Integrate ISE 3.3 with Stealthwatch 7.5.1 Using External CA

Contents

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.

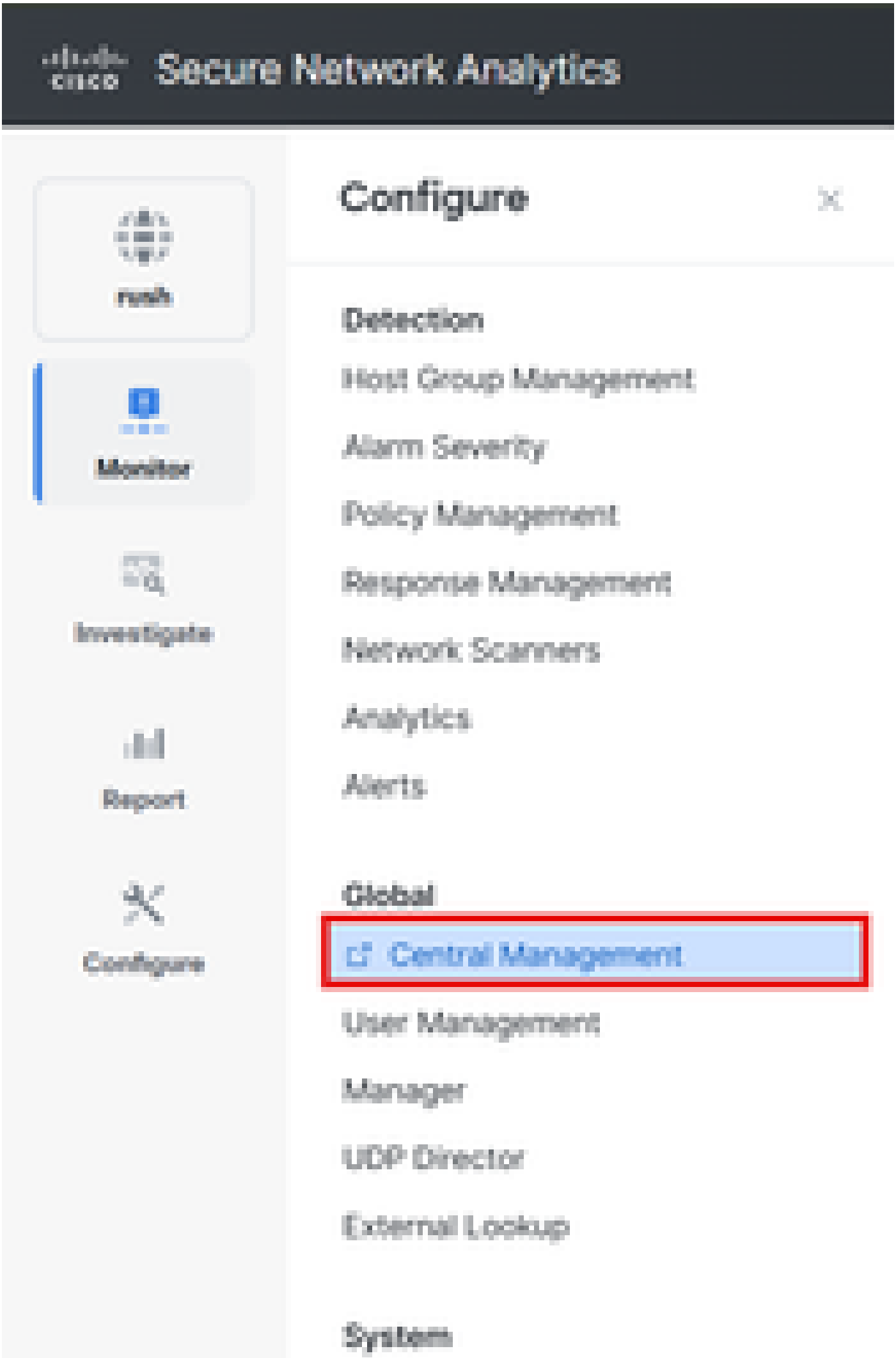
Configure

Section A: Secure Network Analytics (Stealthwatch) Certificate Configuration

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

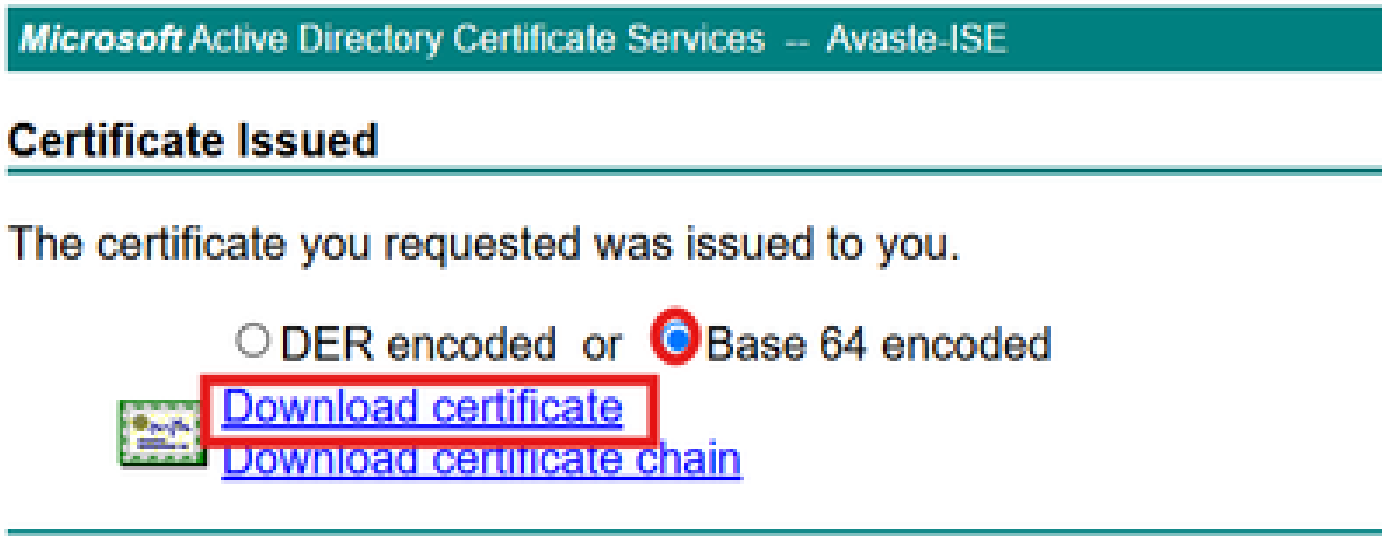
1. Log in to **Stealthwatch Management Console** (SMC).

2. From the main menu, select **Configure > Global > Central Management**.


Secure Network Analytics
rush
Monitor
Investigate
Report
Configure
Configure
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.



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

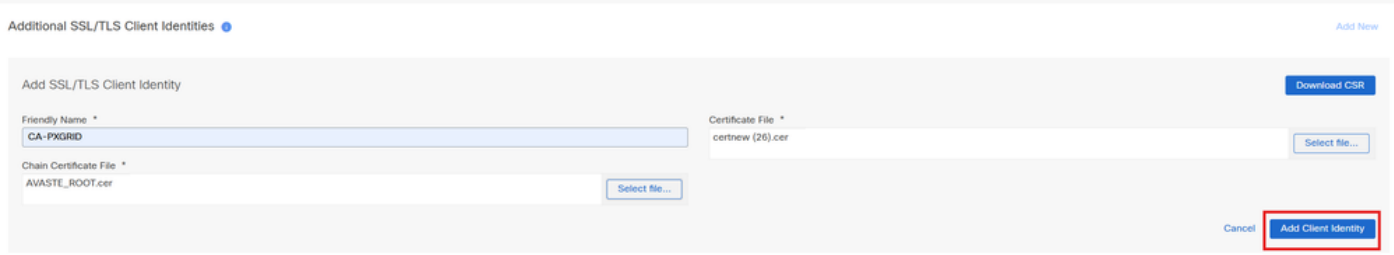
1.**Navigate** to the **Additional SSL/TLS Client Identities** section of the Manager Configuration in **Central Management**.

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.

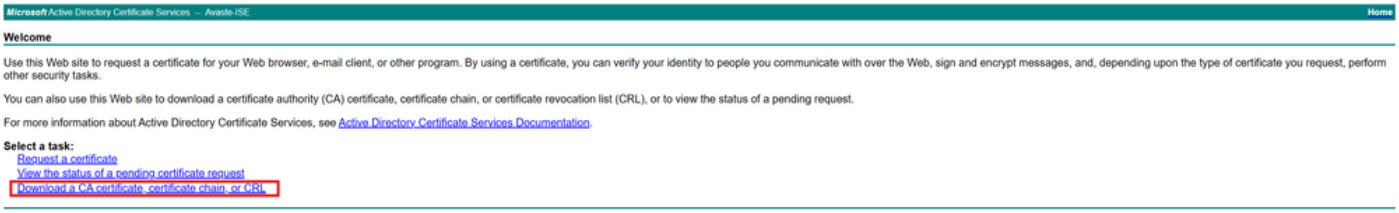
5. Click **Add Client Identity** to add the certificate to the system.



