Cisco TrustSec Policies Configuration

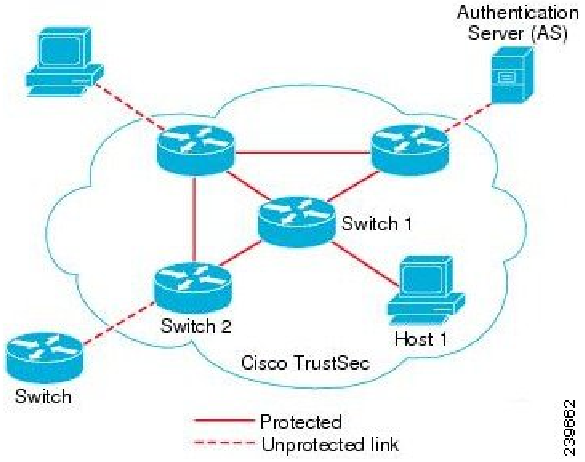
- TrustSec Architecture, page 1
- Configure TrustSec Global Settings, page 4
- Configure TrustSec Devices, page 5
- Configure TrustSec AAA Servers, page 7
- Security Groups Configuration, page 8
- Egress Policy, page 11
- SGT Assignment, page 16
- TrustSec Configuration and Policy Push, page 20
- Run Top N RBACL Drops by User Report, page 30

TrustSec Architecture

The Cisco TrustSec solution establishes clouds of trusted network devices to build secure networks. Each device in the Cisco TrustSec cloud is authenticated by its neighbors (peers). Communication between the devices in the TrustSec cloud is secured with a combination of encryption, message integrity checks, and data-path replay protection mechanisms. The TrustSec 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 TrustSec 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 Cisco ISE to enforce access control policies by enabling the endpoint device to act upon the SGT to filter traffic.

The following figure shows an example of a TrustSec network cloud.

Figure 1: TrustSec Architecture



TrustSec Components

The key TrustSec components include:

- Network Device Admission Control (NDAC)—In a trusted network, during authentication, each network device (for example Ethernet switch) in a TrustSec 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 TrustSec 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 TrustSec domain, Cisco ISE assigns these new entities to the appropriate security groups.
- Security Group Tag (SGT)—TrustSec service assigns to each security group a unique 16-bit security group number whose scope is global within a TrustSec 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 TrustSec service to propagate the IP-SGT bindings across network devices that do not have SGT-capable hardware support to hardware that supports SGT/SGACL.
- Environment Data Download—The TrustSec 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 TrustSec 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 TrustSec device should download or refresh its environment data
- SGT Reservation—An enhancement in Cisco ISE to reserve a range of SGTs to enable IP to SGT mapping.
- IP-to-SGT Mapping—An enhancement in Cisco ISE to bind an endpoint IP to an SGT and provision it to a TrustSec-capable device. Cisco ISE supports entering 1000 IP-to-SGT Mappings.
- 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.

TrustSec Terminology

The following table lists some of the common terms that are used in the TrustSec solution and their meaning in an TrustSec environment.

Table 1: TrustSec 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.

Term	Meaning
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.
TrustSec device	Any of the Cisco Catalyst 6000 Series or Cisco Nexus 7000 Series switches that support the TrustSec solution.
TrustSec-capable device	A TrustSec-capable device will have TrustSec-capable hardware and software. For example, the Nexus 7000 Series Switches with the Nexus operating system.
TrustSec seed device	The TrustSec device that authenticates directly against the Cisco ISE server. It acts as both the authenticator and supplicant.
Ingress	When packets first encounter a TrustSec-capable device that is part of a network where the Cisco TrustSec 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 TrustSec-capable device that is part of a network where the Cisco TrustSec solution is enabled, they are untagged. This point of exit from the trusted network is called the egress.

Supported Switches and Required Components for TrustSec

To set up a Cisco ISE network that is enabled with the Cisco TrustSec solution, you need switches that support the TrustSec solution and other components. Apart from the switches, you also need other components for identity-based user access control using the IEEE 802.1X protocol. For a complete up-to-date list of the Trustsec-supported Cisco switch platforms and the required components, see Cisco TrustSec-Enabled Infrastructure.

Configure TrustSec Global Settings

For Cisco ISE to function as an TrustSec server and provide TrustSec services, you must define some global TrustSec settings.

Before You Begin

- Before you configure global TrustSec settings, ensure that you have defined global EAP-FAST settings (choose **Administration** > **System** > **Settings** > **Protocols** > **EAP-FAST** > **EAP-FAST Settings**).

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

- To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Administration** > **System** > **Settings** > **TrustSec Settings**.

Step 2 Enter the values in the fields.

Step 3 Click **Save**.

