# Integration von ISE 3.3 mit StealthWatch 7.5.1 mithilfe einer externen Zertifizierungsstelle

## Inhalt



## Einleitung

In diesem Dokument werden Verfahren zur Integration von ISE 3.3 mit Secure Network Analytics (StealthWatch) unter Verwendung von pxGrid-Verbindungen beschrieben.

## Voraussetzungen

Cisco empfiehlt Fachwissen in folgenden Bereichen:

- Identity Services Engine
- Platform Exchange Grid (pxGrid)
- Sichere Netzwerkanalysen (StealthWatch)
- TLS/SSL-Zertifikate
- PKI auf Windows Server 2016

## Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Identity Services Engine (ISE) Version 3.3 Patch 4
- Secure Network Analytics (StealthWatch) 7.5.1
- Windows Server 2016 als externer CA-Server (Certificate Authority)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

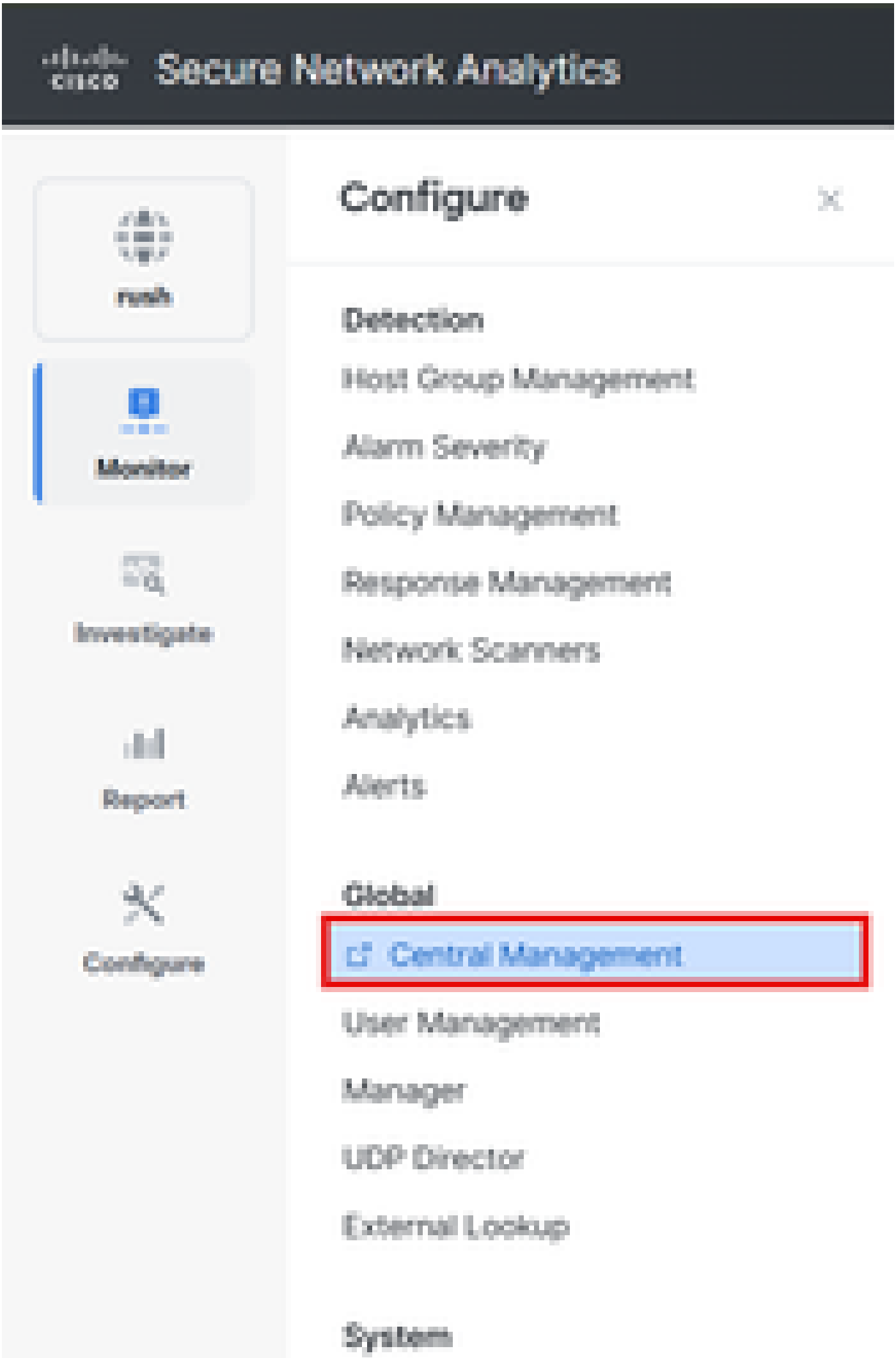
## Konfigurieren

## Abschnitt A: Secure Network Analytics (StealthWatch)-Zertifikatkonfiguration

Teil I - Erstellen einer CSR-Anfrage für das Secure Network Analytics pxGrid Client-Zertifikat

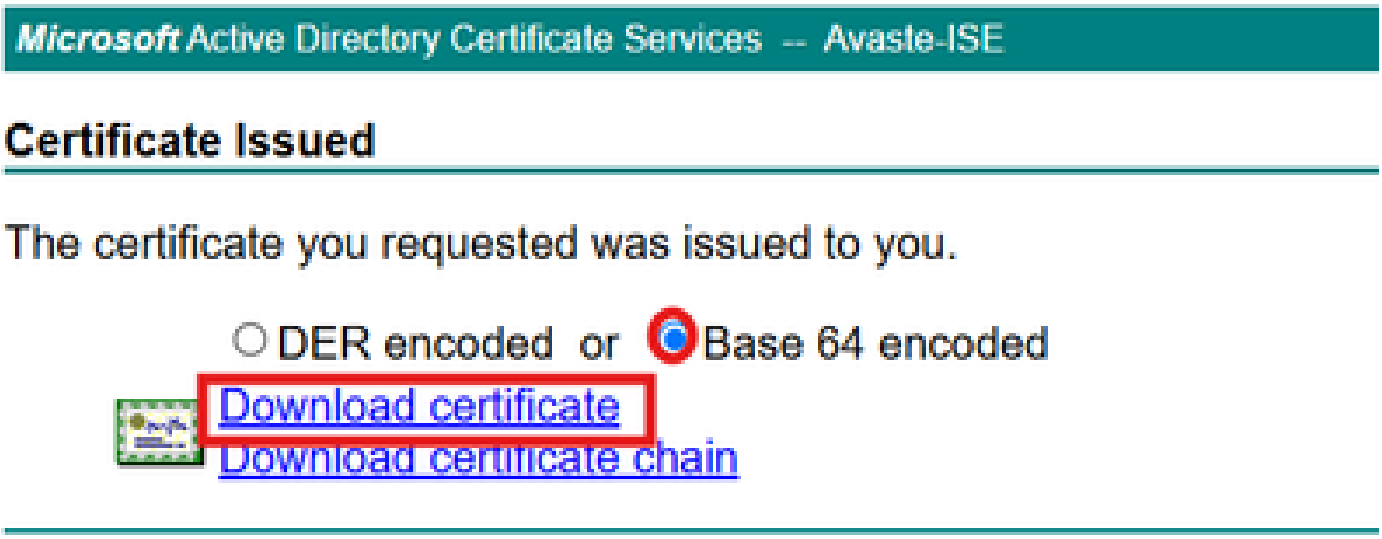
1. Melden Sie sich bei der StealthWatch Management Console (SMC) an.

2. Wählen Sie im Hauptmenü 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

Die verwendete Zertifikatvorlage pxGrid benötigt sowohl die Client- als auch die Serverauthentifizierung im Feld "Enhanced Key Usage" (Erweiterte Schlüsselverwendung).

6. Laden Sie ein generiertes Zertifikat im Base-64-Format herunter und speichern Sie es unter pxGrid_client.cer.




TEIL III - Hinzufügen des Secure Network Analytics-Client-Zertifikats pxGrid zum Manager

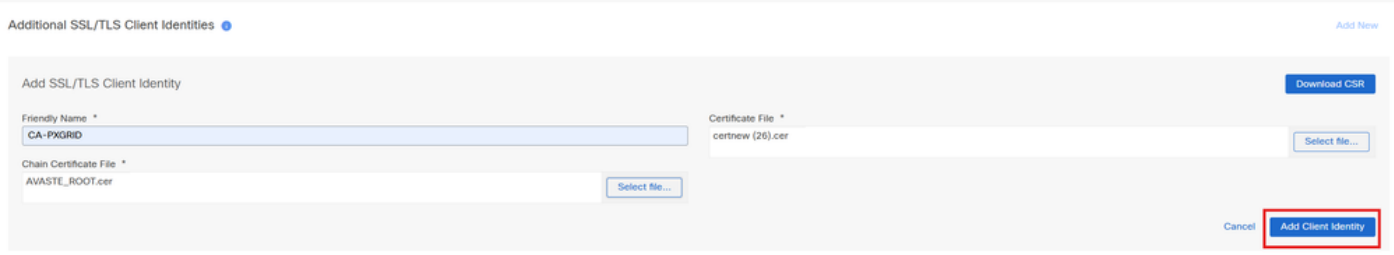
1. Navigieren Sie zum Abschnitt Zusätzliche SSL/TLS-Client-Identitäten der Manager-Konfiguration in der zentralen Verwaltung.

2. Der Abschnitt Zusätzliche SSL/TLS-Client-Identitäten enthält ein Formular zum Importieren des erstellten Client-Zertifikats.

3. Geben Sie dem Zertifikat einen Anzeigenamen, und klicken Sie dann auf Datei auswählen, um die Zertifikatsdatei zu suchen.

4. Wählen Sie im Bereich "Chain Certificate file" die CER-Datei der Stamm- oder Ausstellerzertifizierungsstelle oder die Zertifikatkettendatei (.pem / .cer / .crt ) aus.

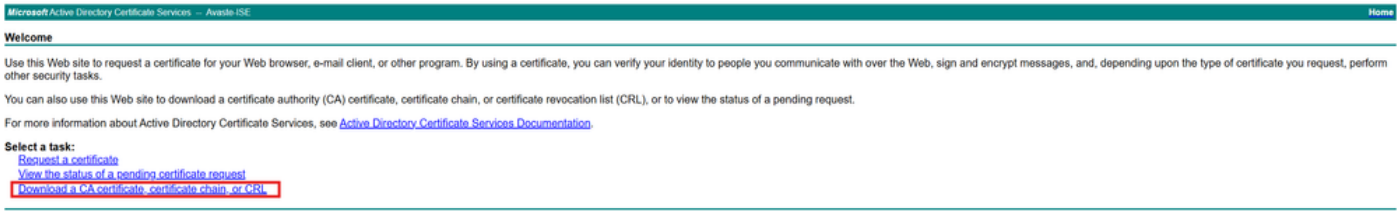
5. Klicken Sie auf Add Client Identity (Client-Identität hinzufügen), um das Zertifikat dem System hinzuzufügen.




