Integración de ISE 3.3 con Stealthwatch 7.5.1 mediante CA externa

Contenido

Introducción

Este documento describe los procedimientos para integrar ISE 3.3 con Secure Network Analytics (StealthWatch) mediante conexiones pxGrid.

Prerequisites

Cisco recomienda conocimientos sobre los siguientes temas:

- Identity Services Engine
- Platform Exchange Grid (pxGrid)
- Secure Network Analytics (StealthWatch)
- Certificados TLS/SSL.

- PKI en Windows Server 2016

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- parche 4 de Identity Services Engine (ISE) versión 3.3
- Secure Network Analytics (StealthWatch) 7.5.1
- Windows Server 2016 como servidor de la Autoridad de certificación (CA) externa.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

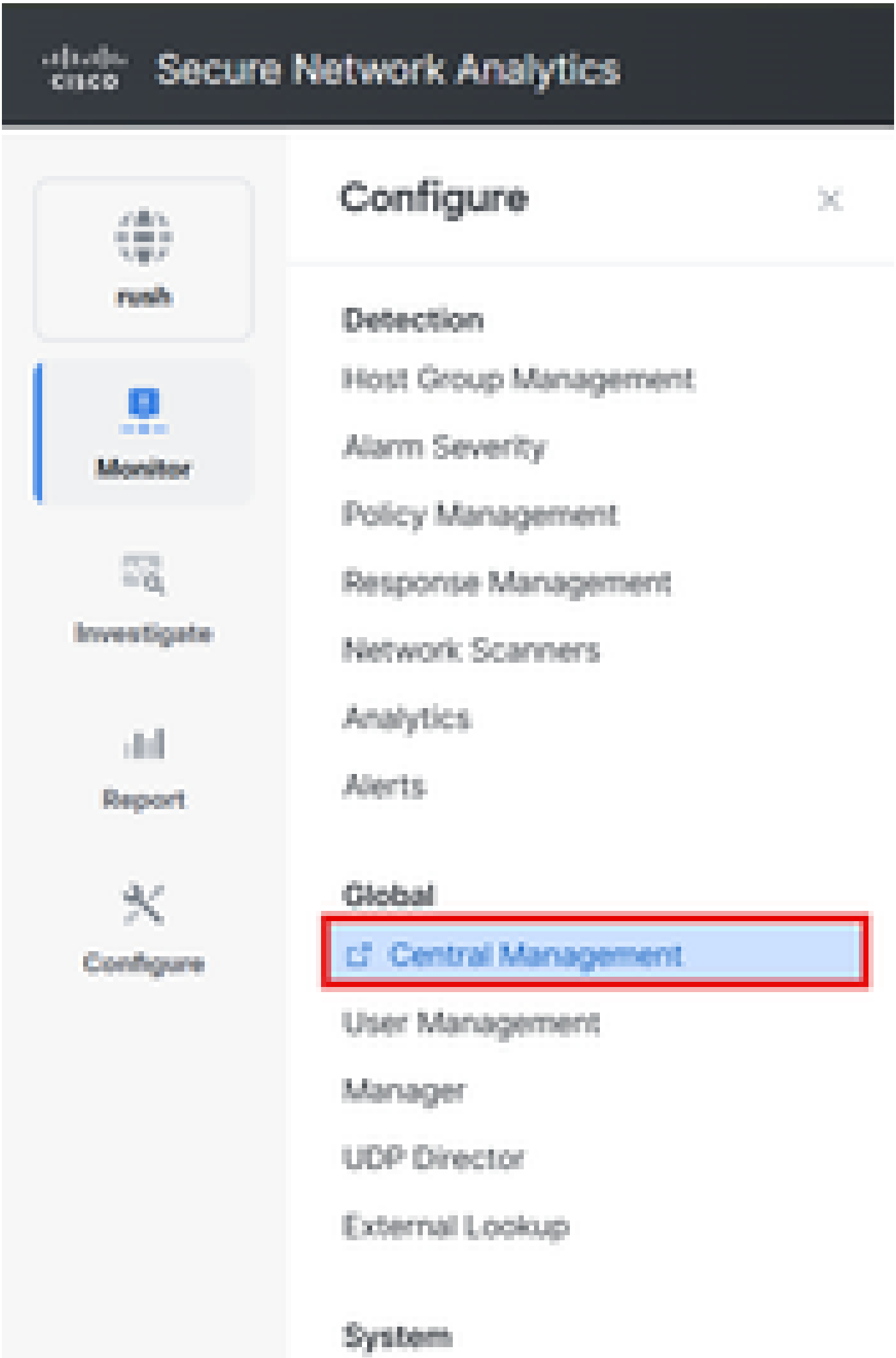
Configurar

Sección A: Configuración del certificado de Secure Network Analytics (Stealthwatch)

Parte I - Generación de una CSR para el certificado de cliente pxGrid de Secure Network Analytics

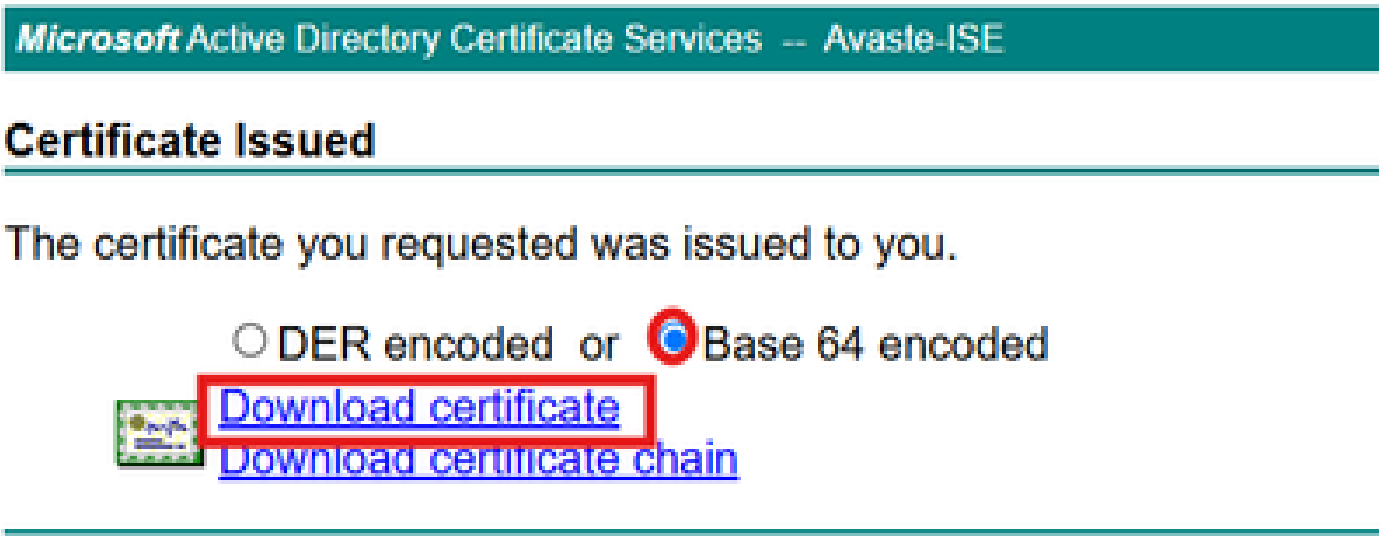
1. Inicie sesión en StealthWatch Management Console (SMC).

2. En el menú principal, seleccione 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

La plantilla de certificado pxGrid utilizada necesita la autenticación de cliente y la autenticación de servidor en el campo "Uso mejorado de claves".

6. Descargue un certificado generado en formato Base-64 y guárdelo como pxGrid_client.cer.



PARTE III - Adición del certificado de cliente de Secure Network Analytics pxGrid al administrador

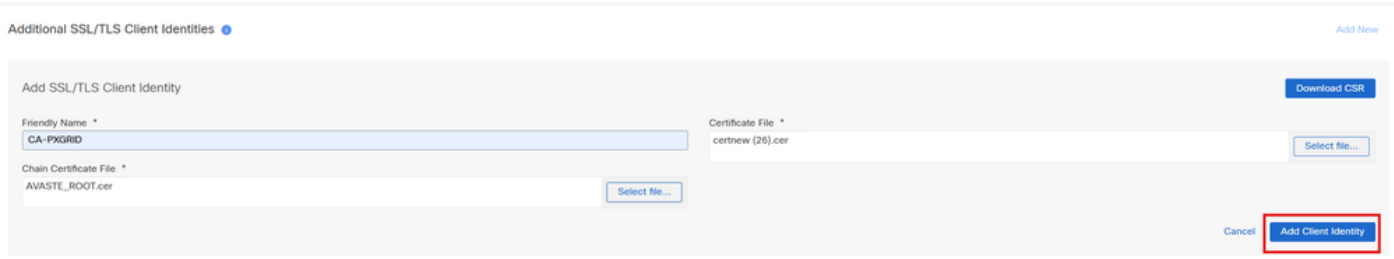
1.Navegue hasta la sección Identidades de Cliente SSL/TLS adicionales de la Configuración del Administrador en Administración central.

2. La sección Identidades de Cliente SSL/TLS Adicionales contiene un formulario para importar el certificado de cliente creado.

3. Asigne un nombre descriptivo al certificado y haga clic en Seleccionar archivo para localizar el archivo del certificado.

4. Seleccione el archivo CA .cer raíz o emisor o el archivo de cadena de certificados (.pem / .cer / .crt) en la sección Archivo de certificado de cadena.

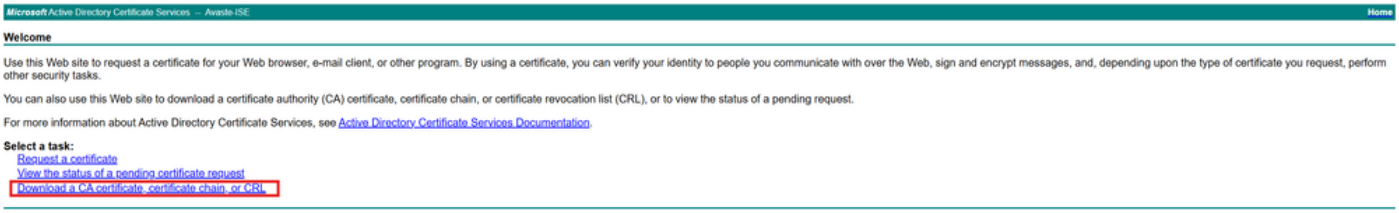
5. Haga clic en Agregar identidad de cliente para agregar el certificado al sistema.



