



Cisco Secure Network Analytics

ISE and ISE-PIC Configuration Guide 7.5.1



Table of Contents

Introduction	4
Overview	4
Requirements	4
Certificate Requirements	4
Testing the Configuration	5
Deploying Certificates	6
Option 1 - Deploying Certificates using ISE Internal Certificate Authority (Recommended)	6
Generating a Secure Network Analytics pxGrid client certificate	6
Generating a CSR for the client certificate from Central Management	6
Creating a certificate CSR using internal ISE CA	6
Adding the Client Identity Certificates to Central Management	7
Adding the ISE Sub-CA Certificate to the Secure Network Analytics Trust Store	8
Option 2 - Deploying Certificates Using an External Certificate Authority (CA) Server	8
Generating a Secure Network Analytics pxGrid client certificate	8
Generating a CSR for the Secure Network Analytics pxGrid Client certificate	8
Creating a Secure Network Analytics pxGrid Client certificate using an external CA	9
Adding the Secure Network Analytics pxGrid client certificate to the Manager	9
Importing the CA root certificate into the Manager Trust Store	10
Generating an ISE server pxGrid certificate	10
Generating a CSR for an ISE server pxGrid certificate	10
Creating an ISE Server pxGrid certificate using an external CA	11
Importing the CA root certificate into the ISE Trust Store	11
Binding the ISE certificate to the Certificate Signing Request (CSR)	11
Adding ISE Configuration	13
Open ISE Configuration Setup Page	13
Settings	13

Integration Options	14
Additional Parameters	15
Node status indicator	15
Refresh icon	15
Approve pxGrid in ISE or ISE-PIC	15
Refresh the ISE Configuration page	16
Verify the ISE Configuration	16
Edit or Delete a Saved ISE cluster	17
Configure ISE Integration Failover	18
Adjusting Secure Network Analytics Configuration to Support Scaled ISE deployment	19
Contacting Support	20
Change History	21

Introduction

Overview

This document provides Cisco engineers and customers deploying Cisco Secure Network Analytics (formerly Stealthwatch) with Cisco Identity Services Engine (ISE) the changes to the configuration workflow required to connect Secure Network Analytics v7.5.1 to ISE pxGrid.

Requirements

ISE requires TLS v1.3 for administrator HTTPS access over Port 443. For more details, refer to the following:

- [Cisco Identity Services Engine Administrator Guide, Release 3.3](#)
- [Configure Ciphers in ISE 3.3 and Later](#)

Certificate Requirements

To connect Secure Network Analytics and ISE, it's required that certificates are deployed correctly for trusted communication between the two systems. Deploying certificates requires that you use several different product or application interfaces: the Web App, the Central Management interface, and the ISE Server management portal. Before you get started, review the procedures to make sure you understand the requirements and instructions.

Secure Network Analytics imports client certificates to connect to ISE pxGrid node. Use the following guidelines for your client identity certificates.

- **Generate CSR in Central Management:** If you generate the CSR in Central Management, the listed requirements designated with (*) are included in the CSR (refer to the **Generate the CSR in Central Management** column).
- **Skip the CSR in Central Management:** If you generate the CSR outside of Central Management, confirm the CSR includes the requirements in this table (refer to the **Skip CSR in Central Management** column).
- **Verifying Certificate Requirements:** Whether you generate the CSR in Central Management or skip the CSR, confirm your certificates meet the requirements in this table before you add them to your Manager.

Requirements	Generate CSR in Central Management	Skip CSR in Central Management
File Format*	PEM (.cer, .crt, .pem) or PKCS#12 (.p12, .pfx, .pks)	PKCS#12 (.p12, .pfx, .pks)
Keys*	RSA Key Lengths Available: 2048 bits (not recommended), 4096 bits, or 8192 bits ECDSA Curves: Not available	RSA Key Lengths Required: 2048 bits (not recommended) or more or ECDSA Key Curves Required: NIST P-256, P-384, or P-521
Signed By	Confirm the client identity certificate is self-signed or signed by a Certificate Authority.	Confirm the client identity certificate is self-signed or signed by a Certificate Authority.
Authentication (Extended Key Usage)*	The CSR requests client (clientAuth) authentication.	Client (clientAuth) authentication is required for client identity certificates.
Date Range	Confirm the certificate dates are current and not expired.	Confirm the certificate dates are current and not expired.

