Integrate the Cisco Identity Services Engine

This chapter contains the following sections:

Overview of the Identity Services Engine Service

Cisco's Identity Services Engine (ISE) is an application that runs on separate servers in your network to provide enhanced identity management. AsyncOS can access user-identity information from an ISE server. If configured, user names and associated Secure Group Tags will be obtained from the Identity Services Engine for appropriately configured Identification Profiles, to allow transparent user identification in policies configured to use those profiles.

Note The ISE service is not available in Connector mode.

Related Topics

- About pxGrid, on page 1
- About the ISE Server Deployment and Failover, on page 2

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) and user-group and profiling information.
- pxGrid controller – In this case, the ISE 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 Server Deployment and Failover

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

- Two pxGrid nodes
- Two Monitoring 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 that network deployments section in the Installation Guide for additional information.

Related Topics

- Identity Services Engine Certificates , on page 2
- Tasks for Certifying and Integrating the ISE Service, on page 3
- Connect to the ISE Services, on page 6
- Troubleshooting Identity Services Engine Problems, on page 8

Identity Services Engine Certificates

Note This section describes the certificates necessary for ISE connection. Tasks for Certifying and Integrating the ISE Service, on page 3 provides detailed information about these certificates. Certificate Management, provides general certificate-management information for AsyncOS.

A set of three certificates is required for mutual authentication and secure communication between the Web Security appliance and each ISE server:

- **WSA Client Certificate** – Used by the ISE server to authenticate the Web Security appliance.
- **ISE Admin Certificate** – Used by the Web Security appliance to authenticate an ISE server on port 443 for bulk download of ISE user-profile data.
- **ISE pxGrid Certificate** – Used by the Web Security appliance to authenticate an ISE server on port 5222 for WSA-ISE data subscription (on-going publish/subscribe queries to the ISE server).

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

Related Topics

- Using Self-signed Certificates, on page 3
- Using CA-signed Certificates, on page 3
- Overview of the Identity Services Engine Service, on page 1
- Tasks for Certifying and Integrating the ISE Service, on page 3
- Connect to the ISE Services, on page 6

Using Self-signed Certificates

When self-signed certificates are used on the ISE server, all three certificates—the ISE pxGrid and Admin certificates, developed on the ISE server, as well as the WSA Client certificate, developed on the WSA—must be added to the Trusted Certificates store on the ISE server (Administration > Certificates > Trusted Certificates > Import).

Using CA-signed Certificates

In the case of CA-signed certificates:

- On the ISE server, ensure the appropriate CA root certificate for the WSA Client certificate is present in the Trusted Certificates store (Administration > Certificates > Trusted Certificates).
- On the WSA, 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(s) for the ISE Admin and pxGrid certificates.

Tasks for Certifying and Integrating the ISE Service

Step	Task	Links to Related Topics and Procedures
1a	On the WSA, add a WSA Client certificate.	• Create or upload a CA-signed or self-signed WSA Client certificate on the WSA. See Connect to the ISE Services, on page 6 , and Certificate Management.
1b	On the WSA, download this WSA Client certificate for upload to the ISE server.	• Download the WSA Client certificate, save it, and then transfer it to the ISE server. See Connect to the ISE Services, on page 6.
2	If the WSA Client Certificate is self-signed, upload it and its signing certificate to the ISE server.	• Import the WSA Client certificate downloaded from the WSA in the previous step, adding it to the ISE server's Trusted Certificate store. (**Administration > Certificates > Trusted Certificates > Import**.) • Be sure to also add the appropriate signing certificate for this WSA Client certificate to the Trusted Certificates store on the ISE server, as discussed in Using Self-signed Certificates, on page 3.

Step	Task	Links to Related Topics and Procedures
3	On the ISE server, add ISE Admin and pxGrid certificates.	• Navigate to the **Administration > Certificates** page, and generate or upload ISE Admin and pxGrid certificates: • For CA-signed certificates, generate two Certificate Signing Requests, one each for Admin and pxGrid Usage, and then have the certificates signed. Upon receipt of the signed certificates, upload both to the ISE server. Perform the "Bind the CA Signed Certificate" operation for both. Be sure to add the CA root certificate to the ISE server's Trusted Certificates store. Restart the ISE server. • For self-signed certificates, navigate to **Administration > Certificates > System Certificates**, and generate two Self Signed Certificates, one each for Admin and pxGrid. (You can also elect to generate one common certificate for both.) Add both to the Trusted Certificates store. Export the self-signed certificate(s) for import onto the WSA. **Note** Ensure the appropriate self-signed or CA root certificates for these ISE Admin and pxGrid certificates are added to the Trusted Certificates store, as discussed in Identity Services Engine Certificates , on page 2.