6. Haga clic en Aplicar configuración para guardar los cambios.

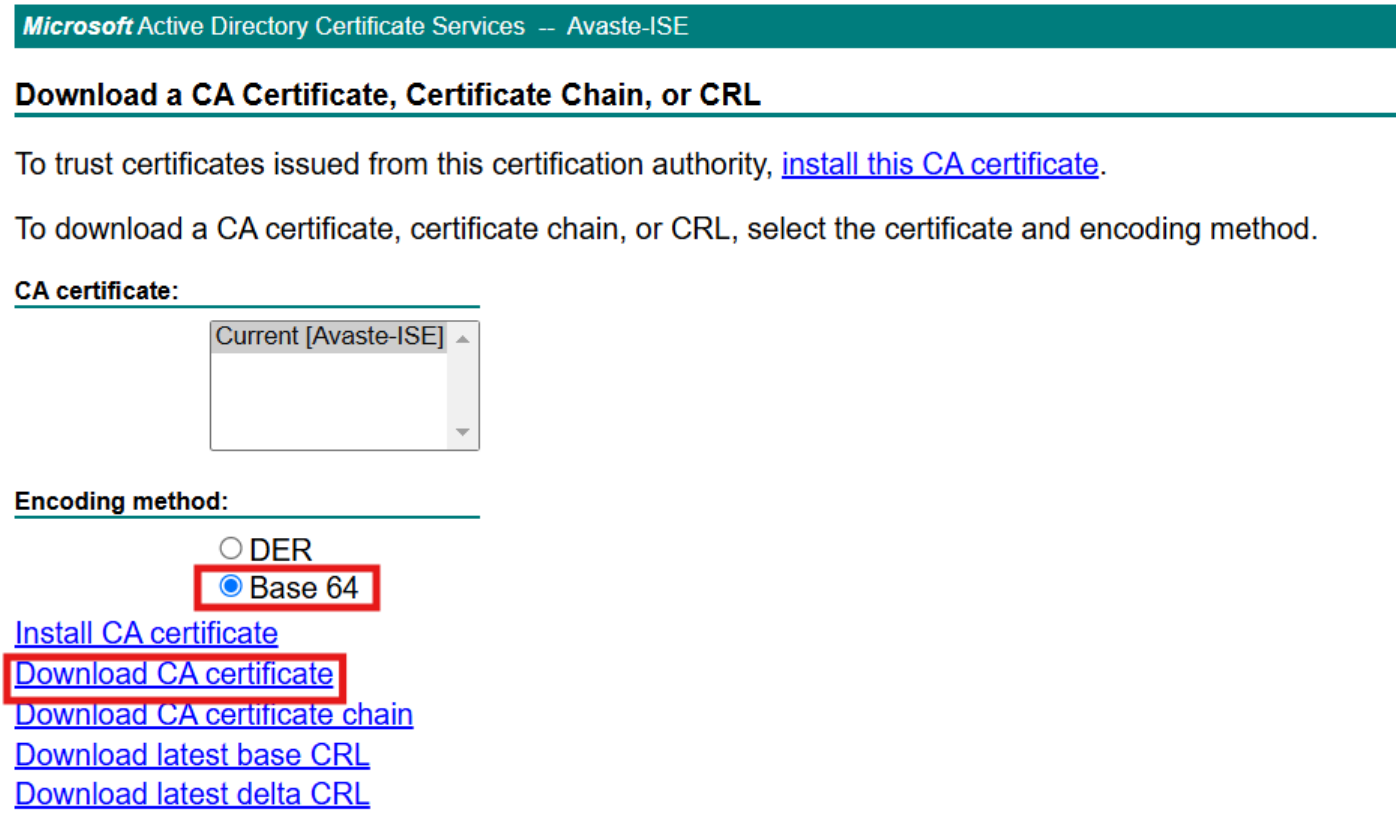
PARTE IV - Importación del certificado raíz de la CA en el almacén de confianza del administrador

1. Navegue hasta la página de inicio del Servicio de certificados de Active Directory de MS y seleccione Descargar un certificado de CA, cadena de certificados o CRL.



2. Seleccione el formato Base-64, luego haga clic en Descargar certificado CA.

3. Guarde el certificado como CA_Root.cer.



4. Inicie sesión en StealthWatch Management Console (SMC).

5. En el menú principal, seleccione Configure > Global > Central Management.

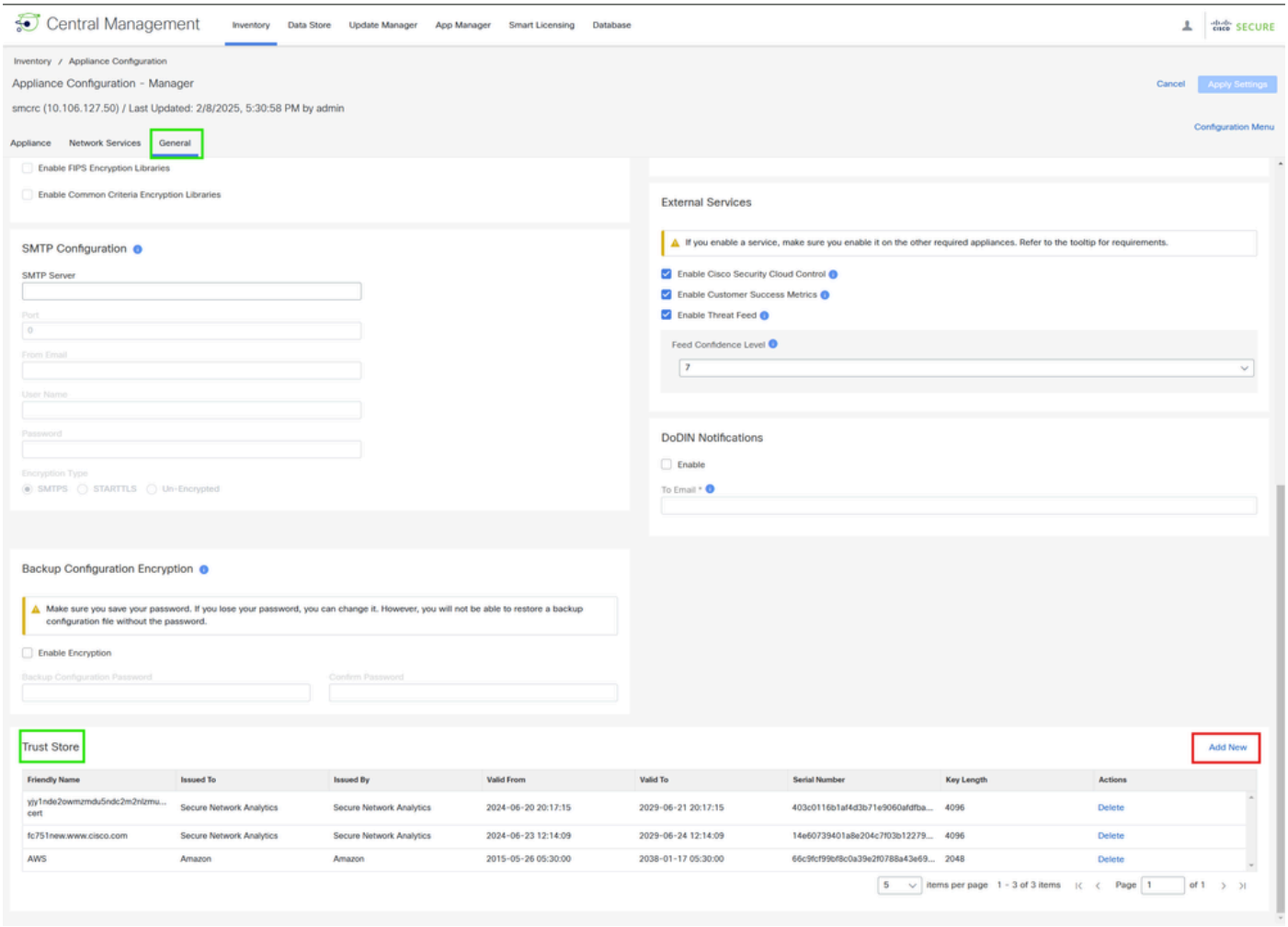
6. En la página Inventario, haga clic en el icono (puntos suspensivos) del jefe.

7. Seleccione Editar Configuración de Dispositivo.

8. Seleccione la pestaña General.

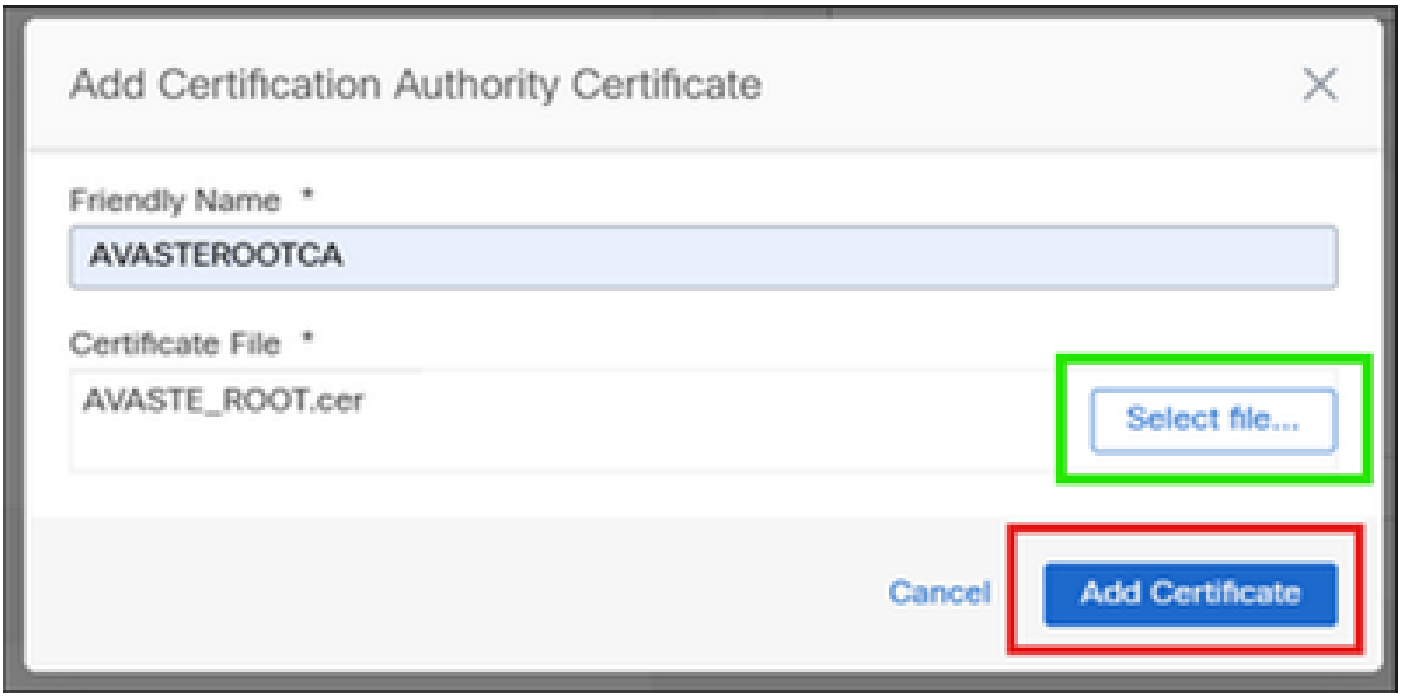
9. Navegue hasta la sección Trust Store e importe el certificado CA_Root.cer exportado anteriormente.