**If you generate the CSR in Central Management, the listed requirements designated with (*) are included in the CSR.*

Testing the Configuration

After deploying the certificates, go to ISE Troubleshooting TechNotes article, <https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/217511-troubleshoot-sna-ise-integration-conn.html>, to verify that the ISE integration with Secure Network Analytics is configured correctly.

Deploying Certificates

Option 1 – Deploying Certificates using ISE Internal Certificate Authority (Recommended)

Using the Internal ISE Certificate Authority (CA) is the recommended method of deploying certificates. Use the procedure below to proceed with this option:

Generating a Secure Network Analytics pxGrid client certificate

Generating a CSR for the client certificate from Central Management



If you are generating the CSR outside of Central Management, skip this section and proceed to **Creating a certificate CSR using internal ISE CA**. Before you start the procedure, confirm your CSR meets requirements shown in **Certificate Requirements**.

1. Log in to the Manager (formerly Stealthwatch Management Console).
2. From the main menu, select **Configure > Global > Central Management**.
3. On the Inventory page, click the **⋮ (Ellipsis)** icon for the Manager that you want to connect to ISE.
4. Choose **Edit Appliance Configuration**.
5. Go to the **Additional SSL/TLS Client Identities** section under the **Appliance** tab.
6. Click **Add New**.
7. Do you need to generate a CSR (Certificate Signing Request)? Choose **Yes**. Click **Next**.
8. Select an **RSA Key Length** and complete the rest of the fields in the **Generate a CSR** section.
9. Click **Generate CSR**. The generation process may take several minutes.
10. Click **Download CSR** and save the CSR file on your computer.

Creating a certificate CSR using internal ISE CA

1. Log in to your ISE Management Interface.
2. Go to **Administration > pxGrid Services > Client Management > Certificates**. The **Generate pxGrid Certificates** form opens.



The path can be different for ISE-PIC.

3. In the **I want to** field select **Generate a single certificate (with certificate signing request)**.
4. Open the CSR with your preferred text editor, copy the contents of the file, and paste them to the **Certificate Signing Request Details** field.
5. If desired, enter a description.
6. In the **Certificate Download Format** field, select **PKCS12** format (including certificate chain; one file for both the certificate chain and key).
7. In the **Certificate Password** and **Confirm Password** fields, type the password which will be requested when you upload the certificate to Central Management in the **Additional SSL/TLS Client Identities** section.
8. Click **Create**.



If your certificate fails to generate, make sure the key length of the pxGrid_Certificate_Template matches the key length of the CSR you created in Secure Network Analytics. Click the link next to the **Certificate Template** field to edit the key length of the pxGrid_Certificate_Template.

9. If you skipped the CSR in Central Management, re-package the PKCS12 file to include the private key.

Adding the Client Identity Certificates to Central Management

1. Unzip the file created in the section above to access the PKCS12 file.



You may need to unblock pop-up menus in order to download this file.

2. Go to the **Additional SSL/TLS Client Identities** section of the Manager Configuration in Central Management.
3. **If you generated the CSR in Central Management**, the **Additional SSL/TLS Client Identities** section will contain a form to import the created client certificate.

If you skipped the CSR in Central Management, click **Add New**.

- Do you need to generate a CSR? Choose **No**.
 - Click **Next**.
4. Give the certificate a friendly name, then click **Choose File** to locate the certificate file.
 5. Type the password you entered in the previous section.

6. Click **Add Client Identity** to add the certificate to the system.
7. Click **Apply Settings** to save the changes.

Adding the ISE Sub-CA Certificate to the Secure Network Analytics Trust Store

1. Log in to your ISE Management Interface.
2. Go to **Administration > System > Certificates**, then click **Certificate Authority Certificates**.
3. Find the **Certificate Services Endpoint Sub CA** certificate and export it to your computer.



If the ISE Sub-CA certificate is not the Certificate Authority that issued the certificate used by the ISE pxGrid node, you will need to procure that CA certificate in this step.

4. Log in to the Manager.
5. From the main menu, select **Configure > Global > Central Management**.
6. On the Inventory page, click the **⋮ (Ellipsis)** icon for the Manager.
7. Choose **Edit Appliance Configuration**.
8. Select the **General** tab.
9. Go to the **Trust Store** section and import previously exported ISE CA certificate.
10. Click **Add New**.
11. Give the certificate a friendly name, then click **Choose File** to select the previously exported ISE CA certificate.
12. Click **Add Certificate** to save the changes.

