Integrazione di ISE 3.3 con Stealthwatch 7.5.1 tramite un'autorità di certificazione esterna

Sommario

Introduzione

Questo documento descrive le procedure per integrare ISE 3.3 con Secure Network Analytics (Stealthwatch) usando le connessioni pxGrid.

Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Identity Services Engine
- Piattaforma Exchange Grid (pxGrid)
- Secure Network Analytics (Stealthwatch)
- Certificati TLS/SSL.
- PKI su Windows Server 2016

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Patch 4 per Identity Services Engine (ISE) versione 3.3
- Secure Network Analytics (Stealthwatch) 7.5.1
- Windows Server 2016 come server CA esterno.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

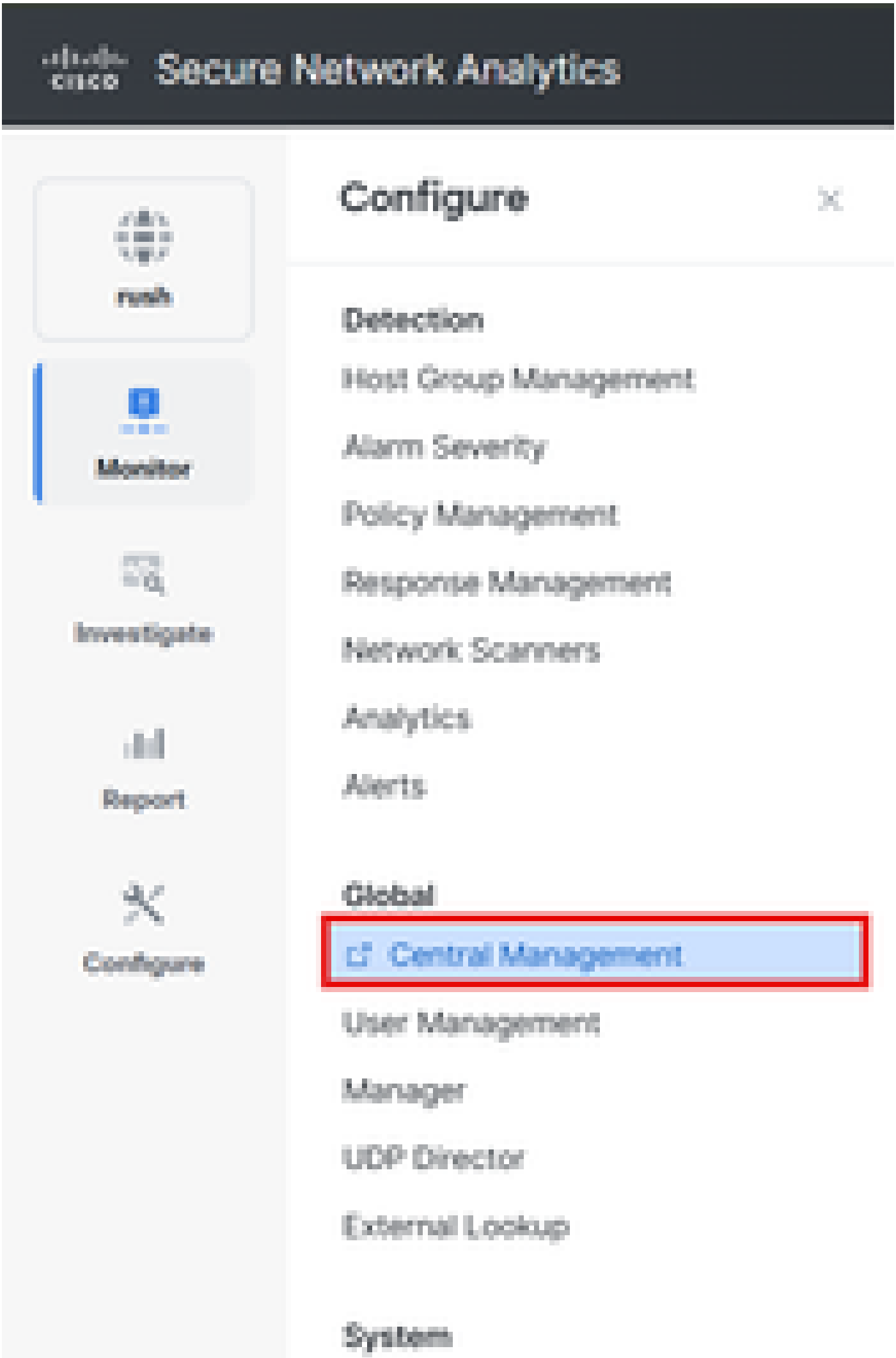
Configurazione

Sezione A: Configurazione certificato Secure Network Analytics (Stealthwatch)

