Integrate the Cisco Identity Services Engine (ISE) / ISE Passive Identity Controller (ISE-PIC)

This topic contains the following sections:

Overview of the Identity Services Engine (ISE) / ISE Passive Identity Controller (ISE-PIC) Service

Cisco's Identity Services Engine (ISE), and Passive Identity Connector (ISE-PIC) are applications that run on separate servers in your network to provide enhanced identity management. The Web Security Appliance can access user-identity information from an ISE or ISE-PIC server. When either ISE, or ISE-PIC is configured, information is retrieved (user names and associated Secure Group Tags from ISE, user names and Active Directory groups from ISE-PIC) for appropriately configured Identification Profiles, to allow transparent user identification in policies configured to use those profiles.

- You can construct access policies using Secure Group Tags and Active Directory groups.
- For users that fail transparent identification with ISE/ISE-PIC, you can configure fallback authentication with Active Directory based realms. See Fallback Authentication, on page 4.
- You can configure authentication of users in Virtual Desktop Environments (Citrix, Microsoft shared/remote desktop services etc.). See VDI (Virtual Desktop Infrastructure) User Authentication in ISE/ISE-PIC Integrations, on page 12.

Note

- The ISE/ISE-PIC service is not available in Connector mode.
- ISE/ISE-PIC version 2.4, and PxGrid version 2.0 are supported.
- The ISE configuration page in the Web Security Appliance 's web interface is used to configure ISE or ISE-PIC servers, upload certificates, and to connect to either ISE or ISE-PIC services. The steps to configure ISE or ISE-PIC are similar and the any details specific for ISE-PIC configurations have been mentioned where applicable.

For more information on Secure Web Appliance ISE version support matrix, see ISE Compatibility Matrix Information.

Table 1: Web Security Appliance -ISE Scale Support Matrix

Models	Session Scale Without AD Group Enabled	Session Scale With AD Group Enabled	
-	Maximum Supported Active Sessions	Maximum Supported Active Sessions	Maximum Supported End Points (AD group entries for each user, and end point in ISE database.)
S680*,S690,S695	200K	125K	400K
S380*,S390, S600V	150K	50K	150K
S190,S195,S300V	50K	50K	75K
S100V	50K	40K	50K

Related Topics

- About pxGrid, on page 2
- About the ISE/ISE-PIC Server Deployment and Failover, on page 3

About pxGrid

Cisco's Platform Exchange Grid (pxGrid) enables collaboration between components of the network infrastructure, including security-monitoring and network-detection systems, identity and access management platforms, and so on. These components can use pxGrid to exchange information via a publish/subscribe method.

There are essentially three pxGrid components: the pxGrid publisher, the pxGrid client, and the pxGrid controller.

- pxGrid publisher – Provides information for the pxGrid client(s).

- pxGrid client – Any system, such as the Web Security Appliance , that subscribes to published information; in this case, Security Group Tag (SGT), Active Directory groups, user-group, and profiling information.
- pxGrid controller – In this case, the ISE/ISE-PIC pxGrid node that controls the client registration/management and topic/subscription processes.

Trusted certificates are required for each component, and these must be installed on each host platform.

About the ISE/ISE-PIC Server Deployment and Failover

A single ISE/ISE-PIC node set-up is called a standalone deployment, and this single node runs the Administration, and Policy Service. To support failover and to improve performance, you must set up multiple ISE/ISE-PIC nodes in a distributed deployment. The minimum required distributed ISE/ISE-PIC configuration to support ISE/ISE-PIC failover on your Web Security Appliance is:

- Two pxGrid nodes
- Two Administration nodes
- One Policy Service node

This configuration is referred to in the *Cisco Identity Services Engine Hardware Installation Guide* as a 'Medium-Sized Network Deployment'. Refer to the network deployments section in that installation guide for additional information.

Related Topics

- ISE/ISE-PIC Certificates, on page 3
- Tasks for Integrating the ISE/ISE-PIC Service, on page 5
- Connect to the ISE/ISE-PIC Services, on page 7
- Troubleshooting Identity Services Engine Problems, on page 12

ISE/ISE-PIC Certificates

Note This section describes the certificates necessary for an ISE/ISE-PIC connection. Tasks for Integrating the ISE/ISE-PIC Service, on page 5 provides detailed information about these certificates. Certificate Management, provides general certificate-management information for AsyncOS.

A set of two certificates is required for mutual authentication and secure communication between the Web Security Appliance and each ISE/ISE-PIC server:

- **Web Appliance Client Certificate** – Used by the ISE/ISE-PIC server to authenticate the Web Security Appliance .
- **ISE pxGrid Certificate** – Used by the Web Security Appliance to authenticate an ISE/ISE-PIC server on port 5222 for Web Security Appliance -ISE/ISE-PIC data subscription (on-going publish/subscribe queries to the ISE/ISE-PIC server).