What to Do Next

- Configure TrustSec Devices, on page 5

Configure TrustSec Devices

For Cisco ISE to process requests from TrustSec-enabled devices, you must define these TrustSec-enabled devices in Cisco ISE.

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

Step 2 Click **Add**.

Step 3 Enter the required information in the **Network Devices** section.

Step 4 Check the **Advanced Trustsec Settings** check box to configure a Trustsec-enabled device.

Step 5 Click **Submit**.

OOB TrustSec PAC

All TrustSec network devices possess a TrustSec 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 TrustSec network device identity, namely the Device ID.

If a device is identified using TrustSec 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 TrustSec devices (for example, Cisco firewall ASA) do not support the EAP-FAST protocol. Therefore, Cisco ISE cannot provision these devices with TrustSec PAC over EAP-FAST. Instead, the TrustSec PAC is generated on Cisco ISE and manually copied to the device; hence this is called as the Out of Band (OOB) TrustSec 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:

Generate a TrustSec PAC from the Settings Screen

You can generate a TrustSec PAC from the Settings screen.

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**.

Step 4 Generate TrustSec PAC.

Generate a TrustSec PAC from the Network Devices Screen

You can generate a TrustSec PAC from the Network Devices screen.

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

Step 2 Click **Add**. You can also click **Add new device** from the action icon on the Network Devices navigation pane.

Step 3 If you are adding a new device, provide a device name.

Step 4 Check the **Advanced TrustSec Settings** check box to configure a TrustSec device.

Step 5 Under the **Out of Band (OOB) TrustSec PAC** sub section, click **Generate PAC**.

Step 6 Provide the following details:

- PAC Time to Live—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—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 a TrustSec 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 defined under TrustSec section in the Network Device creation page, authentication will fail.

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

Step 7 Click **Generate PAC.**

Generate a TrustSec PAC from the Network Devices List Screen

You can generate a TrustSec PAC from the Network Devices list screen.

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

Step 2 Click **Network Devices**.

Step 3 Check the check box next to a device for which you want to generate the TrustSec PAC and click **Generate PAC.**

Step 4 Provide the details in the fields.

Step 5 Click **Generate PAC.**

Push Button

The Push option in the egress policy initiates a CoA notification that calls the Trustsec devices to immediately request for updates from Cisco ISE regarding the configuration changes in the egress policy.

Configure TrustSec AAA Servers

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

This page lists the Cisco ISE servers in your deployment that you have configured as your TrustSec AAA servers.

You can click the **Push** button to initiate an environment CoA notification after you configure multiple TrustSec AAA servers. This environment CoA notification goes to all TrustSec network devices and provides an update of all TrustSec AAA servers that were changed.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

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

Step 2 Click **Add**.

Step 3 Enter the values as described:

- Name—Name that you want to assign to the Cisco ISE server in this AAA Server list. This name can be different from the hostname of the Cisco ISE server.

- Description—An optional description.
- IP—IP address of the Cisco ISE server that you are adding to the AAA Server list.
- Port—Port over which communication between the TrustSec device and server should take place. The default is 1812.

Step 4 Click **Submit**.

What to Do Next

Configure Security Groups.

Security Groups Configuration

A Security Group (SG) or Security Group Tag (SGT) is an element that is used in TrustSec 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 generated in a sequential manner, but you have the option to reserve a range of SGTs for IP to SGT mapping. Cisco ISE skips the reserved numbers while generating SGTs.

TrustSec service uses these SGTs to enforce the TrustSec policy at egress.

You can configure security groups from the following pages in the Admin portal:

- **Policy** > **Policy Elements** > **Results** > **Trustsec** > **Security Groups**.
- Directly from egress policy page at **Configure** > **Create New Security Group**.

You can click the **Push** button to initiate an environment CoA notification after updating multiple SGTs. This environment CoA notification goes to all TrustSec network devices forcing them to start a policy/data refresh request.

Add Security Groups

Each security group in your TrustSec solution should be assigned a unique SGT. Even though Cisco ISE supports 65,535 SGTs, having fewer number of SGTs would enable you to deploy and manage the TrustSec solution easily. We recommend a maximum of 4,000 SGTs.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Policy** > **Policy Elements** > **Results** > **TrustSec** > **Security Groups**.

Step 2 Click **Add** to add a new security group.

Step 3 Enter a name and description (optional) for the new security group.

Step 4 Enter a Tag Value. Tag value can be set to be entered manually or autogenerate. You can also reserve a range for the SGT. You can configure it from the Trustsec global settings page under **Administration** > **System** > **Settings** > **TrustSec Settings**.

Step 5 Click **Save**.

What to Do Next

Configure Security Group Access Control Lists

Import Security Groups into Cisco ISE

You can import security groups in to a Cisco ISE node using a comma-separated value (CSV) file. You must first update the template before you can import security groups into Cisco ISE. You cannot run import of the same resource type at the same time. For example, you cannot concurrently import security groups from two different import files.