Parte I - Generazione di un CSR per il certificato client PxGrid di Secure Network Analytics

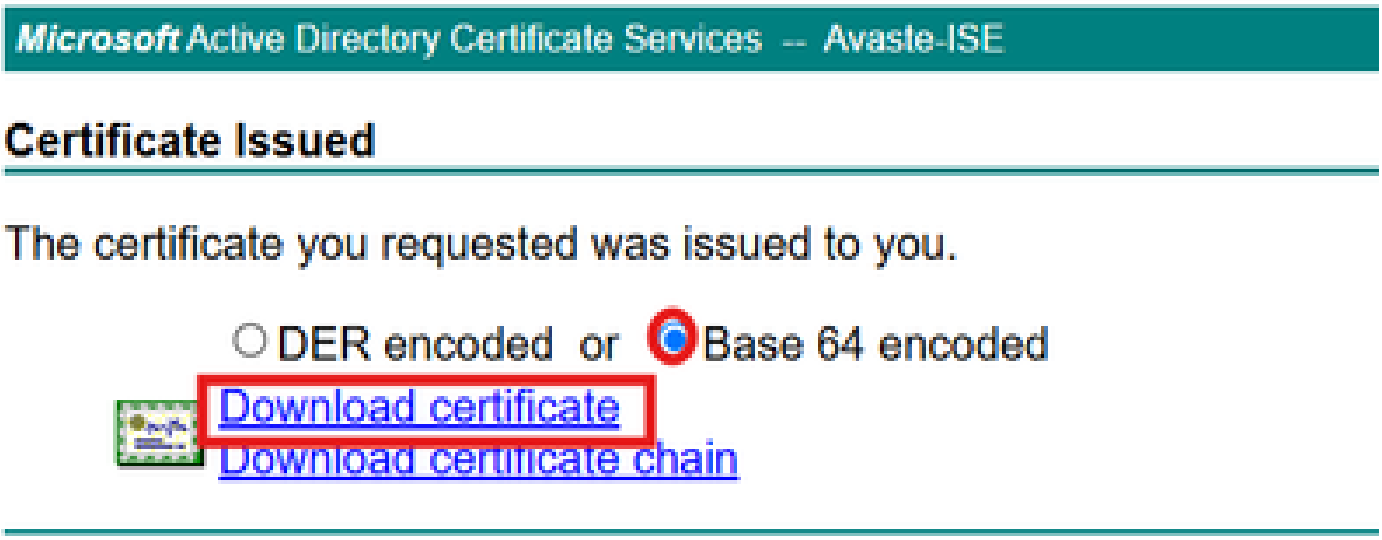
1. Accedere a Stealthwatch Management Console (SMC).

2. Dal menu principale, selezionare Configura > Globale > Gestione centrale.


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

Il modello di certificato pxGrid utilizzato richiede sia l'autenticazione client che l'autenticazione server nel campo "Utilizzo chiavi avanzato".

6. Scaricare un certificato generato in formato Base-64 e salvarlo come pxGrid_client.cer.



PARTE III - Aggiunta del certificato client pxGrid di Secure Network Analytics a Gestione