6. Klicken Sie auf Einstellungen übernehmen, um die Änderungen zu speichern.

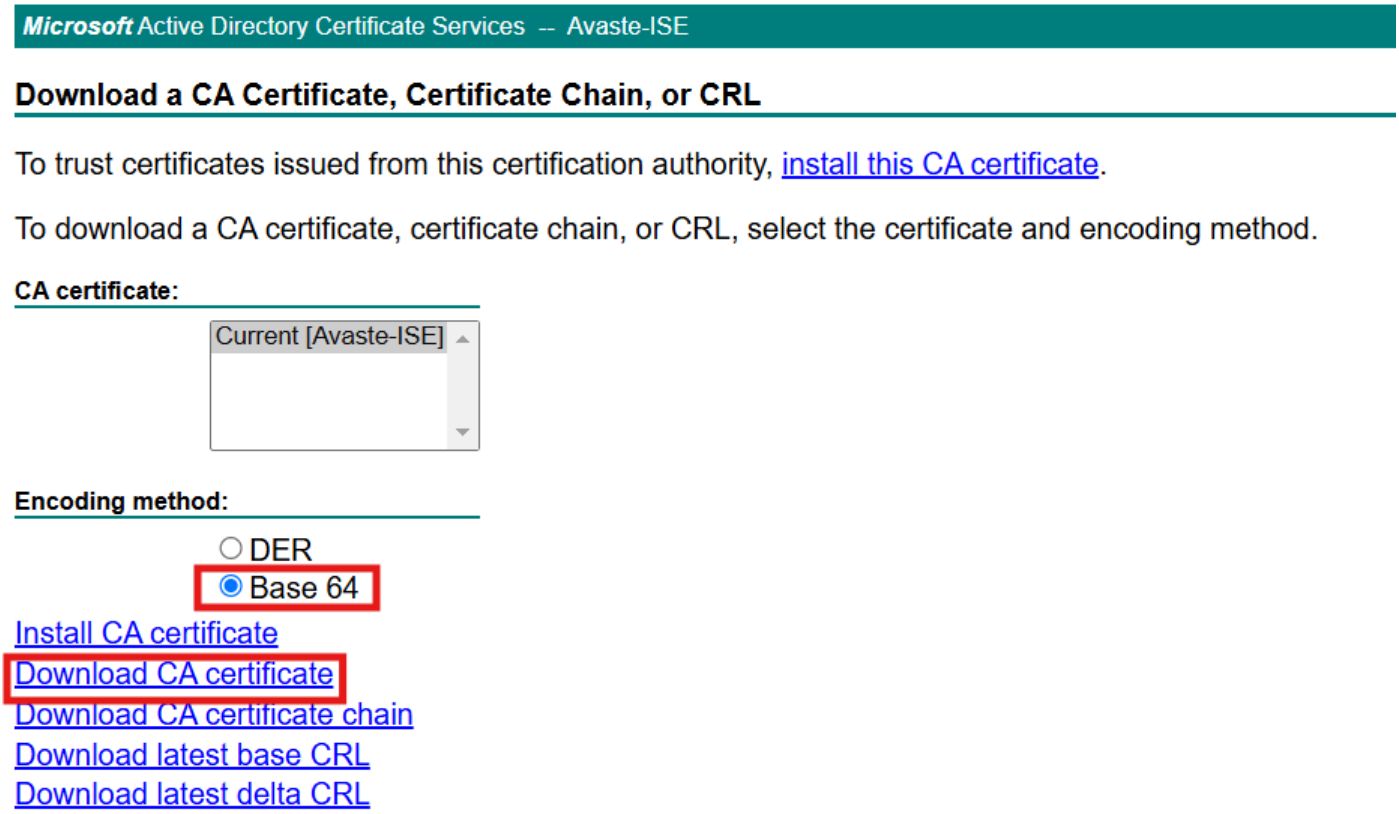
TEIL IV - Importieren des CA-Stammzertifikats in den Manager Trust Store

1. Navigieren Sie zur Homepage des MS Active Directory-Zertifikatdiensts, und wählen Sie CA-Zertifikat, Zertifikatskette oder Zertifikatsperrliste herunterladen aus.




2. Wählen Sie Base-64-Format und klicken Sie dann auf CA-Zertifikat herunterladen.

3. Speichern Sie das Zertifikat als CA_Root.cer.




4. Melden Sie sich bei der StealthWatch Management Console (SMC) an.

5. Wählen Sie im Hauptmenü Configure > Global > Central Management.

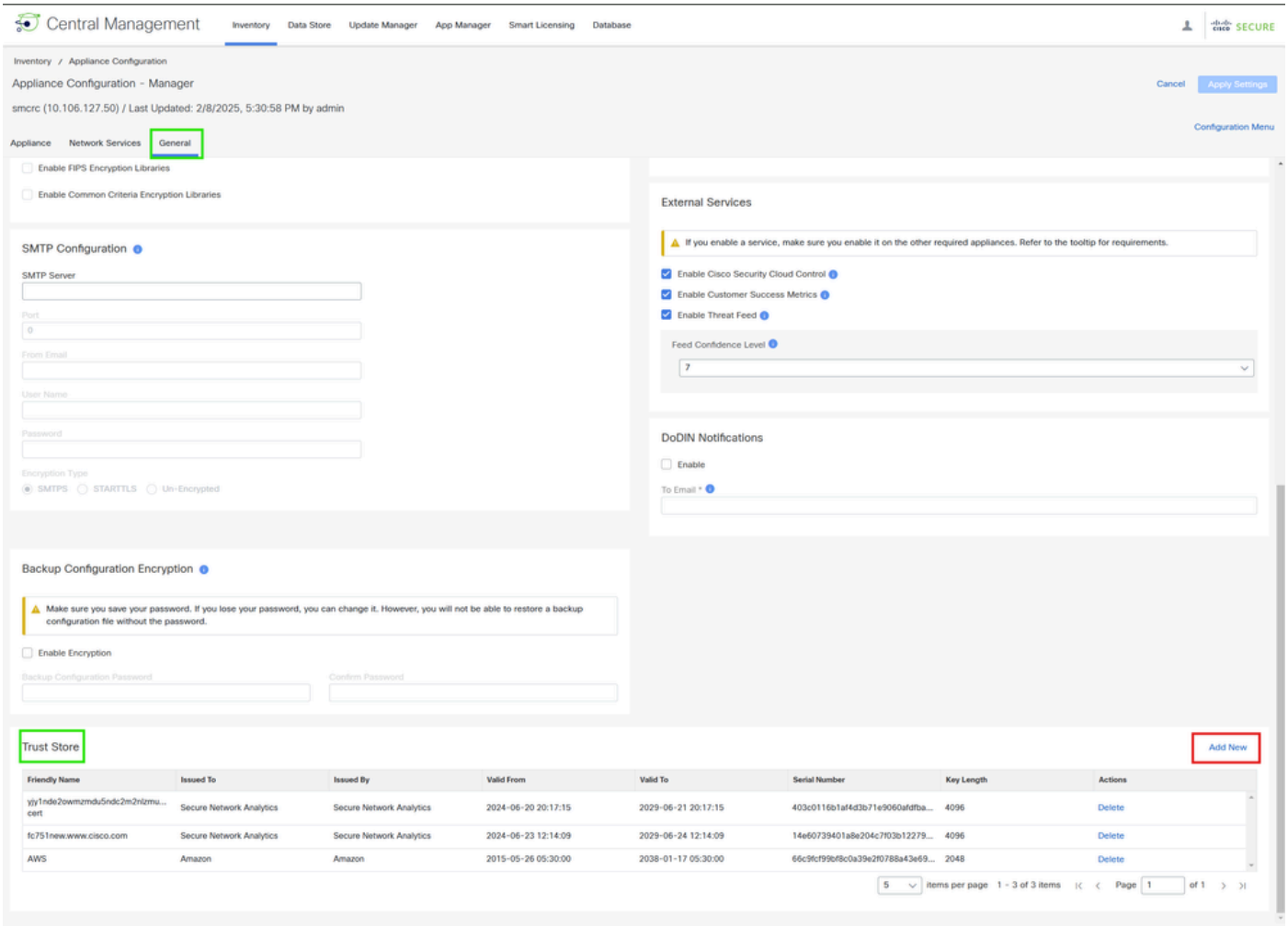
6. Klicken Sie auf der Seite "Inventar" auf das (Auslassungszeichen) Symbol für den Manager.