These two certificates can be Certificate Authority (CA)-signed or self-signed. AsyncOS provides the option to generate a self-signed Web Appliance Client Certificate, or a Certificate Signing Request (CSR) instead, if a CA-signed certificate is needed. Similarly, the ISE/ISE-PIC server provides the option to generate self-signed ISE/ISE-PIC pxGrid certificates, or CSRs instead if CA-signed certificates are needed.

Related Topics

- Using Self-signed Certificates, on page 4
- Using CA-signed Certificates, on page 4
- Overview of the Identity Services Engine (ISE) / ISE Passive Identity Controller (ISE-PIC) Service, on page 1
- Tasks for Integrating the ISE/ISE-PIC Service, on page 5
- Connect to the ISE/ISE-PIC Services, on page 7

Using Self-signed Certificates

When self-signed certificates are used on the ISE/ISE-PIC server, the ISE/ISE-PIC pxGrid certificate developed on the ISE/ISE-PIC server, as well as the Web Appliance Client Certificate developed on the Web Security Appliance must be added to the Trusted Certificates store on the ISE/ISE-PIC server (On **ISE** - Administration > Certificates > Trusted Certificates > Import; on **ISE-PIC** - Certificates > Trusted Certificates > Import).

Caution We do not recommend using self-signed certificates for authentication as it is not as secured as other authentication methods. Also, a self-signed certificate does not support revocation policy.

Using CA-signed Certificates

In the case of CA-signed certificates:

- On the ISE/ISE-PIC server, ensure the appropriate CA root certificate for the Web Appliance Client Certificate is present in the Trusted Certificates store (Administration > Certificates > Trusted Certificates).
- On the Web Security Appliance , ensure the appropriate CA root certificates are present in the Trusted Certificates list (Network > Certificate Management > Manage Trusted Root Certificates).
- On the Identity Services Engine page (Network > Identity Services Engine), be sure to upload the CA root certificate for the ISE/ISE-PIC pxGrid certificate.

Fallback Authentication

For user information not available in ISE/ISE-PIC, you can configure a fallback authentication. Ensure you have the following for successful fallback authentication.

- Identification profile configured with a fallback option of Active Directory based realm.
- Access policy with the correct Identification profile which contains the fallback option.

Tasks for Integrating the ISE/ISE-PIC Service

Note

- ISE/ISE-PIC version 2.4, and PxGrid version 2.0 are supported.
- To continue using existing access policies with ISE-PIC, you must edit the respective identification profiles to use ISE-PIC and identify users transparently. This applies to identification profiles using CDA. If you are migrating from CDA identification, to ISE-PIC based identification, you must edit the respective identification profiles.

Note

- Reconfigure the ISE on the Web Security Appliance , if you are upgrading from AsyncOS 11.5 or earlier versions to AsyncOS 11.7 or later versions.
- The certificate must be generated through the ISE/ISE-PIC device and the generated certificate must be uploaded to the Web Security Appliance .

Step	Task	Links to Topics and Procedures
1	Generate certificate through ISE/ISE-PIC device	Generating Certificate through ISE/ISE-PIC, on page 6
2	Configure the ISE/ISE-PIC for Web Security Appliance access.	Configuring ISE/ISE-PIC server for Web Security Appliance Access, on page 6
3	Configure and enable ISE/ISE-PIC Services in the Web Security Appliance .	Connect to the ISE/ISE-PIC Services, on page 7
4	If the Web Security Appliance Client Certificate is self-signed, import it to ISE/ISE-PIC.	Import the Self-signed Web Security Appliance Client Certificate to ISE/ISE-PIC Standalone Deployment, on page 9 Import the Self-signed Web Security Appliance Client Certificate to ISE/ISE-PIC Distributed Deployment, on page 9
5	If required, configure logging in the Web Security Appliance .	Configuring logging for ISE/ISE-PIC, on page 11
6	Acquire ISE/ISE-PIC ERS server details.	Acquiring ISE/ISE-PIC ERS Server Details from ISE/ISE-PIC, on page 11

Related Topics

- Overview of the Identity Services Engine (ISE) / ISE Passive Identity Controller (ISE-PIC) Service, on page 1
- ISE/ISE-PIC Certificates, on page 3
- Troubleshooting Identity Services Engine Problems, on page 12

Generating Certificate through ISE/ISE-PIC

Note The certificate that is generated through the ISE/ISE-PIC device must be in the PKCS12 format.

