

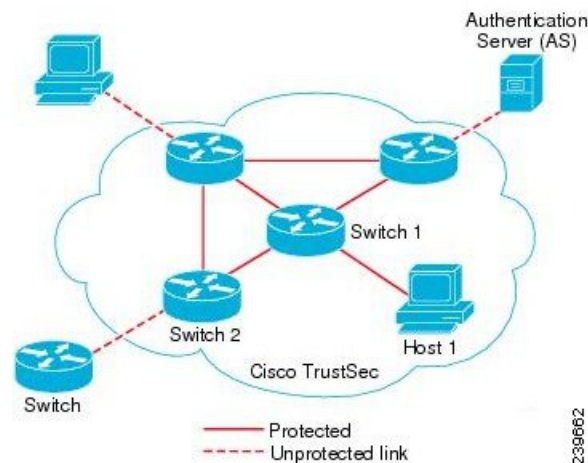


## TrustSec Architecture

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**



### [ISE Community Resource](#)

For information on how to simplify network segmentation and improve security using Cisco TrustSec, see [Simplify Network Segmentation with Cisco TrustSec](#) and [Policy-Based Software Defined Segmentation and Cisco TrustSec Improve Security White Paper](#).

For a complete list of Cisco TrustSec platform support matrices, see [Cisco TrustSec Platform Support Matrix](#).

For a complete list of support documentation available for TrustSec, see [Cisco TrustSec](#).

For a complete list of TrustSec community resources, see [TrustSec Community](#).

- [TrustSec Components, on page 2](#)
- [TrustSec Terminology, on page 3](#)
- [Supported Switches and Required Components for TrustSec, on page 4](#)
- [Integration with Cisco Catalyst Center, on page 4](#)
- [TrustSec Dashboard, on page 6](#)
- [Configure TrustSec Global Settings, on page 8](#)
- [Configure TrustSec Matrix Settings, on page 12](#)
- [Configure TrustSec Devices, on page 13](#)
- [Configure Cisco TrustSec AAA Servers, on page 15](#)
- [Security Groups Configuration, on page 16](#)
- [Egress Policy, on page 22](#)
- [SGT Assignment, on page 37](#)
- [TrustSec Configuration and Policy Push, on page 39](#)
- [Security Group Tag Exchange Protocol , on page 47](#)
- [Add an SXP Domain Filter, on page 48](#)
- [Configure SXP Settings, on page 49](#)
- [Connect Cisco Application Centric Infrastructure with Cisco ISE, on page 50](#)
- [Configure Cisco ACI Settings, on page 51](#)
- [Run Top N RBACL Drops by User Report, on page 52](#)

## 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. Cisco ISE has CTS Provisioning (EAP-FAST) TLSv1.2 support for switching platforms starting IOSXE 17.1, and for routing platforms starting IOSXE 17.6.
- **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
- **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](#).

## Integration with Cisco Catalyst Center

Catalyst Center provides a mechanism to create a trusted communications link with Cisco ISE and to share data with Cisco ISE in a secure manner. After Cisco ISE is registered with Catalyst Center, any device that Catalyst Center discovers, along with relevant configuration and other data, is pushed to Cisco ISE. You can use Catalyst Center to discover devices and then apply both Catalyst Center and Cisco ISE functions to them because these devices will be displayed in both the applications. Catalyst Center and Cisco ISE devices are all uniquely identified by their device names.

## Connecting Catalyst Center to Cisco ISE

For information about configuring Catalyst Center for Cisco ISE, see the [Cisco Catalyst Center Installation Guide](#).

This section provides additional information about the Cisco ISE configuration for Catalyst Center.

- Passwords: Catalyst Center uses the Cisco ISE admin username and password when it connects to Cisco ISE. For information about system passwords, see [Administrative Access to Cisco ISE](#).



---

**Note** Catalyst Center versions earlier than 2.2.1.0 used Cisco ISE CLI to perform the initial integration steps. Hence, the Cisco ISE CLI and admin usernames and passwords had to be the same. From Catalyst Center Release 2.2.1.0 onwards, the use of Cisco ISE CLI has been dropped, and hence the Cisco ISE CLI and admin usernames and passwords need not be the same.

---

- APIs: External RESTful Services (ERS) API service must be enabled in Cisco ISE. Ensure that the **Use CSRF Check for Enhanced Security** option is disabled in Cisco ISE.
- pxGrid: Cisco ISE is a pxGrid controller, and Catalyst Center is a subscriber. Both Cisco ISE and Catalyst Center monitor the TrustSec (SD-Access) content, which contains SGT and SGACL information. Synchronize the system clocks between Cisco ISE and Catalyst Center. For more information about pxGrid in Cisco ISE, see [Cisco pxGrid Node](#).



---

**Note** Cisco ISE 2.4 and later supports pxGrid 2.0 and pxGrid 1.0. Although pxGrid 2.0 allows up to 4 pxGrid nodes in the Cisco ISE deployment, Catalyst Center does not currently support more than 2 pxGrid nodes.

---

- Cisco ISE IP Address: The connection between the Cisco ISE PAN and Catalyst Center must be direct. It cannot be through a proxy, a load balancer, or virtual IP address.  
Verify that Cisco ISE is not using a proxy. Otherwise, exclude the Catalyst Center IP from the proxy.
- SXP: Catalyst Center does not require SXP. You may want to enable SXP when you connect Cisco ISE to the Catalyst Center-managed network, so that Cisco ISE can communicate with network devices that don't have hardware support for TrustSec (SD-Access).



---

**Note** When configuring your Cisco ISE deployment to support TrustSec, or when Cisco ISE is integrated with Catalyst Center, do not configure a Policy Service node as SXP-only. SXP is an interface between TrustSec and non-TrustSec devices. It does not communicate with the TrustSec-enabled network devices.

---

- Certificate for connections to Cisco ISE:
  - The Cisco ISE admin certificate must contain the Cisco ISE IP or FQDN in subject name or SAN.
  - ECDSA is not supported for SSH keys, ISE SSH access, or in certificates for the Catalyst Center and Cisco ISE connection.

- Selfsigned certificates on Catalyst Center must have the Basic Constraint's extension with cA:TRUE (RFC5280 section-4.2.19).



**Note** In Catalyst Center releases earlier than 2.2.1.0, there was a requirement to enable SSH. From Catalyst Center Release 2.2.1.0 onwards, the use of SSH been dropped, and hence, there is no need to enable SSH.

## TrustSec Dashboard

The TrustSec dashboard is a centralized monitoring tool for the TrustSec network.

The TrustSec dashboard contains the following dashlets:

- **Metrics:** The Metrics dashlet displays statistics about the behavior of the TrustSec network.
- **Active SGT Sessions:** The Active SGT Sessions dashlet displays the SGT sessions that are currently active in the network. The Alarms dashlet displays alarms that are related to the TrustSec sessions.
- **Alarms**
- **NAD / SGT Quick View:** The Quick View dashlet displays TrustSec-related information for NADs and SGTs.
- **TrustSec Sessions / NAD Activity Live Log:** In the Live Log dashlet, click the TrustSec Sessions link to view the active TrustSec sessions. You can also view information about TrustSec protocol data requests and responses from NADs to Cisco ISE.

## Metrics

This section displays statistics about the behavior of the TrustSec network. You can select the time frame (for example, past 2 hours, past 2 days, and so on) and the chart type (for example, bars, line, spline).

The latest bar values are displayed on the graphs. It also displays the percentage change from the previous bar. If there is an increase in the bar value, it will be displayed in green with a plus sign. If there is a decrease in the value, it will be displayed in red with a minus sign.

Place your cursor on a bar of a graph to view the time at which the value was calculated and its exact value in the following format: <Value:xxxx Date/Time: xxx>

You can view the following metrics:

SGT sessions	<p>Displays the total number of SGT sessions created during the chosen time frame.</p> <p><b>Note</b> SGT sessions are the user sessions that received an SGT as part of the authorization flow.</p>
--------------	--

SGTs in use	Displays the total number of unique SGTs that were used during the chosen time frame. For example, in one hour, if there were 200 TrustSec sessions, but ISE responded with only 6 types of SGTs in the authorization responses, the graph will display a value 6 for this hour.
Alarms	Displays the total number of alarms and errors that occurred during the chosen time frame. Errors are displayed in red and alarms are displayed in yellow.
NADs in use	Displays the number of unique NADs, which took part in TrustSec authentications during the chosen time frame.

