

Objects

Objects are reusable containers that define criteria that you want to use in policies or other settings. For example, network objects define host and subnet addresses.

Objects let you define criteria so that you can easily reuse the same criteria in different policies. When you update an object, all policies that use the object are automatically updated.

- Object Types, on page 1
- Guidelines and Limitations for Objects, on page 4
- Managing Objects, on page 4

Object Types

You can create the following types of object. In most cases, if a policy or setting allows an object, you must use an object.

Object Type	Main Use	Description
AnyConnect Client Profile	Remote access VPN.	AnyConnect Client profiles are downloaded to clients along with the AnyConnect Client software. These profiles define many client-related options, such as auto connect on startup and auto reconnect, and whether the end user is allowed to change the option from the AnyConnect Client preferences and advanced settings. See Configure and Upload Client Profiles.
Application Filter	Access control rules.	An application filter object defines the applications used in an IP connection, or a filter that defines applications by type, category, tag, risk, or business relevance. You can use these objects in policies to control traffic instead of using port specifications. See Configuring Application Filter Objects, on page 9.

Object Type	Main Use	Description
Certificates	Identity policies. Remote access VPN. SSL decryption rules. Management web server.	Digital certificates provide digital identification for authentication. Certificates are used for SSL (Secure Socket Layer), TLS (Transport Layer Security), and DTLS (Datagram TLS) connections, such as HTTPS and LDAPS. See Configuring Certificates.
DNS Groups	DNS settings for the management and data interfaces.	DNS groups define a list of DNS servers and some associated attributes. DNS servers are needed to resolve fully-qualified domain names (FQDN), such as www.example.com, to IP addresses. See Configuring DNS Groups.
Event List Filters	System logging settings for select logging destinations.	Event list filters create a custom filter list for syslog messages. You can use them to limit the messages that are sent to a particular logging location, such as a syslog server or the internal log buffer. See Configure Event List Filters.
Geolocation	Security policies.	A geolocation object defines countries and continents that host the device that is the source or destination of traffic. You can use these objects in policies to control traffic instead of using IP addresses. See Configuring Geolocation Objects, on page 12.
Identity Sources	Identity policies. Remote access VPN. Firewall Device Manager access.	Identity sources are servers and databases that define user accounts. You can use this information in a variety of ways, such as providing the user identity associated with an IP address, or authenticating remote access VPN connections or access to the Firewall Device Manager. See Identity Sources.
IKE Policy	VPN.	Internet Key Exchange (IKE) Policy objects define the IKE proposal used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs). There are separate objects for IKEv1 and IKEv2. See Configuring the Global IKE Policy.
IPsec Proposal	VPN.	IPsec Proposal objects configure the IPsec proposal used during IKE Phase 2 negotiations. The IPsec proposal defines the combination of security protocols and algorithms that secure traffic in an IPsec tunnel. There are separate objects for IKEv1 and IKEv2. See Configuring IPsec Proposals.

Object Type	Main Use	Description
Network	Security policies and a wide variety of device settings.	Network groups and network objects (collectively referred to as network objects) define the addresses of hosts or networks. See Configuring Network Objects and Groups, on page 5.
Port	Security policies.	Port groups and port objects (collectively referred to as port objects) define the protocols, ports, or ICMP services for traffic. See Configuring Port Objects and Groups, on page 6.
Secret Keys	Smart CLI and FlexConfig policies.	Secret key objects define passwords or other authentication strings that you want to encrypt and hide. See Configuring Secret Key Objects.
Security Zone	Security policies.	A security zone is a grouping of interfaces. Zones divide the network into segments to help you manage and classify traffic. See Configuring Security Zones, on page 8.
SGT Groups	Access control policies.	Trustsec Security Group Tags (SGT) define tags for traffic as defined in Cisco Identity Services Engine (ISE). You must configure ISE before you can create these objects. You can then use the objects as source/destination matching criteria in access control rules. See Configuring Security Group Tag (SGT) Groups, on page 15.
SLA Monitors	Static routes.	An SLA Monitor defines a target IP address to use for monitoring a static route. If the monitor determines the target IP address can no longer be reached, the system can install a backup static route. See Configure SLA Monitor Objects.
SSL Ciphers	SSL settings.	An SSL Cipher object defines a combination of security level, TLS/DTLS protocol versions, and encryption algorithms that can be used when establishing an SSL connection to Firewall Threat Defense. Use these objects in the system settings to define the security requirements for users who make TLS/SSL connections to the box. See Configuring TLS/SSL Cipher Settings.