10. Haga clic en Agregar nuevo.



11. Asigne un nombre descriptivo al certificado y, a continuación, haga clic en Seleccionar archivo... para seleccionar el certificado de CA de ISE exportado anteriormente.

12. Haga clic en Agregar certificado para guardar los cambios.



13. Haga clic en Aplicar configuración para guardar los cambios.

Sección B: Configuración del certificado de Cisco Identity Services Engine 3.3

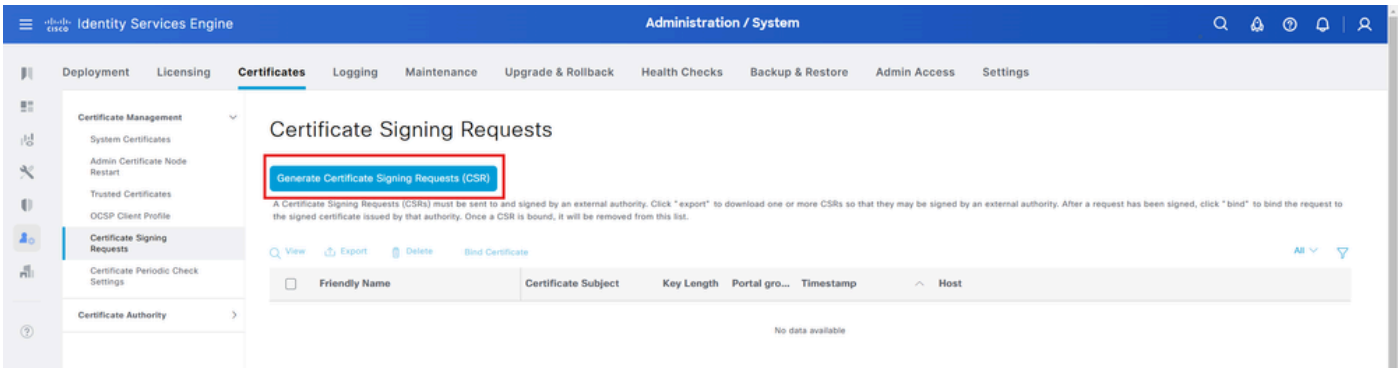
PARTE I - Generación de un certificado ISE Server pxGrid

Generar una CSR para un certificado pxGrid de servidor ISE:

1. Inicie sesión en la GUI de Cisco Identity Services Engine (ISE).

2. Navegue hasta Administración > Sistema > Certificados > Administración de certificados >Solicitudes de firma de certificado.

3. Seleccione Generar Solicitud de Firma de Certificado (CSR).

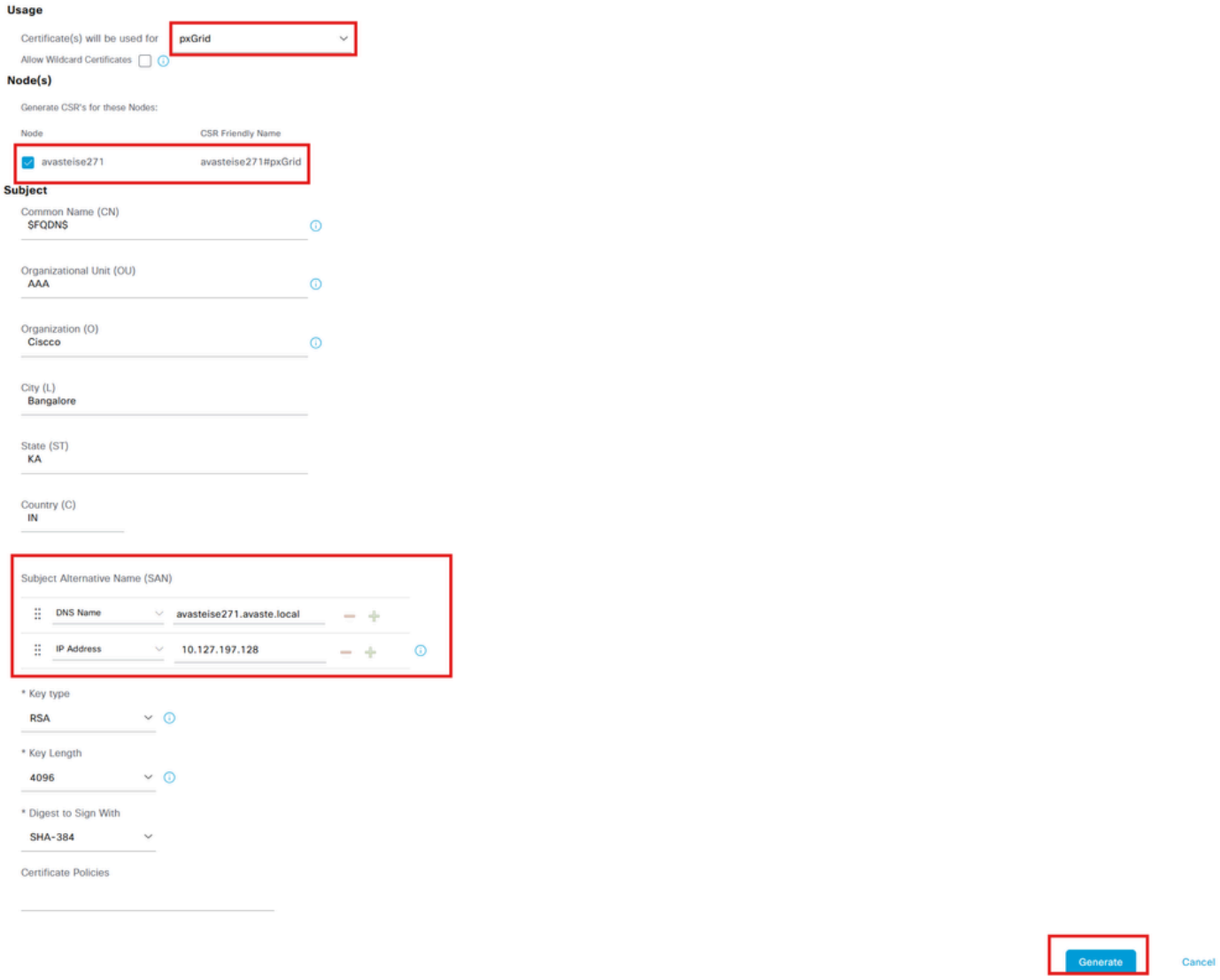


4. Seleccione pxGrid en el campo Certificate(s) is used for.

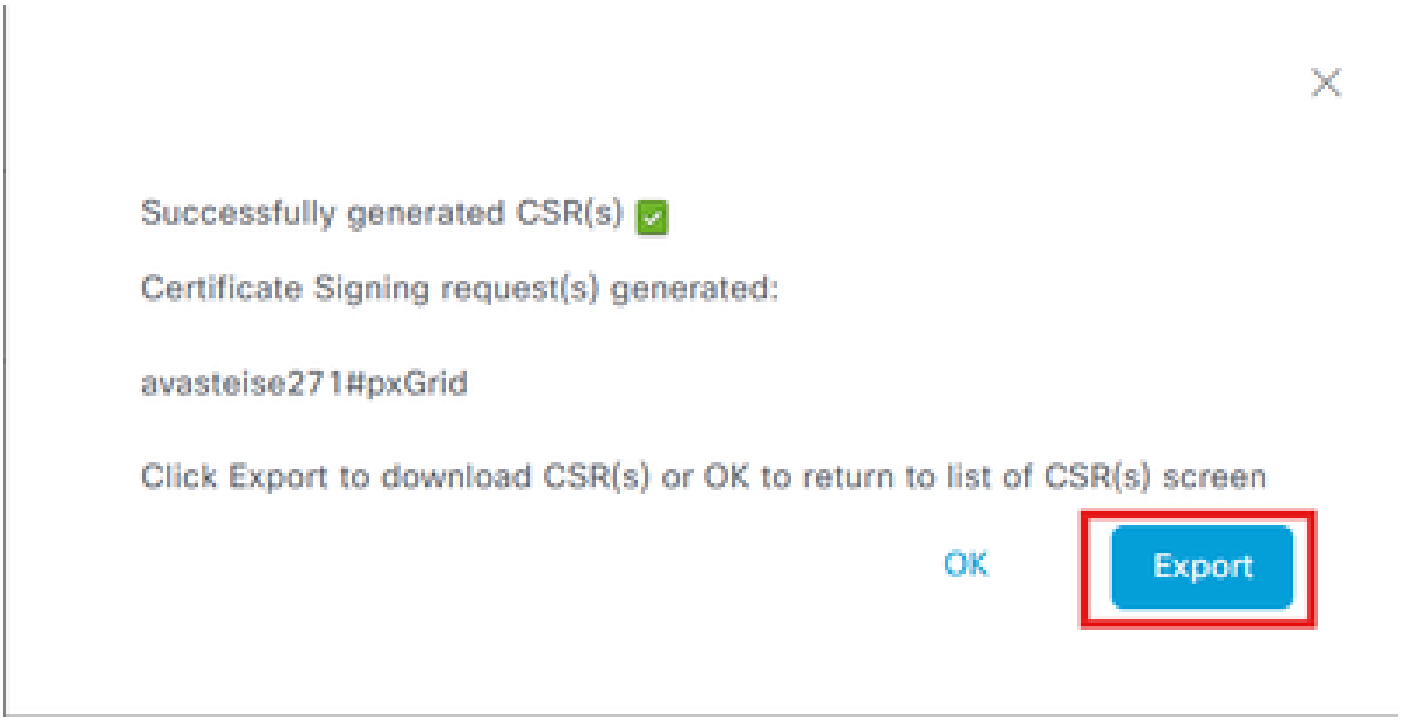
5. Seleccione el nodo ISE para el que se genera el certificado.

