

Identity Source: ISE/ISE-PIC

The following topics discuss how to perform user awareness and user control with ISE/ISE-PIC:

- The ISE/ISE-PIC identity source, on page 1
- License requirements for ISE/ISE-PIC, on page 3
- Requirements and prerequisites for ISE/ISE-PIC, on page 3
- Best practices for ISE/ISE-PIC integration, on page 4
- ISE/ISE-PIC configurations for user control , on page 6
- ISE/ISE-PIC configuration, on page 9
- Configure ISE for user control, on page 15
- Troubleshoot Cisco ISE/ISE-PIC or Cisco TrustSec issues, on page 18
- History for ISE/ISE-PIC, on page 19

The ISE/ISE-PIC identity source

The ISE/ISE-PIC identity source is an authoritative identity source that

- provides user awareness data for users who authenticate using Active Directory (AD), LDAP, RADIUS, or RSA
- enables passive authentication and user control on Active Directory-authenticated users
- integrates with the system to manage network access and classify traffic in a Cisco TrustSec environment, and
- supports security group tags (SGT) for access control.

ISE/ISE-PIC integration capabilities

You can integrate your Cisco Identity Services Engine (ISE) or ISE Passive Identity Connector (ISE-PIC) deployment with the system to use ISE/ISE-PIC for passive authentication.

In addition to user awareness and control, if you use Cisco ISE to define and use security group tags (SGT) for classifying traffic in a Cisco TrustSec network, you can write access control rules that use SGT as both source and destination matching criteria. This enables you to block or allow access based on security group membership rather than IP addresses or network objects. Also see Best practices for ISE/ISE-PIC integration, on page 4.

ISE/ISE-PIC does not report failed login attempts or the activity of ISE Guest Services users.

Note The system does not parse IEEE 802.1x machine authentication but it *does* parse 802.1x user authentication. If you are using 802.1x with ISE, you must include user authentication. 802.1x machine authentication will not provide a user identity to the Cloud-Delivered Firewall Management Center that can be used in policy.

For more information on Cisco ISE/ISE-PIC, see the Identity Services Engine Passive Identity Connector administrator guides or the Identity Services Engine administrator guides.

Note We strongly recommend you use the latest version of ISE/ISE-PIC to get the latest feature set and the most number of issue fixes. For specific compatible ISE/ISE-PIC versions and feature support, refer to the Cisco Secure Firewall Compatibility Guide.

Source and destination security group tag (SGT) matching

If you use Cisco ISE to define and use security group tags (SGT) for classifying traffic in a Cisco TrustSec network, you can write access control rules that use SGT as both source and destination matching criteria. This enables you to block or allow access based on security group membership rather than IP addresses or network objects.

You can also use source SGT matching in DNS rules, as explained in Controlling traffic based on security group tag or dynamic attributes.

Benefits and implementation details

Matching on SGT tags provides these benefits:

- The Cloud-Delivered Firewall Management Center can subscribe to Security Group Tag eXchange Protocol (SXP) mappings from ISE.

  ISE uses SXP to propagate the IP-to-SGT mapping database to managed devices. When you configure Cloud-Delivered Firewall Management Center to use an ISE server, you enable the option to listen to the SXP topic from ISE. This causes the Cloud-Delivered Firewall Management Center to learn about the security group tags and mappings directly from ISE. The Cloud-Delivered Firewall Management Center then publishes SGTs and mappings to managed devices.

  The SXP Topic receives security group tags based on static and dynamic mappings learned through the SXP protocol between ISE and other SXP compliant devices (like switches).

  You can create security group tags in ISE and assign host or network IP addresses to each tag. You can also assign SGTs to user accounts, and the SGT is assigned to the user's traffic. If the switches and routers in the network are configured to do so, these tags then get assigned to packets as they enter the network controlled by ISE, the Cisco TrustSec cloud.

  SXP is *not* supported by ISE-PIC.

- The Cloud-Delivered Firewall Management Center and managed devices can learn about SGT mappings without deploying additional policy. (In other words, you can view connection events for SGT mappings without deploying an access control policy.)

- Supports Cisco TrustSec, which enables you to segment your network to protect critical business assets.

- When a managed device evaluates SGT as a traffic matching criteria for a rule, it uses this priority:
  1. The source SGT tag defined in the packet, if any.

     For the SGT tag to be in the packet, the switches and routers in the network must be configured to add them. See the ISE documentation for information on how to implement this method.
  2. The SGT assigned to the user session, as downloaded from the ISE session directory. The SGT can be matched to source or destination.
  3. The SGT-to-IP address mapping downloaded using SXP. If the IP address is in the range for an SGT, then the traffic matches the rule that uses the SGT. The SGT can be matched to source or destination.

SGT matching examples

- In ISE, create an SGT tag named Guest Users and associate it with the 192.0.2.0/24 network.

  For example, you could use Guest Users as a source SGT condition in your access control rule and restrict access to certain URLs, web site categories, or networks from anyone who accesses your network.
- In ISE, create an SGT tag named Restricted Networks and associate it with the 198.51.100.0/8 network.

  For example, you could use Restricted Networks as a destination SGT rule condition and block access from Guest Users and other networks that have users who are not authorized to access the network.

License requirements for ISE/ISE-PIC

This reference provides license requirements for ISE and ISE-PIC systems.

Threat Defense License

Any

Classic License

Control

Requirements and prerequisites for ISE/ISE-PIC

Supported domains

Any

User roles

- Administrator

- Access Admin
- Network Admin

Best practices for ISE/ISE-PIC integration

ISE/ISE-PIC version and configuration compatibility

Ensure your ISE/ISE-PIC version and configuration supports proper integration with the Cloud-Delivered Firewall Management Center.