## Current Network Status

The middle section of the dashboard displays information about the current status of the TrustSec network. The values displayed in the graphs are updated when the page is loaded and can be refreshed by using the Refresh Dashboard option.

### Active SGT Sessions

This dashlet displays the SGT sessions that are currently active in the network. You can view the top 10 most used or least used SGTs. The X-axis shows the SGT usage and the Y-axis displays the names of the SGTs.

To view the TrustSec session details for an SGT, click on the bar corresponding to that SGT. The details of the TrustSec sessions related to that SGT are displayed in the Live Log dashlet.

### Alarms

This dashlet displays the alarms related to the TrustSec sessions. You can view the following details:

- Alarm Severity—Displays an icon that represents the severity level of the alarm.
  - High—Includes the alarms that indicate failure in the TrustSec network (for example, device failed to refresh its PAC). Marked with red icon.
  - Medium—Includes warnings that indicate wrong configuration of the network device (for example, device failed to accept CoA message). Marked with yellow.
  - Low—Includes general information and update on network behavior (for example, configuration changes in TrustSec). Marked with blue.
- Alarm description
- Number of times the alarm occurred since this alarm counter was last reset.
- Alarm last occurrence time

### Quick View

The Quick View dashlet displays TrustSec-related information for NADs. You can also view the TrustSec-related information for an SGT.

### NAD Quick View

Enter the name of the TrustSec network device for which you want to view the details in the Search box and press **Enter**. The search box provides an autocomplete feature, which filters and shows the matched device names in a drop-down as the user types into the text box.

The following information is displayed in this dashlet:

- **NDGs**: Lists the Network Device Groups (NDGs) to which this network device belongs.
- **IP Address**: Displays the IP address of the network device. Click on this link to view the NAD activity details in the Live Logs dashlet.
- **Active sessions**: Lists the number of active TrustSec sessions connected to this device.
- **PAC expiry**: Displays the PAC expiry date.
- **Last Policy Refresh**: Displays the policy last download date.
- **Last Authentication**: Displays the last authentication report timestamp for this device.
- **Active SGTs**: Lists the SGTs used in the active sessions that are related to this network device. The number displayed within the brackets denotes the number of sessions that are currently using this SGT. Click on an SGT link to view the TrustSec session details in the Live Log dashlet.

You can use the Show Latest Logs option to view the NAD activity live logs for the device.

### SGT Quick View

Enter the name of the SGT for which you want to view the details in the Search box and press **Enter**.

The following information is displayed in this dashlet:

- **Value**: Displays the SGT value (both decimal and hexadecimal).
- **Icon**: Displays the icon that is assigned to this SGT.
- **Active sessions**: Lists the number of active sessions that are currently using this SGT.
- **Unique users**: Lists the number of unique usernames, which hold this SGT in their active sessions.
- **Updated NADs**: Lists the number of NADs which downloaded policies for this SGT.

## Live Log

Click the link to view the active TrustSec sessions (sessions that have SGT as part of their response).

Click the **NAD Activity** link to view information regarding TrustSec protocol data requests and responses from NADs to Cisco ISE.

Click the **ACI endpoint Activity** link to view the IP-SGT information learnt by Cisco ISE from Cisco ACI.

## Configure TrustSec Global Settings

For Cisco ISE to function as a 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 **Work Centers > TrustSec > Settings > General TrustSec Settings**.
- Step 2** Enter the values in the fields. For information about the fields, see [General TrustSec Settings, on page 9](#)
- Step 3** Click **Save**.
- 

### What to do next

- [Configure TrustSec Devices, on page 13](#)

## General TrustSec Settings

### Verify Trustsec Deployment

This option helps you to verify that the latest TrustSec policies are deployed on all network devices. Alarms are displayed in the Alarms dashlet, under **Work Centers > TrustSec > Dashboard and Home > Summary**, if there are any discrepancies between the policies configured on Cisco ISE and on the network device. The following alarms are displayed in the TrustSec dashboard:

- An alarm displays with an **Info** icon whenever the verification process starts or completes.
- An alarm displays with an **Info** icon if the verification process was cancelled due to a new deployment request.
- An alarm displays with a **Warning** icon if the verification process fails with an error. For example, failure to open the SSH connection with the network device, or if the network device is unavailable, or if there is any discrepancy between the policies configured on Cisco ISE and on the network device.

The **Verify Deployment** option is also available from the below windows.

- **Work Centers > TrustSec > Components > Security Groups**
- **Work Centers > TrustSec > Components > Security Group ACLs**
- **Work Centers > TrustSec > TrustSec Policy > Egress Policy > Matrix**
- **Work Centers > TrustSec > TrustSec Policy > Egress Policy > Source Tree**

- **Work Centers > TrustSec > TrustSec Policy > Egress Policy > Destination Tree**

**Automatic Verification After Every Deploy:** Check this check box if you want Cisco ISE to verify the updates on all the network devices after every deployment. When the deployment process is complete, the verification process starts after the time you specify in the **Time after Deploy Process** field.

**Time After Deploy Process:** Specify the time for which you want Cisco ISE to wait for after the deployment process is complete, before starting the verification process. The valid range is 10–60 minutes.

The current verification process is cancelled if a new deployment request is received during the waiting period or if another verification is in progress.

**Verify Now:** Click this option to start the verification process immediately.

### **Protected Access Credential (PAC)**

- **Tunnel PAC Time to Live :**

Specify 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. The following are the valid ranges:

- 1–157680000 seconds
- 1–2628000 minutes
- 1–43800 hours
- 1–1825 days
- 1–260 weeks

- **Proactive PAC Update Will Occur After:** Cisco ISE proactively provides a new PAC to a client after successful authentication when a configured percentage of the Tunnel PAC TTL remains. The server starts the tunnel PAC update if the first successful authentication occurs before the PAC expires. This mechanism updates the client with a valid PAC. The default value is 10%.

### **Security Group Tag Numbering**

- **System will Assign SGT Numbers:** Choose this option if you want Cisco ISE to automatically generate the SGT numbers.
- **Except Numbers in Range:** Choose this option to reserve a range of SGT numbers for manual configuration. Cisco ISE will not use the values in this range while generating the SGTs.
- **User Must Enter SGT Numbers Manually:** Choose this option to define the SGT numbers manually.

### **Security Group Tag Numbering for APIC EPGs**

**Security Group Tag Numbering for APIC EPGs :** Check this check box and specify the range of numbers to be used for the SGTs created based on the EPGs learnt from APIC.

### **Automatic Security Group Creation**

**Auto Create Security Groups When Creating Authorization Rules:** Check this check box to create the SGTs automatically while creating the authorization policy rules.

If you select this option, the following message displays at the top of the **Authorization Policy** window: Auto Security Group Creation is On

The autocreated SGTs are named based on the rule attributes.



---

**Note** The autocreated SGTs are not deleted if you delete the corresponding authorization policy rule.

---

By default, this option is disabled after a fresh install or upgrade.

- **Automatic Naming Options:** Use this option to define the naming convention for the autocreated SGTs.

(Mandatory) **Name Will Include:** Choose one of the following options:

- **Rule name**
- **SGT number**
- **Rule name and SGT number**

By default, the **Rule name** option is selected.

Optionally, you can add the following information to the SGT name:

- **Policy Set Name** (this option is available only if **Policy Sets** are enabled)
- **Prefix** (up to 8 characters)
- **Suffix** (up to 8 characters)

Cisco ISE displays a sample SGT name in the **Example Name** field, based on your selections.

If an SGT exists with the same name, ISE appends `_x` to the SGT name, where `x` is the first value, starting with 1 (if 1 is not used in the current name). If the new name is longer than 32 characters, Cisco ISE truncate its to the first 32 characters.

