



CHAPTER 22

Configuring Cisco Security Group Access Policies

This chapter describes how to configure a Cisco Identity Services Engine (ISE) node as an authentication server, using Cisco security group access policies (SGA). This requires a Cisco SGA solution enabled network.

This chapter covers the following topics:

- [Understanding the SGA Architecture, page 22-1](#)
 - [SGA Features and Terminology, page 22-2](#)
 - [SGA Requirements, page 22-4](#)
- [Configuring ISE to Enable the SGA Solution, page 22-5](#)
 - [Configuring SGA Settings on the Switches, page 22-6](#)
 - [Configuring SGA Devices, page 22-6](#)
 - [Configuring Security Group Access Settings, page 22-8](#)
 - [Configuring Security Groups, page 22-10](#)
 - [Configuring Security Group Access Control Lists, page 22-12](#)
 - [Mapping Security Groups to Devices, page 22-14](#)
 - [Configuring SGA Policy by Assigning SGTs to Devices, page 22-16](#)
- [Assigning Security Groups to Users and End Points, page 22-17](#)
- [Egress Policy, page 22-18](#)
- [OOB SGA PAC, page 22-31](#)
- [SGA CoA, page 22-34](#)

Understanding the SGA Architecture

The Cisco Security Group Access (SGA) solution establishes clouds of trusted network devices to build secure networks. Each device in the Cisco SGA cloud is authenticated by its neighbors (peers). Communication between the devices in the SGA cloud is secured with a combination of encryption, message integrity checks, and data-path replay protection mechanisms. The SGA solution uses the device and user identity information that it obtains during authentication to classify, or color, the packets as they enter the network. This packet classification is maintained by tagging packets when they enter

the SGA network so that they can be properly identified for the purpose of applying security and other policy criteria along the data path. The tag, also called the security group tag (SGT), allows ISE to enforce access control policies by enabling the endpoint device to act upon the SGT to filter traffic.

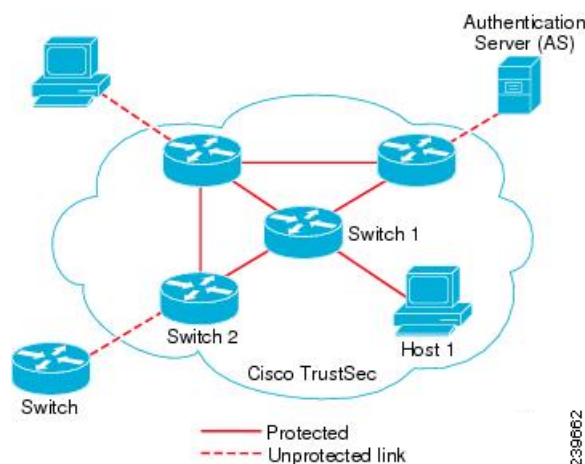
**Note**

You need an Advanced License Package for ISE to enable SGA services.

For more information on the SGA solution, see <http://www.cisco.com/en/US/netsol/ns1051/index.html>.

Figure 22-1 shows an example of an SGA network cloud.

Figure 22-1 SGA Architecture



SGA Features and Terminology

The key features of the SGA solution include:

- **Network Device Admission Control (NDAC)**—In a trusted network, during authentication, each network device (for example ethernet switch) in an SGA cloud is verified for its credential and trustworthiness by its peer device. NDAC uses the IEEE 802.1x port-based authentication and uses Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) as its Extensible Authentication Protocol (EAP) method. Successful authentication and authorization in the NDAC process results in Security Association Protocol negotiation for IEEE 802.1AE encryption.
- **Endpoint Admission Control (EAC)**—An authentication process for an endpoint user or a device connecting to the SGA cloud. EAC typically happens at the access level switch. Successful authentication and authorization in EAC process results in SGT assignment to the user or device. EAC access methods for authentication and authorization includes:
 - 802.1X port-based authentication
 - MAC authentication bypass (MAB)
 - Web authentication (WebAuth)
- **Security Group (SG)**—A grouping of users, endpoint devices, and resources that share access control policies. SGs are defined by the administrator in Cisco ISE. As new users and devices are added to the SGA domain, Cisco ISE assigns these new entities to the appropriate security groups.

- **Security Group Tag (SGT)**—SGA service assigns to each security group a unique 16-bit security group number whose scope is global within an SGA domain. The number of security groups in the switch is limited to the number of authenticated network entities. You do not have to manually configure security group numbers. They are automatically generated, but you have the option to reserve a range of SGTs for IP-to-SGT mapping.
- **Security Group Access Control List (SGACL)**—SGACLs allow you to control the access and permissions based on the SGTs that are assigned. The grouping of permissions into a role simplifies the management of security policy. As you add devices, you simply assign one or more security groups, and they immediately receive the appropriate permissions. You can modify the security groups to introduce new privileges or restrict current permissions.
- **Security Exchange Protocol (SXP)**—SGT Exchange Protocol (SXP) is a protocol developed for SGA service to propagate the IP-to-SGT binding table across network devices that do not have SGT-capable hardware support to hardware that supports SGT/SGACL.
- **Environment Data Download**—The SGA device obtains its environment data from Cisco ISE when it first joins a trusted network. You can also manually configure some of the data on the device. The device must refresh the environment data before it expires. The SGA device obtains the following environment data from Cisco ISE:
 - **Server lists**—List of servers that the client can use for future RADIUS requests (for both authentication and authorization)
 - **Device SG**—Security group to which the device itself belongs
 - **Expiry timeout**—Interval that controls how often the SGA device should download or refresh its environment data
- **SGT Reservation**—An enhancement in ISE to reserve a range of SGTs to enable IP to SGT mapping.
- **IP-to-SGT Mapping**—An enhancement in ISE to bind an endpoint IP to an SGT and provision it to an SGA-capable device.
- **Identity-to-Port Mapping**—A method for a switch to define the identity on a port to which an endpoint is connected, and to use this identity to look up a particular SGT value in the Cisco ISE server.

Table 22-1 lists some of the common terms that are used in the SGA solution and their meaning in an SGA environment.

Table 22-1 SGA Terminology

Term	Meaning
Supplicant	A device that tries to join a trusted network.
Authentication	The process of verifying the identity of each device before allowing it to be part of the trusted network.
Authorization	The process of deciding the level of access to a device that requests access to a resource on a trusted network based on the authenticated identity of the device.
Access control	The process of applying access control on a per-packet basis based on the SGT that is assigned to each packet.
Secure communication	The process of encryption, integrity, and data-path replay protection for securing the packets that flow over each link in a trusted network.
SGA device	Any of the Cisco Catalyst 6000 Series or Cisco Nexus 7000 Series switches that support the SGA solution.

Table 22-1 SGA Terminology (continued)

Term	Meaning
SGA-capable device	An SGA-capable device will have SGA-capable hardware and software. For example, the Nexus 7000 Series Switches with the Nexus operating system.
SGA seed device	The SGA device that authenticates directly against the ISE server. It acts as both the authenticator and supplicant.
Ingress	When packets first encounter an SGA-capable device that is part of a network where the Cisco SGA solution is enabled, they are tagged with an SGT. This point of entry into the trusted network is called the ingress.
Egress	When packets pass the last SGA-capable device that is part of a network where the Cisco SGA solution is enabled, they are untagged. This point of exit from the trusted network is called the egress.

SGA Requirements

To set up a Cisco ISE network that is enabled with the Cisco SGA solution, you need switches that support the SGA solution and other components. [Table 22-2](#) lists the supported Cisco switch platforms.

Table 22-2 SGA Requirements

Supported Cisco Switch Platforms		
Platform	Operating System Version	Requirement
Cisco Nexus 7000 Series	Cisco Nexus operating system 5.0.2a. Note You would need Advanced Service Package license for Cisco SGA.	Mandatory as enforcement point
Cisco Catalyst 6500E Switch with Supervisor Engine 32 or 720 or Virtual Switching System (VSS) 720	Cisco IOS Software 12.2(33) SX13 or later	Optional as an access switch
Cisco Catalyst 4900 Series Switch	Cisco IOS Software 12.2(50) SG7 or later	Optional as an access switch
Cisco Catalyst 4500E Switch with Supervisor 6L-E or 6-E	Cisco IOS Software 12.2(50) SG7 or later	Optional as an access switch
Cisco Catalyst 3750-X or 3560-X Series Switches	Cisco IOS Software 12.2(53) SE1 or later	Optional as an access switch
Cisco Catalyst 3750 or 3560 Series Switches	Cisco IOS Software 12.2(53) SE1 or later	Optional as an access switch
Cisco Catalyst Blade Switch 3000 or 3100 Series	Cisco IOS Software 12.2(53) SE1 or later	Optional as an access switch

Apart from the switches listed in [Table 22-2](#) above, you need other components for identity-based user access control using the IEEE 802.1X protocol. These include Microsoft Windows 2003 or 2008 Server running Microsoft Active Directory, Certificate Authority (CA) server, Domain Name System (DNS)

server, and Dynamic Host Configuration Protocol (DHCP) server. An end host running the Microsoft Windows operating system can also be a part of this environment. [Table 22-3](#) lists other components that may be required for your Cisco SGA environment.

Table 22-3 **Other Components**

Component	Description
User Identity Repository	Although you can use the ISE internal user database, we recommend that you use an external database for identity authentication. ISE supports connections to Microsoft Active Directory and Lightweight Directory Access Protocol (LDAP) service
DHCP Service	Any DHCP server that provides DHCP service. For example, Microsoft Windows Server 2008 DHCP server
DNS Service	Any DNS server that provides DNS service. For example, Microsoft Windows Server 2008 DNS server
Certificate Authority Server	Any Certificate Authority server that provides standalone CA service. For example, Microsoft Windows Server 2008 CA server
Target Servers	Servers that provide Internet services such as HTTP, FTP, Secure Shell (SSH), and even file sharing to test the SGACLs
Endpoint PC	SGA is a supplicant-agnostic solution and does not require any specific agent or IEEE 802.1X supplicant running on the endpoint PC. You can use the Cisco Secure Services Client supplicant, Microsoft Windows or another operating system-embedded supplicant, or other third-party supplicant

To enable Cisco ISE to interoperate with SGA deployments, you must configure SGA switch ports on your switches. See [“Enable Cisco Security Group Access Switch Ports”](#) section on [page C-6](#) for more information.

Configuring ISE to Enable the SGA Solution

This section describes the tasks that you must perform to enable the SGA solution in your Cisco ISE network.