- Use the latest version of ISE/ISE-PIC to get the latest feature set.
- Synchronize the time on the ISE/ISE-PIC server and the Cloud-Delivered Firewall Management Center. Otherwise, the system might perform user timeouts at unexpected intervals.
- Configure and enable a realm for the ISE server assuming the pxGrid persona to implement user control using ISE or ISE-PIC data as described in Create an LDAP realm or an Active Directory realm and realm directory.
- Ensure each Cloud-Delivered Firewall Management Center host name that connects to an ISE server is unique; otherwise, the connection to one of the Cloud-Delivered Firewall Management Centers will be dropped.
- If you use ISE 3.4 Patch 4 or later as an identity source for Cloud-Delivered Firewall Management Center in a hybrid deployment, where authorization can use either Microsoft Entra ID (Azure) or on-prem Active Directory, ensure that your ISE authorization policy rule order evaluates on-premises Active Directory external identity source rules before any Entra ID-based authorization rules. This guideline applies to hybrid deployments in which remote access VPN users can authenticate with Microsoft Entra ID, and Cloud-Delivered Firewall Management Center uses the on-premises Microsoft Active Directory realm for user identity and user-based access control.

For the specific versions of ISE/ISE-PIC that are compatible with this version of the system, see the Cisco Firepower Compatibility Guide.

If you configure ISE/ISE-PIC to monitor a large number of user groups, the system might drop user mappings based on groups due to managed device memory limitations. As a result, rules with realm or user conditions might not perform as expected.

For any device running version 6.7 or later, you can optionally use the **configure identity-subnet-filter** command to limit the subnets that the managed device monitors. For more information, see the *Cisco Secure Firewall Threat Defense Command Reference*.

Alternatively, you can configure a network object and apply that object as an Identity Mapping Filter in the identity policy. See Create an identity policy.

IPv6 support

Verify IPv6 compatibility between ISE/ISE-PIC and your managed devices.

- Compatible versions of ISE/ISE-PIC version 2.x include support for IPv6-enabled endpoints.
- Version 3.0 (patch 2) and later of ISE/ISE-PIC enables IPv6 communication between ISE/ISE-PIC and the Cloud-Delivered Firewall Management Center.

Proxy sequence configuration

A *proxy sequence* is one or more managed devices that can be used to communicate with an LDAP, Active Directory, or ISE/ISE-PIC server. It is necessary only if Security Cloud Control cannot communicate with your Active Directory or ISE/ISE-PIC server. (For example, Security Cloud Control might be in a public cloud but Active Directory or ISE/ISE-PIC might be in a private cloud.)

Although you can use one managed device as a proxy sequence, we strongly recommend you set up two or more so that, in the event one managed device cannot communicate with Active Directory or ISE/ISE-PIC, another managed device can take over.

Because of its limited capacity, we recommend you *do not* use a Secure Firewall 220 as a proxy sequence.

Client approval in ISE

Manually approve clients in ISE before the connection between the ISE server and the Cloud-Delivered Firewall Management Center succeeds. Typically, there are two clients: one for the connection test and another for ISE agent.

You can also enable **Automatically approve new accounts** in ISE as discussed in the chapter on Managing users and external identity sources in the *Cisco Identity Services Engine Administrator Guide*.

Unreachable session management

If a user session in ISE/ISE-PIC is reported as unreachable, the system prunes that session so another user with the same IP cannot match the unreachable user's identity rules.

You can control this behavior in ISE/ISE-PIC by going to **Providers** > **Endpoint Probes** and clicking one of these options:

- **Enabled** to cause ISE/ISE-PIC to monitor endpoint connections and therefore to cause the Cloud-Delivered Firewall Management Center prune a session from an unreachable user.
- **Disabled** to cause ISE/ISE-PIC to ignore endpoint connections.

Security group tags (SGT) implementation

A Security Group Tag (SGT) specifies the privileges of a traffic source within a trusted network. Cisco ISE and Cisco TrustSec use a feature called Security Group Access (SGA) to apply SGT attributes to packets as they enter the network. These SGTs correspond to a user's assigned security group within ISE or TrustSec. If you configure ISE as an identity source, the Firepower System can use these SGTs to filter traffic.

Security Group Tags can be used both as source and destination matching criteria in access control and DNS rules.



Note

- To implement user control using only the ISE SGT attribute tag, you do not need to configure a realm for the ISE server. ISE SGT attribute conditions can be configured in policies with or without an associated identity policy.
- In some rules, custom SGT conditions can match traffic tagged with SGT attributes that were *not* assigned by ISE. This is not considered user control, and works only if you are not using ISE/ISE-PIC as an identity source.

To match destination SGT tags in addition to source SGT tags, verify these requirements:

Required ISE version: 2.6 patch 6 or later, 2.7 patch 2 or later

Router support: Any Cisco router that supports SGT inline tagging over Ethernet. For more information, consult a reference such as the Cisco Group Based Policy Platform and Capability Matrix Release

Limitations:

- Quality of Service (QoS) policy uses source SGT matching only; it does *not* use destination SGT matching
- RA-VPN does not receive SGT mappings directly through RADIUS

ISE and high availability

When the primary ISE/ISE-PIC server fails, understand the impact on operations.

As a result of the integration with pxGrid v2, the Cloud-Delivered Firewall Management Center round-robins between both configured ISE hosts until one accepts the connection.

If the connection is lost, the Cloud-Delivered Firewall Management Center resumes round-robin attempts to the connected hosts.

Endpoint location (or location IP)

An Endpoint Location attribute is the IP address of the network device that used ISE to authenticate the user, as identified by ISE.