6. Rellene los detalles de otros certificados según sea necesario.

7. Haga clic en Generar.



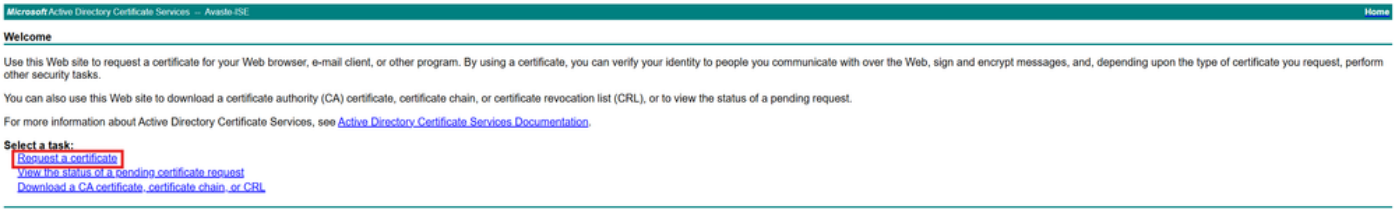
8. Haga clic en Exportar y Guardar el archivo localmente.



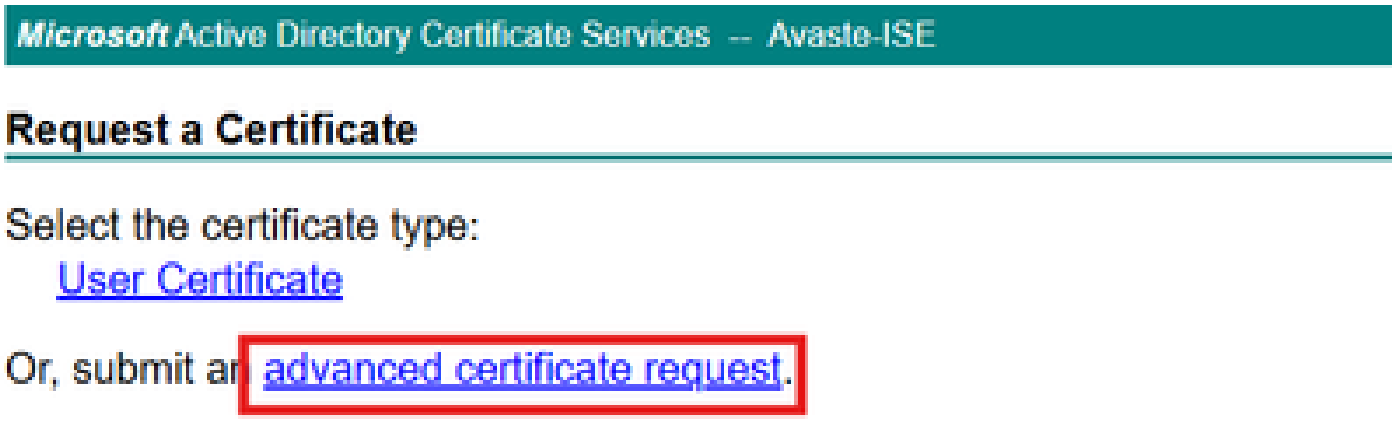
PARTE II - Creación de un certificado pxGrid de servidor ISE mediante una CA externa

1. Navegue hasta Servicio de certificados de Active Directory de MS, https://server/certsrv/, donde el servidor es IP o DNS de su servidor MS.

2. Haga clic en Solicitar un certificado.

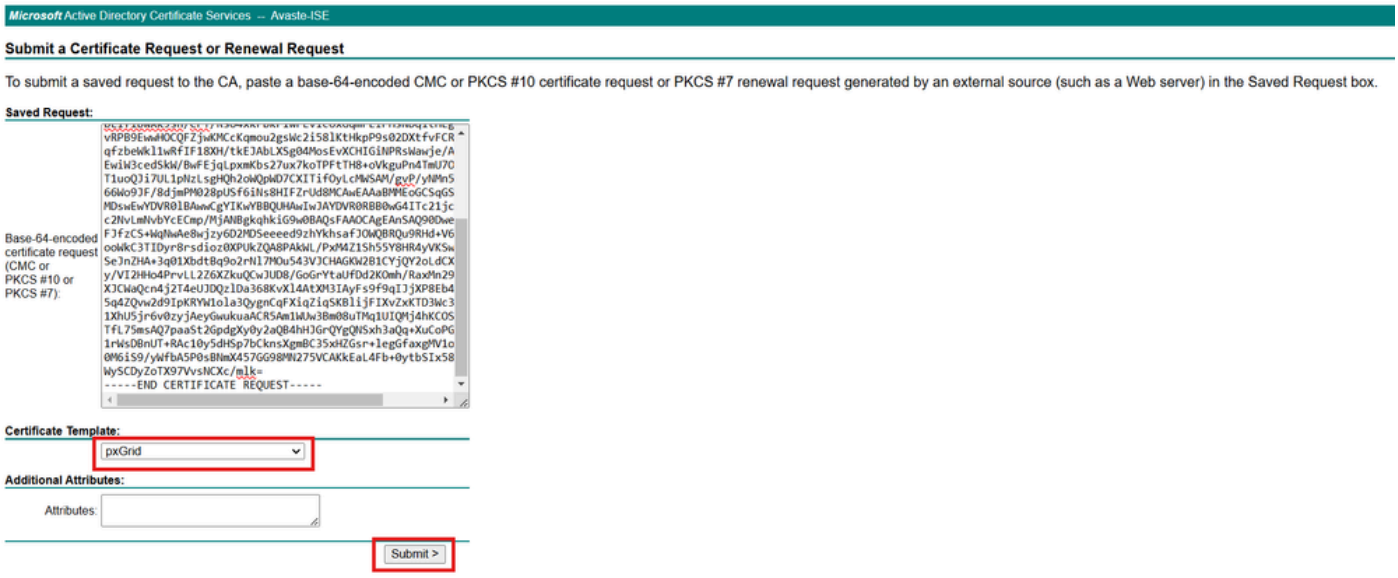


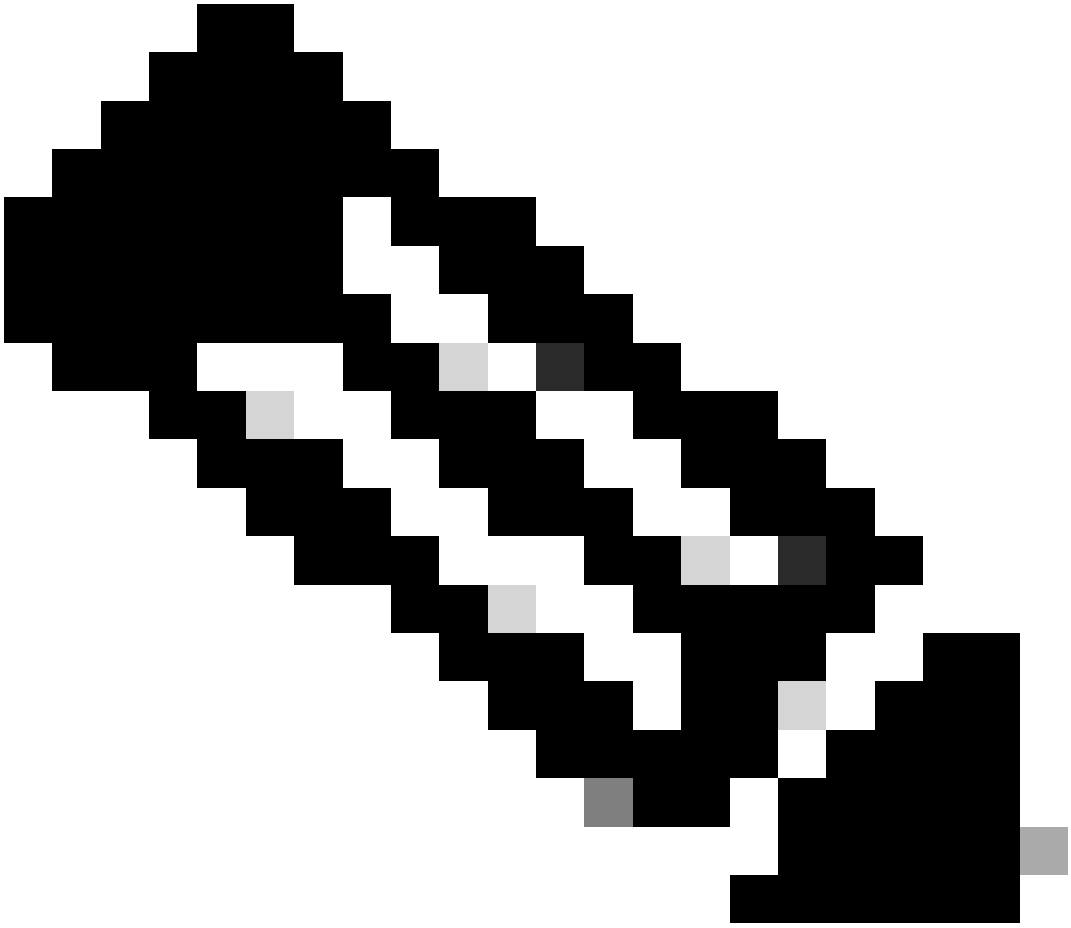
3. Seleccione esta opción para ejecutar una solicitud de certificado avanzada.