You can download the CSV template from the Admin portal, enter your security group details in the template, and save the template as a CSV file, which you can then import back into Cisco ISE.

While importing security groups, you can stop the import process when Cisco ISE encounters the first error.

Step 1 Choose **Policy** > **Policy Elements** > **Results** > **TrustSec** > **Security Groups**.

Step 2 Click **Import**.

Step 3 Click **Browse** to choose the CSV file from the system that is running the client browser.

Step 4 Check the **Stop Import on First Error** check box.

Step 5 Click **Import** .

Export Security Groups from Cisco ISE

You can export security groups configured in Cisco ISE in the form of a CSV file that you can use to import these security groups into another Cisco ISE node.

Step 1 Choose **Policy** > **Policy Elements** > **Results** > **TrustSec** > **Security Groups**.

Step 2 Click **Export**.

Step 3 To export security groups, you can do one of the following:

- Check the check boxes next to the group that you want to export, and choose **Export** > **Export Selected**.
- Choose **Export** > **Export All** to export all the security groups that are defined.

Step 4 Save the export.csv file to your local hard disk.

Add Security Group Access Control Lists

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Policy** > **Policy Elements** > **Results** > **TrustSec** > **Security Group ACLs**.

Step 2 Click **Add** to create a new Security Group ACL.

Step 3 Enter 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
- Security Group ACL Content—Access control list (ACL) commands. For example:

  permit icmp

  deny all

  The ACL command should match the syntax of your network device.

Step 4 Click **Submit**.

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 these preset filters. When the source SGT tries to reach the destination SGT, the TrustSec-capable device enforces the SGACLs based on the TrustSec policy as defined in the Egress Policy. Cisco ISE creates and provisions the policy.

After you create the SGTs and SGACLs, which are the basic building blocks required to create a TrustSec 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.

You can view the Egress Policy in the **Policy** > **TrustSec** > **Egress Policy** page.

You can view the Egress policy in three different ways:

- Source Tree View
- Destination Tree View
- Matrix View

Source Tree View

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 and the corresponding policy (SGACLs) 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 View

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 and the corresponding policy (SGACLs) 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.

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.

The Matrix view has the same GUI elements as the Source and Destination views. However, it has these additional elements:

Matrix Dimensions

The **Dimension** drop-down list in the Matrix view enables you to set the dimensions of the matrix.

Condensed View

The Condensed option in the egress policy matrix view allows you to display the matrix without empty cells. Check the **Condensed** check box to hide empty cells.

Import/Export Matrix

The **Import** and **Export** buttons enable you to import or export the matrix.

Matrix Operations

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.

Configure SGACL from Egress Policy

You can create Security Group ACLs directly from the Egress Policy page.

Step 1 Choose **Policy** > **TrustSec** > **Egress Policy**.

Step 2 From the Source or Destination Tree View page, choose **Configure > Create New Security Group ACL**.

Step 3 Enter the required details and click **Submit**.

Egress Policy Table Cells Configuration

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

Add the Mapping of Egress Policy Cells

You can add the mapping cell for Egress Policy from the Policy page.

Step 1 Choose **Policy** > **TrustSec** > **Egress Policy**.

Step 2 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 3 Click **Add** to add a new mapping cell.

Step 4 Select appropriate values for:

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

Step 5 Click **Save**.

Export Egress Policy

Step 1 Choose **Policy** > **TrustSec** > **Egress Policy > Matrix**.

Step 2 Click **Export**.

Step 3 Save the CSV file to your local system.

Import Egress Policy

You can create the egress policy offline and then import it in to Cisco ISE. If you have a large number of security group tags, then creating the security group ACL mapping one by one might take some time. Instead, creating the egress policy offline and importing it in to Cisco ISE saves time for you. During import, Cisco ISE appends the entries from the CSV file to the egress policy matrix and does not overwrite the data.

Egress policy import fails if the:

- Source or destination SGTs do not exist
- SGACL does not exist
- Monitor status is different than what is currently configured in Cisco ISE for that cell

Step 1 Choose **Policy** > **TrustSec** > **Egress Policy > Matrix**.

Step 2 Click **Generate a Template**.

Step 3 Download the template (CSV file) from the Egress Policy page and enter the following information in the CSV file:

- Source SGT
- Destination SGT
- SGACL
- Monitor status (enabled, disabled, or monitored)

Step 4 Check the **Stop Import on First Error** check box for Cisco ISE to abort the import if it encounters any errors.

Step 5 Click **Import**.

Configure SGT from Egress Policy

You can create Security Groups directly from the Egress Policy page.

Step 1 Choose **Policy** > **TrustSec** > **Egress Policy**.