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

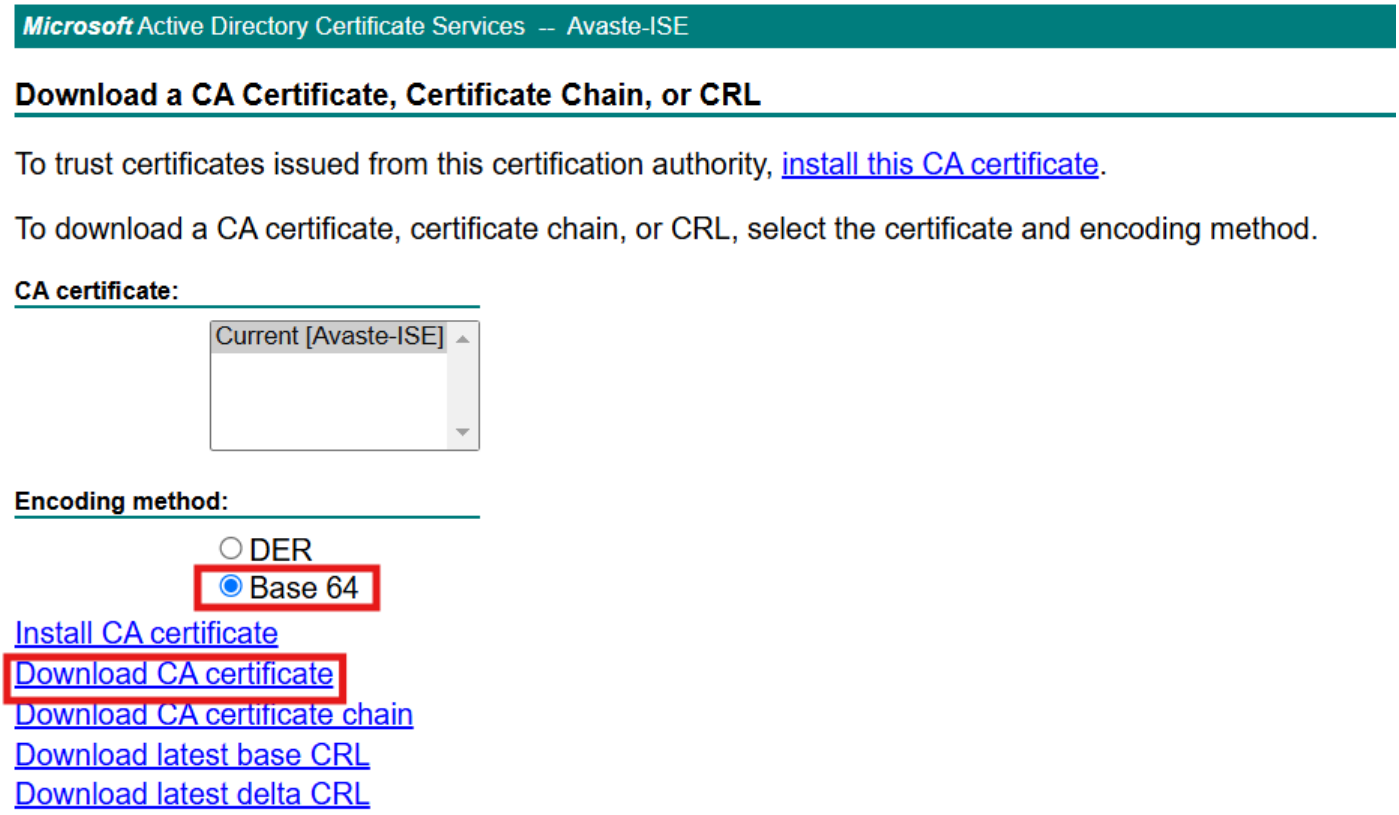
PART IV - Importing the CA Root Certificate into the Manager Trust Store

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



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

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



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

5. From the main menu, select **Configure > Global > Central Management.**

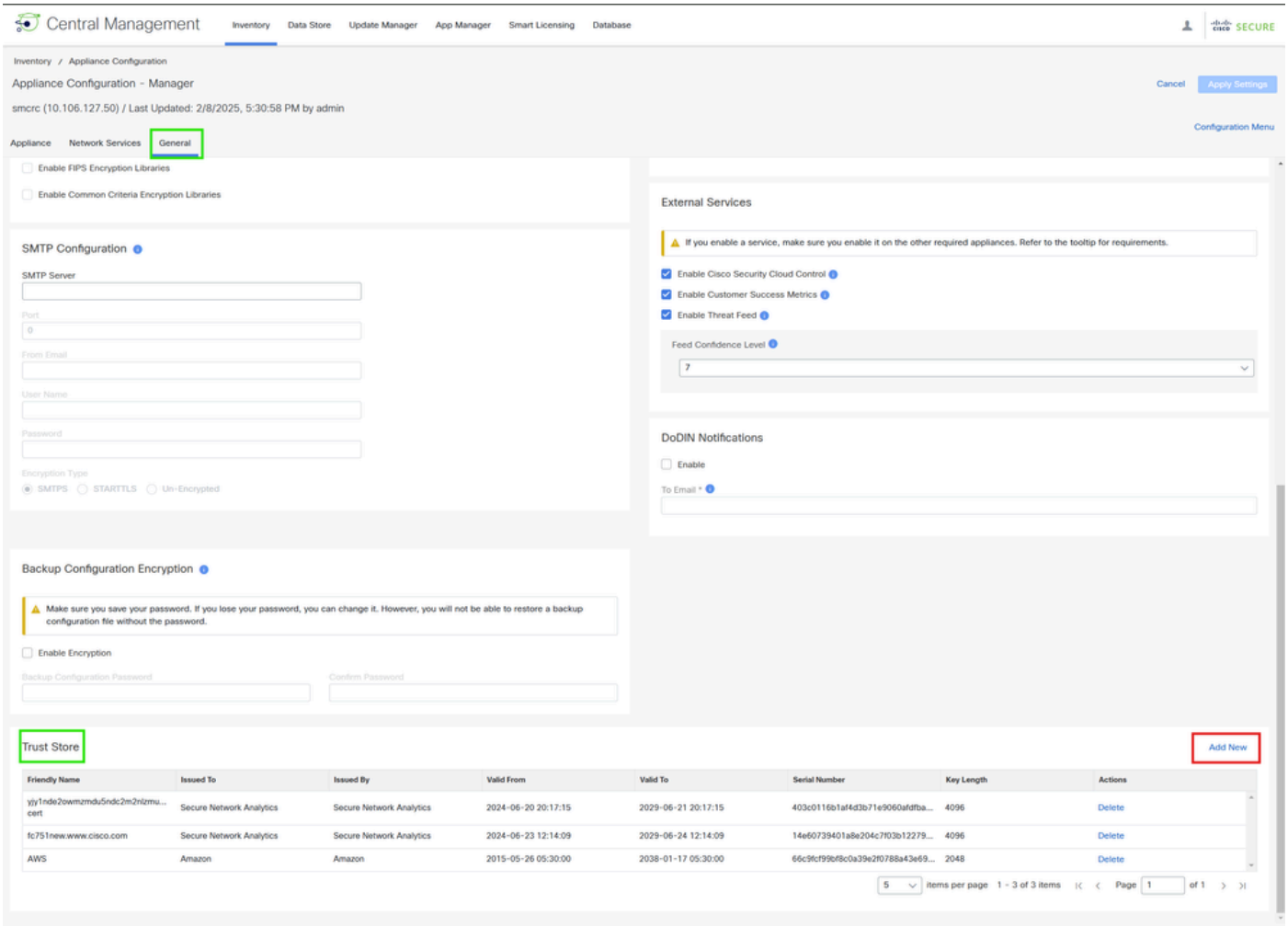
6. On the **Inventory** page, **click the (ellipsis)** icon for the Manager.

7. Choose **Edit Appliance Configuration.**

8. Select the **General** tab.

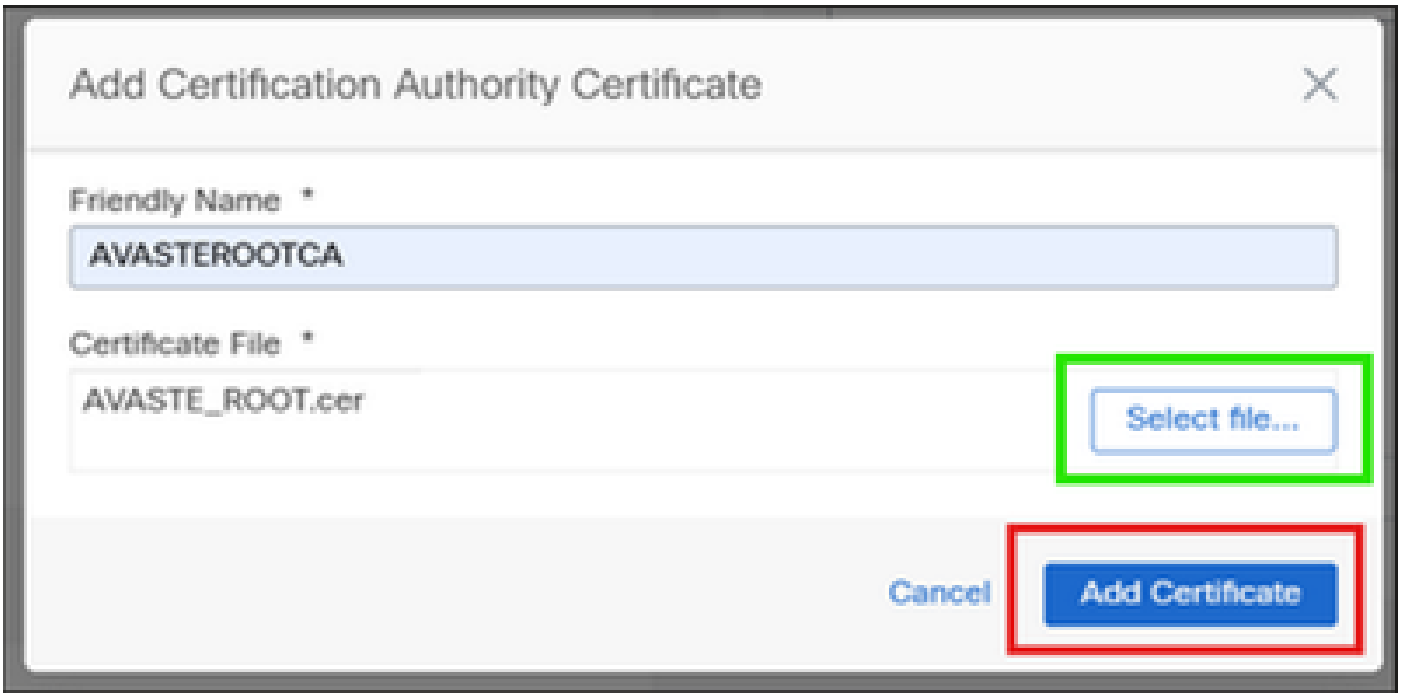
9. **Navigate** to the **Trust Store** section and import previously exported CA_Root.cer certificate.

