Reusable Objects

The following topics describe how to manage reusable objects in the Firepower System:

- Introduction to Reusable Objects, page 2
- The Object Manager, page 4
- Network Objects, page 11
- Port Objects, page 13
- Tunnel Zones, page 17
- Application Filters, page 17
- VLAN Tag Objects, page 17
- Security Group Tag Objects, page 18
- URL Objects, page 19
- Geolocation Objects, page 20
- Variable Sets, page 21
- Security Intelligence Lists and Feeds, page 38
- Sinkhole Objects, page 47
- File Lists, page 48
- Cipher Suite Lists, page 54
- Distinguished Name Objects, page 55
- PKI Objects, page 57
- SLA Monitor Objects, page 73
- Prefix Lists, page 74
- Route Maps, page 76
- Access List, page 79
- AS Path Objects, page 82
- Community Lists, page 83
Introduction to Reusable Objects

For increased flexibility and web interface ease-of-use, the Firepower System uses named objects, which are reusable configurations that associate a name with a value. When you want to use that value, use the named object instead. The system supports object use in various places in the web interface, including many policies and rules, event searches, reports, dashboards, and so on. The system provides many predefined objects that represent frequently used configurations.

Use the object manager to create and manage objects. Many configurations that use objects also allow you to create objects on the fly, as needed. You can also use the object manager to:

- Group objects to reference multiple objects with a single configuration; see Object Groups, on page 6.
- Override object values for selected devices or, in a multidomain deployment, selected domains; see Object Overrides, on page 8.

After you edit an object used in an active policy, you must redeploy the changed configuration for your changes to take effect. You cannot delete an object that is in use by an active policy.

Object Types

The following table lists the objects you can create in the Firepower System, and indicates whether each object type can be grouped or configured to allow overrides.

<table>
<thead>
<tr>
<th>Object Type</th>
<th>Groupable?</th>
<th>Allows Overrides?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Port</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Interface:</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>• Security Zone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Interface Group</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tunnel Zone</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Application Filter</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>VLAN Tag</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Security Group Tag (SGT)</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td><strong>Object Type</strong></td>
<td><strong>Groupable?</strong></td>
<td><strong>Allows Overrides?</strong></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>URL</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Geolocation</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Variable Set</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Security Intelligence: Network, DNS, and URL lists and feeds</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Sinkhole</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>File List</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Cipher Suite List</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Distinguished Name</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Public Key Infrastructure (PKI):</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>• Internal and Trusted CA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Internal and External Certs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SLA Monitor</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Prefix List: IPv4 and IPv6</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Route Map</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Access List: Standard and Extended</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>AS Path</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Community List</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Policy List</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>FlexConfig: Text and FlexConfig objects</td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>

**Objects and Multitenancy**

In a multidomain deployment, you can create objects in Global and descendant domains with the exception of Security Group Tag (SGT) objects, which you can create only in the Global domain. The system displays objects created in the current domain, which you can edit. It also displays objects created in ancestor domains, which you cannot edit, with the exception of security zones and interface groups.
Because security zones and interface groups are tied to device interfaces, which you configure at the leaf level, administrators in descendant domains can view and edit zones and groups created in ancestor domains. Subdomain users can add and delete interfaces from ancestor zones and groups, but cannot delete or rename the zones/groups.

Object names must be unique within the domain hierarchy. The system may identify a conflict with the name of an object you cannot view in your current domain.

For objects that support grouping, you can group objects in the current domain with objects inherited from ancestor domains.

Object overrides allow you to define device-specific or domain-specific values for certain types of object, including network, port, VLAN tag, and URL. In a multidomain deployment, you can define a default value for an object in an ancestor domain, but allow administrators in descendant domains to add override values for that object.

The Object Manager

You can use the object manager to create and manage objects and object groups.

The object manager displays 20 objects or groups per page. If you have more than 20 of any type of object or group, use the navigation links at the bottom of the page to view additional pages. You can also go to a specific page or click the refresh icon to refresh your view.

By default, the page lists objects and groups alphabetically by name. However, you can sort each type of object or group by any column in the display. You can also filter the objects on the page by name or value.

Editing Objects

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network</td>
</tr>
</tbody>
</table>

In a multidomain deployment, the system displays objects created in the current domain, which you can edit. It also displays objects created in ancestor domains, which in most cases you cannot edit. To view and edit objects in a descendant domain, switch to that domain.

Procedure

**Step 1** Choose Objects > Object Management.

**Step 2** Choose an object type from the list; see Introduction to Reusable Objects, on page 2.

**Step 3** Click the edit icon next to the object you want to edit.
If a view icon ( ) appears instead, the object belongs to an ancestor domain and has been configured not to allow overrides, or you do not have permission to modify the object.

**Step 4** Modify the object settings as desired.

**Step 5** If you are editing a variable set, manage the variables in the set; see Managing Variables, on page 35.

**Step 6** For objects that can be configured to allow overrides:

- If you want to allow overrides for this object, check the Allow Overrides check box; see Allowing Object Overrides, on page 10. You can change this setting only for objects that belong to the current domain.

- If you want to add override values to this object, expand the Override section and click Add; see Adding Object Overrides, on page 10.

**Step 7** Click Save.

**Step 8** If you are editing a variable set, and that set is in use by an access control policy, click Yes to confirm that you want to save your changes.

---

**What to Do Next**

- If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes.

---

**Filtering Objects or Object Groups**

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access Admin/Network Admin</td>
</tr>
</tbody>
</table>

In a multidomain deployment, the system displays objects created in the current and ancestor domains, which you can filter.

**Procedure**

**Step 1** Choose Objects > Object Management.

**Step 2** Enter your filter criteria in the Filter field. The page updates as you type to display matching items.

You can use the following metacharacters:

- The asterisk (*) matches zero or more occurrences of a character.
- The caret (^) matches content at the beginning of a string.
- The dollar sign ($) matches content at the end of a string.
## Sorting Objects

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>

In a multidomain deployment, the system displays objects created in the current domain, which you can edit. It also displays objects created in ancestor domains, which in most cases you cannot edit. To view and edit objects in a descendant domain, switch to that domain.

### Procedure

**Step 1** Choose **Objects > Object Management**.

**Step 2** Click a column heading. To sort in the opposite direction, click the heading again.

## Object Groups

Grouping objects allows you to reference multiple objects with a single configuration. The system allows you to use objects and object groups interchangeably in the web interface. For example, anywhere you would use a port object, you can also use a port object group.

You can group network, port, VLAN tag, URL, and PKI objects. Network object groups can be nested, that is, you can add a network object group to another network object group up to 10 levels.

Objects and object groups of the same type cannot have the same name. In a multidomain deployment, the names of object groups must be unique within the domain hierarchy. Note that the system may identify a conflict with the name of an object group you cannot view in your current domain.

When you edit an object group used in a policy (for example, a network object group used in an access control policy), you must re-deploy the changed configuration for your changes to take effect.

Deleting a group does not delete the objects in the group, just their association with each other. Additionally, you cannot delete a group that is in use in an active policy. For example, you cannot delete a VLAN tag group that you are using in a VLAN condition in a saved access control policy.
Grouping Reusable Objects

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>

In a multidomain deployment, the system displays objects created in the current domain, which you can edit. It also displays objects created in ancestor domains, which in most cases you cannot edit. To view and edit objects in a descendant domain, switch to that domain.

You can group objects in the current domain with objects inherited from ancestor domains.

Procedure

**Step 1** Choose **Objects > Object Management**.

**Step 2** If the object type you want to group is **Network**, **Port**, **URL**, or **VLAN Tag**:

a) Choose the object type from the list of object types.
b) Choose **Add Group** from the **Add [Object Type]** drop-down list.

**Step 3** If the object type you want to group is **Distinguished Name**:

a) Expand the **Distinguished Name** node.
b) Choose **Object Groups**.
c) Click **Add Distinguished Name Group**.

**Step 4** If the object type you want to group is **PKI**:

a) Expand the **PKI** node.
b) Choose one of the following:
   - **Internal CA Groups**
   - **Trusted CA Groups**
   - **Internal Cert Groups**
   - **External Cert Groups**

c) Click the **Add [Object Type] Group** button.

**Step 5** Enter a unique **Name**.

**Step 6** Choose one or more objects from the list, and click **Add**.

You can also:

- Use the filter field 🕵️ to search for existing objects to include, which updates as you type to display matching items. Click the reload icon 🔄 above the search field or click the clear icon ( ✗ ) in the search field to clear the search string.

- Click the add icon ( ✖️ ) to create objects on the fly if no existing objects meet your needs.
Step 7 Optionally for Network, Port, URL, and VLAN Tag groups:
- Enter a Description.
- Check the Allow Overrides check box to allow overrides for this object group; see Allowing Object Overrides, on page 10.

Step 8 Click Save.

What to Do Next
- If an active policy references your object group, deploy configuration changes; see Deploying Configuration Changes.

Object Overrides

An object override allows you to define an alternate value for an object, which the system uses for the devices you specify.

You can create an object whose definition works for most devices, and then use overrides to specify modifications to the object for the few devices that need different definitions. You can also create an object that needs to be overridden for all devices, but its use allows you to create a single policy for all devices. Object overrides allow you to create a smaller set of shared policies for use across devices without giving up the ability to alter policies when needed for individual devices.

For example, you might want to deny ICMP traffic to the different departments in your company, each of which is connected to a different network. You can do this by defining an access control policy with a rule that includes a network object called Departmental Network. By allowing overrides for this object, you can then create overrides on each relevant device that specifies the actual network where that device is connected.

In a multidomain deployment, you can define a default value for an object in an ancestor domain and allow administrators in descendant domains to add override values for that object. For example, a managed security service provider (MSSP) might use a single Firepower Management Center to manage network security for multiple customers. Administrators at the MSSP can define an object in the Global domain for use in all customers' deployments. Administrators for each customer can log into descendant domains to override that object for their organizations. These local administrators cannot view or affect the override values of other customers of the MSSP.

You can target an object override to a specific domain. In this case, the system uses the object override value for all devices in the targeted domain unless you override it at the device level.

From the object manager, you can choose an object that can be overridden and define a list of device-level or domain-level overrides for that object.

You can use object overrides with the following object types only:
- Network
- Port
- VLAN tag
- URL
- SLA Monitor
If you can override an object, the **Override** column appears for the object type in the object manager. Possible values for this column include:

- **Green checkmark** — indicates that you can create overrides for the object and no overrides have been added yet
- **Red X** — indicates that you cannot create overrides for the object
- **Number** — represents a count of the overrides that have been added to that object (for example, "2" indicates two overrides have been added)

## Managing Object Overrides

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access Admin/Network Admin</td>
</tr>
</tbody>
</table>

## Procedure

**Step 1** Choose **Objects > Object Management**.

**Step 2** Choose from the list of object types; see **Introduction to Reusable Objects, on page 2**.

**Step 3** Click the edit icon ( jogador de futebol ) next to the object you want to edit.

If a view icon ( jogador de futebol ) appears instead, the object belongs to an ancestor domain and has been configured not to allow overrides, or you do not have permission to modify the object.

**Step 4** Manage the object overrides:

- **Add**—Add object overrides; see **Adding Object Overrides, on page 10**.
- **Allow**—Allow object overrides; see **Allowing Object Overrides, on page 10**.
- **Delete**—In the object editor, click the delete icon ( jogador de futebol ) next to the override you want to remove.
- **Edit**—Edit object overrides; see **Editing Object Overrides, on page 11**.
Allowing Object Overrides

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>

Procedure

Step 1 In the object editor, check the Allow Overrides check box.
Step 2 Click Save.

What to Do Next

- Add object override values; see Adding Object Overrides, on page 10.

Adding Object Overrides

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>

Before You Begin

- Allow object overrides; see Allowing Object Overrides, on page 10.

Procedure

Step 1 In the object editor, expand the Override section.
Step 2 Click Add.
Step 3 On the Targets tab, choose domains or devices in the Available Devices and Domains list and click Add.
Step 4 On the Override tab, enter a Name.
Step 5 Optionally, enter a Description.
Step 6 Enter an override value.
Example:
For a network object, enter a network value.

Step 7  Click Add.
Step 8  Click Save.

What to Do Next
• If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes.

Editing Object Overrides

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>

You can modify the description and the value of an existing override, but you cannot modify the existing target list. Instead, you must add a new override with new targets, which replaces the existing override.

Procedure

Step 1  In the object editor, expand the Override section.
Step 2  Click the edit icon (-pencil) next to the override you want to modify.
Step 3  Optionally, modify the Description.
Step 4  Modify the override value.
Step 5  Click Save to save the override.
Step 6  Click Save to save the object.

What to Do Next
• If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes.

Network Objects

A network object represents one or more IP addresses. You can use network objects and groups in various places in the system’s web interface, including access control policies, network variables, intrusion rules, identity rules, network discovery rules, event searches, reports, and so on.
When you configure an option that requires a network object, the list is automatically filtered to show only those objects that are valid for the option. For example, some options require host objects, while other options require subnets.

A network object can be one of the following types:

**Host**
- A single IP address.
- IPv4 example:
  - 209.165.200.225
- IPv6 example:
  - 2001:DB8::0DB8:800:200C:417A or 2001:DB8:0:0:0DB8:800:200C:417A

**Network**
- An address block, also known as a subnet.
- IPv4 example:
  - 209.165.200.224/27
- IPv6 example:
  - 2001:DB8:0:CD30::/60

**Address Range**
- A range of IP addresses.
- IPv4 example:
  - 209.165.200.225-209.165.200.250
- IPv6 example:
  - 2001:db8:0:cd30::1-2001:db8:0:cd30::1000

**Group**
- A group of network objects or other network object groups.
- For example:
  - 209.165.200.225
  - 209.165.201.1
  - 209.165.202.129

You can create nested groups by adding one network object group to another network object group. You can nest up to 10 levels of groups.
Creating Network Objects

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network Admin</td>
</tr>
</tbody>
</table>

**Procedure**

**Step 1** Choose **Objects > Object Management**.

**Step 2** Choose **Network** from the list of object types.

**Step 3** Choose **Add Object** from the **Add Network** drop-down menu.

**Step 4** Enter a **Name**.
In a multidomain deployment, object names must be unique within the domain hierarchy. The system may identify a conflict with the name of an object you cannot view in your current domain.

**Step 5** Optionally, enter a **Description**.

**Step 6** In the **Network** field, enter an appropriate value; see **Network Objects**, on page 11.

**Step 7** Manage overrides for the object:
- If you want to allow overrides for this object, check the **Allow Overrides** check box; see **Allowing Object Overrides**, on page 10.
- If you want to add override values to this object, expand the Override section and click **Add**; see **Adding Object Overrides**, on page 10.

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

**What to Do Next**
- If an active policy references your object, deploy configuration changes; see **Deploying Configuration Changes**.

**Port Objects**

Port objects represent different protocols in slightly different ways:

**TCP and UDP**
A port object represents the transport layer protocol, with the protocol number in parentheses, plus an optional associated port or port range. For example: `TCP(6)/22`.
ICMP and ICMPv6 (IPv6-ICMP)

A port object represents the Internet layer protocol plus an optional type and code. For example: ICMP (1):3:3.

You can restrict an ICMP or IPv6-ICMP port object by type and, if applicable, code. For more information on ICMP types and codes, see:

- [http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml](http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml)
- [http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml](http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml)

Other

A port object can represent other protocols that do not use ports.

The Firepower System provides default port objects for well-known ports. You cannot modify or delete these default objects. You can create custom port objects in addition to the default objects.

You can use port objects and groups in various places in the system’s web interface, including access control policies, identity rules, network discovery rules, port variables, and event searches. For example, if your organization uses a custom client that uses a specific range of ports and causes the system to generate excessive and misleading events, you can configure your network discovery policy to exclude monitoring those ports.

When using port objects, observe the following guidelines:

- You cannot add any protocol other than TCP or UDP for source port conditions in access control rules. Also, you cannot mix transport protocols when setting both source and destination port conditions in a rule.

- If you add an unsupported protocol to a port object group used in a source port condition, the rule where it is used does not take affect on the managed device when the configuration is deployed.

- If you create a port object containing both TCP and UDP ports, then add it as a source port condition in a rule, you cannot add a destination port, and vice versa.

### Creating Port Objects

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access Admin/Access Admin/Network Admin</td>
</tr>
</tbody>
</table>
Procedure

**Step 1** Choose **Objects > Object Management**.

**Step 2** Choose **Port** from the list of object types.

**Step 3** Choose **Add Object** from the **Add Port** drop-down list.

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

**Step 5** Choose a **Protocol**.

**Step 6** Depending on the protocol you chose, constrain by **Port**, or choose an ICMP **Type** and **Code**. You can enter ports from 1 to 65535. Use a hyphen to specify a port range. You must constrain the object by port if you chose to match **All** protocols, using the **Other** drop-down list.

**Step 7** Manage overrides for the object:

- If you want to allow overrides for this object, check the **Allow Overrides** check box; see **Allowing Object Overrides**, on page 10.

- If you want to add override values to this object, expand the Override section and click **Add**; see **Adding Object Overrides**, on page 10.

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

**What to Do Next**

- If an active policy references your object, deploy configuration changes; see **Deploying Configuration Changes**.

### Interface Objects: Interface Groups and Security Zones

Interface objects segment your network to help you manage and classify traffic flow. An interface object simply groups interfaces. These groups may span multiple devices; you can also configure multiple interface objects on a single device.

There are two types of interface objects:

- **Security zones**—An interface can belong to only one security zone.

- **Interface groups**—An interface can belong to multiple interface groups (and to one security zone).

You can use interface groups in Firepower Threat Defense NAT policies, prefilter policies, and QoS policies.

Although tunnel zones are not interface objects, you can use them in place of security zones in certain configurations; see **Tunnel Zones and Prefiltering**.

All interfaces in an interface object must be of the same type: all inline, passive, switched, routed, or ASA FirePOWER. After you create an interface object, you cannot change the type of interfaces it contains.

The Interface Objects page of the object manager lists the security zones and interface groups configured on your managed devices. The page also displays the type of interfaces in each interface object, and you can expand each interface object to view which interfaces on which devices belong to each object.
Model-Specific Notes and Warnings

During initial configuration of a 7000 or 8000 Series device, the system creates security zones based on the detection mode you selected for the device. For example, the system creates a Passive zone in passive deployments, while in inline deployments the system creates External and Internal zones. When you register the device to the Firepower Management Center, those security zones are added to the Management Center.

If you modify ASA FirePOWER security contexts, switching from single context mode to multi-context mode or vice versa, the system removes all the device's interfaces from their assigned security zones.

Interface Objects and Multitenancy

In a multidomain deployment, you can create interface objects at any level. An interface object created in an ancestor domain can contain interfaces that reside on devices in different domains. In this situation, subdomain users viewing the ancestor interface object configuration in the object manager can see only the interfaces in their domain.

Unless restricted by role, subdomain users can view and edit interface objects created in ancestor domains. Subdomain users can add and delete interfaces from these interface objects. They cannot, however, delete or rename the interface objects. You can neither view nor edit interface objects created in descendant domains.