Object Type	Main Use	Description
Syslog Servers	Access control rules. Diagnostic logging. Security Intelligence policies. SSL decryption rules. Intrusion policies. File/malware policies	A syslog server object identifies a server that can receive connection-oriented or diagnostic system log (syslog) messages. See Configuring Syslog Servers, on page 13.
URL	Access control rules. Security Intelligence policies.	URL objects and groups (collectively referred to as URL objects) define the URL or IP addresses of web requests. See Configuring URL Objects and Groups, on page 11.
Users	Remote access VPN.	You can create user accounts directly on the device for use with remote access VPN. You can use the local user accounts instead of, or in addition to, an external authentication source. See Configure Local Users.

Guidelines and Limitations for Objects

- Objects share the same name space. You cannot use the same name for two objects, even if they are different types of objects.
- The system considers the following names reserved. You cannot use these names as object names: object, network, host, fqdn, no, range, subnet, description, nat, after-auto, source, destination, static, dynamic, any, dns, inactive, interface, service, pat-pool, round-robin, extended, flat, include-reserve, tcp, udp, no-proxy-arp, route-lookup, remark, rule-id, access-list, line, ip, icmp, icmp6, advanced, ifc, object-group, vlan, event-log, flow-start, flow-end, both, permit, trust, deny, group-object.

Managing Objects

You can configure objects directly through the Objects page, or you can configure them while editing policies. Either method yields the same results, a new or updated object, so use the technique that suits your needs at the time.

The following procedure explains how you can create and manage your objects directly through the Objects page.

Note When you edit a policy or setting, if a property requires an object, you are shown a list of the ones that are already defined, and you select the appropriate object. If the desired object does not yet exist, simply click the **Create New Object** link shown in the list.

Procedure

Step 1 Select **Objects**.

The Objects page has a table of contents listing the available types of objects. When you select an object type, you see a list of existing objects, and you can create new ones from here. You can also see the object contents and type.

Step 2 Select the object type from the table of contents and do any of the following:

- To create an object, click the + button. The content of the objects differ based on type; see the configuration topic for each object type for specific information.
- To create a group object, click the **Add Group** ( ) button. Group objects include more than one item.
- To edit an object, click the edit icon ( ) for the object. You cannot edit the contents of a pre-defined object.
- To delete an object, click the delete icon ( ) for the object. You cannot delete an object if it is currently being used in a policy or another object, or if it is a pre-defined object.

Configuring Network Objects and Groups

Use network group and network objects (collectively referred to as network objects) to define the addresses of hosts or networks. You can then use the objects in security policies for purposes of defining traffic matching criteria, or in settings to define the addresses of servers or other resources.

A network object defines a single host or network address, whereas a network group object can define more than one address.

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create network objects while editing an address property by clicking the **Create New Network** link shown in the object list.

Procedure

Step 1 Select **Objects**, then select **Network** from the table of contents.

Step 2 Do one of the following:

- To create an object, click the + button.
- To create a group, click the **Add Group** ( ) button.

- To edit an object or group, click the edit icon ( ) for the object.

To delete an unreferenced object, click the trash can icon ( ) for the object.

Step 3 Enter a Name for the object and optionally, a description, and define the object contents.

We recommend that you do not use an IP address alone for the name so that you can easily tell object names from object contents or standalone IP addresses. If you want to use an IP address in the name, prefix it with something meaningful, such as host-192.168.1.2 or network-192.168.1.0. If you use an IP address as the name, the system adds a vertical bar as a prefix, for example, |192.168.1.2. Firewall Device Manager does not show the bar in the object selectors, but you will see this naming standard if you examine the running configuration using the **show running-config** command in the CLI.

Step 4 Configure the contents of the object.