10. Click **Add New.**



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.



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

Section B: Cisco Identity Services Engine 3.3 Certificate Configuration

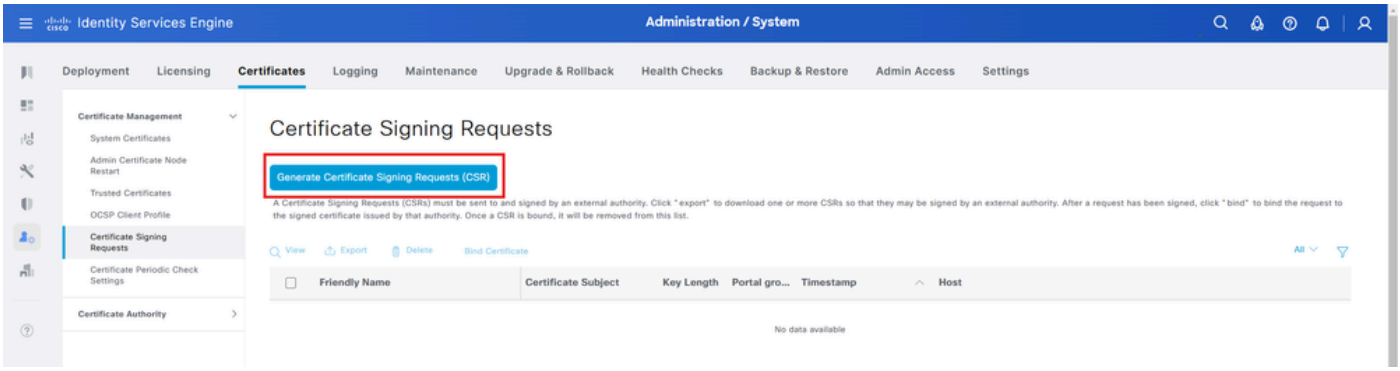
PART I - Generating an ISE Server pxGrid Certificate

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).**

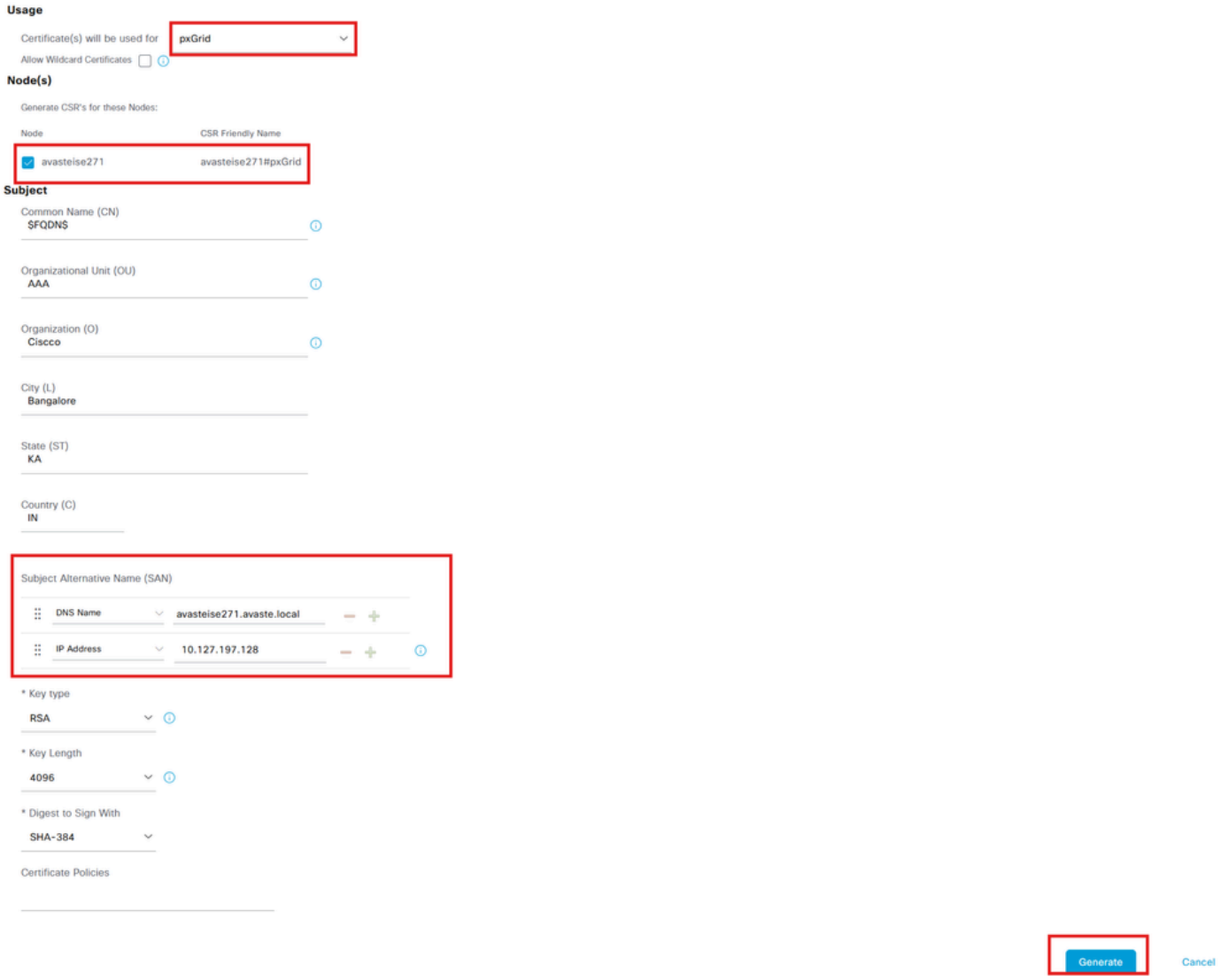


4. Select **pxGrid** in the Certificate(s) is used for field.

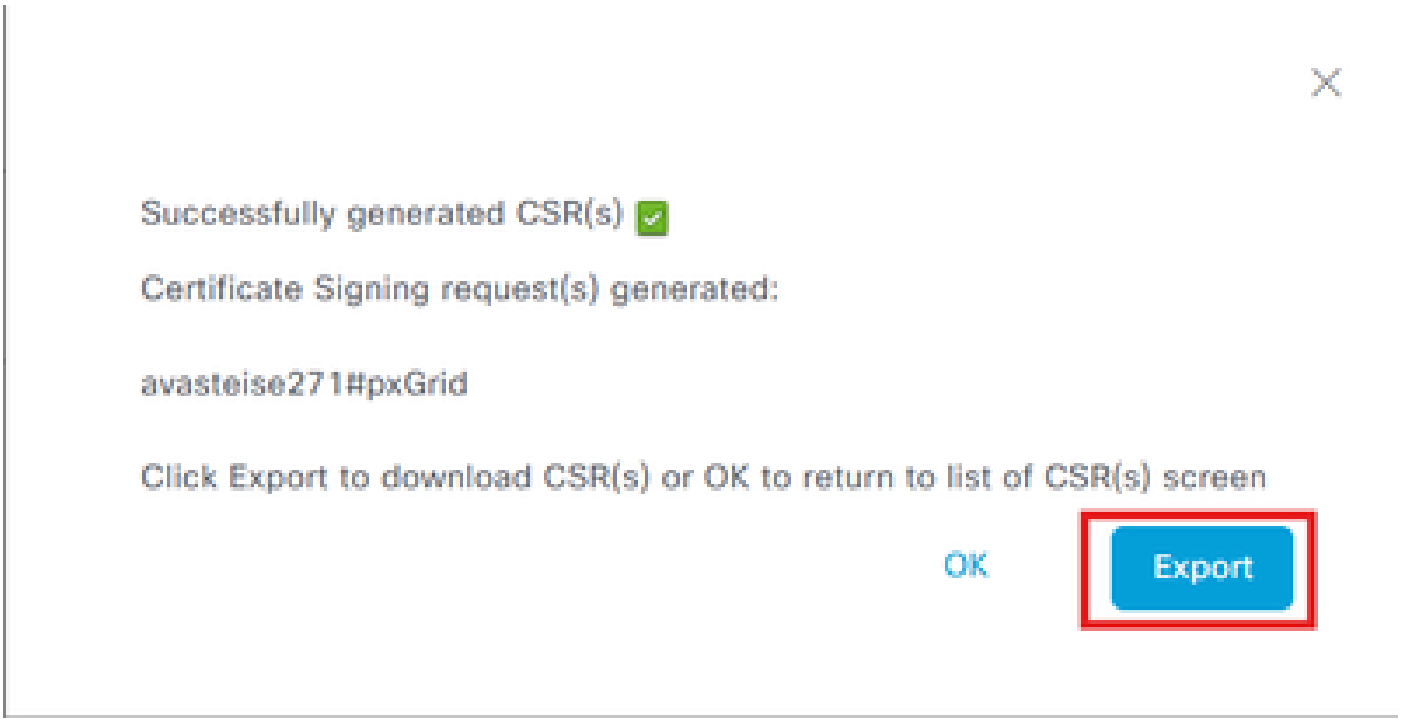
5. Select **ISE node** for which the certificate is generated.