7. Wählen Sie Einheit-Konfiguration bearbeiten.

8. Wählen Sie die Registerkarte Allgemein.

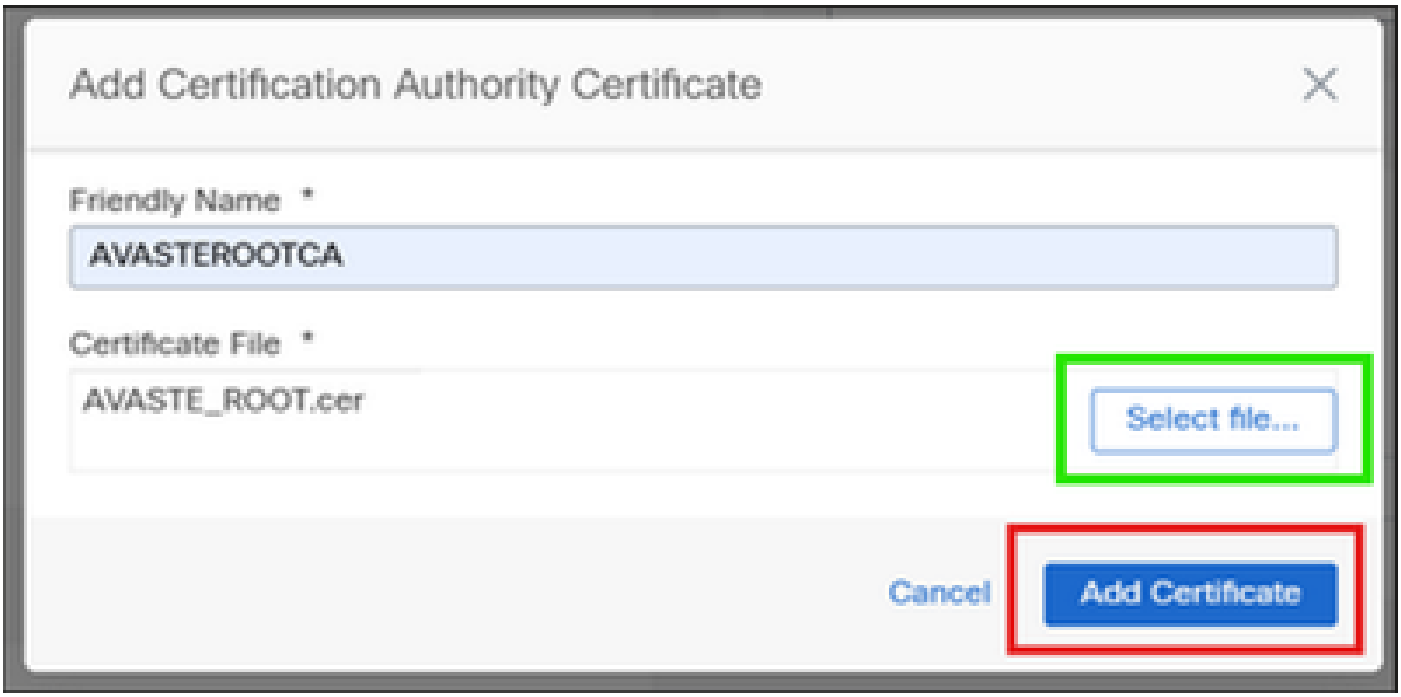
9. Navigieren Sie zum Abschnitt Trust Store, und importieren Sie das zuvor exportierte Zertifikat "CA_Root.cer".

10. Klicken Sie auf Neu hinzufügen.




11. Geben Sie dem Zertifikat einen Anzeigenamen, und klicken Sie dann auf Datei auswählen ..., um das zuvor exportierte ISE-Zertifizierungsstellenzertifikat auszuwählen.

12. Klicken Sie auf Zertifikat hinzufügen, um die Änderungen zu speichern.



13. Klicken Sie auf Einstellungen übernehmen, um die Änderungen zu speichern.

## Abschnitt B: Zertifikatskonfiguration der Cisco Identity Services Engine 3.3

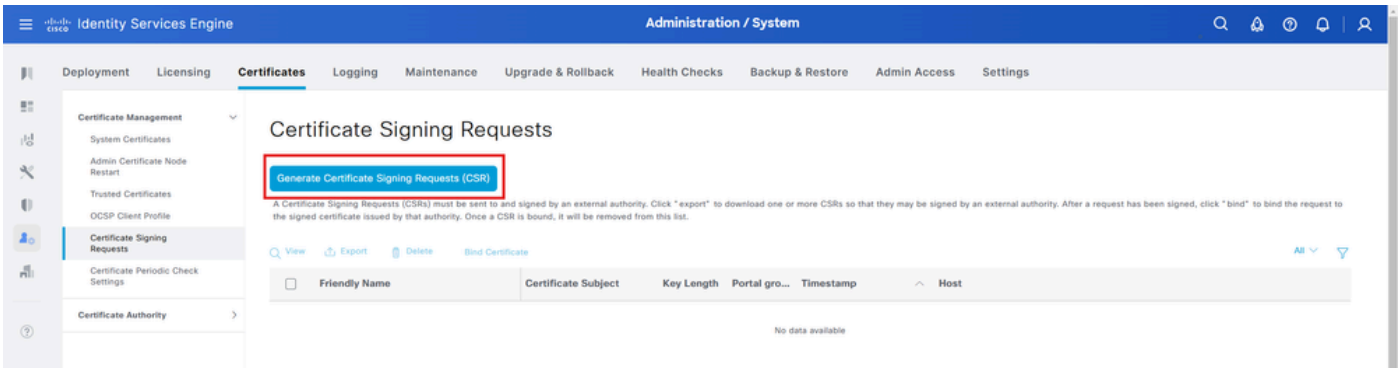
TEIL I - Generieren eines ISE-Server-pxGrid-Zertifikats

Generieren Sie einen CSR für ein pxGrid-Zertifikat des ISE-Servers:

1. Melden Sie sich bei der Cisco Identity Services Engine (ISE)-GUI an.

2. Navigieren Sie zu Administration > System > Certificates > Certificate Management > Certificate Signing Requests.

3. Wählen Sie Zertifikatsignierungsanforderung (CSR) generieren aus.

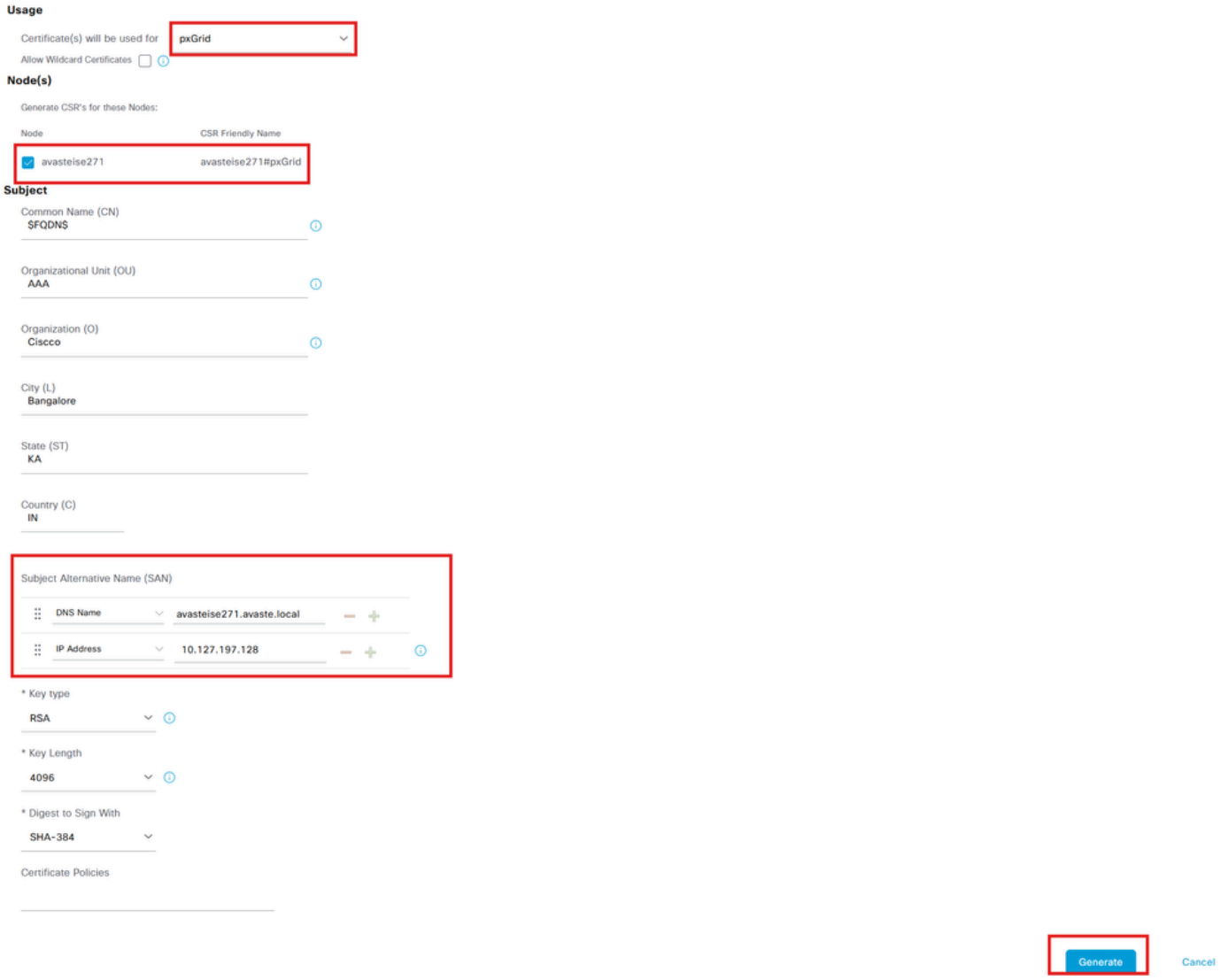



4. Wählen Sie pxGrid im Feld Zertifikat(e) wird verwendet für.

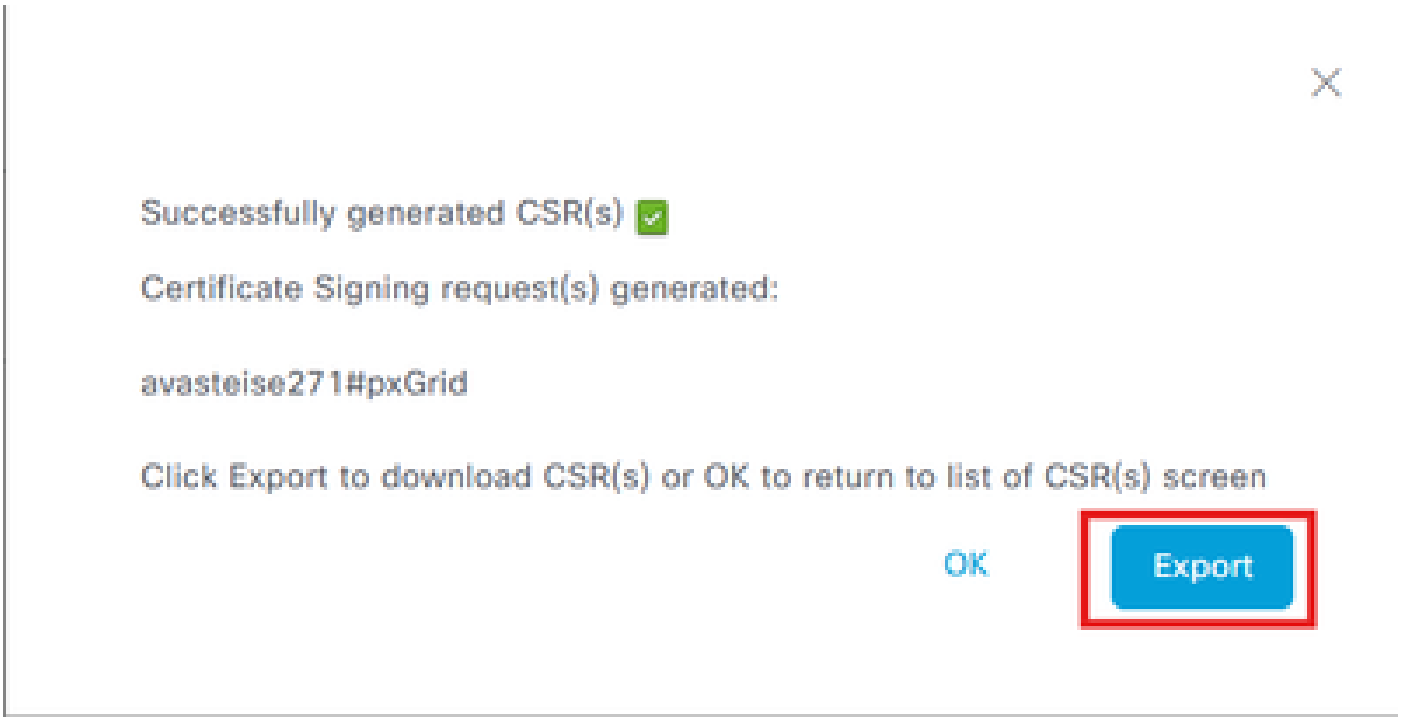
5. Wählen Sie den ISE-Knoten, für den das Zertifikat generiert wird.