Network Objects

Select the object **Type** and configure the contents:

- **Network**—Enter a network address using one of the following formats:
  - IPv4 network including subnet mask, for example, 10.100.10.0/24 or 10.100.10.0/255.255.255.0.
  - IPv6 network including prefix, for example, 2001:DB8:0:CD30::/60.
- **Host**—Enter a host IP address using one of the following formats:
  - IPv4 host address, for example, 10.100.10.10.
  - IPv6 host address, for example, 2001:DB8::0DB8:800:200C:417A or 2001:DB8:0:0:0DB8:800:200C:417A.
- **Range**—A range of addresses, with the starting and ending address separated by a hyphen. You can specify IPv4 or IPv6 ranges. Do not include masks or prefixes. For example, 192.168.1.10-192.168.1.250 or 2001:DB8:0:CD30::10-2001:DB8:0:CD30::100.
- **FQDN**—Enter a single fully-qualified domain name, such as www.example.com. You cannot use wildcards. Also, select the **DNS Resolution** to determine whether you want the IPv4, IPv6, or both IPv4 and IPv6 addresses associated with the FQDN. The default is both IPv4 and IPv6. You can use these objects in access control rules only. The rules match the IP address obtained for the FQDN through a DNS lookup.

Network Groups

Click the + button to select network objects or groups to add to the group. You can also create new objects.

Step 5 Click **OK** to save your changes.

Configuring Port Objects and Groups

Use port group and port objects (collectively referred to as port objects) to define the protocols, ports, or ICMP services for traffic. You can then use the objects in security policies for purposes of defining traffic matching criteria, for example, to use access rules to allow traffic to specific TCP ports.

A port object defines a single protocol, TCP/UDP port or port range, or ICMP service, whereas a port group object can define more than one service.

The system includes several pre-defined objects for common services. You can use these objects in your policies. However, you cannot edit or delete system-defined objects.

Note When creating port group objects, ensure that the combination of objects makes sense. For example, you cannot have a mixture of protocols in an object if you use it to specify both source and destination ports in an access rule. Exercise care when editing an object that is already being used, or you could invalid (and disable) policies that use the object.

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create port objects while editing a service property by clicking the **Create New Port** link shown in the object list.

Procedure

Step 1 Select **Objects**, then select **Ports** from the table of contents.

Step 2 Do one of the following:

- To create an object, click the + button.
- To create a group, click the **Add Group** ( ) button.
- To edit an object or group, click the edit icon ( ) for the object.

To delete an unreferenced object, click the trash can icon ( ) for the object.

Step 3 Enter a name for the object and optionally, a description, and define the object contents.

Port Objects

Select the **Protocol**, then configure the protocol as follows:

- **TCP**, **UDP**—Enter the single port or port range number, for example, 80 (for HTTP) or 1-65535 (to cover all ports).
- **ICMP**, **IPv6-ICMP**—Select the ICMP **Type** and optionally, the **Code**. Select **Any** for the type to apply to all ICMP messages. For information on the types and codes, see the following pages:
  - ICMP—http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
  - ICMPv6—http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml
- **Other**—Select the desired protocol.

Port Groups

Click the + button to select port objects to add to the group. You can also create new objects.

Step 4 Click **OK** to save your changes.

Configuring Security Zones

A security zone is a grouping of interfaces. Zones divide the network into segments to help you manage and classify traffic. You can define multiple zones, but a given interface can be in one zone only.

The system creates the following zones during initial configuration. You can edit these zones to add or remove interfaces, or you can delete the zones if you no longer use them.

- **inside_zone**—Includes the inside interface. If the inside interface is a bridge group, this zone includes all the bridge group member interfaces instead of the inside Bridge Virtual Interface (BVI). This zone is intended to represent internal networks.
- **outside_zone**—Includes the outside interface. This zone is intended to represent networks external to your control, such as the Internet.

Typically, you would group interfaces by the role they play in your network. For example, you would place the interface that connects to the Internet in the **outside_zone** security zone, and all of the interfaces for your internal networks in the **inside_zone** security zone. Then, you could apply access control rules to traffic coming from the outside zone and going to the inside zone.