Creating Security Zone and Interface Group Objects

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Security Zones: Any</td>
<td>Any</td>
<td>Admin/Access Admin/Network Admin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Interface Groups: Firepower Threat Defense</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Tip

You can create empty interface objects and add interfaces to them later. To add an interface, the interface must have a name. You can also create security zones (but not interface groups) while configuring interfaces in Devices > Device Management.

Before You Begin

- Understand the usage requirements and restrictions for each type of interface object. See Interface Objects: Interface Groups and Security Zones, on page 15.
- Carefully determine the interface objects you need. You cannot change an existing security zone to an interface group or vice-versa; instead you must create a new interface object.
Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Objects &gt; Object Management</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Choose <strong>Interface</strong> from the list of object types.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Add &gt; Security Zone</strong> or <strong>Add &gt; Interface Group</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter a <strong>Name</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Choose an <strong>Interface Type</strong>.</td>
</tr>
<tr>
<td>Step 6</td>
<td>From the <strong>Device &gt; Interfaces</strong> drop-down list, choose a device that contains interfaces you want to add.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Choose one or more interfaces.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Click <strong>Add</strong> to add the interfaces you chose, grouped by device.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

What to Do Next

- If an active policy references your object, deploy configuration changes; see [Deploying Configuration Changes](#).

Tunnel Zones

A *tunnel zone* represents certain types of plaintext, passthrough tunnels that you explicitly tag for special analysis. A tunnel zone is not an interface object, even though you can use it as an interface constraint in some configurations.

For detailed information, see [Tunnel Zones and Prefiltering](#).

Application Filters

System-provided application filters help you perform application control by organizing applications according to basic characteristics: type, risk, business relevance, category, and tags. In the object manager, you can create and manage reusable user-defined application filters based on combinations of the system-provided filters, or on custom combinations of applications. For detailed information, see [Application Conditions (Application Control)](#).

VLAN Tag Objects

Each VLAN tag object you configure represents a VLAN tag or range of tags.

You can group VLAN tag objects. Groups represent multiple objects; using a range of VLAN tags in a single object is not considered a group in this sense.

You can use VLAN tag objects and groups in various places in the system's web interface, including rules and event searches. For example, you could write an access control rule that applies only to a specific VLAN.
Creating VLAN Tag Objects

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin Network Admin</td>
</tr>
</tbody>
</table>

Procedure

Step 1 Choose **Objects** > **Object Management**.
Step 2 Choose **VLAN Tag** from the list of object types.
Step 3 Choose **Add Object** from the **Add VLAN Tag** drop-down list.
Step 4 Enter a **Name**.
Step 5 Enter a **Description**.
Step 6 Enter a value in the **VLAN Tag** field. Use a hyphen to specify a range of VLAN tags.
Step 7 Manage overrides for the object:
   • If you want to allow overrides for this object, check the **Allow Overrides** check box; see **Allowing Object Overrides**, on page 10.
   • If you want to add override values to this object, expand the Override section and click **Add**; see **Adding Object Overrides**, on page 10.
Step 8 Click **Save**.

What to Do Next

• If an active policy references your object, deploy configuration changes; see **Deploying Configuration Changes**.

Security Group Tag Objects

A Security Group Tag (SGT) object specifies a single SGT value. You can use SGT objects in rules to control traffic with SGT attributes that were **not** assigned by Cisco ISE. You cannot group or override SGT objects.

Related Topics

- Autotransition from Custom SGTs to ISE SGTs
- Custom SGT Conditions
- ISE SGT vs Custom SGT Rule Conditions
Creating Security Group Tag Objects

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Control</td>
<td>Any</td>
<td>Global only</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>

Before You Begin

- Disable ISE connections. You cannot create custom SGT objects if you use ISE as an identity source.

Procedure

Step 1 Choose **Objects > Object Management**.
Step 2 Choose **Security Group Tag** from the list of object types.
Step 3 Click **Add Security Group Tag**.
Step 4 Enter a **Name**.
Step 5 Optionally, enter a **Description**.
Step 6 In the **Tag** field, enter a single SGT.
Step 7 Click **Save**.

What to Do Next

- If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes.

URL Objects

Each URL object you configure represents a single URL or IP address. You can use URL objects and groups in various places in the system's web interface, including access control policies and event searches. For example, you could write an access control rule that blocks a specific website.

When creating URL objects, especially if you do not configure SSL inspection to decrypt or block encrypted traffic, keep the following points in mind:

- If you plan to use a URL object to match HTTPS traffic in an access control rule, create the object using the subject common name in the public key certificate used to encrypt the traffic. Also, the system disregards subdomains within the subject common name, so do not include subdomain information. For example, use example.com rather than www.example.com.

- When matching web traffic using access control rules with URL conditions, the system disregards the encryption protocol (HTTP vs HTTPS). In other words, if you block a website, both HTTP and HTTPS traffic to that website is blocked, unless you use an application condition to refine the rule. When creating
a URL object, you do not need to specify the protocol when creating an object. For example, use example.com rather than http://example.com/.

Creating URL Objects

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>

Procedure

**Step 1** Choose Objects > Object Management.
**Step 2** Choose URL from the list of object types.
**Step 3** Choose Add Object from the Add URL drop-down list.
**Step 4** Enter a Name.
In a multidomain deployment, object names must be unique within the domain hierarchy. The system may identify a conflict with the name of an object you cannot view in your current domain.
**Step 5** Optionally, enter a Description.
**Step 6** Enter the URL or IP address.
**Step 7** Manage overrides for the object:
- If you want to allow overrides for this object, check the Allow Overrides check box; see Allowing Object Overrides, on page 10.
- If you want to add override values to this object, expand the Override section and click Add; see Adding Object Overrides, on page 10.
**Step 8** Click Save.

**What to Do Next**
- If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes.

Geolocation Objects

Each geolocation object you configure represents one or more countries or continents that the system has identified as the source or destination of traffic on your monitored network. You can use geolocation objects in various places in the system’s web interface, including access control policies, SSL policies, and event searches. For example, you could write an access control rule that blocks traffic to or from certain countries.
To ensure that you are using up-to-date information to filter your network traffic, Cisco strongly recommends that you regularly update your Geolocation Database (GeoDB).

Creating Geolocation Objects

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>

Procedure

**Step 1** Choose **Objects > Object Management**.

**Step 2** Choose **Geolocation** from the list of object types.

**Step 3** Click **Add Geolocation**.

**Step 4** Enter a **Name**.
In a multidomain deployment, object names must be unique within the domain hierarchy. The system may identify a conflict with the name of an object you cannot view in your current domain.

**Step 5** Check the check boxes for the countries and continents you want to include in your geolocation object. Checking a continent chooses all countries within that continent, as well as any countries that GeoDB updates may add under that continent in the future. Unchecking any country under a continent unchecks the continent. You can choose any combination of countries and continents.

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

What to Do Next

- If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes.

Variable Sets

Variables represent values commonly used in intrusion rules to identify source and destination IP addresses and ports. You can also use variables in intrusion policies to represent IP addresses in rule suppressions, adaptive profile updates, and dynamic rule states.

**Tip**
Preprocessor rules can trigger events regardless of the hosts defined by network variables used in intrusion rules.

You use variable sets to manage, customize, and group your variables. You can use the default variable set provided by the system or create your own custom sets. Within any set you can modify predefined default variables and add and modify user-defined variables.
Most of the shared object rules and standard text rules that the Firepower System provides use predefined default variables to define networks and port numbers. For example, the majority of the rules use the variable $HOME_NET to specify the protected network and the variable $EXTERNAL_NET to specify the unprotected (or outside) network. In addition, specialized rules often use other predefined variables. For example, rules that detect exploits against web servers use the $HTTP_SERVERS and $HTTP_PORTS variables.

Rules are more effective when variables more accurately reflect your network environment. At a minimum, you should modify default variables in the default set. By ensuring that a variable such as $HOME_NET correctly defines your network and $HTTP_SERVERS includes all web servers on your network, processing is optimized and all relevant systems are monitored for suspicious activity.

To use your variables, you link variable sets to intrusion policies associated with access control rules or with the default action of an access control policy. By default, the default variable set is linked to all intrusion policies used by access control policies.

Adding a variable to any set adds it to all sets; that is, each variable set is a collection of all variables currently configured on your system. Within any variable set, you can add user-defined variables and customize the value of any variable.

Initially, the Firepower System provides a single, default variable set comprised of predefined default values. Each variable in the default set is initially set to its default value, which for a predefined variable is the value set by the Cisco Talos Security Intelligence and Research Group (Talos) and provided in rule updates.

Although you can leave predefined default variables configured to their default values, Cisco recommends that you modify a subset of predefined variables.

You could work with variables only in the default set, but in many cases you can benefit most by adding one or more custom sets, configuring different variable values in different sets, and perhaps even adding new variables.

When using multiple sets, it is important to remember that the current value of any variable in the default set determines the default value of the variable in all other sets.

When you select Variable Sets on the Object Manager page, the object manager lists the default variable set and any custom sets you created.

On a freshly installed system, the default variable set is comprised only of the default variables predefined by Cisco.

Each variable set includes the default variables provided by the system and all custom variables you have added from any variable set. Note that you can edit the default set, but you cannot rename or delete the default set.

In a multidomain deployment, the system generates a default variable set for each subdomain.

---

**Caution**

Importing an access control or an intrusion policy overwrites existing default variables in the default variable set with the imported default variables. If your existing default variable set contains a custom variable not present in the imported default variable set, the unique variable is preserved.

---

**Related Topics**

- Managing Variables, on page 35
- Managing Variable Sets, on page 34
Variable Sets in Intrusion Policies

By default, the Firepower System links the default variable set to all intrusion policies used in an access control policy. When you deploy an access control policy that uses an intrusion policy, intrusion rules that you have enabled in the intrusion policy use the variable values in the linked variable set.

When you modify a custom variable set used by an intrusion policy in an access control policy, the system reflects the status for that policy as out-of-date on the Access Control Policy page. You must re-deploy the access control policy to implement changes in your variable set. When you modify the default set, the system reflects the status of all access control policies that use intrusion policies as out-of-date, and you must re-deploy all access control policies to implement your changes.

Variables

Variables belong to one of the following categories:

Default Variables

Variables provided by the Firepower System. You cannot rename or delete a default variable, and you cannot change its default value. However, you can create a customized version of a default variable.

Customized Variables

Variables you create. These variables can include:

• customized default variables

When you edit the value for a default variable, the system moves the variable from the Default Variables area to the Customized Variables area. Because variable values in the default set determine the default values of variables in custom sets, customizing a default variable in the default set modifies the default value of the variable in all other sets.

• user-defined variables

You can add and delete your own variables, customize their values within different variable sets, and reset customized variables to their default values. When you reset a user-defined variable, it remains in the Customized Variables area.

User-defined variables can be one of the following types:

• network variables specify the IP addresses of hosts in your network traffic.

• port variables specify TCP or UDP ports in network traffic, including the value any for either type.

For example, if you create custom standard text rules, you might also want to add your own user-defined variables to more accurately reflect your traffic or as shortcuts to simplify the rule creation process. Alternatively, if you create a rule that you want to inspect traffic in the “demilitarized zone” (or DMZ) only, you can create a variable named $DMZ whose value lists the server IP addresses that are exposed. You can then use the $DMZ variable in any rule written for this zone.
Advanced Variables

Variables provided by the Firepower System under specific conditions. These variables have a very limited deployment.

Predefined Default Variables

By default, the Firepower System provides a single default variable set, which is comprised of predefined default variables. The Cisco Talos Security Intelligence and Research Group (Talos) uses rule updates to provide new and updated intrusion rules and other intrusion policy elements, including default variables.

Because many intrusion rules provided by the system use predefined default variables, you should set appropriate values for these variables. Depending on how you use variable sets to identify traffic on your network, you can modify the values for these default variables in any or all variable sets.

Caution

Importing an access control or an intrusion policy overwrites existing default variables in the default variable set with the imported default variables. If your existing default variable set contains a custom variable not present in the imported default variable set, the unique variable is preserved.

The following table describes the variables provided by the system and indicates which variables you typically would modify. For assistance determining how to tailor variables to your network, contact Professional Services or Support.
### Table 1: System-Provided Variables

<table>
<thead>
<tr>
<th>Variable Name</th>
<th>Description</th>
<th>Modify?</th>
</tr>
</thead>
<tbody>
<tr>
<td>$AIM_SERVERS</td>
<td>Defines known AOL Instant Messenger (AIM) servers, and is used in chat-based rules and rules that look for AIM exploits.</td>
<td>Not required.</td>
</tr>
<tr>
<td>$DNS_SERVERS</td>
<td>Defines Domain Name Service (DNS) servers. If you create a rule that affects DNS servers specifically, you can use the $DNS_SERVERS variable as a destination or source IP address.</td>
<td>Not required in current rule set.</td>
</tr>
<tr>
<td>$EXTERNAL_NET</td>
<td>Defines the network that the Firepower System views as the unprotected network, and is used in many rules to define the external network.</td>
<td>Yes, you should adequately define $HOME_NET and then exclude $HOME_NET as the value for $EXTERNAL_NET.</td>
</tr>
<tr>
<td>$FILE_DATA_PORTS</td>
<td>Defines non-encrypted ports used in intrusion rules that detect files in a network stream.</td>
<td>Not required.</td>
</tr>
<tr>
<td>$FTP_PORTS</td>
<td>Defines the ports of FTP servers on your network, and is used for FTP server exploit rules.</td>
<td>Yes, if your FTP servers use ports other than the default ports (you can view the default ports in the web interface).</td>
</tr>
<tr>
<td>$GTP_PORTS</td>
<td>Defines the data channel ports where the packet decoder extracts the payload inside a GTP (General Packet Radio Service [GPRS] Tunneling Protocol) PDU.</td>
<td>Not required.</td>
</tr>
<tr>
<td>$HOME_NET</td>
<td>Defines the network that the associated intrusion policy monitors, and is used in many rules to define the internal network.</td>
<td>Yes, to include the IP addresses for your internal network.</td>
</tr>
<tr>
<td>$HTTP_PORTS</td>
<td>Defines the ports of web servers on your network, and is used for web server exploit rules.</td>
<td>Yes, if your web servers use ports other than the default ports (you can view the default ports in the web interface).</td>
</tr>
<tr>
<td>$HTTP_SERVERS</td>
<td>Defines the web servers on your network. Used in web server exploit rules.</td>
<td>Yes, if you run HTTP servers.</td>
</tr>
<tr>
<td>$ORACLE_PORTS</td>
<td>Defines Oracle database server ports on your network, and is used in rules that scan for attacks on Oracle databases.</td>
<td>Yes, if you run Oracle servers.</td>
</tr>
<tr>
<td>$SHELLCODE_PORTS</td>
<td>Defines the ports you want the system to scan for shell code exploits, and is used in rules that detect exploits that use shell code.</td>
<td>Not required.</td>
</tr>
<tr>
<td>$SIP_PORTS</td>
<td>Defines the ports of SIP servers on your network, and is used for SIP exploit rules.</td>
<td>Not required.</td>
</tr>
<tr>
<td>$SIP_SERVERS</td>
<td>Defines SIP servers on your network, and is used in rules that address SIP-targeted exploits.</td>
<td></td>
</tr>
<tr>
<td>Variable Name</td>
<td>Description</td>
<td>Modify?</td>
</tr>
<tr>
<td>----------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>$SMTP_SERVERS</td>
<td>Defines SMTP servers on your network, and is used in rules that address</td>
<td>Yes, if you run SMTP servers.</td>
</tr>
<tr>
<td></td>
<td>exploits that target mail servers.</td>
<td></td>
</tr>
<tr>
<td>$SNMP_SERVERS</td>
<td>Defines SNMP servers on your network, and is used in rules that scan</td>
<td>Yes, if you run SNMP servers.</td>
</tr>
<tr>
<td></td>
<td>for attacks on SNMP servers.</td>
<td></td>
</tr>
<tr>
<td>$SNORT_BPF</td>
<td>Identifies a legacy advanced variable that appears only when it existed</td>
<td>No, you can only view or delete this variable. You cannot edit it or</td>
</tr>
<tr>
<td></td>
<td>on your system in a Firepower System software release before Version</td>
<td>recover it after deleting it.</td>
</tr>
<tr>
<td></td>
<td>5.3.0 that you subsequently upgraded to Version 5.3.0 or greater.</td>
<td></td>
</tr>
<tr>
<td>$SQL_SERVERS</td>
<td>Defines database servers on your network, and is used in rules that address</td>
<td>Yes, if you run SQL servers.</td>
</tr>
<tr>
<td></td>
<td>database-targeted exploits.</td>
<td></td>
</tr>
<tr>
<td>$SSH_PORTS</td>
<td>Defines the ports of SSH servers on your network, and is used for SSH</td>
<td>Yes, if your SSH servers use ports other than the default port (you</td>
</tr>
<tr>
<td></td>
<td>server exploit rules.</td>
<td>can view the default ports in the web interface).</td>
</tr>
<tr>
<td>$SSH_SERVERS</td>
<td>Defines SSH servers on your network, and is used in rules that address</td>
<td>Yes, if you run SSH servers.</td>
</tr>
<tr>
<td></td>
<td>SSH-targeted exploits.</td>
<td></td>
</tr>
<tr>
<td>$TELNET_SERVERS</td>
<td>Defines known Telnet servers on your network, and is used in rules that</td>
<td>Yes, if you run Telnet servers.</td>
</tr>
<tr>
<td></td>
<td>address Telnet server-targeted exploits.</td>
<td></td>
</tr>
<tr>
<td>$USER_CONF</td>
<td>Provides a general tool that allows you to configure one or more features</td>
<td>No, only as instructed in a feature description or with the guidance of</td>
</tr>
<tr>
<td></td>
<td>not otherwise available via the web interface.</td>
<td>Support.</td>
</tr>
<tr>
<td></td>
<td>Conflicting or duplicate $USER_CONF configurations will halt the system.</td>
<td></td>
</tr>
</tbody>
</table>

**Network Variables**

Network variables represent IP addresses you can use in intrusion rules that you enable in an intrusion policy and in intrusion policy rule suppressions, dynamic rule states, and adaptive profile updates. Network variables differ from network objects and network object groups in that network variables are specific to intrusion policies and intrusion rules, whereas you can use network objects and groups to represent IP addresses in various places in the system's web interface, including access control policies, network variables, intrusion rules, network discovery rules, event searches, reports, and so on.
You can use network variables in the following configurations to specify the IP addresses of hosts on your network:

- **intrusion rules**—Intrusion rule **Source IPs** and **Destination IPs** header fields allow you to restrict packet inspection to the packets originating from or destined to specific IP addresses.

- **suppressions**—The **Network** field in source or destination intrusion rule suppressions allows you to suppress intrusion event notifications when a specific IP address or range of IP addresses triggers an intrusion rule or preprocessor.

- **dynamic rule states**—The **Network** field in source or destination dynamic rule states allows you to detect when too many matches for an intrusion rule or preprocessor rule occur in a given time period.

- **adaptive profile updates**—When you enable adaptive profile updates, the **Networks** field identifies hosts where you want to improve reassembly of packet fragments and TCP streams in passive deployments.

When you use variables in the fields identified in this section, the variable set you link to an intrusion policy determines the variable values in the network traffic handled by an access control policy that uses the intrusion policy.