6. Geben Sie bei Bedarf weitere Angaben zu den Zertifikaten ein.

7. Klicken Sie auf Generieren.



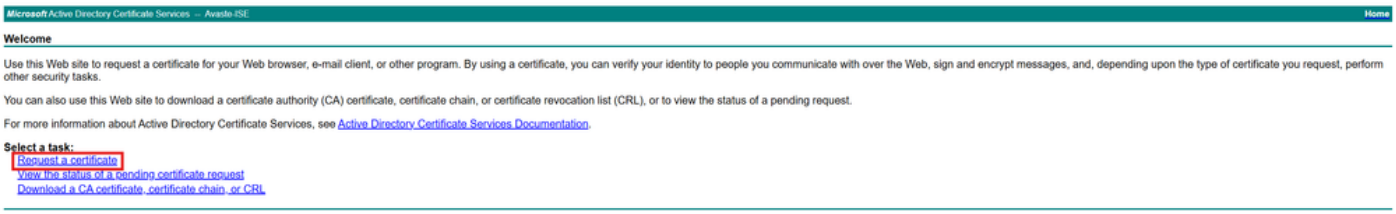

8. Klicken Sie auf Exportieren und die Datei lokal speichern.



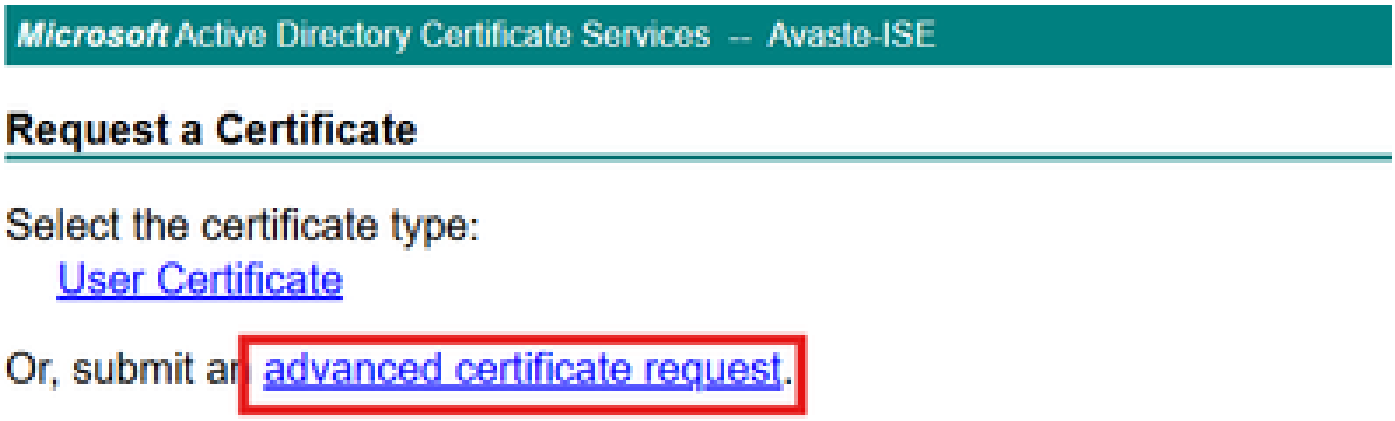
TEIL II - Erstellen eines ISE-Server-pxGrid-Zertifikats mithilfe einer externen Zertifizierungsstelle

1. Navigieren Sie zum MS Active Directory-Zertifikatdienst, https://server/certsrv/, wobei Server die IP-Adresse oder der DNS des MS-Servers ist.

