

Integrate ISE 3.3 with Stealthwatch 7.5.1 Using External CA

Contents

[Introduction](#)

[Prerequisites](#)

[Components Used](#)

[Configure](#)

[Section A: Secure Network Analytics \(Stealthwatch\) Certificate Configuration](#)

[Part I - Generating a CSR for the Secure Network Analytics pxGrid Client Certificate](#)

[Part II - Creating a Secure Network Analytics pxGrid Client Certificate Using an External CA](#)

[PART III - Adding the Secure Network Analytics pxGrid Client Certificate to the Manager](#)

[PART IV - Importing the CA Root Certificate into the Manager Trust Store](#)

[Section B: Cisco Identity Services Engine 3.3 Certificate Configuration](#)

[PART I - Generating an ISE Server pxGrid Certificate](#)

[PART II - Creating an ISE Server pxGrid Certificate Using an External CA](#)

[PART III - Importing the CA Root Certificate into the ISE Trust Store](#)

[PART IV - Binding the ISE certificate to the Certificate Signing Request \(CSR\)](#)

[Integrate](#)

[Verify](#)

[Troubleshooting](#)

[DNS Resolution Issue](#)

[Solution](#)

[Unknown CA Error or Trusted Certificate Missing](#)

[Solution](#)

[Known Defects](#)

Introduction

This document describes procedures to integrate ISE 3.3 with Secure Network Analytics (Stealthwatch) using pxGrid connections.

Prerequisites

Cisco recommends knowledge in these topics:

- Identity Services Engine
- Platform Exchange Grid (pxGrid)
- Secure Network Analytics(Stealthwatch)
- TLS/SSL Certificates.
- PKI on Windows Server 2016

Components Used

The information in this document is based on these software and hardware versions:

- Identity Services Engine (ISE) version 3.3 patch 4
- Secure Network Analytics (Stealthwatch) 7.5.1
- Windows server 2016 as an external Certificate Authority(CA) server.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Section A: Secure Network Analytics (Stealthwatch) Certificate Configuration

Part I - Generating a CSR for the Secure Network Analytics pxGrid Client Certificate

1. Log in to **Stealthwatch Management Console (SMC)**.
2. From the main menu, select **Configure > Global > Central Management**.



Risk



Monitor



Investigate



Report



Configure

Configure

X

Detection

Host Group Management

Alarm Severity

Policy Management

Response Management

Network Scanners

Analytics

Alerts

Global

Central Management

User Management

Manager

UDP Director

External Lookup

System

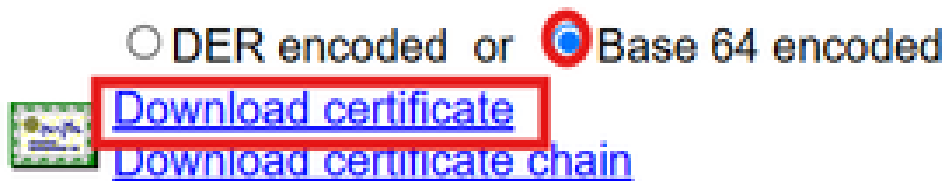
: Certificate Template pxGrid used needs both Client authentication and server authentication in the "Enhanced Key Usage" field.

6. **Download** a generated certificate in **Base-64 format** and **Save** it as pxGrid_client.cer.

Microsoft Active Directory Certificate Services -- Avaste-ISE

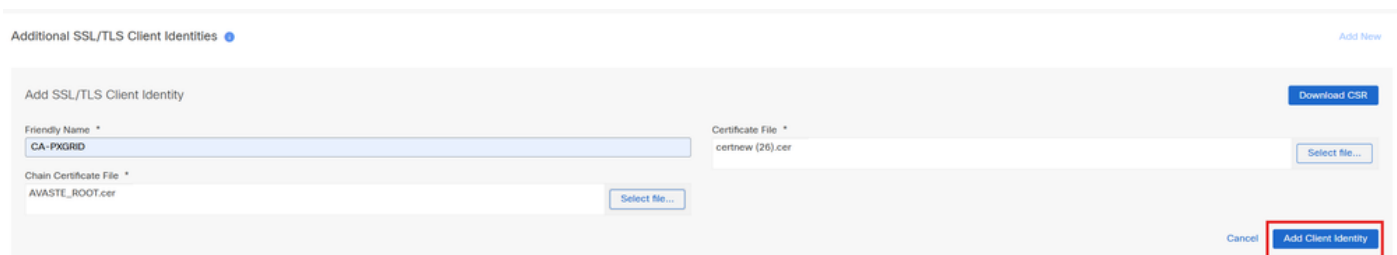
Certificate Issued

The certificate you requested was issued to you.