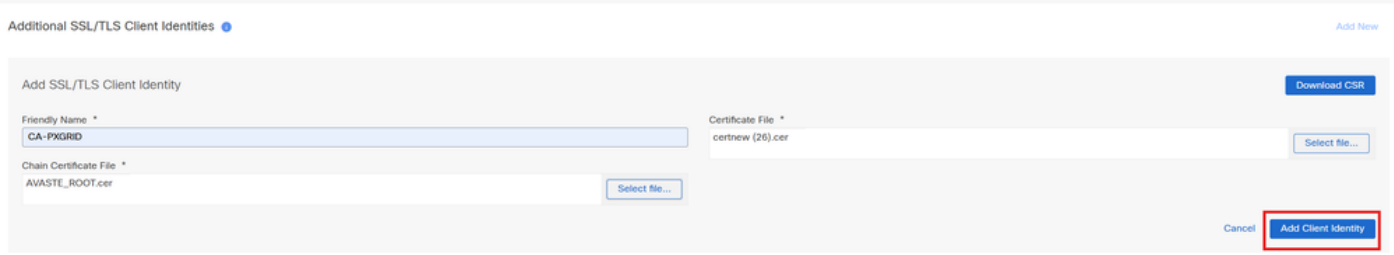
1.Passare alla sezione Identità client SSL/TLS aggiuntive della configurazione manager in Gestione centrale.

2. La sezione Identità client SSL/TLS aggiuntive contiene un modulo per importare il certificato client creato.

3. Assegnare al certificato un nome descrittivo, quindi fare clic su Seleziona file per individuare il file del certificato.

4. Selezionare il file radice o il file della catena di certificati dell'autorità di certificazione o il file della catena di certificati (.pem / .cer / .crt) nella sezione File di certificati della catena.

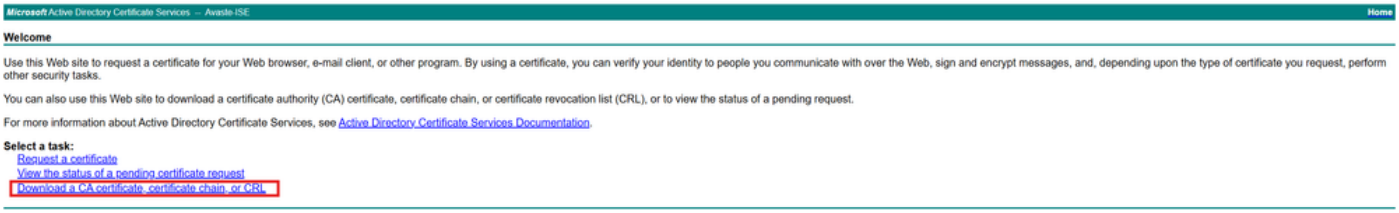
5. Fare clic su Aggiungi identità client per aggiungere il certificato al sistema.