6. **Fill** in other certificates details as necessary.

7. Click **Generate**.



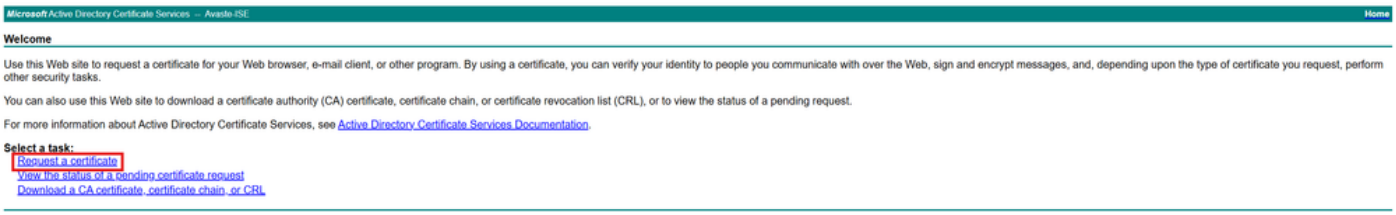
8. Click **Export** and **Save** the file locally.



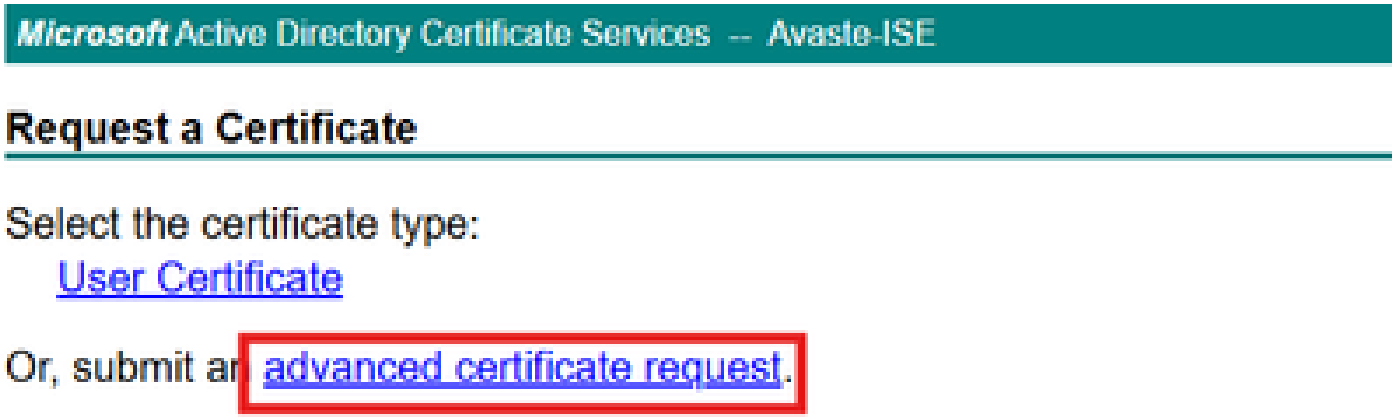
PART II - Creating an ISE Server pxGrid Certificate Using an External CA

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.**

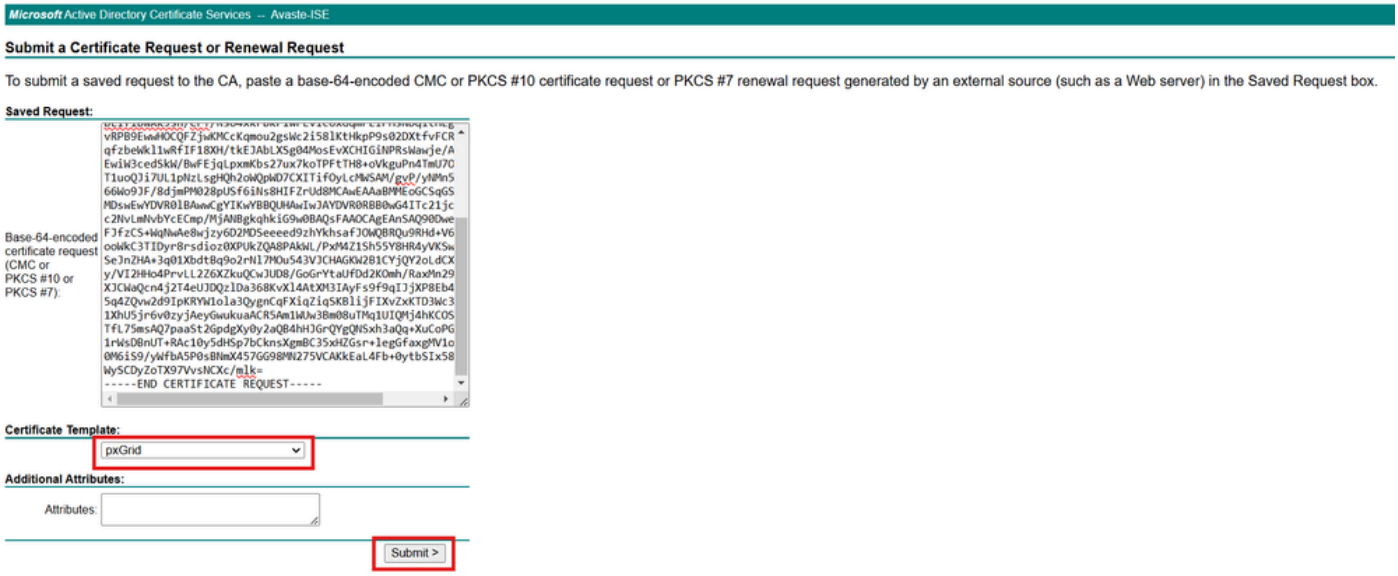


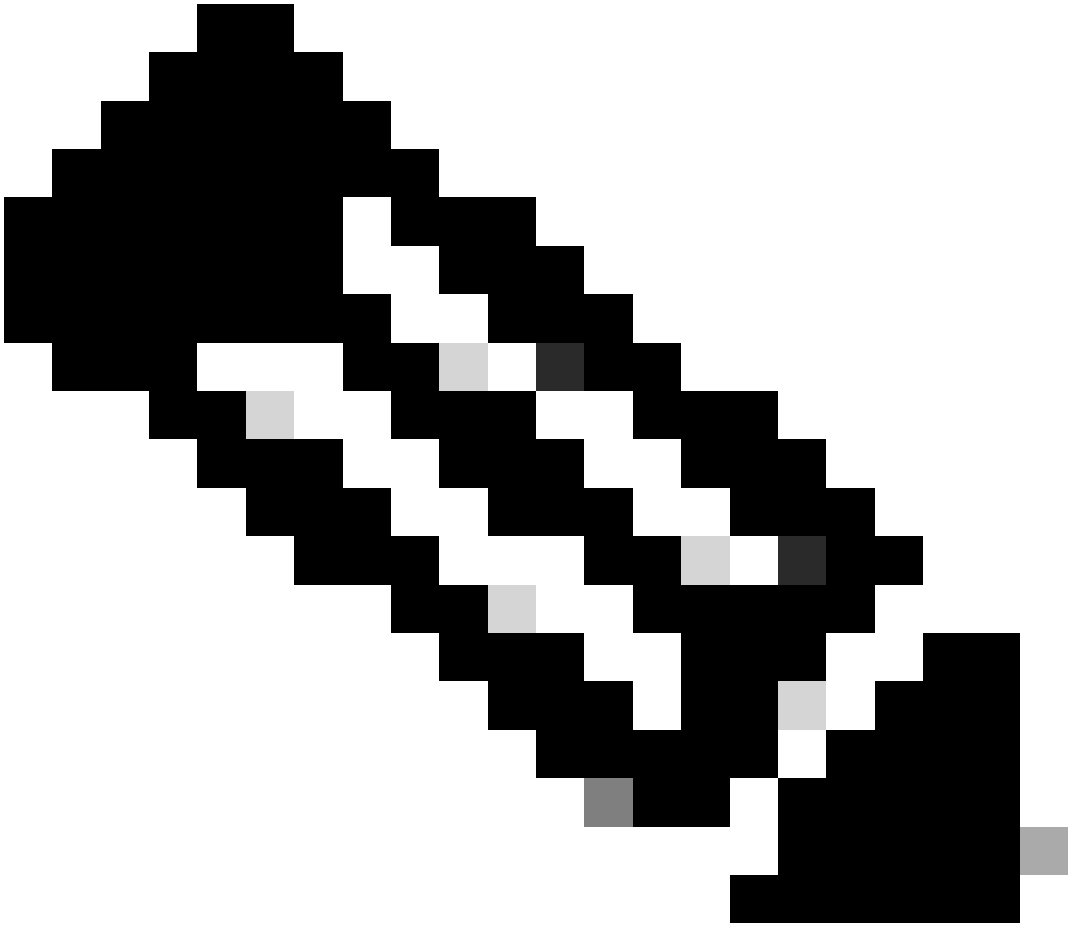
3. Choose to submit an **advanced certificate request.**



4. **Copy** the contents of the CSR generated in the previous section into the **Saved Request field.**