Certificates are now deployed and the two systems (Secure Network Analytics and ISE) trust each other. Continue to the [Adding ISE Configuration](#) chapter to setup connection to ISE pxGrid nodes.

Option 2 – Deploying Certificates Using an External Certificate Authority (CA) Server

Generating a Secure Network Analytics pxGrid client certificate

Generating a CSR for the Secure Network Analytics pxGrid Client certificate

1. Log in to Manager.
2. From the main menu, select **Configure > Global > Central Management**.

3. On the Inventory page, click the **⋮ (Ellipsis)** icon for the Manager that you want to connect to ISE.
4. Choose **Edit Appliance Configuration**.
5. Go to the **Additional SSL/TLS Client Identities** section under the **Appliance** tab.
6. Click **Add New**.
7. Do you need to generate a CSR (Certificate Signing Request)? Choose **Yes**. Click **Next**.
8. Select an **RSA Key Length** and complete the rest of the fields in the **Generate a CSR** section.
9. Click **Generate CSR**. The generation process may take several minutes.
10. Click **Download CSR** and save the CSR file locally.

Creating a Secure Network Analytics pxGrid Client certificate using an external CA



This example uses Microsoft Active Directory Certificate Service of MS Server 2012. You can use a different external CA.

1. Go to MS Active Directory Certificate Service, <https://server/certsrv/>, where server is ip or dns of your MS Server.
2. Click **Request a certificate**.
3. Choose to submit an **advanced certificate request**.
4. Copy the contents of the CSR file generated in the previous section into the **Saved Request** field.
5. Select **pxGrid** as the Certificate Template, then click **Submit**.
6. Download a generated certificate in **Base-64** format and save it as **pxGrid_client.cer**.

Adding the Secure Network Analytics pxGrid client certificate to the Manager

1. Go to the **Additional SSL/TLS Client Identities** section of the Manager Configuration in Central Management.
2. The **Additional SSL/TLS Client Identities** section will contain a form to import the created client certificate.
3. Give the certificate a friendly name, then click **Choose File** to locate the certificate file.
4. Type the password you entered in the previous section.

5. Click **Add Client Identity** to add the certificate to the system.
6. Click **Apply Settings** to save the changes.

Importing the CA root certificate into the Manager Trust Store

1. Go to MS Active Directory Certificate Service home page and select **Download a CA certificate, certificate chain, or CRL**.
2. Select **Base-64** format, then click **Download CA certificate**.
3. Save the certificate as **CA_Root.cer**.
4. Log in to the Manager.
5. From the main menu, select **Configure > Global > Central Management**.
6. On the Inventory page, click the **⋮ (Ellipsis)** icon for the Manager.
7. Choose **Edit Appliance Configuration**.
8. Select the **General** tab.
9. Go to the **Trust Store** section and import previously exported CA_Root.cer certificate.
10. Click **Add New**.
11. Give the certificate a friendly name, then click **Choose File** to select the previously exported ISE CA certificate.
12. Click **Add Certificate** to save the changes.

Generating an ISE server pxGrid certificate

Generating a CSR for an ISE server pxGrid certificate

1. Open your ISE Management interface.
2. Go to **Administration > System > Certificates > Certificate Management > Certificate Signing Requests**.
3. Select **Generate Certificate Signing Request (CSR)**.
4. Select **pxGrid** in the **Certificate(s) will be used for** field.
5. Select ISE node for which the certificate is generated.
6. Fill in other certificates details as necessary.
7. Click **Generate**.
8. Click **Export** and save the file locally.

Creating an ISE Server pxGrid certificate using an external CA

1. Go to MS Active Directory Certificate Service, <https://server/certsrv/>, where server is ip or dns of your MS Server.
2. Click **Request a certificate**.
3. Choose to submit an **advanced certificate request**.
4. Copy the contents of the CSR generated in the previous section into the **Saved Request** field.
5. Select **pxGrid** as the Certificate Template, then click **Submit**.
6. Download the generated certificate in **Base-64** format and save it as **ISE_pxGrid.cer**.

Importing the CA root certificate into the ISE Trust Store

1. Go to MS Active Directory Certificate Service home page and select **Download a CA certificate, certificate chain, or CRL**.
2. Select **Base-64** format, then click **Download CA certificate**.
3. Save the certificate as **CA_Root.cer**.
4. Log in to your ISE management interface.
5. Select **Administration > System > Certificates > Certificate Management > Trusted Certificates**.
6. Select **Import > Certificate file** and import the root certificate.
7. Make sure the **Trust for authentication within ISE** check box is selected.
8. Click **Submit**.