6. Fare clic su Applica impostazioni per salvare le modifiche.

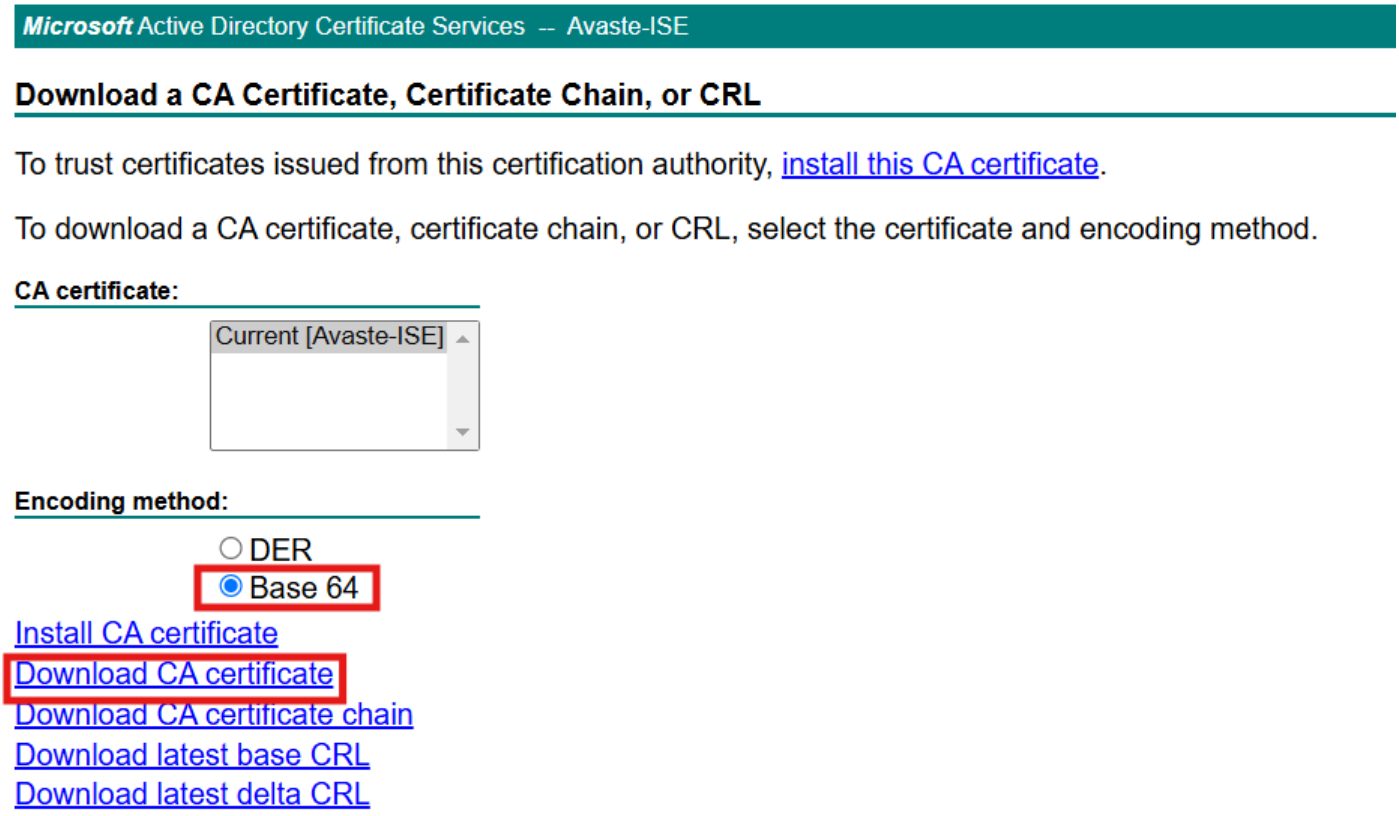
PARTE IV - Importazione del certificato radice CA nell'archivio di attendibilità del manager

1. Passare alla home page del servizio certificati Microsoft Active Directory e selezionare Scarica un certificato CA, una catena di certificati o un elenco di revoche di certificati.