### IP SGT static mapping of hostnames

**IP SGT Static Mapping of Hostnames:** If you use FQDN and hostnames, Cisco ISE looks for the corresponding IP addresses in the PAN and PSN nodes while deploying the mappings and checking the deployment status. You can use this option to specify the number of mappings that are created for the IP addresses returned by the DNS query. You can select one of the following options:

- **Create mappings for all IP addresses returned by a DNS query**
- **Create mappings only for the first IPv4 address and the first IPv6 address that is returned by a DNS query**

### Related Topics

[TrustSec Architecture](#), on page 1

[TrustSec Components](#), on page 2

[Configure TrustSec Global Settings](#), on page 8

# Configure TrustSec Matrix Settings

## Before you begin

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

- 
- Step 1** Choose **Work Centers > TrustSec > Settings > TrustSec Matrix Settings**.
- Step 2** Enter the required details in the TrustSec Matrix Settings page.
- Step 3** Click **Save**.
- 

## TrustSec Matrix Settings

*Table 2: Configuring TrustSec Matrix Settings*

Field Name	Usage Guidelines
<b>Allow Multiple SGACLs</b>	<p>Check this check box if you want to allow multiple SGACLs in a cell. If this option is not selected, Cisco ISE will allow only one SGACL per cell.</p> <p>By default, this option is disabled upon fresh install.</p> <p>After upgrade, Cisco ISE will scan the Egress cells and if it identifies at least one cell with multiple SGACLs assigned to it, it allows the admin to add multiple SGACLs in a cell. Otherwise, it allows only one SGACL per cell.</p> <p><b>Note</b> Before disabling multiple SGACLs, you must edit the cells containing multiple SGACLs to include only one SGACL.</p>
<b>Allow Monitoring</b>	<p>Check this check box to enable monitoring for all cells in the matrix. If monitoring is disabled, Monitor All icon is greyed out and the Monitor option is disabled in the Edit Cell dialog.</p> <p>By default, monitoring is disabled upon fresh install.</p> <p><b>Note</b> Before disabling monitoring at matrix level, you must disable monitoring for the cells that are currently being monitored.</p>
<b>Show SGT Numbers</b>	<p>Use this option to display or hide the SGT values (both decimal and hexadecimal) in the matrix cells.</p> <p>By default, the SGT values are displayed in the cells.</p>

Field Name	Usage Guidelines
<b>Appearance Settings</b>	<p>The following options are available:</p> <ul style="list-style-type: none"> <li>• <b>Custom settings:</b> The default theme (colors with no patterns) is displayed initially. You can set your own colors and patterns.</li> <li>• <b>Default settings:</b> Predefined list of colors with no patterns (not editable).</li> <li>• <b>Accessibility settings:</b> Predefined list of colors with patterns (not editable).</li> </ul>
<b>Color/Pattern</b>	<p>To make the matrix more readable, you can apply coloring and patterns to the matrix cells based on the cell contents.</p> <p>The following display types are available:</p> <ul style="list-style-type: none"> <li>• <b>Permit IP/Permit IP Log:</b> Configured inside the cell</li> <li>• <b>Deny IP/Deny IP Log:</b> Configured inside the cell</li> <li>• <b>SGACLs:</b> For SGACLs configured inside the cell</li> <li>• <b>Permit IP/Permit IP Log (Inherited):</b> Taken from the default policy (for non-configured cells)</li> <li>• <b>Deny IP/Deny IP Log (Inherited):</b> Taken from the default policy (for non-configured cells)</li> <li>• <b>SGACLs (Inherited):</b> Taken from the default policy (for non-configured cells)</li> </ul>

**Related Topics**

[Egress Policy](#), on page 22

[Matrix View](#), on page 23

[Configure TrustSec Matrix Settings](#), on page 12

## 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 **Work Centers > TrustSec > Components > 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 **Work Centers > TrustSec > Components > 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 **Work Centers > TrustSec > Components > 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 Cisco TrustSec AAA Servers

You can configure a list of Cisco TrustSec-enabled Cisco ISE servers in the AAA server list for Cisco TrustSec devices to authenticate against any of these servers. When you click Push, the new servers in this list download to the TrustSec devices. When a Cisco TrustSec device tries to authenticate, it chooses any Cisco ISE server from this list. If the first server is down or busy, the Cisco TrustSec device can authenticate itself against any of the other servers from this list. By default, the primary Cisco ISE server is a Cisco TrustSec AAA server. We recommend that you configure more Cisco ISE servers for a more reliable Cisco TrustSec environment.

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

### Before you begin

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

---

**Step 1** Choose **Work Centers > TrustSec > Components > Trustsec Servers > 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 Cisco TrustSec device and server should take place. The default is 1812.

**Step 4** Click **Submit**.

**Step 5** In the **AAA Servers** window that is then displayed, click **Push**.

---

### 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:

- **Work Centers > TrustSec > Components > 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.



---

**Note** Frequent use of the **Push** or **Deploy** button is not advised. When there is a change in a matrix or SGACL, check the notification bar for any pending deployment requests before performing the next deployment operation.

---


## Managing Security Groups in Cisco ISE

### Prerequisites

To create, edit or delete Security Groups, you must be a Super Admin or System Admin.



### Add a Security Group

1. ChooseIn the Cisco ISE GUI, click the **Menu** icon () and choose **Work Centers > TrustSec > Components > Security Groups**.
2. Click **Add** to add a new security group.
3. Enter a name and description (optional) for the new security group.
4. Check the **Propagate to ACI** check box if you want to propagate this SGT to Cisco ACI. The SXP mappings that are related to this SGT will be propagated to Cisco ACI only if they belong to a VPN that is selected in the Cisco ACI Settings page.

This option is disabled by default.

5. 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 General TrustSec Settings page (**Work Centers > TrustSec > Settings > General TrustSec Settings**).
6. Click **Save**.

### Delete a Security Group

You can't delete security groups that are still in use by a source or destination. That includes the default groups, which are mapped to a function in Cisco ISE:

- BYOD
- Guest
- Trustsec Devices

## 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 **Work Centers > TrustSec > Components > 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 **Work Centers > TrustSec > Components > 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 IP SGT Static Mapping

You can use the IP-SGT static mappings to deploy the mappings on TrustSec devices and SXP domains in a unified manner. While creating a new IP-SGT static mapping, you can specify the SXP domains and the devices on which you want to deploy this mapping. You can also associate the IP-SGT mapping to a mapping group.

- 
- Step 1** Choose **Work Centers > TrustSec > Components > IP SGT Static Mapping**.
- Step 2** Click **Add**.
- Step 3** In the **New** area displayed, choose **IP Address** or **Hostname** from the drop-down list, and enter the corresponding value in the field next to it.
- In the **Map to SGT individually** option in the following step, you can specify a SXP domain to map to. However, the **Send to SXP Domain** field is not accessible if you choose **Hostname** in this step. To add an SXP domain in the next step, you must choose **IP Address** here.
- Step 4** If you want to use an existing mapping group, click **Add to a Mapping Group** and select the required group from the **Mapping Group** drop-down list.
- If you want to map this IP address/hostname to an SGT individually, click **Map to SGT Individually** and do the following:
- Select an SGT from the SGT drop-down list.
  - 
  - Select the SXP VPN groups on which the mapping must be deployed.
  - Specify the devices on which you want to deploy this mapping. You can deploy the mapping on all TrustSec devices, on selected network device groups, or on selected network devices.
- Step 5** Click **Save**.
-

## Deploy IP SGT Static Mappings

After adding the mappings, deploy the mappings on the target network devices using the **Deploy** option. You must do this explicitly even if you have saved the mappings earlier. Click **Check Status** to check the deployment status of the devices.

- 
- Step 1** From the **Work Centers** tab, choose **TrustSec > Components > IP SGT Static Mapping**.
- Step 2** Check the check boxes near the mappings that you want to deploy. Check the check box at the top if you want to deploy all the mappings.
- Step 3** Click **Deploy**.
- All the TrustSec devices are listed in the **Deploy IP SGT Static Mapping** window.
- Step 4** Check the check boxes near the devices or the device groups to which the selected mappings must be deployed.
- Check the check box at the top if you want to select all the devices.
  - Use the filter option to search for specific devices.
  - If you do not select any device, the selected mappings are deployed on all the TrustSec devices.
  - When you select devices to deploy new mapping, ISE selects **all** the devices that will be affected by the new mapping.
- Step 5** Click **Deploy**. The deploy button updates the mapping on all the devices affected by the new maps.
- The **Deployment Status** window shows the order in which the devices are updated and the devices that are not getting updated because of an error or because the device is unreachable. After the deployment is complete, the window displays the total number of devices that are successfully updated and the number of devices that are not updated.