PART III - Adding the Secure Network Analytics pxGrid Client Certificate to the Manager

1. **Navigate** to the **Additional SSL/TLS Client Identities** section of the Manager Configuration in **Central Management**.
2. The **Additional SSL/TLS Client Identities** section contains a form to import the created client certificate.
3. Give the certificate a **friendly name**, then click **Select File** to locate the certificate file.
4. Select the root or issuer CA .cer file or the certificate chain file (.pem / .cer / .crt) under the Chain Certificate file section.
5. Click **Add Client Identity** to add the certificate to the system.



6. Click **Apply Settings** to save the changes.

PART IV - Importing the CA Root Certificate into the Manager Trust Store

1. **Navigate** to **MS Active Directory Certificate Service** homepage and select **Download a CA certificate, certificate chain, or CRL**.

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:[Request a certificate](#)[View the status of a pending certificate request](#)[Download a CA certificate, certificate chain, or CRL](#)

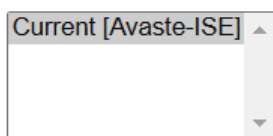
2. Select **Base-64 format**, then click **Download CA certificate**.

3. Save the certificate as **CA_Root.cer**.

Microsoft Active Directory Certificate Services -- Avaste-ISE**Download a CA Certificate, Certificate Chain, or CRL**

To trust certificates issued from this certification authority, [install this CA certificate](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:**Encoding method:**☐ DER☒ Base 64[Install CA certificate](#)[Download CA certificate](#)[Download CA certificate chain](#)[Download latest base CRL](#)[Download latest delta CRL](#)

4. **Log in** to the Stealthwatch Management Console (SMC).

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. **Navigate** to the **Trust Store** section and import previously exported CA_Root.cer certificate.

10. Click **Add New**.

Central Management Inventory Data Store Update Manager App Manager Smart Licensing Database

Inventory / Appliance Configuration

Appliance Configuration - Manager

smrc (10.106.127.50) / Last Updated: 2/8/2025, 5:30:58 PM by admin

Appliance Network Services **General**

☐ Enable FIPS Encryption Libraries

☐ Enable Common Criteria Encryption Libraries

SMTP Configuration

SMTP Server

Port

From Email

User Name

Password

Encryption Type

☒ SMTPS ☐ STARTTLS ☐ Un-Encrypted

Backup Configuration Encryption

☐ Enable Encryption

Backup Configuration Password

Confirm Password

External Services

☒ Enable Cisco Security Cloud Control

☒ Enable Customer Success Metrics

☒ Enable Threat Feed

Feed Confidence Level

7

DoDIN Notifications

☐ Enable

To Email

Trust Store

Add New

Friendly Name	Issued To	Issued By	Valid From	Valid To	Serial Number	Key Length	Actions
yy1nde2owmzmdu5ndc2m2rzm...	Secure Network Analytics	Secure Network Analytics	2024-06-20 20:17:15	2029-06-21 20:17:15	403cd116b1af4d3b71e9060afdb...	4096	Delete
fc751new.www.cisco.com	Secure Network Analytics	Secure Network Analytics	2024-06-23 12:14:09	2029-06-24 12:14:09	14e60739401a8e204c703b12279...	4096	Delete
AWS	Amazon	Amazon	2015-05-26 05:30:00	2038-01-17 05:30:00	66c9fc998f8c0a39e2f0788a43e69...	2048	Delete

5 items per page 1 - 3 of 3 items Page 1 of 1

11. Give the certificate a friendly name, then click **Select File...** to select the previously exported ISE CA certificate.

12. Click **Add Certificate** to save the changes.

Add Certification Authority Certificate

Friendly Name *

AVASTEROOTCA

Certificate File *

AVASTE_ROOT.cer

Select file...