2. Klicken Sie auf Zertifikat anfordern.

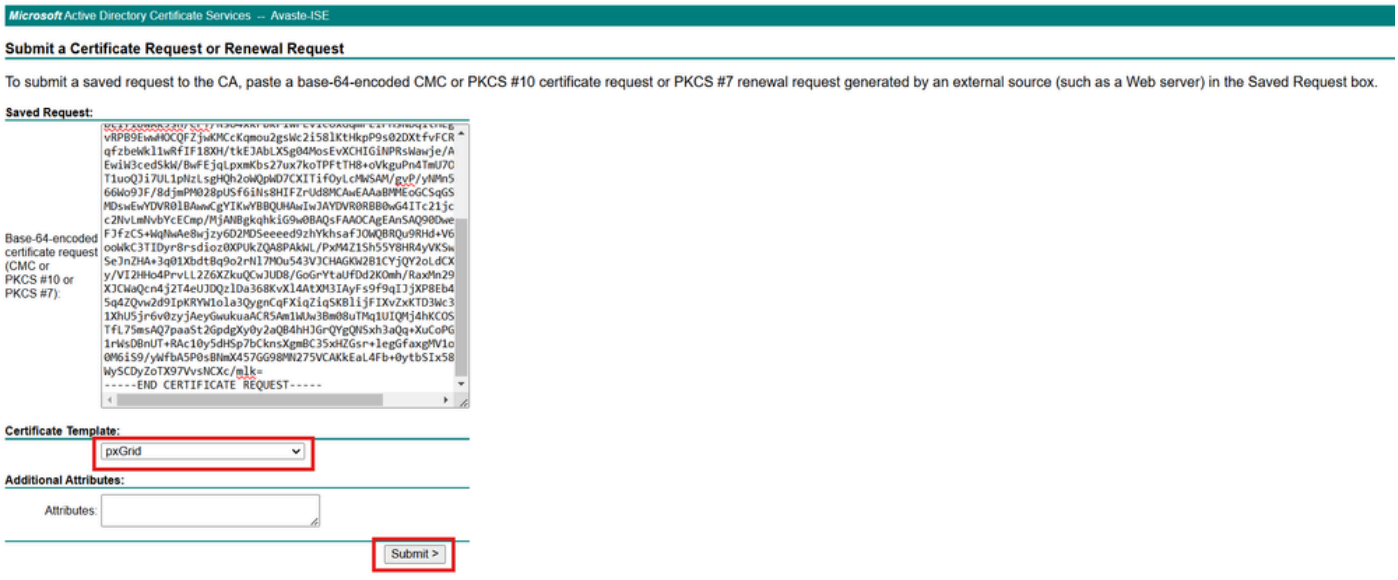


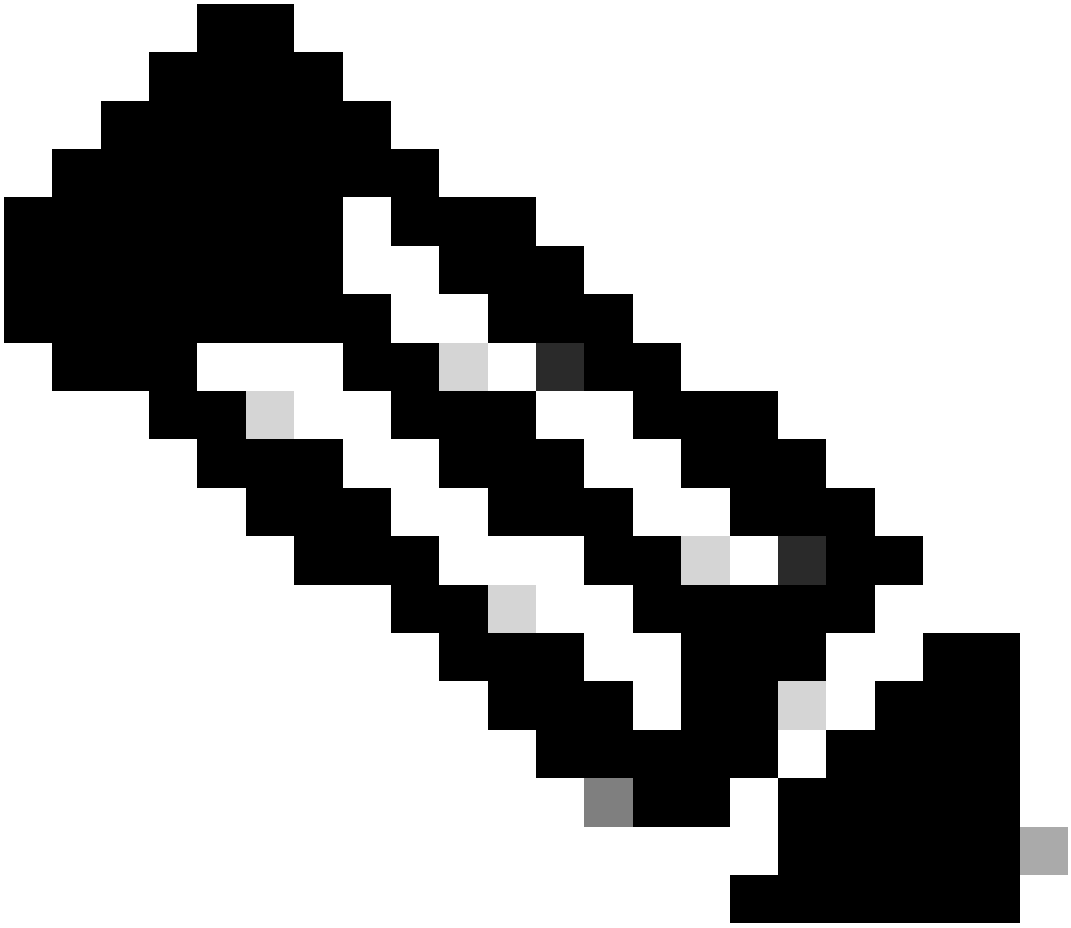

3. Wählen Sie diese Option, um eine Anforderung für ein erweitertes Zertifikat zu senden.




4. Kopieren Sie den Inhalt der CSR-Anfrage aus dem vorherigen Abschnitt in das Feld "Gespeicherter Antrag".

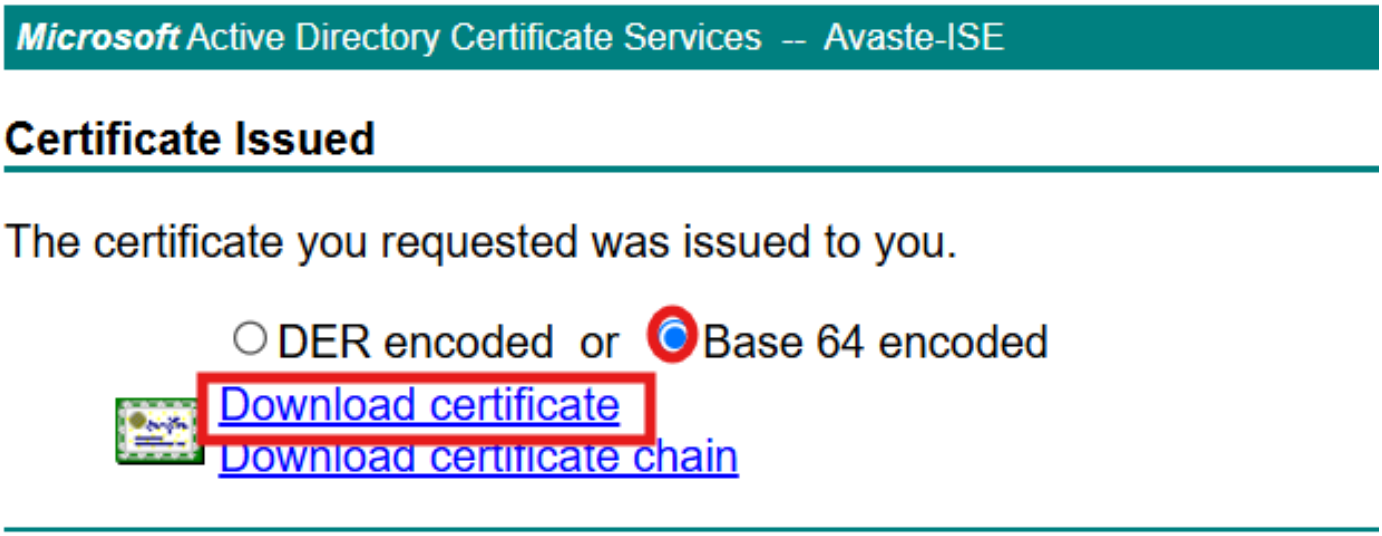
5. Wählen Sie pxGrid als Zertifikatvorlage aus, und klicken Sie dann auf Senden.





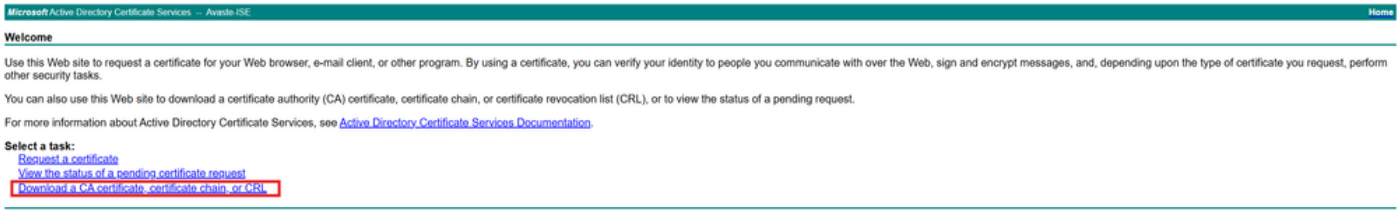
Anmerkung: Die verwendete Zertifikatvorlage pxGrid benötigt sowohl die Client- als auch die Serverauthentifizierung im Feld "Enhanced Key Usage" (Erweiterte Schlüsselverwendung).

6. Laden Sie das generierte Zertifikat im Base-64-Format herunter und speichern Sie es unter ISE_pxGrid.cer.

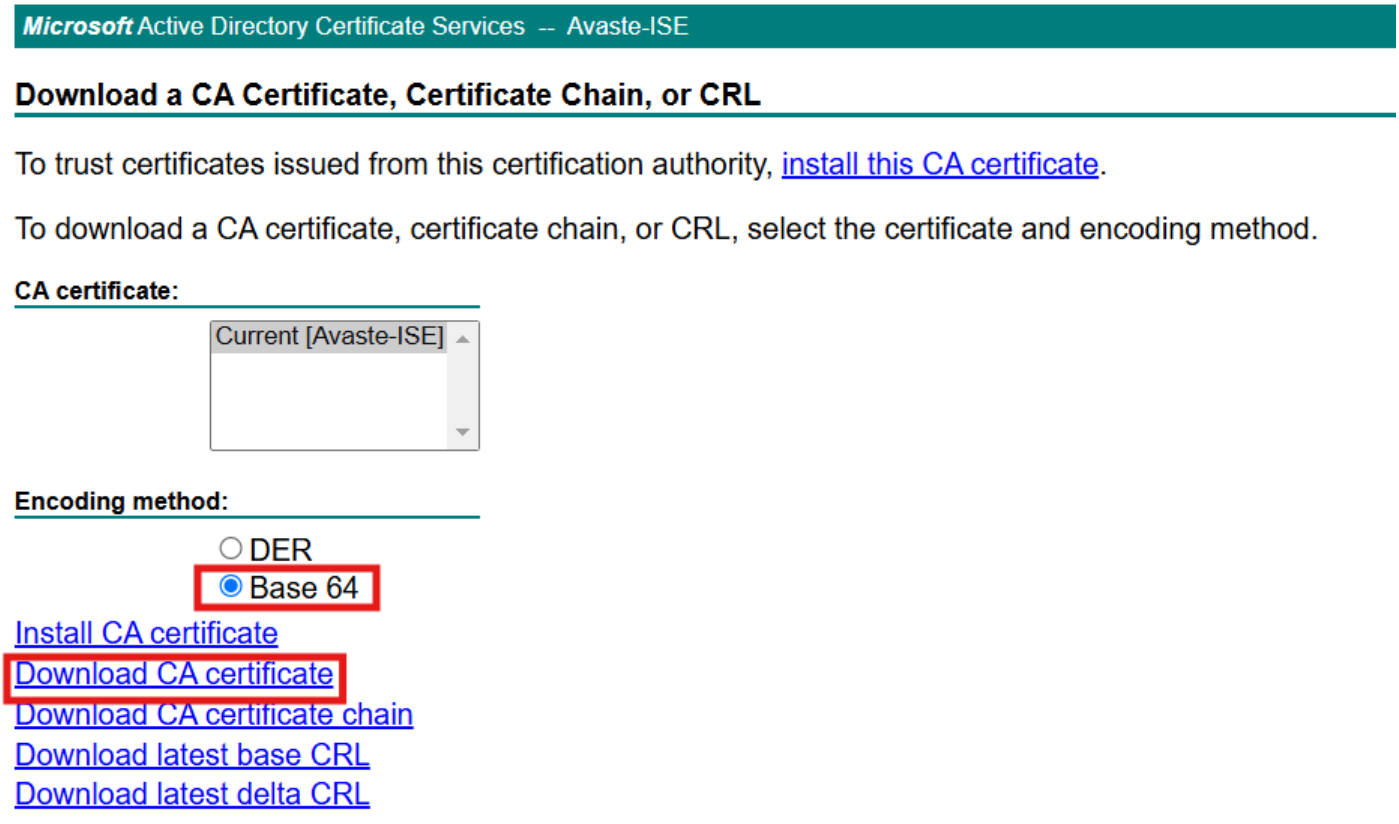



TEIL III - Importieren des CA-Stammzertifikats in den ISE Trust Store

1. Navigieren Sie zur Homepage des MS Active Directory-Zertifikatdiensts, und wählen Sie Download a CA certificate, certificate chain or CRL (Zertifizierungsstellenzertifikat herunterladen) aus.