---

Use the **Check Status** option in the **IP SGT Static Mapping** page to check if different SGTs are assigned to the same IP address for a specific device. You can use this option to locate the devices that have conflicting mappings, IP addresses that are mapped to multiple SGTs, and the SGTs that are assigned to the same IP address. The **Check Status** option can be used even if device groups, FQDN, hostname, or IPv6 addresses are used in the deployment. You must remove the conflicting mappings or modify the scope of deployment before deploying these mappings.

IPv6 addresses can be used in IP SGT static mappings. These mappings can be propagated using SSH or SXP to specific network devices or network device groups.

If FQDN and hostnames are used, Cisco ISE looks for the corresponding IP addresses in the PAN and PSN nodes while deploying the mappings and checking the deployment status.

Use the **IP SGT Static Mapping of Hostnames** option in the **General TrustSec Settings** window to specify the number of mappings created for the IP addresses returned by the DNS query. Select one of the following options:

- **Create mappings for all the IP addresses returned by a DNS query.**
- **Create mappings only for the first IPv4 address and the first IPv6 address returned by a DNS query.**

## Import IP SGT Static Mappings into Cisco ISE

You can import IP SGT mappings using a CSV file.

You can also download the CSV template from the Admin portal, enter your mapping details, save the template as a CSV file, and then import it back into Cisco ISE.

- 
- Step 1** Choose **Work Centers > TrustSec > Components > IP SGT Static Mapping**.
  - Step 2** Click **Import**.
  - Step 3** Click **Browse** to select the CSV file from the system that is running the client browser.
  - Step 4** Click **Upload**.
- 

## Export IP SGT Static Mappings from Cisco ISE

You can export the IP SGT mappings in the form of a CSV file. You can use this file to import these mappings into another Cisco ISE node.

- 
- Step 1** Choose **Work Centers > TrustSec > Components > IP SGT Static Mapping**.
  - Step 2** Do one of the following:
    - Check the check boxes next to the mappings that you want to export, and choose **Export > Selected**.
    - Choose **Export > All** to export all the mappings.
  - Step 3** Save the mappings.csv file to your local hard disk.
- 

## Add SGT Mapping Group

### Before you begin

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

- 
- Step 1** Choose **Work Centers > TrustSec > Components > IP SGT Static Mapping > Manage Groups**.
  - Step 2** Click **Add**.
  - Step 3** Enter a name and description for the mapping group.
  - Step 4** Do the following:
    - Select an SGT from the **SGT** drop-down list.
    - 
    - Select the SXP VPN groups on which the mappings must be deployed.
    - Specify the devices on which you want to deploy the mappings. You can deploy the mappings on all TrustSec devices, on selected network device groups, or on selected network devices.

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

You can move an IP SGT mapping from one mapping group to another mapping group.

You can also update or delete the mappings and mapping groups. To update a mapping or mapping group, check the check box next to the mapping or mapping group that you want to update, and then click **Edit**. To delete a mapping or mapping group, check the check box next to the mapping or mapping group that you want to delete, and then click **Trash > Selected**. When a mapping group is deleted, the IP SGT mappings within that group are also deleted.

## 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 **Work Centers > TrustSec > Components > 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 ip**

The syntax of SGACL input is not checked within ISE. Make sure you are using the correct syntax so that switches, routers and access points can apply them without errors. The default policy can be configured as **permit IP**, **permit ip log**, **deny ip**, or **deny ip log**. A TrustSec network device attaches the default policy to the end of the specific cell policy.

Here are two examples of SGACLs for guidance. Both include a final catch all rule. The first one denies as the final catch all rule, and the second one permits.

Permit\_Web\_SGACL

```
permit tcp dst eq 80
permit tcp dst eq 443
deny ip
```

Deny\_JumpHost\_Protocols

```
deny tcp dst eq 23
deny tcp dst eq 23
```

```
deny tcp dst eq 3389
permit ip
```

The following table lists syntax for SGACL for IOS, IOS XE and NS-OS operating systems.

SGACL CLI and ACEs	Syntax common across IOS, IOS XE, and NX-OS
config acl	deny, exit, no, permit
deny permit	ahp, eigrp, gre, icmp, igmp, ip, nos, ospf, pcp, pim, tcp, udp
deny tcp deny tcp src deny tcp dst	dst, log, src
deny tcp dst eq deny tcp src eq	range 0 65535
deny udp deny udp src deny udp dest	Dst, log, src
deny tcp dst eq www deny tcp src eq www	range 0 65535

**Note** Hypens are not allowed by some Cisco switches. So `permit dst eq 32767-65535` is not valid. Use `permit dst eq range 32767 65535`. Some Cisco switches do not require `eq` in their command syntax. Thus, `permit dst eq 32767-65535` is not valid in these switches. Use `permit dst 32767-65535` or `permit dst range 32767 65535` instead.

#### Step 4 Click **Push**.

The Push option initiates a CoA notification that tells the Trustsec devices to immediately request updates from Cisco ISE about the configuration changes.



**Note** Cisco ISE has the following predefined SGACLs: Permit IP, Permit IP Log, Deny IP, and Deny IP Log. You can use these SGACLs to configure the TrustSec Matrix using the GUI or ERS API. Though these SGACLs are not listed in the Security Group ACLs listing page in the GUI, these SGACLs will be listed when you use the ERS API to list the available SGACLs (ERS getAll call).

## 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 **Work Centers > TrustSec > TrustSec Policy > 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 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 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.

You can use the following options in the **View** drop-down list to change the matrix view.

- Condensed with SGACL names—If you select this option, the empty cells are hidden and the SGACL names are displayed in the cells.
- Condensed without SGACL names—The empty cells are hidden and the SGACL names are not displayed in the cells. This view is useful when you want to see more matrix cells and differentiate between the content of the cells using colors, patterns, and icons (cell status).
- Full with SGACL names—If you select this option, the left and upper menus are hidden and the SGACL names are displayed in the cells.
- Full without SGACL names—When this option is selected, the matrix is displayed in full screen mode and the SGACL names are not displayed in the cells.

ISE allows you to create, name, and save the custom views. To create custom views, choose **Show > Create Custom View**. You can also update the view criteria or delete unused views.

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.

## Create Custom View

### Before you begin

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

---

**Step 1** In the Matrix View page, select the **Create Custom View** option from the **Show** drop-down list.

**Step 2** In the **Edit View** dialog box, enter the following details:

- View Name—Enter a name for the custom view.
- Source Security Groups—Move the SGTs that you want to include in the custom view to the Show transfer box.



- Show Relevant for Destination—Check this check box if you want to override your selection in the Source Security Group Show transfer box and copy all the entries in the Destination Security Group Hide transfer box. If there are more than 200 entries, the data will not be copied and a warning message will be displayed.
- Destination Security Groups—Move the SGTs that you want to include in the custom view to the Show transfer box.
- Show Relevant for Source—Check this check box if you want to override your selection in the Destination Security Group Show transfer box and copy all the entries in the Source Security Group Hide transfer box.
- Sort Matrix By—Select one of the following options:
  - Manual Order
  - Tag Number
  - SGT Name

**Step 3** Click **Save**.

---

## 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 **Work Centers > TrustSec > TrustSec Policy > 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**.

---

# Configure Work Process Settings

## Before you begin

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

---

**Step 1** Choose **Work Centers > TrustSec > Settings > Work Process Settings**.

**Step 2** Select one of the following options:

- **Single Matrix**—Select this option if you want to create only one Policy matrix for all the devices in the TrustSec network.
- **Multiple Matrices**—Allows you to create multiple policy matrices for different scenarios. You can use these matrices to deploy different policies to different network devices.