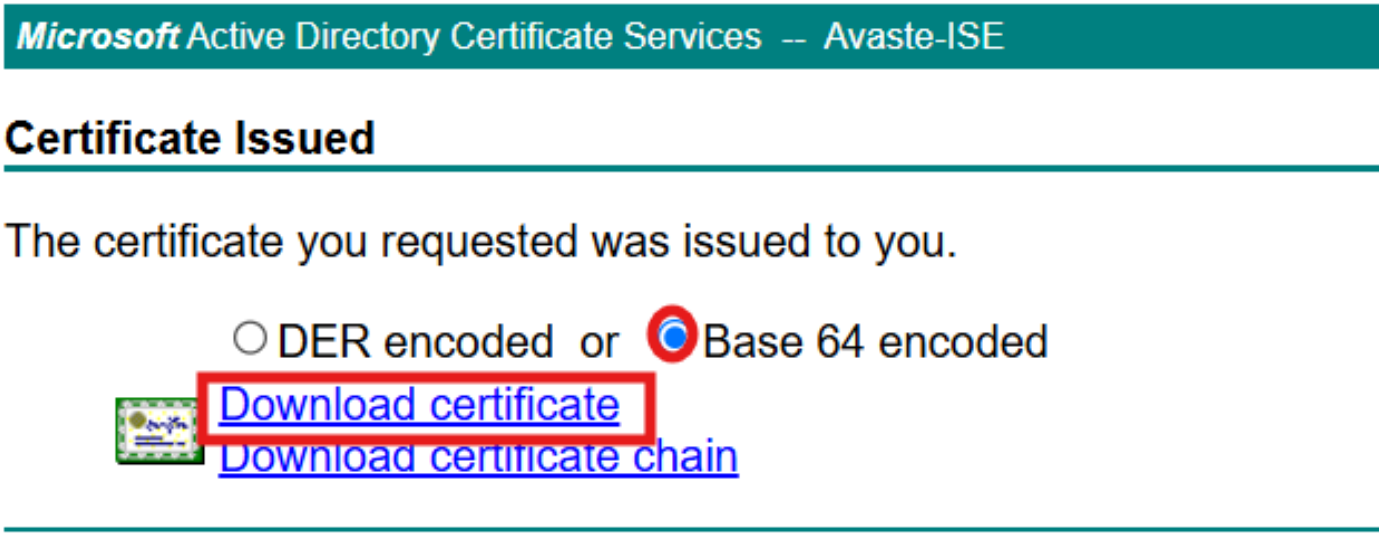
5. Select **pxGrid** as the **Certificate Template**, then click **Submit**.





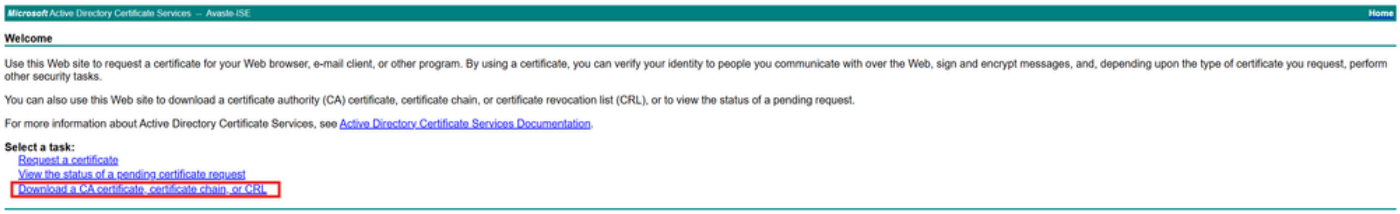
Note: Certificate Template pxGrid used needs both Client authentication and server authentication in the "Enhanced Key Usage" field.

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

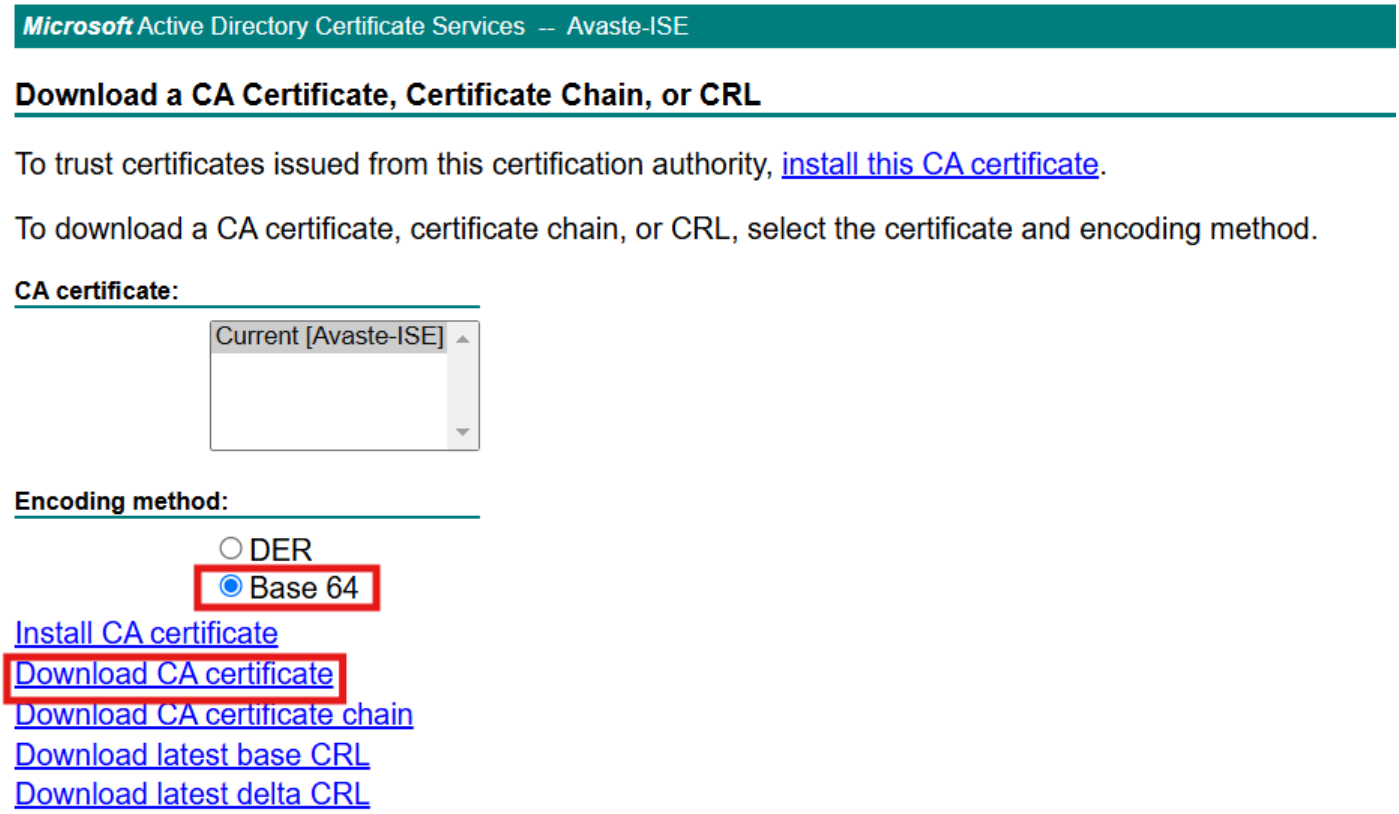


PART III - Importing the CA Root Certificate into the ISE Trust Store

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



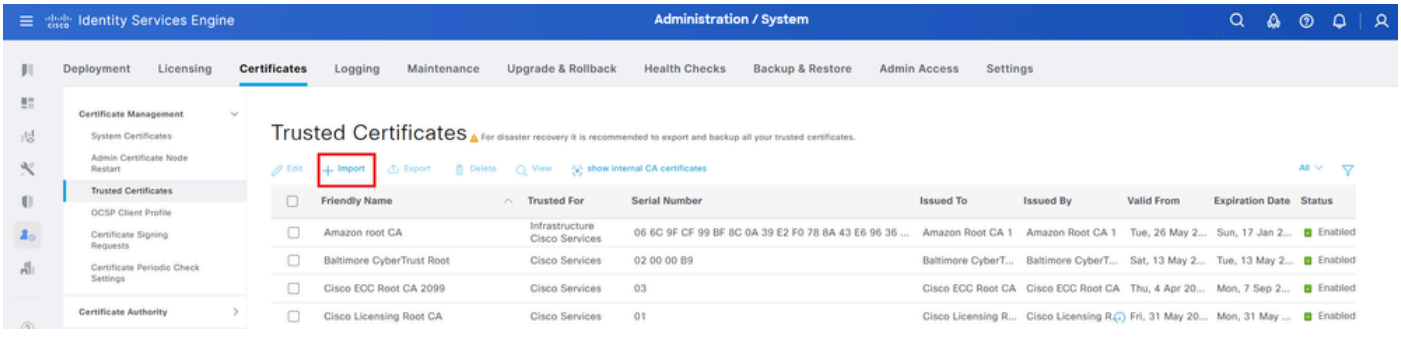
2. Select **Base-64** format, then click **Download** CA certificate.