Note

To enable the SGA solution, you need an advanced ISE license. For more information on licensing, see [Chapter 12, “Managing Licenses.”](#)

This section covers the following tasks:

- [Configuring SGA Settings on the Switches, page 22-6](#)
- [Configuring SGA Devices, page 22-6](#)
- [Configuring Security Group Access Settings, page 22-8](#)
- [Configuring Security Group Access AAA Servers, page 22-9](#)
- [Configuring Security Groups, page 22-10](#)
- [Configuring Security Group Access Control Lists, page 22-12](#)
- [Mapping Security Groups to Devices, page 22-14](#)
- [Configuring SGA Policy by Assigning SGTs to Devices, page 22-16](#)

Configuring SGA Settings on the Switches

To enable Cisco ISE to interoperate with SGA deployments, you must configure SGA switch ports on your switches. See “[Enable Cisco Security Group Access Switch Ports](#)” section on page C-6 for more information.

In addition to configuring SGA settings on Cisco ISE, you must also configure some settings on the SGA devices. These configurations vary for the Catalyst and Nexus switches and are described in the Catalyst and Nexus switch configuration guides that are available at:

- For Catalyst 6500 Series Switches:
<http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/trustsec.html>
- For Nexus 7000 Series Switches:
http://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/nx-os/security/configuration/guide/b_Cisco_Nexus_7000_NX-OS_Security_Configuration_Guide__Release_5.x.html
- Configuration Example Using Nexus 7000 Series Switches:
http://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/nx-os/configuration_examples/configuration/guide/Cisco_Nexus_7000_Series_NX-OS_Configuration_Examples_Release_5.x_chapter4.html#con_1191129

Configuring SGA Devices

For Cisco ISE to process requests from SGA-enabled devices, you must define these SGA-enabled devices in Cisco ISE. This section describes how to define SGA-enabled devices in Cisco ISE.

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have any one of the following roles assigned: Super Admin or Network Device Admin. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

To configure an SGA device, complete the following steps:

-
- | | |
|---------------|--|
| Step 1 | Follow the instructions in the “ Adding and Editing Devices ” section on page 6-3 to add a network device. Table 22-4 describes the SGA-specific settings. |
| Step 2 | Click Submit to save the SGA device definition. |
-

Next Step:

[Configuring Security Group Access Settings, page 22-8](#)

Network Devices: SGA Attributes

Table 22-4 lists the SGA-specific fields in the Network Devices page and their descriptions.

Table 22-4 Network Devices: SGA Attributes

Field	Description
SGA Attributes	(Required) Check this check box to configure settings that are specific to the SGA solution. SGA devices use these settings to communicate with ISE.
SGA Notifications and Updates	
Use Device ID for SGA Identification	Check this check box if you want the Device Name to be listed as the device identifier in the Device ID field.
Device Id	(Required) Used for identifying the SGA device. By default, this field is empty. If you check the Use Device ID for SGA Identification check box, then the Device Name appears in this field. You can change this ID to a descriptive name of your choice.
Password	(Required) Password to authenticate the SGA device (same password that you have configured on the SGA device command-line interface [CLI]).
Download Environment Data Every	(Required) Specifies the expiry time for environment data. The SGA device downloads its environment information from ISE. You can configure the time interval in seconds, minutes, hours, or days between these downloads. For example, if you enter 60 sec, the device would download its environment data from ISE every minute. The default value is 86,400 seconds or 1 day. Valid range is from 1 to 24850.
Download Peer Authorization Policy Every	(Required) Specifies the expiry time for the peer authorization policy. The SGA device downloads its peer authorization policy from ISE. You can configure the time interval in seconds, minutes, hours, or days between these downloads. For example, if you enter 60 sec, the device would download its peer authorization policy from ISE every minute. The default value is 86,400 seconds or 1 day. Valid range is from 1 to 24850.
Reauthentication Every	(Required) Specifies the 802.1X reauthentication period. In a network that is configured with the SGA solution, after initial authentication, the SGA device reauthenticates itself against ISE. You can configure the time interval in seconds, minutes, hours, or days between these authentications. For example, if you enter 1000 sec, the device would authenticate itself against ISE every 1000 sec. The default value is 86,400 seconds or 1 day. Valid range is from 1 to 24850.
Download SGACL Lists Every	(Required) Specifies the expiry time for SGACL lists. The SGA device downloads the SGACLs from ISE. You can configure the time interval between these downloads. For example, if you enter 3600 sec, the device obtains the SGACL lists from ISE every 3600 sec. The default value is 86,400 seconds or 1 day. Valid range is from 1 to 24850.
Other SGA Devices to Trust This Device (SGA Trusted)	Check this check box if you want all the peer devices to trust this device. If you uncheck this device, the peer devices do not trust it, and all packets that arrive from this device will be colored or tagged accordingly. This option is enabled by default.
Include This Device When Deploying Security Group Tag Mapping Updates	Check this check box if you want this SGA device to obtain the IP-SGT mappings using the Device Configuration credentials.

Table 22-4 Network Devices: SGA Attributes (continued)

Field	Description
Notify this device about SGA configuration changes	Check this check box if you want ISE to send SGA CoA notifications to this SGA device. This option is enabled by default.
Out of Band (OOB) SGA PAC	
Issuing Date ¹	Holds the issuing date of the last SGA PAC that has been generated by ISE for this device.
Expiration Date ¹	Holds the expiration date of the last SGA PAC that has been generated by ISE for this device.
Issued By ¹	Holds the name of the issuer (an SGA administrator) of the last SGA PAC that has been generated by ISE for this device.

1. This field is read only and is always disabled, and empty by default. It is automatically populated with the issuing date, expiration date or issuer of the last SGA PAC that has been generated for this device in ISE. See [SGA PAC Provisioning](#), page 22-31 for details on how to generate SGA PAC.

Configuring Security Group Access Settings

For ISE to function as an SGA server and provide SGA services, you must define some global SGA settings. This section describes how to complete this task.

Prerequisites:

- Before you configure global SGA settings, ensure that you have defined global EAP-FAST settings (choose **Administration > System > Global Options > Protocol Settings > EAP-FAST > EAP-FAST Settings**).

You must change the Authority Identity Info Description to your Cisco ISE server name. This description is a user-friendly string that describes the ISE server that sends credentials to an endpoint client. The client in a Cisco SGA architecture can be either the endpoint running EAP-FAST as its EAP method for IEEE 802.1X authentication or the supplicant network device performing NDAC. The client can discover this string in the protected access credentials (PAC) type-length-value (TLV) information. The default value is Cisco Identity Services Engine. You should change the value so that the ISE PAC information can be uniquely identified on network devices upon NDAC authentication.

- Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have any one of the following roles assigned: Super Admin or Policy Admin. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

To configure general SGA settings, complete the following steps:

-
- Step 1** Choose **Administration > System > Settings**.
- Step 2** From the Settings navigation pane on the left, click **Security Group Access**.
The Security Group Access page appears.
- Step 3** Enter the values as described:

- **Tunnel PAC Time to Live**—Specifies the expiry time for the PAC. The tunnel PAC generates a tunnel for the EAP-FAST protocol. You can specify the time in seconds, minutes, hours, days, or weeks. The default value is 90 days. Valid ranges are:
 - 1 to 157680000 seconds
 - 1 to 2628000 minutes
 - 1 to 43800 hours
 - 1 to 1825 days
 - 1 to 260 weeks
- **Proactive PAC Update Will Occur After**—The proactive PAC update time is configured in this field. ISE proactively provides a new PAC to the client after successful authentication when a configured percentage of the Tunnel PAC TTL remains. The tunnel PAC update is initiated by the server after the first successful authentication that is performed before the PAC expiration. This mechanism allows the client to be always updated with a valid PAC. The default value is 10%. Valid range is from 1 to 100.
- **All Tags Automatically Generated by System**—Choose this option if you want all the SGTs to be automatically generated by Cisco ISE. See the [“Mapping Security Groups to Devices” section on page 22-14](#) for more information.

**Note**

Cisco recommends that you use this option only if you plan to manually configure specific security groups and policies on the SGA device.

- **Reserve a Range**—Choose this option if you want to reserve a range of security group tags (SGTs) to be configured on the device manually. If you choose this option, you must also specify a range from 1 to 65535.

Cisco ISE creates an SGT by default: Unknown, which has takes the value of 0.

**Note**

If you configure a range of SGTs, Cisco ISE will not use the values in this range while generating SGT values.

Step 4 Click **Save** to save the general SGA settings.

Next Step:

[Configuring Security Group Access AAA Servers, page 22-9](#)

Configuring Security Group Access AAA Servers

You can configure a list of Cisco ISE servers in your deployment in the AAA server list to allow SGA devices to be authenticated against any of these servers. When you add ISE servers to this list, all these server details are downloaded to the SGA device. When an SGA device tries to authenticate, it would choose any ISE server from this list and, if the first server is down or busy, the SGA device can authenticate itself against any of the other servers from this list. By default, the primary ISE server is an SGA AAA server. We recommend that you configure additional ISE servers in this AAA server list (**Administration > Network Resources > SGA AAA Servers**) so that if one server is busy, another server from this list can handle the SGA request.

This page lists the ISE servers in your deployment that you have configured as your SGA AAA servers. You can click the **Push** button to initiate an environment CoA notification after you configure multiple SGA AAA servers. This environment CoA notification goes to all SGA network devices and provides an update of all SGA AAA servers that were changed.

Related Topics

[Adding and Editing Security Group Access AAA Servers](#)

Adding and Editing Security Group Access AAA Servers

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have any one of the following roles assigned: Super Admin or Network Device Admin. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

To add or edit the AAA server list, complete the following steps:

-
- Step 1** Choose **Administration > Network Resources > SGA AAA Servers**.
The AAA Servers page appears.
- Step 2** Do one of the following:
- Click **Add** to add an ISE server to this list.
 - Check the check box next to the ISE server that you want to edit, and then click **Edit**.
- Step 3** Enter the values as described:
- Name—(Required) Name that you want to assign to the ISE server in this AAA Server list. This name can be different from the hostname of the ISE server.
 - Description—An optional description.
 - IP—(Required) IP address of the ISE server that you are adding to the AAA Server list.
 - Port—(Required) Port over which communication between the SGA device and server should take place. The default is 1812.
- Step 4** Click **Submit** to save the changes.
-

Next Step:

[Configuring Security Groups, page 22-10](#)

Configuring Security Groups

A security Group (SG) or Security Group Tag (SGT) is an element that is used in SGA policy configuration. SGTs are attached to packets when they move within a trusted network. These packets are tagged when they enter a trusted network (ingress) and untagged when they leave the trusted network (egress).

SGTs are automatically generated in a sequential manner, but you have the option to reserve a range of SGTs for IP to SGT mapping. ISE skips the reserved numbers while generating SGTs.

If you have deleted a particular security group, the SGT assigned to this security group does not get reused until all the succeeding SGTs are deleted.

For example, if you have SGTs 2, 3, and 4 defined and you delete SGT 2, the next SGT that is generated would be SGT 5. If you want SGT 2 to be generated next, you must delete SGTs 3 and 4.

SGA service uses these SGTs to enforce the SGA policy at egress. See the [“Configuring SGA Policy by Assigning SGTs to Devices”](#) section on page 22-16.