**Note** The matrices are independent and each network device can be assigned to only one matrix.

- **Production and Staging Matrices with Approval Process**—Select this option if you want to enable the Workflow mode. Select the users that are assigned to the editor and approver roles. You can select the users only from the Policy Admin and Super Admin groups. A user cannot be assigned to both editor and approver roles.

Ensure that email addresses are configured for the users that are assigned to the editor and approver roles, otherwise email notifications regarding the workflow process will not be sent to these users.

When the Workflow mode is enabled, a user that is assigned to the editor role can create a staging matrix, select the devices on which he wants to deploy the staging policy, and submit the staging policy to the approver for approval. The user that is assigned to the approver role can review the staging policy and approve or reject the request. The staging policy can be deployed on the selected network devices only after the staging policy is reviewed and approved by the approver.

**Step 3** Check the **Use DEFCONS** check box if you want to create DEFCON matrices.

DEFCON matrices are standby policy matrices that can be easily deployed in the event of network security breaches.

You can create DEFCON matrices for the following severity levels: Critical, Severe, Substantial, and Moderate.

When a DEFCON matrix is activated, the corresponding DEFCON policy is immediately deployed on all the TrustSec network devices. You can use the Deactivate option to remove the DEFCON policy from the network devices.

**Step 4** Click **Save**.

---

## Matrices Listing Page

TrustSec policy matrices and DEFCON matrices are listed in the Matrices Listing page (**Work Centers > TrustSec > TrustSec Policy > Egress Policy > Matrices List**). You can also view the number of devices that are assigned to each matrix.



---

**Note** Matrices Listing page is not displayed when Single Matrix mode is enabled with DEFCON matrix option disabled.

---

You can do the following from the Matrices Listing page:

- Add a new matrix
- Edit an existing matrix
- Delete a matrix
- Duplicate an existing matrix
- Assign NADs to a matrix

You can assign NADs to a matrix by using the Assign NADs option. To do this:

1. In the Assign Network Devices window, select the network devices that you want to assign to a matrix. You can also use the filter option to select the network devices.
2. Select the matrix from the Matrix drop-down list. All the existing matrices and the default matrix are listed in this drop-down list.

After assigning the devices to a matrix, click Push to notify the TrustSec configuration changes to the relevant network devices.

Note the following points while working on the Matrices Listing page:

- You cannot edit, delete, or rename the default matrix.
- While creating a new matrix you can start with a blank matrix or copy the policy from an existing matrix.
- If you delete a matrix, the NADs that are assigned to that matrix are automatically moved to the default matrix.
- When you copy an existing matrix, a copy of the matrix will be created but devices are not automatically assigned to the copied matrix.
- In the Multiple Matrices mode, all the devices are assigned to the default matrix at the initial stage.
- In the Multiple Matrices mode, some of the SGACLs might be shared among the matrices. In such cases, changing an SGACL content will affect all matrices that contain this SGACL in one of their cells.
- Multiple matrices cannot be enabled if staging is in progress.
- When you are moving from Multiple Matrices mode to Single Matrix mode, all the NADs are automatically assigned to the default matrix.
- You cannot delete a DEFCON matrix if it is currently activated.

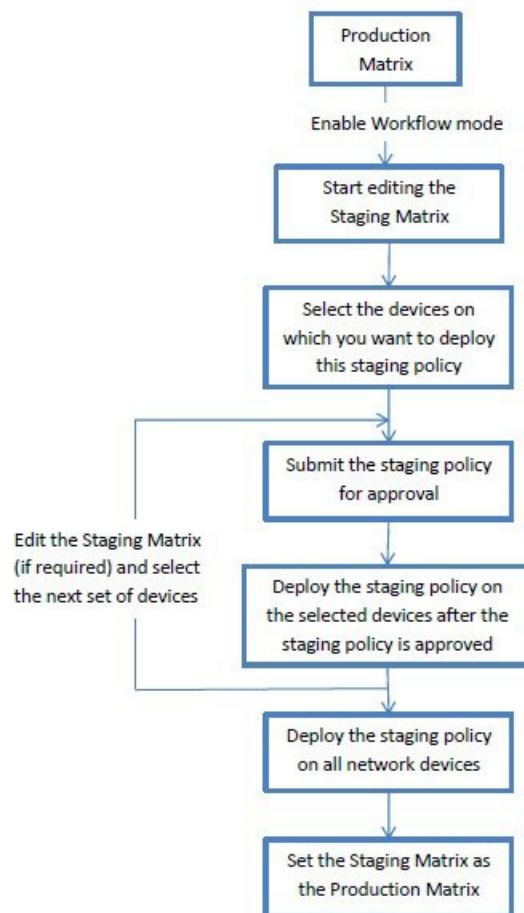
## TrustSec Matrix Workflow Process

The Matrix Workflow feature helps you to test a new policy on a limited set of devices by using a draft version of the matrix (called staging matrix) before deploying the policy on all the network devices. You can submit the staging policy for approval and deploy the staging policy on the selected network devices after it is approved. This feature helps you to deploy the new policy on a limited set of devices, check whether it is working fine, and make any changes, if required. You can continue deploying the policy on next set of devices or on all the devices. When the staging policy is deployed on all the network devices, the staging matrix can be set as the new production matrix.

When the Workflow mode is enabled, a user that is assigned to the editor role can create a staging matrix and edit the matrix cells. The staging matrix is a copy of the production matrix that is currently deployed on the TrustSec network. The editor can select the devices on which he wants to deploy the staging policy and submit the staging policy to the approver for approval. The user that is assigned to the approver role can review the staging policy and approve or reject the request. The staging policy can be deployed on the selected network devices only after the staging policy is reviewed and approved by the approver.

The following figure describes the workflow process.

**Figure 2: Matrix Workflow Process**



Super Admin user can select the users that are assigned to the editor and approver roles in the Workflow Process Settings page (**Work Centers > TrustSec > Settings > Workflow Process**).

You cannot edit the SGTs and SGACLs after the staging policy is deployed on the selected devices, however, you can edit the matrix cells. You can use the Configuration Delta report to track the difference between the production matrix and the staging matrix. You can also click on the Delta icon on a cell to view the changes made to that cell during the staging process.

The following table describes the different stages of the workflow:

Stage	Description
Staging in Edit	<p>The matrix is moved to Staging in Edit state, when an editor starts editing the staging matrix. After editing the staging matrix, the editor can select the devices on which he wants to deploy the new staging policy.</p>
Staging Awaiting Approval	<p>After editing the matrix, the editor submits the staging matrix to the approver for review and approval.</p> <p>While submitting the staging matrix for approval, the editor can add the comments that will be included in the email sent to the approver.</p> <p>The approver can review the staging policy and approve or reject the request. The approver can also view the selected network devices and the Configuration Delta report. While approving or rejecting a request, the approver can add the comments that will be included in the email sent to the editor.</p> <p>The editor can cancel the approval request as long as the staging policy is not deployed on any of the network devices.</p>
Deploy Approved	<p>When the approver approves the request, the staging matrix is moved to Deploy Approved state. If the request is rejected, the matrix is moved back to Staging in Edit state.</p> <p>The editor can deploy the staging policy on the selected network devices only after the staging policy is approved by the approver.</p>
Partially Deployed	<p>After the staging matrix is deployed on the selected devices, the matrix is moved to Partially Deployed state. The matrix remains in the Partially Deployed stage till the staging policy is deployed on all the network devices.</p> <p>You cannot edit the SGTs and SGACLs at this stage, however, you can edit the matrix cells.</p> <p>The devices that are not deployed with the latest policy (out-of-sync devices) are displayed in orange (with italic font) in the Network Device Deployment window. This status is also displayed on the deployment progress status bar. The editor can select these devices and request approval to synchronize the devices that were updated in different deployment cycles.</p>

Stage	Description
Fully Deployed	<p>The above process is repeated till the staging policy is deployed on all the network devices. When the staging matrix is deployed on all the network devices, the approver can set the staging matrix as the production matrix.</p> <p>We recommend that you take a copy of the production matrix before setting the staging matrix as the new production matrix, because after replacing the production matrix with the staging matrix, you cannot rollback to the previous version of the production matrix.</p>