Cancel Add Certificate

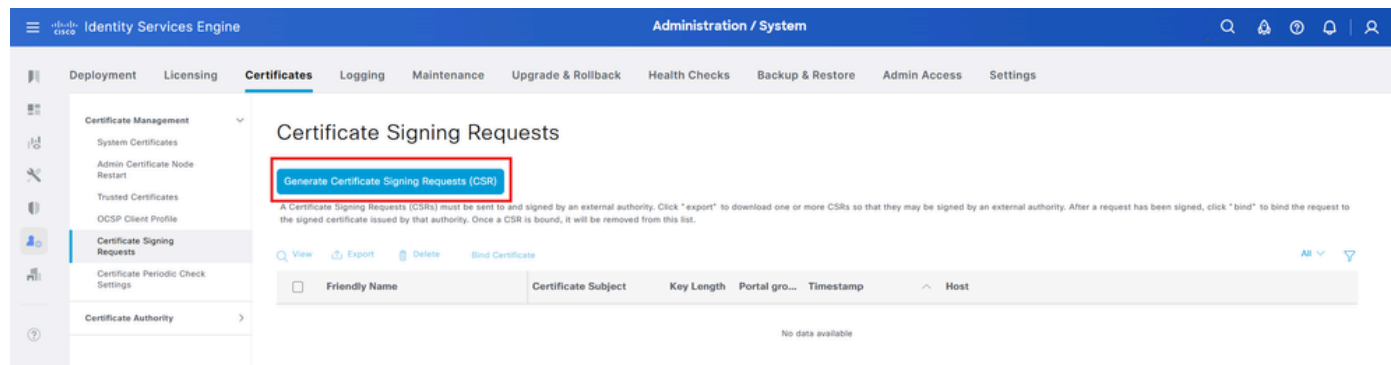
13. Click **Apply Settings** to save the changes.

Section B: Cisco Identity Services Engine 3.3 Certificate Configuration

PART I - Generating an ISE Server pxGrid Certificate

Generate a CSR for an ISE server pxGrid certificate:

1. **Log in** to Cisco Identity Services Engine (ISE) GUI.
2. **Navigate** to **Administration > System > Certificates > Certificate Management > Certificate Signing Requests**.
3. Select **Generate Certificate Signing Request (CSR)**.



4. Select **pxGrid** in the Certificate(s) is used for field.
5. Select **ISE node** for which the certificate is generated.
6. **Fill** in other certificates details as necessary.
7. Click **Generate**.

Usage

Certificate(s) will be used forpxGrid

Allow Wildcard Certificates

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☒ avasteise271	avasteise271#pxGrid

Subject

Common Name (CN)
SFQDNS

Organizational Unit (OU)
AAA

Organization (O)
Cisco

City (L)
Bangalore

State (ST)
KA

Country (C)
IN

Subject Alternative Name (SAN)

DNS Name

avasteise271.avaste.local

IP Address

10.127.197.128

* Key type

RSA

* Key Length

4096

* Digest to Sign With

SHA-384

Certificate Policies

Generate

Cancel

8. Click **Export** and **Save** the file locally.

✕

Successfully generated CSR(s) 

Certificate Signing request(s) generated:

avasteise271#pxGrid

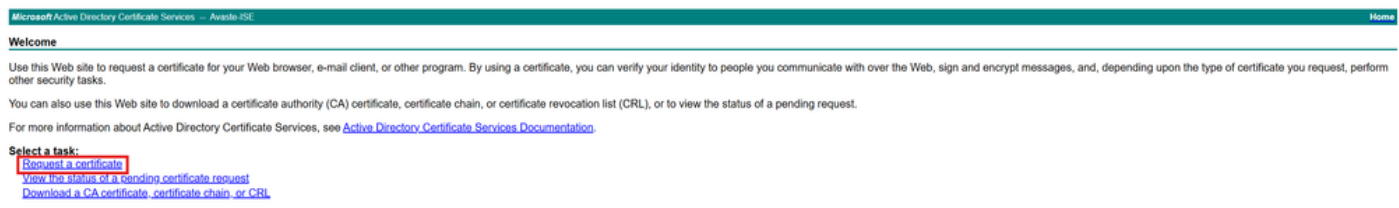
Click Export to download CSR(s) or OK to return to list of CSR(s) screen