Step 2 From the Source or Destination Tree View page, choose **Configure > Create New Security Group**.

Step 3 Enter the required details and click **Submit**.

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.

Features of 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

The Unknown Security Group

The Unknown security group is a pre-configured security group that cannot be modified and represents the Trustsec with tag value 0.

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 TrustSec 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 Cisco 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 any of the following: Permit IP, Deny IP, Permit IP log, or Deny IP log. Clearly the None option is not available here because there is no safety net beyond the default policy.

Push Button

The Push option in the egress policy initiates a CoA notification that calls the Trustsec devices to immediately request for updates from Cisco ISE regarding the configuration changes in the egress policy.

SGT Assignment

Cisco ISE allows you to assign an SGT to a TrustSec device if you know the device hostname or IP address. When a device with the specific hostname or IP address joins the network, Cisco ISE will assign the SGT before authenticating it.

Sometimes, devices need to be manually configured to map the security group tags to the endpoint. 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.

ISE allows you to create up to 10,000 IP-to-SGT mappings. You can create IP-to-SGT mapping groups to logically group such large scale mappings. Each group of IP-to-SGT mappings contains a list of IP addresses, a single security group it would map to and a network device or network device group which is the deployment target for those mappings.

NDAC Authorization

You can configure the TrustSec policy by assigning SGTs to devices. You can assign security groups to devices based on TrustSec device ID attribute.

Configure NDAC Authorization

Before You Begin

- Ensure that you create the security groups for use in the policy.
- To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Policy** > **TrustSec** > **Network Device Authorization**.

Step 2 Click the **Action** icon on the right-hand side of the Default Rule row, and click **Insert New Row Above**.

Step 3 Enter the name for this rule.

Step 4 Click the plus sign (+) next to **Conditions** to add a policy condition.

Step 5 You can click **Create New Condition (Advance Option)** and create a new condition.

Step 6 From the **Security Group** drop-down list, select the SGT that you want to assign if this condition evaluates to true.

Step 7 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 TrustSec 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 8 Click **Save** to save your TrustSec policy.
If a TrustSec 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.

Configure End User Authorization

Cisco 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.

Before You Begin

- Read the information on authorization policies.
- To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Policy** > **Authorization**.

Step 2 Create a new authorization policy.

Step 3 Select a security group, for Permissions.

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.

Add Single IP-to-SGT Mappings

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Policy** > **Policy Elements** > **Results** > **TrustSec** > **Security Group Mappings** > **Hosts**.

Step 2 Click **Add** to add a new single IP-SGT mapping.

Step 3 Choose if you want to enter the **Hostname** or the **IP Address** of the device. You can also enter the subnet mask for the IP address.

Step 4 Choose one of the following:

- **Group Mapping—**To set the IP mapping to be part of existing Mapping Group.
- **Security Group Tag—**To create a flat mapping between this IP and SGT.

Step 5 Choose the destination network device on which you want to deploy this mapping. You can deploy the mappings on all trustsec devices, on selected network device groups, or on selected network devices.

Step 6 Click **Submit**.

Add Group IP-to-SGT Mappings

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Policy** > **Policy Elements** > **Results** > **TrustSec** > **Security Group Mappings** > **Groups**.

Step 2 Click **Add** to add a new group IP-SGT mapping.

Step 3 Enter a **Name** and a **Description** for the new group.

Step 4 Enter the **Security Group Tag** to which this group will be mapped to.

Step 5 Choose the destination network device on which you want to deploy this mapping. You can deploy the mappings on all trustsec devices, on selected network device groups, or on selected network devices.

Step 6 Click **Submit**.

Import Security Group Mappings Hosts

You can import a list of security group mappings hosts into a Cisco ISE node using a comma-separated value (CSV) file. You cannot run an import of the same resource type at the same time. For example, you cannot concurrently import security group mappings hosts from two different import files.

You can download the CSV template from the **Policy** > **Policy Elements** > **Results** > **Trustsec** > **Security Group Mappings** > **Hosts** > **Import** page. Enter your security group mappings hosts details in the template, and save it as a CSV file, which you can then import this back in to Cisco ISE.

While importing hosts, you can create new records or update existing records. Cisco ISE displays the summary of the number of hosts that are imported and also reports any errors that were found during the import process. When you import hosts, you can also define whether you want Cisco ISE to stop the import process when Cisco ISE encounters the first error.

Step 1 Choose **Policy** > **Policy Elements** > **Results** > **TrustSec** > **Security Group Mappings** > **Hosts**.

Step 2 Click **Import**.

Step 3 Click **Browse** to choose the CSV file from the system that is running the client browser.

Step 4 Check the **Stop Import on First Error** check box, if required.

Step 5 Click **Import**.