- **ISE/ISE-PIC:**

Step 1 Choose **Work Centres** > **PassiveID** > **Subscribers** > **Certificates**.

Step 2 Choose **PKCS 12 format** from the **Certificate Download Format** drop-down list. Enter other appropriate information on the **Certificates** tab and generate a pxGrid certificate.

Step 3 Extract Root CA, Web Appliance Client Certificate, and Web Appliance Client Key from the generated XXX.pk12 file using the `openssl` command:

- **Root CA:** openssl pkcs12 -in XXX.p12 -cacerts -nokeys -chain -out RootCA.pem
- **Web Appliance Client Certificate:** openssl pkcs12 -in XXX.p12 -clcerts -nokeys -out publicCert.pem
- **Web Appliance Client Key:** openssl pkcs12 -in XXX.p12 -nocerts -nodes -out privateKey.pem

Note Use the same certificate password that you have entered on the ISE web interface while performing step 2.

Note Follow the same steps to generate the secondary Root CA, Web Appliance Client Certificate, and Web Appliance Client Key through the secondary/failover ISE server.

Configuring ISE/ISE-PIC server for Web Security Appliance Access

- **ISE**
  - Each ISE server must be configured to allow identity topic subscribers (such as Web Security Appliance) to obtain session context in real-time.
    1. Choose **Administration** > **pxGrid Services** > **Settings** > **pxGrid Settings**.
    2. Ensure **Automatically approve new certificate-based accounts** is checked.

    Delete any old Web Security Appliance s configured that do not take part in any authentication with ISE/ISE-PIC.

    Ensure the ISE server footer is green, and says **Connected to pxGrid**.

- **ISE-PIC**
  - Each ISE-PIC server must be configured to allow identity topic subscribers (such as Web Security Appliance) to obtain session context in real-time.

    1. Choose **Subscribers** > **Settings**.
    2. Ensure **Automatically approve new certificate-based accounts** is checked.

    Delete any old Web Security Appliance s configured that do not take part in any authentication with ISE/ISE-PIC.

    Ensure the ISE server footer is green, and says **Connected to pxGrid**.

Refer to Cisco *Identity Services Engine* documentation for more information.

Connect to the ISE/ISE-PIC Services

Note If the ISE Admin, pxGrid, and MNT certificates are signed by your Root CA certificate, then upload the Root CA certificate itself to the ISE pxGrid Node Certificate fields on the appliance (**Network** > **Identity Services Engine**).

Before you begin

- Be sure each ISE/ISE-PIC server is configured appropriately for Web Security Appliance access; see Tasks for Integrating the ISE/ISE-PIC Service, on page 5.
- Obtain valid ISE/ISE-PIC-related certificates and keys. See Generating Certificate through ISE/ISE-PIC, on page 6for related information.
- Import the obtained RootCA.pem to the Web Security Appliance (**Network** > **CertificateManagement** > **TrustedRootCertificate** > **Client on ManageTrustedRootCertificate**). To extract Root CA, Web Appliance Client Certificate, and Web Appliance Client Key from the generated XXX.pk12 file, see Generating Certificate through ISE/ISE-PIC, on page 6.

Note Follow the same procedure for RootCA.pem extracted from secondary XXXX.pk12 file (if secondary/failover ISE Sever is available).

- The ISE configuration page in the Web Security Appliance 's web interface is used to configure ISE or ISE-PIC servers, upload certificates, and to connect to either ISE or ISE-PIC services. The steps to configure ISE or ISE-PIC are identical, and any details specific to ISE-PIC configurations have been mentioned where applicable.
- Enable ERS if you are building access policies using Active Directory groups provided by ISE/ISE-PIC.

Step 1 Choose **Network > Identification Service Engine**.

Step 2 Click **Edit Settings**.

If you are configuring ISE/ISE-PIC for the first time, click **Enable and Edit Settings**.

Step 3 Check **Enable ISE Service**.

Step 4 Identify the **Primary Admin Node** using its host name or IPv4 address and provide the following information on the **Primary ISE pxGrid Node Tab** on the Web Security Appliance .

a) Provide an **ISE pxGrid Node Certificate** for Web Security Appliance -ISE/ISE-PIC data subscription (on-going queries to the ISE/ISE-PIC server).

Browse to and select the certificate (or the certificate chain that includes any intermediate certificates) which is generated from the primary ISE server as Root CA (i.e. RootCA.pem); see ,Generating Certificate through ISE/ISE-PIC, on page 6 and then click **Upload File**. See Uploading a Certificate and Key for additional information.

