SaveWhite List**.

Managing Compliance White Lists

You can use the White List page to manage compliance white lists and shared host profiles. The default white list represents recommended settings and uses a special category of shared host profiles, called *built-in host profiles*.

In a multidomain deployment, the system displays compliance white lists created in the current domain, which you can edit. It also displays selected white lists from ancestor domains, which you cannot edit. To view and edit white lists created in a lower domain, switch to that domain.

Note The system does not display configurations from ancestor domains if the configurations expose information about unrelated domains, including names, managed devices, and so on. The default white list is only available in the Global domain.

Procedure

Step 1 Choose **Policies** > **Correlation**, then click **White List**.

Step 2 Manage your compliance white lists:

- Create — To create a new white list, click **NewWhite List** and proceed as described in Creating a Compliance White List, on page 6.
- Delete — To delete a white list that is not in use, click **Delete** ( ), then confirm you want to delete the white list. Deleting a white list also removes its associated host attribute from all hosts on your network. If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.
- Edit — To modify an existing white list, click **Edit** ( ) and proceed as described in Editing a Compliance White List, on page 12. If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.
- Shared Host Profiles — To manage your white lists' shared host profiles, click **Edit Shared Profiles** and proceed as described in Managing Shared Host Profiles, on page 14.

Editing a Compliance White List

When you modify and save a compliance white list that is included in an active correlation policy, the system immediately re-evaluates the compliance of the hosts in the white list's target networks. Although this re-evaluation may bring some hosts into or out of compliance, the system does not generate any white list events.

Procedure

Step 1 Choose **Policies** > **Correlation**, then click **White List**.

Step 2 Next to the white list you want to modify, click **Edit** ( ).

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

Step 3 Edit your compliance white list:

- Name and Description — To change the name or description, click the white list name in the left panel to display basic white list information, then type the new information.
- Allow Jailbroken Devices — To allow jailbroken mobile devices on your network, click the white list name in the left panel to display basic white list information, then enable **Allow Jailbroken Mobile Devices**. Disabling this option causes jailbroken devices to generate white list violations.
- Add Allowed Host Profile — To create an operating system-specific host profile for this white list, click **Add** ( ) next to Allowed Host Profiles and proceed as described in Building White List Host Profiles, on page 8.
- Add Shared Host Profile — To add an existing shared host profile to the white list, click **Add Shared Host Profile**, select the shared host profile you want to add, then click **OK**. Shared host profiles appear in italics.
- Add Target Network — To add a new target network without surveying its hosts, click **Add** ( ) next to Target Networks and proceed as described in Setting Target Networks for a Compliance White List, on page 7.
- Delete Host Profile — To delete a shared or operating-system specific host profile from the white list, click **Delete** ( ) next to the host profile, then confirm your choice. Deleting a shared host profile removes it from the white list, but does not delete the profile or remove it from any other white lists that use it. You cannot delete a white list's global host profile.
- Delete Target Network — To remove a target network from the white list, click **Delete** ( ) next to the network, then confirm your choice.
- Edit Global Host Profile — To edit the white list's global host profile, click **Any Operating System** and proceed as described in Building White List Host Profiles, on page 8.
- Edit Other Host Profile — To edit a shared or operating-system specific host profile, click the host profile's name and proceed as described in Building White List Host Profiles, on page 8.
- Edit Target Network — To edit a target network, click the network's name and proceed as directed in Setting Target Networks for a Compliance White List, on page 7.

Step 4 To immediately implement all changes made since the last time you saved, click **SaveWhite List**.

Managing Shared Host Profiles

In a compliance white list, *shared host profiles* are tied to specific operating systems, but you can use each shared host profile in more than one white list. If you create multiple white lists but want to use the same host profile to evaluate hosts running a particular operating system across the white lists, use a shared host profile.

In a multidomain deployment, the system displays shared host profiles created in the current domain, which you can edit. It also displays shared host profiles from ancestor domains, which you cannot edit. To view and edit shared host profiles created in a lower domain, switch to that domain.

Note If you modify a shared host profile (including built-ins), or modify a built-in application protocol, protocol, or client, your change affects every white list that uses it. If you make unintended changes to or delete these built-in elements, you can reset to factory defaults.

Procedure

Step 1 Choose **Policies** > **Correlation**, then click **White List**.

Step 2 Click **Edit Shared Profiles**.

Step 3 Manage your shared host profiles:

- Create Shared Host Profile — To create a new shared host profile without surveying hosts, click **Add** ( ) next to Shared Host Profiles and proceed as described in Building White List Host Profiles, on page 8.
- Create Shared Host Profile by Survey — To create multiple new shared host profiles by surveying a network, click **Add Target Network** and proceed as described in Setting Target Networks for a Compliance White List, on page 7 .
- Delete — To delete a shared host profile, click **Delete** ( ), then confirm your choice.
- Edit — To modify an existing shared host profile (including a built-in shared host profile), click its name and proceed as described in Building White List Host Profiles, on page 8.
- Reset Built-In Host Profiles — To reset all built-in host profiles to factory defaults, click **Built-in Host Profiles**, then click **Reset to Factory Defaults** and confirm your choice.

Step 4 To immediately implement all changes made since the last time you saved, click **Save All Profiles**.