Control Users with 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 2
- Requirements and Prerequisites for ISE/ISE-PIC, on page 2
- ISE/ISE-PIC Guidelines and Limitations, on page 2
- How to Configure ISE/ISE-PIC for User Control, on page 4
- Configure ISE/ISE-PIC, on page 6
- Configure ISE/ISE-PIC for User Control, on page 8
- Troubleshoot the ISE/ISE-PIC or Cisco TrustSec Issues, on page 10
- History for ISE/ISE-PIC, on page 12

The ISE/ISE-PIC Identity Source

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

ISE/ISE-PIC is an authoritative identity source, and provides user awareness data for users who authenticate using Active Directory (AD), LDAP, RADIUS, or RSA. Additionally, you can perform user control on Active Directory users. ISE/ISE-PIC does not report failed login attempts or the activity of ISE Guest Services users.

Note The Firepower 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 FMC that can be used in policy.

For more information on Cisco ISE/ISE-PIC, see the *Cisco Identity Services Engine Administrator Guide* and the *Identity Services Engine Passive Identity Connector (ISE-PIC) Installation and Administrator Guide*.

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.

License Requirements for ISE/ISE-PIC

FTD License

Any

Classic License

Control

Requirements and Prerequisites for ISE/ISE-PIC

Model Support

Any except NGIPSv.

Supported Domains

Any

User Roles

- Admin
- Access Admin
- Network Admin

ISE/ISE-PIC Guidelines and Limitations

Use the guidelines discussed in this section when configuring ISE/ISE-PIC with the Firepower System.

ISE/ISE-PIC Version and Configuration Compatibility

Your ISE/ISE-PIC version and configuration affects its integration and interaction with Firepower, as follows:

- We strongly recommend you 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 Firepower Management Center. Otherwise, the system might perform user timeouts at unexpected intervals.
- To implement user control using ISE or ISE-PIC data, configure and enable a realm for the ISE server assuming the pxGrid persona as described in Create a Realm.
- Each Firepower Management Center host name that connects to an ISE server must be unique; otherwise, the connection to one of the Firepower Management Centers will be dropped.

- If ISE Endpoint Protection Service (EPS) is enabled and configured in your ISE deployment, you can use your ISE connection to run ISE EPS remediations on the source or destination host involved in a correlation policy violation.
- If you configured your ISE deployment to update a user's SGT after the user's EPSStatus changes, your ISE EPS remediations also update the SGT on the Firepower Management Center.
- ISE-PIC does not provide ISE attribute data or support ISE EPS remediations.

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

IPv6 support

Version 2.0 (patch 4) and later of ISE/ISE-PIC includes support for IPv6-enabled endpoints.

Approve clients in ISE

Before a connection between the ISE server and the Firepower 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 *Cisco Identity Services Engine Administrator Guide*.

Security Group Tags (SGT)

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.

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. For more information, see Configuring ISE Attribute Conditions.

Note 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; see Custom SGT Conditions.

ISE and High Availability

When the primary Firepower Management Center fails, the following occur:

- Until the standby is promoted to primary, the user database on the secondary Firepower Management Center is read-only.

  Users added to the repository (for example, Active Directory) are not downloaded to the Firepower Management Center and those users are identified as Unknown.

  New SGTs are not used.

- After the standby is promoted to primary, all operations return to normal; that is, users are downloaded, new SGTs are used, and users are identified if possible.

When the ISE primary server fails, you must manually promote the secondary to primary; there is no automatic failover.

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 Firepower Management Center database with ISE attribute data. You can use the following 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)**.

How to Configure ISE/ISE-PIC for User Control

You can use ISE/ISE-PIC in any of the following 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.

Related Topics

How to Configure ISE Without a Realm, on page 4
How to Configure ISE/ISE-PIC for User Control Using a Realm, on page 5

How to Configure ISE Without a Realm

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

	Command or Action	Purpose
Step 1	Export system certificates from ISE/ISE-PIC.	The certificates are required to connect securely between the ISE/ISE-PIC pxGrid, monitoring (MNT) servers and

	Command or Action	Purpose
		the FMC. See Export Certificates from the ISE/ISE-PIC Server for Use in the FMC, on page 6
Step 2	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. See Configure ISE/ISE-PIC for User Control, on page 8.
Step 3	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 SGT metadata as matching criteria in the access control rule. See Introduction to Access Control Rules.
Step 4	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 FMC, on page 6

How to Configure ISE/ISE-PIC for User Control Using a Realm

Before you begin

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. Users and groups can be stored in any server listed in Supported Servers for Realms.

Procedure

	Command or Action	Purpose
Step 1	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 FMC. See Export Certificates from the ISE/ISE-PIC Server for Use in the FMC, on page 6
Step 2	Create a realm.	You must create a realm only to control access to the network by the users and groups you choose. See Create a Realm.
Step 3	Download users and groups, and enable the realm.	Downloading users and groups enables you to use them in access control rules. See See Download Users and Groups.
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. See Configure ISE/ISE-PIC for User Control, on page 8.

	Command or Action	Purpose
Step 5	Create an identity policy.	An identity policy is a container for one or more identity rules. See Create an Identity Policy.
Step 6	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 7	Associate the identity policy with an access control policy.	This enables the access control policy to use users and groups in the realm.
Step 8	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 SGT metadata as matching criteria in the access control rule. See Introduction to 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 FMC, on page 6

Configure ISE/ISE-PIC

The following topics discuss how to configure the ISE/ISE-PIC server for use with identity policies in the FMC.

You must export certificates from the ISE/ISE-PIC server to authenticate with the FMC.