Step 5 If you are using a second ISE/ISE-PIC server for failover, identify its **Primary Admin Node** using its host name or IPv4 address and provide the following information on the **Secondary ISE pxGrid Node** tab on the Web Security Appliance using its host name or IPv4 address.

a) Provide the secondary **ISE pxGrid Node Certificate**.

Browse to and select the certificate (or the certificate chain that includes any intermediate certificates) which is generated from the secondary ISE server as Root CA (i.e. **RootCA.pem**); see Generating Certificate through ISE/ISE-PIC, on page 6, and then click **Upload File** .See Uploading a Certificate and Key for additional information.

Note During failover from primary to secondary ISE servers, any user not in the existing ISE SGT cache will be required to authenticate, or will be assigned Guest authorization, depending on your Web Security Appliance configuration. After ISE failover is complete, normal ISE authentication resumes.

Step 6 Provide a **Web Appliance Client Certificate** for Web Security Appliance -ISE/ISE-PIC server mutual authentication:

- **Use Uploaded Certificate and Key**

For both the certificate and the key, click Choose and browse to the respective file.

Note Select and upload publicCert.pem and privateKey.pem generated through the ISE/ISE-PIC device. See Generating Certificate through ISE/ISE-PIC, on page 6.

If the **Key is Encrypted**, check this box.

Click **Upload Files**. (See Uploading a Certificate and Key for additional information about this option.)

Step 7 Enable the ISE External Restful Service (ERS).

- Enter the username and password of the ERS administrator. SeeAcquiring ISE/ISE-PIC ERS Server Details from ISE/ISE-PIC, on page 11.
- If ERS is available on the same ISE/ISE-PIC pxGrid nodes, check the **Server name same as ISE pxGrid Node** check box. Otherwise, enter the primary and secondary (if configured), servers' hostnames or IPv4 addresses.

Step 8 Click **Start Test** to test the connection with the ISE/ISE-PIC pxGrid node(s).

Step 9 Click **Submit**.

What to do next

- Classifying Users and Client Software

- Create Policies to Control Internet Requests

Related Information

- http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-implementation-design-guides-list.html , particularly “How To Integrate Cisco Web Security Appliance using ISE/ISE-PIC and TrustSec through pxGrid..”

Import the Self-signed Web Security Appliance Client Certificate to ISE/ISE-PIC Standalone Deployment

The basic steps are:

- **ISE Admin Node**
  - Choose **Administration** > **Certificates** > **Certificate Management** > **Trusted Certificates** > **Import**.

  Ensure that the following options are checked:
  - Trust for Authentication within ISE
  - Trust for client authentication and syslog
  - Trust for authentication of Cisco services
- **ISE-PIC Admin Node**
  - Choose **Certificates** > **Certificate Management** > **Trusted Certificates** > **Import**.

    Ensure that the following options are checked:
    - Trust for Authentication within ISE
    - Trust for client authentication and syslog
    - Trust for authentication of Cisco services

Refer to Cisco *Identity Services Engine* documentation for more information.

Import the Self-signed Web Security Appliance Client Certificate to ISE/ISE-PIC Distributed Deployment

The basic steps are:

- **ISE Admin Node:**
  - Choose **Administration** > **Certificates** > **Certificate Management** > **Trusted Certificates** > **Import**.

  Ensure that the following options are checked:
  - Trust for Authentication within ISE

- Trust for client authentication and syslog
- Trust for authentication of Cisco services

- **ISE-PIC Admin Node:**
  - Choose **Certificates** > **Certificate Management** > **Trusted Certificates** > **Import**.

    Ensure that the following options are checked:
    - Trust for Authentication within ISE
    - Trust for client authentication and syslog
    - Trust for authentication of Cisco services

Refer to Cisco *Identity Services Engine* documentation for more information.

Note In Distributed ISE Deployment, the Web Security Appliance communicates with MNT, PAN, and PxGrid nodes. In this case, the certificates or the issuer for all of the certificates, must be available in the 'Extracted Root certificate' i.e. in the RootCA which is generated through the ISE/ISE-PIC device. See Generating Certificate through ISE/ISE-PIC, on page 6.

Step 1 Follow the steps in the Generating Certificate through ISE/ISE-PIC, on page 6 to generate RootCA, Web Appliance Client Certificate, and Web Appliance Client Key.

Step 2 On **ISE/ISE-PIC Admin Node**, export the self-signed certificates manually through **ISE/ISE-PIC** > **Administration** > **System** > **Certificates** > **System Certificates**

a. Select a certificate which is having 'Used by' one of these:[pxGrid, EAP Authentication, Admin, Portal, RADIUS DTLS].

b. Click **Export** and save the generated .pem file.