4. Copie el contenido del CSR generado en la sección anterior en el campo Solicitud Guardada.

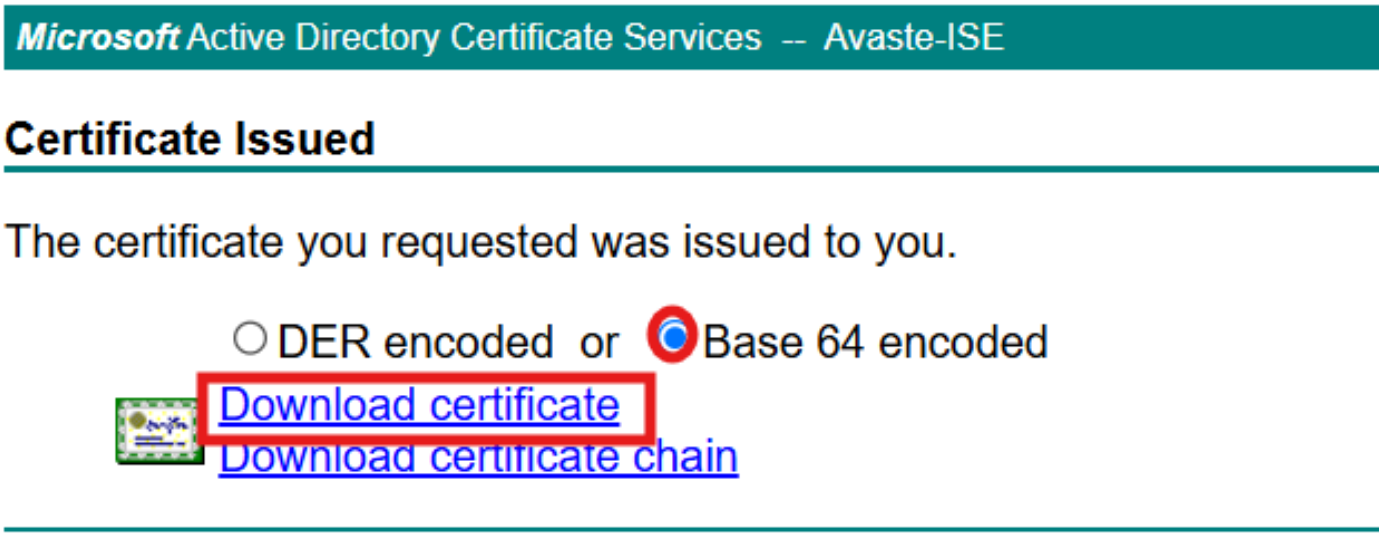
5. Seleccione pxGrid como Plantilla de Certificado y, a continuación, haga clic en Enviar.





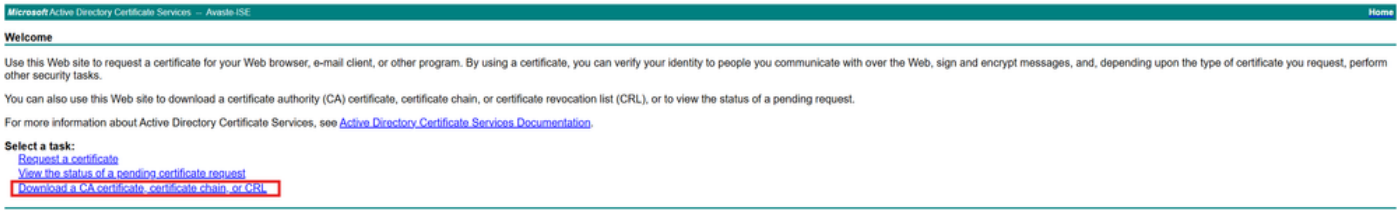
Nota: La plantilla de certificado pxGrid utilizada necesita la autenticación de cliente y la autenticación de servidor en el campo "Uso mejorado de claves".

6. Descargue el certificado generado en formato Base-64 y guárdelo como ISE_pxGrid.cer.

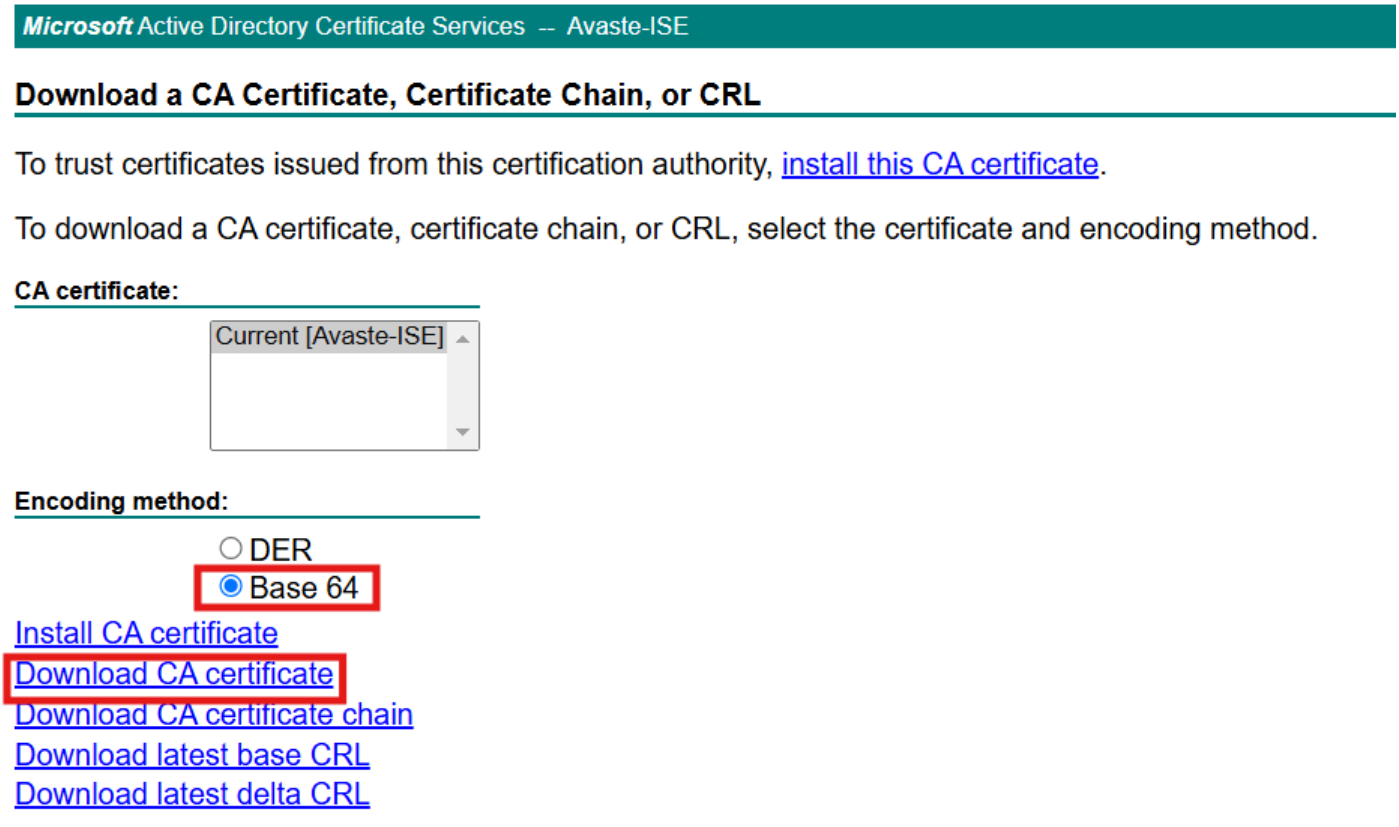


PARTE III: Importación del certificado raíz de la CA en el almacén de confianza de ISE

1. Navegue hasta la página de inicio del Servicio de certificados de MS Active Directory y seleccione Descargar un certificado de CA, cadena de certificados o CRL.



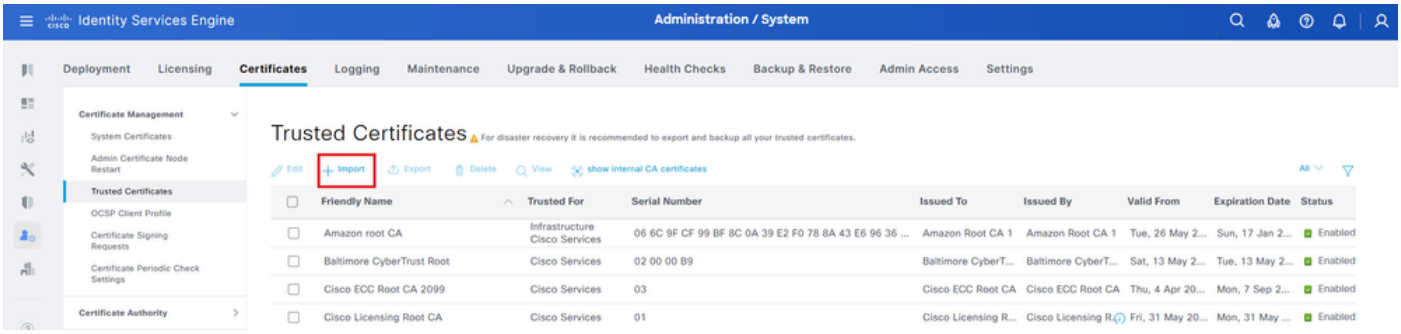
2. Seleccione el formato Base-64, luego haga clic en Descargar certificado CA.