Binding the ISE certificate to the Certificate Signing Request (CSR)

1. Log in to your ISE Management interface.
2. Select **Administration > System > Certificates > Certificate Management > Certificate Signing Requests**.
3. Select the CSR generated in the previous section, then click **Bind Certificate**.
4. On the **Bind CA Signed Certificate** form, choose the **ISE_pxGrid.cer** certificate generated previously.
5. Give the certificate a friendly name, then click **Submit**.
6. Click **Yes** if the system asks for restart.
7. Click **Yes** if the system asks to replace the certificate.

-
8. Select **Administration > System > Certificates > System Certificates**.
 9. You should see the created pxGrid certificate signed by the external CA in the list.

Certificates are now deployed and the two systems (Secure Network Analytics and ISE) trust each other. Continue to the [Adding ISE Configuration](#) chapter to setup connection to ISE pxGrid nodes.

Adding ISE Configuration

Complete the following steps to configure an ISE cluster for the current domain.



- You must configure an ISE cluster for each Secure Network Analytics domain in which it is used.
- You can add multiple independent ISE clusters to a domain in Secure Network Analytics, but you cannot use the same IP address across clusters within the same domain.
- Each ISE configuration requires a unique client name that connects to ISE.
- You must configure your firewall to allow your Manager and ISE to communicate through port TCP/8910 and TCP/443.

Open ISE Configuration Setup Page

1. Select **Configure > Integrations > Cisco ISE**.
2. In the upper right corner of the page, click **Add new configuration**.

Settings

Define the following settings:

- **Cluster Name:** This name will display in the Enterprise Tree in the Desktop Client and in the list of your ISE configurations in the Manager Web UI.
- **Certificate:** This is the same name that is entered in the Friendly Name field in the Additional SSL/TLS Client Identities section in the Manager Configuration interface that enables the appliance to authenticate its identity as a client (i.e., it is the client certificate that the Manager presents to ISE).
- **PxGrid Node 1:** The IP address, hostname, or FQDN of the primary pxGrid node on the ISE cluster with which the appliance is integrating.
- **PxGrid Node 2 (optional):** The IP address, hostname, or FQDN of the second pxGrid node on the ISE cluster with which the appliance is integrating. This node is used for failover purposes. If the connection to the first node fails, the second node is used.
- **PxGrid Node 3 (optional):** The IP address, hostname, or FQDN of the third pxGrid node on the ISE cluster with which the appliance is integrating. This node is used for failover purposes. If the connection to the first and second node fails, the third node is used.

- **Client Name:** This unique name is displayed in the pxGrid client list on the ISE cluster in the ISE appliance.
- **Enable Strict ISE Server Identity Verification:** Enable this setting to require server identity verification when your Manager communicates with your ISE cluster nodes. In addition to our other security checks, we allow communication if the ISE node identity certificate meets one of the following:
 - It includes the node name or identification information (such as FQDN) listed as a Common Name or Subject Alternative Name of the certificate.
 - It matches a certificate in your Manager trust store.



- The **Enable Strict ISE Server Identity Verification** option is turned off by default if you're upgrading from releases prior to v7.4 for which ISE integration has been configured. This option is turned on by default for ISE integration configurations beginning with v7.4.
- For successful connection and functioning of the selected integration options, make sure you configure your Manager DNS settings so the Manager can resolve FQDNs (Fully Qualified Domain Names) of your ISE server (all nodes in case of distributed deployment including PAN, Mnt, SXP, pxGrid), since services provided by these nodes are dynamically discovered and referred to using node FQDNs.

Integration Options

Select the ISE product for the integration:

- **ISE:** Allows enabling all integration options.
- **ISE-PIC:** Allows enabling session updates only.

Select the integration options to enable for the ISE cluster:




- **Adaptive Network Control:** Allows you to apply classification (ANC Policy) to the endpoint on ISE and change network access for it, according to the authorization policy configured on ISE.
- **Static TrustSec Classifications:** Allows you to receive information about TrustSec security group tags (SGTs) which have been statically associated with the endpoint IP beyond the authentication process. This could be IP-to-SGT bindings manually configured on ISE, access layer device, or learned from other systems within the SXP process. This data is used to augment flows where a SGT is missing for a matched endpoint IP address in the original flow and there is no session associated with the SGT assigned endpoint IP address.