You must configure and deploy an identity policy to control traffic based on **Endpoint Location (Location IP)**.

ISE attributes

Configuring an ISE connection populates the Cloud-Delivered Firewall Management Center database with ISE attribute data. You can use ISE attributes for user awareness and user control. This is not supported with ISE-PIC.

Endpoint profile (or device type)

An Endpoint Profile attribute is the user's endpoint device type, as identified by ISE.

You must configure and deploy an identity policy to control traffic based on **Endpoint Profile (Device Type)**.

ISE/ISE-PIC configurations for user control

An ISE/ISE-PIC configuration uses realms, identity policies, and access control policies to control user access to network resources.

Configuration options

You can use ISE/ISE-PIC in any of these configurations:

- With a realm, identity policy, and associated access control policy: Use a realm to control *user* access to network resources in policy. You can still use ISE/ISE-PIC Security Group Tags (SGT) metadata in your policies.
- With an access control policy only. No realm or identity policy are necessary: Use this method to control network access using SGT metadata alone.

Configure ISE/ISE-PIC without a realm

Configure ISE to allow or block access to the network using SGT tags for enhanced network security and access control.

This topic provides a high-level overview of tasks you must complete to configure ISE to be able to allow or block access to the network using SGT tags.

Procedure

Step 1 SGT matching: Enable SXP on ISE.

This enables the Cloud-Delivered Firewall Management Center to receive updates from ISE when SGT metadata changes.

Step 2 Export system certificates from ISE/ISE-PIC.

The certificates are required to connect securely between the ISE/ISE-PIC pxGrid, monitoring (MNT) servers and the Cloud-Delivered Firewall Management Center. See Export certificates from the ISE/ISE-PIC server for use in the Cloud-Delivered Firewall Management Center, on page 12

Step 3 Import the certificates in the Cloud-Delivered Firewall Management Center.

The certificates must be imported as follows:

- pxGrid client certificate: internal certificate with key (**Objects** > **PKI** > **Internal Certs**)
- pxGrid server certificate: trusted CA (**Objects** > **PKI** > **Trusted CAs**)
- MNT certificate: trusted CA

Step 4 Create the ISE/ISE-PIC identity source.

The ISE/ISE-PIC identity source enables you to control user activity using Security Group Tags (SGT) provided by ISE/ISE-PIC.

Step 5 Create an access control rule.

The access control rule specifies an action to take (for example, allow or block) if traffic matches the rule criteria. You can use source and destination SGT metadata as matching criteria in the access control rule. See Access control rules.

Step 6 Deploy the access control policy to managed devices.

Before your policy can take effect, it must be deployed to managed devices. See Deploy configuration changes.

What to do next

Export certificates from the ISE/ISE-PIC server for use in the Cloud-Delivered Firewall Management Center, on page 12

Configure ISE/ISE-PIC for user control using a realm

This task enables you to configure ISE/ISE-PIC for user control and to allow or block user or group access to the network. Users and groups can be stored in any server listed in Supported servers for realms.

This topic provides a high-level overview of tasks you must complete to configure ISE/ISE-PIC for user control and to be able to allow or block user or group access to the network.

Procedure

Step 1 Enable SXP on ISE for destination SGT only.

This enables the Cloud-Delivered Firewall Management Center to receive updates from ISE when SGT metadata changes.

Step 2 Export system certificates from ISE/ISE-PIC.

The certificates are required to connect securely between the ISE/ISE-PIC pxGrid, monitoring (MNT) servers and the Cloud-Delivered Firewall Management Center. See the following:

- pxGrid server and MNT server certificate: Export certificates from the ISE/ISE-PIC server for use in the Cloud-Delivered Firewall Management Center, on page 12
- pxGrid client certificate: Generate a self-signed certificate, on page 13

Step 3 Import the certificates in the Cloud-Delivered Firewall Management Center.

The certificates must be imported as follows:

- pxGrid client certificate: internal certificate with key (**Objects** > **PKI** > **Internal Certs**)
- pxGrid server certificate: trusted CA (**Objects** > **PKI** > **Trusted CAs**)
- MNT certificate: trusted CA

Step 4 Create a proxy sequence for use with the realm and also with ISE/ISE-PIC (optional).

A *proxy sequence* is one or more managed devices that can be used to communicate with an LDAP, Active Directory, or ISE/ISE-PIC server. It is necessary only if Security Cloud Control cannot communicate with your Active Directory or ISE/ISE-PIC server. (For example, Security Cloud Control might be in a public cloud but Active Directory or ISE/ISE-PIC might be in a private cloud.)

Although you can use one managed device as a proxy sequence, we strongly recommend you set up two or more so that, in the event one managed device cannot communicate with Active Directory or ISE/ISE-PIC, another managed device can take over.

Step 5 Create a realm.

You must create a realm only to control access to the network by the users and groups you choose.

See Create an LDAP realm or an Active Directory realm and realm directory.

a) Download users and groups, and enable the realm.

Downloading users and groups enables you to use them in access control rules. See Synchronize users and groups.

Step 6 Create the ISE/ISE-PIC identity source.

The ISE/ISE-PIC identity source enables you to control user activity using Security Group Tags (SGT) provided by ISE/ISE-PIC.

Step 7 Create an identity policy.

An identity policy is a container for one or more identity rules. See Create an identity policy.

a) Create an identity rule.

An identity rule specifies how a realm is used to control access to the network by users and groups. See Create an identity rule.

Step 8 Associate the identity policy with an access control policy.

This enables the access control policy to use users and groups in the realm.

a) Create an access control rule.