You can add any combination of the following network configurations to a variable:

- any combination of network variables, network objects, and network object groups that you select from the list of available networks

- individual network objects that you add from the New Variable or Edit Variable page, and can then add to your variable and to other existing and future variables

- literal, single IP addresses or address blocks

You can list multiple literal IP addresses and address blocks by adding each individually. You can list IPv4 and IPv6 addresses and address blocks alone or in any combination. When specifying IPv6 addresses, you can use any addressing convention defined in RFC 4291.

The default value for included networks in any variable you add is the word **any**, which indicates any IPv4 or IPv6 address. The default value for excluded networks is **none**, which indicates no network. You can also specify the address :: in a literal value to indicate any IPv6 address in the list of included networks, or no IPv6 addresses in the list of exclusions.

Adding networks to the excluded list negates the specified addresses and address blocks. That is, you can match any IP address with the exception of the excluded IP address or address blocks.

For example, excluding the literal address 192.168.1.1 specifies any IP address other than 192.168.1.1, and excluding 2001:db8:ca2e::fa4c specifies any IP address other than 2001:db8:ca2e::fa4c.

You can exclude any combination of networks using literal or available networks. For example, excluding the literal values 192.168.1.1 and 192.168.1.5 includes any IP address other than 192.168.1.1 or 192.168.1.5. That is, the system interprets this as “not 192.168.1.1 and not 192.168.1.5,” which matches any IP address other than those listed between brackets.

Note the following points when adding or editing network variables:

- You cannot logically exclude the value **any** which, if excluded, would indicate no address. For example, you cannot add a variable with the value **any** to the list of excluded networks.
• Network variables identify traffic for the specified intrusion rule and intrusion policy features. Note that preprocessor rules can trigger events regardless of the hosts defined by network variables used in intrusion rules.

• Excluded values must resolve to a subset of included values. For example, you cannot include the address block 192.168.5.0/24 and exclude 192.168.6.0/24.

Port Variables

Port variables represent TCP and UDP ports you can use in the Source Port and Destination Port header fields in intrusion rules that you enable in an intrusion policy. Port variables differ from port objects and port object groups in that port variables are specific to intrusion rules. You can create port objects for protocols other than TCP and UDP, and you can use port objects in various places in the system’s web interface, including port variables, access control policies, network discovery rules, and event searches. You can use port variables in the intrusion rule Source Port and Destination Port header fields to restrict packet inspection to packets originating from or destined to specific TCP or UDP ports.

When you use variables in these fields, the variable set you link to the intrusion policy associated with an access control rule or policy determines the values for these variables in the network traffic where you deploy the access control policy.

You can add any combination of the following port configurations to a variable:

• any combination of port variables and port objects that you select from the list of available ports
  Note that the list of available ports does not display port object groups, and you cannot add these to variables.

• individual port objects that you add from the New Variable or Edit Variable page, and can then add to your variable and to other existing and future variables
  Only TCP and UDP ports, including the value any for either type, are valid variable values. If you use the new or edit variables page to add a valid port object that is not a valid variable value, the object is added to the system but is not displayed in the list of available objects. When you use the object manager to edit a port object that is used in a variable, you can only change its value to a valid variable value.

• single, literal port values and port ranges
  You must separate port ranges with a dash (-). Port ranges indicated with a colon (:) are supported for backward compatibility, but you cannot use a colon in port variables that you create.
  You can list multiple literal port values and ranges by adding each individually in any combination.

Note the following points when adding or editing port variables:

• The default value for included ports in any variable you add is the word any, which indicates any port or port range. The default value for excluded ports is none, which indicates no ports.

Tip

To create a variable with the value any, name and save the variable without adding a specific value.

• You cannot logically exclude the value any which, if excluded, would indicate no ports. For example, you cannot save a variable set when you add a variable with the value any to the list of excluded ports.
• Adding ports to the excluded list negates the specified ports and port ranges. That is, you can match any port with the exception of the excluded ports or port ranges.

• Excluded values must resolve to a subset of included values. For example, you cannot include the port range 10-50 and exclude port 60.

Advanced Variables

Advanced variables allow you to configure features that you cannot otherwise configure via the web interface. The Firepower System currently provides only two advanced variables, and you can only edit the USER_CONF advanced variable.

USER_CONF

USER_CONF provides a general tool that allows you to configure one or more features not otherwise available via the web interface.

Caution

Do not use the advanced variable USER_CONF to configure an intrusion policy feature unless you are instructed to do so in the feature description or by Support. Conflicting or duplicate configurations will halt the system.

When editing USER_CONF, you can type up to 4096 total characters on a single line; the line wraps automatically. You can include any number of valid instructions or lines until you reach the 8192 maximum character length for a variable or a physical limit such as disk space. Use the backslash (\) line continuation character after any complete argument in a command directive.

Resetting USER_CONF empties it.

SNORT_BPF

SNORT_BPF is a legacy advanced variable that appears only when it was configured on your system in a Firepower System software release before Version 5.3.0 that you subsequently upgraded to Version 5.3.0 or greater. You can only view or delete this variable. You cannot edit it or recover it after deleting it.

This variable allowed you to apply a Berkeley Packet Filter (BPF) to filter traffic before it reached the system. You should now use access control rules instead of this variable to enforce the filtering once offered by SNORT_BPF. This variable appears only with configurations that existed before system upgrade.

Variable Reset

You can reset a variable to its default value on the variable set new or edit variables page. The following table summarizes the basic principles of resetting variables.

Table 2: Variable Reset Values

<table>
<thead>
<tr>
<th>Resetting this variable type...</th>
<th>In this set type...</th>
<th>Resets it to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>default</td>
<td>the rule update value</td>
</tr>
<tr>
<td>user-defined</td>
<td>default</td>
<td>any</td>
</tr>
</tbody>
</table>
Resets it to... In this set type... Resets it to...

| default or user-defined | custom | the current default set value (modified or unmodified) |

Resetting a variable in a custom set simply resets it to the current value for that variable in the default set. Conversely, resetting or modifying the value of a variable in the default set always updates the default value of that variable in all custom sets. When the reset icon is grayed out, indicating that you cannot reset the variable, this means that the variable has no customized value in that set. Unless you have customized the value for a variable in a custom set, a change to the variable in the default set updates the value used in any intrusion policy where you have linked the variable set.

**Note**

It is good practice when you modify a variable in the default set to assess how the change affects any intrusion policy that uses the variable in a linked custom set, especially when you have not customized the variable value in the custom set.

You can hover your pointer over the reset icon (谤) in a variable set to see the reset value. When the customized value and the reset value are the same, this indicates one of the following:

- you are in the custom or default set where you added the variable with the value *any*
- you are in the custom set where you added the variable with an explicit value and elected to use the configured value as the default value

**Adding Variables to Sets**

Adding a variable to a variable set adds it to all other sets. When you add a variable from a custom set, you must choose whether to use the configured value as the customized value in the default set:

- If you **do use** the configured value (for example, 192.168.0.0/16), the variable is added to the default set using the configured value as a customized value with a default value of *any*. Because the current value in the default set determines the default value in other sets, the initial, default value in other custom sets is the configured value (which in the example is 192.168.0.0/16).
- If you **do not use** the configured value, the variable is added to the default set using only the default value *any* and, consequently, the initial, default value in other custom sets is *any*.

**Example: Adding User-Defined Variables to Default Sets**

The following diagram illustrates set interactions when you add the user-defined variable *Var1* to the default set with the value 192.168.1.0/24.
You can customize the value of Var1 in any set. In Custom Set 2 where Var1 has not been customized, its value is 192.168.1.0/24. In Custom Set 1 the customized value 192.168.2.0/24 of Var1 overrides the default value. Resetting a user-defined variable in the default set resets its default value to any in all sets.

It is important to note in this example that, if you do not update Var1 in Custom Set 2, further customizing or resetting Var1 in the default set consequently updates the current, default value of Var1 in Custom Set 2, thereby affecting any intrusion policy linked to the variable set.

Although not shown in the example, note that interactions between sets are the same for user-defined variables and default variables except that resetting a default variable in the default set resets it to the value configured by Cisco in the current rule update.

Example: Adding User-Defined Variables to Custom Sets

The next two examples illustrate variable set interactions when you add a user-defined variable to a custom set. When you save the new variable, you are prompted whether to use the configured value as the default value for other sets. In the following example, you elect to use the configured value.

Note that, except for the origin of Var1 from Custom Set 1, this example is identical to the example above where you added Var1 to the default set. Adding the customized value 192.168.1.0/24 for Var1 to Custom Set 1 copies the value to the default set as a customized value with a default value of any. Thereafter, Var1 values and interactions are the same as if you had added Var1 to the default set. As with the previous example, keep in mind that further customizing or resetting Var1 in the default set consequently updates the current, default value of Var1 in Custom Set 2, thereby affecting any intrusion policy linked to the variable set.

In the next example, you add Var1 with the value 192.168.1.0/24 to Custom Set 1 as in the previous example, but you elect not to use the configured value of Var1 as the default value in other sets.
This approach adds `Var1` to all sets with a default value of `any`. After adding `Var1`, you can customize its value in any set. An advantage of this approach is that, by not initially customizing `Var1` in the default set, you decrease your risk of customizing the value in the default set and thus inadvertently changing the current value in a set such as Custom Set 2 where you have not customized `Var1`.

**Nesting Variables**

You can nest variables so long as the nesting is not circular. Nested, negated variables are not supported.

**Valid Nested Variables**

In this example, SMTP_SERVERS, HTTP_SERVERS, and OTHER_SERVERS are valid nested variables.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Type</th>
<th>Included Networks</th>
<th>Excluded Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP_SERVERS</td>
<td>customized default</td>
<td>10.1.1.1</td>
<td>—</td>
</tr>
<tr>
<td>HTTP_SERVERS</td>
<td>customized default</td>
<td>10.1.1.2</td>
<td>—</td>
</tr>
<tr>
<td>OTHER_SERVERS</td>
<td>user-defined</td>
<td>10.2.2.0/24</td>
<td>—</td>
</tr>
<tr>
<td>HOME_NET</td>
<td>customized default</td>
<td>10.1.1.0/24</td>
<td>SMTP_SERVERS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OTHER_SERVERS</td>
<td>HTTP_SERVERS</td>
</tr>
</tbody>
</table>

**An Invalid Nested Variable**

In this example, HOME_NET is an invalid nested variable because the nesting of HOME_NET is circular; that is, the definition of OTHER_SERVERS includes HOME_NET, so you would be nesting HOME_NET in itself.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Type</th>
<th>Included Networks</th>
<th>Excluded Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP_SERVERS</td>
<td>customized default</td>
<td>10.1.1.1</td>
<td>—</td>
</tr>
<tr>
<td>HTTP_SERVERS</td>
<td>customized default</td>
<td>10.1.1.2</td>
<td>—</td>
</tr>
<tr>
<td>OTHER_SERVERS</td>
<td>user-defined</td>
<td>10.2.2.0/24</td>
<td>HOME_NET</td>
</tr>
<tr>
<td>HOME_NET</td>
<td></td>
<td>10.1.1.0/24</td>
<td>SMTP_SERVERS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OTHER_SERVERS</td>
<td>HTTP_SERVERS</td>
</tr>
</tbody>
</table>
### An Unsupported Nested, Negated Variable

Because nested, negated variables are not supported, you cannot use the variable `NONCORE_NET` as shown in this example to represent IP addresses that are outside of your protected networks.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Type</th>
<th>Included Networks</th>
<th>Excluded Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOME_NET</td>
<td>customized default</td>
<td>10.1.0.0/16</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.2.0.0/16</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.3.0.0/16</td>
<td></td>
</tr>
<tr>
<td>EXTERNAL_NET</td>
<td>customized default</td>
<td></td>
<td>HOME_NET</td>
</tr>
<tr>
<td>DMZ_NET</td>
<td>user-defined</td>
<td>10.4.0.0/16</td>
<td></td>
</tr>
<tr>
<td>NOT_DMZ_NET</td>
<td>user-defined</td>
<td></td>
<td>DMZ_NET</td>
</tr>
<tr>
<td>NONCORE_NET</td>
<td>user-defined</td>
<td>EXTERNAL_NET</td>
<td>NOT_DMZ_NET</td>
</tr>
</tbody>
</table>

### Alternative to an Unsupported Nested, Negated Variable

As an alternative to the example above, you could represent IP addresses that are outside of your protected networks by creating the variable `NONCORE_NET` as shown in this example.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Type</th>
<th>Included Networks</th>
<th>Excluded Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOME_NET</td>
<td>customized default</td>
<td>10.1.0.0/16</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.2.0.0/16</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.3.0.0/16</td>
<td></td>
</tr>
<tr>
<td>DMZ_NET</td>
<td>user-defined</td>
<td>10.4.0.0/16</td>
<td></td>
</tr>
<tr>
<td>NONCORE_NET</td>
<td>user-defined</td>
<td></td>
<td>HOME_NET</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DMZ_NET</td>
</tr>
</tbody>
</table>
Managing Variable Sets

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat</td>
<td>Protection</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network Admin</td>
</tr>
</tbody>
</table>

In a multidomain deployment, the system displays objects created in the current domain, which you can edit. It also displays objects created in ancestor domains, which in most cases you cannot edit. To view and edit objects in a descendant domain, switch to that domain.

Procedure

**Step 1** Choose Objects > Object Management.
**Step 2** Choose Variable Set from the list of object types.
**Step 3** Manage your variable sets:

- **Add** — If you want to add a custom variable set, click Add Variable Set; see Creating Variable Sets, on page 34.

- **Delete** — If you want to delete a custom variable set, click the delete icon ( ) next to the variable set, then click Yes. You cannot delete the default variable set or variable sets belonging to ancestor domains.

  **Note** Variables created in a variable set you delete are not deleted or otherwise affected in other sets.

- **Edit** — If you want to edit a variable set, click the edit icon ( ) next to the variable set you want to modify; see Editing Objects, on page 4.

- **Filter** — If you want to filter variable sets by name, begin entering a name; as you type, the page refreshes to display matching names. If you want to clear name filtering, click the clear icon ( ) in the filter field.

- **Manage Variables** — To manage the variables included in variable sets, see Managing Variables, on page 35.

Creating Variable Sets

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network Admin</td>
</tr>
</tbody>
</table>
Procedure

Step 1  Choose Objects > Object Management.
Step 2  Choose Variable Set from the list of object types.
Step 3  Click Add Variable Set.
Step 4  Enter a Name.
   In a multidomain deployment, object names must be unique within the domain hierarchy. The system may identify a conflict with the name of an object you cannot view in your current domain.
Step 5  Optionally, enter a Description.
Step 6  Manage the variables in the set; see Managing Variables, on page 35.
Step 7  Click Save.

What to Do Next

• If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes.

Managing Variables

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat</td>
<td>Protection</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>

In a multidomain deployment, the system displays objects created in the current domain, which you can edit. It also displays objects created in ancestor domains, which in most cases you cannot edit. To view and edit objects in a descendant domain, switch to that domain.

Procedure

Step 1  Choose Objects > Object Management.
Step 2  Choose Variable Set from the list of object types.
Step 3  Click the edit icon (ред) next to the variable set you want to edit.
   If a view icon (вид) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.
Step 4  Manage your variables:
   • Display — If you want to display the complete value for a variable, hover your pointer over the value in the Value column next to the variable.
   • Add — If you want to add a variable, click Add; see Adding Variables, on page 36.
Delete — Click the delete icon (🗑️) next to the variable. If you have saved the variable set since adding the variable, click Yes to confirm that you want to delete the variable.
You cannot delete the following:

- default variables
- user-defined variables that are used by intrusion rules or other variables
- variables belonging to ancestor domains

Edit — Click the edit icon (📝) next to the variable you want to edit; see Editing Variables, on page 37.

Reset — If you want to reset a modified variable to its default value, click the reset icon (🪤) next to a modified variable. If the reset icon is dimmed, one of the following is true:

- The current value is already the default value.
- The configuration belongs to an ancestor domain.

Tip Hover your pointer over an active reset icon to display the default value.

Step 5 Click Save to save the variable set. If the variable set is in use by an access control policy, click Yes to confirm that you want to save your changes.
Because the current value in the default set determines the default value in all other sets, modifying or resetting a variable in the default set changes the current value in other sets where you have not customized the default value.

What to Do Next

- If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes.

Adding Variables

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat</td>
<td>Protection</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>
Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the variable set editor, click Add.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Enter a unique variable Name.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the Type drop-down list, choose either Network or Port.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Specify values for the variable:</td>
</tr>
<tr>
<td></td>
<td>• If you want to move items from the list of available networks or ports to the list of included or excluded items, you can choose one or more items and then drag and drop, or click Include or Exclude.</td>
</tr>
<tr>
<td></td>
<td>Tip  If addresses or ports in the included and excluded lists for a network or port variable overlap, excluded addresses or ports take precedence.</td>
</tr>
<tr>
<td></td>
<td>• Enter a single literal value, then click Add. For network variables, you can enter a single IP address or address block. For port variables you can add a single port or port range, separating the upper and lower values with a hyphen (-). Repeat this step as needed to enter multiple literal values.</td>
</tr>
<tr>
<td></td>
<td>• If you want to remove an item from the included or excluded lists, click the delete icon (Trash) next to the item.</td>
</tr>
<tr>
<td>Note</td>
<td>The list of items to include or exclude can be comprised of any combination of literal strings and existing variables, objects, and network object groups in the case of network variables.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Save to save the variable. If you are adding a new variable from a custom set, you have the following options:</td>
</tr>
<tr>
<td></td>
<td>• Click Yes to add the variable using the configured value as the customized value in the default set and, consequently, the default value in other custom sets.</td>
</tr>
<tr>
<td></td>
<td>• Click No to add the variable as the default value of any in the default set and, consequently, in other custom sets.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click Save to save the variable set. Your changes are saved, and any access control policy the variable set is linked to displays an out-of-date status.</td>
</tr>
</tbody>
</table>

What to Do Next

• If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes.

Editing Variables

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat</td>
<td>Protection</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access Admin/Network Admin</td>
</tr>
</tbody>
</table>
In a multidomain deployment, the system displays objects created in the current domain, which you can edit. It also displays objects created in ancestor domains, which in most cases you cannot edit. To view and edit objects in a descendant domain, switch to that domain.

You can edit both custom and default variables.

You cannot change the **Name** or **Type** values in an existing variable.

**Procedure**

**Step 1**
In the variable set editor, click the edit icon (éd) next to the variable you want to modify.

If a view icon (ê) appears instead, the object belongs to an ancestor domain, or you do not have permission to modify the object.

**Step 2**
Modify the variable:

- If you want to move items from the list of available networks or ports to the list of included or excluded items, you can select one or more items and then drag and drop, or click **Include** or **Exclude**.

  **Tip**
  If addresses or ports in the included and excluded lists for a network or port variable overlap, excluded addresses or ports take precedence.

- Enter a single literal value, then click **Add**. For network variables, you can enter a single IP address or address block. For port variables you can add a single port or port range, separating the upper and lower values with a hyphen (-). Repeat this step as needed to enter multiple literal values.

- If you want to remove an item from the included or excluded lists, click the delete icon (éd) next to the item.

  **Note**
  The list of items to include or exclude can be comprised of any combination of literal strings and existing variables, objects, and network object groups in the case of network variables.