You can configure security groups from the following ISE administrative user interfaces:

- **Policy > Policy Elements > Results > Security Group Access > Security Groups.** See the [“Adding and Editing Security Groups”](#) section on page 22-11 for more information.
- Directly from egress policy page. See [Configuring SGT and SGACL from Egress Policy](#), page 22-27 to configure SGT from egress policy page.
- Clicking the **Generate SGTs** button on the **Policy > Policy Elements > Results > Security Group Access > Security Groups** page. See the [“Adding and Editing Security Groups”](#) section on page 22-11 for more information.

You can click the **Push** button to initiate an environment CoA notification after updating multiple SGTs. This environment CoA notification goes to all SGA network devices and provides an update of all SGTs that were changed.

Related Topics

[Adding and Editing Security Groups](#)

Adding and Editing Security Groups

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have any one of the following roles assigned: Super Admin or Policy Admin. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

To add or edit a security group, complete the following steps:

-
- | | |
|---------------|--|
| Step 1 | Choose Policy > Policy Elements > Results . |
| Step 2 | From the Results navigation pane on the left, click the > button next to Security Group Access and click Security Groups .

The Security Groups page appears. There is a default security group in ISE: Unknown. This page provides the name, the SGT in decimal and hexadecimal formats, and an optional description of the security groups. |
| Step 3 | Click Generate SGTs . |
| Step 4 | Do one of the following: <ul style="list-style-type: none">• Click Add to add a new security group.• From the navigation pane, click the expand button next to Security Groups and select the security group that you want to edit, or check the check box next to the security group in the list page that you want to edit, and click Edit. |



Note You cannot edit the predefined unknown security group.

Step 5 Enter the values as described:

- **Name**—Name of the security group.
- **Description**—An optional description of the security group.
- **Allow System to Automatically Generate Tag**—(Visible only if you have chosen the Reserve a Range option in the Security Group Access Settings page) Choose this option if you want ISE to generate an SGT automatically. The tag value will be automatically populated if you choose this option. This option will be visible only if you reserve a range of SGTs while configuring the Global SGA settings. See the [“Configuring Security Group Access Settings” section on page 22-8](#) for more information.
- **Select Value from Reserved Range**—(Visible only if you have chosen the Reserve a Range option in the Security Group Access Settings page) Choose this option if you want to assign an SGT from the reserved range to a specific IP address. This option will be visible only if you reserve a range of SGTs while configuring the Global SGA settings. See the [“Configuring Security Group Access Settings” section on page 22-8](#) for more information.
- **Security Group Tag (Dec/Hex)**—ISE assigns this value automatically. This value is sequentially numbered from 0 to 65,535. You can reserve a range of tags for specific security groups and ensure that these numbers are not automatically generated. See the [“Configuring Security Group Access Settings” section on page 22-8](#) for more information.

Step 6 Click **Submit** to save the security group.



Note

Each security group in your SGA solution should be assigned a unique SGT. Even though ISE supports 65,535 SGTs, having fewer number of SGTs would enable you to deploy and manage the SGA solution easily. We recommend a maximum of 64000 SGTs.

Next Steps:

- [Configuring Security Group Access Control Lists, page 22-12](#)
- [Assigning Security Groups to Users and End Points, page 22-17](#)

Configuring Security Group Access Control Lists

Security group access control lists (SGACLs) are permissions that will be assigned after the SGA policy evaluation. SGACLs restrict the operations that a user can perform based on the role of the user instead of the IP address or subnet mask alone. You can configure SGACLs from the ISE administrative user interface (**Policy > Policy Elements > Results > Security Group Access > Security Group ACLs**). You can also configure the security groups ACLs directly from the egress policy page. See [Configuring SGT and SGACL from Egress Policy, page 22-27](#) to configure SGACLs from the egress policy page.

You can click the **Push** button to initiate an environment CoA notification after updating multiple SGACLs. This environment CoA notification goes to all SGA network devices and provides an update of all SGACLs that were changed.

See [“Adding and Editing Security Group Access Control Lists” section on page 22-13](#) for more information.

Adding and Editing Security Group Access Control Lists

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have any one of the following roles assigned: Super Admin or Policy Admin. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

To create or edit an SGACL, complete the following steps:

-
- Step 1** Choose **Policy > Policy Elements > Results**.
- Step 2** From the Results navigation pane on the left, click the > button next to Security Group Access and click **Security Group ACLs**.
- The Security Group ACLs page appears with a list of SGACLs and provides the following information:
- Name—Name of the SGACL
 - Description—An optional description of the SGACL
 - IP Version—IP version that this SGACL supports:
 - IPv4—Supports IP version 4 (IPv4)
 - IPv6—Supports IP version 6 (IPv6)
 - Agnostic—Supports both IPv4 and IPv6
- Step 3** Do one of the following:
- Click **Add** to add an SGACL.
 - Check the check box next to the SGACL that you want to edit, and then click **Edit** or select the SGACL from the Security Group ACLs object selector.
- Step 4** Enter the values as described:
- Name—(Required) Name of the SGACL.
 - Description—An optional description of the SGACL.
 - IP Version—Specifies which IP version this SGACL supports.
 - IPv4—Supports IPv4
 - IPv6—Supports IPv6
 - Agnostic—Supports both IPv4 and IPv6
 - Security Group ACL Content—(Required) Access control list (ACL) commands. For example:
permit icmp
deny all
- Step 5** Click **Submit** to save the SGACL.
-

The Nexus 7000 Series with Cisco Nexus operating system 4.2 supports the following access control list entries:

deny all

deny icmp

```
deny igmp
deny ip
deny tcp [{dest | src} {{eq | gt | lt | neq} port-number | range port-number1 port-number2}]
deny udp [{dest | src} {{eq | gt | lt | neq} port-number | range port-number1 port-number2}]
permit all
permit icmp
permit igmp
permit ip
permit tcp [{dest | src} {{eq | gt | lt | neq} port-number | range port-number1 port-number2}]
permit udp [{dest | src} {{eq | gt | lt | neq} port-number | range port-number1 port-number2}]
```

For more information on syntax and usage, go to:

http://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/nx-os/security/command/reference/sec_cmds_d.html#wp1057446

When you change SGACL ACE, SGACL name, or IP version of an SGACL, all the accumulative changes can be pushed to the SGA network devices by clicking the **Push** button. See [Update RBACL Named List CoA](#), page 22-37 for more details.

Next Step:

[Configuring SGA Policy by Assigning SGTs to Devices](#), page 22-16

Mapping Security Groups to Devices

Cisco ISE allows you to assign an SGT to an SGA device if you know the device hostname or IP address. When a device with the specific hostname or IP address joins the network, ISE will assign the SGT before authenticating it. You can create this mapping from the Security Group Mappings page. Before you perform this action, ensure that you have reserved a range of SGTs. See [Reserve a Range](#) option for more information. You can map the security groups to devices from the ISE administrative user interface (**Policy > Policy Elements > Results > Security Group Access > Security Group Mappings**). This page lists the security group mappings that you have configured.

See “[Adding and Editing Security Group Mappings](#)” section on page 22-14 for more information.

Adding and Editing Security Group Mappings

Cisco ISE allows you to add and edit security group mappings from the Cisco ISE user interface. This section describes how to complete this task.

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have any one of the following roles assigned: Super Admin or Policy Admin. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

To create or edit a security group mapping, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results navigation pane on the left, click the > button next to Security Group Access and click **Security Group Mappings**.

The Security Group Mappings page appears.

Step 3 Do one of the following:

- Click **Add** to add a new security group mapping.
- Check the check box next to an existing security group mapping that you want to edit, and then click **Edit**.
- Check the check box next to an existing security group mapping that you want to reassign, and then click **Reassign Groups**. See the “[Reassigning SGTs to Devices](#)” section on page 22-15 for more information.
- Check the check box next to an existing security group mapping that you want to deploy, and then click **Deploy**. See the “[Deploying SGTs on SGA Devices](#)” section on page 22-15 for more information.
- Check the check box next to an existing security group mapping whose status you want to check, then choose >> and click **Check Status**. See the “[Checking the Status of Security Group Mapping on Devices](#)” section on page 22-15 for more information.

Step 4 Enter the values as described in [Table 22-5](#).

Table 22-5 Security Group to Host Mappings

Field	Description
Security Group	Click Select to choose an SGT to be applied to this device.
Hostname	Enter the hostname of the SGA device.
IP Address	Enter the IP address of the SGA device.

Step 5 Click **Submit** to save the settings.

Step 6 Click the **Security Group Mapping List** link at the top of this screen to go back to the list page.

You can also set filters to view only certain records. You can set a Quick Filter based on a simple condition or an Advanced Filter for an enhanced search. You can also save the advanced custom view.

Deploying SGTs on SGA Devices

You can check the check box next to the security group mapping and click **Deploy** to download the SGT to the SGA device. This option connects to the device through SSH and runs the command to download the SGT on the device. Click **OK** to close this page.

Checking the Status of Security Group Mapping on Devices

You can check the check box next to the security group mapping and click **Check Status** to see if the SGTs have been downloaded on the device. This option allows you to check the status on the SGA device. Click **OK** to close this page.

Reassigning SGTs to Devices

You can check the check box next to the security group mappings and click **Reassign Groups** to assign a different SGT to a set of devices. The Reassign Security Groups page appears:

1. Click **Select** to select the new SGT.

2. Click **OK** to save the changes.

**Note**

You can use the Edit option to edit the SGT mapping for a single device. To change the SGT mapping for multiple devices at the same time, you can use the Reassign Groups option.

Configuring SGA Policy by Assigning SGTs to Devices

Cisco ISE allows you to configure the SGA policy by assigning SGTs to devices. This section describes how to complete this task.

Prerequisites:

- Before you configure an SGA policy, you must create the security groups for use in the policy. See the [“Configuring Security Groups” section on page 22-10](#) for more information.

You can assign security groups to devices by using the SGA device ID.

- Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have any one of the following roles assigned: Super Admin or Policy Admin. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

To configure an SGA policy, complete the following steps:

Step 1 Choose **Policy > Security Group Access > Network Device Authorization**.

The Network Device Authorization page appears. You can define an SGA device policy on this page based on conditions. Cisco ISE supports device attributes for use in policy conditions:

Step 2 Click the action icon in the Default Rule row and click **Insert New Row Above**.

Step 3 Click the drop-down list box to select the status of this rule. The Status can be any one of the following:

- Enable—The policy rule is active.
- Disable—The policy rule is inactive and will not be evaluated.
- Monitor—The policy rule will be evaluated, but the result will not be enforced. You can use this option for testing purposes. You can view the results of this policy condition in the monitoring and report viewer. For example, you may want to add a new policy condition, but are not sure if the condition would provide you with the correct results. In this situation, you can create the policy condition in the monitored mode to view the results and then enable it if you are satisfied with the results.

Step 4 Enter the name for this rule in the first text box.

Step 5 Click the plus sign (+) next to Conditions to add a policy condition.