3. Guarde el certificado como CA_Root.cer.

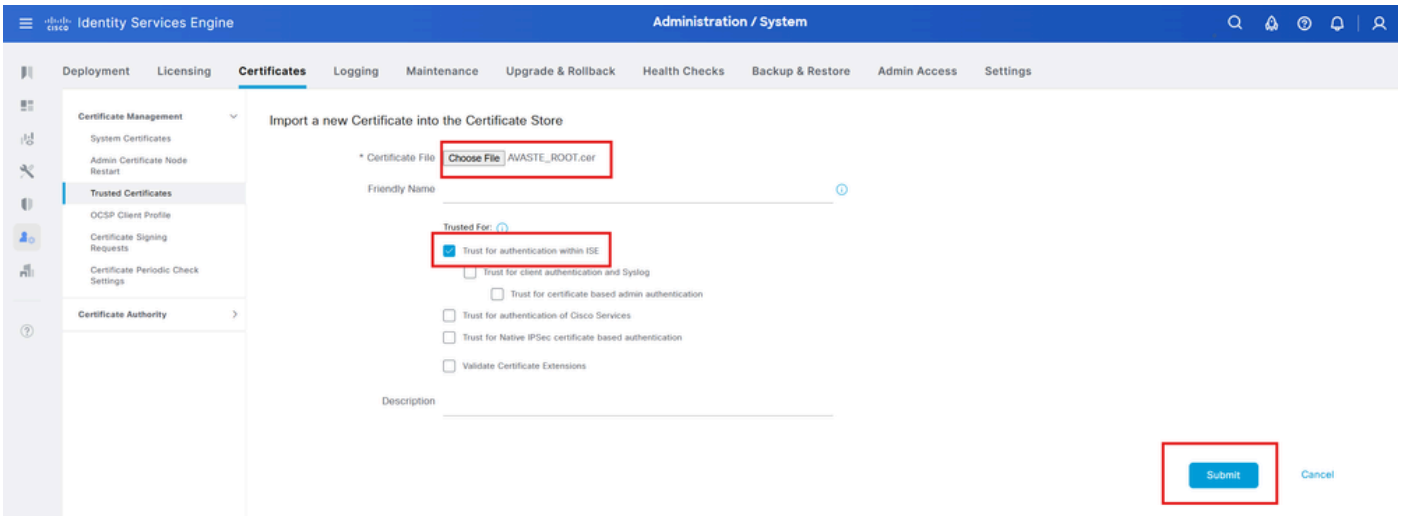
4. Inicie sesión en la GUI de Cisco Identity Services Engine (ISE).

5. Seleccione Administration > System > Certificates > Certificate Management >Trusted Certificates.



6. Seleccione Importar > Archivo de certificado e Importar el certificado raíz.

7. Asegúrese de que la casilla de verificación Confiar en la autenticación dentro de ISE esté activada.



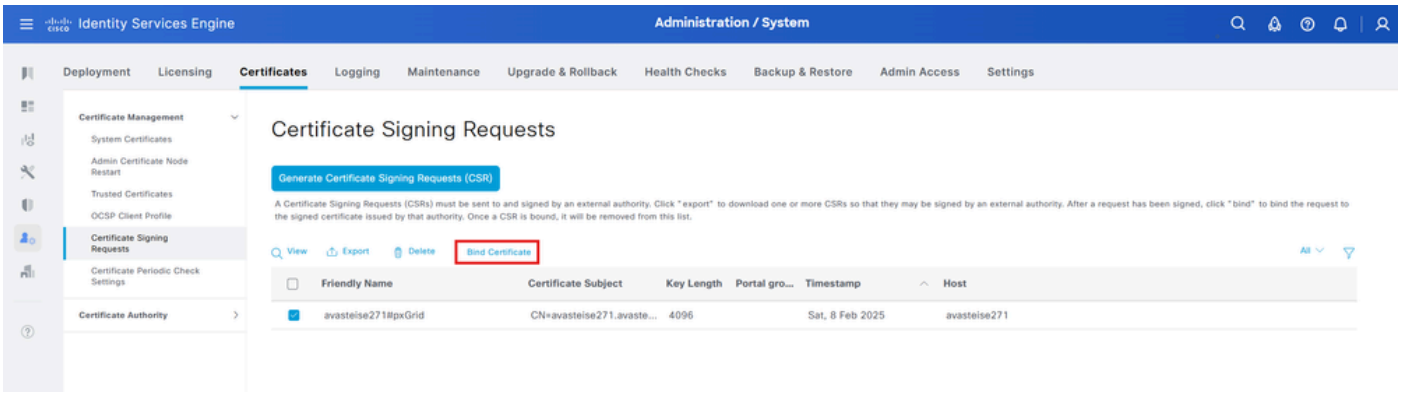
8. Haga clic en Enviar.

PARTE IV: Vincular el certificado ISE a la solicitud de firma de certificado (CSR)

1. Inicie sesión en la GUI de Cisco Identity Services Engine (ISE).

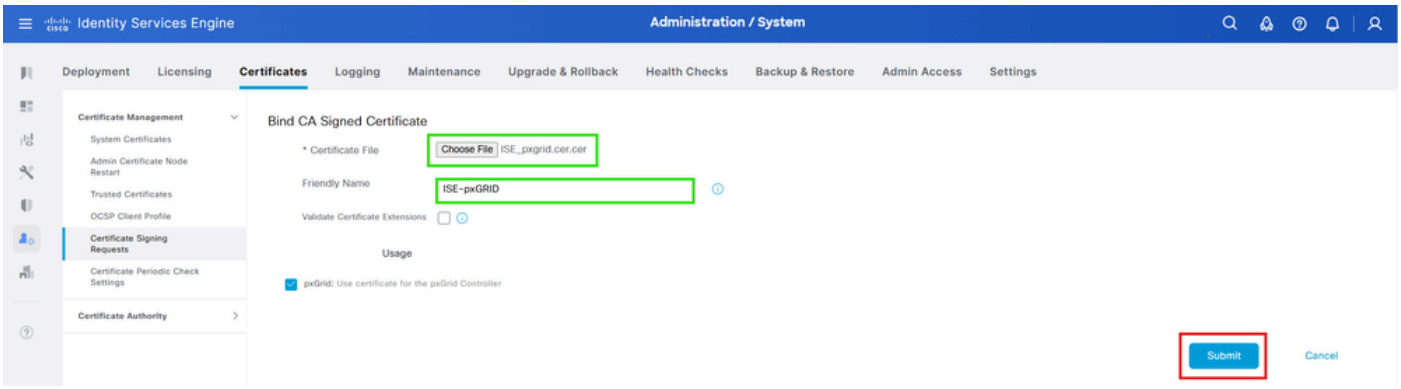
2. Seleccione Administración > Sistema > Certificados > Administración de certificados > Solicitudes de firma de certificado.

3. Seleccione el CSR generado en la sección anterior y, a continuación, haga clic en Enlazar certificado.



4. En el formulario de certificado firmado de CA de enlace, seleccione el certificado ISE_pxGrid.cer generado anteriormente.

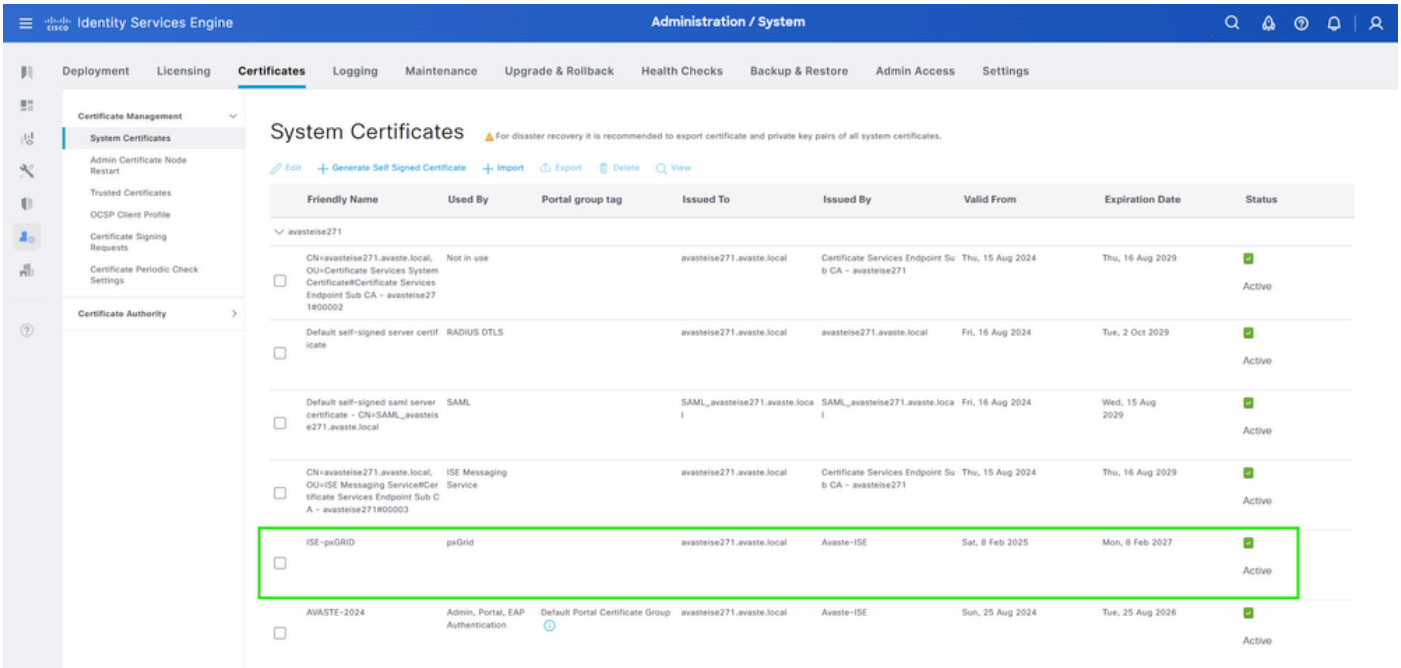
5. Asigne un nombre descriptivo al certificado y, a continuación, haga clic en Enviar.