**Step 3**
Click **Save** to save the variable.

**Step 4**
Click **Save** to save the variable set. If the variable set is in use by an access control policy, click **Yes** to confirm that you want to save your changes. Your changes are saved, and any access control policy the variable set is linked to displays an out-of-date status.

**What to Do Next**

- If an active policy references your object, deploy configuration changes; see *Deploying Configuration Changes*.

---

**Security Intelligence Lists and Feeds**

Security Intelligence *lists* and *feeds* help you quickly filter traffic by collecting:

- IP address and address blocks—Use in access control policies to blacklist and whitelist as part of Security Intelligence.
- Domain Names—Use in DNS policies to blacklist and whitelist as part of Security Intelligence.
- **URLs**—Use in access control policies to blacklist and whitelist as part of Security Intelligence. You can also use URL lists in access control and QoS rules, whose analysis and traffic handling phases occur after Security Intelligence.

**Lists**

A list is a static collection that you manage manually.

By default, access control and DNS policies use Global blacklists and whitelists as part of Security Intelligence. **Whitelist Now** and **Blacklist Now** actions allow you to build and implement these lists without redeploying; see Blacklist Now, Whitelist Now, and Global Lists, on page 40.

Custom lists can augment and fine-tune feeds and the Global lists, although implementing custom lists requires redeploy.

**Feeds**

A feed is a dynamic collection that updates on an interval over HTTP or HTTPS.

The regularly updated Cisco Intelligence Feed allows you to filter network traffic based on the latest threat intelligence from Talos. You can also use third-party feeds. Or, with a custom internal feed, you could easily maintain an enterprise-wide blacklist in a large deployment with multiple Firepower Management Centers.

When the system updates a feed, although it may take a few minutes for your changes to propagate, you do not have to redeploy. If you want strict control over when the system updates a feed from the Internet, you can disable automatic updates for that feed. However, automatic updates ensure the most up-to-date, relevant data.

The system does **not** perform peer SSL certificate verification when downloading custom feeds, nor does the system support the use of certificate bundles or self-signed certificates to verify the remote peer.

**List and Feed Formatting**

Each list or feed must be a simple text file no larger than 500MB. List files must have the .txt extension. Include one entry or comment per line: one IP address, one URL, one domain name.

The number of entries you can include is limited by the maximum size of the file. For example, a URL list with no comments and an average URL length of 100 characters (including Punycode or percent Unicode representations and newlines) can contain more than 5.24 million entries.

In a DNS list entry, you can specify an asterisk (*) wildcard character for a domain label. All labels match the wildcard. For example, an entry of www.example.* matches both www.example.com and www.example.co.

If you add comment lines within the source file, they must start with the pound (#) character. If you upload a source file with comments, the system removes your comments during upload. Source files you download contain all your entries without your comments.

If the system downloads a corrupt feed or a feed with no recognizable entries, the system continues using the old feed data (unless it is the first download). However, if the system can recognize even one entry in the feed, it uses the entries it can recognize.
Security Intelligence Object Quick Reference

<table>
<thead>
<tr>
<th>Object Type</th>
<th>Edit Capabilities</th>
<th>Requires Redeploy After Edit?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default (but custom-populated) whitelists and blacklists: Global, descendant, and domain-specific</td>
<td>Add entries using the context menu. Delete entries using the object manager.</td>
<td>No after adding entries. Yes after deleting entries.</td>
</tr>
<tr>
<td>Custom whitelists and blacklists</td>
<td>Upload new and replacement lists using the object manager.</td>
<td>Yes</td>
</tr>
<tr>
<td>System-provided Intelligence Feeds</td>
<td>Disable or change update frequency using the object manager.</td>
<td>No</td>
</tr>
<tr>
<td>Custom feeds</td>
<td>Fully modify using the object manager.</td>
<td>No</td>
</tr>
<tr>
<td>Sinkhole</td>
<td>Fully modify using the object manager.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Blacklist Now, Whitelist Now, and Global Lists

The Firepower Management Center context menu (see The Context Menu) allows you to quickly blacklist and whitelist with Security Intelligence. For example, if you notice a set of routable IP addresses in intrusion events associated with exploit attempts, you can immediately blacklist those IP addresses. Although it may take a few minutes for your changes to propagate, you do not have to redeploy.

**Blacklist Now** and **Whitelist Now** context-menu options are available on IP address, URL, and DNS request hotspots. Blacklisting or whitelisting with the context menu adds the chosen item to the appropriate default Global list. By default, Access control and DNS policies use these Global lists, which apply to all security zones. You can opt not to use these lists on a per-policy basis.

These options apply to Security Intelligence only. Security Intelligence cannot blacklist traffic that has already been fastpathed. Similarly, Security Intelligence whitelisting does not automatically trust or fastpath matching traffic. For more information, see About Security Intelligence.

<table>
<thead>
<tr>
<th>Context Menu Option</th>
<th>Target Item</th>
<th>Affected Global Lists</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blacklist Now</td>
<td>An IP address</td>
<td>Global Blacklist</td>
</tr>
<tr>
<td>Whitelist Now</td>
<td></td>
<td>Global Whitelist</td>
</tr>
<tr>
<td>Blacklist HTTP/S Connections to URL Now</td>
<td>A URL</td>
<td>Global Blacklist for URL</td>
</tr>
<tr>
<td>Whitelist HTTP/S Connections to URL Now</td>
<td></td>
<td>Global Whitelist for URL</td>
</tr>
</tbody>
</table>
In a multidomain deployment, you can choose the Firepower System domains where you want to enforce the blacklisting or whitelisting by adding items to Domain lists as well as the Global lists; see Security Intelligence Lists and Multitenancy, on page 41.

Because adding an entry to a Security Intelligence list affects access control, you must have one of:

- Administrator access
- A combination of default roles: Network Admin or Access Admin, plus Security Analyst and Security Approver
- A custom role with both Modify Access Control Policy and Deploy Configuration to Devices permissions

## Security Intelligence Lists and Multitenancy

In a multidomain deployment, the Global domain owns the Global blacklists and whitelists. Only Global administrators can add to or remove items from the Global lists. So that subdomain users can whitelist and blacklist networks, domain names, and URLs, multitenancy adds:

- Domain lists—Whitelists or blacklists whose contents apply to a particular subdomain only. The Global lists are Domain lists for the Global domain.
- Descendant Domain lists—Whitelists or blacklists that aggregate the Domain lists of the current domain’s descendants.

### Domain Lists

In addition to being able to access (but not edit) the Global lists, each subdomain has its own named lists, the contents of which apply only to that subdomain. For example, a subdomain named Company A owns:

- Domain Blacklist - Company A and Domain Whitelist - Company A
- Domain Blacklist for DNS - Company A, Domain Whitelist for DNS - Company A
- Domain Blacklist for URL - Company A, Domain Whitelist for URL - Company A

Any administrator at or above the current domain can populate these lists. You can use the context menu to whitelist or blacklist an item in the current and all descendant domains. However, only an administrator in the associated domain can remove an item from a Domain list.
For example, a Global administrator could choose to blacklist the same IP address in the Global domain and Company A’s domain, but not blacklist it in Company B’s domain. This action would add the same IP address to:

- Global Blacklist (where it can be removed only by Global administrators)
- Domain Blacklist - Company A (where it can be removed only by Company A administrators)

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.

**Descendant Domain Lists**

A Descendant Domain list is a whitelist or blacklist that aggregates the Domain lists of the current domain’s descendants. Leaf domains do not have Descendant Domain lists.

Descendant Domain lists are useful because a higher-level domain administrator can enforce general Security Intelligence settings, while still allowing subdomain users to blacklist and whitelist items in their own deployment.

For example, the Global domain has the following Descendant Domain lists:

- Descendant Blacklists - Global, Descendant Whitelists - Global
- Descendant Blacklists for URL - Global, Descendant Whitelists for URL - Global
- Descendant Blacklists for URL - Global, Descendant Whitelists for URL - Global

---

**Note**

Descendant Domain lists do not appear in the object manager because they are symbolic aggregations, not hand-populated lists. They appear where you can use them: in access control and DNS policies.

---

### Changing the Update Frequency for Security Intelligence Feeds

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat</td>
<td>Protection</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access Admin/Network Admin</td>
</tr>
</tbody>
</table>

Although you cannot delete the system-provided feeds, you can change the frequency of (or disable) their updates. By default, each feed updates every two hours.

In a multidomain deployment, the system-provided feeds belong to the Global domain and can be modified only by an administrator in that domain. You can modify the update frequency for custom feeds belonging to your domain.
Reusable Objects

Custom Security Intelligence Feeds

Procedure

Step 1 Choose **Objects > Object Management**.
Step 2 Expand the **Security Intelligence** node, then choose the feed type whose frequency you want to change.
Step 3 Next to the feed you want to update, click the edit icon (-pencil).

If a view icon (-eye) appears instead, the object belongs to an ancestor domain, or you do not have permission to modify the object.

Step 4 Edit the **Update Frequency**.
Step 5 Click **Save**.

Custom Security Intelligence Feeds

Custom or third-party Security Intelligence feeds allow you to augment the system-provided Intelligence Feeds with other regularly-updated reputable whitelists and blacklists on the Internet. You can also set up an internal feed, which is useful if you want to update multiple Firepower Management Centers in your deployment using one source list.

Note You cannot whitelist or blacklist address blocks using a /0 netmask in a Security Intelligence feed. If you want to monitor or block all traffic targeted by a policy, use an access control rule with the **Monitor** or **Block** rule action, respectively, and a default value of *any* for the **Source Networks** and **Destination Networks**.

When you configure a feed, you specify its location using a URL; the URL cannot be Punycode-encoded. By default, the system downloads the entire feed source on the interval you configure, then automatically updates its managed devices.

You also can configure the system to use an md5 checksum to determine whether to download an updated feed. If the checksum has not changed since the last time the system downloaded the feed, the system does not need to re-download it. You may want to use md5 checksums for internal feeds, especially if they are large. The md5 checksum must be stored in a simple text file with only the checksum. Comments are not supported.

Manually updating Security Intelligence feeds updates all feeds, including the Intelligence Feeds.

Creating Security Intelligence Feeds

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat</td>
<td>Protection</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>

Firepower Management Center Configuration Guide, Version 6.2

43
Procedure

Step 1 Choose Objects > Object Management.
Step 2 Expand the Security Intelligence node, then choose a feed type you want to add.
Step 3 Click the option appropriate to the feed type you chose above:
   • Add Network Lists and Feeds
   • Add DNS Lists and Feeds
   • Add URL Lists and Feeds
Step 4 Enter a Name for the feed.
   In a multidomain deployment, object names must be unique within the domain hierarchy. The system may identify a conflict with the name of an object you cannot view in your current domain.
Step 5 Choose Feed from the Type drop-down list.
Step 6 Enter a Feed URL.
Step 7 Optionally, enter an MD5 URL.
Step 8 Choose an Update Frequency.
Step 9 Click Save.
   Unless you disabled feed updates, the system attempts to download and verify the feed.

Manually Updating Security Intelligence Feeds

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat (Security Intelligence)</td>
<td>Protection (Security Intelligence)</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access Admin/Network Admin</td>
</tr>
</tbody>
</table>

Procedure

Step 1 Choose Objects > Object Management.
Step 2 Expand the Security Intelligence node, then choose a feed type.
Step 3 Click Update Feeds, then confirm.
Step 4 Click OK.

After the Firepower Management Center downloads and verifies the feed updates, it communicates any changes to its managed devices. Your deployment begins filtering traffic using the updated feeds.
Custom Security Intelligence Lists

Security Intelligence lists are simple static lists of IP addresses and address blocks, URLs, or domain names that you manually upload to the system. Custom lists are useful if you want to augment and fine-tune feeds or one of the global lists, for a single Firepower Management Center’s managed devices.

For example, if a reputable feed improperly blocks your access to vital resources but is overall useful to your organization, you can create a custom whitelist that contains only the improperly classified IP addresses, rather than removing the IP address feed object from the access control policy’s blacklist.

You cannot whitelist or blacklist address blocks using a /0 netmask in a Security Intelligence list. If you want to monitor or block all traffic targeted by a policy, use an access control rule with the Monitor or Block rule action, respectively, and a default value of any for the Source Networks and Destination Networks.

Regarding list entry formatting, note the following:

- Netmasks for address blocks can be integers from 0 to 32 or 0 to 128, for IPv4 and IPv6, respectively.
- Unicode in domain names must be encoded in Punycode format, and are case insensitive.
- Characters in domain names are case-insensitive.
- Unicode in URLs should be encoded in percent-encoding format.
- Characters in URL subdirectories are case-sensitive.
- List entries that start with the pound sign (#) are treated as comments.

Regarding matching list entries, note the following:

- The system matches sub-level domains if a higher-level domain exists in a URL or DNS list. For example, if you add example.com to a DNS list, the system matches both www.example.com and test.example.com.
- The system does not perform DNS lookups (forward or reverse) on DNS or URL list entries. For example, if you add http://192.168.0.2 to a URL list, and it resolves to http://www.example.com, the system only matches http://192.168.0.2, not http://www.example.com.
- If you add a URL ending in a forward slash (/) character to a URL list, only exact URLs match that entry.
- If you add a URL that does not end in a forward slash to a URL or DNS list, any URL that shares the same common prefix matches that entry. For example, if you add www.example.com to a URL list, the system matches both www.example.com and www.example.com/example.

Uploading New Security Intelligence Lists to the Firepower Management Center

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>
To modify a Security Intelligence list, you must make your changes to the source file and upload a new copy. You cannot modify the file’s contents using the web interface. If you do not have access to the source file, download a copy from the system.

**Procedure**

**Step 1** Choose Objects > Object Management.

**Step 2** Expand the **Security Intelligence** node, then choose a list type.

**Step 3** Click the option appropriate to the list you chose above:

- Add Network Lists and Feeds
- Add DNS Lists and Feeds
- Add URL Lists and Feeds

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

In a multidomain deployment, object names must be unique within the domain hierarchy. The system may identify a conflict with the name of an object you cannot view in your current domain.

**Step 5** From the **Type** drop-down list, choose **List**.

**Step 6** Click **Browse** to browse to the list .txt file, then click **Upload**.

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

**What to Do Next**

- If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes.

**Updating Security Intelligence Lists**

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network Admin</td>
</tr>
</tbody>
</table>

In a multidomain deployment, the system displays objects created in the current domain, which you can edit. It also displays objects created in ancestor domains, which in most cases you cannot edit. To view and edit objects in a descendant domain, switch to that domain.
Procedure

Step 1  Choose Objects > Object Management.
Step 2  Expand the Security Intelligence node, then choose a list type.
Step 3  Next to the list you want to update, click the edit icon (EDIT).
        If a view icon (VIEW) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.
Step 4  If you need a copy of the list to edit, click Download, then follow your browser’s prompts to save the list as a text file.
Step 5  Make changes to the list as necessary.
Step 6  On the Security Intelligence pop-up window, click Browse to browse to the modified list, then click Upload.
Step 7  Click Save.

What to Do Next

- If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes.

Sinkhole Objects

A sinkhole object represents either a DNS server that gives non-routeable addresses for all domain names within the sinkhole, or an IP address that does not resolve to a server. You can reference the sinkhole object within a DNS policy rule to redirect matching traffic to the sinkhole. You must assign the object both an IPv4 address and an IPv6 address.

Creating Sinkhole Objects

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat</td>
<td>Protection</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access Admin/Access Admin/Network Admin</td>
</tr>
</tbody>
</table>

Procedure

Step 1  Choose Objects > Object Management.
Step 2  Choose Sinkhole from the list of object types.
Step 3  Click Add Sinkhole.
Step 4  Enter a Name.
In a multidomain deployment, object names must be unique within the domain hierarchy. The system may identify a conflict with the name of an object you cannot view in your current domain.

**Step 5** Enter the IPv4 Address and IPv6 Address of your sinkhole.

**Step 6** You have the following options:
- If you want to redirect traffic to a sinkhole server, choose Log Connections to Sinkhole.
- If you want to redirect traffic to a non-resolving IP address, choose Block and Log Connections to Sinkhole.

**Step 7** If you want to assign an Indication of Compromise (IoC) type to your sinkhole, choose one from the Type drop-down.

**Step 8** Click Save.

---

### File Lists

If you use AMP for Firepower, and the AMP cloud incorrectly identifies a file’s disposition, you can add the file to a file list to better detect the file in the future. These files are specified using SHA-256 hash values. Each file list can contain up to 10000 unique SHA-256 values.

There are two predefined categories of file lists:

**Clean List**

If you add a file to this list, the system treats it as if the AMP cloud assigned a clean disposition.

**Custom Detection List**

If you add a file to this list, the system treats it as if the AMP cloud assigned a malware disposition.

In a multidomain deployment, a clean list and custom detection list is present for each domain. In lower-level domains, you can view but not modify ancestor's lists.

Because you manually specify the blocking behavior for the files included in these lists, the system does not query the AMP cloud for these files’ dispositions. You must configure a rule in the file policy with either a Malware Cloud Lookup or Block Malware action and a matching file type to calculate a file’s SHA value.

**Caution** Do not include malware on the clean list. The clean list overrides both the AMP cloud and the custom detection list.

---

### Source Files for File Lists

You can add multiple SHA-256 values to a file list by uploading a comma-separated value (CSV) source file containing a list of SHA-256 values and descriptions. The Firepower Management Center validates the contents and populates the file list with valid SHA-256 values.
The source file must be a simple text file with a .csv file name extension. Any header must start with a pound sign (#); it is treated as a comment and not uploaded. Each entry should contain a single SHA-256 value followed by a description and end with either the \n or CR+LF Newline character. The system ignores any additional information in the entry.

Note the following:

- Deleting a source file from the file list also removes all associated SHA-256 hashes from the file list.
- You cannot upload multiple files to a file list if the successful source file upload results in the file list containing more than 10000 distinct SHA-256 values.
- The system truncates descriptions exceeding 256 characters to the first 256 characters on upload. If the description contains commas, you must use an escape character (\,). If no description is included, the source file name is used instead.
- All non-duplicate SHA-256 values are added to the file list. If a file list contains a SHA-256 value, and you upload a source file containing that value, the newly uploaded value does not modify the existing SHA-256 value. When viewing captured files, file events, or malware events related to the SHA-256 value, any threat name or description is derived from the individual SHA-256 value.
- The system does not upload invalid SHA-256 values in a source file.
- If multiple uploaded source files contain an entry for the same SHA-256 value, the system uses the most recent value.
- If a source file contains multiple entries for the same SHA-256 value, the system uses the last one.
- You cannot directly edit a source file within the object manager. To make changes, you must first modify your source file directly, delete the copy on the system, then upload the modified source file.
- The number of entries associated with a source file refers to the number of distinct SHA-256 values. If you delete a source file from a file list, the total number of SHA-256 entries the file list contains decreases by the number of valid entries in the source file.

### Adding Individual SHA-256 Values to File Lists

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware</td>
<td>Malware</td>
<td>Firepower</td>
<td>Any</td>
<td>Admin/Network, Admin/Access, Admin</td>
</tr>
</tbody>
</table>

You can submit a file's SHA-256 value to add it to a file list. You cannot add duplicate SHA-256 values.