OK

Export

PART II - Creating an ISE Server pxGrid Certificate Using an External CA

1. Navigate 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**.

Microsoft Active Directory Certificate Services -- Avaste-ISE

Request a Certificate

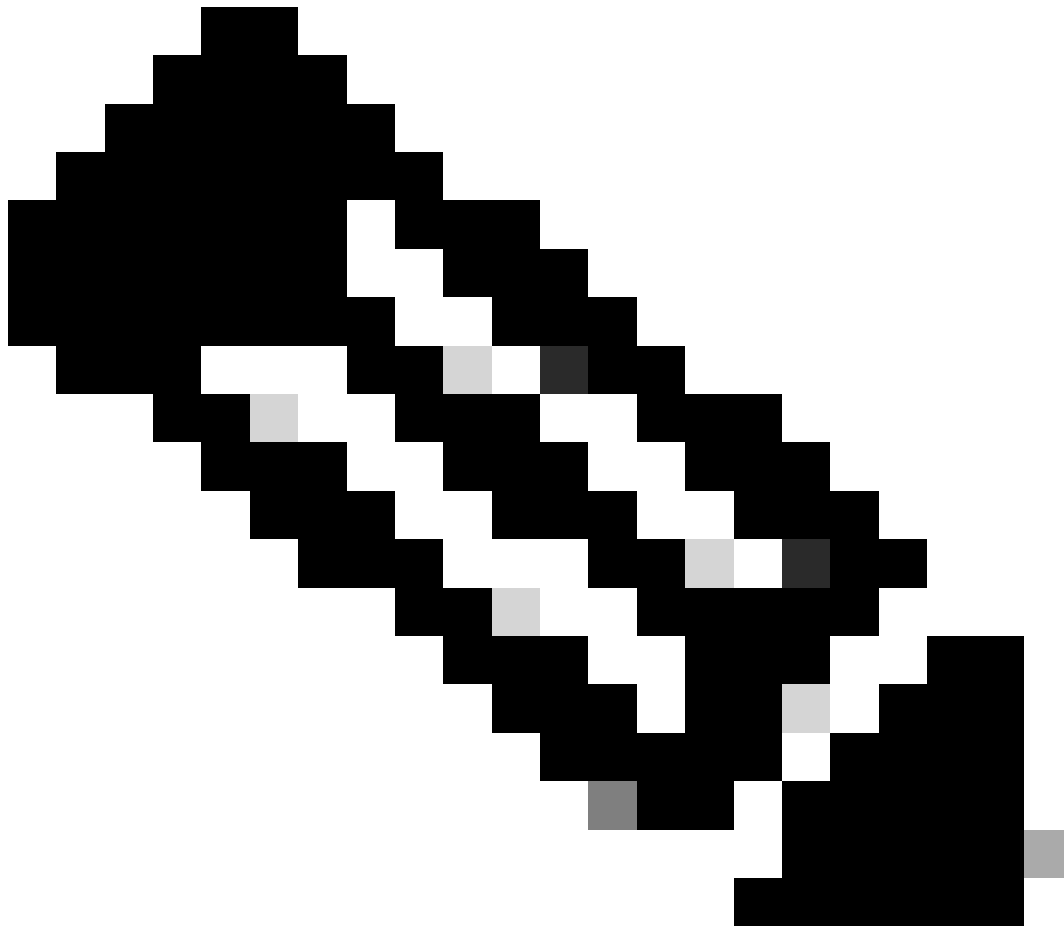
Select the certificate type:

[User Certificate](#)

Or, 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**.

A screenshot of the 'Submit a Certificate Request or Renewal Request' form. The form has a teal header with the text 'Microsoft Active Directory Certificate Services -- Avaste-ISE'. Below the header is a 'Submit a Certificate Request or Renewal Request' section with a description. The 'Saved Request:' section contains a text area with a base-64 encoded CSR. Below this is a 'Certificate Template:' dropdown menu with 'pxGrid' selected. There is also an 'Additional Attributes:' section with an 'Attributes:' text area. At the bottom right is a 'Submit >' button, which is highlighted with a red box.



Note: Certificate Template pxGrid used needs both Client authentication and server authentication in the "Enhanced Key Usage" field.

6. **Download** the generated certificate in **Base-64** format and **Save** it as ISE_pxGrid.cer.

Microsoft Active Directory Certificate Services -- Avaste-ISE

Certificate Issued

The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

PART III - Importing the CA Root Certificate into the ISE Trust Store

1. Navigate to MS Active Directory Certificate Service home page and select **Download a CA certificate, certificate chain, or CRL**.

Microsoft Active Directory Certificate Services -- Avaste-ISE

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

2. Select **Base-64** format, then click **Download CA certificate**.

Microsoft Active Directory Certificate Services -- Avaste-ISE

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [Avaste-ISE]

Encoding method:

☐ DER

☒ Base 64

[Install CA certificate](#)

[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

[Download latest delta CRL](#)

3. **Save** the certificate as CA_Root.cer.
4. **Log in** to Cisco Identity Services Engine (ISE) GUI.
5. Select **Administration > System > Certificates > Certificate Management > Trusted Certificates**.

Identity Services Engine Administration / System

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Admin Certificate Node Restart
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Settings
- Certificate Authority

Trusted Certificates

For disaster recovery it is recommended to export and backup all your trusted certificates.