The access control rule specifies an action to take (for example, allow or block) if traffic matches the rule criteria. You can use source and destination SGT metadata as matching criteria in the access control rule. See Access control rules.

Step 9 Deploy the access control policy to managed devices.

Before your policy can take effect, it must be deployed to managed devices. See Deploy configuration changes.

What to do next

Export certificates from the ISE/ISE-PIC server for use in the Cloud-Delivered Firewall Management Center, on page 12

ISE/ISE-PIC configuration

This section explains how to configure the ISE/ISE-PIC server for use with identity policies in the Cloud-Delivered Firewall Management Center, including:

- export certificates from the ISE/ISE-PIC server to authenticate with the Cloud-Delivered Firewall Management Center
- publish SXP topics so the Cloud-Delivered Firewall Management Center can be updated with Security Group Tags (SGT) on the ISE server.

Configure security groups and SXP publishing in ISE

This task enables static SGT-to-IP address mappings for Secure Firewall Threat Defense devices, allowing TrustSec policies and access control based on source and destination security group tags (SGT).

There is a lot of configuration that you must do in Cisco Identity Services Engine (ISE) to create the TrustSec policy and security group tags (SGT). Please look at the ISE documentation for more complete information on implementing TrustSec.

The following procedure picks out the highlights of the core settings you must configure in ISE for the Firewall Threat Defense device to be able to download and apply static SGT-to-IP address mappings, which can then be used for source and destination SGT matching in access control rules. See the ISE documentation for detailed information.

The figures in this procedure are based on ISE 2.4. The exact paths to these features might change in subsequent releases, but the concepts and requirements will be the same. Although ISE 2.4 or later is recommended, and preferably 2.6 or later, the configuration should work starting with ISE 2.2 patch 1.

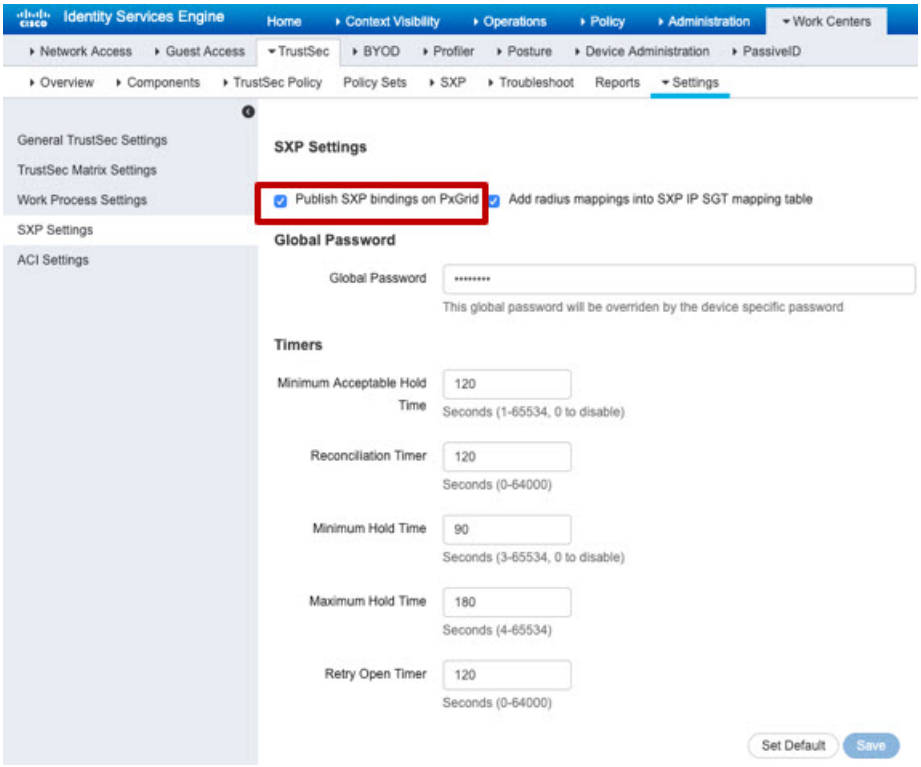
Before you begin

You must have the ISE Plus license to publish SGT-to-IP address static mappings and to get user session-to-SGT mappings so that the Firewall Threat Defense device can receive them.

Procedure

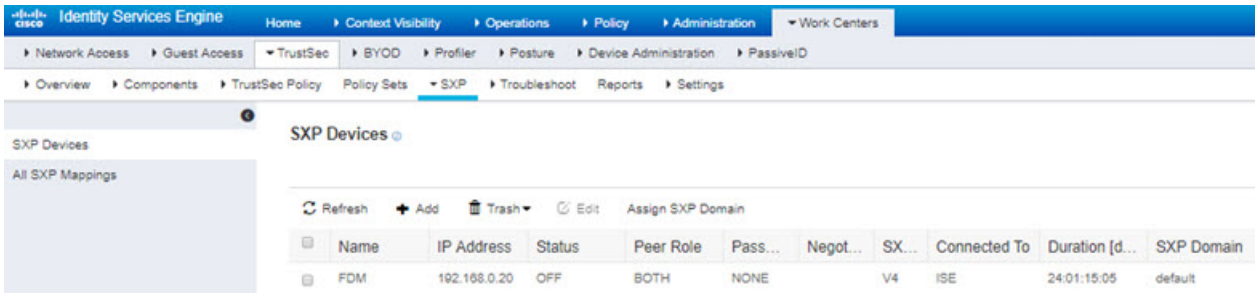
Step 1 Choose **Work Centers** > **TrustSec** > **Settings** > **SXP Settings**, and select the **Publish SXP Bindings on PxGrid** option.