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

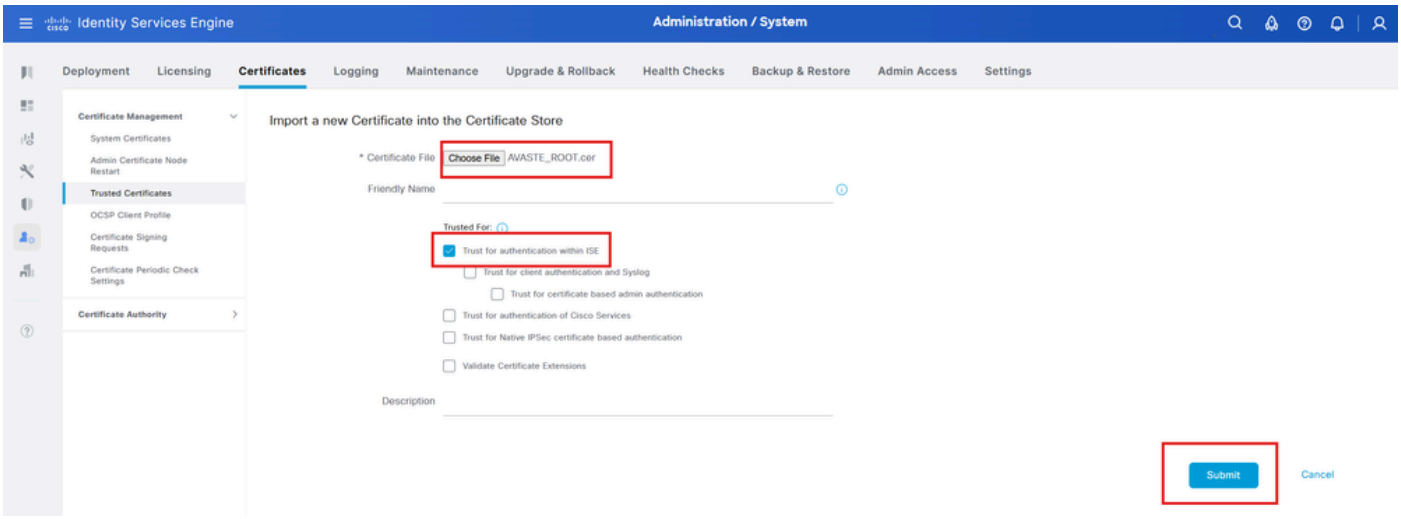
4. **Log in** to Cisco Identity Services Engine (ISE) GUI.

5. Select **Administration > System > Certificates > Certificate Management >Trusted Certificates.**



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

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



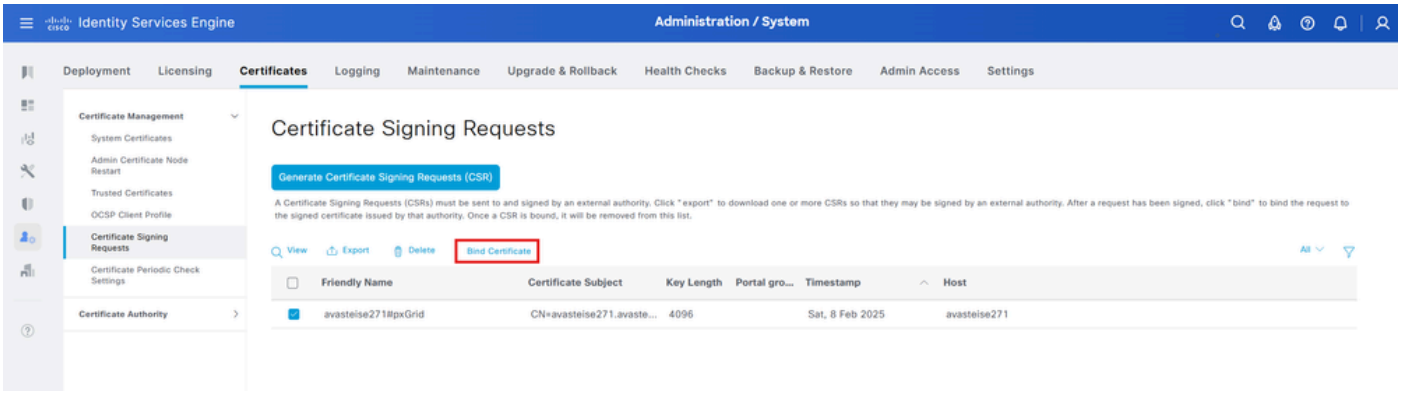
8. Click **Submit**.

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

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

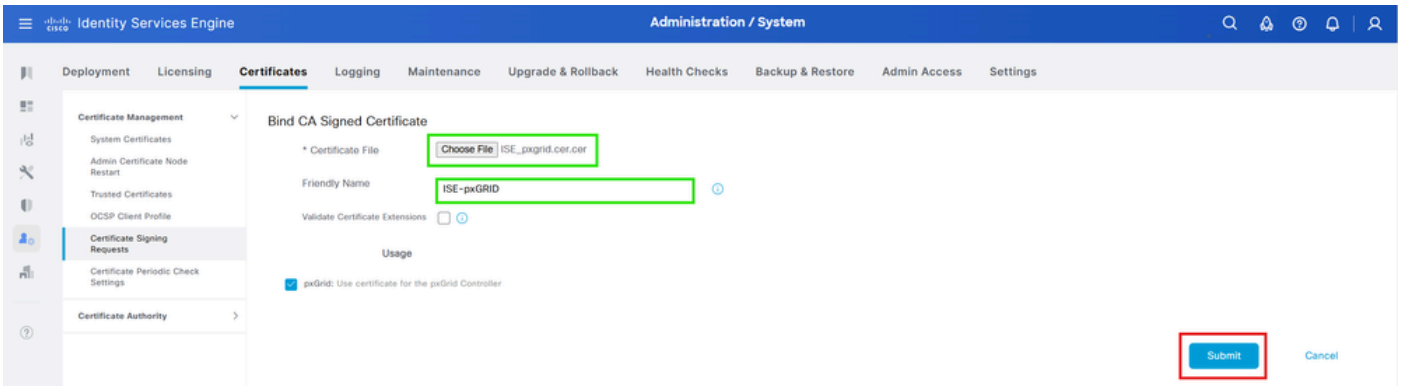
2. Select **Administration > System > Certificates > Certificate Management >Certificate Signing Requests.**

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



4. On the Bind CA Signed Certificate form, **choose** the ISE_pxGrid.cer certificate generated previously.

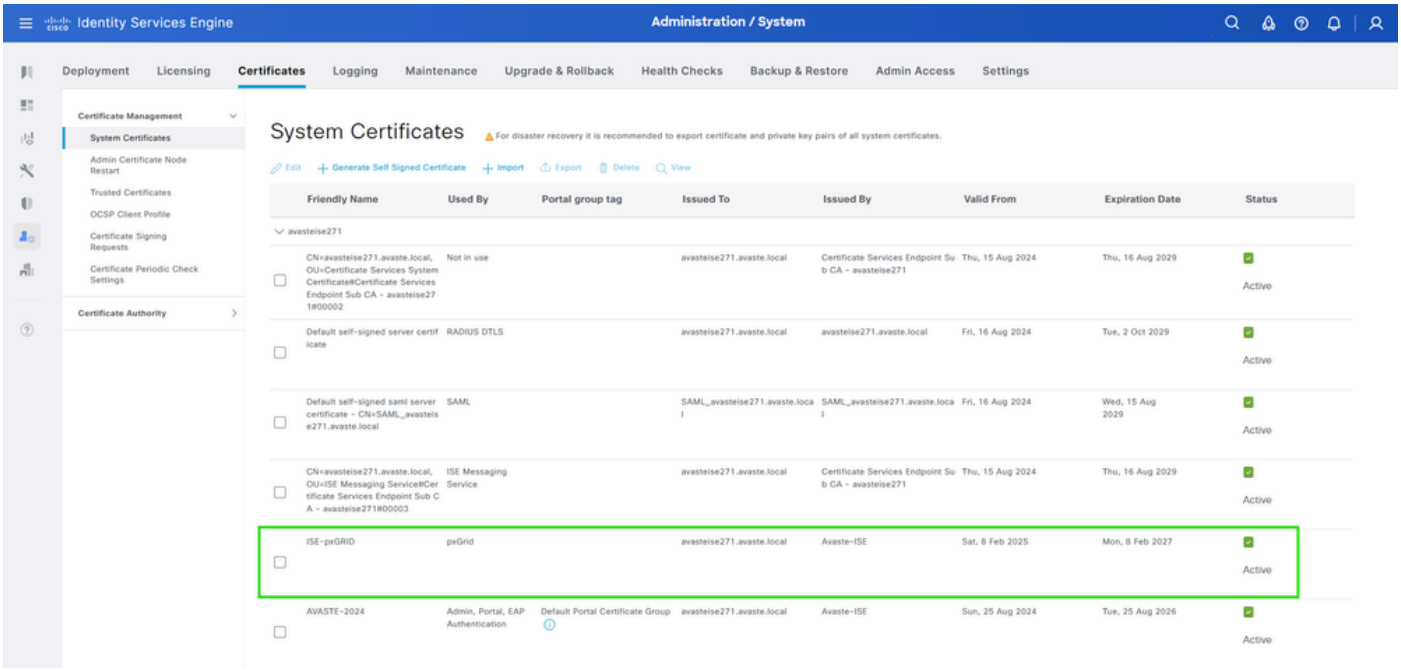
5. Give the certificate a friendly name, then click **Submit**.



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.