Related Topics

Export Certificates from the ISE/ISE-PIC Server for Use in the FMC, on page 6

Export Certificates from the ISE/ISE-PIC Server for Use in the FMC

The following sections discuss how to:

- Export system certificates from the ISE/ISE-PIC server.

  These certificates are required to securely connect to the ISE/ISE-PIC server. 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 FMC

- Import these certificates into the FMC.

Related Topics

Export a System Certificate, on page 7
Import ISE/ISE-PIC Certificates, on page 7

Export a System Certificate

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.

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.

Import ISE/ISE-PIC Certificates

This procedure is optional. You can also import ISE server certificates when you create the ISE/ISE-PIC identity source as discussed in Configure ISE/ISE-PIC for User Control, on page 8.

Before you begin

Export certificates from the ISE/ISE-PIC server as discussed in Export a System Certificate, on page 7. The certificates and key must be present on the machine from which you log in to the FMC.

You import two types of certificate objects:

- An internal certificate and private key for the FMC to authenticate with ISE/ISE-PIC.
- One or more trusted certificates authorities (CAs) for pxGrid and your ISE monitoring (MNT) server.

  Depending on how you set up your ISE/ISE-PIC system, this could be two separate certificates or one certificate.

Step 1 Log in to the FMC if you have not already done so.
Step 2 Click **Objects** > **Object Management**.
Step 3 Expand **PKI**.
Step 4 Click **Internal Certs**.
Step 5 Click **Add Internal Cert**.
Step 6 Follow the prompts on your screen to import the certificate and private key.
Step 7 Click **Trusted CAs**.
Step 8 Click **Add Trusted CA**.
Step 9 Follow the prompts on your screen to import the pxGrid server certificate.
Step 10 Repeat the preceding steps, if necessary, to import the MNT server's trusted CA.

What to do next

Configure ISE/ISE-PIC for User Control, on page 8

Configure ISE/ISE-PIC for User 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.

Before you begin

- To get user sessions from a Microsoft Active Directory Server or supported LDAP server, configure and enable a realm for the ISE server, assuming the pxGrid persona, as discussed in Create a Realm.
- Configure a connection to ISE or ISE-PIC. For more information, see The ISE/ISE-PIC Identity Source, on page 1 and ISE/ISE-PIC Configuration Fields, on page 9.

Step 1 Log in to the Firepower Management Center.
Step 2 Click **System** > **Integration**.
Step 3 Click **Identity Sources**.
Step 4 Click **Identity Services Engine** for the **Service Type** to enable the ISE connection.

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

Step 5 Enter a **Primary Host Name/IP Address** and, optionally, a **Secondary Host Name/IP Address**.
Step 6 Click the appropriate certificate authorities from the **pxGrid Server CA** and **MNT Server CA** lists, and the appropriate certificate from the **FMC Server Certificate** list. You can also click **Add** ( ) to add a certificate.

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

Step 7 (Optional.) Enter an **ISE Network Filter** using CIDR block notation.

Step 8 To test the connection, click **Test**.

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

Note When you run two ISE pxGrid 1.0 nodes, it is normal for one host to show Success and one to show Failure. Because pxGrid 1.0 only runs actively on one ISE node at a time, the likelihood of success depends on which node in ISE is the active 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 rule with an access control policy, which filters and optionally inspects traffic, as discussed in Associating Other Policies with Access Control.
- Deploy your identity and access control policies to managed devices as discussed in Deploy Configuration Changes.
- Monitor user activity as discussed in Using Workflows.

Related Topics

Troubleshoot the ISE/ISE-PIC or Cisco TrustSec Issues, on page 10
Trusted Certificate Authority Objects
Internal Certificate Objects

ISE/ISE-PIC Configuration Fields

The following fields are used to configure a connection to ISE/ISE-PIC.

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 Firepower Management Center.

pxGrid Server CA

The 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 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.

FMC Server Certificate

The certificate and key that the Firepower Management Center must provide to ISE/ISE-PIC to connect to ISE/ISE-PIC or to perform bulk downloads.

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

ISE Network Filter

An optional filter you can set to restrict the data that ISE reports to the Firepower Management Center. If you provide a network filter, ISE reports data from the networks within that filter. You can specify a filter in the following 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.

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

Related Topics

Trusted Certificate Authority Objects
Internal Certificate Objects

Troubleshoot the ISE/ISE-PIC or Cisco TrustSec Issues

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.

FMC health monitor issue

The ISE/ISE-PIC Connection Status Monitor (health monitor) displays `check connectivity error` if ISE/ISE-PIC uses pxgrid v1 even though there is nothing wrong with the connection.

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 the following:

- The pxGrid Identity Mapping feature in ISE must be enabled before you can successfully integrate ISE with the Firepower 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 Firepower 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 *Cisco Identity Services Engine Administrator Guide*.

- The **FMC Server 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 Firepower 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 Firepower 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 the following:

- 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 Firepower Management Center does not receive user data for ISE Guest Services users.

- If ISE monitors the same users as TS Agent, the Firepower 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 Firepower Management Center.

- Your ISE version and configuration impact how you can use ISE in the Firepower System. For more information, see The ISE/ISE-PIC Identity Source, on page 1.

- If you have Firepower Management Center high availability configured and the primary fails, see the section on ISE and High Availability in ISE/ISE-PIC Guidelines and Limitations, on page 2.

- ISE-PIC does not provide ISE attribute data.

- ISE-PIC cannot perform ISE EPS 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, see 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.

Troubleshoot 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 Firepower Management Center. For more information, see Realm Fields.

History for ISE/ISE-PIC

Feature	Version	Details
Integration with ISE-PIC	6.2.1	You can now use data from ISE-PIC.
SGT tags for user control.	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.	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).