This option makes ISE send the SGT mappings out using SXP. You must select this option for the Firewall Threat Defense device to "hear" anything by subscribing or publishing to the SXP topic. This option must be selected for the Firewall Threat Defense device to get static SGT-to-IP address mapping information. It is not necessary if you simply want to use SGT tags defined in the packets, or SGTs that are assigned to a user session.

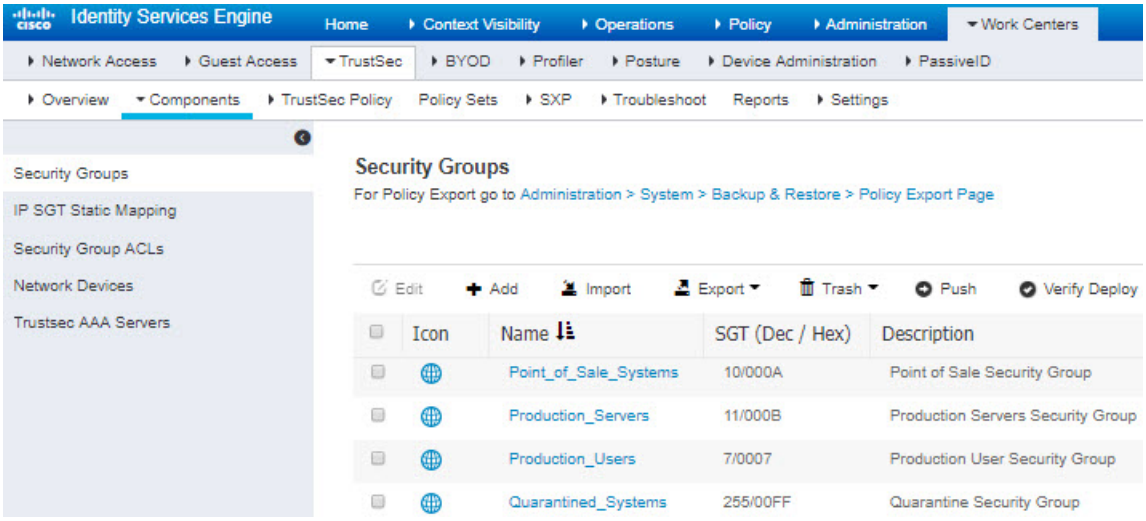


Step 2 Choose **Work Centers** > **TrustSec** > **SXP** > **SXP Devices**, and add a device.

This does not have to be a real device, you can even use the management IP address of the Firewall Threat Defense device. The table simply needs at least one device to induce ISE to publish the static SGT-to-IP address mappings. This step is not necessary if you simply want to use SGT tags defined in the packets, or SGTs that are assigned to a user session.

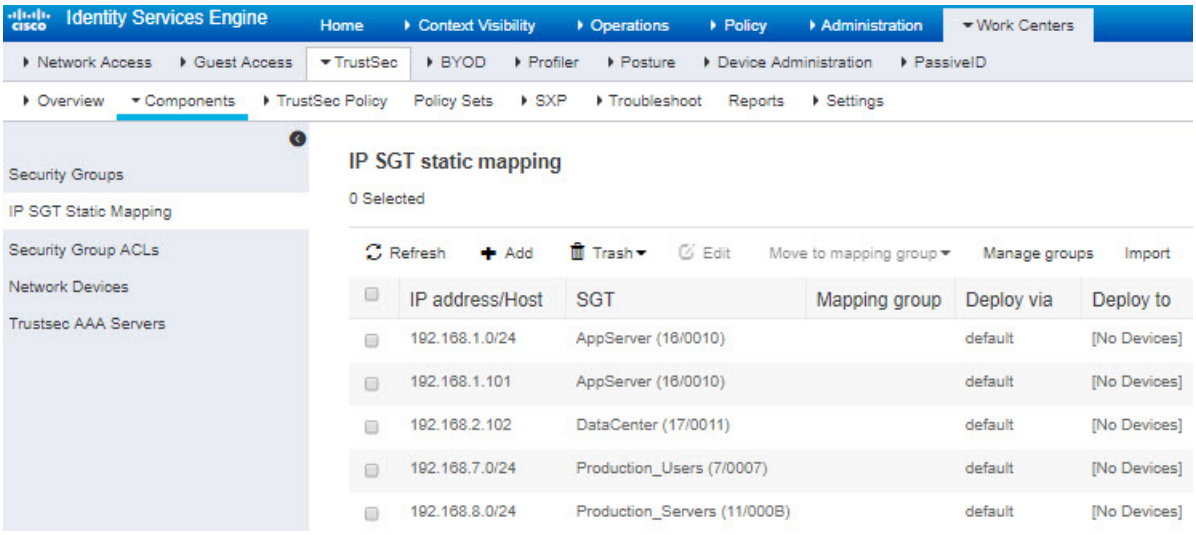


Step 3 Choose **Work Centers** > **TrustSec** > **Components** > **Security Groups** and verify there are security group tags defined. Create new ones as necessary.



Step 4 Choose **Work Centers** > **TrustSec** > **Components** > **IP SGT Static Mapping** and map host and network IP addresses to the security group tags.

This step is not necessary if you simply want to use SGT tags defined in the packets, or SGTs that are assigned to a user session.



You have configured ISE with the necessary security groups, SXP publishing settings, and static SGT-to-IP mappings required for Secure Firewall Threat Defense devices to receive and apply TrustSec policies.

Export certificates from the ISE/ISE-PIC server for use in the Cloud-Delivered Firewall Management Center

Certificate exported from Identity Services Engine (ISE) / Identity Services Engine - Passive Identity Connector (ISE-PIC) servers enables secure authentication between the Cloud-Delivered Firewall Management Center and ISE systems.