Before creating zones, consider the access rules and other policies you want to apply to your networks. For example, you do not need to put all internal interfaces into the same zone. If you have 4 internal networks, and you want to treat one differently than the other three, you can create two zones rather than one. If you have an interface that should allow outside access to a public web server, you might want to use a separate zone for the interface.

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create security zones while editing a security zone property by clicking the **Create New Security Zone** link shown in the object list.

Procedure

Step 1 Select **Objects**, then select **Security Zones** from the table of contents.

Step 2 Do one of the following:

- To create an object, click the + button.
- To edit an object, click the edit icon () for the object.

To delete an unreferenced object, click the trash can icon () for the object.

Step 3 Enter a Name for the object and optionally, a description.

Step 4 Select the **Mode** for the zone.

The mode relates directly to the interface mode. The zone can contain a single type of interface.

- **Routed**—Routed interfaces are the normal interfaces for through traffic that can apply security policies.
- **Passive**—Passive interfaces do not affect traffic that flows through the device.

Step 5 In the **Interfaces** list, click + and select the interfaces to add to the zone.

The list shows all named interfaces that are not currently in a zone. You must configure an interface and give it a name before you can add it to a zone.

If all named interfaces are already in zones, the list is empty. If you are trying to move an interface to a different zone, you must first remove it from its current zone.

Note
You cannot add a bridge group interface (BVI) to a zone. Instead, add the member interfaces. You can put the members into different zones.

Step 6 Click **OK** to save your changes.

Configuring Application Filter Objects

An application filter object defines the applications used in an IP connection, or a filter that defines applications by type, category, tag, risk, or business relevance. You can use these objects in policies to control traffic instead of using port specifications.

Although you can specify individual applications, application filters simplify policy creation and administration. For example, you could create an access control rule that identifies and blocks all high risk, low business relevance applications. If a user attempts to use one of those applications, the session is blocked.

You can select applications and application filters directly in a policy without using application filter objects. However, an object is convenient if you want to create several policies for the same group of applications or filters. The system includes several pre-defined application filters, which you cannot edit or delete.



Note Cisco frequently updates and adds additional application detectors via system and vulnerability database (VDB) updates. Thus, a rule blocking high risk applications can automatically apply to new applications without you having to update the rule manually.

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create application filter objects while editing an access control rule by clicking the **Save As Filter** link after adding application criteria to the Applications tab.

Before you begin

When editing a filter, if a selected application was removed by a VDB update, "(Deprecated)" appears after the application name. You must remove these applications from the filter, or subsequent deployments and system software upgrades will be blocked.

Procedure

Step 1 Select **Objects**, then select **Application Filters** from the table of contents.

Step 2 Do one of the following:

- To create an object, click the + button.
- To edit an object, click the edit icon () for the object.

To delete an unreferenced object, click the trash can icon ( ) for the object.

Step 3 Enter a Name for the object and optionally, a description.

Step 4 In the **Applications** list, click **Add +** and select the applications and filters to add to the object.

The initial list shows applications in a continually scrolling list. Click **Advanced Filter** to see the filter options and to get an easier view for selecting applications. Click **Add** when you have made your selections. You can repeat the process to add additional applications or filters.

Note
Multiple selections within a single filter criteria have an OR relationship. For example, Risk is High OR Very High. The relationship between filters is AND, so Risk is High OR Very High, AND Business Relevance is Low OR Very Low. As you select filters, the list of applications in the display updates to show only those that meet the criteria. You can use these filters to help you find applications that you want to add individually, or to verify that you are selecting the desired filters to add to the rule.

Risks

The likelihood that the application is used for purposes that might be against your organization's security policy, from very low to very high.

Business Relevance

The likelihood that the application is used within the context of your organization's business operations, as opposed to recreationally, from very low to very high.

Types

The type of application:

- **Application Protocol**—Application protocols such as HTTP and SSH, which represent communications between hosts.
- **Client Protocol**—Clients such as web browsers and email clients, which represent software running on the host.
- **Web Application**—Web applications such as MPEG video and Facebook, which represent the content or requested URL for HTTP traffic.

Categories

A general classification for the application that describes its most essential function.

Tags

Additional information about the application, similar to category.