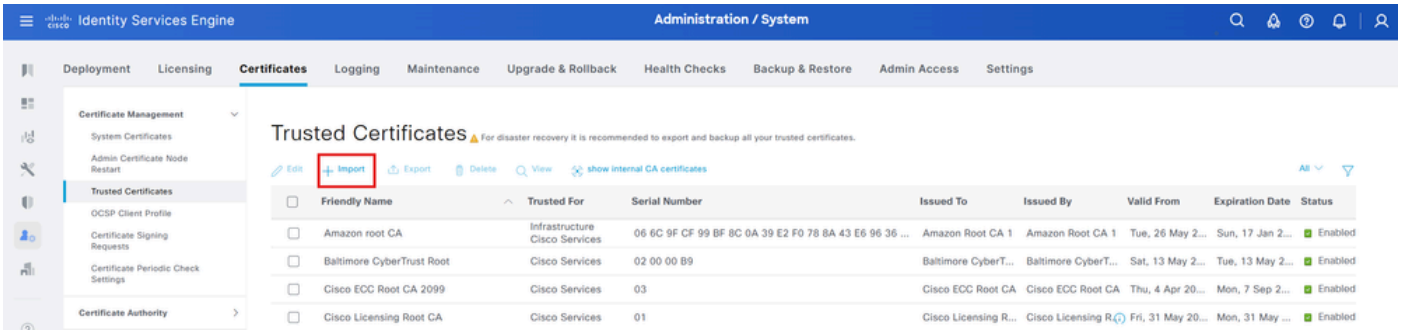

2. Wählen Sie Base-64-Format und klicken Sie dann auf CA-Zertifikat herunterladen.



3. Speichern Sie das Zertifikat als CA_Root.cer.

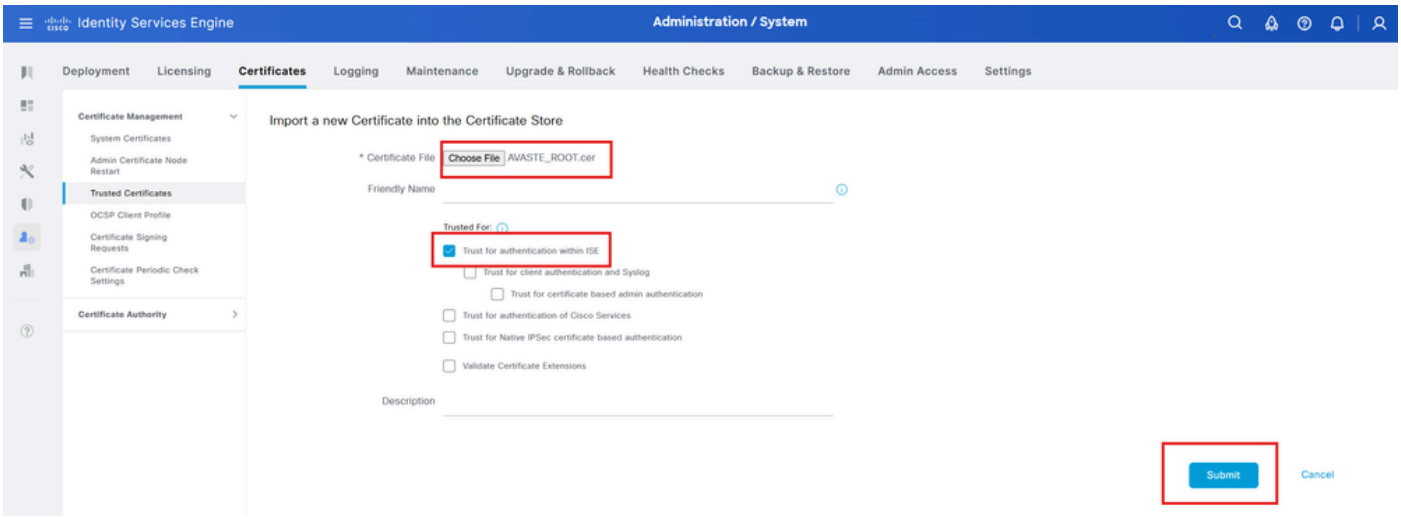
4. Melden Sie sich bei der Cisco Identity Services Engine (ISE)-GUI an.

5. Wählen Sie Administration > System > Certificates > Certificate Management > Trusted Certificates.




6. Wählen Sie Importieren > Zertifikatsdatei und Importieren Sie das Stammzertifikat.

7. Stellen Sie sicher, dass das Kontrollkästchen Bei Authentifizierung innerhalb der ISE vertrauen aktiviert ist.



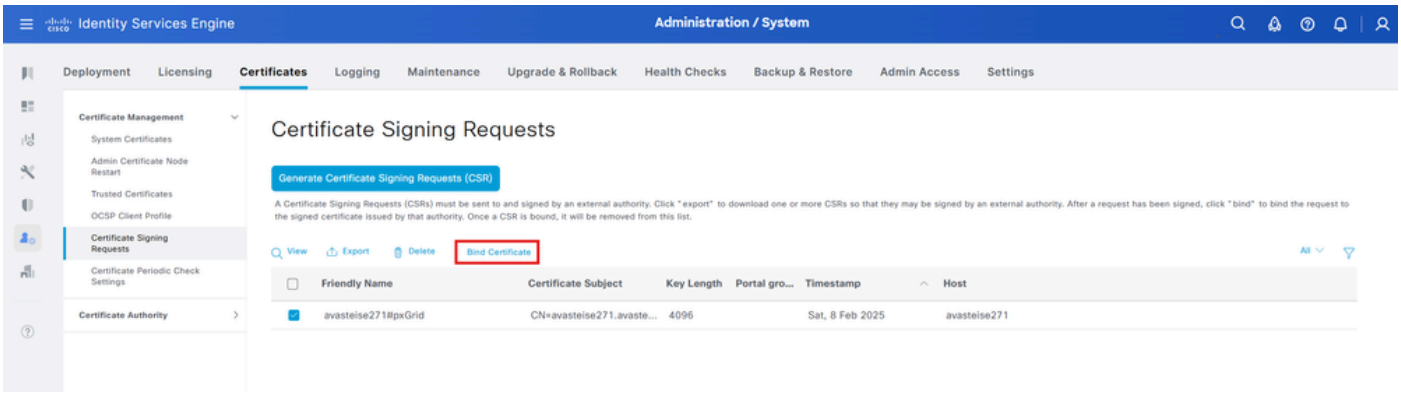

8. Klicken Sie auf Senden.

TEIL IV - Bindung des ISE-Zertifikats an die Certificate Signing Request (CSR)

1. Melden Sie sich bei der Cisco Identity Services Engine (ISE)-GUI an.

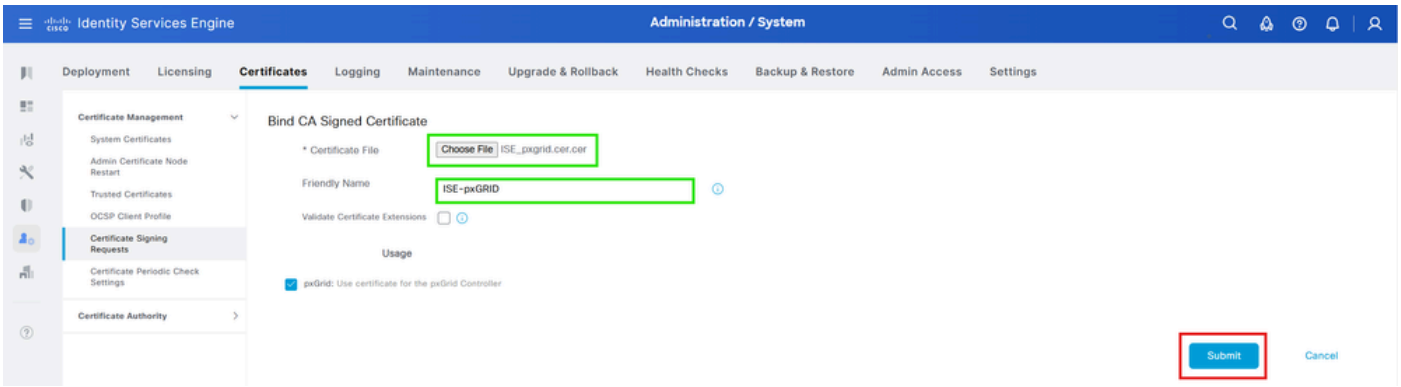
2. Wählen Sie Administration > System > Certificates > Certificate Management > Certificate Signing Requests.

3. Wählen Sie den im vorherigen Abschnitt erstellten CSR, und klicken Sie dann auf Zertifikat binden.




4. Wählen Sie im Formular "Bind CA Signed Certificate" (Signiertes Zertifikat der Bindungszertifizierungsstelle) das zuvor generierte Zertifikat ISE_pxGrid.cer.

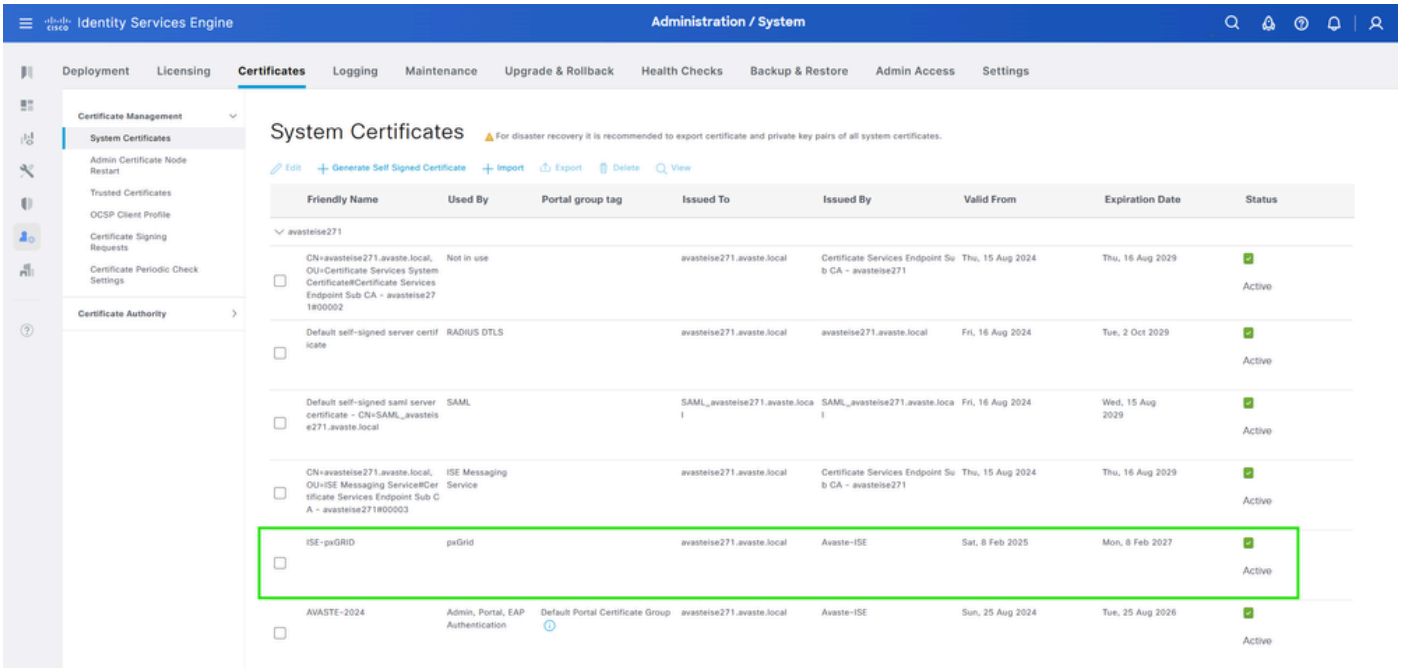
5. Geben Sie dem Zertifikat einen Anzeigenamen, und klicken Sie dann auf Senden.




7. Klicken Sie auf Ja, wenn das System das Zertifikat ersetzen soll.

8. Wählen Sie Administration > System > Certificates > System Certificates.

9. Sie können das erstellte pxGrid-Zertifikat in der Liste sehen, das von der externen Zertifizierungsstelle signiert wurde.