You might need to export one, or as many as three, certificates, depending on how your ISE system is set up:

- One certificate for the pxGrid server
- One certificate for the monitoring (MNT) server
- One certificate, including the private key, for the pxGrid client (that is, the Cloud-Delivered Firewall Management Center)

  Unlike the first two certificates, this is a self-signed certificate.

These certificates are then imported into the Cloud-Delivered Firewall Management Center:

- pxGrid client certificate: internal certificate with key (**Objects** > **PKI** > **Internal Certs**)
- pxGrid server certificate: trusted CA (**Objects** > **PKI** > **Trusted CAs**)
- MNT certificate: trusted CA

Export a system certificate

Export a system certificate or a certificate with its associated private key for backup or transfer to another system.

You can export a system certificate or a certificate and its associated private key. If you export a certificate and its private key for backup purposes, you can reimport them later if needed.

Before you begin

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

Procedure

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **System Certificates**.

Step 2 Check the check box next to the certificate that you want to export and click **Export**.

Step 3 Choose whether to export only the certificate, or the certificate and its associated private key.

Tip We do not recommend exporting the private key that is associated with a certificate because its value may be exposed. If you must export a private key (for example, when you export a wildcard system certificate to be imported into the other Cisco ISE nodes for inter-node communication), specify an encryption password for the private key. You must specify this password while importing this certificate into another Cisco ISE node to decrypt the private key.

Step 4 Enter the password if you have chosen to export the private key. The password should be at least eight characters long.

Step 5 Click **Export** to save the certificate to the file system that is running your client browser.

If you export only the certificate, the certificate is stored in the PEM format. If you export both the certificate and private key, the certificate is exported as a .zip file that contains the certificate in the PEM format and the encrypted private key file.

Generate a self-signed certificate

Generate a self-signed certificate to add a new local certificate for internal testing and evaluation purposes in Cisco ISE.

Add a new local certificate by generating a self-signed certificate. Cisco recommends that you only employ self-signed certificates for your internal testing and evaluation needs. If you plan to deploy Cisco ISE in a production environment, use CA-signed certificates whenever possible to ensure more uniform acceptance around a production network.

Note If you use a self-signed certificate and you want to change the hostname of your Cisco ISE node, log in to the administration portal of the Cisco ISE node, delete the self-signed certificate that has the old hostname, and generate a new self-signed certificate. Otherwise, Cisco ISE continues to use the self-signed certificate with the old hostname.

Before you begin

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

Follow these steps to generate a self-signed certificate:

Procedure

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **System Certificates**.

To generate a self-signed certificate from a secondary node, choose **Administration** > **System** > **Server Certificate**.

Step 2 In the ISE-PIC GUI, click the **Menu** icon (☰) and choose **Certificates** > **System Certificates**.

Step 3 Click **Generate Self Signed Certificate** and enter the details in the window displayed.

Step 4 Check the check boxes in the **Usage** area based on the service for which you want to use this certificate.

Step 5 Click **Submit** to generate the certificate.

To restart the secondary nodes, from the CLI, enter these commands in this order:

a) **application stop ISE**
b) **application start ISE**

Import ISE/ISE-PIC certificates

Import certificates and keys from your ISE or ISE-PIC server to the firewall to enable secure pxGrid and MNT integration for cloud-delivered firewall management.

This procedure is optional.

- pxGrid client certificate: internal certificate with key (**Objects** > **PKI** > **Internal Certs**)
- pxGrid server certificate: trusted CA (**Objects** > **PKI** > **Trusted CAs**)
- MNT certificate: trusted CA

Before you begin

Export certificates from the ISE/ISE-PIC server as discussed in Export a system certificate, on page 12. The certificates and key must be present on the machine from which you log in to the Cloud-Delivered Firewall Management Center.

Procedure

Step 1 Log in to the Cloud-Delivered Firewall Management Center if you have not already done so.

Step 2 Click **Objects** > **PKI** > **Internal Certs**.

Step 3 Click **Add Internal Cert**.

Step 4 Follow the prompts on your screen to import the certificate and private key.

Step 5 Click **Trusted CAs**.

Step 6 Click **Add Trusted CA**.

Step 7 Follow the prompts on your screen to import the pxGrid server certificate.

Step 8 Repeat the preceding steps, if necessary, to import the MNT server's trusted CA.

Configure ISE for user control

Configure ISE/ISE-PIC identity source to enable user session retrieval from Microsoft Active Directory or LDAP servers for identity-based access control.

The following procedure discusses how to configure the ISE/ISE-PIC identity source. You must be in the global domain to perform this task.

Firewall Threat Defense Feature History:

7.2—Optionally add a proxy, which is a connection to one or more Security Cloud Control in the event Security Cloud Control cannot communicate with the ISE/ISE-PIC server. .

Before you begin

- To get user sessions from a Microsoft Active Directory Server or supported LDAP server, configure and enable a realm for the Cisco ISE server, assuming the pxGrid persona, as discussed in Create an LDAP realm or an Active Directory realm and realm directory.
- To get all mappings that are defined in Cisco ISE, including SGT-to-IP address mappings published through SXP, use the procedure that follows. As an alternative, you have the following options:
  - To use the SGT information in the packets only, and not use mappings downloaded from Cisco ISE, skip the steps discussed in Create and edit access control rules. Note that in this case, you can use SGT tags as a source condition only; these tags will never match destination criteria.
  - To use SGT in packets and user-to-IP-address/SGT mappings only, do not subscribe to the SXP topic in the Cisco ISE identity source, and do not configure ISE to publish SXP mappings. You can use this information for both source and destination matching conditions.
- (Advanced configuration only.) Export certificates from the ISE/ISE-PIC server and optionally import them into the Cloud-Delivered Firewall Management Center as discussed in Export certificates from the ISE/ISE-PIC server for use in the Cloud-Delivered Firewall Management Center, on page 12.
- To publish SXP topics so the Cloud-Delivered Firewall Management Center can be updated with Security Group Tags (SGT) on the ISE server, see ISE/ISE-PIC configuration, on page 9.