2. Selezionare il formato Base 64, quindi fare clic su Scarica certificato CA.

3. Salvare il certificato come CA_Root.cer.



4. Accedere a Stealthwatch Management Console (SMC).

5. Dal menu principale, selezionare Configura > Globale > Gestione centrale.

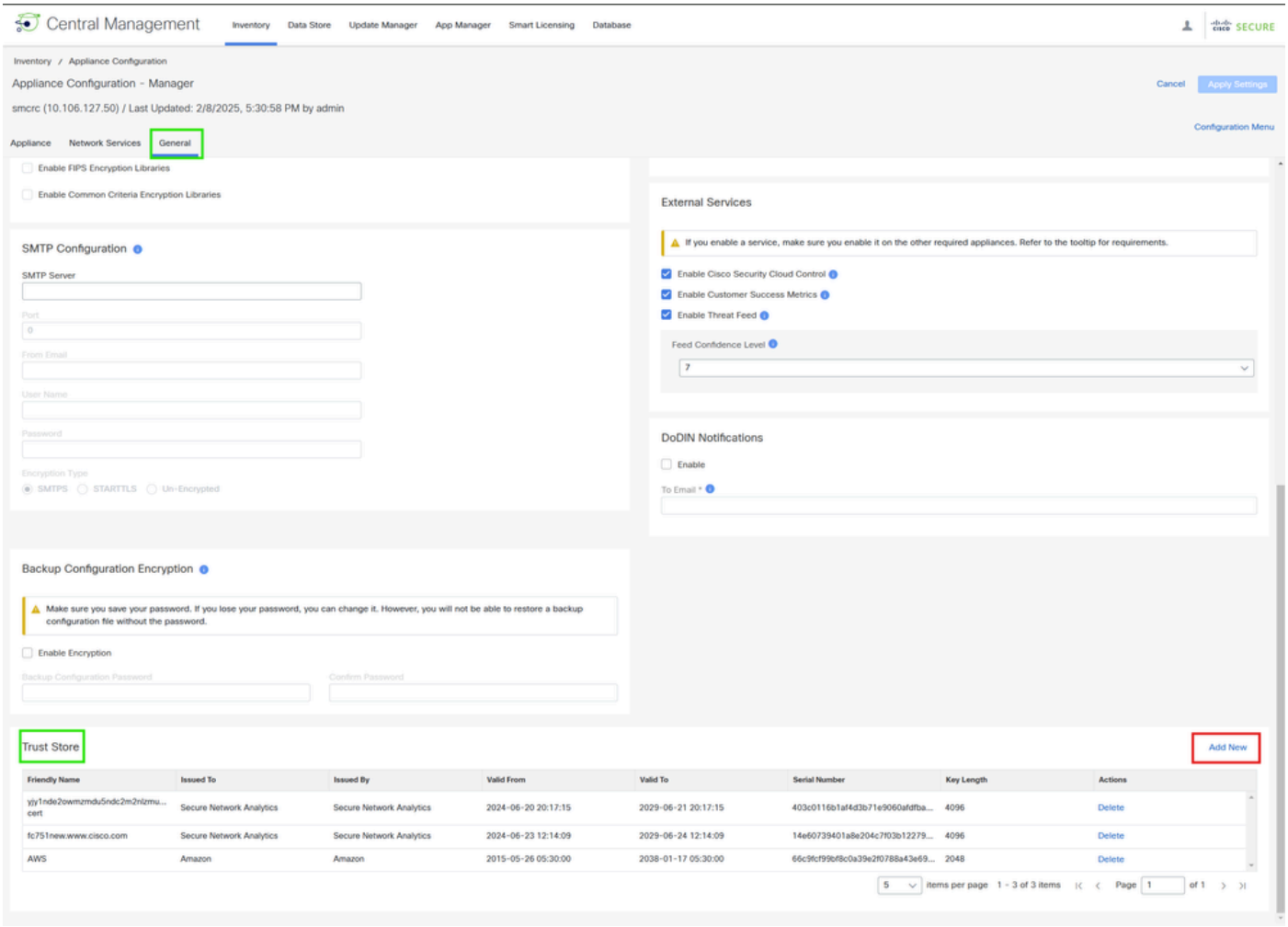
6. Nella pagina Magazzino, fare clic sull'icona (con i puntini di sospensione) del Manager.

7. Scegliere Modifica configurazione accessorio.

8. Selezionare la scheda Generale.

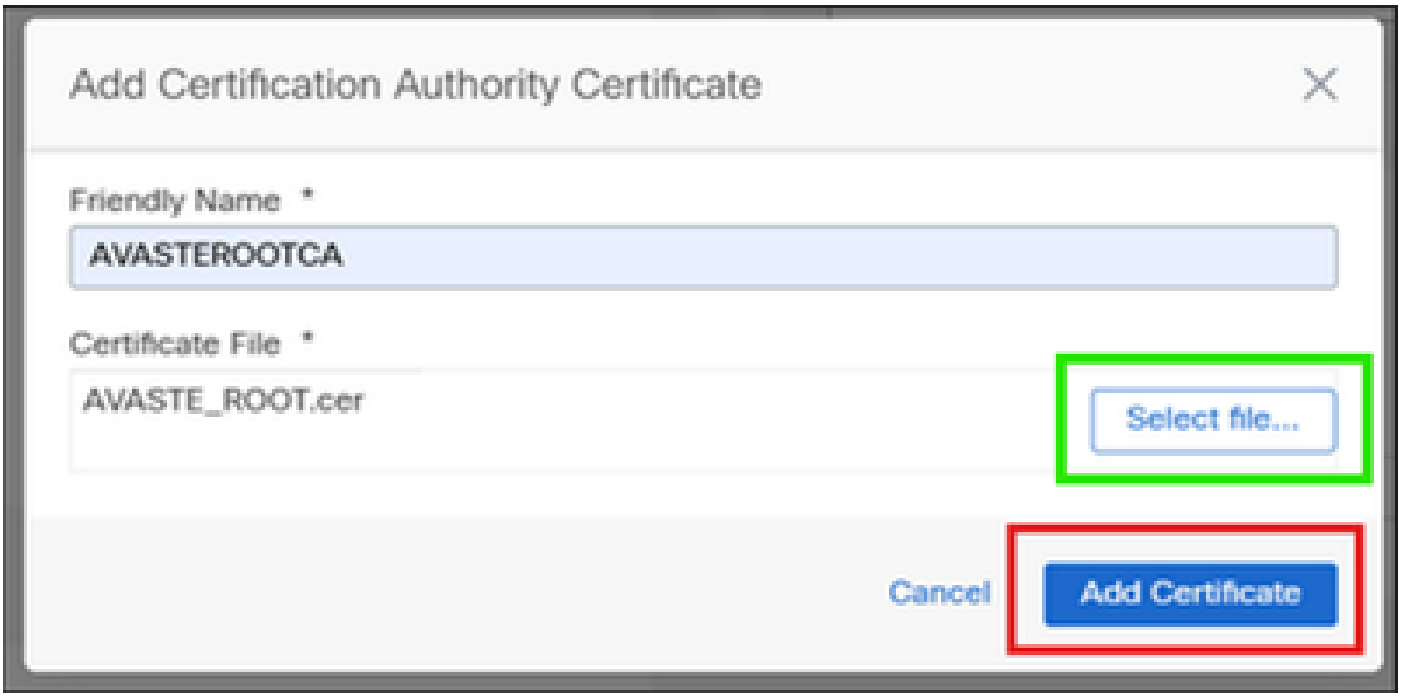
9. Passare alla sezione Archivio attendibile e importare il certificato CA_Root.cer esportato in precedenza.