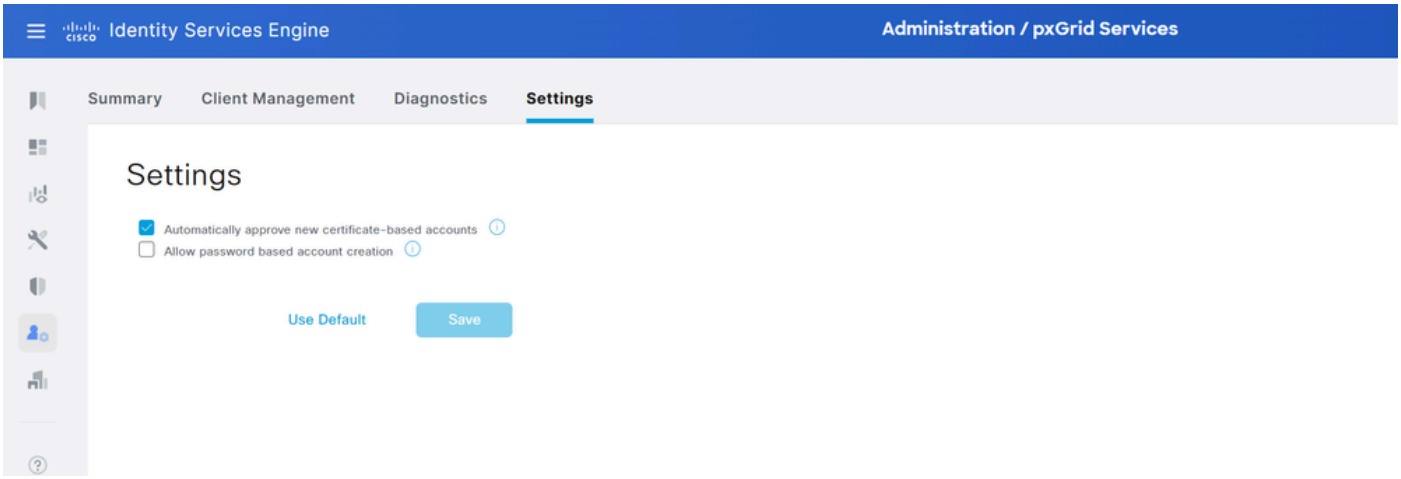


Zertifikate werden jetzt bereitgestellt. Fahren Sie mit der Integration fort.

## Integration

Bevor Sie mit der Integration beginnen, stellen Sie Folgendes sicher:

Für Cisco ISE unter Administration > pxGrid Services > Settings and Check Neue zertifikatbasierte Konten für Client-Anforderung zum automatischen Genehmigen und Speichern automatisch genehmigen.

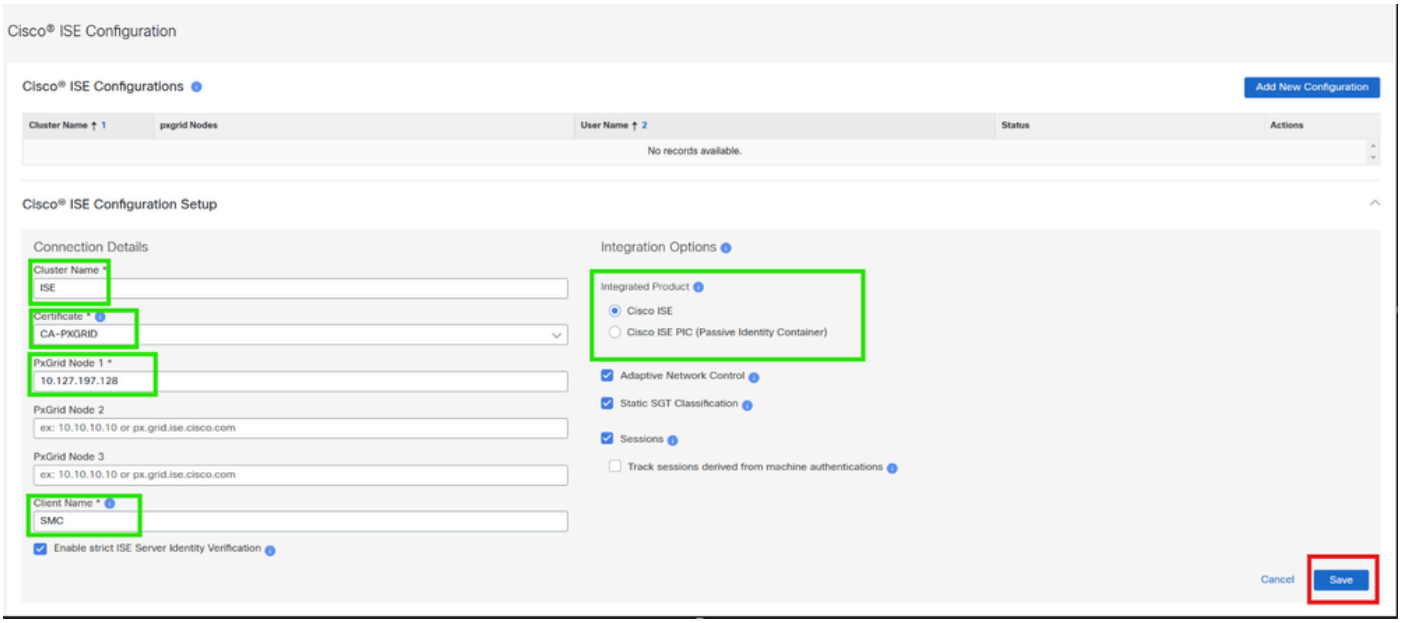



So öffnen Sie auf der StealthWatch Management Console (SMC) die Seite ISE Configuration Setup (ISE-Konfiguration einrichten):

1. Wählen Sie Configure > Integrations > Cisco ISE.

2. Klicken Sie in der oberen rechten Ecke der Seite auf Neue Konfiguration hinzufügen.

3. Geben Sie den Clusternamen ein, wählen Sie das Zertifikat & Integrationsprodukt, die pxGrid-Knoten-IP aus, und klicken Sie auf Speichern.

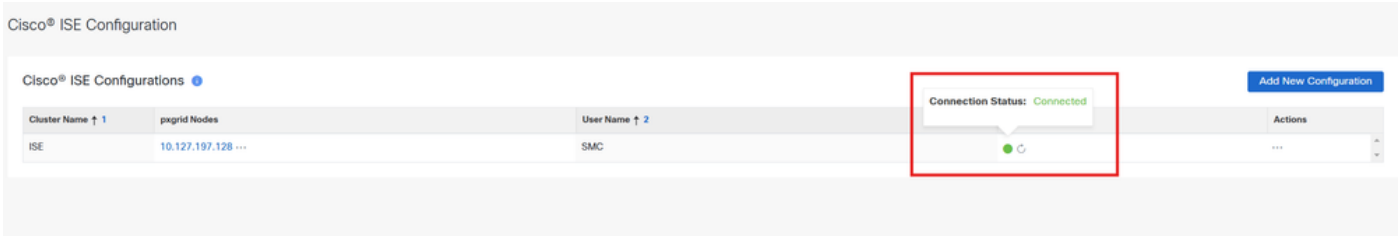



## Überprüfung

Aktualisieren Sie die ISE-Konfigurationsseite auf der StealthWatch Management Console (SMC).

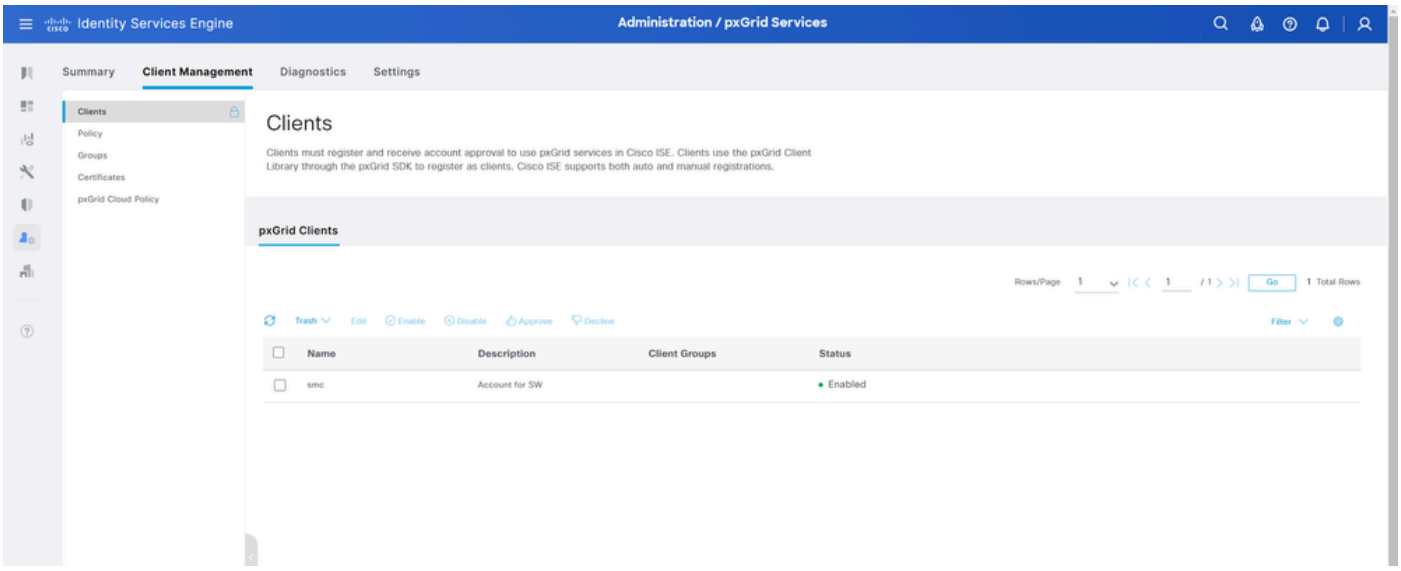
1. Kehren Sie zur ISE-Konfigurationsseite in der Web-App zurück, und aktualisieren Sie die Seite.

2. Vergewissern Sie sich, dass die Knotenstatusanzeige neben dem entsprechenden IP-Adressfeld grün leuchtet und anzeigt, dass eine Verbindung zum ISE- oder ISE-PIC-Cluster hergestellt wurde.




Navigieren Sie auf der Cisco ISE zu Administration > pxGrid Services > Client Management > Clients.