Step	Task	Links to Related Topics and Procedures
4	Ensure the ISE server is configured appropriately for WSA access.	Each ISE server must be configured to allow identity topic subscribers (such as WSA) to obtain session context in real-time. The basic steps are: • Ensure "Enable Auto Registration" is turned ON (Administration > pxGrid Services > Top Right). • Delete all existing WSA clients from the ISE server (Administration > pxGrid Services > Clients). • Be sure the ISE server footer (Administration > pxGrid Services) says "Connected to pxGrid." • Configure SGT groups on ISE server (Policy > Results > TrustSec > Security Groups). • Configure policies that associate the SGT groups with users. Refer to *Cisco Identity Services Engine* documentation for more information.
5	On the WSA, add the exported ISE Admin and pxGrid certificates.	• Upload the ISE Admin and pxGrid certificates for each ISE server you are configuring on this WSA. See Connect to the ISE Services, on page 6. • If using a single self-signed certificate for both ISE Admin and pxGrid, upload the file twice, once each in the ISE Admin Certificate and ISE pxGrid Certificate fields. See Connect to the ISE Services, on page 6. • If using CA-signed certificates, be sure the Certificate Authority that signed each pair of ISE certificates is listed in the Trusted Root Certificates list on the WSA. If not, import the CA root certificate. See Managing Trusted Root Certificates. **Note** If the ISE Admin and pxGrid certificates are signed by your Root CA certificate, be sure to upload Root CA certificate itself to the ISE Admin Certificate and ISE pxGrid Certificate fields on the WSA (Network > Identity Services Engine).

Step	Task	Links to Related Topics and Procedures
6	Complete configuration of the WSA for ISE access and logging.	• Connect to the ISE Services, on page 6 • Add the custom field %m to the Access Logs to log the Authentication mechanism – Customizing Access Logs. • Verify that the ISE Service Log was created; if it was not, create it – Adding and Editing Log Subscriptions. • Ensure the ISE Service Log was created; if not, add it – Adding and Editing Log Subscriptions. • Define Identification Profiles that access ISE for user identification and authentication – Classifying Users and Client Software. • Configure access policies that utilize ISE identification to define criteria and actions for user requests – Policy Configuration.

Note Whenever you upload or change certificates on the ISE server, you must restart the ISE service. Also, a few minutes may be required before the services and connections are restored.

Related Topics

- Overview of the Identity Services Engine Service, on page 1
- Identity Services Engine Certificates , on page 2
- Troubleshooting Identity Services Engine Problems, on page 8

Connect to the ISE Services

Before you begin

- Be sure each ISE server is configured appropriately for WSA access; see Tasks for Certifying and Integrating the ISE Service, on page 3 .
- Obtain ISE server connection information.
- Obtain valid ISE-related certificates (client, Portal and pxGrid) and keys. See also Identity Services Engine Certificates , on page 2for related information.

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

Step 2 Click **Edit Settings**.

Step 3 Check **Enable ISE Service**.

Step 4 Identify the **Primary ISE pxGrid Node** using its host name or IPv4 address.

a) Provide an **ISE pxGrid Node Certificate** for WSA-ISE data subscription (on-going queries to the ISE server).

Browse to and select the certificate file, and then click **Upload File**. See Uploading a Certificate and Key for additional information.

Step 5 If using a second ISE server for failover, identify the **Secondary ISE pxGrid Node** using its host name or IPv4 address.

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

Browse to and select the certificate file, 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 WSA configuration. After ISE failover is complete, normal ISE authentication resumes.

Step 6 Upload the **ISE Monitoring Node Admin Certificates**:

a) Provide the **Primary ISE Monitoring Node Admin Certificate** for use in bulk download of ISE user-profile data to the WSA.

Browse to and select the certificate file, and then click **Upload File**. See Uploading a Certificate and Key for additional information.

b) If using a second ISE server for failover, provide the **Secondary ISE Monitoring Node Admin Certificate**.

Step 7 Provide a **WSA Client Certificate** for WSA-ISE server mutual authentication:

Note This must be a CA trusted-root certificate. See Identity Services Engine Certificates , on page 2 for related information.

- **Use Uploaded Certificate and Key**

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

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

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

- **Use Generated Certificate and Key**

  Click **Generate New Certificate and Key**. (See Generating a Certificate and Key for additional information about this option.)

Step 8 Download the WSA Client Certificate, save it, and then upload it to the ISE server host (Administration > Certificates > Trusted Certificates > Import on the specified server).

Step 9 (Optional) Click **Start Test** to test the connection with the ISE pxGrid node(s).

Step 10 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 WSA using ISE and TrustSec through pxGrid..”

Troubleshooting Identity Services Engine Problems