[Edit](#) [+ Import](#) [Export](#) [Delete](#) [View](#) [show internal CA certificates](#)

Friendly Name	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Status
☐ Amazon root CA	Infrastructure Cisco Services	06 6C 9F CF 99 BF 8C 0A 39 E2 F0 78 8A 43 E5 96 36 ...	Amazon Root CA 1	Amazon Root CA 1	Tue, 26 May 2...	Sun, 17 Jan 2...	Enabled
☐ Baltimore CyberTrust Root	Cisco Services	02 00 00 B9	Baltimore CyberT...	Baltimore CyberT...	Sat, 13 May 2...	Tue, 13 May 2...	Enabled
☐ Cisco ECC Root CA 2099	Cisco Services	03	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 20...	Mon, 7 Sep 2...	Enabled
☐ Cisco Licensing Root CA	Cisco Services	01	Cisco Licensing R...	Cisco Licensing R...	Fri, 31 May 20...	Mon, 31 May ...	Enabled

6. Select **Import** > **Certificate file** and **Import** the root certificate.

7. Ensure the **Trust for authentication within ISE** check box is selected.

Identity Services Engine Administration / System

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Certificate Management System Certificates Admin Certificate Node Restart Trusted Certificates OCSP Client Profile Certificate Signing Requests Certificate Periodic Check Settings Certificate Authority

Import a new Certificate into the Certificate Store

* Certificate File **Choose File** AVASTE_ROOT.cer

Friendly Name

Trusted For:

☒ Trust for authentication within ISE

☐ Trust for client authentication and Syslog

☐ Trust for certificate based admin authentication

☐ Trust for authentication of Cisco Services

☐ Trust for Native IPsec certificate based authentication

☐ Validate Certificate Extensions

Description

Submit Cancel

8. Click **Submit**.

PART IV - Binding the ISE certificate to the Certificate Signing Request (CSR)

1. **Log in** to Cisco Identity Services Engine (ISE) GUI.

2. Select **Administration** > **System** > **Certificates** > **Certificate Management** > **Certificate Signing Requests**.

3. Select the CSR generated in the previous section, then click **Bind Certificate**.

Identity Services Engine Administration / System

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Certificate Management System Certificates Admin Certificate Node Restart Trusted Certificates OCSP Client Profile Certificate Signing Requests Certificate Periodic Check Settings Certificate Authority

Certificate Signing Requests

Generate Certificate Signing Requests (CSR)

A Certificate Signing Requests (CSR) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

Bind Certificate

	Friendly Name	Certificate Subject	Key Length	Portal gro...	Timestamp	Host
☒	avasteise271@pxGrid	CN=avasteise271.avaste...	4096		Sat, 8 Feb 2025	avasteise271

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**.

Identity Services Engine Administration / System

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Admin Certificate Node Restart
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests**
- Certificate Periodic Check Settings
- Certificate Authority

Bind CA Signed Certificate

* Certificate File Choose File ISE_pxgrid.cer

Friendly Name ISE-pxGRID

Validate Certificate Extensions ☐

Usage

☒ pxGrid: Use certificate for the pxGrid Controller

Submit Cancel

7. Click **Yes** if the system asks to replace the certificate.

8. Select **Administration > System > Certificates > System Certificates**.

9. You can see the created pxGrid certificate signed by the external CA in the list.

Identity Services Engine Administration / System

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates**
- Admin Certificate Node Restart
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Settings
- Certificate Authority

System Certificates

For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

[Edit](#) [Generate Self Signed Certificate](#) [Import](#) [Export](#) [Delete](#) [View](#)