The options displayed in the Workflow drop-down list vary based on the workflow state and the user role (editor or approver). The following table lists the menu options displayed for an editor and approver:

Workflow state	Menu displayed for Editor	Menu displayed for Approver
Staging in Edit	<ul style="list-style-type: none"> <li>• Select network devices</li> </ul> <p>The following options are available in the Network Device Deployment window:</p> <ul style="list-style-type: none"> <li>• Request approval for selected devices</li> <li>• Request approval for all/filtered Staging list</li> <li>• Request approval for all/filtered Production list</li> <li>• Request approval for all/filtered devices</li> <li>• Request approval for all devices</li> <li>• Discard staging</li> <li>• View deltas</li> </ul>	<ul style="list-style-type: none"> <li>• View network devices</li> <li>• View deltas</li> </ul>

Workflow state	Menu displayed for Editor	Menu displayed for Approver
Staging Awaiting Approval	<ul style="list-style-type: none"> <li>• Cancel approval request</li> <li>• View network devices</li> </ul> <p>The following option is available in the Network Device Deployment window:</p> <ul style="list-style-type: none"> <li>• Cancel approval request</li> </ul> <ul style="list-style-type: none"> <li>• View deltas</li> </ul>	<ul style="list-style-type: none"> <li>• Approve deploy</li> <li>• Reject deploy</li> <li>• View network devices</li> </ul> <p>The following options are available in the Network Device Deployment window:</p> <ul style="list-style-type: none"> <li>• Approve deploy</li> <li>• Reject deploy</li> </ul> <ul style="list-style-type: none"> <li>• View deltas</li> </ul>
Approved - ready to deploy	<ul style="list-style-type: none"> <li>• Deploy</li> <li>• Cancel approval request</li> <li>• View network devices</li> </ul> <p>The following options are available in the Network Device Deployment window:</p> <ul style="list-style-type: none"> <li>• Deploy</li> <li>• Cancel approval request</li> </ul> <ul style="list-style-type: none"> <li>• View deltas</li> </ul>	<ul style="list-style-type: none"> <li>• Reject deploy</li> <li>• View network devices</li> </ul> <p>The following option is available in the Network Device Deployment window:</p> <ul style="list-style-type: none"> <li>• Reject deploy</li> </ul> <ul style="list-style-type: none"> <li>• View deltas</li> </ul>

Workflow state	Menu displayed for Editor	Menu displayed for Approver
Partially deployed	<ul style="list-style-type: none"> <li>• Select network devices</li> </ul> <p>The following options are available in the Network Device Deployment window:</p> <ul style="list-style-type: none"> <li>• Request approval for selected devices</li> <li>• Request approval for all/filtered Staging list</li> <li>• Request approval for all/filtered Production list</li> <li>• Request approval for all/filtered devices</li> <li>• Request approval for all devices</li> <li>• View deltas</li> </ul>	<ul style="list-style-type: none"> <li>• View network devices</li> <li>• View deltas</li> </ul>



Workflow state	Menu displayed for Editor	Menu displayed for Approver
Fully deployed	<ul style="list-style-type: none"> <li>• Select network devices</li> </ul> <p>The following options are available in the Network Device Deployment window:</p> <ul style="list-style-type: none"> <li>• Request approval for selected devices</li> <li>• Request approval for all/filtered Staging list</li> <li>• Request approval for all/filtered Production list</li> <li>• Request approval for all/filtered devices</li> <li>• Request approval for all devices</li> <li>• View deltas</li> </ul>	<ul style="list-style-type: none"> <li>• Set as production</li> <li>• View network devices</li> <li>• View deltas</li> </ul>

The workflow options are also available in the Source and Destination Tree view.

You can view the list of devices that downloaded the staging/production policy by using the TrustSec Policy Download report (Work Centers > TrustSec > Reports). The TrustSec Policy Download lists the requests sent by the network devices for policy (SGT/SGACL) download and the details sent by ISE. If the Workflow mode is enabled, the requests can be filtered for production or staging matrix.

## 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 **Work Centers > TrustSec > TrustSec Policy > 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** **Work Centers > TrustSec > TrustSec Policy > Egress Policy > Matrix > Export.**
- Step 2** Check the **Include Empty Cells** check box if you want to include the empty cells (which do not have any SGACL configured) in the exported file.
- When this option is enabled, the whole matrix is exported and the empty cells are marked with the "Empty" keyword in the SGACL column.
- Note** Ensure that the exported file does not contain more than 500000 lines, otherwise the export may fail.
- Step 3** Select one of the following options:
- Local Disk—Select this option if you want to export the file to a local drive on your computer.
  - Repository—Select this option if you want to export the file to a remote repository.
- You must configure the repositories before exporting the file. To configure the repositories, choose **Administration > Maintenance > Repository**. Ensure that read and write access privileges are provided for the repository that you have selected.
- You can encrypt the exported file by using an encryption key.
- You can modify the file name. File name should not include more than 50 characters. By default, the file name includes the current time, however, if the same file name exists on the remote repository, the file will be overwritten.
- Step 4** Click **Export**.
- 

## 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 **Work Centers > TrustSec > TrustSec Policy > Egress Policy > Matrix > Import**.
- 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 **Overwrite Existing Data with New Data** check box if you want to overwrite the existing policy with the one that you are importing. If empty cells (cells that are marked with the "Empty" keyword in the SGACL column) are included in the imported file, the existing policy in the corresponding matrix cells will be deleted.
- While exporting the egress policy, if you want to include the empty cells, check the **Include Empty Cells** check box. For more information, see [Export Egress Policy, on page 34](#).
- Step 5** Click **Validate File** to validate the imported file. Cisco ISE validates the CSV structure, SGT names, SGACL, and file size before importing the file.
- Step 6** Check the **Stop Import on First Error** check box for Cisco ISE to cancel the import if it encounters any errors.
- Step 7** Click **Import**.
- 

## Configure SGT from Egress Policy

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

- 
- Step 1** Choose **Work Centers > TrustSec > TrustSec Policy > 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 an 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.

## 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.

The following SGTs are created by default:

- SGT\_TrustSecDevices
- SGT\_NetworkServices
- SGT\_Employee
- SGT\_Contractor
- SGT\_Guest
- SGT\_ProductionUser
- SGT\_Developer
- SGT\_Auditor
- SGT\_PointofSale
- SGT\_ProductionServers
- SGT\_DevelopmentServers
- SGT\_TestServers
- SGT\_PCIServers
- SGT\_BYOD
- SGT\_Quarantine

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 **Work Centers > TrustSec > TrustSec Policy > 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 **Work Centers > TrustSec > Authorization Policy**.
- 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.

---

## 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 device sends all its 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 **Work Centers > 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 **Work Centers > 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.

---

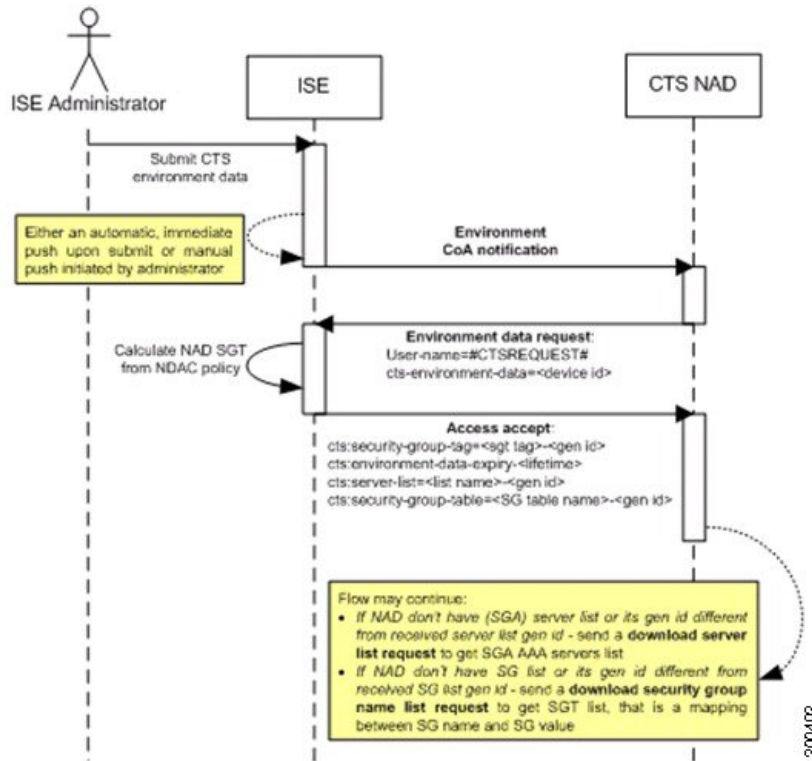
The network device is now communicating with the Cisco ISE using SSH key validation.