Export Security Group Mappings Hosts

You can export security group mappings hosts configured in Cisco ISE in the form of a CSV file that you can use to import these hosts into another Cisco ISE node.

Step 1 Choose **Policy** > **Policy Elements** > **Results** > **TrustSec** > **Security Group Mappings** > **Hosts**.

Step 2 Click **Export**.

Step 3 To export security group mappings hosts, you can do one of the following:

- Check the check boxes next to the hosts that you want to export, and choose **Export** > **Export Selected**.
- Choose **Export** > **Export All** to export all the security group mappings hosts that are defined.

Step 4 Save the export.csv file to your local hard disk.

Deploy IP-to-SGT Mappings

After you add IP-to-SGT mappings to Cisco ISE you must deploy these to the target network device. You must do this explicitly even though you have saved the mappings earlier. Cisco ISE provides you the option to deploy all or only a subset of the mappings.

Before You Begin

You must have added IP-to-SGT mappings to Cisco ISE or created IP-to-SGT mappings groups that contain IP-to-SGT mappings .

Step 1 To deploy IP-to-SGT mappings to devices, you can do one of the following:

- Choose **Policy** > **Policy Elements** > **Results** > **Trustsec** > **Security Group Mappings** > **Groups**, if you want to deploy IP-to-SGT mapping groups to devices.
- Choose **Policy** > **Policy Elements** > **Results** > **Trustsec** > **Security Group Mappings** > **Hosts**, if you want to deploy single IP-to-SGT mappings to devices.

Step 2 Do one of the following:

- Check the check box next to the group or mapping that you want to deploy, and choose **Deploy** to deploy only the selected mappings.
- Choose **Deploy** to deploy all the IP-to-SGT mappings configured in Cisco ISE.

Cisco ISE deploys the mappings to the specific network devices defined in the group or mapping. It also displays a report with details such as deployed devices, configuration, deployment status and failure reason if any.

TrustSec Configuration and Policy Push

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

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

You can also push a configuration change to devices that do not intrinsically support the TrustSec CoA feature.

CoA Supported Network Devices

Cisco ISE sends CoA notifications to the following network devices:

- Network device with single IP address (subnets are not supported)
- Network device configured as a TrustSec 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, TrustSec network devices need to be configured with the Cisco ISE primary node as the CoA client.

The devices return CoA NAK or ACK back to the Cisco ISE primary node. However, the following TrustSec session coming from the network device would be sent to the Cisco ISE node to which the network devise sends all it's other AAA requests and not necessarily to the primary node.

Push Configuration Changes to Non-CoA Supporting Devices

Some platforms do not support Cisco ISE's "Push" feature for Change of Authorization (CoA), for example: some versions of the Nexus network device. For this case, ISE will connect to the network device and make it to trigger an updated configuration request towards ISE. To achieve this, ISE opens an SSHv2 tunnel to the network device, and the Cisco ISE sends a command that triggers a refresh of the TrustSec policy matrix. This method can also be carried out on network platforms that support CoA pushing.

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

Step 2 Check the checkbox next to the required network device and click **Edit**.
Verify that the network device's name, IP address, RADIUS and TrustSec settings are properly configured.

Step 3 Scroll down to **Advanced TrustSec Settings**, and in the **TrustSec Notifications and Updates** section, check the **Send configuration changes to device** checkbox, and click the **CLI (SSH)** radio button.

Step 4 (Optional) Provide an SSH key.

Step 5 Check the **Include this device when deploying Security Group Tag Mapping Updates** check box, for this SGA device to obtain the IP-SGT mappings using device interface credentials.

Step 6 Enter the username and password of the user having privileges to edit the device configuration in the Exec mode.

Step 7 (Optional) Enter the password to enable Exec mode password for the device that would allow you to edit its configuration. You can click **Show** to display the Exec mode password that is already configured for this device.

Step 8 Click **Submit** at the bottom of the page.

The network device is now configured to push Trustsec changes. After you change a Cisco ISE policy, click **Push** to have the new configuration reflected on the network device.

SSH Key Validation

You may want to harden security by using an SSH key. Cisco ISE supports this with its SSH key validation feature.

To use this feature, you open an SSHv2 tunnel from the Cisco ISE to the network device, then use the network device's own CLI to retrieve the SSH key. You then copy this key and paste it into Cisco ISE for validation. Cisco ISE terminates the connection if the SSH key is wrong.

Limitation: Currently, Cisco ISE can validate only one IP (not on ranges of IP, or subnets within an IP)

Before You Begin

You will require:

- Login credentials
- CLI command to retrieve the SSH key

for the network device with which you want the Cisco ISE to communicate securely.

Step 1 On the network device:

a) Log on to the network device with which you want the Cisco ISE to communicate using SSH key validation.
b) Use the device's CLI to show the SSH key.