Step 6 Click **Create New Condition (Advance Option)**.

- a. From the Expression drop-down list box, choose any one of the following attributes to define the policy condition. For example, Device Type:
 - SGADeviceID
 - Device Type
 - Location

- Model Name
- Software Version
- b. Select the operator from the drop-down list box. You can select EQUALS (is equal to), NOT EQUALS (is not equal to), or MATCHES (is an exact match of).
- c. Enter a value for the attribute. For example Nexus 7K.

You can create a compound condition by adding more conditions using the AND or OR operator.

- d. To create a compound condition, from within the Conditions popup, click the action icon that appears in the same row as the condition that you have already created, and click **Add Attribute/Value** to add a new row. Repeat the process as described in [Step 5a](#).

**Note**

While creating a compound condition, you can only use AND or OR operator throughout. You cannot use both AND and OR operators in the same compound condition.

For example, you can create a compound condition that checks for all devices in New York and are of the Catalyst 6K model. Your compound condition would appear as follows:


DEVICE:Location EQUALS All Locations:New York

AND

DEVICE:Model Name EQUALS Catalyst 6K

Step 7 Click the minus sign (-) in the popup to close it.

Step 8 From the Security Group drop-down list, select the SGT that you want to assign if this condition evaluates to true.

Step 9 Click the action icon from this row to add additional rules based on device attributes either above or below the current rule. You can repeat this process to create all the rules that you need for the SGA policy. You can drag and drop the rules to reorder them by clicking the  icon. You can also duplicate an existing condition, but ensure that you change the policy name.

The first rule that evaluates to true determines the result of the evaluation. If none of the rules match, the default rule will be applied; you can edit the default rule to specify the SGT that must be applied to the device if none of the rules match.

Step 10 Click **Save** to save your SGA policy.

If an SGA device tries to authenticate after you have configured the network device policy, the device will get its SGT and the SGT of its peers and will be able to download all the relevant details.

Assigning Security Groups to Users and End Points

ISE allows you to assign a security group as the result of an authorization policy evaluation. Using this option, you can assign a security group to users and end points.

Prerequisites:

- Read the “[Understanding Authorization Policies](#)” section on page 17-1 for information on authorization policies.

- Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have any one of the following roles assigned: Super Admin or Policy Admin. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

To assign security groups to users and endpoints, complete the following steps:

-
- Step 1** Create a new authorization policy as described in “[Creating a New Authorization Policy](#)” section on [page 17-14](#).
- Step 2** For Permissions, instead of selecting an authorization profile, select a security group.
- If the conditions specified in this authorization policy is true for a user or endpoint, then this security group will be assigned to that user or endpoint and all data packets that are sent by this user or endpoint will be tagged with this particular SGT.
-

Egress Policy

The egress table lists the source and destination SGTs, both reserved and unreserved. This page also allows you to filter the egress table to view specific policies and also to save custom views. When the source SGT tries to reach the destination SGT, the SGA-capable device enforces the SGACLs based on the SGA policy as defined in the Egress Policy. ISE creates and provisions the policy.

After you create the SGTs and SGACLs, which are the basic building blocks required to create an SGA policy, you can establish a relationship between them by assigning SGACLs to source and destination SGTs.

Each combination of a source SGT to a destination SGT is a cell in the egress policy.



Tip

Before you create the SGA policy, you can configure security groups and SGACLs. See the “[Configuring Security Groups](#)” section on [page 22-10](#) and the “[Configuring Security Group Access Control Lists](#)” section on [page 22-12](#) for more information.

This section contains the following:

- [Viewing the Egress Policy, page 22-19](#)
- [Matrix Operations, page 22-22](#)
- [Sorting and Filtering Egress Policy Table, page 22-22](#)
- [Configuring Egress Policy Table Cells, page 22-25](#)
- [Configuring SGT and SGACL from Egress Policy, page 22-27](#)
- [The Unknown Security Group, page 22-30](#)

Viewing the Egress Policy

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have any one of the following roles assigned: Super Admin or Policy Admin. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

To view the egress policy:

Step 1 Choose **Policy > Security Group Access > Egress Policy**.

The Egress Policy page appears with the following elements:

- **Header**—Shows the Egress Policy and the selected view in parenthesis. That is, Egress Policy (Matrix View) or Egress Policy (Source Tree view) or Egress Policy (Destination view)
- **View tabs**—Allows you to jump among the three views.
- **Toolbar**—Contains buttons and widgets that are common to all views. [Table 22-6](#) lists all the toolbar items.

Table 22-6 Egress Policy Page Options

Option	Description
Edit	Opens the Edit Permissions popup to edit the configuration of the selected mapped cell. This feature is enabled when at least one mapped cell is selected.
Add	Opens the Create Security Group ACL Mapping popup to configure the selected unmapped cells.
Clear Mapping	Deletes the configuration of a selected mapped cell. This feature is enabled when at least one mapped cell is selected. It does not have any impact on the unmapped cells.
Configure	Allows you to create SGTs and SGACLs directly. See Configuring SGT and SGACL from Egress Policy, page 22-27 .
Push	Pushes the Egress Policy data to the SGA network devices. See Push Button, page 22-28 .
Monitor All	Changes the status of all enabled cells to Monitor mode automatically when this option is selected. See Monitor Mode, page 22-28 .
Dimension	Allows you to change the dimension of the matrix cells. This works only in the Matrix view.
Content Area	Displays and manages the Egress Policy data in different views.
Show	Manages the Filters and Preset Filters.
Default Policy	Shows the default policy configuration settings.

You can view the Egress policy in three different ways:

- [Source Tree, page 22-20](#)
- [Destination Tree, page 22-20](#)

- [Matrix View, page 22-20](#)

Source Tree

The Source Tree view lists a compact and organized view of source SGTs in a collapsed state. You can expand any source SGT to see the internal table that lists all information related to that selected source SGT. This view displays only the source SGTs that are mapped to destination SGTs. If you expand a specific source SGT, it lists all destination SGTs that are mapped to this source SGT and their configurations in a table.

You will see three dots (...) next to some fields. This signifies that there is more information contained in the cell. You can position the cursor over the three dots to view the rest of the information in a quick view popup. When you position the cursor over an SGT name or an SGACL name, a quick view popup opens to display the content of that particular SGT or SGACL.

Destination Tree

The Destination Tree view lists a compact and organized view of destination SGTs in a collapsed state. You can expand any destination SGTs to see the internal table that lists all information related to that selected destination SGT. This view displays only the destination SGTs that are mapped to source SGTs. If you expand a specific destination SGT, it lists all source SGTs that are mapped to this destination SGT and their configurations in a table.

You will see three dots (...) next to some fields. This signifies that there is more information contained in the cell. You can position the cursor over the three dots to view the rest of the information in a quick view popup. When you position the cursor over an SGT name or an SGACL name, a quick view popup opens to display the content of that particular SGT or SGACL.

Matrix View

The Matrix View of the Egress policy looks like a spreadsheet. It contains two axis:

- Source Axis—The vertical axis lists all the source SGTs.
- Destination Axis—The horizontal axis lists all the destination SGTs.

The mapping of a source SGT to a destination SGT is represented as a cell. If a cell contains data, then it represents that there is a mapping between the corresponding source SGT and the destination SGT. There are two types of cells in the matrix view:

- Mapped cells—When a source and destination pair of SGTs is related to a set of ordered SGACLs and has a specified status.
- Unmapped cells—When a source and destination pair of SGTs is not related to any SGACLs and has no specified status.

[Table 22-7](#) lists the fields of the mapped cells and the descriptions.

Table 22-7 **Mapped Cell Fields**

Field	Description
Source Security Group	Contains the name of the source SGT and its decimal and hexadecimal value in the format Name (Dec/Hex). For example: Employee (75/004B).
Destination Security Group	Contains the name of the destination SGT and its decimal and hexadecimal value in the same format as Source Security Group.
Status	This field shows the status of the mapping. You can configure the following three status: <ul style="list-style-type: none"> • Enabled—The SGA device downloads the list of SGACLs from the cell and enforce the policy accordingly. • Disabled—The SGA device ignores this cell. It will not download the list of SGACLs from this cell. • Monitored—The SGA device downloads the list of SGACLs from this cell. It will not enforce the policy accordingly. It just monitors the cell by logging a match between packets and the cell. <p>Note The default status is Enabled. Only Enabled and Monitored status are available for the default policy.</p>
Description	(Optional). You can add a description to the cell.
Security Group ACLs	(Required) Contains the ordered list of SGACLs. Note This is not a mandatory field for default policy. It can be empty.
Final Catch All Rule	(Required) Contains the set of ACEs defined by the SGACLs list. The status can be any one of the following values: <ul style="list-style-type: none"> • Permit IP • Deny IP • None <p>Note The default value is Permit IP. For default policy, only permit IP and Deny IP are available.</p>

The Egress Policy cell displays the source SGT, the destination SGT, and the Final Catch All Rule as a single list under SGACLs, separated by commas. The Final Catch All Rule is not displayed if it is set to None. An empty cell in a matrix represents an unmapped cell.

In the Egress Policy matrix view, you can scroll across the matrix to view the required set of cells. The browser does not load the entire matrix data at once. The browser requests the server for the data that falls in the area you are scrolling in. This prevents memory overflow and performance issues.

See the [“Matrix Operations” section on page 22-22](#) for more information on different actions that you can perform on a matrix cell.

Matrix Operations

The Matrix view in Cisco ISE looks similar to a spreadsheet. It has source SGT as a row title and destination SGT as a column title. A cell is a crossing of source and destination SGTs. The cell in the matrix view contains the configuration information of source and destination pair to SGACLs. The Matrix view does not display all the fields in order to save the cell area.

Navigating through the Matrix

You can navigate through the matrix either by dragging the matrix content area with the cursor or by using horizontal and vertical scroll bars. You can click and hold on a cell to drag it along with the entire matrix content in any direction. The source and destination bar moves along with the cells. The matrix view highlights the cell and the corresponding row (Source SGT) and column (Destination SGT) when a cell is selected. The coordinates (Source SGT and Destination SGT) of the selected cell are displayed below the matrix content area.

Selecting a Cell in the Matrix

To select a cell in the matrix view, click on it. The selected cell is displayed in different color, and the source and destination SGTs are highlighted. You can deselect a cell either by clicking it again or by selecting another cell. Multiple cell selection is not allowed in the matrix view. Double-click the cell to edit the cell configuration. See [Adding and Editing the Mapping of Egress Policy Cells, page 22-25](#), for more information on editing a matrix cell.

Sorting and Filtering Egress Policy Table

Cisco ISE allows you to sort and filter the egress policy tables. By default, no filter is applied to the Egress Policy table. The Egress Policy table is automatically set to default filtering and sorting in the following cases:

- Switching between views
- Refreshing the egress policy page
- After successful submission of an edited cell (default policy excluded)
- After successful submission of a added cell (default policy excluded)
- After deleting a mappings of a cell (default policy excluded)
- Exiting the SGT/SGACL direct create popup

You can sort the Egress policy in either ascending or descending alphabetical order. It is not case sensitive.