## Environment CoA Notification Flow

The following figure depicts the Environment CoA notification flow.

Figure 3: Environment CoA Notification Flow



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 **Work Centers > Device 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 In the Cisco ISE GUI, click the **Menu** icon () and choose **Work Centers > TrustSec > Components > 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 **Work Centers > TrustSec > Components > 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.

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

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.

**Step 2** Choose **Work Centers > TrustSec > TrustSec Policy > Network Device Authorization**.

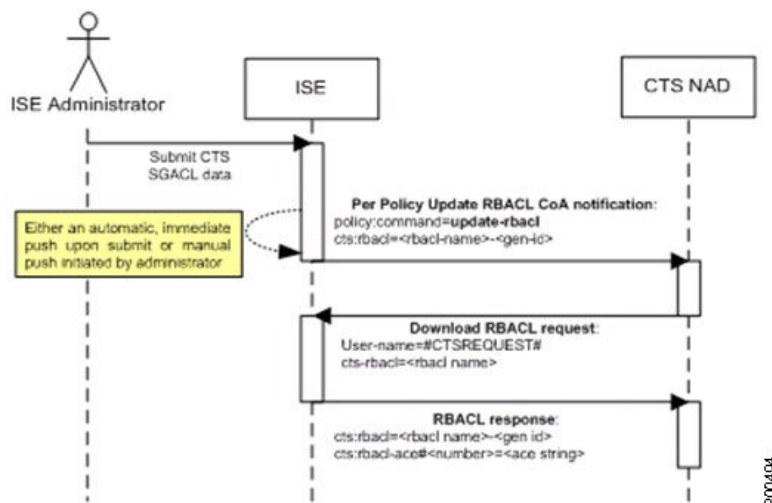
In the NDAC policy page you can create, delete, or update rules of the NDAC policy. These environment changes are notified to all network devices.

**Step 3** 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 4: Update SGACL Content Flow**



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 **Work Centers > TrustSec > Components > Security Group ACLs**.
- Step 2** Change the content of the SGACL. After you submit a SGACL, it promotes the generation ID of the SGACL.
- Step 3** 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.

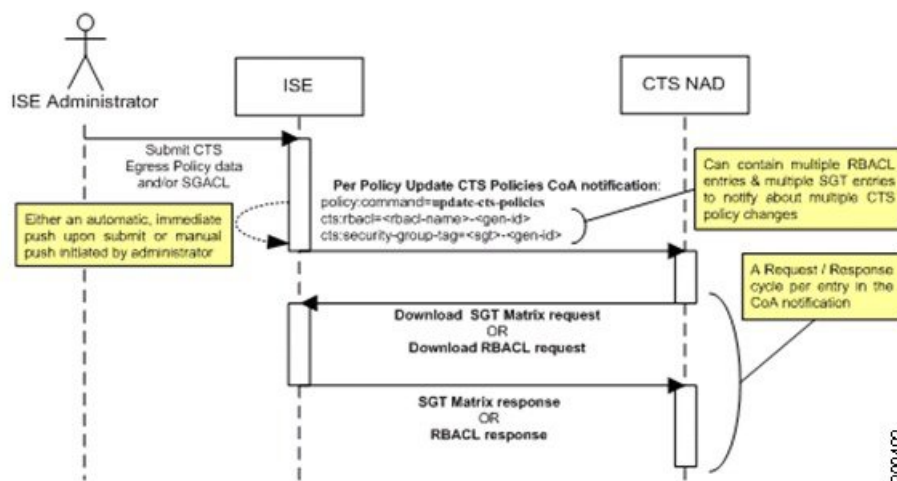
Changing the name or the IP version of an SGACL does not change its generation ID; hence it does not require sending an update SGACL named list CoA notification.

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 5: Policies CoA Notification flow**



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.



Table 3: 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

# Security Group Tag Exchange Protocol

Security Group Tag (SGT) Exchange Protocol (SXP) is used to propagate the SGTs across network devices that do not have hardware support for TrustSec. SXP is used to transport an endpoint's SGT along with the IP address from one SGT-aware network device to another. The data that SXP transports is called as IP-SGT mapping. The SGT to which an endpoint belongs can be assigned statically or dynamically, and the SGT can be used as a classifier in network policies.

To enable SXP service on a node, check the Enable SXP Service check box in the General Node Settings page. You must also specify the interface to be used for SXP service.

SXP uses TCP as its transport protocol to set up SXP connection between two separate network devices. Each SXP connection has one peer designated as SXP speaker and the other peer as SXP listener. The peers can also be configured in a bi-directional mode where each of them act as both speaker and listener. Connections can be initiated by either peers, but mapping information is always propagated from a speaker to a listener.




---

**Note** Session bindings are always propagated on the default SXP domain.

---

The following table lists some of the common terms used in the SXP environment:

IP-SGT mapping	The IP Address to SGT mapping that is exchanged over SXP connection.  To view all the mappings learned by the SXP devices (including static mappings and session mappings), choose <b>Work Centers &gt; TrustSec &gt; SXP &gt; All SXP Mappings</b> .
SXP Speaker	The peer that sends the IP-SGT mappings over the SXP connection.
SXP Listener	The peer that receives the IP-SGT mappings over the SXP connection.

To view the SXP peer devices that are added to Cisco ISE, choose **Work centers > TrustSec > SXP > SXP Devices**.




---

**Note** We recommend that you run the SXP service on a standalone node.

---

Note the following points while using the SXP service:

- When you deregister an SXP node and reregister it back to the existing deployment, the SXP devices that are connected to that node are removed from the deployment. These devices are not displayed in the **SXP Devices** window (**Work Centers > TrustSec > SXP > SXP Devices**). You must manually re-add these devices after reregistering the SXP node to the deployment. However, the SXP devices are not removed if the SXP service on an SXP node is disabled.
- Cisco ISE does not support multiple SXP session bindings with same IP address.

- If the RADIUS accounting updates are too frequent (for example, around 6 to 8 accounting updates in few seconds), sometimes the accounting update packet might be dropped and SXP might not receive the IP-SGT binding.
- After upgrading from a previous version of ISE, SXP does not start automatically. After the upgrade, you must change the SXP password and restart the SXP process.

## Add an SXP Device

### Before you begin

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

---

**Step 1** Choose **Work Centers > TrustSec > SXP > SXP Devices**.

**Step 2** Click **Add**.

**Step 3** Enter the device details:

- Click **Upload from a CSV file** to add the SXP devices using a CSV file. Browse and select the CSV file, and then click **Upload**.

You can also download the CSV template file, fill in the details of the devices that you want to add, and upload the CSV file.

- Click **Add Single Device** to add the device details manually for each SXP device.

Enter the name, IP address, SXP role (listener, speaker, or both), password type, SXP version, and connected PSNs for the peer device. You must also specify the SXP domain to which the peer device is connected.

**Step 4** (Optional) Click **Advanced Settings** and enter the following details:

- **Minimum Acceptable Hold Timer**—Specify the time, in seconds, a speaker will send keepalive messages for keeping the connection alive. The valid range is from 1 to 65534.
- **Keep Alive Timer**—Used by a speaker to trigger the dispatch of keepalive messages during intervals when no other information is exported via update messages. The valid range is from 0 to 64000.

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

---

## Add an SXP Domain Filter

You can view all the mappings learned by the SXP devices (including static mappings and session mappings) on the **Work Centers > TrustSec > SXP > All SXP Mappings** page.