For encrypted traffic, the system can identify and filter traffic using only the applications tagged **SSL Protocol**. Applications without this tag can only be detected in unencrypted or decrypted traffic. Also, the system assigns the **decrypted traffic** tag to applications that the system can detect in decrypted traffic only, not encrypted or unencrypted.

Applications List (bottom of the display)

This list updates as you select filters from the options above the list, so you can see the applications that currently match the filter. Use this list to verify that your filter is targeting the desired applications when you intend to add filter criteria to the rule. If your intention is to add specific applications, select them from this list.

Step 5 Click **OK** to save your changes.

Configuring URL Objects and Groups

Use URL objects and groups (collectively referred to as URL objects) to define the URL or IP addresses of web requests. You can use these objects to implement manual URL filtering in access control policies, or blocking in Security Intelligence policies.

A URL object defines a single URL or IP address, whereas a URL group object can define more than one URL or address.

When creating URL objects, keep the following points in mind:

- If you do not include a path (that is, there are no / characters in the URL), the match is based on the server's hostname only. If you include one or more / character, the entire URL string is used for a substring match. Then, a URL is considered a match if any of the following are true:
  - The string is at the beginning of the URL.
  - The string follows a dot.
  - The string contains a dot in the beginning.
  - The string follows the :// characters.

  For example, ign.com matches ign.com or www.ign.com, but not versign.com.



Note We recommend that you do not use manual URL filtering to block or allow individual web pages or parts of sites (that is, URL strings with / characters), as servers can be reorganized and pages moved to new paths.

- 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 target a specific protocol. 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.
- 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.

  However, please understand that the subject common name in the certificate might be completely unrelated to a web site's domain name. For example, the subject common name in the certificate for youtube.com is *.google.com (this of course might change at any time). You will get more consistent results if you use the SSL Decryption policy to decrypt HTTPS traffic so that URL filtering rules work on decrypted traffic.

Note URL objects will not match HTTPS traffic if the browser resumes a TLS session because the certificate information is no longer available. Thus, even if you carefully configure the URL object, you might get inconsistent results for HTTPS connections.

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create URL objects while editing a URL property by clicking the **Create New URL** link shown in the object list.

Procedure

Step 1 Select **Objects**, then select **URL** from the table of contents.

Step 2 Do one of the following:

- To create an object, click the + button.
- To create a group, click the **Add Group** ( ) button.
- To edit an object or group, click the edit icon ( ) for the object.

To delete an unreferenced object, click the trash can icon ( ) for the object.

Step 3 Enter a Name for the object and optionally, a description.

Step 4 Define the object contents.

URL Objects

Enter a URL or IP address in the **URL** box. You cannot use wildcards in the URL.

URL Groups

Click the + button to select URL objects to add to the group. You can also create new objects.

Step 5 Click **OK** to save your changes.

Configuring Geolocation Objects

A geolocation object defines countries and continents that host the device that is the source or destination of traffic. You can use these objects in policies to control traffic instead of using IP addresses. For example, using geographical location, you could easily restrict access to a particular country without needing to know all of the potential IP addresses used there.

You can typically select geographical locations directly in a policy without using geolocation objects. However, an object is convenient if you want to create several policies for the same group of countries and continents.

Note To ensure that you are using up-to-date geographical location data to filter your traffic, Cisco strongly recommends that you regularly update the geolocation database (GeoDB).

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create geolocation objects while editing a network property by clicking the **Create New Geolocation** link shown in the object list.

Procedure

Step 1 Select **Objects**, then select **Geolocation** from the table of contents.

Step 2 Do one of the following:

- To create an object, click the + button.
- To edit an object, click the edit icon ( ) for the object.

To delete an unreferenced object, click the trash can icon ( ) for the object.

Step 3 Enter a Name for the object and optionally, a description.

Step 4 In the **Continents/Countries** list, click **Add +** and select the continents and countries to add to the object.

Selecting a continent selects all countries within the continent.

Step 5 Click **OK** to save your changes.

Configuring Syslog Servers

A syslog server object identifies a server that can receive connection-oriented or diagnostic system log (syslog) messages. If you have a syslog server set up for log collection and analysis, create objects to define them and use the objects in the related policies.