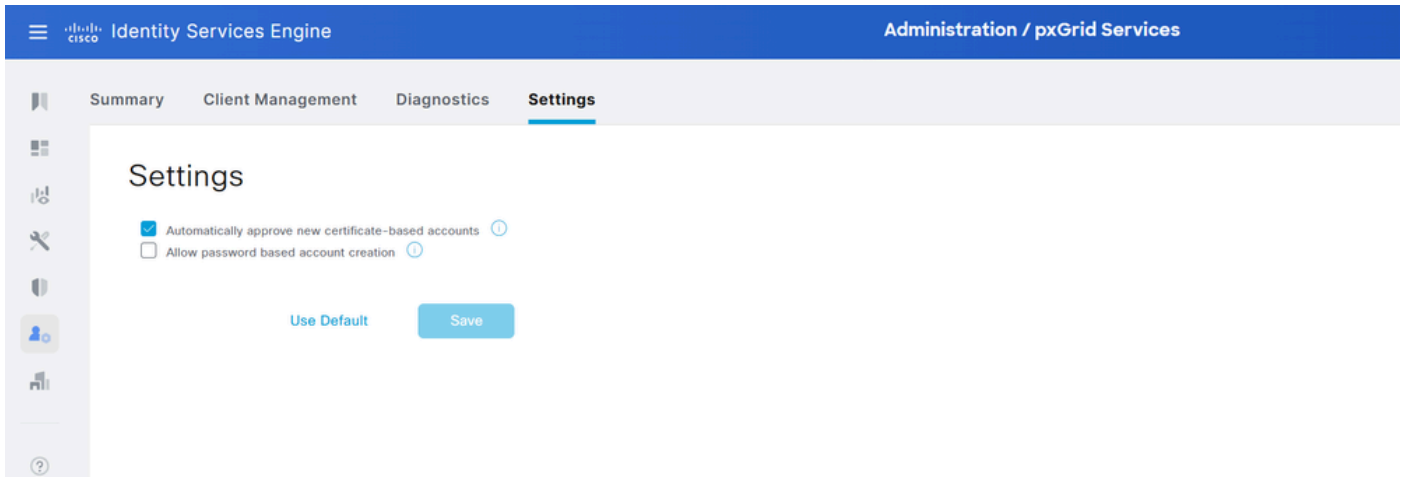
	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
▼ avasteise271								
☐	CN=avasteise271.avaste.local, OU=Certificate Services System Certificate/Certificate Services Endpoint Sub CA - avasteise271800002	Not in use		avasteise271.avaste.local	Certificate Services Endpoint Sub CA - avasteise271	Thu, 15 Aug 2024	Thu, 16 Aug 2029	Active
☐	Default self-signed server certificate	RADIUS DTLS		avasteise271.avaste.local	avasteise271.avaste.local	Fri, 16 Aug 2024	Tue, 2 Oct 2029	Active
☐	Default self-signed saml server certificate - CN=SAML_avasteise271.avaste.local	SAML		SAML_avasteise271.avaste.local	SAML_avasteise271.avaste.local	Fri, 16 Aug 2024	Wed, 15 Aug 2029	Active
☐	CN=avasteise271.avaste.local, OU=ISE Messaging Service/Certificate Services Endpoint Sub CA - avasteise271800003	ISE Messaging Service		avasteise271.avaste.local	Certificate Services Endpoint Sub CA - avasteise271	Thu, 15 Aug 2024	Thu, 16 Aug 2029	Active
☐	ISE-pxGRID	pxGrid		avasteise271.avaste.local	Avaste-ISE	Sat, 8 Feb 2025	Mon, 8 Feb 2027	Active
☐	AVASTE-2024	Admin, Portal, EAP Authentication	Default Portal Certificate Group	avasteise271.avaste.local	Avaste-ISE	Sun, 25 Aug 2024	Tue, 25 Aug 2026	Active

Certificates are now deployed, proceed for Integration.

Integrate

Before proceeding to integrate, ensure that:

For Cisco ISE under **Administration > pxGrid Services > Settings** and **Check** Automatically approve new certificate-based accounts for Client request to Auto-approve and **Save**.



On the Stealthwatch Management Console (SMC), To open ISE Configuration Setup Page:

1. Select **Configure > Integrations > Cisco ISE**.
2. In the upper right corner of the page, click **Add new configuration**.
3. Enter **Cluster Name**, Select the **certificate & Integration Product**, pxGrid node **IP** and Click **Save**.

Verify

Refresh the ISE Configuration page on the Stealthwatch Management Console (SMC).

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.

Cisco® ISE Configuration

Cisco® ISE Configurations

Cluster Name ↑ 1	pxgrid Nodes	User Name ↑ 2	Connection Status: Connected	Actions
ISE	10.127.197.128 ...	SMC	●	...

Add New Configuration

On Cisco ISE, navigate to **Administration >pxGrid Services > Client Management > Clients**.

This generates the SMC as a pxgrid client with the status **Enabled**.

Identity Services Engine

Administration / pxGrid Services

Summary

Client Management

Diagnostics

Settings

Clients

Policy

Groups

Certificates

pxGrid Cloud Policy

Clients

Clients must register and receive account approval to use pxGrid services in Cisco ISE. Clients use the pxGrid Client Library through the pxGrid SDK to register as clients. Cisco ISE supports both auto and manual registrations.

pxGrid Clients

Rows/Page

1

<<

<

1

>

>>

Go

1 Total Rows

Trash

Edit

Enable

Disable

Approve

Decline

Filter

☐	Name	Description	Client Groups	Status
☐	smc	Account for SW		● Enabled

To verify topic subscription on Cisco ISE, navigate to **Administration >pxGrid Services > Diagnostics > Websocket > Topics**

This produces an SMC subscribed to these topics.