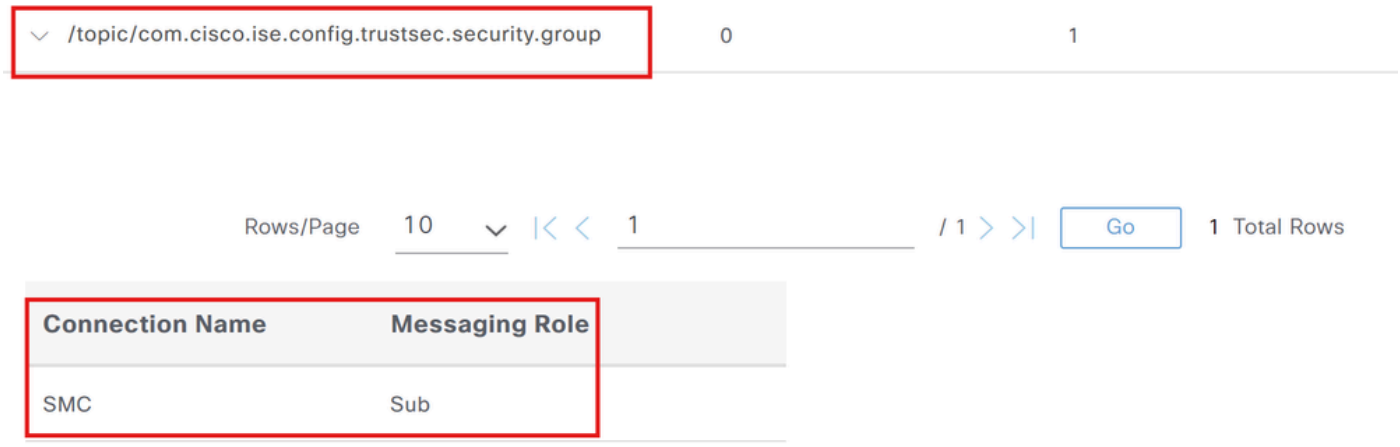
Dadurch wird der SMC als pxgrid-Client mit dem Status Enabled (Aktiviert) generiert.



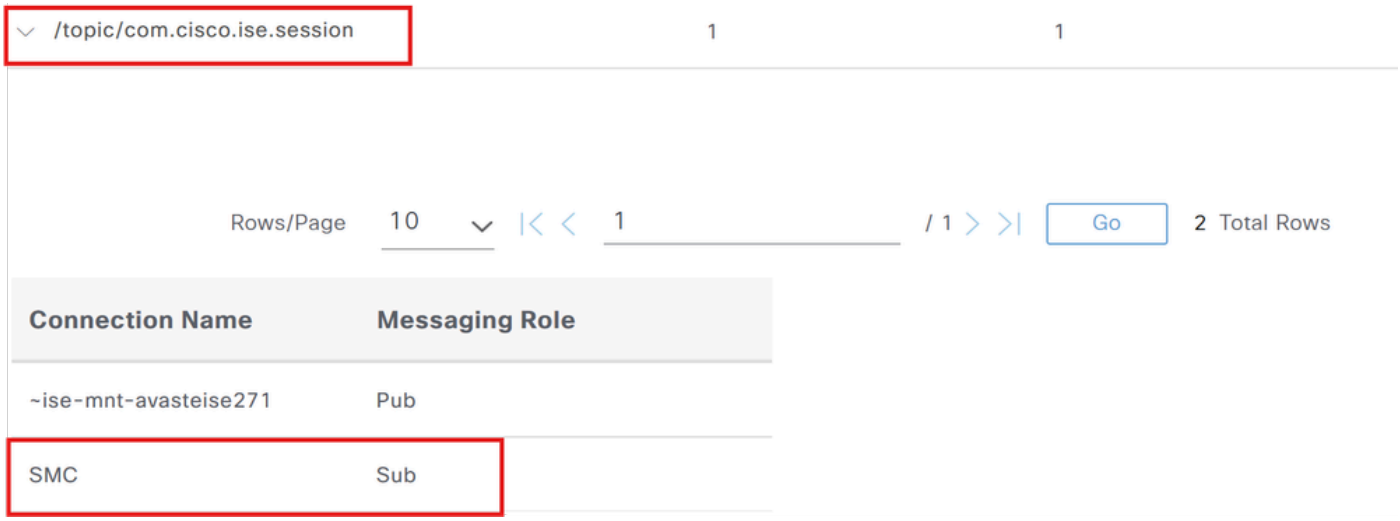

Um das Themenabonnement auf der Cisco ISE zu überprüfen, navigieren Sie zu Administration > pxGrid Services > Diagnostics > WebSocket > Topics.

Dadurch wird eine SMC erstellt, die für diese Themen abonniert ist.

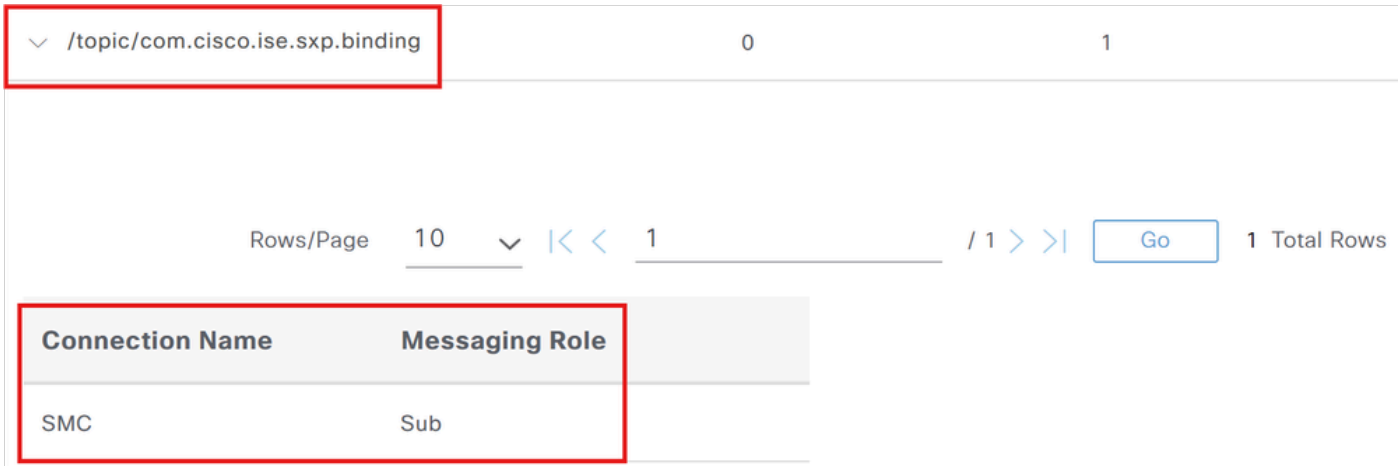
TrustSec SGT-Thema




ISE-Sitzungsverzeichnisthema




ISE SXP-Bindungen - Thema




Cisco ISE Pxgrid-server.log auf TRACE-Ebene.

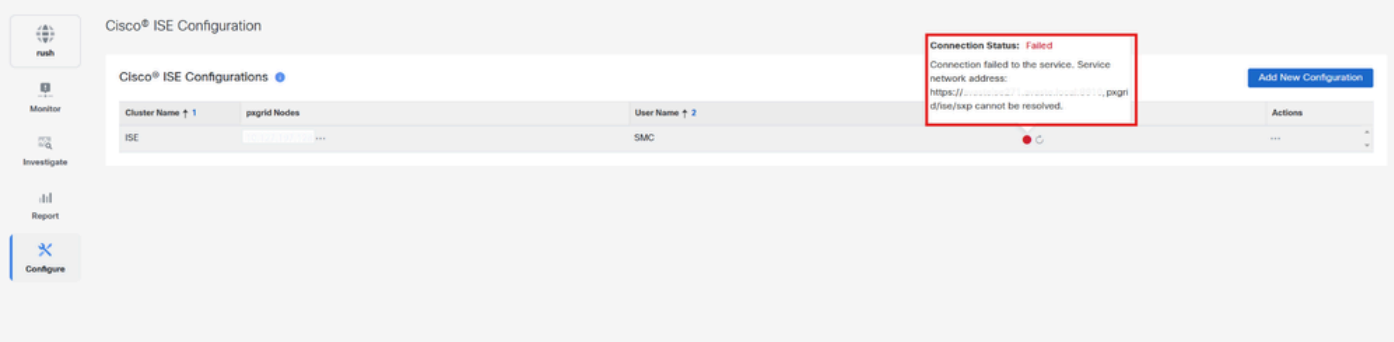
```
2025-02-08 18:07:11,086 TRACE  [pxgrid-http-pool15][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribu
2025-02-08 18:07:11,087 TRACE  [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint
2025-02-08 18:07:11,102 TRACE  [pxgrid-http-pool19][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint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

# Fehlerbehebung

DNS-Auflösung

Daraus ergibt sich die Fehlermeldung "Connection Status; Fehler beim Verbinden mit dem Dienst. Servicenetzwerkadresse: https:isehostnameme.domain.com:891pxgridiisessxpxp kann nicht aufgelöst werden":




Lösung

Im Idealfall muss dies auf dem DNS-Server behoben werden, damit Forward- und Reverse-Lookups für diesen ISE-FQDN durchgeführt werden können. Für eine lokale Lösung kann jedoch eine temporäre Problemumgehung hinzugefügt werden:

1. Melden Sie sich bei der StealthWatch Management Console (SMC) an.

2. Wählen Sie im Hauptmenü Configure > Global > Central Management.

3. Klicken Sie auf der Seite "Inventar" auf das Symbol (Ellipse) für den Manager.

4. Wählen Sie Einheit-Konfiguration bearbeiten.

5. Network Services-Registerkarte und fügen Sie einen lokalen Auflösungseintrag für diesen ISE FQDN hinzu.


Unbekannter Zertifizierungsstellenfehler oder fehlendes vertrauenswürdiges Zertifikat

Dies erzeugt eine Fehlermeldung, die lautet: "ISE präsentiert ein Zertifikat, das von diesem Manager nicht vertrauenswürdig ist":


Ein ähnlicher Protokollverweis ist in der Datei "oSMCMsvcvisese-client.log" zu finden. Pfad: 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.
```

Lösung

1. Melden Sie sich bei der StealthWatch Management Console (SMC) an.

2. Wählen Sie im Hauptmenü Configure > Global > Central Management.

3. Klicken Sie auf der Inventarseite auf das (Auslassungszeichen) Symbol für den Manager.

4. Wählen Sie Einheit-Konfiguration bearbeiten.

5. Wählen Sie die Registerkarte Allgemein.

6. Navigieren Sie zum Abschnitt "Trust Store", und stellen Sie sicher, dass der Aussteller des PXGridid-Zertifikats der Cisco ISE Teil des Trust Store ist.

## Bekannte Fehler

| Bug-ID | Beschreibung |
|---|---|
| Cisco Bug-ID: 18119 | ISE wählt nicht unterstütztes Cipher-ITLS-Server-Hello Packet aus |
| Cisco Bug-ID: 01634 | Geräte können nicht mithilfe der EPS-Bedingung in Quarantäne verschoben werden |

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.