7. Haga clic en Sí si el sistema le solicita que sustituya el certificado.

8. Seleccione Administration > System > Certificates > System Certificates.

9. Puede ver el certificado pxGrid creado firmado por la CA externa en la lista.

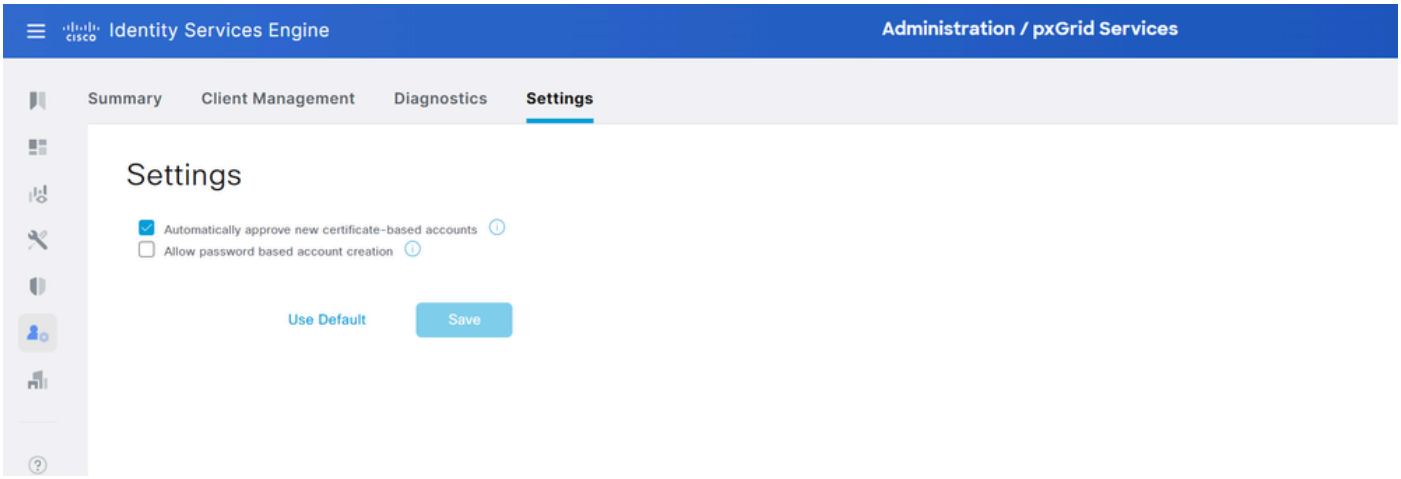


Los certificados ya están implementados. Continúe con la integración.

Integrar

Antes de proceder a la integración, asegúrese de que:

Para Cisco ISE, en Administration > pxGrid Services > Settings y Check Apruebe automáticamente las nuevas cuentas basadas en certificados para que la solicitud del cliente se apruebe automáticamente y se guarde.

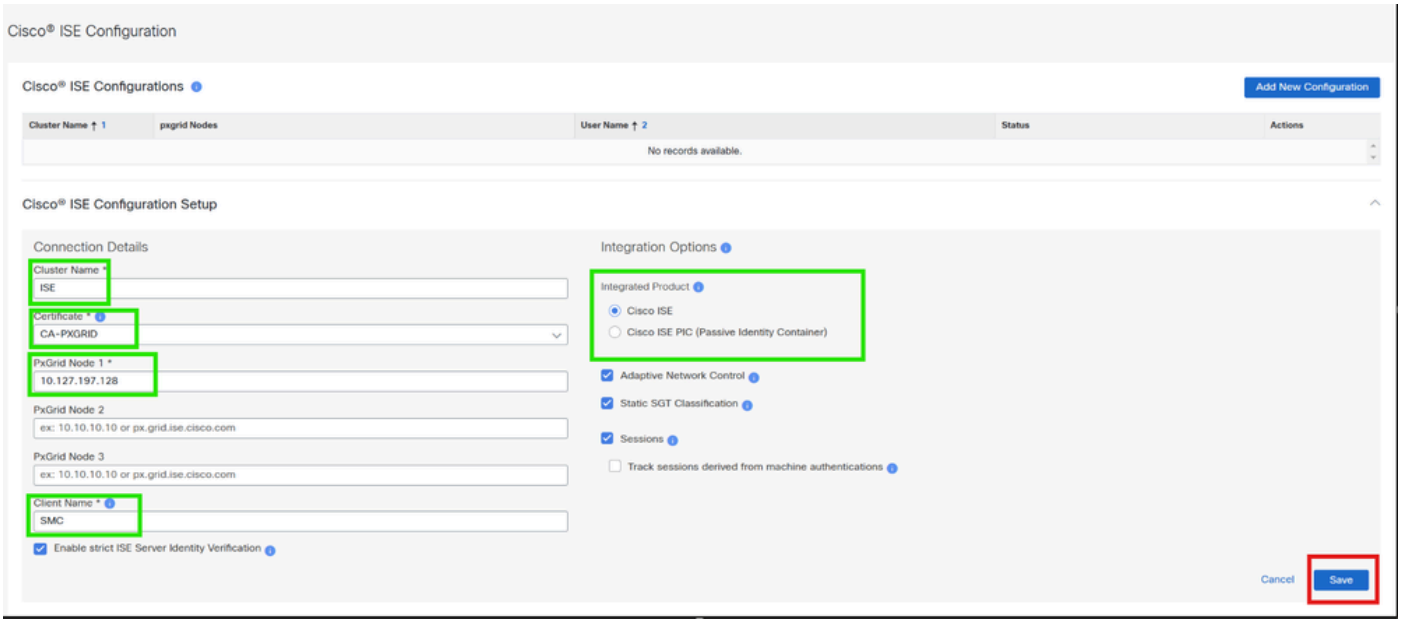


En StealthWatch Management Console (SMC), Para abrir la página de configuración de ISE:

1. Seleccione Configurar > Integraciones > Cisco ISE.

2. En la esquina superior derecha de la página, haga clic en Agregar nueva configuración.

3. Introduzca el nombre del cluster, seleccione el certificado & Integration Product, el nodo pxGrid IP y haga clic en Save.

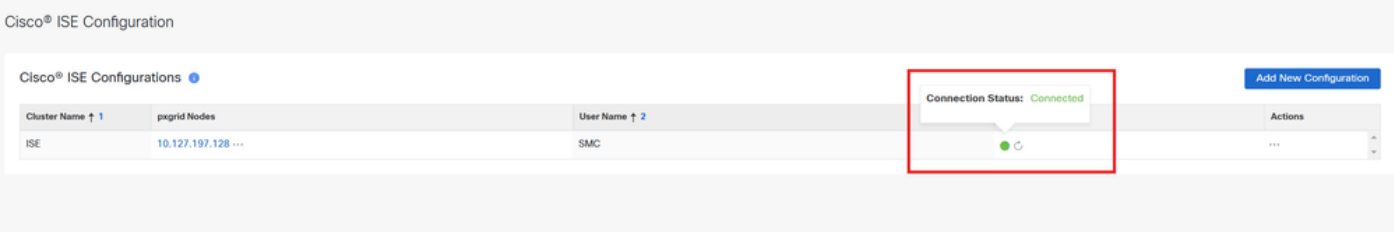


Verificación

Actualice la página de configuración de ISE en StealthWatch Management Console (SMC).

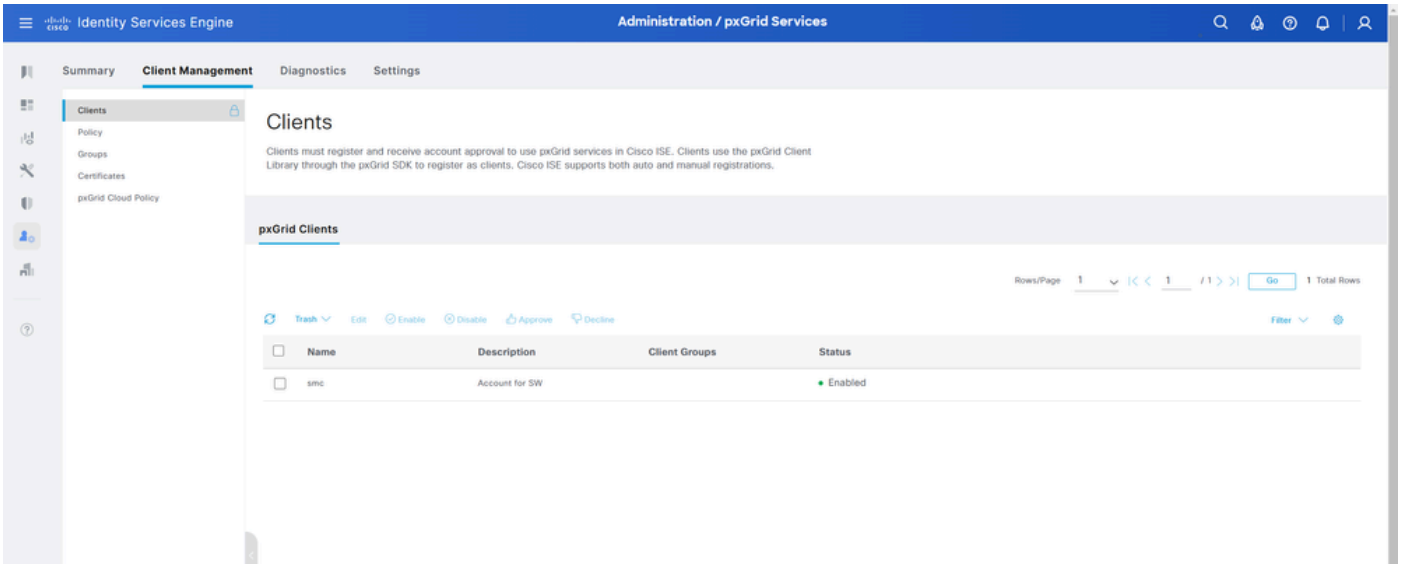
1. Vuelva a la página de configuración de ISE en la aplicación web y actualice la página.

2. Confirme que el indicador de estado del nodo situado junto al campo Dirección IP aplicable es Verde, lo que indica que se ha establecido una conexión con el clúster ISE o ISE-PIC.



En Cisco ISE, navegue hasta Administration > pxGrid Services > Client Management > Clients.