Procedure

Step 1 Log in to the Firewall Management Center.

Step 2 Click **Integrations** > **Identity** > **Identity Sources**.

Step 3 Click **Identity Services Engine** for the **Service Type** to enable the ISE connection.

Note To disable the connection, click **None**.

Step 4 Enter a **Primary Host Name/IP Address** and, optionally, a **Secondary Host Name/IP Address**.

Step 5 Click the appropriate certificate authorities from the **pxGrid Server CA** and **MNT Server CA** lists, and the appropriate certificate from the **pxGrid Client Certificate** list. You can also click **Add** (+) to add a certificate.

Note The **pxGrid Client Certificate** must include the **clientAuth** extended key usage value, or it must not include any extended key usage values.

Step 6 (Optional.) Enter an **ISE Network Filter** using CIDR block notation.

Step 7 In the Subscribe To section, check the following:

- **Session Directory Topic** to receive ISE user session information from the ISE server.
- **SXP Topic** to receive updates to SGT-to-IP mappings when available from the ISE server. This option is required to use destination SGT tagging in access control rules.

Step 8 (Optional.) From the **Proxy** list, click either a managed device or a proxy sequence.
If Security Cloud Control cannot communicate with your ISE/ISE-PIC server, you can choose either a managed device or proxy sequence to do it. For example, your Security Cloud Control might be in a public cloud but the ISE/ISE-PIC server might be on an internal intranet.

Step 9 To test the connection, click **Test**.

If the test fails, click **Additional Logs** for more information about the connection failure.

Note If you set up load balancing with ISE, the node that responds to the test should be the currently active node. For more information, see Cisco pxGrid Node.

What to do next

- Specify users to control and other options using an identity policy as described in Create an identity policy.
- Associate the identity policy with an access control policy, which filters and optionally inspects traffic, as discussed in Associate prefilter, decryption, and identity policies with an access control.
- Use Security Group Tags (SGT) from Cisco ISE as dynamic attributes in access control policies.
- Deploy your identity and access control policies to managed devices as discussed in Deploy configuration changes.
- Monitor user activity .

ISE/ISE-PIC configuration fields

The fields in this reference are used to configure a connection to ISE/ISE-PIC.

Connection and certificate configuration fields for ISE/ISE-PIC integration:

- **Primary and Secondary Host Name/IP Address**: The hostname or IP address for the primary and, optionally, the secondary pxGrid ISE servers. The ports used by the host names you specify must be reachable by both ISE and the Cloud-Delivered Firewall Management Center.
- **pxGrid Server CA**: The trusted certificate authority for the pxGrid framework. If your deployment includes a primary and a secondary pxGrid node, the certificates for both nodes must be signed by the same certificate authority.
- **MNT Server CA**: The trusted certificate authority for the ISE certificate when performing bulk downloads. If your deployment includes a primary and a secondary MNT node, the certificates for both nodes must be signed by the same certificate authority.
- pxGrid Client Certificate: The internal certificate and key that the Cloud-Delivered Firewall Management Center must provide to connect to ISE/ISE-PIC or to perform bulk downloads.

Note The **pxGrid Client Certificate** must include the clientAuth extended key usage value, or it must not include any extended key usage values.

Data filtering, subscription, and proxy configuration fields:

- **ISE Network Filter**: An optional filter you can set to restrict the data that ISE reports to the Cloud-Delivered Firewall Management Center. If you provide a network filter, ISE reports data from the networks within that filter. You can specify a filter in these ways:
  - Leave the field blank to specify **`any`**.
  - Enter a single IPv4 address block using CIDR notation.
  - Enter a list of IPv4 address blocks using CIDR notation, separated by commas.
- **Subscribe to**: **Session Directory Topic**: Check this box to subscribe to user session information from the ISE server. Includes SGT and endpoint metadata. **SXP Topic**: Check this box to subscribe to SXP mappings from the ISE server.
- **Proxy**: You can optionally choose either a managed device or a proxy sequence to communicate with ISE/ISE-PIC if Security Cloud Control is unable to do so. For example, your Security Cloud Control might be in a public cloud but the ISE/ISE-PIC server might be on an internal intranet.

Note This version of the system does not support filtering using IPv6 addresses, regardless of your ISE version.

Troubleshoot Cisco ISE/ISE-PIC or Cisco TrustSec issues

This reference helps you troubleshoot issues with Cisco TrustSec, ISE, or ISE-PIC integration to ensure Security Group Tag propagation, user mapping, and certificate requirements are correctly configured for Cloud-Delivered Firewall Management Center deployment.

Troubleshoot Cisco TrustSec issues

A device interface can be configured to propagate Security Group Tags (SGTs) either from ISE/ISE-PIC or from a Cisco device on the network (referred to as Cisco TrustSec.) On the device management page (**Devices** > **Device Management**), the **Propagate Security Group Tag** check box for an interface is checked after a device reboot. If you do not want the interface to propagate TrustSec data, uncheck the box.

Troubleshoot ISE/ISE-PIC issues

For other related troubleshooting information, see Troubleshoot realms and user downloads and Troubleshoot user control.