10. Fare clic su Aggiungi nuovo.



11. Assegnare al certificato un nome descrittivo, quindi fare clic su Seleziona file... per selezionare il certificato CA ISE esportato in precedenza.

12. Fare clic su Aggiungi certificato per salvare le modifiche.



13. Fare clic su Applica impostazioni per salvare le modifiche.

Sezione B: Configurazione certificato Cisco Identity Services Engine 3.3

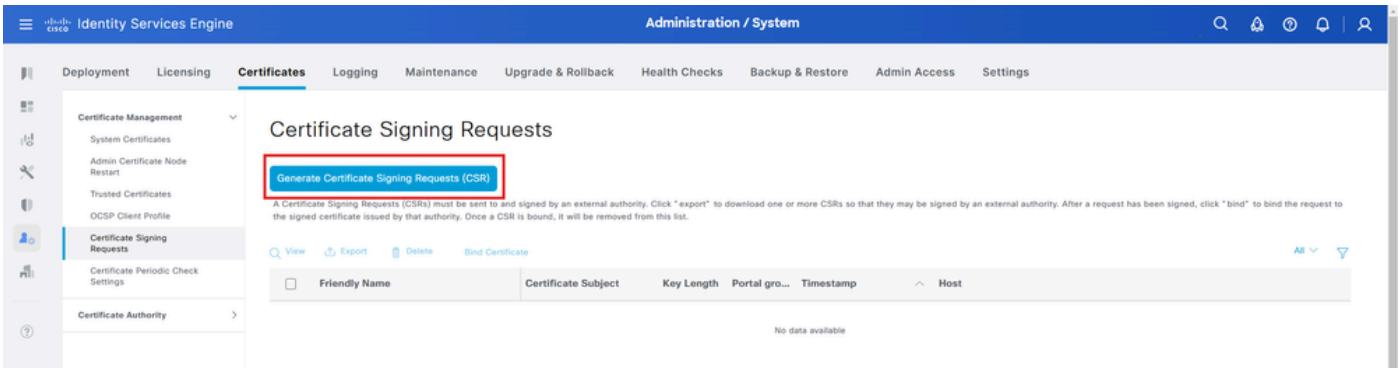
PARTE I - Generazione di un certificato ISE Server pxGrid

Generare un CSR per un certificato pxGrid di un server ISE:

1. Accedere all'interfaccia utente di Cisco Identity Services Engine (ISE).

2. Passare a Amministrazione > Sistema > Certificati > Gestione certificati > Richieste di firma del certificato.

3. Selezionare Genera richiesta di firma certificato (CSR).

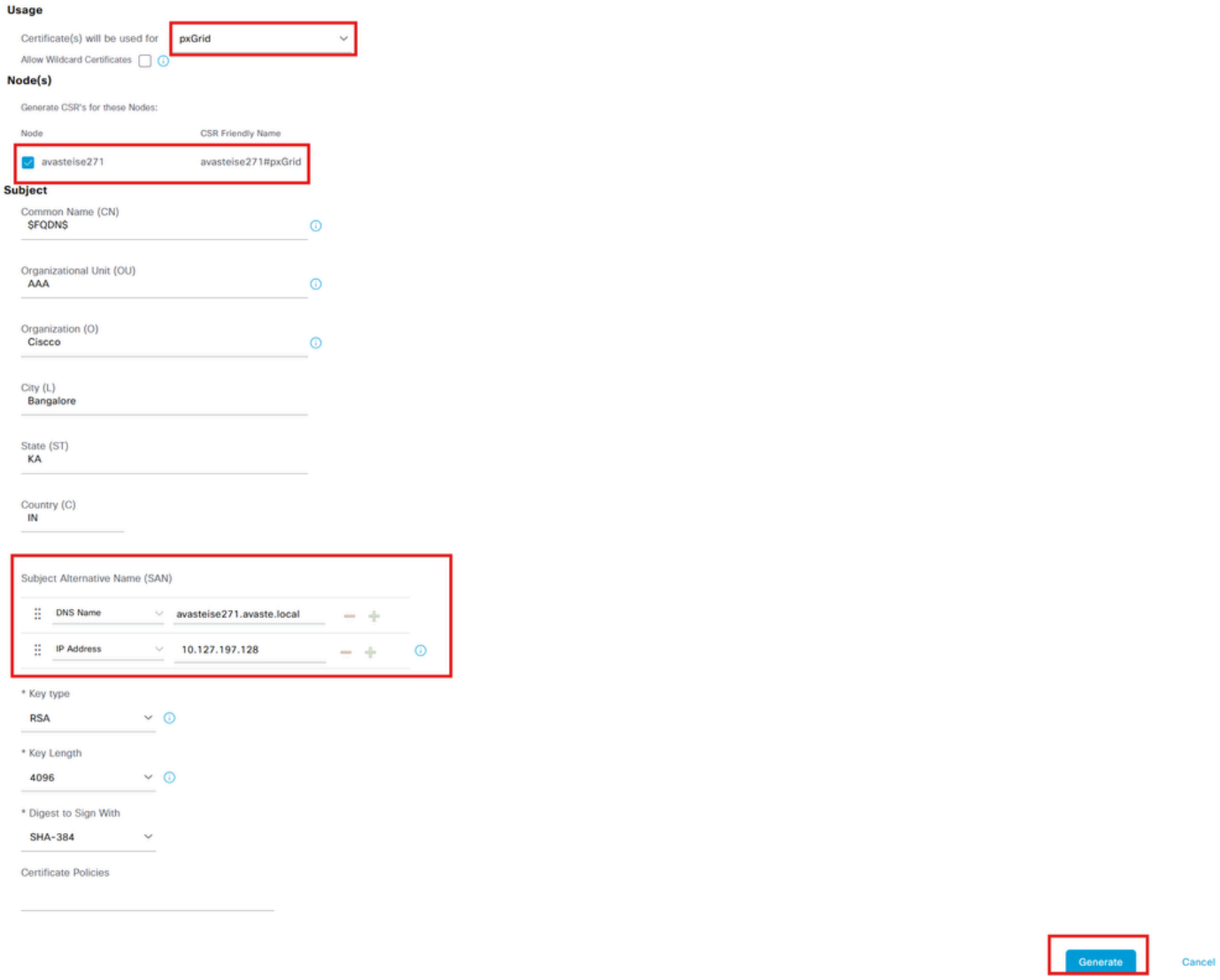