In a multidomain deployment, the system displays objects created in the current domain, which you can edit. It also displays objects created in ancestor domains, which in most cases you cannot edit. To view and edit objects in a descendant domain, switch to that domain.

### Before You Begin

- Right-click a file or malware event from the event view, choose **Show Full Text** in the context menu, and copy the full SHA-256 value for pasting into the file list.
Procedure

Step 1 Choose Objects > Object Management.
Step 2 Choose File List from the list of object types.
Step 3 Click the edit icon (-pencil) next to the clean list or custom detection list where you want to add a file.
   If a view icon (-eye) appears instead, the object belongs to an ancestor domain, or you do not have permission to modify the object.
Step 4 Choose Enter SHA Value from the Add by drop-down list.
Step 5 Enter a description of the source file in the Description field.
Step 6 Enter or paste the file’s entire value in the SHA-256 field. The system does not support matching partial values.
Step 7 Click Add.
Step 8 Click Save.

What to Do Next

- If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes.

Note
After configuration changes are deployed, the system no longer queries the AMP cloud for files on the list.

Uploading Individual Files to File Lists

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware</td>
<td>Malware</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access Admin/Network Admin</td>
</tr>
</tbody>
</table>

If you have a copy of the file you want to add to a file list, you can upload the file to the Firepower Management Center for analysis; the system calculates the file’s SHA-256 value and adds the file to the list. The system does not enforce a limit on the size of files for SHA-256 calculation.

In a multidomain deployment, the system displays objects created in the current domain, which you can edit. It also displays objects created in ancestor domains, which in most cases you cannot edit. To view and edit objects in a descendant domain, switch to that domain.
Procedure

Step 1
Choose Objects > Object Management.

Step 2
Choose File List from the list of object types.

Step 3
Click the edit icon ( ) next to the clean list or custom detection list where you want to add a file.

If a view icon ( ) appears instead, the object belongs to an ancestor domain, or you do not have permission to modify the object.

Step 4
From the Add by drop-down list, choose Calculate SHA.

Step 5
Optionally, enter a description of the file in the Description field. If you do not enter a description, the file name is used for the description on upload.

Step 6
Click Browse, and choose a file to upload.

Step 7
Click Calculate and Add SHA.

Step 8
Click Save.

What to Do Next

• If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes.

Note
After you deploy configuration changes, the system no longer queries the AMP cloud for files on the list.

Uploading Source Files to File Lists

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware</td>
<td>Malware</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>

In a multidomain deployment, the system displays objects created in the current domain, which you can edit. It also displays objects created in ancestor domains, which in most cases you cannot edit. To view and edit objects in a descendant domain, switch to that domain.

Procedure

Step 1
Choose Objects > Object Management.

Step 2
Click File List.

Step 3
Click the edit icon ( ) next to the file list where you want to add values from a source file.
Step 4 In the Add by drop-down list, choose List of SHAs.
Step 5 Optionally, enter a description of the source file in the Description field. If you do not enter a description, the system uses the file name.
Step 6 Click Browse to browse to the source file, then click Upload and Add List.
Step 7 Click Save.

What to Do Next

- If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes.

Note After you deploy the policies, the system no longer queries the AMP cloud for files on the list.

Editing SHA-256 Values in File Lists

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware</td>
<td>Malware</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>

You can edit or delete individual SHA-256 values on a file list. Note that you cannot directly edit a source file within the object manager. To make changes, you must first modify your source file directly, delete the copy on the system, then upload the modified source file.

In a multidomain deployment, the system displays objects created in the current domain, which you can edit. It also displays objects created in ancestor domains, which in most cases you cannot edit. To view and edit objects in a descendant domain, switch to that domain.

Procedure

Step 1 Choose Objects > Object Management.
Step 2 Click File List.
Step 3 Click the edit icon (📝) next to the clean list or custom detection list where you want to modify a file.
   If a view icon (استعراض) appears instead, the object belongs to an ancestor domain, or you do not have permission to modify the object.
Step 4 You can:
Reusable Objects

Downloading Source Files from File Lists

- Click the edit icon (-pencil) next to the SHA-256 value you want to change, and modify the SHA-256 or Description values as desired.
- Click the delete icon (-trash) next to the SHA-256 value you want to delete.

**Step 5**
Click **Save** to update the file entry in the list.

**Step 6**
Click **Save** to save the file list.

**What to Do Next**
- If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes.

**Note**
After configuration changes are deployed, the system no longer queries the AMP cloud for files on the list.

### Downloading Source Files from File Lists

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware</td>
<td>Malware</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access Admin/Network Admin</td>
</tr>
</tbody>
</table>

In a multidomain deployment, the system displays objects created in the current domain, which you can edit. It also displays objects created in ancestor domains, which in most cases you cannot edit. To view and edit objects in a descendant domain, switch to that domain.

**Procedure**

**Step 1**
Choose **Objects > Object Management**.

**Step 2**
Choose **File List** from the list of object types.

**Step 3**
Click the edit icon (-pencil) next to the clean list or custom detection list where you want to download a source file.

If a view icon (-eye) appears instead, the object belongs to an ancestor domain, or you do not have permission to modify the object.

**Step 4**
Next to the source file you want to download, click the view icon (-eye).

**Step 5**
Click **Download SHA List** and follow the prompts to save the source file.

**Step 6**
Click **Close**.
Cipher Suite Lists

A cipher suite list is an object comprised of several cipher suites. Each predefined cipher suite value represents a cipher suite used to negotiate an SSL- or TLS-encrypted session. You can use cipher suites and cipher suite lists in SSL rules to control encrypted traffic based on whether the client and server negotiated the SSL session using that cipher suite. If you add a cipher suite list to an SSL rule, SSL sessions negotiated with any of the cipher suites in the list match the rule.

Note
Although you can use cipher suites in the web interface in the same places as cipher suite lists, you cannot add, modify, or delete cipher suites.

Creating Cipher Suite Lists

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any except NGIPSv</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>

Procedure

Step 1 Choose Objects > Object Management.
Step 2 Choose Cipher Suite List from the list of object types.
Step 3 Click Add Cipher Suites.
Step 4 Enter a Name.
   In a multidomain deployment, object names must be unique within the domain hierarchy. The system may identify a conflict with the name of an object you cannot view in your current domain.
Step 5 Choose one or more cipher suites from the Available Ciphers list.
Step 6 Click Add.
Step 7 Optionally, click the delete icon (🗑️) next to any cipher suites in the Selected Ciphers list that you want to remove.
Step 8 Click Save.

What to Do Next

• If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes.
Distinguished Name Objects

Each distinguished name object represents the distinguished name listed for a public key certificate's subject or issuer. You can use distinguished name objects and groups in SSL rules to control encrypted traffic based on whether the client and server negotiated the SSL session using a server certificate with the distinguished name as subject or issuer.

Your distinguished name object can contain the common name attribute (CN). If you add a common name without "CN=" then the system prepends "CN=" before saving the object.

You can also add a distinguished name with one of each attribute listed in the following table, separated by commas.

Table 3: Distinguished Name Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Allowed Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>Country Code</td>
<td>two alphabetic characters</td>
</tr>
<tr>
<td>CN</td>
<td>Common Name</td>
<td>up to 64 alphanumeric, backslash (/), hyphen (-), quotation ('), or asterisk (*) characters, or spaces</td>
</tr>
<tr>
<td>O</td>
<td>Organization</td>
<td>up to 64 alphanumeric, backslash (/), hyphen (-), quotation ('), or asterisk (*) characters, or spaces</td>
</tr>
<tr>
<td>OU</td>
<td>Organizational Unit</td>
<td>up to 64 alphanumeric, backslash (/), hyphen (-), quotation ('), or asterisk (*) characters, or spaces</td>
</tr>
</tbody>
</table>

You can define one or more asterisks (*) as wildcards in an attribute. In a common name attribute, you can define one or more asterisks per domain name label. Wildcards match only within that label, though you can define multiple labels with wildcards. See the following table for examples.

Table 4: Common Name Attribute Wild Card Examples

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Matches</th>
<th>Does Not Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN=&quot;*ample.com&quot;</td>
<td>example.com</td>
<td>mail.example.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>example.text.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ampleexam.com</td>
</tr>
<tr>
<td>CN=&quot;exam*.com&quot;</td>
<td>example.com</td>
<td>mail.example.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>example.text.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ampleexam.com</td>
</tr>
<tr>
<td>CN=&quot;<em>xamp</em>.com&quot;</td>
<td>example.com</td>
<td>mail.example.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>example.text.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ampleexam.com</td>
</tr>
</tbody>
</table>
Creating Distinguished Name Objects

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Matches</th>
<th>Does Not Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN=&quot;*.example.com&quot;</td>
<td>mail.example.com</td>
<td>example.com example.text.com ampleexam.com</td>
</tr>
<tr>
<td>CN=&quot;*.com&quot;</td>
<td>example.com ampleexam.com</td>
<td>mail.example.com example.text.com</td>
</tr>
<tr>
<td>CN=&quot;<em>..</em>.com&quot;</td>
<td>mail.example.com example.text.com</td>
<td>example.com ampleexam.com</td>
</tr>
</tbody>
</table>

Creating Distinguished Name Objects

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any except NGIPSv</td>
<td>Any</td>
<td>Admin/Admin/Access Admin/Network Admin</td>
</tr>
</tbody>
</table>

Procedure

**Step 1** Choose **Objects > Object Management**.

**Step 2** Expand the **Distinguished Name** node, and choose **Individual Objects**.

**Step 3** Click **Add Distinguished Name**.

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

In a multidomain deployment, object names must be unique within the domain hierarchy. The system may identify a conflict with the name of an object you cannot view in your current domain.

**Step 5** In the **DN** field, enter a value for the distinguished name or common name. You have the following options:

- If you add a distinguished name, you can include one of each attribute listed in **Distinguished Name Objects**, on page 55 separated by commas.

- If you add a common name, you can include multiple labels and wild cards.

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

**What to Do Next**

- If an active policy references your object, deploy configuration changes; see **Deploying Configuration Changes**.
PKI Objects

**PKI Objects for SSL Application**

PKI objects represent the public key certificates and paired private keys required to support your deployment. Internal and trusted CA objects consist of certificate authority (CA) certificates; internal CA objects also contain the private key paired with the certificate. Internal and external certificate objects consist of server certificates; internal certificate objects also contain the private key paired with the certificate.

If you use trusted certificate authority objects and internal certificate objects to configure a connection to ISE, you can use ISE as an identity source.

If you use internal certificate objects to configure captive portal, the system can authenticate the identity of your captive portal device when connecting to users’ web browsers.

If you use trusted certificate authority objects to configure realms, you can configure secure connections to LDAP or AD servers.

If you use PKI objects in SSL rules, you can match traffic encrypted with:

- the certificate in an external certificate object
- a certificate either signed by the CA in a trusted CA object, or within the CA’s chain of trust

If you use PKI objects in SSL rules, you can decrypt:

- outgoing traffic by re-signing the server certificate with an internal CA object
- incoming traffic using the known private key in an internal certificate object

You can manually input certificate and key information, upload a file containing that information, or in some cases, generate a new CA certificate and private key.

When you view a list of PKI objects in the object manager, the system displays the certificate’s Subject distinguished name as the object value. Hover your pointer over the value to view the full certificate Subject distinguished name. To view other certificate details, edit the PKI object.

**Note**

The Firepower Management Center and managed devices encrypt all private keys stored in internal CA objects and internal certificate objects with a randomly generated key before saving them. If you upload private keys that are password protected, the appliance decrypts the key using the user-supplied password, then reencrypts it with the randomly generated key before saving it.

**PKI Objects for Certificate Enrollment**

A certificate enrollment object contains the Certification Authority (CA) server information and enrollment parameters that are required for creating Certificate Signing Requests (CSRs) and obtaining Identity Certificates from the specified CA. These activities occur in your Private Key Infrastructure (PKI).

The certificate enrollment object may also include certificate revocation information. For more information on PKI, digital certificates, and certificate enrollment see [PKI Infrastructure and Digital Certificates](#).
Internal Certificate Authority Objects

Each internal certificate authority (CA) object you configure represents the CA public key certificate of a CA your organization controls. The object consists of the object name, CA certificate, and paired private key. You can use internal CA objects and groups in SSL rules to decrypt outgoing encrypted traffic by re-signing the server certificate with the internal CA.

**Note**

If you reference an internal CA object in a Decrypt - Resign SSL rule and the rule matches an encrypted session, the user’s browser may warn that the certificate is not trusted while negotiating the SSL handshake. To avoid this, add the internal CA object certificate to either the client or domain list of trusted root certificates.

You can create an internal CA object in the following ways:

- import an existing RSA-based or elliptic curve-based CA certificate and private key
- generate a new self-signed RSA-based CA certificate and private key
- generate an unsigned RSA-based CA certificate and private key. You must submit a certificate signing request (CSR) to another CA to sign the certificate before using the internal CA object.

After you create an internal CA object containing a signed certificate, you can download the CA certificate and private key. The system encrypts downloaded certificates and private keys with a user-provided password. Whether system-generated or user-created, you can modify the internal CA object name, but cannot modify other object properties.

You cannot delete an internal CA object that is in use. Additionally, after you edit an internal CA object used in an SSL policy, the associated access control policy goes out-of-date. You must re-deploy the access control policy for your changes to take effect.

CA Certificate and Private Key Import

You can configure an internal CA object by importing an X.509 v3 CA certificate and private key. You can upload files encoded in one of the following supported formats:

- Distinguished Encoding Rules (DER)
- Privacy-enhanced Electronic Mail (PEM)

If the private key file is password-protected, you can supply the decryption password. If the certificate and key are encoded in the PEM format, you can also copy and paste the information.

You can upload only files that contain proper certificate or key information, and that are paired with each other. The system validates the pair before saving the object.

**Note**

If you configure a rule with the Decrypt - Resign action, the rule matches traffic based on the referenced internal CA certificate’s encryption algorithm type, in addition to any configured rule conditions. You must upload an elliptic curve-based CA certificate to decrypt outgoing traffic encrypted with an elliptic curve-based algorithm, for example.
Importing a CA Certificate and Private Key

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any except NGIPSv</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>

In a multidomain deployment, the system displays objects created in the current domain, which you can edit. It also displays objects created in ancestor domains, which in most cases you cannot edit. To view and edit objects in a descendant domain, switch to that domain.

**Procedure**

**Step 1** Choose **Objects > Object Management**.
**Step 2** Expand the **PKI** node, and choose **Internal CAs**.
**Step 3** Click **Import CA**.
**Step 4** Enter a **Name**.
In a multidomain deployment, object names must be unique within the domain hierarchy. The system may identify a conflict with the name of an object you cannot view in your current domain.
**Step 5** Above the **Certificate Data** field, click **Browse** to upload a DER or PEM-encoded X.509 v3 CA certificate file.
**Step 6** Above the **Key** field, click **Browse** to upload a DER or PEM-encoded paired private key file.
**Step 7** If the uploaded file is password-protected, check the **Encrypted, and the password is**: check box, and enter the password.
**Step 8** Click **Save**.

**What to Do Next**

- If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes.

Generating a New CA Certificate and Private Key

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any except NGIPSv</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>

You can configure an internal CA object by providing identification information to generate a self-signed RSA-based CA certificate and private key.
The generated CA certificate is valid for ten years. The Valid From date is a week before generation.

In a multidomain deployment, the system displays objects created in the current domain, which you can edit. It also displays objects created in ancestor domains, which in most cases you cannot edit. To view and edit objects in a descendant domain, switch to that domain.

**Procedure**

**Step 1** Choose **Objects > Object Management**.

**Step 2** Expand the **PKI** node, and choose **Internal CAs**.

**Step 3** Click **Generate CA**.

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

In a multidomain deployment, object names must be unique within the domain hierarchy. The system may identify a conflict with the name of an object you cannot view in your current domain.

**Step 5** Enter the identification attributes.

**Step 6** Click **Generate self-signed CA**.

---

**New Signed Certificates**

You can configure an internal CA object by obtaining a signed certificate from a CA. This involves two steps:

- Provide identification information to configure the internal CA object. This generates an unsigned certificate and paired private key, and creates a certificate signing request (CSR) to a CA you specify.

- After the CA issues the signed certificate, upload it to the internal CA object, replacing the unsigned certificate.

You can only reference an internal CA object in an SSL rule if it contains a signed certificate.

**Creating an Unsigned CA Certificate and CSR**

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any except NGIPSv</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>

**Procedure**

**Step 1** Choose **Objects > Object Management**.

**Step 2** Expand the **PKI** node, and choose **Internal CAs**.

**Step 3** Click **Generate CA**.

**Step 4** Enter a **Name**.
In a multidomain deployment, object names must be unique within the domain hierarchy. The system may identify a conflict with the name of an object you cannot view in your current domain.

Step 5 Enter the identification attributes.
Step 6 Click Generate CSR.
Step 7 Copy the CSR to submit to a CA.
Step 8 Click OK.

What to Do Next

- You must upload a signed certificate issued by a CA as described in Uploading a Signed Certificate Issued in Response to a CSR, on page 61

### Uploading a Signed Certificate Issued in Response to a CSR

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any except NGIPSv</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin Admin</td>
</tr>
</tbody>
</table>

In a multidomain deployment, the system displays objects created in the current domain, which you can edit. It also displays objects created in ancestor domains, which in most cases you cannot edit. To view and edit objects in a descendant domain, switch to that domain.

Once uploaded, the signed certificate can be referenced in SSL rules.

**Procedure**

Step 1 Choose Objects > Object Management.
Step 2 Expand the PKI node, and choose Internal CAs.
Step 3 Click the edit icon (✎) next to the CA object containing the unsigned certificate awaiting the CSR.
Step 4 Click Install Certificate.
Step 5 Click Browse to upload a DER or PEM-encoded X.509 v3 CA certificate file.
Step 6 If the uploaded file is password protected, check the Encrypted, and the password is: check box, and enter the password.
Step 7 Click Save to upload a signed certificate to the CA object.

What to Do Next

- If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes.
CA Certificate and Private Key Downloads

You can back up or transfer a CA certificate and paired private key by downloading a file containing the certificate and key information from an internal CA object.

⚠️ Caution
Always store downloaded key information in a secure location.

The system encrypts the private key stored in an internal CA object with a randomly generated key before saving it to disk. If you download a certificate and private key from an internal CA object, the system first decrypts the information before creating a file containing the certificate and private key information. You must then provide a password the system uses to encrypt the downloaded file.

⚠️ Caution
Private keys downloaded as part of a system backup are decrypted, then stored in the unencrypted backup file.

Downloading a CA Certificate and Private Key

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any except NGIPSv</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>

In a multidomain deployment, the system displays objects created in the current domain, which you can edit. It also displays objects created in ancestor domains, which in most cases you cannot edit. To view and edit objects in a descendant domain, switch to that domain.

You can download CA certificates for both the current domain and ancestor domains.