If you experience issues with the ISE or ISE-PIC connection, check these items:

- The pxGrid Identity Mapping feature in ISE must be enabled before you can successfully integrate ISE with the system.
- When the primary server fails, you must manually promote the secondary to primary; there is no automatic failover.
- Before a connection between the ISE server and the Cloud-Delivered Firewall Management Center succeeds, you must manually approve the clients in ISE. (Typically, there are two clients: one for the connection test and another for ISE agent.)

  You can also enable **Automatically approve new accounts** in ISE as discussed in the chapter on Managing users and external identity sources in the Identity Services Engine administrator guides.
- The **pxGrid Client Certificate** must include the **clientAuth** extended key usage value, or it must not include any extended key usage values.
- The time on your ISE server must be synchronized with the time on the Cloud-Delivered Firewall Management Center. If the appliances are not synchronized, the system may perform user timeouts at unexpected intervals.
- If your deployment includes a primary and a secondary pxGrid node,
  - The certificates for both nodes must be signed by the same certificate authority.
  - The ports used by the host name must be reachable by both the ISE server and by the Cloud-Delivered Firewall Management Center.
- If your deployment includes a primary and a secondary MNT node, the certificates for both nodes must be signed by the same certificate authority.

To exclude subnets from receiving user-to-IP and Security Group Tag (SGT)-to-IP mappings from ISE, use the **configure identity-subnet-filter** {**add** | **remove**} command. You should typically do this for lower-memory managed devices to prevent Snort identity health monitor memory errors.

If you experience issues with user data reported by ISE or ISE-PIC, note these items:

- After the system detects activity from an ISE user whose data is not yet in the database, the system retrieves information about them from the server. Activity seen by the ISE user is *not* handled by access control rules, and is *not* displayed in the web interface until the system successfully retrieves information about them in a user download.
- You cannot perform user control on ISE users who were authenticated by an LDAP, RADIUS, or RSA domain controller.
- The Cloud-Delivered Firewall Management Center does not receive user data for ISE Guest Services users.
- If ISE monitors the same users as TS Agent, the Cloud-Delivered Firewall Management Center prioritizes the TS Agent data. If the TS Agent and ISE report identical activity from the same IP address, only the TS Agent data is logged to the Cloud-Delivered Firewall Management Center.
- Your ISE version and configuration impact how you can use ISE in the system. For more information, see The ISE/ISE-PIC identity source, on page 1.
- If you have Cloud-Delivered Firewall Management Center high availability configured and the primary fails, see the section on ISE and high availability in Best practices for ISE/ISE-PIC integration, on page 4.
- ISE-PIC does not provide ISE attribute data.
- ISE-PIC cannot perform ISE ANC remediations.
- Active FTP sessions are displayed as the **Unknown** user in events. This is normal because, in active FTP, the server (not the client) initiates the connection and the FTP server should not have an associated user name. For more information about active FTP, refer to RFC 959.

If you experience issues with supported functionality, see The ISE/ISE-PIC identity source, on page 1 for more information about version compatibility.

ISE/ISE-PIC user timeout

If you're setting up ISE/ISE-PIC without a realm, be aware there is a user session timeout that affects how users are seen by the Cloud-Delivered Firewall Management Center.

History for ISE/ISE-PIC

This reference provides the historical development of ISE and ISE-PIC integration features across different software versions.

Feature	Minimum Cloud-Delivered Firewall Management Center	Minimum Firewall Threat Defense	Details
Proxy	Any	7.2.0	One or more managed devices that can communicate with Security Cloud Control in the event Security Cloud Control cannot communicate with the ISE/ISE-PIC server. **New/updated screen**: **Integration** > **Other Integrations** > **Realms** > **Proxy Sequence**
pxGrid 2.0 is the default for supported ISE/ISE-PIC versions	Any	6.7.0	Note: • Supported ISE/ISE-PIC versions: 2.6 patch 6 or later, 2.7 patch 2 or later • Adaptive Network Control (ANC) policies replace Endpoint Protection Service (EPS) remediations. If you have EPS policies configured in the Cloud-Delivered Firewall Management Center, you must migrate them to use ANC.
Optionally exclude subnets from receiving user-to-IP and Security Group Tag (SGT)-to-IP mappings from ISE. You should typically do this for lower-memory managed devices to prevent Snort identity health monitor memory errors.	Any	6.7.0	New command: **configure identity-subnet-filter** {**add** | **remove**}
Destination Security Group Tag matching (SGT)	Any	6.5.0	Feature introduced. Enables you to use ISE SGT tags for both source and destination matching criteria in access control rules. SGT tags are tag-to-host/network mappings obtained by ISE. New/modified screens: • New options to configure Destination SGT matching: **System** > **Integration** > **Identity Sources** > **ISE/ISE-PIC** • **Session Directory Topic**: Subscribe to ISE user session information. • **SXP Topic**: Subscribe to SGT tag updates on the ISE server. • New and renamed columns in **Analysis** > **Connections** > **Events** • Renamed: Security Groups Tags renamed to Source SGT • New: Destination SGT
Integration with ISE-PIC	Any	6.2.1	You can now use data from ISE-PIC.

Feature	Minimum Cloud-Delivered Firewall Management Center	Minimum Firewall Threat Defense	Details
SGT tags for user control.	Any	6.2.0	You no longer need to create a realm or identity policy to perform user control based on ISE Security Group Tag (SGT) data.
Integration with ISE.	Any	6.0	Feature introduced. By subscribing to Cisco's Platform Exchange Grid (PxGrid), the Firepower Management Center can download additional user data, device type data, device location data, and Security Group Tags (SGTs) —a method used by ISE to provide network access control).