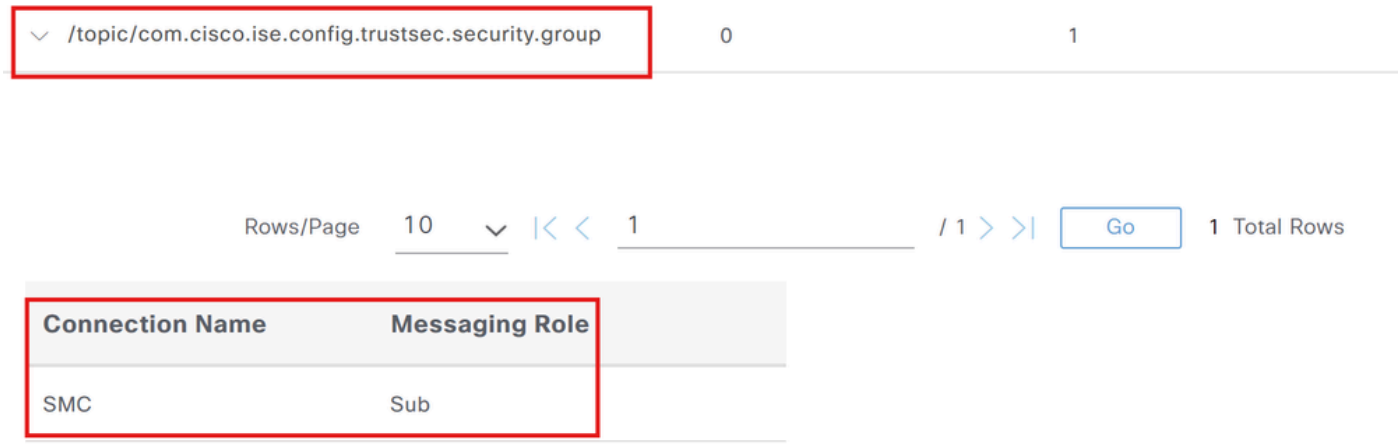
Esto genera el SMC como un cliente pxgrid con el estado Enabled.



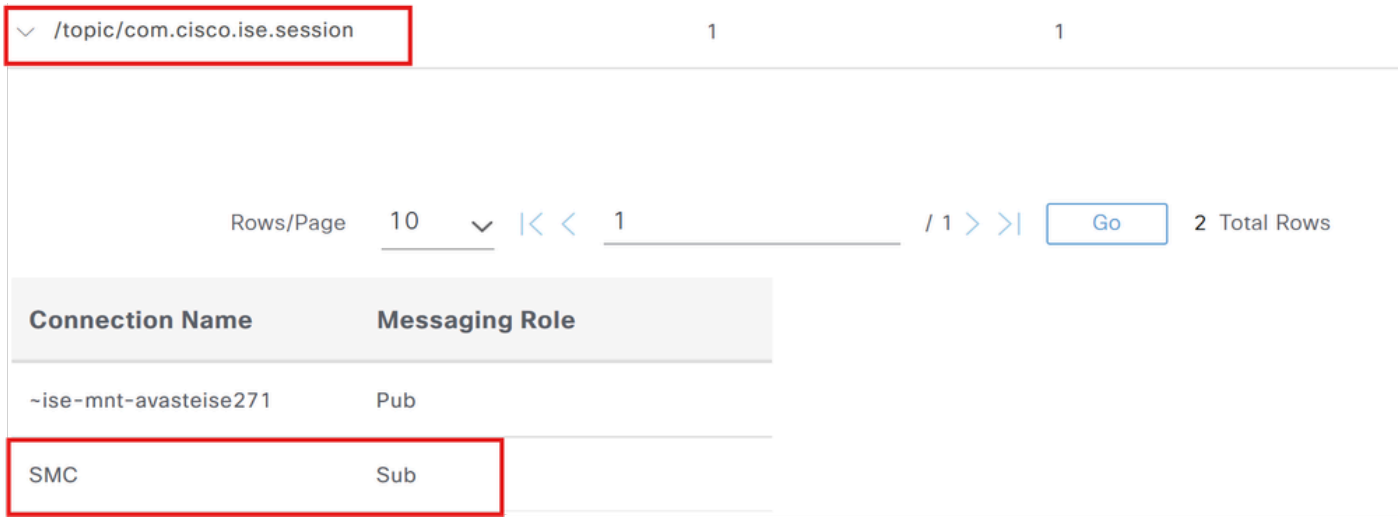
Para verificar la suscripción a los temas en Cisco ISE, navegue hasta Administration > pxGrid Services > Diagnostics > Websocket > Topics

Esto genera un SMC suscrito a estos temas.

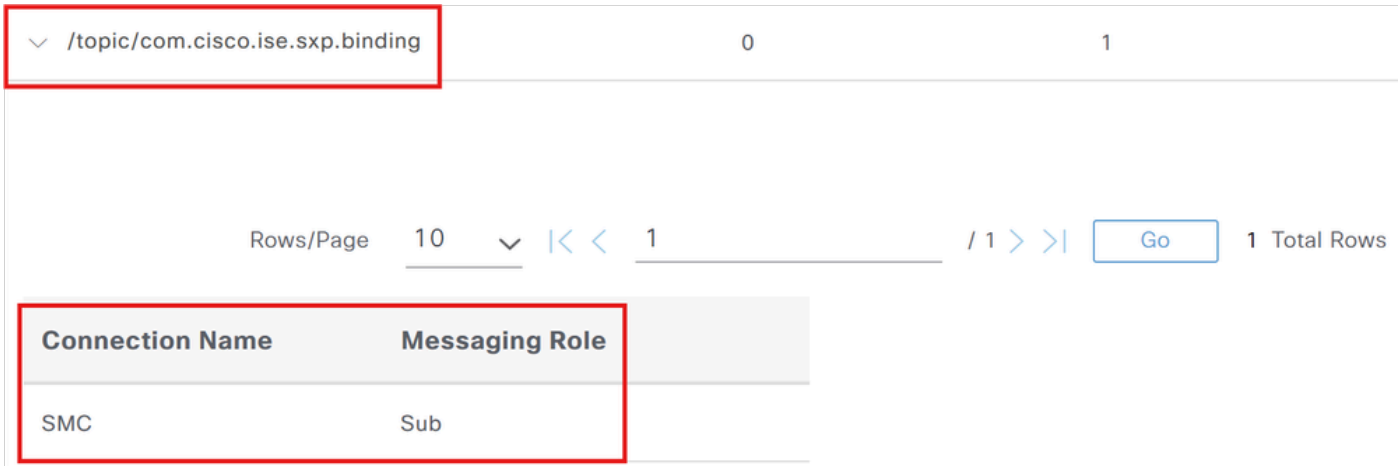
tema SGT de Trustsec



tema de directorio de sesión de ISE



tema Enlaces de ISE SXP



Cisco ISE Pxgrid-server.log en el nivel TRACE.

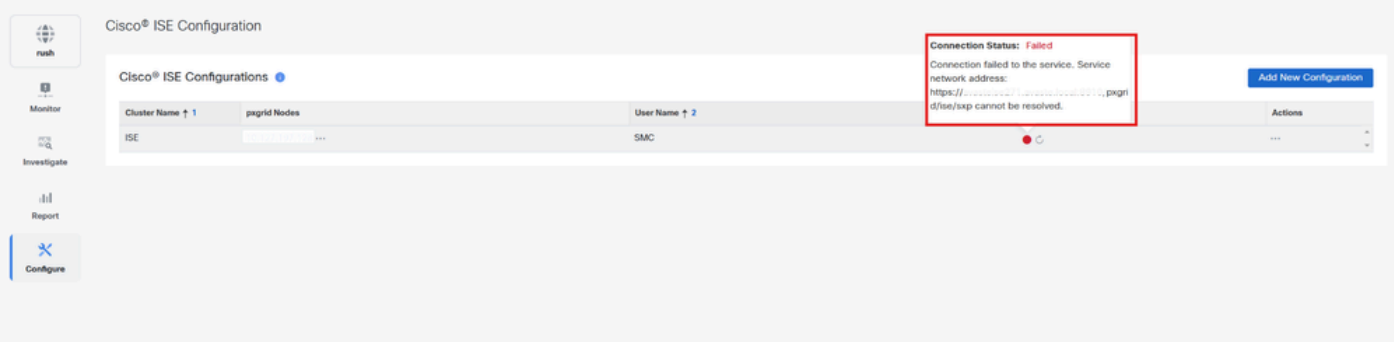
```
2025-02-08 18:07:11,086 TRACE  [pxgrid-http-pool15][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribu
2025-02-08 18:07:11,087 TRACE  [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint
2025-02-08 18:07:11,102 TRACE  [pxgrid-http-pool19][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint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



       ]
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



        ] session=[id=8,client=SMC,server=wss://avasteise271.avaste.local:8910/pxgrid/ise/pubsub]
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.SubscriptionDistribut
2025-02-08 18:07:11,324 TRACE  [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribut



         ]
2025-02-08 18:07:11,324 TRACE  [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribut
2025-02-08 18:07:11,324 TRACE  [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribut



          ]
2025-02-08 18:07:11,324 TRACE  [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribut
2025-02-08 18:07:11,324 TRACE  [sub-sender-0][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionSender -::::::



           ] from=[id=7,client=~ise-admin-avasteise271,server=wss://avasteise271.avaste.local:8910/pxgr
2025-02-08 18:07:11,324 TRACE  [sub-sender-0][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionSender -::::::
```

Resolución de problemas

Problema de resolución de DNS

Esto produce un mensaje de error como "Connection Status; Error de conexión al servicio. Dirección de red del servicio: https:isehostnameme.domain.com:891pxgridiisessxpxp no se puede resolver":



Solución

Idealmente, esto debe solucionarse en el servidor DNS para las búsquedas directas e inversas de este FQDN de ISE. Sin embargo, se puede agregar una solución temporal para la resolución local:

1. Inicie sesión en StealthWatch Management Console (SMC).

2. En el menú principal, seleccione Configure > Global > Central Management.

3. En la página Inventario, haga clic en el icono (Puntos suspensivos) del jefe.

4. Seleccione Editar Configuración del Dispositivo.

5. Servicios de red y agregue una entrada de resolución local para este FQDN de ISE.

Error de CA desconocido o falta certificado de confianza

Esto produce un mensaje de error como "ISE está presentando un certificado que no es de confianza para este administrador":

Se puede ver una referencia de registro similar en el archivo oSMCMsvcvisese-client.log. Ruta: 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.
```

Solución

1. Inicie sesión en StealthWatch Management Console (SMC).

2. En el menú principal, seleccione Configure > Global > Central Management.

3. En la página Inventario, haga clic en el icono (puntos suspensivos) del jefe.

4. Seleccione Editar Configuración del Dispositivo.

5. Seleccione la pestaña General.

6. Navegue hasta la sección Almacén de confianza y asegúrese de que el emisor del certificado Pxgrid de Cisco ISE forme parte del almacén de confianza.

Defectos conocidos

ID de la falla	Descripción
ID de bug de Cisco 18119	ISE está seleccionando un paquete de saludo del servidor Cipher ITLS no compatible
ID de bug de Cisco 01634	No se pueden poner en cuarentena los dispositivos mediante la condición EPS

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).