Procedure

Step 1  Choose Objects > Object Management.
Step 2  Expand the PKI node, and choose Internal CAs.
Step 3  Next to the internal CA object whose certificate and private key you want to download, click the edit icon (✏️).
In a multidomain deployment, click the view icon (смотреть) to download the certificate and private key for an object in an ancestor domain.
Step 4  Click Download.
Step 5  Enter an encryption password in the Password and Confirm Password fields.
Step 6  Click OK.
Trusted Certificate Authority Objects

Each trusted certificate authority (CA) object you configure represents a CA public key certificate belonging to a trusted CA. The object consists of the object name and CA public key certificate. You can use external CA objects and groups in:

- your SSL policy to control traffic encrypted with a certificate signed either by the trusted CA, or any CA within the chain of trust.
- your realm configurations to establish secure connections to LDAP or AD servers.
- your ISE connection. Select trusted certificate authority objects for the pxGrid Server CA and MNT Server CA fields.

After you create the trusted CA object, you can modify the name and add certificate revocation lists (CRL), but cannot modify other object properties. There is no limit on the number of CRLs you can add to an object. If you want to modify a CRL you have uploaded to an object, you must delete the object and recreate it.

Note
Adding a CRL to an object has no effect when the object is used in your ISE integration configuration.

You cannot delete a trusted CA object that is in use. Additionally, after you edit a trusted CA object that is in use, the associated access control policy goes out-of-date. You must re-deploy the access control policy for your changes to take effect.

Trusted CA Object

You can configure an external CA object by uploading an X.509 v3 CA certificate. You can upload a file encoded in one of the following supported formats:

- Distinguished Encoding Rules (DER)
- Privacy-enhanced Electronic Mail (PEM)

If the file is password-protected, you must supply the decryption password. If the certificate is encoded in the PEM format, you can also copy and paste the information.

You can upload a CA certificate only if the file contains proper certificate information; the system validates the certificate before saving the object.

Adding a Trusted CA Object

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any except NGIPSv</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>

Firepower Management Center Configuration Guide, Version 6.2
Procedure

Step 1  Choose Objects > Object Management.
Step 2  Expand the PKI node, and choose Trusted CAs.
Step 3  Click Add Trusted CAs.
Step 4  Enter a Name.
In a multidomain deployment, object names must be unique within the domain hierarchy. The system may identify a conflict with the name of an object you cannot view in your current domain.
Step 5  Click Browse to upload a DER or PEM-encoded X.509 v3 CA certificate file.
Step 6  If the file is password-protected, check the Encrypted, and the password is: check box, and enter the password.
Step 7  Click Save.

What to Do Next

• If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes.

Certificate Revocation Lists in Trusted CA Objects
You can upload CRLs to a trusted CA object. If you reference that trusted CA object in an SSL policy, you can control encrypted traffic based on whether the CA that issued the session encryption certificate subsequently revoked the certificate. You can upload files encoded in one of the following supported formats:

• Distinguished Encoding Rules (DER)
• Privacy-enhanced Electronic Mail (PEM)

After you add the CRL, you can view the list of revoked certificates. If you want to modify a CRL you have uploaded to an object, you must delete the object and recreate it.

You can upload only files that contain a proper CRL. There is no limit to the number of CRLs you can add to a trusted CA object. However, you must save the object each time you upload a CRL, before adding another CRL.

Note  Adding a CRL to an object has no effect when the object is used in your ISE integration configuration.

Adding a Certificate Revocation List to a Trusted CA Object

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any except NGIPSv</td>
<td>Any</td>
<td>Admin/Access Admin/Network Admin</td>
</tr>
</tbody>
</table>
In a multidomain deployment, the system displays objects created in the current domain, which you can edit. It also displays objects created in ancestor domains, which in most cases you cannot edit. To view and edit objects in a descendant domain, switch to that domain.

**Note**

Adding a CRL to an object has no effect when the object is used in your ISE integration configuration.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose <strong>Objects</strong> &gt; <strong>Object Management</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Expand the <strong>PKI</strong> node, and choose <strong>Trusted CAs</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>Click the edit icon (📝) next to a trusted CA object.</td>
</tr>
<tr>
<td></td>
<td>If a view icon (🔍) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.</td>
</tr>
<tr>
<td>4</td>
<td>Click <strong>Add CRL</strong> to upload a DER or PEM-encoded CRL file.</td>
</tr>
<tr>
<td>5</td>
<td>Click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

**What to Do Next**

- If an active policy references your object, deploy configuration changes; see [Deploying Configuration Changes](#).

**External Certificate Objects**

Each external certificate object you configure represents a server public key certificate that does not belong to your organization. The object consists of the object name and certificate. You can use external certificate objects and groups in SSL rules to control traffic encrypted with the server certificate. For example, you can upload a self-signed server certificate that you trust, but cannot verify with a trusted CA certificate.

You can configure an external certificate object by uploading an X.509 v3 server certificate. You can upload a file in one of the following supported formats:

- Distinguished Encoding Rules (DER)
- Privacy-enhanced Electronic Mail (PEM)

You can upload only files that contain proper server certificate information; the system validates the file before saving the object. If the certificate is encoded in the PEM format, you can also copy and paste the information.
Adding External Certificate Objects

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any except NGIPSv</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin Admin</td>
</tr>
</tbody>
</table>

Procedure

**Step 1** Choose **Objects > Object Management**.

**Step 2** Expand the **PKI** node, and choose **External Certs**.

**Step 3** Click **Add External Cert**.

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

In a multidomain deployment, object names must be unique within the domain hierarchy. The system may identify a conflict with the name of an object you cannot view in your current domain.

**Step 5** Above the **Certificate Data** field, click **Browse** to upload a DER or PEM-encoded X.509 v3 server certificate file.

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

**What to Do Next**

- If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes.

Internal Certificate Objects

Each internal certificate object you configure represents a server public key certificate belonging to your organization. The object consists of the object name, public key certificate, and paired private key. You can use internal certificate objects and groups in:

- your SSL rules to decrypt traffic incoming to one of your organization’s servers using the known private key.

- your ISE connection. Select an internal certificate object for the **MC Server Certificate** field.

- your captive portal configuration to authenticate the identity of your captive portal device when connecting to users' web browsers. Select an internal certificate object for the **Server Certificate** field.

You can configure an internal certificate object by uploading an X.509 v3 RSA-based or elliptic curve-based server certificate and paired private key. You can upload a file in one of the following supported formats:

- Distinguished Encoding Rules (DER)

- Privacy-enhanced Electronic Mail (PEM)
If the file is password-protected, you must supply the decryption password. If the certificate and key are encoded in the PEM format, you can also copy and paste the information.

You can upload only files that contain proper certificate or key information, and that are paired with each other. The system validates the pair before saving the object.

After you create the internal certificate object, you can modify the name, but cannot modify other object properties.

You cannot delete an internal certificate object that is in use. Additionally, after you edit an internal certificate object that is in use, the associated access control policy goes out-of-date. You must re-deploy the access control policy for your changes to take effect.

## Adding Internal Certificate Objects

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any except NGIPSv</td>
<td>Any</td>
<td>Admin/Access Admin/Network Admin</td>
</tr>
</tbody>
</table>

### Procedure

**Step 1** Choose Objects > Object Management.

**Step 2** Expand the PKI node, and choose Internal Certs.

**Step 3** Click Add Internal Cert.

**Step 4** Enter a Name.

In a multidomain deployment, object names must be unique within the domain hierarchy. The system may identify a conflict with the name of an object you cannot view in your current domain.

**Step 5** Above the Certificate Data field, click Browse to upload a DER or PEM-encoded X.509 v3 server certificate file.

**Step 6** Above the Key field, or click Browse to upload a DER or PEM-encoded paired private key file.

**Step 7** If the uploaded private key file is password-protected, check the Encrypted, and the password is: check box, and enter the password.

**Step 8** Click Save.

## Certificate Enrollment Objects

Trustpoints let you manage and track CAs and certificates. A trustpoint is a representation of a CA or identity pair. A trustpoint includes the identity of the CA, CA-specific configuration parameters, and an association with one, enrolled identity certificate.

A certificate enrollment object contains the Certification Authority (CA) server information and enrollment parameters that are required for creating Certificate Signing Requests (CSRs) and obtaining Identity Certificates from the specified CA. These activities occur in your Private Key Infrastructure (PKI).
The certificate enrollment object may also include certificate revocation information. For more information on PKI, digital certificates, and certificate enrollment see PKI Infrastructure and Digital Certificates.

**How to Use Certificate Enrollment Objects**

Certificate Enrollment Objects are used to enroll your managed devices into your PKI infrastructure, and create trust points (CA objects) on devices that support VPN connections by doing the following:

1. Define parameters for CA authentication and enrollment in a Certificate Enrollment Object. Specify shared parameters and use the override facility to specify unique object setting for different devices.

2. Associate and install this object on each managed device that requires the identity certificate. On the device, it becomes a trustpoint.

When a certificate enrollment object is associated with and then installed on a device, the process of certificate enrollment starts immediately. The process is automatic for self-signed and SCEP enrollment types, meaning it does not require any additional administrator action. Manual certificate enrollment and importing a PKCS12 file requires extra administrator action.

3. Specify the created trustpoint in your VPN configuration.

**Managing Certificate Enrollment Objects**

To manage certificate enrollment objects, go to Objects > Object Management, then from the navigation pane choose PKI > Cert Enrollment. The following information is shown:

- Existing certificate enrollment objects are listed in the **Name** column.
  
  Use the search field (the magnifying glass) to filter the list.

- The enrollment type of each object is shown in the **Type** column. The following enrollment methods can be used:
  
  - **Self Signed**—The managed device generates its own self signed root certificate.
  
  - **SCEP**—(Default) Simple Certificate Enrollment Protocol is used by the device to obtain an identity certificate from the CA.
  
  - **Manual**—The process of enrolling is carried out manually by the administrator.
  
  - **PKCS12 File**—Import a PKCS12 file on a Firepower Threat Defense managed device that supports VPN connectivity. A PKCS#12, or PFX, file holds the server certificate, any intermediate certificates, and the private key in one encrypted file.

- The **Override** column indicates whether the object allows overrides (a green check mark) or not (a red X). If a number is displayed, it is the number of overrides in place.

  Use the Override option to customize the object settings for each device that is part of the VPN configuration. Overriding makes each device's trustpoint details unique. Typically the Common Name or Subject is overridden for each device in the VPN configuration.

  See Object Overrides, on page 8 for details and procedures on overriding objects of any type.

- **Edit** a previously created certificate enrollment object by clicking on the edit icon (a pencil). Editing can only be done if the enrollment object is not associated with any managed devices. Refer to the adding instructions for editing a certificate enrollment object.

- **Delete** a previously created certificate enrollment object by clicking on the delete icon (a trash can). You cannot delete a certificate enrollment object if it is associated with any managed device.
Press (+) Add Cert Enrollment to open the Add Cert Enrollment dialog and configure a Certificate Enrollment Object, see Adding Certificate Enrollment Objects, on page 69. Then install the certificate on each managed, headend device.

Related Topics

Installing a Certificate Using Self-Signed Enrollment
Installing a Certificate Using SCEP Enrollment
Installing a Certificate Using Manual Enrollment
Installing a Certificate by importing a PKCS12 File

Adding Certificate Enrollment Objects

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export-Compliance</td>
<td>N/A</td>
<td>Firepower Threat</td>
<td>Any</td>
<td>Admin/Organization Admin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Defense</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Procedure

Step 1 Open the Add Cert Enrollment dialog:

- Directly from Object Management: In the Objects > Object Management screen, choose PKI > Cert Enrollment from the navigation pane, and press Add Cert Enrollment.
- While configuring a managed device: In the Devices > Certificates screen, choose Add > Add New Certificate and click (+) for the Certificate Enrollment field.

Step 2 Enter the Name, and optionally, a Description of this enrollment object.
When enrollment is complete, this name is the name of the trustpoint on the managed devices with which it is associated.

Step 3 Open the CA Information tab and choose the Enrollment Type.

- **Self-Signed Certificate**—The managed device, acting as a CA, generates its own self-signed root certificate. No other information is needed in this pane.
  
  **Note** When enrolling a self-signed certificate you must specify the Common Name (CN) in the certificate parameters.


- **Manual**—Paste an obtained CA certificate in the CA Certificate field. You can obtain a CA certificate by copying it from another device.
• **PKCS12 File**—Import a PKCS12 file on a Firepower Threat Defense managed device that supports VPN connectivity. A PKCS#12, or PFX, file holds a server certificate, intermediate certificates, and a private key in one encrypted file.

**Step 4** (Optional) Open the **Certificate Parameters** tab and specify the certificate contents. See Certificate Enrollment Object Certificate Parameters, on page 71. This information is placed in the certificate and is readable by any party who receives the certificate from the router.

**Step 5** (Optional) Open the **Key** tab and specify the Key information. See Certificate Enrollment Object Key Options, on page 72.

**Step 6** (Optional) Click the **Revocation** tab, and specify the revocation options: See Certificate Enrollment Object Revocation Options, on page 72.

**Step 7** Allow Overrides of this object if desired. See Object Overrides, on page 8 for a full description of object overrides.

**What to Do Next**

Associate and install the enrollment object on a device to create a trustpoint on that device.

**Related Topics**

- Installing a Certificate Using Self-Signed Enrollment
- Installing a Certificate Using SCEP Enrollment
- Installing a Certificate Using Manual Enrollment
- Installing a Certificate by importing a PKCS12 File

**Certificate Enrollment Object SCEP Options**

**Firepower Management Center Navigation Path**

Objects > Object Management, then from the navigation pane choose PKI > PKI Enrollment. Press (+) Add PKI Enrollment to open the Add PKI Enrollment dialog, and select the CA Information tab.

**Fields**

**Enrollment Type**—set to SCEP.

**Enrollment URL**—The URL of the CA server to which devices should attempt to enroll.

Use an HTTP URL in the form of http://CA_name:port, where CA_name is the host DNS name or IP address of the CA server. The port number is mandatory.

If the CA cgi-bin script location at the CA is not the default (/cgi-bin/pkiclient.exe), you must also include the nonstandard script location in the URL, in the form of http://CA_name:port/script_location, where script_location is the full path to the CA scripts.

**Challenge Password / Confirm Password**—The password used by the CA server to validate the identity of the device. You can obtain the password by contacting the CA server directly or by entering the following address in a web browser: http://URLHostName/certsrv/mscep/mscep.dll. The password is good for 60 minutes from the time you obtain it from the CA server. Therefore, it is important that you deploy the password as soon as possible after you create it.
**Retry Period**—The interval between certificate request attempts, in minutes. Value can be 1 to 60 minutes. The default is 1 minute.

**Retry Count**—The number of retries that should be made if no certificate is issued upon the first request. Value can be 1 to 100. The default is 10.

**CA Certificate Source**—Specify how the CA certificate will be obtained.

- **Retrieve Using SCEP** (Default, and only supported option)—Retrieve the certificate from the CA server using the Simple Certificate Enrollment Process (SCEP). Using SCEP requires a connection between your device and the CA server. Ensure there is a route from your device to the CA server before beginning the enrollment process.

**Fingerprint**—When retrieving the CA certificate using SCEP, you may enter the fingerprint for the CA server. Using the fingerprint to verify the authenticity of the CA server’s certificate helps prevent an unauthorized party from substituting a fake certificate in place of the real one. Enter the Fingerprint for the CA server in hexadecimal format. If the value you enter does not match the fingerprint on the certificate, the certificate is rejected. Obtain the CA’s fingerprint by contacting the server directly, or by entering the following address in a web browser: http://<URLHostName>/certsrv/mscep/mscep.dll.

---

**Certificate Enrollment Object Certificate Parameters**

Specify additional information in certificate requests sent to the CA server. This information is placed in the certificate and can be viewed by any party who receives the certificate from the router.

**Firepower Management Center Navigation Path**

Objects > Object Management, then from the navigation pane choose PKI > PKI Enrollment. Press (+) Add PKI Enrollment to open the Add PKI Enrollment dialog, and select the Certificate Parameters tab.

**Fields**

Enter all information using the standard LDAP X.500 format.

- **Include FQDN**—Whether to include the device’s fully qualified domain name (FQDN) in the certificate request. Choices are:
  - Use Device Hostname as FQDN
  - Don’t use FQDN in certificate
  - Custom FQDN—Select this and then specify it in the Custom FQDN field that displays.

- **Include Device's IP Address**—The interface whose IP address is included in the certificate request.

- **Common Name (CN)**—The X.500 common name to include in the certificate.

**Note**

When enrolling a self-signed certificate you must specify the Common Name (CN) in the certificate parameters.

- **Organization Unit (OU)**—The name of the organization unit (for example, a department name) to include in the certificate.
• **Organization (O)** — The organization or company name to include in the certificate.

• **Locality (L)** — The locality to include in the certificate.

• **State (ST)** — The state or province to include in the certificate.

• **County Code (C)** — The country to include in the certificate. These codes conform to ISO 3166 country abbreviations, for example "US" for the United States of America.

• **Email (E)** — The email address to include in the certificate.

• **Include Device’s Serial Number** — Whether to include the serial number of the device in the certificate. The CA uses the serial number to either authenticate certificates or to later associate a certificate with a particular device. If you are in doubt, include the serial number, as it is useful for debugging purposes.

## Certificate Enrollment Object Key Options

**Firepower Management Center Navigation Path**

*Objects > Object Management*, then from the navigation pane choose **PKI > PKI Enrollment**. Press (+) **Add PKI Enrollment** to open the **Add PKI Enrollment** dialog, and select the **Key** tab.

**Fields**

• **Key Type** — RSA (default, and only supported option) or ECDSA.

• **Key Name** — If the key pair you want to associate with the certificate already exists, this field specifies the name of that key pair. If the key pair does not exist, this field specifies the name to assign to the key pair that will be generated during enrollment. If you do not specify an RSA key pair, the fully qualified domain name (FQDN) key pair is used instead.

• **Key Size** — If the key pair does not exist, defines the desired key size (modulus), in bits. The recommended size is 1024. The larger the modulus size, the more secure the key. However, keys with larger modulus sizes take longer to generate (a minute or more when larger than 512 bits) and longer to process when exchanged.

## Certificate Enrollment Object Revocation Options

Specify whether to check the revocation status of a certificate by choosing and configuring the method. Revocation checking is off by default, neither method (CRL or OCSP) is checked.

**Firepower Management Center Navigation Path**

*Objects > Object Management*, then from the navigation pane choose **PKI > PKI Enrollment**. Press (+) **Add PKI Enrollment** to open the **Add PKI Enrollment** dialog, and select the **Revocation** tab.

**Fields**

• **Enable Certificate Revocation Lists** — Check to enable CRL checking.

  • **Use CRL distribution point from the certificate** — Check to obtain the revocation lists distribution URL from the certificate.
Use static URL configured—Check this to add a static, pre-defined distribution URL for revocation lists. Then add the URLs.

CRL Server URLs—The URL of the LDAP server from which the CRL can be downloaded. This URL must start with ldap://, and include a port number in the URL.

• Enable Online Certificate Status Protocol (OCSP)—Check to enable OCSP checking.

OCSP Server URL—The URL of the OCSP server checking for revocation if you require OCSP checks. This URL must start with http://.

• Consider the certificate valid if revocation information can not be reached—Checked by default. Uncheck if you do not want to allow this.