Trustsec SGT topic

▼ /topic/com.cisco.ise.config.trustsec.security.group	0	1
--	---	---

Rows/Page

10

<<

<

1

>

>>

Go

1 Total Rows

Connection Name	Messaging Role
SMC	Sub

ISE Session directory topic

▼ /topic/com.cisco.ise.session	1	1
--------------------------------	---	---

Rows/Page	10	▼	1	/ 1 > >	Go	2 Total Rows
-----------	----	---	---	---------	----	--------------

Connection Name	Messaging Role
~ise-mnt-avasteise271	Pub
SMC	Sub

ISE SXP Bindings topic

▼ /topic/com.cisco.ise.sxp.binding	0	1
------------------------------------	---	---

Rows/Page	10	▼	1	/ 1 > >	Go	1 Total Rows
-----------	----	---	---	---------	----	--------------

Connection Name	Messaging Role
SMC	Sub

Cisco ISE Pxgrid-server.log in TRACE level.

```

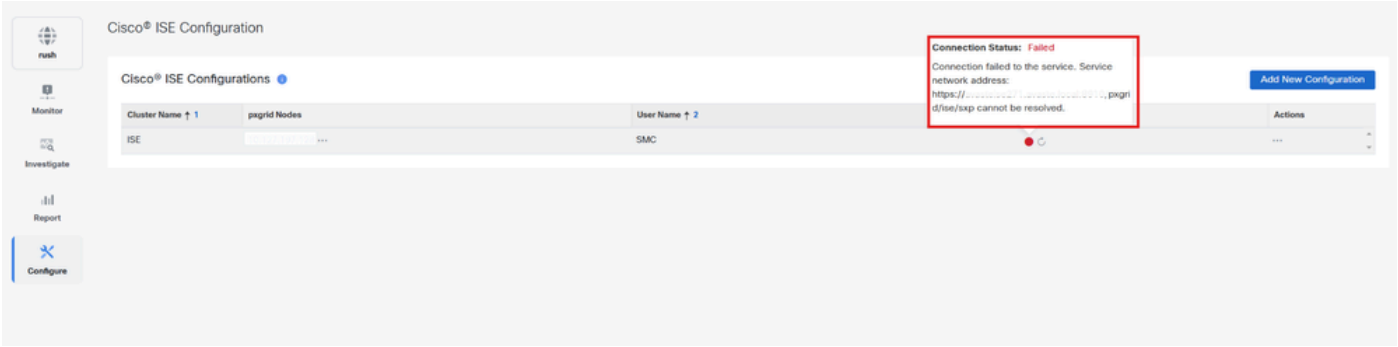
2025-02-08 18:07:11,086 TRACE [pxgrid-http-pool15][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribu
2025-02-08 18:07:11,087 TRACE [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint
2025-02-08 18:07:11,102 TRACE [pxgrid-http-pool19][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint
2025-02-08 18:07:11,110 DEBUG [pxgrid-http-pool22][[]] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::
2025-02-08 18:07:11,111 DEBUG [pxgrid-http-pool22][[]] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::
2025-02-08 18:07:11,111 DEBUG [pxgrid-http-pool22][[]] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::
2025-02-08 18:07:11,111 DEBUG [pxgrid-http-pool22][[]] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::
2025-02-08 18:07:11,111 DEBUG [pxgrid-http-pool22][[]] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::
2025-02-08 18:07:11,112 DEBUG [pxgrid-http-pool22][[]] cisco.cpm.pxgridwebapp.data.AuthzDaoImpl -:::
2025-02-08 18:07:11,321 DEBUG [pxgrid-http-pool19][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribu
2025-02-08 18:07:11,322 DEBUG [pxgrid-http-pool20][[]] cisco.cpm.pxgridwebapp.config.AuthzEvaluator -:
2025-02-08 18:07:11,322 INFO [pxgrid-http-pool19][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint
2025-02-08 18:07:11,323 TRACE [pxgrid-http-pool19][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint
2025-02-08 18:07:11,323 TRACE [WsIseClientConnection-1010][[]] cpm.pxgrid.ws.client.WsEndpoint -:::
2025-02-08 18:07:11,323 TRACE [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint
2025-02-08 18:07:11,323 TRACE [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint
2025-02-08 18:07:11,324 TRACE [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint
2025-02-08 18:07:11,324 TRACE [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribu
2025-02-08 18:07:11,324 TRACE [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribu
2025-02-08 18:07:11,324 TRACE [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribu
2025-02-08 18:07:11,324 TRACE [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribu
2025-02-08 18:07:11,324 TRACE [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribu
2025-02-08 18:07:11,324 TRACE [sub-sender-0][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionSender -:::