Quick Filter

The Quick Filter in Egress Policy works only with Source and Destination Tree views. It is not case sensitive.

Applying Quick Filter to Egress Policy Cells

To perform a quick filter in Source Tree or Destination Tree, complete the following steps:

Step 1 Choose **Policy > Security Group Access > Egress Policy**

The Egress Policy page appears.

- Step 2** Select the desired **tree** view.
The selected Tree view of the Egress Policies is displayed.
- Step 3** From the **Show** drop-down list, choose **Quick Filter**.
This adds a filter bar at the top of the external table.
- Step 4** Select the appropriate Security group from the drop-down lists.
The Tree view gets filtered according to the selected Group.
- Step 5** Expand a Security group to see its internal table.
It opens the internal table with the quick filter options. The filter bar contains the Status, Security Group ACLs, and Description fields. You can filter based on any of the fields.
- Step 6** Choose the Status from the drop-down list or enter a value in the Security Group ACLs and Description fields.
The application generates a filter based on the input as soon as you enter a value. You can use single or compound filtering conditions.
For example:
- Single condition—If you enter a value *A* in the field Source Security Group, the application generates a filter of Source Security Group that contains *A*.
 - Compound condition—If you enter a value *A* in the field Source Security Group and *B* in the Destination Security Group, the application generates a filter with the AND condition. That is, the resulting filter lists the Source SGT that contains *A* and the Destination that contains *B*.

Advanced Filter


The Advanced filter in the Egress Policy is available in all the three views. Using the Advanced Filter option, you can set a filter based on the source and destination security groups, SGACL, and descriptions.

To perform an advanced filter in the Egress table, complete the following steps.

- Step 1** Choose **Policy > Security Group Access > Egress Policy >**
- Step 2** From the Egress Policy page, choose **>>** and then **Filter**, and click **Quick Filter** to set a simple filter condition or click **Advanced Filter** to set a compound filter condition.



Note The Egress Policy table displays only the source and destination SGTs that have SGACLs assigned.

- Step 3** From the **Filter** drop-down list box, select the field on that you want to set the filter condition. For example, Source Security Group (Dec/Hex).
- Step 4** From the **Next** drop-down list, select the operator. For example, Contains.
- Step 5** In the **Next** text box, enter the name of the source security group. For example, SGT1.
- Step 6** You can click the + button to add additional conditions.
- Step 7** After you add all the conditions, click **Go** to view the results of your search.
- Step 8** Click the **Save** button () to save this custom Egress table to be viewed later.

**Note**

The filter is specific to the view it was created in. For example, a filter saved in the Source Tree would be visible only in the Source Tree view and not in the Destination Tree or the Egress Matrix views.

The advanced filter provides a Match field that usually determines if the logical operator between all conditions defined by the filter is an AND or an OR (named All and Any respectively). The conditions are organized by field. So all the conditions related to the same field are grouped together with the logical operator defined by the Match field. Between these grouped conditions there is an implicit AND.

For example:

Set the advanced filter with the following conditions:

- Match Any (OR)
- Source SGT starts with A+
- Destination SGT starts with B+
- Source SGT starts with C+
- Destination SGT starts with D+

Result:

Mapped Cells where [(Source SGT starts with A) OR (Source SGT starts with C)] AND [(Destination SGT starts with B) OR (Destination SGT starts with D)]

The fields that can be filtered are dependent on the view you use.

[Table 22-8](#) lists all the fields that can be filtered.

Table 22-8 Filterable Fields

	Source SGT	Destination SGT	Status	SGACLs list	Description
Source Tree	Yes	Yes	Yes	Yes	Yes
Destination Tree	Yes	Yes	Yes	Yes	Yes
Matrix	Yes	Yes	No	No	No

The advanced filter operator is explicit and selectable. [Table 22-9](#) lists the list of operators available for each field to enhance your filter.

Table 22-9 Operators to Enhance Advanced Filtering

	Contains	Does not contain	Does not Equal	Ends with	IS Empty	IS exactly (or equal)	IS not empty	Starts with
Source Security Group	Yes	Yes	Yes	Yes	No	Yes	No	Yes
Destination Security Group	Yes	Yes	Yes	Yes	No	Yes	No	Yes
Status	No	No	Yes	No	No	Yes	No	No

Table 22-9 Operators to Enhance Advanced Filtering

	Contains	Does not contain	Does not Equal	Ends with	IS Empty	IS exactly (or equal)	IS not empty	Starts with
Description	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Security Group ACLs	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Presetting Filters

Preset Filter is an advanced filter option available in the show drop-down list. This option contains all the saved advanced filter data. The advanced filter prompts for a name when you click **Save**. Choose **Show** menu and select the required filter from the saved filter to open the filter results. Use the **Manage Preset Filters** option to rename or delete the preset filters.

Configuring Egress Policy Table Cells

Cisco ISE allows you to configure cells using various options that are available in the tool bar. ISE does not allow a cell configuration if the selected source and destination SGTs are identical to a mapped cell.

This section contains:

- [Adding and Editing the Mapping of Egress Policy Cells, page 22-25](#)
- [Editing the Default Policy, page 22-26](#)
- [Deleting a Mapping of a Cell, page 22-27](#)

Adding and Editing the Mapping of Egress Policy Cells

To add or edit a mapping, complete the following steps:

-
- Step 1** Choose **Policy > Security Group Access > Egress Policy**
- The Egress Policy page is displayed.
- Step 2** Click the appropriate view tab to see the matrix cells.
- Step 3** To select the matrix cells, do the following:
- In the matrix view, click a cell to select it.
 - In the Source and Destination tree view, check the check box of a row in the internal table to select it.

Step 4 Click one of the following:

- **Add** to add a new mapping cell
- **Edit** to edit an existing mapping cell

If you click **Add**, the create Security Group ACL mapping dialog box appears displaying the source and the destination SGTs of the selected cell.

If you click **Edit**, a single cell edit pop up is displayed with the fields Source and Destination Security Groups, Status, Description, Security Group ACLs, and Final Catch All Rule.

The Edit button becomes enabled as soon as you select a cell. You can also double-click a matrix cell to edit.

Step 5 Select appropriate values for:

- Source Security Group
- Destination Security Group
- Status, Security Group ACLs
- Final Catch All Rule

See [Table 22-7](#) for the description of these fields.

Step 6 Click **Submit** to save the configuration.

You have successfully added a mapping to a cell or edited a mapped cell.

Step 7 Click **Cancel** to delete the configuration changes.

Editing the Default Policy

The default policy is given as a link at the bottom of the content area.

To edit the default policy, complete the following steps:

Step 1 Choose **Policy > Security Group Access > Egress Policy**.

The Egress Policy page is displayed.

Step 2 Click **Default Policy**.

The default policy edit popup is displayed with the following fields.

- Source and Destination Security Group—Contains a fixed value <ANY,ANY>
- Status—(Required) The default value is Enabled. Only Enabled and Disabled are available for the default policy status.
- Description—(Optional) Enter the description of the selected configuration.
- Security Group ACLs —(Optional)
- Final Catch All Rule—(Required) The default value as Permit IP. Only Permit IP and Deny IP are available for the default policy Final Catch All Rule.

Step 3 Click **Submit** to save the new configuration.

The system displays an appropriate validation error if any of the entry is invalid.

- Step 4** Click **Cancel** to delete the configuration changes.
-

Deleting a Mapping of a Cell

The Clear Mapping feature deletes the configuration of the selected cells. It is enabled only if you select a cell.

To delete a mapping of a cell, complete the following steps:

- Step 1** Choose **Policy > Security Group Access > Egress Policy**.
The Egress Policy page is displayed.
- Step 2** Do the following to access different views of the egress policy table:
- Click **Matrix** to access the matrix view.
 - Click **Source Tree** to access the source tree view.
 - Click **Destination Tree** to access the destination tree view.
- Step 3** Select the cells whose mapping you want to delete:
- In Matrix view, click a matrix cell to select it.
 - In source and destination view, check the check box of the rows in the internal table whose mapping you want to delete.
- Step 4** Click **Clear Mapping**.
The following warning messages are displayed in different views:
- Matrix view:
Are you sure you want to clear the mappings of the selected cell? OK to continue, Cancel to abort.
 - Source and Destination Tree view:
Are you sure you want to clear the mappings of X cells? OK to continue, Cancel to abort.
- Step 5** Click **OK**.
The configurations of the selected cells are deleted.
-

Configuring SGT and SGACL from Egress Policy

Security groups and Security group ACLs can be created directly from the Egress Policy page.

To create Security Group directly from the Egress Policy page, complete the following steps:

- Step 1** Choose **Policy > Security Group Access > Egress Policy**.
The Egress Policy page is displayed.
- Step 2** Choose **Create Security Group** from the Configure option drop-down list.

- Step 3** Follow the procedure as explained in [Configuring Security Groups, page 22-10](#) to create a Security Group.

To create Security Group ACLs directly from the Egress Policy page, complete the following steps:

- Step 1** Choose **Policy > Security Group Access > Egress Policy**.
The Egress Policy page is displayed.
- Step 2** Choose **Create Security Group ACLs** from the Configure option drop-down list.
- Step 3** Follow the procedure as explained in [Configuring Security Group Access Control Lists, page 22-12](#) to create a Security Group ACLs.
-

Push Button

The Push option in the egress policy initiates a CoA notification that calls the SGA devices to immediately request for updates from Cisco ISE regarding the configuration changes in the egress policy. For more information on Egress Policy CoA, see [Update SGT Matrix CoA, page 22-38](#)

Monitor Mode

The Monitor All option in the egress policy allows you to change the entire egress policy configuration status to monitor mode with a single click. Check the **Monitor All** check box in the egress policy page to change the egress policy configuration status of all the cells to monitor mode. When you check the Monitor All check box, the following changes take place in the configuration status:

- The cells whose status is Enabled will act as monitored but appears as if they are enabled.
- The cells whose status is Disable will not be affected.
- The cells whose status is Monitor will remain Monitored.

Uncheck the Monitor All check box to restore the original configuration status. It does not change the actual status of the cell in the database. When you deselect Monitor All, each cell in the egress policy regains its original configuration status.