You can send the following types of events to the syslog server:

- Connection events. Configure the syslog server object on the following types of policy: access control rules and default action, SSL decryption rules and default action, Security Intelligence policy.
- Intrusion events. Configure the syslog server object on the intrusion policy.
- Diagnostic events. See Configure Logging to a Remote Syslog Server.
- File/malware events. Configure the syslog server on **Device** > **System Settings** > **Logging Settings**.

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create syslog server objects while editing a syslog server property by clicking the **Add Syslog Server** link shown in the object list.

Procedure

Step 1 Select **Objects**, then select **Syslog Servers** from the table of contents.

Step 2 Do one of the following:

- To create an object, click the + button.
- To edit an object, click the edit icon ( ) for the object.

To delete an unreferenced object, click the trash can icon ( ) for the object.

Step 3 Configure the syslog server properties:

- **IP Address**—Enter the IP address of the syslog server.
- **Protocol Type**, **Port Number**—Select the protocol and enter the port number to use for syslog. The default is UDP/514. If you select **TCP**, the system can recognize when the syslog server is not available, and stops sending events until the server is available again. The default UDP port is 514, the default TCP port is 1470. If you change the default, the port must be in the range 1025 to 65535.

  Note
  If you use TCP as the transport protocol, the system opens 4 connections to the syslog server to ensure that messages are not lost. If you are using the syslog server to collect messages from a very large number of devices, and the combined connection overhead is too much for the server, use UDP instead.

- **Interface for Device Logs**—Select which interface should be used for sending diagnostic syslog messages. The following types of event always use the management interface: connection, intrusion, file, malware. Your interface selection determines the IP address associated with syslog messages. Select one of the following options:
  - **Data Interface**—Use the data interface you select for diagnostic syslog messages. If the server is accessible through a bridge group member interface, select the bridge group interface (BVI) instead. If it is accessible through the Diagnostic interface (the physical management interface), we recommend that you select **Management Interface** instead of this option. You cannot select a passive interface.

    For connection, intrusion, file, and malware syslog messages, the source IP address will either be for the management interface, or for the gateway interface if you route through data interfaces. Note that there must be appropriate routes in the routing table that direct traffic to the syslog server out the selected interface for these event types.
  - **Management Interface**—Use the virtual Management interface for all types of syslog messages. The source IP address will either be for the Management interface, or for the gateway interface if you route through data interfaces.

Step 4 Click **OK** to save your changes.

Configuring Security Group Tag (SGT) Groups

Use Security Group Tag (SGT) group objects to identify source or destination addresses based on an SGT assigned by Identity Services Engine (ISE). You can then use the objects in access control rules for purposes of defining traffic matching criteria.

You cannot use the information retrieved from ISE directly in an access control rule. Instead, you need to create SGT groups, which refer to the downloaded SGT information. Your SGT groups can refer to more than one SGT, so you can apply policy based on relevant collections of tags if that is appropriate.

For detailed information on how to use SGTs for access control, see How to Control Network Access Using TrustSec Security Group Tags.

Before you begin

Before you create SGT groups, you must configure the ISE identity source to subscribe to SXP mappings and deploy changes. The system then retrieves SGT information from the ISE server. Only after SGTs are downloaded will be you able to create SGT groups.

Procedure

Step 1 Select **Objects**, then select **SGT Groups** from the table of contents.

Step 2 Do one of the following:

- To create an object, click the + button.
- To edit an object, click the edit icon ( ) for the object.

To delete an unreferenced object, click the trash can icon ( ) for the object.

Step 3 Enter a **Name** for the object and optionally, a description,

Step 4 Under **Tags**, click + and select the downloaded SGTs to include in the object.

To remove an SGT, click **x** on the right side of the tag name.

If the list is empty, then the system was not able to download any SGT mappings. If this happens:

- Ensure that the ISE identity object is subscribing to the SXP Topic. You must subscribe to SXP to get the mappings.
- Verify that static mappings are defined in ISE, and that ISE is configured to publish these mappings. If no mappings exist, there is simply nothing to download. See Configure security groups and SXP publishing in ISE.

Step 5 Click **OK**.