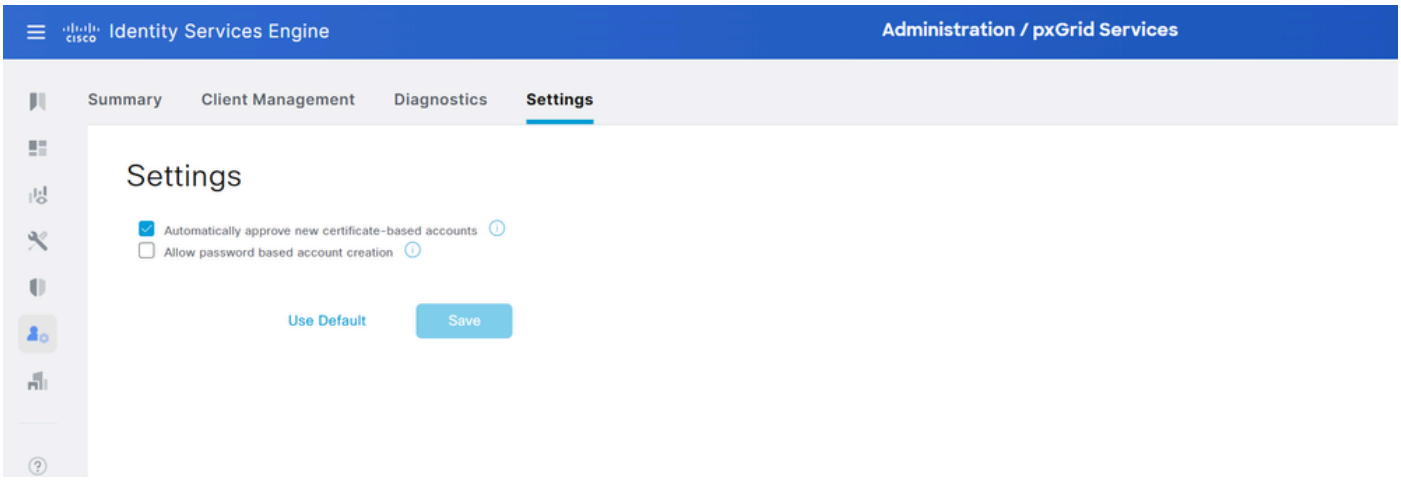


Certificates are now deployed, proceed for Integration.

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**.

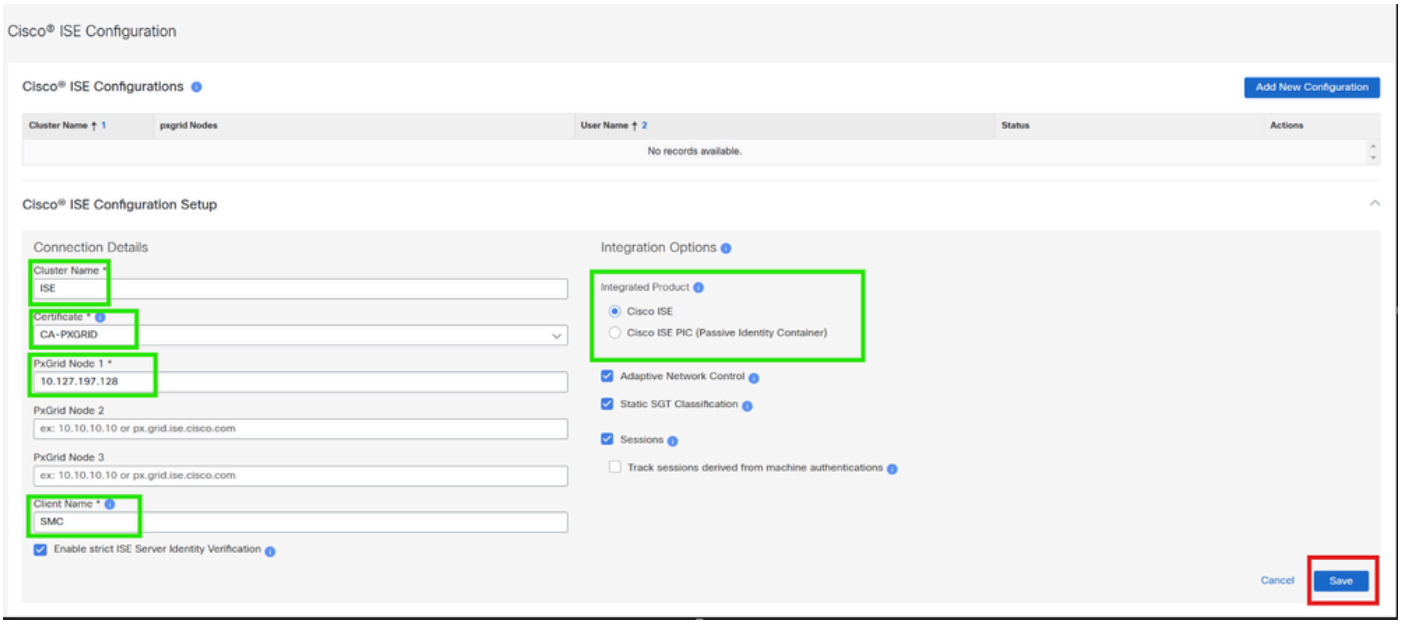


On the Stealthwatch Management Console (SMC), To open ISE Configuration Setup Page:

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**.

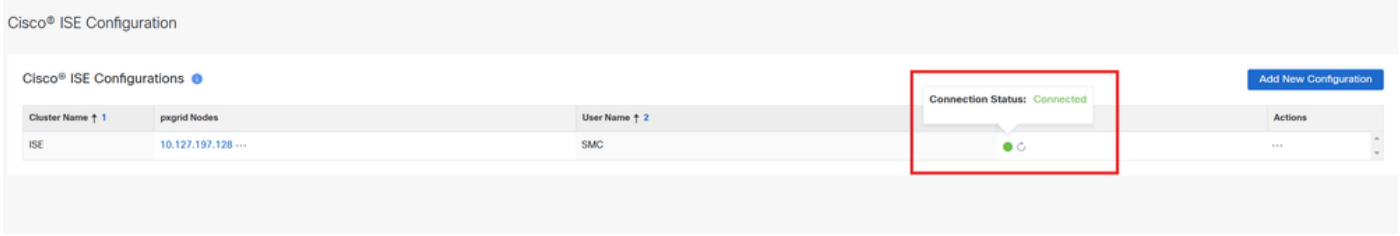


Verify

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

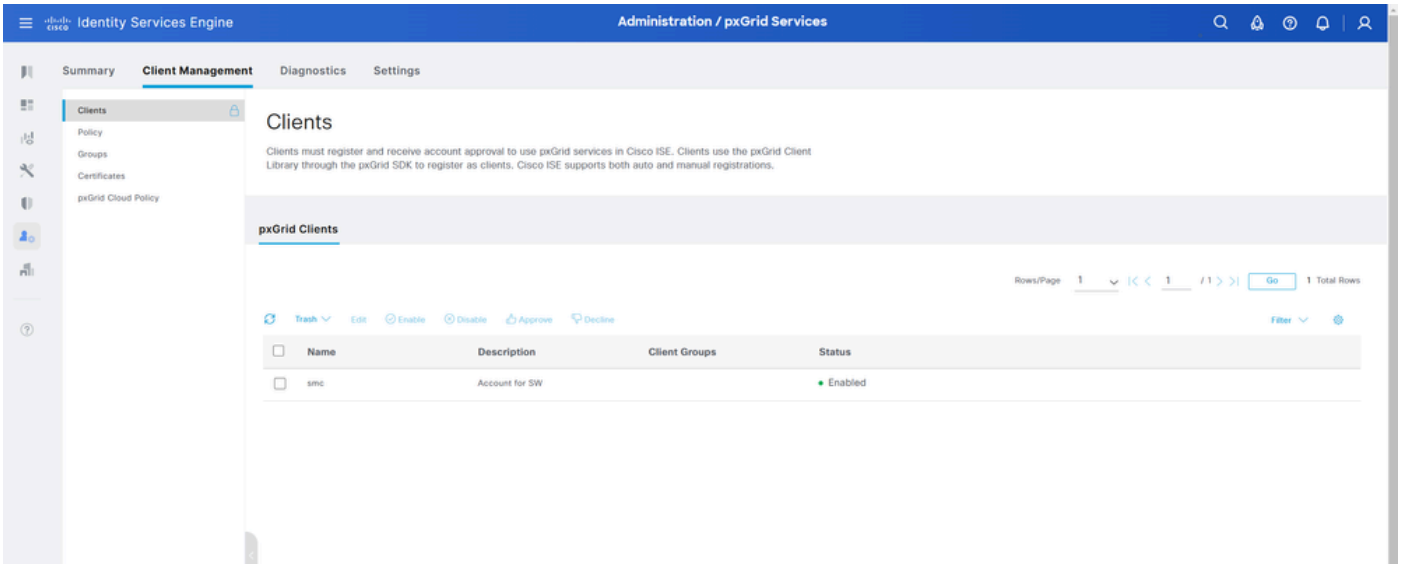
1. **Return** to the ISE Configuration page in the Web App and refresh the page.

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.



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

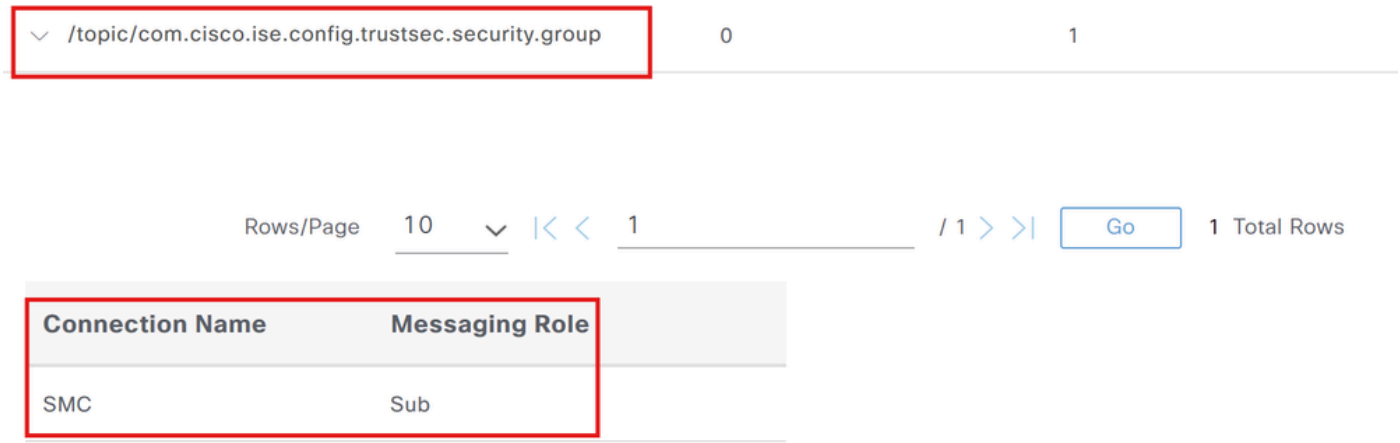
This generates the SMC as a pxgrid client with the status **Enabled**.