- **Sessions:** Allows you to receive user session updates that include information about the username, MAC address of the endpoint, device profile, and TrustSec security group. This information will be used to augment flows with TrustSec security group information and to monitor users and sessions on Manager reports. Enable **Track sessions derived from machine authentications** to receive machine sessions updates along with user sessions updates.

Additional Parameters

Node status indicator

The node status indicator located beside each IP Address field indicates the connection status for each added node. These appear after you configure and save the first node.

- A  (**Green Status**) icon signifies that a connection to the node has been established and the system is subscribed to all required topics of information on pxGrid.
- A  (**Yellow Status**) icon signifies that a connection to the node is pending and connection is in progress or waiting for the client to be approved on the pxGrid Services page on ISE.
- A  (**Red Status**) icon signifies that a connection to the node has not been established or subscription to the required topics of information on pxGrid failed. To determine why there is no connection, or what subscription failed, click the icon, which will display an error message.

Refresh icon

Click the  (**Refresh**) icon to refresh the connection to the associated cluster.

Approve pxGrid in ISE or ISE-PIC

1. Do one of the following:
 - a. If using ISE, log in to this appliance, and from the main menu click **Administration**. On the page that opens, click the **pxGrid Services** tab.
 - b. If using ISE-PIC, log in to this appliance, and from the main menu click **Subscribers**. On the page that opens, click the **Clients** tab.
2. In the table that opens, select the check box beside the applicable subscriber's name in the Client Name column and click **Approve** from the submenu at the top of the table.

Refresh the ISE Configuration page

1. Return to the ISE Configuration page in the Web App and refresh the page.
2. Confirm that the node status indicator located beside the applicable IP Address field is green, indicating that a connection to the ISE or ISE-PIC cluster has been established

Verify the ISE Configuration

Go to the ISE Troubleshooting TechNotes article, <https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/217511-troubleshoot-sna-ise-integration-conn.html>, to verify that the ISE integration with Secure Network Analytics is configured correctly.

Edit or Delete a Saved ISE cluster

Click the **⋮ (Ellipsis)** icon in the **Actions** column to open the submenu, then select the appropriate option.


- You cannot remove the last remaining node from a ISE cluster that still exists in Secure Network Analytics.
- If the Unlicensed Feature alarm is active for a ISE cluster, you can still remove all of the ISE clusters. After you have done so, within a few minutes the alarm becomes inactive.
- When you delete an ISE cluster, for historical purposes the client user name is not deleted from ISE. The user name still appears in the ISE Box in the pxGrid Username list.

Configure ISE Integration Failover

ISE integration failover allows you to configure your primary and secondary Managers to receive ISE session updates, so that when the primary Manager fails and the secondary Manager switches to the primary role, the information about your users is still available on Manager reports.

The ISE Integration failover configuration requires you to do the following:

- Configure ISE Integration on both the primary Manager and the secondary Manager.
- Generate different ISE client certificates for both the primary Manager and the secondary Manager.
- Specify different client names in ISE Configuration for both the primary Manager and the secondary Manager.

 If you have already established the Manager failover relationship, you may need to switch the secondary Manager to be the primary Manager in order to make changes to your ISE integration configuration.

To configure ISE integration failover, complete the following steps:

1. Configure the primary Manager by following the steps in [Adding ISE Configuration](#). Make sure you generate a unique ISE client certificate and that you assign a unique client name.
2. Repeat these steps for the secondary Manager, ensuring that you generate a unique ISE client certificate and that you assign a unique client name.

Make sure that the pxGrid nodes and ISE Integration options match those of the primary Manager.

Adjusting Secure Network Analytics Configuration to Support Scaled ISE deployment

By default, the number of simultaneous active sessions the Secure Network Analytics Flow Collector can process depends on the total amount of memory available on your appliance.

Refer to the following specifications:

Total RAM	Total Number of Sessions
From 16G to 128G	524,288
More than 128G	2,097,152

To allow the Flow Collector to process more ISE sessions than supported by default, the appliance needs to be additionally configured. The configuration will set the size of the in-memory data structures that keep the information about critical objects such as hosts, users, sessions, and devices.

Please contact [Cisco Support](#) to adjust the configuration of the appliance.

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: <http://www.cisco.com/c/en/us/support/index.html>
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers:
<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

Change History

Document Version	Published Date	Description
1_0	July 24, 2024	Initial Version.

Copyright Information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