SLA Monitor Objects

Each SLA monitor defines a connectivity policy to a monitored address and tracks the availability of a route to the address. The route is periodically checked for availability by sending ICMP echo requests and waiting for the response. If the requests time out, the route is removed from the routing table and replaced with a backup route. SLA monitoring jobs start immediately after deployment and continue to run unless you remove the SLA monitor from the device configuration (that is, they do not age out). The SLA Monitor Object is used in the Route Tracking field of an IPv4 Static Route Policy. IPv6 routes do not have the option to use SLA monitor via route tracking.

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>N/A</td>
<td>Firepower Threat Defense</td>
<td>Any</td>
<td>Access Admin Administrator Network Admin</td>
</tr>
</tbody>
</table>

Procedure

Step 1 Select Objects > Object Management and choose SLA Monitor from the table of contents.
Step 2 Click Add SLA Monitor.
Step 3 Enter a name for the object in the Name field.
Step 4 (Optional) Enter a description for the object in the Description field.
Step 5 Enter the frequency of ICMP echo request transmissions, in seconds, in the Frequency field. Valid values range from 1 to 604800 seconds (7 days). The default is 60 seconds.

Note The frequency cannot be less than the timeout value; you must convert frequency to milliseconds to compare the values.

Step 6 Enter the ID number of the SLA operation in the SLA Monitor ID field. Values range from 1 to 2147483647. You can create a maximum of 2000 SLA operations on a device. Each ID number must be unique to the policy and the device configuration.

Step 7 Enter the amount of time that must pass after an ICMP echo request before a rising threshold is declared, in milliseconds, in the Threshold field. Valid values range from 0 to 2147483647 milliseconds. The default is 5000 milliseconds. The threshold value is used only to indicate events that exceed the defined value. You can
use these events to evaluate the proper timeout value. It is not a direct indicator of the reachability of the monitored address.

**Note**  The threshold value should not exceed the timeout value.

**Step 8** Enter the amount of time that the SLA operation waits for a response to the ICMP echo requests, in milliseconds, in the **Timeout** field. Values range from 0 to 604800000 milliseconds (7 days). The default is 5000 milliseconds. If a response is not received from the monitored address within the amount of time defined in this field, the static route is removed from the routing table and replaced by the backup route.

**Note**  The timeout value cannot exceed the frequency value (adjust the frequency value to milliseconds to compare the numbers).

**Step 9** Enter the size of the ICMP request packet payload, in bytes, in the **Data Size** field. Values range from 0 to 16384 bytes. The default is 28 bytes, which creates a total ICMP packet of 64 bytes. Do not set this value higher than the maximum allowed by the protocol or the Path Maximum Transmission Unit (PMTU). For purposes of reachability, you might need to increase the default data size to detect PMTU changes between the source and the target. A low PMTU can affect session performance and, if detected, might indicate that the secondary path should be used.

**Step 10** Enter a value for type of service (ToS) defined in the IP header of the ICMP request packet in the **ToS** field. Values range from 0 to 255. The default is 0. This field contains information such as delay, precedence, reliability, and so on. It can be used by other devices on the network for policy routing and features such as committed access rate.

**Step 11** Enter the number of packets that are sent in the **Number of Packets** field. Values range from 1 to 100. The default is 1 packet.

**Note**  Increase the default number of packets if you are concerned that packet loss might falsely cause the Firepower Threat Defense device to believe that the monitored address cannot be reached.

**Step 12** Enter the IP address that is being monitored for availability by the SLA operation, in the **Monitored Address** field.

**Step 13** In the **Zones/Interfaces** list, add the zones that contain the interfaces through which the device communicates with the management station. For interfaces not in a zone, you can type the interface name into the field below the **Selected Zone/Interface** list and click **Add**. The host will be configured on a device only if the device includes the selected interfaces or zones.

**Step 14** Click **Save**.

---

**Prefix Lists**

You can create prefix list objects for IPv4 and IPv6 to use when you are configuring route maps, policy maps, OSPF Filtering, or BGP Neighbor Filtering.

**Configure IPv6 Prefix List**

Use the Configure IPv6 Prefix list page to create, copy and edit prefix list objects. You can create prefix list objects to use when you are configuring route maps, policy maps, OSPF Filtering, or BGP Neighbor Filtering.
Procedure

**Step 1** Select **Objects > Object Management** and choose **Prefix Lists > IPv6 Prefix List** from the table of contents.

**Step 2** Click **Add Prefix List**.

**Step 3** Enter a name for the prefix list object in the **Name** field on the **New Prefix List Object** window.

**Step 4** Click **Add** on the **New Prefix List Object** window.

**Step 5** Select the appropriate action, Allow or Block from the **Action** drop-down list, to indicate the redistribution access.

**Step 6** Enter a unique number that indicates the position a new prefix list entry will have in the list of prefix list entries already configured for this object, in the **Sequence No.** field. If left blank, the sequence number will default to five more than the largest sequence number currently in use.

**Step 7** Specify the IPv6 address in the IP address/mask length format in the **IP address** field. The mask length must be a valid value between 1-128.

**Step 8** Enter the minimum prefix length in the **Minimum Prefix Length** field. The value must be greater than the mask length and less than or equal to the Maximum Prefix Length, if specified.

**Step 9** Enter the maximum prefix length in the **Maximum Prefix Length** field. The value must be greater than or equal to the Minimum Prefix Length, if present, or greater than the mask length if the Minimum Prefix Length is not specified.

**Step 10** Click **Add**.

**Step 11** If you want to allow overrides for this object, check the **Allow Overrides** check box; see **Allowing Object Overrides**, on page 10.

**Step 12** Click **Save**.

**Configure IPv4 Prefix List**

Use the Configure IPv4 Prefix list page to create, copy and edit prefix list objects. You can create prefix list objects to use when you are configuring route maps, policy maps, OSPF Filtering, or BGP Neighbor Filtering.

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>N/A</td>
<td>Firepower Threat</td>
<td>Any</td>
<td>Access Admin Administrator Network Admin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Defense</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Procedure

Step 1  Select **Objects > Object Management** and choose **Prefix Lists > IPv4 Prefix List** from the table of contents.

Step 2  Click **Add Prefix List**.

Step 3  Enter a name for the prefix list object in the **Name** field on the **New Prefix List Object** window.

Step 4  Click **Add**.

Step 5  Select the appropriate action, Allow or Block from the **Action** drop-down list, to indicate the redistribution access.

Step 6  Enter a unique number that indicates the position a new prefix list entry will have in the list of prefix list entries already configured for this object, in the **Sequence No.** field. If left blank, the sequence number will default to five more than the largest sequence number currently in use.

Step 7  Specify the IPv4 address in the IP address/mask length format in the **IP address** field. The mask length must be a valid value between 1-32.

Step 8  Enter the minimum prefix length in the **Minimum Prefix Length** field. The value must be greater than the mask length and less than or equal to the Maximum Prefix Length, if specified.

Step 9  Enter the maximum prefix length in the **Maximum Prefix Length** field. The value must be greater than or equal to the Minimum Prefix Length, if present, or greater than the mask length if the Minimum Prefix Length is not specified.

Step 10  Click **Add**.

Step 11  If you want to allow overrides for this object, check the **Allow Overrides** check box; see **Allowing Object Overrides**, on page 10.

Step 12  Click **Save**.

Route Maps

Route maps are used when redistributing routes into any routing process. They are also used when generating a default route into a routing process. A route map defines which of the routes from the specified routing protocol are allowed to be redistributed into the target routing process. Configure a route map, to create a new route map entry for a Route Map object or to edit an existing one.

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>N/A</td>
<td>Firepower Threat Defense</td>
<td>Any</td>
<td>Access Admin Administrator Network Admin</td>
</tr>
</tbody>
</table>

Before You Begin

A Route Map may use one or more of these objects; it is not mandatory to add all these objects. Create and use any of these objects as required, to configure your route map.

- Add ACLs.
- Add Prefix Lists.
Procedure

Step 1 Select **Objects** > **Object Management** and choose **Route Map** from the table of contents.

Step 2 Click Add Route Map.

Step 3 Click Add on the **New Route Map Object** window.

Step 4 In the **Sequence No.** field, enter a number, between 0 and 65535, that indicates the position a new route map entry will have in the list of route maps entries already configured for this route map object.

**Note** We recommend that you number clauses in intervals of at least 10 to reserve numbering space in case you need to insert clauses in the future.

Step 5 Select the appropriate action, Allow or Block from the **Redistribution** drop-down list, to indicate the redistribution access.

Step 6 Click the **Match Clauses** tab to match (routes/traffic) based on the following criteria, which you select in the table of contents:

- **Security Zones** — Match traffic based on the (ingress/egress) interfaces. You can select zones and add them, or type in interface names and add them.

- **IPv4** — Match IPv4 (routes/traffic) based on the following criteria; select the tab to define the criteria.
  
  1. Click the **Address** tab to match routes based on the route address. For IPv4 addresses, choose whether to use an Access list or Prefix list for matching from the drop-down list and then enter or select the ACL objects or Prefix list objects you want to use for matching.

  2. Click the **Next Hop** tab to match routes based on the next hop address of a route. For IPv4 addresses, choose whether to use an access list or Prefix list for matching from the drop-down list and then enter or select the ACL objects or Prefix list objects you want to use for matching.

  3. Click the **Route Source** tab to match routes based on the advertising source address of the route. For IPv4 addresses, choose whether to use an access list or Prefix list for matching from the drop-down list and then enter or select the ACL objects or Prefix list objects you want to use for matching.

- **IPv6** — Match IPv6 (routes/traffic) based on the route address, next-hop address or advertising source address of route.

- **BGP** — Match BGP (routes/traffic) based on the following criteria; select the tab to define the criteria.

  1. Click the **AS Path** tab to enable matching the BGP autonomous system path access list with the specified path access list. If you specify more than one path access list, then the route can match either path access list.

  2. Click the **Community List** tab to enable matching the BGP community with the specified community. If you specify more than one community, then the route can match either community. Any route that does not match at least one Match community will not be advertised for outbound route maps.

  3. Click the **Policy List** tab to configure a route map to evaluate and process a BGP policy. When multiple policy lists perform matching within a route map entry, all policy lists match on the incoming attribute only.
• Others — Match routes or traffic based on the following criteria.

1. Enter the metric values to use for matching in the Metric Route Value field, to enable matching the metric of a route. You can enter multiple values separated by commas. This setting allows you to match any routes that have a specified metric. The metric values can range from 0 to 4294967295.

2. Enter the tag values to use for matching in the Tag Values field. You can enter multiple values separated by commas. This setting allows you to match any routes that have a specified security group tag. The tag values can range from 0 to 4294967295.

3. Check the appropriate Route Type option to enable matching of the route type. Valid route types are External1, External2, Internal, Local, NSSA-External1, and NSSA-External2. You can choose more than one route type from the list.

**Step 7** Click the Set Clauses tab to set routes/traffic based on the following criteria, which you select in the table of contents:

• Metric Values — Set either Bandwidth, all of the values or none of the values.

1. Enter a metric value or bandwidth in Kbits per second in the Bandwidth field. Valid values are an integer value in the range from 0 to 4294967295.

2. Select to specify the type of metric for the destination routing protocol, from the Metric Type drop-down list. Valid values are: internal, type-1, or type-2.

3. Enter the EIGRP route delay in tens of microseconds in the Delay field. Valid values range from 1 to 4294967295.

4. Enter the likelihood of successful packet transmission for EIGRP in the Reliability field. Valid values range from 0 to 255. The value 255 means 100 percent reliability; 0 means no reliability.

5. Enter the effective EIGRP bandwidth of a route in the Effective field. Valid values range from 1 to 255. The value 255 means 100 percent loading.

6. Enter the minimum MTU size of a route for EIGRP, in bytes in the MTU field. Valid values range from 1 to 4294967295.

• BGP Clauses — Set BGP routes based on the following criteria; select the tab to define the criteria.

1. Click the AS Path tab to modify an autonomous system path for BGP routes.

   a. Enter an AS path number in the Prepend AS Path field to prepend an arbitrary autonomous system path string to BGP routes. Usually the local AS number is prepended multiple times, increasing the autonomous system path length. If you specify more than one AS path number then the route can prepend either AS number.

   b. Enter an AS path number in the Prepend Last AS to AS Path field to prepend the AS path with the last AS number. Enter a value for the AS number from 1 to 10.

   c. Check the Convert route tag into AS path check box to convert the tag of a route into an autonomous system path.

2. Click the Community List tab to set the community attributes.

   a. Click the None radio button, to remove the community attribute from the prefixes that pass the route map.
b Click the **Specific Community** radio button, to enter a community number, if applicable. Valid values are from 1 to 4294967295.

c Check the **Add to existing communities** check box, to add the community to the already existing communities.

d Select the **Internet, No-Advertise**, or **No-Export** check-boxes to use one of the well-known communities.

3 Click the **Others** tab to set additional attributes.

a Check the **Set Automatic Tag** check-box to automatically compute the tag value.

b Enter a preference value for the autonomous system path in the **Set Local Preference** field. Enter a value between 0 and 4294967295.

c Enter a BGP weight for the routing table in the **Set Weight** field. Enter a value between 0 and 65535.

d Select to specify the BGP origin code. Valid values are **Local IGP** Local IGP and **Incomplete**.

e In the IPv4 Settings section, specify a next hop IPv4 address of the next hop to which packets are output. It need not be an adjacent router. If you specify more than one IPv4 address then the packets can output at either IP address.

Select to specify an IPv4 prefix list in the **Prefix List** drop-down list.

f In the IPv6 Settings section, specify a next hop IPv6 address of the next hop to which packets are output. It need not be an adjacent router. If you specify more than one IPv6 address then the packets can output at either IP address.

Select to specify an IPv6 prefix in the **Prefix List** drop-down list.

---

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

**Step 9** If you want to allow overrides for this object, check the **Allow Overrides** check box; see **Allowing Object Overrides**, on page 10.

**Step 10** Click **Save**.

---

### Access List

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>N/A</td>
<td>Firepower Threat Defense</td>
<td>Any</td>
<td>Access Admin Administrator Network Admin</td>
</tr>
</tbody>
</table>

An access list object, also known as an access control list (ACL), selects the traffic to which a service will apply. You use these objects when configuring particular features, such as route maps. Traffic identified as
allowed by the ACL is provided the service, whereas "blocked" traffic is excluded from the service. Excluding traffic from a service does not necessarily mean that it is dropped altogether.

You can configure the following types of ACL:

- Extended—Identifies traffic based on source and destination address and ports. Supports IPv4 and IPv6 addresses, which you can mix in a given rule.
- Standard—Identifies traffic based on destination address only. Supports IPv4 only.

An ACL is composed of one or more access control entry (ACE), or rule. The order of ACEs is important. When the ACL is evaluated to determine if a packet matches an "allowed" ACE, the packet is tested against each ACE in the order in which the entries are listed. After a match is found, no more ACEs are checked. For example, if you want to "allow" 10.100.10.1, but "block" the rest of 10.100.10.0/24, the allow entry must come before the block entry. In general, place more specific rules at the top of an ACL.

Packets that do not match an "allow" entry are considered to be blocked.

The following topics explain how to configure ACL objects.

**Configure Extended ACL Objects**

Use extended ACL objects when you want to match traffic based on source and destination addresses, protocol and port, or if the traffic is IPv6.

**Procedure**

**Step 1** Select Objects > Object Management and choose Access Control Lists > Extended from the table of contents.

**Step 2** Do one of the following:

- Click Add Extended ACL to create a new object.
- Click the edit icon (📝) to edit an existing object.

**Step 3** In the Extended ACL Object dialog box, enter a name for the object (no spaces allowed), and configure the access control entries:

a) Do one of the following:

- Click Add to create a new entry.
- Click the edit icon (📝) to edit an existing entry.

The right-click menu also includes options to cut, copy, and paste entries, or to delete them.

b) Select the Action, whether to Allow (match) or Block (not match) the traffic criteria.

**Note** The Logging, Log Level, and Log Interval options are used for access rules only (ACLs attached to interfaces or applied globally). Because ACL objects are not used for access rules, leave these values at their defaults.

c) Configure the source and destination addresses on the Network tab using any of the following techniques:
Reusable Objects

Configure Standard ACL Objects

Use standard ACL objects when you want to match traffic based on destination IPv4 address only. Otherwise, use extended ACLs.

Procedure

Step 1 Select Objects > Object Management and choose Access Control Lists > Standard from the table of contents.

Step 2 Do one of the following:

* Click Add Standard ACL to create a new object.
* Click the edit icon (📝) to edit an existing object.

Step 3 In the Standard ACL Object dialog box, enter a name for the object (no spaces allowed), and configure the access control entries:

a) Do one of the following:

* Click Add to create a new entry.
• Click the edit icon (📝) to edit an existing entry.

The right-click menu also includes options to cut, copy, and paste entries, or to delete them.

b) For each access control entry, configure the following properties:

• **Action**—Whether to Allow (match) or Block (not match) the traffic criteria.
• **Network**—Add the IPv4 network objects or groups that identify the destination of the traffic.

c) Click **Add** to add the entry to the object.

d) If necessary, click and drag the entry to move it up or down in the rule order to the desired location.

Repeat the process to create or edit additional entries in the object.

**Step 4** If you want to allow overrides for this object, check the **Allow Overrides** check box; see **Allowing Object Overrides**, on page 10.

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

---

### AS Path Objects

An AS Path is a mandatory attribute to set up BGP. It is a sequence of AS numbers through which a network can be accessed. An AS-PATH is a sequence of intermediate AS numbers between source and destination routers that form a directed route for packets to travel. Neighboring autonomous systems (ASes) use BGP to exchange and update messages about how to reach different AS prefixes. After each router makes a new local decision on the best route to a destination, it will send that route, or path information, along with the accompanying distance metrics and path attributes, to each of its peers. As this information travels through the network, each router along the path prepends its unique AS number to a list of ASes in the BGP message. This list is the route's AS-PATH. An AS-PATH along with an AS prefix, provides a specific handle for a one-way transit route through the network. Use the Configure AS Path page to create, copy and edit autonomous system (AS) path policy objects. You can create AS path objects to use when you are configuring route maps, policy maps, or BGP Neighbor Filtering. An AS path filter allows you to filter the routing update message by using regular expressions.

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>N/A</td>
<td>Firepower Threat Defense</td>
<td>Any</td>
<td>Access Admin Administrator Network Admin</td>
</tr>
</tbody>
</table>

**Procedure**

**Step 1** Select **Objects** > **Object Management** and choose **AS Path** from the table of contents.

**Step 2** Click **Add AS Path**.

**Step 3** Enter a name for the AS Path object in the **Name** field. Valid values are between 1 and 500.

**Step 4** Click **Add** on the **New AS Path Object** window.
a) Select the Allow or Block options from the **Action** drop-down list to indicate redistribution access.
b) Specify the regular expression that defines the AS path filter in the **Regular Expression** field.
c) Click Add.

**Step 5** If you want to allow overrides for this object, check the **Allow Overrides** check box; see **Allowing Object Overrides**, on page 10.

**Step 6** Click Save.

### Community Lists

A Community is an optional transitive BGP attribute. A community is a group of destinations that share some common attribute. It is used for route tagging. The BGP community attribute is a numerical value that can be assigned to a specific prefix and advertised to other neighbors. Communities can be used to mark a set of prefixes that share a common attribute. Upstream providers can use these markers to apply a common routing policy such as filtering or assigning a specific local preference or modifying other attributes. Use the Configure Community Lists page to create, copy and edit community list policy objects. You can create community list objects to use when you are configuring route maps or policy maps. You can use community lists to create groups of communities to use in a match clause of a route map. The community list is an ordered list of matching statements. Destinations are matched against the rules until a match is found.