```


Troubleshooting

DNS Resolution Issue

This produces an error message as "Connection Status; Failed Connection failed to the service. Service network address: <https://isehostnameeme.domain.com:891pxgridiisessxpxp> cannot be resolved":



Solution

This ideally needs to be fixed on the DNS server for forward and reverse lookups for this ISE FQDN. But a temporary workaround can be added for local resolution:

1. Log in to the **Stealthwatch Management Console (SMC)**.
2. From the main menu, select **Configure > Global > Central Management**.
3. On the Inventory page, **click the (Ellipsis) icon** for the Manager.
4. Choose **Edit Appliance Configuration**.
5. **Network Services** tab and add a local resolution entry for this ISE FQDN.



Unknown CA Error or Trusted Certificate Missing

This produces an error message as "ISE is presenting a certificate that is not trusted by this Manager":



Similar log reference can be seen oSMCMsvcvise-client.log file. Path: catlancopepe/var/logs/containsvcvise-client.log

```
snasmc1 docker/svc-ise-client[1453]: java.util.concurrent.ExecutionException: javax.net.ssl.SSLException:
snasmc1 docker/svc-ise-client[1453]: at java.base/java.util.concurrent.CompletableFuture.reportGet(CompletableFuture.java:356)
snasmc1 docker/svc-ise-client[1453]: at java.base/java.util.concurrent.CompletableFuture.get(CompletableFuture.java:1960)
snasmc1 docker/svc-ise-client[1453]: at org.springframework.web.socket.client.jetty.JettyWebSocketClient.doHandshake(JettyWebSocketClient.java:100)
snasmc1 docker/svc-ise-client[1453]: at java.base/java.util.concurrent.FutureTask.run(FutureTask.java:284)
snasmc1 docker/svc-ise-client[1453]: at java.base/java.lang.Thread.run(Thread.java:829)
snasmc1 docker/svc-ise-client[1453]: Caused by: javax.net.ssl.SSLException: org.bouncycastle.tls.TlsFatalAlert(1): TLS_FATAL_ALERTING
snasmc1 docker/svc-ise-client[1453]: at org.bouncycastle.jsse.provider.ProvSSLEngine.unwrap(ProvSSLEngine.java:100)
snasmc1 docker/svc-ise-client[1453]: at java.base/javax.net.ssl.SSLEngine.unwrap(SSLEngine.java:637)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection.unwrap(SslConnection.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection$DecryptedEndPoint.fill(SslConnection$DecryptedEndPoint.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.client.http.HttpReceiverOverHTTP.process(HttpReceiverOverHTTP.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.client.http.HttpReceiverOverHTTP.receive(HttpReceiverOverHTTP.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.client.http.HttpChannelOverHTTP.receive(HttpChannelOverHTTP.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.client.http.HttpConnectionOverHTTP.onFillable(HttpConnectionOverHTTP.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.AbstractConnection$ReadCallback.succeeded(AbstractConnection$ReadCallback.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.FillInterest.fillable(FillInterest.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection$DecryptedEndPoint.onFillable(SslConnection$DecryptedEndPoint.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection.onFillable(SslConnection.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection$2.succeeded(SslConnection$2.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.FillInterest.fillable(FillInterest.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.SelectableChannelEndPoint$1.run(SelectableChannelEndPoint$1.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.util.thread.QueuedThreadPool.runJob(QueuedThreadPool.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.util.thread.QueuedThreadPool$Runner.run(QueuedThreadPool$Runner.java:100)
snasmc1 docker/svc-ise-client[1453]: ... 1 more
snasmc1 docker/svc-ise-client[1453]: Suppressed: javax.net.ssl.SSLHandshakeException: org.bouncycastle.tls.TlsFatalAlert(1): TLS_FATAL_ALERTING
```

Solution

1. Log in to the **Stealthwatch Management Console (SMC)**.
2. From the main menu, select **Configure > Global > Central Management**.
3. On the Inventory page, **click the (ellipsis) icon** for the Manager.
4. Choose **Edit Appliance Configuration**.
5. Select the **General** tab.
6. **Navigate** to the **Trust Store** section and **ensure** that the issuer of the Pxgridid certificate of Cisco ISE is part of the Trust store.

Known Defects

Bug ID	Description
Cisco bug ID 18119	ISE is Selecting Unsupported Cipher ITLS Server Hello Packet
Cisco bug ID 01634	Unable to quarantine devices using EPS condition