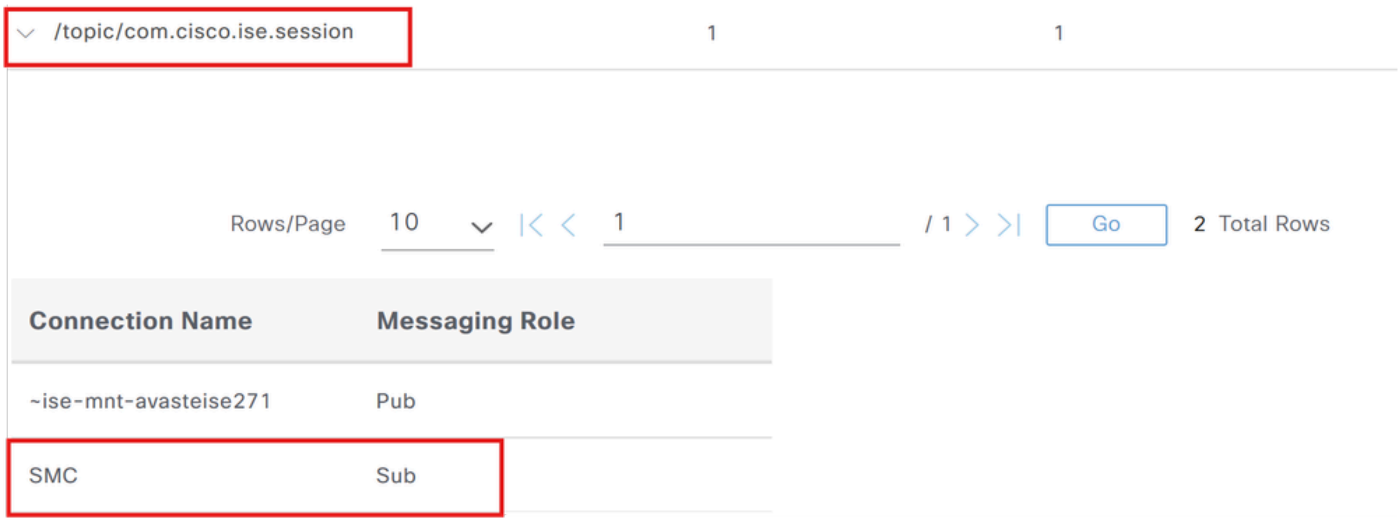
To verify topic subscription on Cisco ISE, navigate to **Administration >pxGrid Services > Diagnostics > Websocket > Topics**

This produces an SMC subscribed to these topics.

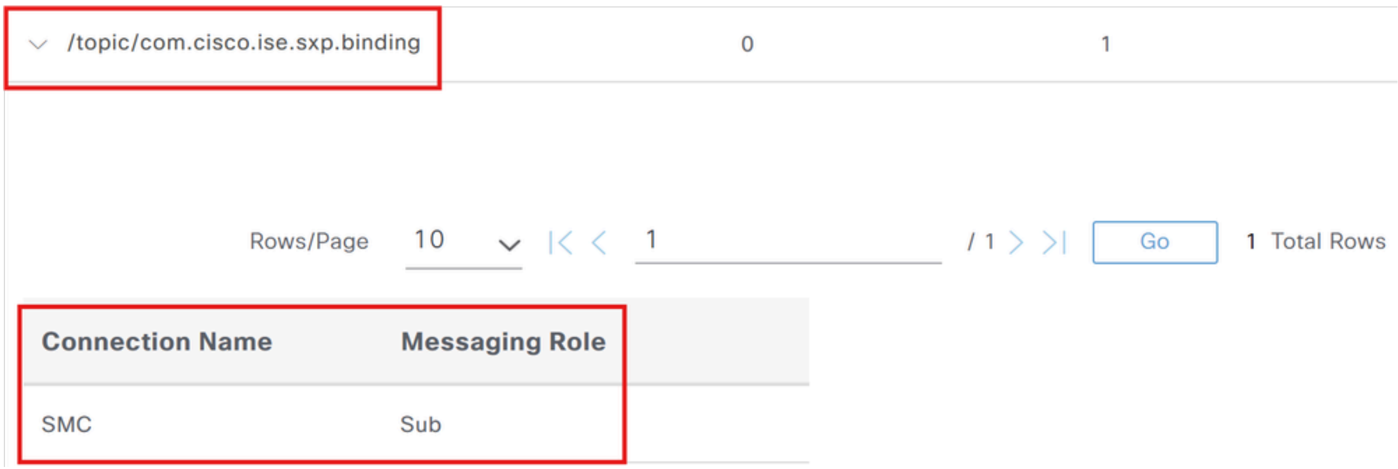
Trustsec SGT topic



ISE Session directory topic



ISE SXP Bindings topic



Cisco ISE Pxgrid-server.log in TRACE level.

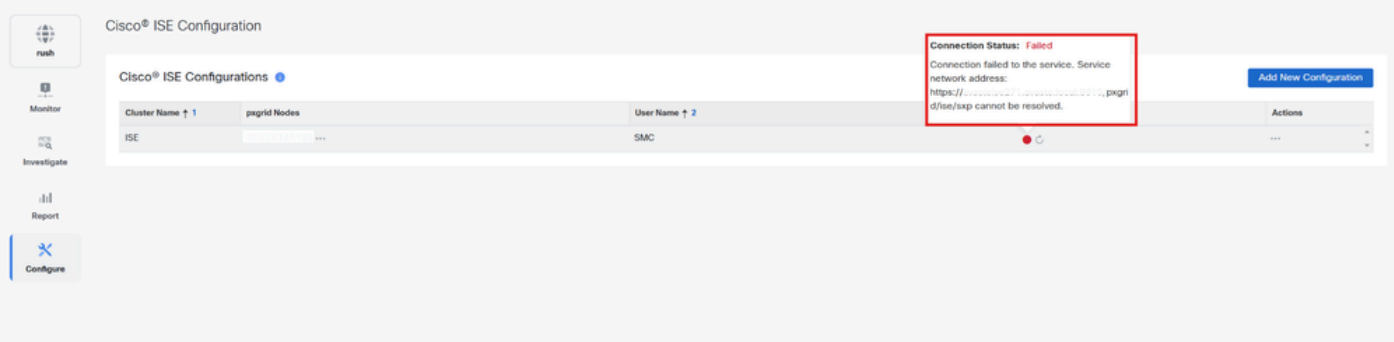
```
2025-02-08 18:07:11,086 TRACE  [pxgrid-http-pool15][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribu
2025-02-08 18:07:11,087 TRACE  [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint
2025-02-08 18:07:11,102 TRACE  [pxgrid-http-pool19][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint
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 -::::::
```

```
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:isehostnameme.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 oSMCMsvcvisese-client.log file. Path: catlancopepe/var/logs/containesvcvisese-client.log

```
snasmc1 docker/svc-ise-client[1453]: java.util.concurrent.ExecutionException: javax.net.ssl.SSLExceptio
snasmc1 docker/svc-ise-client[1453]: at java.base/java.util.concurrent.CompletableFuture.reportGet(Comp
snasmc1 docker/svc-ise-client[1453]: at java.base/java.util.concurrent.CompletableFuture.get(Completabl
snasmc1 docker/svc-ise-client[1453]: at org.springframework.web.socket.client.jetty.JettyWebSocketClien
snasmc1 docker/svc-ise-client[1453]: at java.base/java.util.concurrent.FutureTask.run(FutureTask.java:2
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.TlsFat
snasmc1 docker/svc-ise-client[1453]: at org.bouncycastle.jsse.provider.ProvSSLEngine.unwrap(ProvSSLEngi
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.jav
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection$DecryptedEndPoint.fill(S
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.client.http.HttpReceiverOverHTTP.process(Http
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.client.http.HttpReceiverOverHTTP.receive(Http
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.client.http.HttpChannelOverHTTP.receive(HttpC
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.client.http.HttpConnectionOverHTTP.onFillable
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.AbstractConnection$ReadCallback.succeeded(
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.FillInterest.fillable(FillInterest.java:10
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection$DecryptedEndPoint.onFill
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection.onFillable(SslConnection
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection$2.succeeded(SslConnectio
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.FillInterest.fillable(FillInterest.java:10
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.SelectableChannelEndPoint$1.run(Selectable
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.util.thread.QueuedThreadPool.runJob(QueuedThr
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.util.thread.QueuedThreadPool$Runner.run(Queue
snasmc1 docker/svc-ise-client[1453]: ... 1 more
snasmc1 docker/svc-ise-client[1453]: Suppressed: javax.net.ssl.SSLHandshakeException: org.bouncycastle.
```

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