Repeat the above steps for all ISE/ISE-PIC distributed nodes.

Step 3 Append the downloaded certificate-files in RootCA.pem manually using `openssl` commands. To generate and extract certificate-files in RootCA.pem through the ISE/ISE-PIC device, see Generating Certificate through ISE/ISE-PIC, on page 6.

a. Execute the following command on the downloaded certificate:

```
Example:

openssl x509 -in <DownloadCertificate>.pem -text | egrep "Subject:|Issuer:

Example (output):

Issuer: CN=isehcamnt2.node
Subject: CN=isehcamnt2.node
```

b. Modify the content as follows:

```
Example:
Subject=/CN=isehcamnt2.node
Issuer=/CN=isehcamnt2.node
```

c. Add the following line in the RootCA.pem:

```
Bag Attributes: <Empty Attributes>
```

d. Add Subject and Issuer from step (2) in RootCA.pem along with step (3).

```
Example:
Bag Attributes: <Empty Attributes>
Subject=/CN=isehcamnt2.node
Issuer=/CN=isehcamnt2.node
```

e. Copy the whole content of the downloaded certificate file and paste them at the end of the RootCA after step (4) data.

Repeat steps (1) to (5) for all Distributed ISE/ISE-PIC node downloaded certificates and save the modified RootCA certificate.

Step 4 Upload the modified RootCA.pem in the ISE configuration page of the Web Security Appliance . See Connect to the ISE/ISE-PIC Services, on page 7.

Configuring logging for ISE/ISE-PIC

- Add the custom field %m to the Access Logs to log the Authentication mechanism—Customizing Access Logs.
- Verify that the ISE/ISE-PIC Service Log was created; if it was not, create it—Adding and Editing Log Subscriptions.
- Define Identification Profiles that access ISE/ISE-PIC for user identification and authentication—Classifying Users and Client Software, on page 117.
- Configure access policies that utilize ISE/ISE-PIC identification to define criteria and actions for user requests—Policy Configuration, on page 191.

Acquiring ISE/ISE-PIC ERS Server Details from ISE/ISE-PIC

- Enable the Cisco ISE REST API in ISE/ISE-PIC (the APIs use HTTPS port 9060).

Note You must enable ISE External Restful Service (ERS) on the Web Security Appliance (Network > Identity Services Engine) to configure security policies based on groups. This is applicable to 11.7 and later versions.

- **ISE**
  - Choose **Administration** > **Settings** > **ERS Settings** > **ERS settings for primary admin node** > **Enable ERS**.

    Enable **ERS for Read for All Other Nodes** if there are any secondary nodes.
- **ISE-PIC**
  - Choose **Settings** > **ERS Settings** > **Enable ERS**.

- Ensure you have created an ISE administrator with the correct External RESTful Services group. The External RESTful Services Admin group has full access to all ERS APIs (GET, POST, DELETE, PUT). This user can Create, Read, Update, and Delete ERS API requests. The External RESTful Services Operator has Read Only access (GET request only).
  - **ISE**
    - Choose **Administration** > **System** > **Admin Access** > **Administrators** > **Admin Users**.
  - **ISE-PIC**
    - Choose **Administration** > **Admin Access** > **Admin Users**.

If the ERS service is available on separate servers, and not on the ISE/ISE-PIC pxGrid nodes, you will need the primary and secondary (if configured), servers' hostnames or IPv4 addresses.

Refer to Cisco *Identity Services Engine* documentation for more information.

VDI (Virtual Desktop Infrastructure) User Authentication in ISE/ISE-PIC Integrations

You can configure transparent identification with ISE/ISE-PIC for users on VDI environments based on the source ports used.

You must install the Cisco Terminal Services (TS) Agent, on the VDI servers. The Cisco TS agent provides the identity information to ISE/ISE-PIC. The identity information includes domain, user name, and the port ranges used by each user.

- Download the Cisco TS agent from the support site https://www.cisco.com/c/en/us/support/index.html.
- See the Cisco Terminal Services (TS) Agent Guide https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html for more information.
- Configure the ISE/ISE-PIC API provider to work with a Cisco TS agent. See the Cisco TS agent documentation for information about sending API calls.

Note

- Fallback authentication for VDI environment users is not supported.
- Ensure the number of maximum remote desktop sessions are the same in the Cisco Terminal Services agent and Microsoft server settings. This prevents incorrect session information from being sent to the Web Security Appliance from ISE, and avoids false authentication for new sessions.

Troubleshooting Identity Services Engine Problems

- Identity Services Engine Problems
  - Tools for Troubleshooting ISE Issues

- ISE Server Connection Issues
- ISE-related Critical Log Messages