Monitoring the Monitor Mode

The monitoring functionality of the monitor mode helps you to:

- Know how much traffic is filtered but monitored by the monitor mode
- Know that SGT-DGT pair is in monitor mode or enforce mode, and observe if there is any unusual packet drop is happening in the network
- Understand that SGACL drop is actually enforced by enforce mode or permitted by monitor mode
- Create custom reports based on the type of mode (monitor, enforce, or both)
- Identify which SGACL has been applied on NAD and display discrepancy, if any

You can view the monitor mode data from the following reports:

- [Top N RBACL Drops by Destination](#)
- [Top N RBACL Drops by User](#)
- [RBACL Drop Summary](#)

This section describes the process of running each of these reports. For more information on Cisco ISE reports, see [Chapter 24, “Reporting.”](#)

Top N RBACL Drops by Destination

To run the Top N RBACL Drops by Destination report, complete the following steps:

-
- Step 1** From the ISE Admin dashboard, select **Operations > Reports > Catalog**.
 - Step 2** In the Reports list, select **Security Group Access**.
 - Step 3** In the Reports panel on the right, click the **Top N RBACL Drops by Destination** radio button.
 - Step 4** From the Run drop-down menu, choose a time period over which the report data will be collected:
 - Last hour
 - Last 12 hours
 - Today
 - Yesterday
 - Last 7 days
 - Last 30 days

You can use the Run button to run the report for a specific period, or use the Query and Run option. The Query and Run option allows you to query the output by using various parameters.

- Step 5** If you choose Query and Run from the Run drop-down list, you can specify the mode from the Enforcement mode drop-down list as, Enforce, Monitor or Both.
-

Top N RBACL Drops by User

To run the Top N RBACL Drops by User report, complete the following steps:

-
- Step 1** From the ISE Admin dashboard, select **Operations > Reports > Catalog**.
 - Step 2** In the Reports list, select **Security Group Access**.
 - Step 3** In the Reports panel on the right, click the **Top N RBACL Drops by User** radio button.
 - Step 4** From the Run drop-down menu, choose a time period over which the report data will be collected:
 - Last hour
 - Last 12 hours
 - Today
 - Yesterday
 - Last 7 days
 - Last 30 days

You can use the Run button to run the report for a specific period, or use the Query and Run option. The Query and Run option allows you to query the output by using various parameters.

- Step 5** If you choose Query and Run from the Run drop-down list, you can specify the mode from the Enforcement mode drop-down list as Enforce, Monitor, or Both.
-

RBACL Drop Summary

To run the RBACL Drop Summary report, complete the following steps:

-
- Step 1** From the ISE Admin dashboard, select **Operations > Reports > Catalog**.
- Step 2** In the Reports list, select **Security Group Access**.
- Step 3** In the Reports panel on the right, click the **RBACL Drop Summary** radio button.
- Step 4** From the Run drop-down menu, choose a time period over which the report data will be collected:
- Last hour
 - Last 12 hours
 - Today
 - Yesterday
 - Last 7 days
 - Last 30 days

The report runs upon choosing the time period. You can see the type of mode under the Enforcement mode column. The default value for this is Both.

- Step 5** If you choose Query and Run from the Run drop-down list, you can specify the mode from the Enforcement mode drop-down list as Enforce, Monitor, or Both.
-

The Unknown Security Group

The Unknown security group is a pre-configured security group that cannot be modified and represents the 0x000 SGT.

The Cisco Security Group network devices request for cells that refer to the unknown SGT when they do not have a SGT of either source or destination. If only the source is unknown, the request applies to the <unknown, Destination SGT> cell. If only the destination is unknown, the request applies to the <source SGT, unknown> cell. If both the source and destination are unknown, the request applies to the <Unknown, Unknown> cell.

Default Policy

Default Policy refers to the <ANY,ANY> cell. Any source SGT is mapped to any destination SGT. Here, the ANY SGT cannot be modified and it is not listed in any source or destination SGTs. The ANY SGT can only be paired with ANY SGT. It cannot be paired with any other SGTs. A SGA network device attaches the default policy to the end of the specific cell policy.

- If a cell is empty, that means it contains the default policy alone.

- If a cell contains some policy, the resulting policy is a combination of the cell specific policy followed by the default policy.

According to ISE, the cell policy and the default policy are two separate sets of SGACLs that the devices get in response to two separate policy queries.

Configuration of the default policy is different from other cells:

- Status can take only two values, Enabled or Monitored.
- Security Group ACLs is an optional field for the default policy, so can be left empty.
- Final Catch All Rule can be either Permit IP or Deny IP. Clearly the None option is not available here because there is no safety net beyond the default policy.

OOB SGA PAC

All SGA network devices possess an SGA PAC as part of the EAP-FAST protocol. This is also utilized by the secure RADIUS protocol where the RADIUS shared secret is derived from parameters carried by the PAC. One of these parameters, Initiator-ID, holds the SGA network device identity, namely the Device ID.

If a device is identified using SGA PAC and there is no match between the Device ID, as configured for that device on Cisco ISE, and the Initiator-ID on the PAC, the authentication fails.

Some SGA devices (for example, Cisco firewall ASA) do not support the EAP-FAST protocol. Therefore, ISE can not provision these devices with SGA PAC over EAP-FAST. Instead, the SGA PAC is generated on ISE and manually copied to the device; hence this is called as the Out of Band (OOB) SGA PAC generation.

When you generate a PAC from Cisco ISE, a PAC file encrypted with the Encryption Key is generated.

This section describes the following:

- [SGA PAC Provisioning, page 22-31](#)
- [Monitoring SGA PAC, page 22-33](#)

SGA PAC Provisioning

This section describes the following:

- [Generating an SGA PAC from the Settings Screen, page 22-31](#)
- [Generating an SGA PAC from the Network Devices Screen, page 22-32](#)
- [Generating an SGA PAC from the Network Devices List Screen, page 22-33](#)

Generating an SGA PAC from the Settings Screen

To generate an SGA PAC from the Settings screen, complete the following steps:

-
- Step 1** Choose **Administration > System > Settings**.
- Step 2** From the Settings navigation pane on the left, click **Protocols**.
- Step 3** Choose **EAP-FAST > Generate PAC**.
- The Generate PAC page appears.

- Step 4** Follow the instructions in the “Generating the PAC for EAP-FAST” section on page 16-11 to generate SGA PAC.

Generating an SGA PAC from the Network Devices Screen

To generate an SGA PAC from the Network Devices screen, complete the following steps:

- Step 1** Choose **Administration > Network Resources > Network Devices**.
- Step 2** From the Network Devices navigation pane on the left, click **Network Devices**.
The Network Devices page appears with a list of configured devices.
- Step 3** Click **Add**, or check the check box next to a device and click **Edit** to edit it or click **Duplicate** to create a duplicate entry. You can alternatively click **Add new device** from the action icon on the Network Devices navigation pane or click a device name from the list to edit it.
- Step 4** If you are adding a new device, provide a device name.
- Step 5** Check the Security Group Access (SGA) check box to configure an SGA device.
- Step 6** Under the Out of Band (OOB) SGA PAC sub section, click **Generate PAC**.
- Step 7** The Generate PAC dialog box is displayed, as shown in Figure 22-2.

Figure 22-2 Generate PAC Dialog Box

- Step 8** Provide the following details:
- **PAC Time to Live**—(Required) Enter a value in days, weeks, months, or years. By default, the value is one year. The minimum value is one day and the maximum is ten years.
 - **Encryption Key**—(Required) Enter an encryption key. The length of the key must be between 8 and 256 characters. The key can contain uppercase or lowercase letters, or numbers, or a combination of alphanumeric characters.

The Encryption Key is used to encrypt the PAC in the file that is generated. This key is also used to decrypt the PAC file on the devices. Therefore, it is recommended that the administrator saves the Encryption Key for later use.

The Identity field specifies the Device ID of an SGA network device and is given an initiator ID by the EAP-FAST protocol. If the Identity string entered here does not match that Device ID, authentication will fail.

The expiration date is calculated based on the PAC Time to Live.

Step 9 Click **Generate PAC**.

Generating an SGA PAC from the Network Devices List Screen

To generate an SGA PAC from the Network Devices list screen, complete the following steps:

-
- Step 1** Choose **Administration > Network Resources > Network Devices**.
- Step 2** From the Network Devices navigation pane on the left, click **Network Devices**.
The Network Devices page appears with a list of configured devices.
- Step 3** Check the check box next to a device for which you want to generate the SGA PAC and click **Generate PAC**.
The Generate PAC dialog box is displayed, as shown in [Figure 22-2](#).
- Step 4** Provide the details as described in Step 8 of the [“Generating an SGA PAC from the Network Devices Screen” section on page 22-32](#).
- Step 5** Click **Generate PAC**.
-

Monitoring SGA PAC

You can view SGA PAC provisioning data in the form of a [PAC Provisioning Report](#).

This section describes the process of running this report. For more information on Cisco ISE reports, see [Chapter 24, “Reporting.”](#)

PAC Provisioning Report

To view PAC Provisioning data, complete the following steps:

-
- Step 1** From the ISE Admin dashboard, select **Operations > Reports > Catalog**.
- Step 2** In the Reports list, select **Security Group Access**.
- Step 3** In the Reports panel on the right, click the **PAC Provisioning** radio button.
- Step 4** From the Run drop-down menu, choose a time period over which the report data will be collected:
- Last hour
 - Last 12 hours
 - Today
 - Yesterday
 - Last 7 days
 - Last 30 days
 - Query and run

You can use the **Run** button to run the report for a specific period, or use the Query and Run option. The Query and Run option allows you to query the output by using various parameters.

SGA CoA

Cisco ISE supports SGA Change of Authorization (CoA) which allows ISE to notify SGA devices about Security Group changes, so that the devices can reply with requests to get the relevant data.

A CoA notification can trigger a SGA network device to send either an Environment CoA or a Per Policy CoA.

This section contains:

- [CoA Supported Network Devices, page 22-34](#)
- [Environment CoA, page 22-35](#)
- [Per Policy CoA, page 22-37](#)
- [SGA CoA Summary, page 22-40](#)
- [Monitoring SGA CoA, page 22-40](#)

CoA Supported Network Devices

ISE sends CoA notifications to the following network devices:

- Network device with single IP address (subnets are not supported)
- Network device configured as SGA device
- Network device set as CoA supported

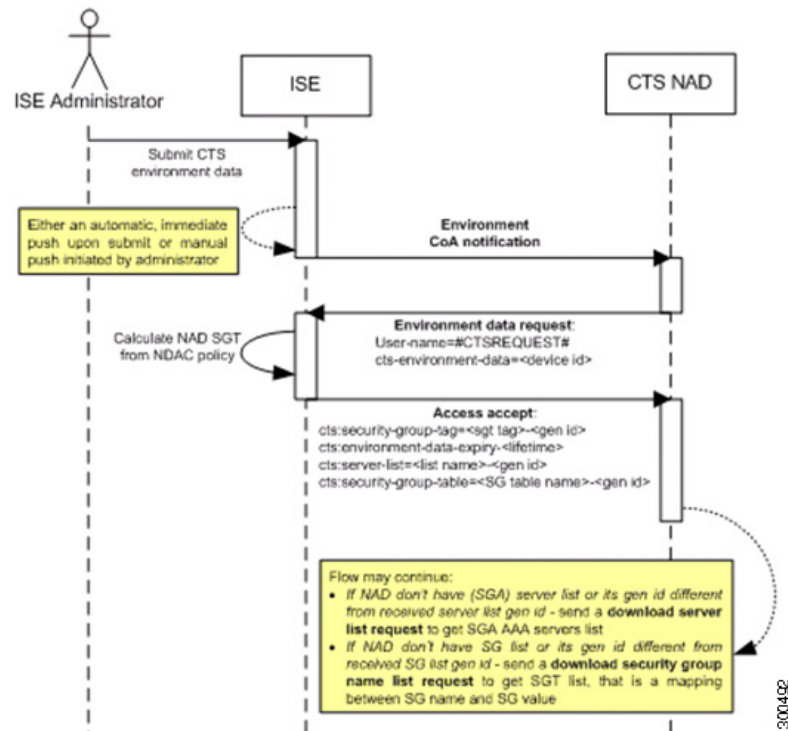
When Cisco ISE is deployed in a distributed environment where there are several secondaries that interoperate with different sets of devices, CoA requests are sent from Cisco ISE primary node to all the network devices. Therefore, SGA network devices need to be configured with the ISE primary node as the CoA client.