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>N/A</td>
<td>Firepower Threat Defense</td>
<td>Any</td>
<td>Access Admin Administrator Network Admin</td>
</tr>
</tbody>
</table>

### Procedure

**Step 1** Select **Objects > Object Management** and choose **Community List** from the table of contents.

**Step 2** Click **Add Community List**.

**Step 3** In the **Name** field, specify a name for the community list object.

**Step 4** Click **Add** on the **New Community List Object** window.

**Step 5** Select the **Standard** radio button to indicate the community rule type. Standard community lists are used to specify well-known communities and community numbers.

**Note** You cannot have entries using Standard and entries using Expanded community rule types in the same Community List object.

a) Select the Allow or Block options from the **Action** drop-down list to indicate redistribution access.

b) In the **Communities** field, specify a community number. Valid values can be from 1 to 4294967295 or from 0:1 to 65534:65535.

c) Select the appropriate **Route Type**.

- **Internet** — Select to specify the Internet well-known community. Routes with this community are advertised to all peers (internal and external).
• No Advertise — Select to specify the no-advertise well-known community. Routes with this community are not advertised to any peer (internal or external).

• No Export — Select to specify the no-export well-known community. Routes with this community are advertised to only peers in the same autonomous system or to only other sub-autonomous systems within a confederation. These routes are not advertised to external peers.

**Step 6** Select the **Expanded** radio button to indicate the community rule type. Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to specify patterns to match COMMUNITIES attributes.

a) Select the Allow or Block options from the **Action** drop-down list to indicate redistribution access.
b) Specify the regular expression in the **Expressions** field.

**Step 7** Click **Add**.

**Step 8** If you want to allow overrides for this object, check the **Allow Overrides** check box; see **Allowing Object Overrides**, on page 10.

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

---

**Policy Lists**

Use the Configure Policy List page to create, copy, and edit policy list policy objects. You can create policy list objects to use when you are configuring route maps. When a policy list is referenced within a route map, all of the match statements within the policy list are evaluated and processed. Two or more policy lists can be configured with a route map. A policy list can also coexist with any other preexisting match and set statements that are configured within the same route map but outside of the policy list. When multiple policy lists perform matching within a route map entry, all policy lists match on the incoming attribute only.

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>N/A</td>
<td>Firepower Threat Defense</td>
<td>Any</td>
<td>Access Admin Administrator Network Admin</td>
</tr>
</tbody>
</table>

**Procedure**

**Step 1** Select **Objects > Object Management** and choose **Policy List** from the table of contents.

**Step 2** Click **Add Policy List**.

**Step 3** Enter a name for the policy list object in the **Name** field. Object names are not case-sensitive.

**Step 4** Select whether to allow or block access for matching conditions from the **Action** drop-down list.

**Step 5** Click the **Interface** tab to distribute routes that have their next hop out of one of the interfaces specified. In the **Zones/Interfaces** list, add the zones that contain the interfaces through which the device communicates with the management station. For interfaces not in a zone, you can type the interface name into the field below the **Selected Zone/Interface** list and click **Add**. The host will be configured on a device only if the device includes the selected interfaces or zones.
Step 6  Click the Address tab to redistribute any routes that have a destination address that is permitted by a standard access list or prefix list. Choose whether to use an Access List or Prefix List for matching and then enter or select the Standard Access List Objects or Prefix list objects you want to use for matching.

Step 7  Click the Next Hop tab to redistribute any routes that have a next hop router address passed by one of the access lists or prefix lists specified. Choose whether to use an Access List or Prefix List for matching and then enter or select the Standard Access List Objects or Prefix list objects you want to use for matching.

Step 8  Click the Route Source tab to redistribute routes that have been advertised by routers and access servers at the address specified by the access lists or prefix list. Choose whether to use an Access List or Prefix List for matching and then enter or select the Standard Access List Objects or Prefix list objects you want to use for matching.

Step 9  Click the AS Path tab to match a BGP autonomous system path. If you specify more than one AS path, then the route can match either AS path.

Step 10  Click the Community Rule tab to enable matching the BGP community with the specified community. If you specify more than one community, then the route can match either community. To enable matching the BGP community exactly with the specified community, check the Match the specified community exactly check box.

Step 11  Click the Metric & tag tab to match the metric and security group tag of a route.
   a) Enter the metric values to use for matching in the Metric field. You can enter multiple values separated by commas. This setting allows you to match any routes that have a specified metric. The metric values can range from 0 to 4294967295.
   b) Enter the tag values to use for matching in the Tag field. You can enter multiple values separated by commas. This setting allows you to match any routes that have a specified security group tag. The tag values can range from 0 to 4294967295.

Step 12  If you want to allow overrides for this object, check the Allow Overrides check box; see Allowing Object Overrides, on page 10.

Step 13  Click Save.

VPN Objects

Firepower Threat Defense IKE Policies

Internet Key Exchange (IKE) is a key management protocol that is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs). The IKE negotiation comprises two phases. Phase 1 negotiates a security association between two IKE peers, which enables the peers to communicate securely in Phase 2. During Phase 2 negotiation, IKE establishes SAs for other applications, such as IPsec. Both phases use proposals when they negotiate a connection. An IKE proposal is a set of algorithms that two peers use to secure the negotiation between them. IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states which security parameters are used to protect subsequent IKE negotiations.
For IKEv1, IKE proposals contain a single set of algorithms and a modulus group. You can create multiple, prioritized policies to ensure that at least one policy matches a remote peer’s policy. Unlike IKEv1, in an IKEv2 proposal, you can select multiple algorithms and modulus groups in one policy. Since peers choose during the Phase 1 negotiation, this makes it possible to create a single IKE proposal, but consider multiple, different proposals to give higher priority to your most desired options. For IKEv2, the policy object does not specify authentication, other policies must define the authentication requirements.

An IKE policy is required when you configure a site-to-site IPsec VPN. For more information, see Firepower Threat Defense VPN.

Configure IKEv1 Policy Objects

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export-Compliance</td>
<td>N/A</td>
<td>Firepower Threat Defense</td>
<td>Leaf only</td>
<td>Admin</td>
</tr>
</tbody>
</table>

Use the IKEv1 Policy page to create, delete, or edit an IKEv1 policy object. These policy objects contain the parameters required for IKEv1 policies.

Procedure

**Step 1** Choose Objects > Object Management and then VPN > IKEv1 Policy from the table of contents. Previously configured policies are listed including system defined defaults. Depending on your level of access, you may Edit ( ), View ( ), or Delete ( ) a proposal.

**Step 2** (Optional) Choose Add IKEv1 Policy to create a new policy object.

**Step 3** Enter a Name for this policy. A maximum of 128 characters is allowed.

**Step 4** (Optional) Enter a Description for this proposal. A maximum of 1,024 characters is allowed.

**Step 5** Enter the Priority value of the IKE policy.

The priority value determines the order of the IKE policy compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your first priority policy, it tries to use the parameters defined in the next lowest priority. Valid values range from 1 to 65,535. The lower the number, the higher the priority. If you leave this field blank, Management Center assigns the lowest unassigned value starting with 1, then 5, then continuing in increments of 5.

**Step 6** Choose the Encryption method.

When deciding which encryption and Hash Algorithms to use for the IKEv1 policy, your choice is limited to algorithms supported by the peer devices. For an extranet device in the VPN topology, you must choose the algorithm that matches both peers. For IKEv1, select one of the options. For a full explanation of the options, see Deciding Which Encryption Algorithm to Use.

**Step 7** Choose the Hash Algorithm that creates a Message Digest, which is used to ensure message integrity.

When deciding which encryption and Hash Algorithms to use for the IKEv1 proposal, your choice is limited to algorithms supported by the managed devices. For an extranet device in the VPN topology, you must choose the algorithm that matches both peers. For a full explanation of the options, see Deciding Which Hash Algorithms to Use.
**Step 8** Set the **DH Group**. The Diffie-Hellman group to use for encryption. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Select the group that you want to allow in the VPN. For a full explanation of the options, see **Deciding Which Diffie-Hellman Modulus Group to Use**.

**Step 9** Set the **Lifetime** of the security association (SA), in seconds. You can specify a value from 120 to 2,147,483,647 seconds. The default is 86400. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. Generally, the shorter the lifetime (up to a point), the more secure your IKE negotiations. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes.

**Step 10** Set the **Authentication Method** to use between the two peers.

- **Preshared Key**—Preshared keys allow for a secret key to be shared between two peers and to be used by IKE during the authentication phase. If one of the participating peers is not configured with the same preshared key, the IKE SA cannot be established.

- **Certificate**—When you use Certificates as the authentication method for VPN connections, peers obtain digital certificates from a CA server in your PKI infrastructure, and trade them to authenticate each other.

**Note** In a VPN topology that supports IKEv1, the **Authentication Method** specified in the chosen IKEv1 Policy object becomes the default in the IKEv1 **Authentication Type** setting. These values must match, otherwise, your configuration will error.

**Step 11** Click **Save**
The new IKEv1 policy is added to the list.

---

### Configure IKEv2 Policy Objects

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export-Compliance</td>
<td>N/A</td>
<td>Firewall Threat Defense</td>
<td>Leaf only</td>
<td>Admin</td>
</tr>
</tbody>
</table>

Use the IKEv2 policy dialog box to create, delete, and edit an IKEv2 policy object. These policy objects contain the parameters required for IKEv2 policies.

**Procedure**

**Step 1** Choose **Objects > Object Management** and then **VPN > IKEv2 Policy** from the table of contents. Previously configured policies are listed including system defined defaults. Depending on your level of access, you may Edit (📝), View (🔍), or Delete (🗑) a policy.

**Step 2** Choose **Add IKEv2 Policy** to create a new policy.

**Step 3** Enter a **Name** for this policy. The name of the policy object. A maximum of 128 characters is allowed.
Step 4  Enter a **Description** for this policy.
A description of the policy object. A maximum of 1024 characters is allowed.

Step 5  Enter the **Priority**.
The priority value of the IKE proposal. The priority value determines the order of the IKE proposals compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your first priority policy, it tries to use the parameters defined in the next lowest priority policy. Valid values range from 1 to 65535. The lower the number, the higher the priority. If you leave this field blank, Management Center assigns the lowest unassigned value starting with 1, then 5, then continuing in increments of 5.

Step 6  Set the **Lifetime** of the security association (SA), in seconds. You can specify a value from 120 to 2,147,483,647 seconds. The default is 86400. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. Generally, the shorter the lifetime (up to a point), the more secure your IKE negotiations. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes.

Step 7  Choose the **Integrity Algorithms** portion of the Hash Algorithm used in the IKE policy. The Hash Algorithm creates a Message Digest, which is used to ensure message integrity. When deciding which encryption and Hash Algorithms to use for the IKEv2 proposal, your choice is limited to algorithms supported by the managed devices. For an extranet device in the VPN topology, you must choose the algorithm that matches both peers. Select all the algorithms that you want to allow in the VPN. For a full explanation of the options, see [Deciding Which Hash Algorithms to Use](#).

Step 8  Choose the **Encryption Algorithm** used to establish the Phase 1 SA for protecting Phase 2 negotiations. When deciding which encryption and Hash Algorithms to use for the IKEv2 proposal, your choice is limited to algorithms supported by the managed devices. For an extranet device in the VPN topology, you must choose the algorithm that matches both peers. Select all the algorithms that you want to allow in the VPN. For a full explanation of the options, see [Deciding Which Encryption Algorithm to Use](#).

Step 9  Choose the **PRF Algorithm**.
The pseudorandom function (PRF) portion of the Hash Algorithm used in the IKE policy. In IKEv1, the Integrity and PRF algorithms are not separated, but in IKEv2, you can specify different algorithms for these elements. Select all of the algorithms that you want to allow in the VPN. For a full explanation of the options, see [Deciding Which Hash Algorithms to Use](#).

Step 10  Select and **Add a DH Group**.
The Diffie-Hellman group used for encryption. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Select the groups that you want to allow in the VPN. For a full explanation of the options, see [Deciding Which Diffie-Hellman Modulus Group to Use](#).

Step 11  Click **Save**
If a valid combination of choices has been selected the new IKEv2 policy is added to the list. If not, errors are displayed and you must make changes accordingly to successfully save this policy.

---

**Firepower Threat Defense IPsec Proposals**

IPsec Proposals (or Transform Sets) are used when configuring VPN topologies. During the IPsec security association negotiation with ISAKMP, the peers agree to use a particular proposal to protect a particular data flow. The proposal must be the same for both peers.
There are separate IPsec proposal objects based on the IKE version, IKEv1, or IKEv2:

- When you create an IKEv1 IPsec Proposal (Transform Set) object, you select the mode in which IPsec operates, and define the required encryption and authentication types. You can select single options for the algorithms. If you want to support multiple combinations in a VPN, create multiple IKEv1 IPsec Proposal objects.

- When you create an IKEv2 IPsec Proposal object, you can select all of the encryption and Hash Algorithms allowed in a VPN. During IKEv2 negotiations, the peers select the most appropriate options that each support.

The Encapsulating Security Protocol (ESP) is used for both IKEv1 and IKEv2 IPsec Proposals. It provides authentication, encryption, and antireplay services. ESP is IP protocol type 50.

Note
We recommend using both encryption and authentication on IPsec tunnels.

Configure IKEv1 IPsec Proposal Objects

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export-Compliance</td>
<td>N/A</td>
<td>Firepower Threat Defense</td>
<td>Leaf only</td>
<td>Admin</td>
</tr>
</tbody>
</table>

Procedure

Step 1 Choose **Objects > Object Management** and then **VPN > IPsec IKEv1 Proposal** from the table of contents. Previously configured Proposals are listed including system defined defaults. Depending on your level of access, you may Edit (редактирование), View (см. данные), or Delete (удалить) a Proposal.

Step 2 Choose **>Add IPsec IKEv1 Proposal** to create a new Proposal.

Step 3 Enter a **Name** for this Proposal
The name of the policy object. A maximum of 128 characters is allowed.

Step 4 Enter a **Description** for this Proposal.
A description of the policy object. A maximum of 1024 characters is allowed.

Step 5 Choose the **ESP Encryption** method. The Encapsulating Security Protocol (ESP) encryption algorithm for this Proposal.
For IKEv1, select one of the options. When deciding which encryption and Hash Algorithms to use for the IPsec proposal, your choice is limited to algorithms supported by the devices in the VPN. For a full explanation of the options, see **Deciding Which Encryption Algorithm to Use**.

Step 6 Select an option for **ESP Hash**.
For a full explanation of the options, see **Deciding Which Hash Algorithms to Use**.

Step 7 Click **Save**
Configure IKEv2 IPsec Proposal Objects

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export-Compliance</td>
<td>N/A</td>
<td>Firepower Threat</td>
<td>Leaf only</td>
<td>Admin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Defense</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Procedure

**Step 1** Choose **Objects > Object Management** and then **VPN > IKEv2 IPsec Proposal** from the table of contents. Previously configured Proposals are listed including system defined defaults. Depending on your level of access, you may Edit (✏️), View (🔍), or Delete (🗑️) a Proposal.

**Step 2** Choose **Add IKEv2 IPsec Proposal** to create a new Proposal.

**Step 3** Enter a **Name** for this Proposal
The name of the policy object. A maximum of 128 characters is allowed.

**Step 4** Enter a **Description** for this Proposal.
A description of the policy object. A maximum of 1024 characters is allowed.

**Step 5** Choose the **ESP Hash** method, the hash or integrity algorithm to use in the Proposal for authentication. For IKEv2, select all the options you want to support for **ESP Hash**. For a full explanation of the options, see **Deciding Which Hash Algorithm to Use**.

**Step 6** Choose the **ESP Encryption** method. The Encapsulating Security Protocol (ESP) encryption algorithm for this Proposal. For IKEv2, click Select to open a dialog box where you can select all of the options you want to support. When deciding which encryption and Hash Algorithms to use for the IPsec proposal, your choice is limited to algorithms supported by the devices in the VPN. For a full explanation of the options, see **Deciding Which Encryption Algorithm to Use**.

**Step 7** Click **Save**
The new Proposal is added to the list.

Address Pools

You can configure IP address pools for both IPv4 and IPv6 that can be used for the Diagnostic interface with clustering.
## Procedure

### Step 1
Select Objects > Object Management > Address Pools > IPv4 Pools.

### Step 2
Click Add IPv4 Pools, and configure the following fields:

- **Name**—Enter the name of the address pool. It can be up to 64 characters
- **Description**—Add an optional description for this pool.
- **IP Address**—Enter a range of addresses available in the pool. Use dotted decimal notation and a dash between the beginning and the end address, for example: 10.10.147.100-10.10.147.177.
- **Mask**—Identifies the subnet on which this IP address pool resides.
- **Allow Overrides**—Check this check box to enable object overrides. Click the expand arrow to show the Overrides table. You can add a new override by clicking Add. See Object Overrides, on page 8 for more information.

### Step 3
Click Save.

### Step 4
Click Add IPv6 Pools, and configure the following fields:

- **Name**—Enter the name of the address pool. It can be up to 64 characters
- **Description**—Add an optional description for this pool.
- **IPv6 Address**—Enter the first IP address available in the configured pool and the prefix length in bits. For example: 2001:DB8::1/64.
- **Number of Addresses**—Identifies the number of IPv6 addresses, starting at the Starting IP Address, that are in the pool.
- **Allow Overrides**—Check this check box to enable overrides. Click the expand arrow to show the Overrides table. You can add a new override by clicking Add. See Object Overrides, on page 8 for more information.

### Step 5
Click Save.

---

## FlexConfig Objects

Use FlexConfig policy objects in FlexConfig policies to provide customized configuration of features on Firepower Threat Defense devices that you cannot otherwise configure using Firepower Management Center. For more information on FlexConfig policies, see FlexConfig Policy Overview.
You can configure the following types of objects for FlexConfig.

Text Objects

Text objects define free-form text strings that you use as variables in a FlexConfig object. These objects can have single values or be a list of multiple values.

There are several predefined text objects that are used in the predefined FlexConfig objects. If you use the associated FlexConfig object, you simply need to edit the contents of the text object to customize how the FlexConfig object configures a given device. When editing a predefined object, it is in general a better option to create device overrides for each device you are configuring, rather than directly change the default values of these objects. This helps avoid unintended consequences if another user wants to use the same FlexConfig object for a different set of devices.

For information on configuring text objects, see Configure FlexConfig Text Objects.

FlexConfig Objects

FlexConfig Objects include device configuration commands, variables, and scripting language instructions. During configuration deployment, these instructions are processed to create a sequence of configuration commands with customized parameters to configure specific features on the target devices.

These instructions are either configured before (prepended) the system configures features defined in regular Firepower Management Center policies and settings, or after (appended). Any FlexConfig that depends on Firepower Management Center-configured objects (for example, a network object) must be appended to the configuration deployment, or the needed objects would not be configured before the FlexConfig needed to refer to the objects.

For more information on configuring FlexConfig objects, see Configure FlexConfig Objects.