Example:
For Catalyst devices, the command is: `sho ip ssh`.

c) Copy the SSH key which is displayed.

Step 2 From the Cisco ISE user interface:

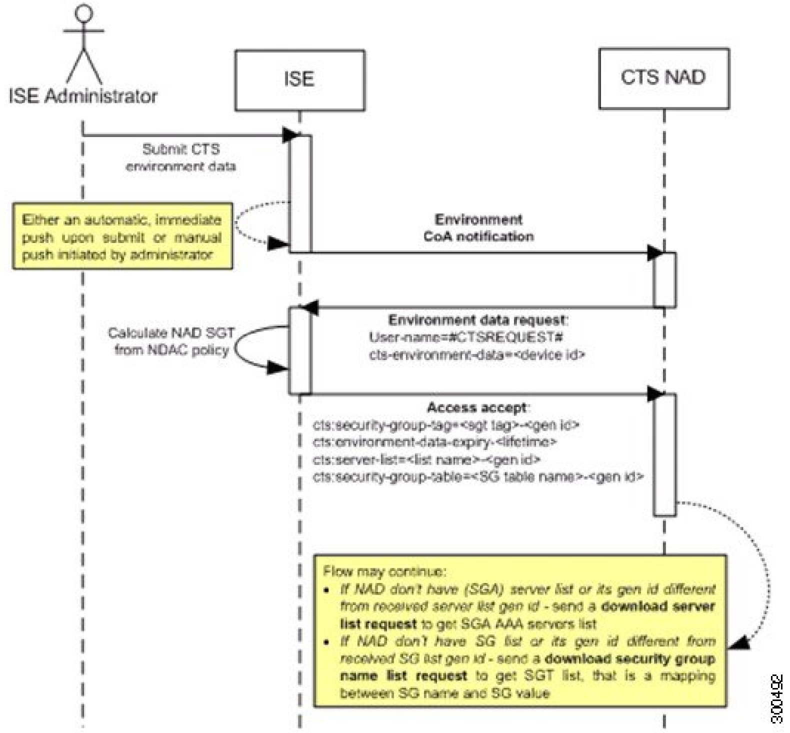
a) Choose **Device Administration** > **Network Resources** > **Network Devices**, and verify the required network device's name, IP address, RADIUS and TrustSec settings are properly configured.
b) Scroll down to **Advanced TrustSec Settings**, and in the **TrustSec Notifications and Updates** section, check the **Send configuration changes to device** checkbox, and click the **CLI (SSH)** radio button.
c) In the **SSH Key** field, paste the SSH key retrieved previously from the network device.
d) Click **Submit** at the bottom of the page.

The network device is now communicating with the Cisco ISE using SSH key validation.

Environment CoA Notification Flow

The following figure depicts the Environment CoA notification flow.

Figure 2: Environment CoA Notification Flow


ISE Administrator
ISE
CTS NAD
Submit CTS environment data
Either an automatic, immediate push upon submit or manual push initiated by administrator
Environment CoA notification
Environment data request:
User-name=#CTSREQUEST#
cts-environment-data=<device id>
Calculate NAD SGT from NDAC policy
Access accept:
cts:security-group-tag=<sgt tag>-<gen id>
cts:environment-data-expiry-<lifetime>
cts:server-list=<list name>-<gen id>
cts:security-group-table=<SG table name>-<gen id>
Flow may continue:
• If NAD don't have (SGA) server list or its gen id different from received server list gen id - send a download server list request to get SGA AAA servers list
• If NAD don't have SG list or its gen id different from received SG list gen id - send a download security group name list request to get SGT list, that is a mapping between SG name and SG value
300492

1. Cisco ISE sends an environment CoA notification to the TrustSec network device.

2. The device returns an environment data request.

3. In response to the environment data request, Cisco ISE returns:

   The environment data of the device that sent the request—This includes the TrustSec device's SGT (as inferred from the NDAC policy) and download environment TTL.

   The name and generation ID of the TrustSec AAA server list.

   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 a TrustSec 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.

Environment CoA Triggers

An Environment CoA can be triggered for:

- Network devices
- Security groups
- AAA servers

Trigger Environment CoA for 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 TrustSec Notifications and Updates parameters under the Advanced TrustSec Settings section.
Changing the environment attribute is notified only to the specific TrustSec network device where the change took place.

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

Trigger Environment CoA for Security Groups

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

Step 1 Choose **Policy** > **Policy Elements** > **Results** > **TrustSec** > **Security Groups**.

Step 2 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 3 Click the **Push** button to initiate an environment CoA notification after changing the names of multiple SGTs. This environment CoA notification goes to all TrustSec network devices and provides an update of all SGTs that were changed.