The devices return CoA NAK or ACK back to the Cisco ISE primary node. However, the SGA session that follows an SGA CoA is handled by the related Cisco ISE secondary node.

Environment CoA

Figure 22-3 depicts the Environment CoA notification flow.

Figure 22-3 Environment CoA Notification Flow



1. Cisco ISE sends an environment CoA notification to the SGA network device.
2. The device returns an environment request.
3. In response to the environment data request, Cisco ISE returns:
 - a. The environment data of the device that sent the request—This includes the SGA device's SGT (as inferred from the NDAC policy) and download environment TTL.
 - b. The name and generation ID of the SGA AAA server list.
 - c. The names and generation IDs of (potentially multiple) SGT tables—These tables list SGT name versus SGT value, and together these tables hold the full list of SGTs.
4. If the device does not hold an SGA AAA server list, or the generation ID is different from the generation ID that is received, the device sends another request to get the AAA server list content.
5. If the device does not hold an SGT table listed in the response, or the generation ID is different from the generation ID that is received, the device sends another request to get the content of that SGT table.

Initiating Environment CoA

An Environment CoA can be triggered for:

- [Network Devices, page 22-36](#)
- [Security Groups, page 22-36](#)
- [SGA AAA Servers, page 22-36](#)
- [NDAC Policy, page 22-37](#)

Network Devices

To trigger an Environment CoA for the Network devices, complete the following steps:

Step 1 Choose **Administration > Network Resources > Network Devices**.

Step 2 Add or edit a network device.

Step 3 Update Security Group parameters under the SGA Attributes section.

Changing the environment TTL is notified only to the specific SGA network device where the change took place.

Since only a single device is impacted, an environmental CoA notification is sent immediately upon submission. The result is a device update of its environment TTL.

Security Groups

To trigger an Environment CoA for the security groups, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results navigation pane on the left, click the > button next to Security Group Access and click **Security Groups**.

Step 3 In the security group page, change the name of an SGT, which will change the name of the mapping value of that SGT. This triggers an environmental change.

Step 4 Click the **Push** button to initiate an environment CoA notification after changing the names of multiple SGTs. This environment CoA notification goes to all SGA network devices and provides an update of all SGTs that were changed.

SGA AAA Servers

To trigger an Environment CoA for the SGA AAA servers, complete the following steps:

Step 1 Choose **Administration > Network Resources > SGA AAA Servers**.

Step 2 In the SGA AAA Servers page create, delete or update the configuration of an SGA AAA server. This triggers an environment change.

Step 3 Click the **Push** button to initiate an environment CoA notification after you configure multiple SGA AAA servers. This environment CoA notification goes to all SGA network devices and provides an update of all SGA AAA servers that were changed.

NDAC Policy

To trigger an Environment CoA for the NDAC Policies, complete the following steps:

In the NDAC policy page you can create, delete, or update rules of the NDAC policy. These environment changes are notified to all network devices.

You can initiate an environment CoA notification by clicking the Push button in the NDAC policy page. This environment CoA notification goes to all SGA network devices and provides an update of network device own SGT, as described in the [“Environment CoA”](#) section on page 22-35.

Per Policy CoA

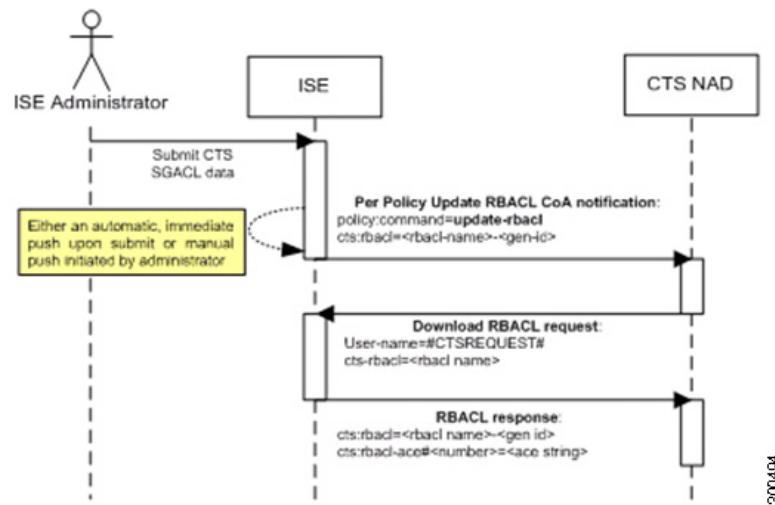
There are three types of Per Policy CoA notification:

- [Update RBACL Named List CoA](#)—Triggers a request to download SGACL (RBACL).
- [Update SGT Matrix CoA](#)—Triggers a request to download all egress policy cells related to a certain destination SGT (to an egress policy column).
- [Policies Update CoA](#)—This is an optimization that allows initiating multiple calls for both RBACL content and egress policy cells with a single CoA notification.

Update RBACL Named List CoA

Figure 22-4 depicts the Update RBACL Named List CoA flow.

Figure 22-4 Update RBACL Named List CoA Notification Flow



1. ISE sends an update RBACL named list CoA notification to a SGA network device. The notification contains the SGACL name and the generation ID.
2. The device may replay with an SGACL (RBACL) data request if both of the following terms are fulfilled:
 - a. If the SGACL is part of an egress cell that the device holds. The device holds a subset of the egress policy data, which are the cells related to the SGTs of its neighboring devices and endpoints (egress policy columns of selected destination SGTs).

- b. The generation ID in the CoA notification is different from the generation ID that the device holds for this SGACL.
3. In response to the SGACL data request, ISE returns the content of the SGACL (the ACE).

Initiating an Update RBACL Named List CoA

To trigger an Update RBACL Named List CoA, complete the following steps:

-
- Step 1** Choose **Policy > Policy Elements > Results**.
 - Step 2** From the Results navigation pane on the left, click the > button next to Security Group Access and click **Security Group ACLs**.
 - Step 3** Add or edit a SGACL as described in [Configuring Security Group Access Control Lists, page 22-12](#).
After you submit a SGACL, it promotes the generation ID of the SGACL.
 - Step 4** Click the **Push** button to initiate an Update RBACL Named List CoA notification after you change the content of multiple SGACLs. This notification goes to all SGA network devices, and provides an update of that SGACL content on the relevant devices.
-

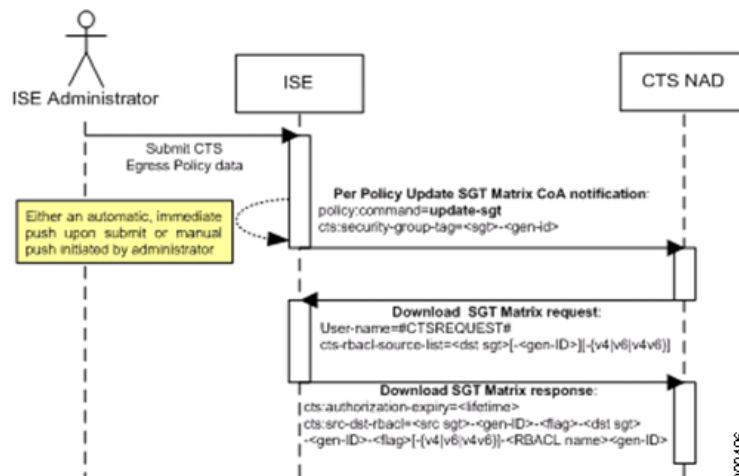
Changing the name or the IP version of an SGACL does not change its generation ID; hence it does not require sending an update RBACL named list CoA notification.

However, changing the name or IP version of an SGACL that is in use in the egress policy indicates a change in the cell that contains that SGACL, and this changes the generation ID of the destination SGT of that cell. See [Initiating Update SGT matrix CoA from Egress Policy, page 22-39](#) that deals with changes in the egress policy.

Update SGT Matrix CoA

Figure 22-5 depicts the Update SGT Matrix CoA flow.

Figure 22-5 Update SGT Matrix CoA flow



300406

1. Cisco ISE sends an updated SGT matrix CoA notification to a SGA network device. The notification contains the SGT value and the generation ID.
2. The device may replay with an SGT data request if both the following terms are fulfilled:
 - a. If the SGT is the SGT of a neighboring device or endpoint, the device downloads and hold the cells related to SGTs of neighboring devices and endpoints (a destination SGT).
 - b. The generation ID in the CoA notification is different from the generation ID that the device holds for this SGT.
3. In response to the SGT data request, ISE returns the data of all egress cells, such as the source and destination SGTs, the status of the cell, and an ordered list of the SGACL names configured in that cell.

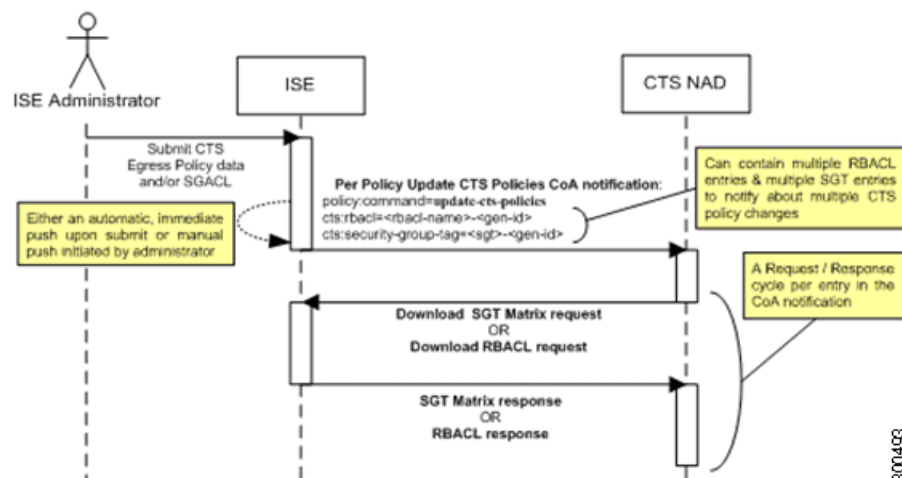
Initiating Update SGT matrix CoA from Egress Policy

-
- Step 1** Choose **Policy > Security Group Access > Egress Policy**.
- Step 2** On the Egress Policy page, change the content of a cell (status, SGACLs).
- Step 3** After you submit the changes, it promotes the generation ID of the destination SGT of that cell.
- Step 4** Click the **Push** button to initiate the Update SGT matrix CoA notification after you change the content of multiple egress cells. This notification goes to all SGA network devices, and provides an update of cells content on the relevant devices.
-

Policies Update CoA

Figure 22-6 depicts the Policies Update CoA flow.