By default, session mappings learnt from the network devices are sent only to the default VPN group (called default). You can create SXP domain filters to send the mappings to different SXP domains (VPNs).

To add an SXP domain filter:



### Before you begin

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

---

**Step 1** Choose **Work Centers > TrustSec > SXP > All SXP Mappings**.

**Step 2** Click **Add SXP Domain Filter**.

**Step 3** Do the following:

- Enter the subnet details. The session mappings of the network devices with IP addresses from this subnet are sent to the SXP domain (VPN) that is selected in the **SXP Domain** field.
- Select an SGT from the SGT drop-down list. The session mappings that are related to this SGT are sent to the SXP domain that is selected in the **SXP Domain** field.

If you have specified both Subnet and SGT, the session mappings that match this filter are sent to the SXP domain that you have selected in the **SXP Domain** field.

- Select the SXP domain to which the mappings must be sent.

**Step 4** Click **Save**.

---

You can also update or delete the SXP domain filters. To update a filter, click **Manage SXP Domain Filter**, check the check box next to the filter that you want to update, and then click **Edit**. To delete a filter, check the check box next to the filter that you want to delete, and then click **Trash > Selected**.

## Configure SXP Settings

### Before you begin

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

---

**Step 1** Choose **Work Centers > TrustSec > Settings > SXP Settings**.

**Step 2** Enter the required details in the SXP Settings page.

If you uncheck the **Publish SXP Bindings on PxGrid** check box, the IP-SGT mappings will not be propagated across the network devices.

**Step 3** Click **Save**.

**Note** When the SXP settings are changed, the SXP service is restarted.

---

# Connect Cisco Application Centric Infrastructure with Cisco ISE

Cisco ISE can synchronize SGTs and SXP mappings with the Internal Endpoint Groups (IEPGs), External Endpoint Groups (EEPGs), and endpoint (EP) configuration of Cisco Application Centric Infrastructure (Cisco ACI).

Cisco ISE supports packets coming from the Cisco ACI domain to the TrustSec domain by synchronizing the IEPGs, and creating correlating read-only SGTs in ISE. These SGTs map the endpoints configured in Cisco ACI, and create correlating SXP mappings in ISE. The SGTs displayed on the Security Groups page (with the value "Cisco ACI" in the Learned From field). You can view the SXP mappings on the All SXP Mappings page. These mappings are sent to Cisco ACI only if the Policy Plane option is selected (in the Cisco ACI Settings page) and the SXP device belongs to an SXP domain, that you configured on the Cisco ACI Settings page.



---

**Note** You can't use read-only SGTs in IP-SGT mappings, mapping groups, and SXP local mappings.

---

When you add a Security Group, you can specify whether the SGT is sent to Cisco ACI by enabling the **Propagate to ACI** option. When this option is enabled, the SXP mappings that are related to this SGT are sent to Cisco ACI. But, only if the Policy Plane option is selected (in the Cisco ACI Settings page) and the SXP device belongs to an SXP Domain, which you configure on the Cisco ACI Settings page.

Cisco ACI supports the packets that are sent from the TrustSec domain to the Cisco ACI domain by synchronizing the SGTs, and creating correlating EEPGs. Cisco ACI creates subnets under EEPG based on the SXP mappings from Cisco ISE. These subnets are not deleted from Cisco ACI, when the corresponding SXP mappings are deleted in Cisco ISE.

When an IEPG is updated in Cisco ACI, the corresponding SGT configuration is updated in Cisco ISE. A new EEPG is created in Cisco ACI, when an SGT is added in Cisco ISE. When an SGT is deleted, the corresponding EEPG is deleted in Cisco ACI. When an endpoint is updated in Cisco ACI, the corresponding SXP mapping is updated in Cisco ISE.

If the connection with the Cisco ACI server is lost, Cisco ISE re-synchronizes the data again when the connection is reestablished.



---

**Note** You must enable the SXP service to use the Cisco ACI integration feature.

---

To successfully integrate Cisco ISE and Cisco ACI, the signed certificate should have proper SAN fields. Cisco ISE will use values specified in the SAN extension property of the certificate presented by the APIC server.



---

**Note** Only IPv4-SXP bindings with Cisco ACI are currently supported by Cisco ISE. IPv6-SGT bindings from Cisco ACI are not supported.

---

# Configure Cisco ACI Settings

## Before you begin

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

- 
- Step 1** Choose **Administration > System > Certificates > Trusted Certificates > Import**.
- Step 2** Import the Cisco ACI certificate. For more information, see [Import a Root Certificate into the Trusted Certificate Store](#).
- Step 3** Choose **Work Centers > TrustSec > Settings > ACI Settings**.
- Step 4** Check the **TrustSec-ACI Policy Element Exchange** check box to synchronize SGTs and SXP mappings with IEPGs, EEPGs, and endpoint configuration of Cisco ACI.
- Step 5** Select one of the following options:
- **Policy Plane**—Select this option if you want Cisco ISE to interact only with APIC data center to interchange SGT, EPG, and SXP information.
  - **Data Plane**—If you select this option, in addition to SGT and EPG, additional information is provided to the ASR devices that are connected between the TrustSec network and the APIC-controlled network. These ASR devices must contain the Translation tables for SGT-to-EPG and EPG-to-SGT conversion.
- Note** SXP mappings are not propagated to Cisco ACI if you select the Data Plane option.
- Step 6** Enter the following details if you have selected the Policy Plane option:
- **IP address / Host name:** Enter the IP address or hostname of the Cisco ACI server. You can enter three IP addresses or host names separated by commas.
  - **Admin name:** Enter the username of the Cisco ACI admin user.
  - **Admin password:** Enter the password of the Cisco ACI admin user.
  - **Tenant name:** Enter the name of the tenant that is configured on the Cisco ACI.
  - **L3 Route network name:** Enter the name of the Layer 3 Route network that is configured on the Cisco ACI for synchronizing the policy elements.
  - Click **Test Settings** to check the connectivity with the Cisco ACI server.
  - **New SGT Suffix:** This suffix will be added to the SGTs that are newly created based on the EPGs learnt from Cisco ACI.
- Note** The EPG name will be truncated if it is greater than 32 characters. However, you can view the full name of the EPG, application profile name, and SGT suffix details in the Description field in the Security Groups listing page.
- **New EPG Suffix:** This suffix will be added to the EPGs that are newly created in Cisco ACI based on the SGTs learnt from Cisco ISE.
  - In the **SXP Propagation** area, you can select all the SXP domains or specify the SXP domains that will share the mappings with Cisco ACI.
- Step 7** Enter the following details if you have selected the Data Plane option:

- **Propagate using SXP:** Check this check box if you want Cisco ISE to learn Endpoint (EP) data from Cisco ACI and propagate the EP data using SXP.

**Note** When you select this option, ensure that the SXP service is enabled on the deployment node (**Administration > System > Deployment**).

- **IP address/Hostname:** Enter the IP address or hostname of the Cisco ACI server. You can enter three IP addresses or host names separated by commas.
- **Admin name:** Enter the username of the Cisco ACI admin user.
- **Admin password:** Enter the password of the Cisco ACI admin user.
- **Tenant name:** Enter the name of the tenant that is configured on the Cisco ACI.
- **Test Settings:** Click this button to check the connectivity with the Cisco ACI server.
- **Max number of IEPGs:** Specify the maximum number of IEPGs that will be converted to SGTs. IEPGs are converted in alphabetical order. Default value is 1000.
- **Max number of SGTs:** Specify the maximum number of SGTs that will be converted to IEPGs. SGTs are converted in alphabetical order. Default value is 500.
- **New SGT Suffix:** This suffix will be added to the SGTs that are newly created based on the EPGs learnt from Cisco ACI.
- **New EPG Suffix:** This suffix will be added to the EPGs that are newly created in Cisco ACI based on the SGTs learnt from Cisco ISE.
- **EEPG name for untagged packets:** Cisco TrustSec packets that are not converted to an EEPG are tagged with this name in Cisco ACI.
- **Default SGT name:** Choose the default name for the SGT from the drop-down list.

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

---

## 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** Choose **Operations > 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.
-