Cisco Stealthwatch

ISE and ISE-PIC Configuration Guide 7.3.2

Table of Contents

Introduction

Overview

This document provides Cisco engineers and customers the configuration workflow required to connect Stealthwatch v7.3.2 to Cisco ISE pxGrid.

> ℹ If you are on Stealthwatch v7.3.0 or v7.3.1, make sure to use the ISE Configuration Guide v7.3.x.

Technical Details

To connect Stealthwatch and Cisco 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 SMC Web App, the Central Management interface, and the Cisco ISE Server management portal.

Starting with v7.0, Stealthwatch only imports client certificates created with a Certificate Signing Request (CSR) generated from Stealthwatch Central Management to connect to ISE pxGrid node. This changes the certificates management workflows comparing to previous versions of Stealthwatch.

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 Stealthwatch is configured correctly.

Contacting support

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

- Contact your local Cisco Partner
- Contact Cisco Stealthwatch 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: www.cisco.com/en/US/partner/support/tsd_cisco_worldwide_contacts.html

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 Stealthwatch pxGrid client certificate

Generating a CSR for the client certificate from Stealthwatch Central Management

1. Log in to Stealthwatch Management Console.
2. Click on the **Global Settings** icon, and then click **Central Management**.
3. On the Appliance Manager inventory page, click the **Actions** menu for the SMC that you want to connect to ISE. Select **Edit Appliance Configuration.**
4. Go to the **Additional SSL/TLS Client Identities** section under the **Appliance** tab.
5. Click **Add New**. The **Generate a CSR** form opens.
6. Select an **RSA Key Length** and complete the rest of the fields in the **Generate a CSR** section.
7. Click **Generate CSR**. The generation process may take several minutes.
8. Click **Download CSR** and save the CSR file on your computer.

Creating a certificate based on the generated CSR using internal ISE CA

1. Log in to your ISE Management Interface.
2. Go to **Administration > pxGrid Services > 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 generated in the previous section with your preferred text editor and copy the contents of the file 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 Stealthwatch Central Management in the **Additional SSL/TLS Client Identities** section (see **Introduction**).
8. Click **Create**.

> If your certificate fails to generate, ensure the key length of the pxGrid_Certificate_Template matches the key length of the CSR you created in Stealthwatch. Click the link next to the **Certificate Template** field to edit the key length of the pxGrid_Certificate_Template.

Stealthwatch 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 SMC Configuration in Central Management.
3. The **Additional SSL/TLS Client Identities** section will contain a form to import the created client certificate.
4. Give the certificate a friendly name and click **Choose File** to locate the certificate file.
5. Type in 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 Cisco ISE Sub-CA Certificate to the Stealthwatch Trust Store

1. Log in to your ISE Management Interface.
2. Go to **Administration > System > Certificates** and click on **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.

1. Log in to Stealthwatch Management Console.
2. Click on the **Global Settings** icon, and then click **Central Management**.
3. On the Appliance Manager inventory page, click the **Actions** menu for the SMC. Select **Edit Appliance Configuration**.
4. Select the **General** tab.
5. Go to the **Trust Store** section and import previously exported ISE CA certificate.
6. Click **Add New**.
7. Give the certificate a friendly name and click **Choose File** to select the previously exported ISE CA certificate.
8. Click **Add Certificate** to save the changes.

Certificates are now deployed and the two systems (Stealthwatch 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 Stealthwatch pxGrid client certificate

Generating a CSR for the Stealthwatch pxGrid Client certificate

1. Log in to Stealthwatch Management Console.
2. Click on the **Global Settings** icon, and then click **Central Management**.
3. On the Appliance Manager inventory page, click the **Actions** menu for the SMC that you want to connect to ISE. Select **Edit Appliance Configuration**.
4. Go to the **Additional SSL/TLS Client Identities** section under the **Appliance** tab.
5. Click **Add New**. The **Generate a CSR** form opens.
6. Select an **RSA Key Length** and complete the rest of the fields in the **Generate a CSR** section.
7. Click **Generate CSR**. The generation process may take several minutes.
8. Click **Download CSR** and save the CSR file locally.

Creating a Stealthwatch 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 and click **Submit**.
6. Download a generated certificate in **Base-64** format and save it as **pxGrid_client.cer**.

Adding the Stealthwatch pxGrid client certificate to the SMC

1. Go to the **Additional SSL/TLS Client Identities** section of the SMC 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 and click **Choose File** to locate the certificate file.
4. Type in 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 SMC 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 and click **Download CA certificate**.
3. Save the certificate as **CA_Root.cer**.
4. Log in to Stealthwatch Management Console.
5. Click on the **Global Settings** icon, and then click **Central Management**.
6. On the Appliance Manager inventory page, click the **Actions** menu for the SMC. Select **Edit Appliance Configuration**.
7. Select the **General** tab.
8. Go to the **Trust Store** section and import previously exported CA_Root.cer certificate.
9. Click **Add New**.

10. Give the certificate a friendly name and click **Choose File** to select the previously exported ISE CA certificate.
11. 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 and 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 and 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** checkbox 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 and 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 and 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 (Stealthwatch 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 a Cisco ISE cluster for the current domain.

> ⓘ
>
> - You must configure a Cisco ISE cluster for each Stealthwatch System domain in which it is used.
> - You can add multiple independent Cisco ISE clusters to a domain in the Stealthwatch System, but you cannot use the same IP address across clusters within the same domain.
> - You must configure your firewall to allow your SMC and ISE to communicate through port TCP/8910 and TCP/443.

Open Cisco ISE Configuration Setup Page

1. From the main menu in the SMC, choose **Deploy > Cisco ISE Integration**.
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 SMC desktop client and in the list of your ISE configurations in SMC 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 SMC Configuration interface that enables the appliance to authenticate its identity as a client (i.e., it is the client certificate that the SMC presents to ISE).
- **PxGrid Node 1:** The IP address of the primary pxGrid node on the ISE cluster with which the appliance is integrating.
- **PxGrid Node 2 (optional):** The IP address 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 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.

Integration Options

Select the ISE product for the integration:

- **Cisco ISE:** Allows enabling all integration options.
- **Cisco 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 SMC 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

see 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 Cisco ISE or Cisco ISE-PIC

1. Do one of the following:
    a. If using Cisco 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 Cisco 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 Cisco ISE Configuration page

1. Return to the Cisco ISE Configuration page in the SMC 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 Cisco ISE or Cisco 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 Stealthwatch is configured correctly.

Edit or Delete a Saved Cisco ISE cluster

In the Actions column, click the ellipsis to open the context menu, and then select the appropriate option.

- You cannot remove the last remaining node from a Cisco ISE cluster that still exists on the Stealthwatch System.
- If the Unlicensed Feature alarm is active for a Cisco ISE cluster, you can still remove all of the Cisco 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 Cisco 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 SMCs to receive ISE session updates, so that when the primary SMC fails and the secondary SMC switches to the primary role, the information about your users is still available on SMC reports.

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

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

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

To configure ISE integration failover, complete the following steps:

1. Configure the primary SMC 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 SMC, 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 SMC.

Adjusting Stealthwatch Configuration to Support Scaled ISE deployment

By default, the number of simultaneous active sessions the Stealthwatch 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 Technical Support to adjust the configuration of the appliance.

Copyright Information