Figure 22-6 Policies Update CoA flow



1. ISE sends an update policies CoA notification to a SGA network device. The notification may contain multiple SGACL names and their generation IDs, and multiple SGT values and their generation IDs.

2. The device may replay with multiple SGACL data requests and/or multiple SGT data.
3. In response to each SGACL data request or SGT data request, ISE returns the relevant data.

SGA CoA Summary

Table 22-10 summarizes the various scenarios that may require initiating an SGA CoA, the type of CoA used in each scenario, and the related UI pages.

Table 22-10 SGA CoA Summary

UI Page	Operation that triggers CoA	How it is triggered	CoA type	Send to
Network Device	Changing the environment TTL in the SGA section of the page	Upon successful Submit of SGA network device	Environment	The specific network device
SGA AAA Server	Any change in the SGA AAA server (create, update, delete, reorder)	Accumulative changes can be pushed by clicking the Push button on the SGA AAA servers list page.	Environment	All SGA network devices
Security Group	Any change in the SGT (create, rename, delete)	Accumulative changes can be pushed by clicking the Push button on the SGT list page.	Environment	All SGA network devices
NDAC Policy	Any change in the NDAC policy (create, update, delete)	Accumulative changes can be pushed by clicking the Push button on the NDAC policy page.	Environment	All SGA network devices
SGACL	Changing SGACL ACE	Accumulative changes can be pushed by clicking the Push button on the SGACL list page.	Update RBACL named list	All SGA network devices
	Changing SGACL name or IP version	Accumulative changes can be pushed by clicking the Push button on the SGACL list page or the policy push button in the Egress table.	Update SGT matrix	All SGA network devices
Egress Policy	Any operation that changes the generation ID of an SGT	Accumulative changes can be pushed by clicking the Push button on the egress policy page.	Update SGT matrix	All SGA network devices

Monitoring SGA CoA

SGA CoA notifications can be viewed as alarms, logs, and reports.

This section describes how to view the following:

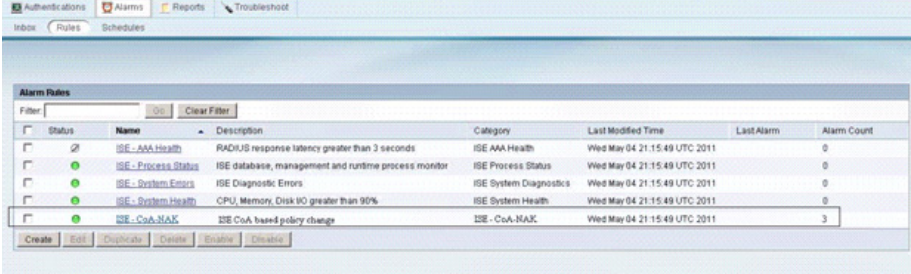
- [SGA CoA Alarms, page 22-41](#)
- [SGA CoA Report, page 22-41](#)

SGA CoA Alarms

When CoA returns CoA-NAK, an alarm is generated, as shown in [Figure 22-7](#).

To view SGA CoA alarms, go to **Operations > Alarms > Rules**.

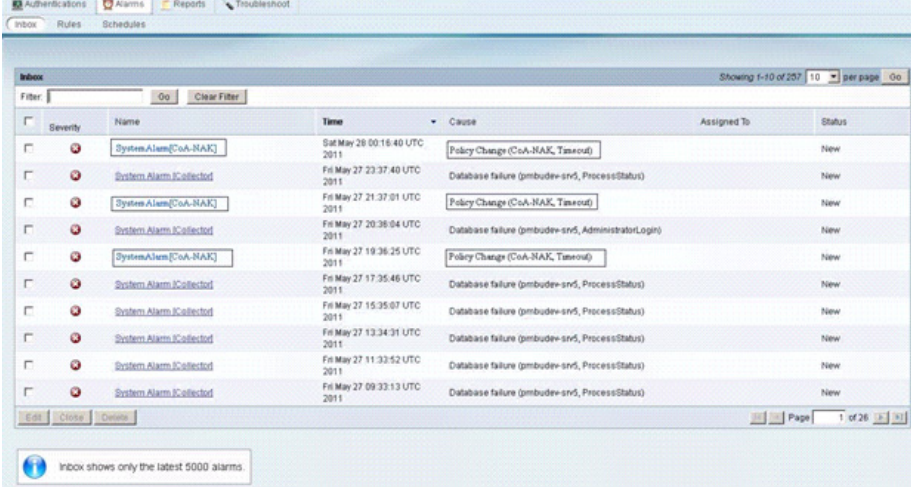
Figure 22-7 SGA CoA Alarms



Status	Name	Description	Category	Last Modified Time	Last Alarm	Alarm Count
<input checked="" type="checkbox"/>	ISE - AAA Health	RADIUS response latency greater than 3 seconds	ISE AAA Health	Wed May 04 21:15:49 UTC 2011	0	0
<input checked="" type="checkbox"/>	ISE - Process Status	ISE database, management and runtime process monitor	ISE Process Status	Wed May 04 21:15:49 UTC 2011	0	0
<input checked="" type="checkbox"/>	ISE - System Errors	ISE Diagnostic Errors	ISE System Diagnostics	Wed May 04 21:15:49 UTC 2011	0	0
<input checked="" type="checkbox"/>	ISE - System Health	CPU, Memory, Disk IO greater than 90%	ISE System Health	Wed May 04 21:15:49 UTC 2011	0	0
<input checked="" type="checkbox"/>	ISE - CoA-NAK	ISE CoA based policy change	ISE - CoA-NAK	Wed May 04 21:15:49 UTC 2011	3	3

You can also view the SGA CoA alarms under Live Logs. To view live logs, go to **Operations > Alarms > Inbox** as shown in [Figure 22-8](#).

Figure 22-8 SGA CoA Alarms Under Live Logs



Severity	Name	Time	Cause	Assigned To	Status
<input checked="" type="checkbox"/>	System Alarm [CoA-NAK]	Sat May 28 00:16:40 UTC 2011	Policy Change (CoA-NAK, Timeout)		New
<input checked="" type="checkbox"/>	System Alarm [Collectd]	Fri May 27 23:37:40 UTC 2011	Database failure (gmbuddev-snd, ProcessStatus)		New
<input checked="" type="checkbox"/>	System Alarm [CoA-NAK]	Fri May 27 21:37:01 UTC 2011	Policy Change (CoA-NAK, Timeout)		New
<input checked="" type="checkbox"/>	System Alarm [Collectd]	Fri May 27 20:36:04 UTC 2011	Database failure (gmbuddev-snd, AdministratorLogin)		New
<input checked="" type="checkbox"/>	System Alarm [CoA-NAK]	Fri May 27 19:36:25 UTC 2011	Policy Change (CoA-NAK, Timeout)		New
<input checked="" type="checkbox"/>	System Alarm [Collectd]	Fri May 27 17:35:46 UTC 2011	Database failure (gmbuddev-snd, ProcessStatus)		New
<input checked="" type="checkbox"/>	System Alarm [Collectd]	Fri May 27 15:35:07 UTC 2011	Database failure (gmbuddev-snd, ProcessStatus)		New
<input checked="" type="checkbox"/>	System Alarm [Collectd]	Fri May 27 13:34:31 UTC 2011	Database failure (gmbuddev-snd, ProcessStatus)		New
<input checked="" type="checkbox"/>	System Alarm [Collectd]	Fri May 27 11:32:52 UTC 2011	Database failure (gmbuddev-snd, ProcessStatus)		New
<input checked="" type="checkbox"/>	System Alarm [Collectd]	Fri May 27 09:33:13 UTC 2011	Database failure (gmbuddev-snd, ProcessStatus)		New

SGA CoA Report

To view SGA CoA notification data, complete the following steps:

- Step 1** From the ISE Admin dashboard, select **Operations > Reports > Catalog**.
- Step 2** In the Reports list, select **Security Group Access**.
- Step 3** In the Reports panel on the right, click the **Policy CoA** radio button.
- Step 4** From the Run drop-down menu, choose a time period over which the report data will be collected:
 - Last hour
 - Last 12 hours

- Today
- Yesterday
- Last 7 days
- Last 30 days
- Query and run

You can use the **Run** button to run the report for a specific period, or use the Query and Run option. The Query and Run option allows you to query the output by using various parameters. See [Figure 22-9](#).

Figure 22-9 SGA CoA Report

Security Group Access > Policy CoA

Showing Page 1 of 1 | First | Prev | Next | Last | Goto Page: | Go

Security Group Access > Policy CoA

Time Range: July 28, 2011 06:05:03 AM - July 28, 2011 06:35:03 AM
Generated on: July 28, 2011 6:35:03 AM UTC

[Reload](#)

Logged At	Device IP	Message	Type	Other Attribute 1	Other Attribute 2	Other Attribute 3
July 28, 2011 6:34:33.878 AM	10.0.2.1	Failed to complete CoA request for update-bac(<Other_Attribute1>)	CTS-3-POLICY_COA_RBACL_FAILED	RBACL002-1234		
July 28, 2011 6:34:32.878 AM	10.0.2.1	Command update-sgt=<Other_Attribute1>	CTS-6-POLICY_COA_SGT_REQUEST	4-1111		
July 28, 2011 6:34:31.879 AM	10.0.2.1	Command update-sgt=<Other_Attribute1> has no session associated	CTS-6-POLICY_COA_NO_SESSION	4368-1111		
July 28, 2011 6:34:30.879 AM	10.0.2.1	Failed to complete CoA request for update-sgt(<Other_Attribute1>)	CTS-3-POLICY_COA_SGT_FAILED	4-1111		
July 28, 2011 6:34:29.879 AM	10.0.2.1	Command update-sgt=<Other_Attribute1> has no change	CTS-6-POLICY_COA_NO_ACTION	4-1111		
July 28, 2011 6:34:28.879 AM	10.0.2.1	Command update-bac=<Other_Attribute1>	CTS-6-POLICY_COA_RBACL_DENIED	RBACL002-1234aa		

Notifications (0) | Alarms (0)

300495