Trigger Environment CoA for TrustSec AAA Servers

To trigger an Environment CoA for the TrustSec AAA servers, complete the following steps.

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

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

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

Trigger Environment CoA for NDAC Policy

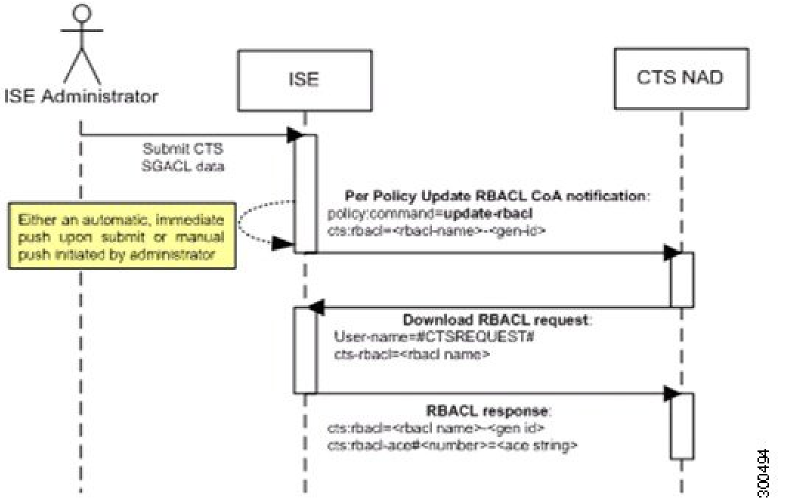
To trigger an Environment CoA for the NDAC Policies, complete the following steps.

You can initiate an environment CoA notification by clicking the **Push** button in the NDAC policy page. This environment CoA notification goes to all TrustSec network devices and provides an update of network device own SGT.

Update SGACL Content Flow

The following figure depicts the Update SGACL Content flow.

Figure 3: Update SGACL Content Flow


ISE Administrator
ISE
CTS NAD
Submit CTS SGACL data
Either an automatic, immediate push upon submit or manual push initiated by administrator
Per Policy Update RBACL CoA notification:
policy:command=update-rbacl
cts:rbacl=<rbacl-name>-<gen-id>
Download RBACL request:
User-name=#CTSREQUEST#
cts-rbacl=<rbacl name>
RBACL response:
cts:rbacl=<rbacl name>-<gen id>
cts:rbacl-ace#<number>=<ace string>
300494

1. Cisco ISE sends an update SGACL named list CoA notification to a TrustSec network device. The notification contains the SGACL name and the generation ID.
2. The device may replay with an SGACL data request if both of the following terms are fulfilled:

   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).

   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, Cisco ISE returns the content of the SGACL (the ACE).

Initiate an Update SGACL Named List CoA

To trigger an Update SGACL 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 **TrustSec** and click **Security Group ACLs**.

Step 3 Change the content of the SGACL. After you submit a SGACL, it promotes the generation ID of the SGACL.

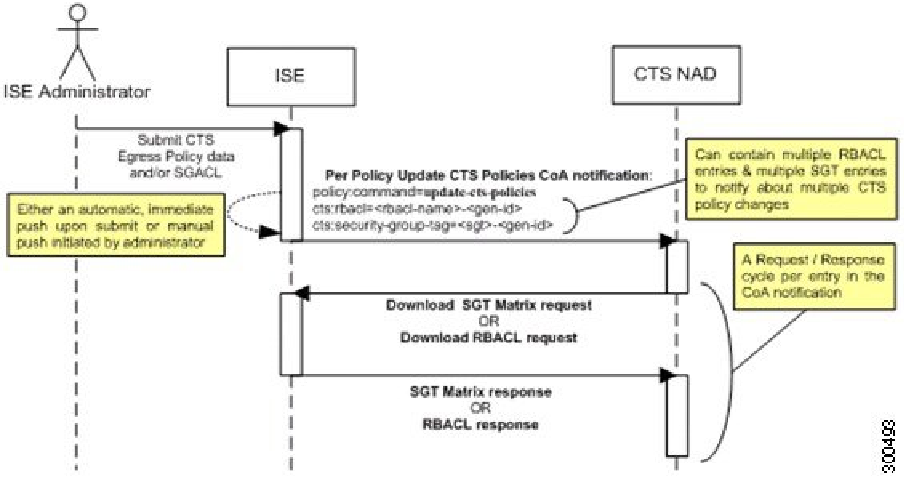
Step 4 Click the **Push** button to initiate an Update SGACL Named List CoA notification after you change the content of multiple SGACLs. This notification goes to all TrustSec network devices, and provides an update of that SGACL content on the relevant devices.
Changing the name or the IP version of an SGACL does not change its generation ID; hence it does not require sending an update SGACL 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.

Policies Update CoA Notification Flow

The following figure depicts the Policies CoA Notification flow.

Figure 4: Policies CoA Notification flow


ISE Administrator
ISE
CTS NAD
Submit CTS Egress Policy data and/or SGACL
Either an automatic, immediate push upon submit or manual push initiated by administrator
Per Policy Update CTS Policies CoA notification:
policy:command=update-cts-policies
cts:rbacl=<rbacl-name>-<gen-id>
cts:security-group-tag=<sgt>-<gen-id>
Can contain multiple RBACL entries & multiple SGT entries to notify about multiple CTS policy changes
A Request / Response cycle per entry in the CoA notification
Download SGT Matrix request OR Download RBACL request
SGT Matrix response OR RBACL response
300493

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

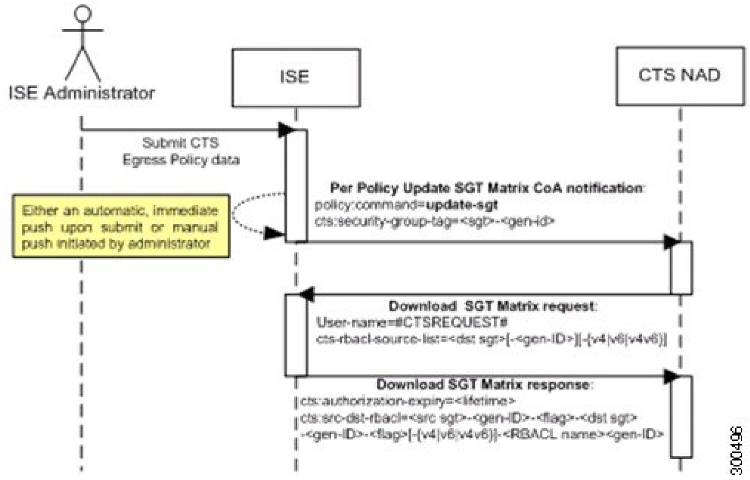
2 The device may replay with multiple SGACL data requests and/or multiple SGT data.

3 In response to each SGACL data request or SGT data request, Cisco ISE returns the relevant data.

Update SGT Matrix CoA Flow

The following figure depicts the Update SGT Matrix CoA flow.

Figure 5: Update SGT Matrix CoA flow


ISE Administrator
ISE
CTS NAD
Submit CTS
Egress Policy data
Either an automatic, immediate push upon submit or manual push initiated by administrator
Per Policy Update SGT Matrix CoA notification:
policy:command=update-sgt
cts:security-group-tag=<sgt>-<gen-id>
Download SGT Matrix request:
User-name=#CTSREQUEST#
cts-rbacl-source-list=<dst sgt>[-<gen-ID>][-{v4|v6|v4v6}]
Download SGT Matrix response:
cts:authorization-expiry=<lifetime>
cts:src-dst-rbacl=<src sgt>-<gen-ID>-<flag>-<dst sgt>
-<gen-ID>-<flag>[-{v4|v6|v4v6}]-<RBACL name><gen-ID>
300496

1 Cisco ISE sends an updated SGT matrix CoA notification to a TrustSec 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:

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).

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, Cisco 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.

Initiate Update SGT Matrix CoA from Egress Policy

Step 1 Choose **Policy** > **TrustSec** > **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 TrustSec network devices, and provides an update of cells content on the relevant devices.

TrustSec CoA Summary

The following table summarizes the various scenarios that may require initiating a TrustSec CoA, the type of CoA used in each scenario, and the related UI pages.

Table 2: TrustSec CoA Summary

UI Page	Operation that triggers CoA	How it is triggered	CoA type	Send to
Network Device	Changing the environment TTL in the TrustSec section of the page	Upon successful Submit of TrustSec network device	Environment	The specific network device
TrustSec AAA Server	Any change in the TrustSec AAA server (create, update, delete, reorder)	Accumulative changes can be pushed by clicking the Push button on the TrustSec AAA servers list page.	Environment	All TrustSec 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 TrustSec 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 TrustSec 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 TrustSec 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 TrustSec 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 TrustSec network devices

Run Top N RBACL Drops by User Report

You can run the Top N RBACL Drops by User report to see the policy violations (based on packet drops) by specific users.

Step 1 From the Cisco ISE Admin dashboard, select **Operations** > **Reports** > **ISE Reports** > **TrustSec**.

Step 2 Click **Top N RBACL Drops by User**.

Step 3 From the **Filters** drop-down menu, add the required monitor modes.

Step 4 Enter the values for the selected parameters accordingly. You can specify the mode from the Enforcement mode drop-down list as Enforce, Monitor, or Both.

Step 5 From the **Time Range** drop-down menu, choose a time period over which the report data will be collected.

Step 6 Click **Run** to run the report for a specific period, along with the selected parameters.