4. Selezionare pxGrid nel campo Certificato/i utilizzato/i per.

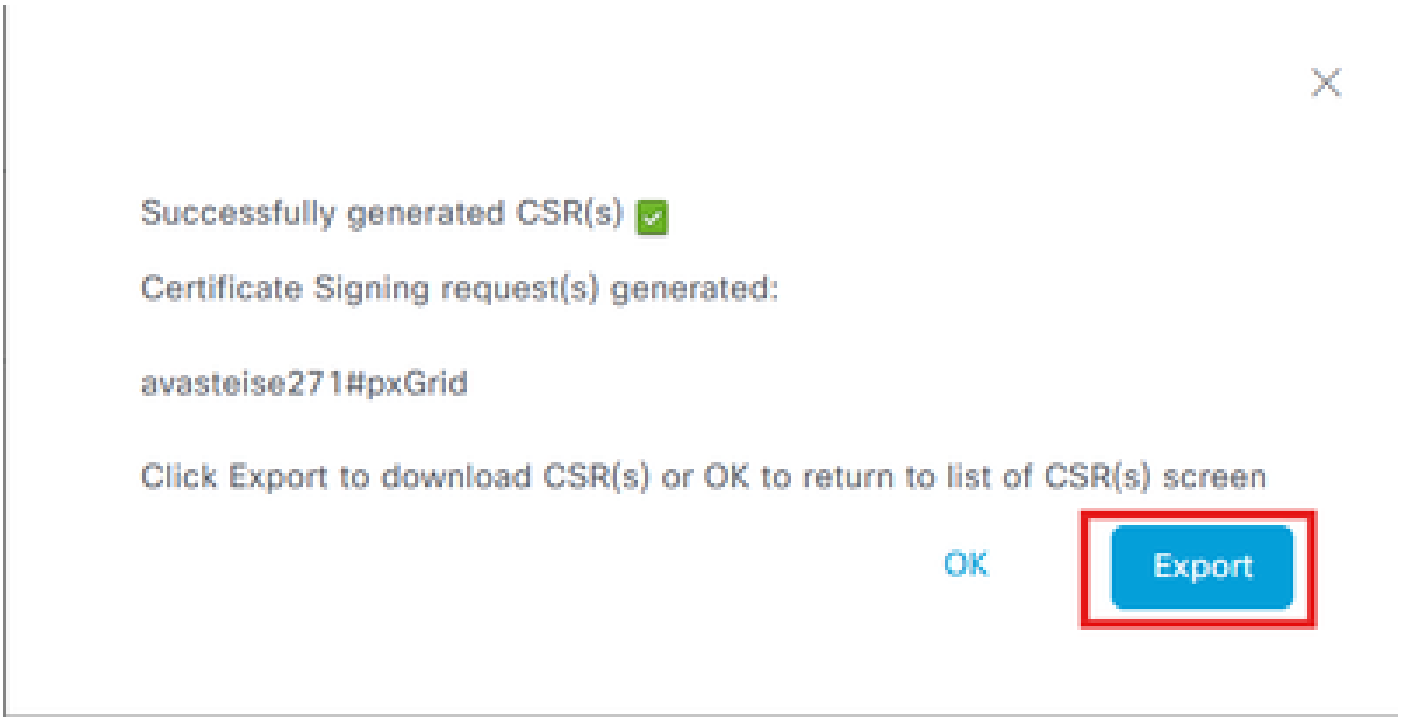
5. Selezionare il nodo ISE per il quale viene generato il certificato.

6. Compilare gli altri certificati come necessario.

7. Fare clic su Genera.



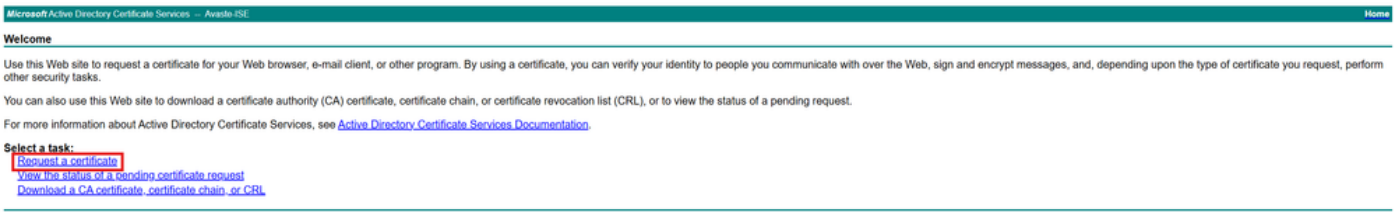
8. Fare clic su Esporta e Salva il file localmente.



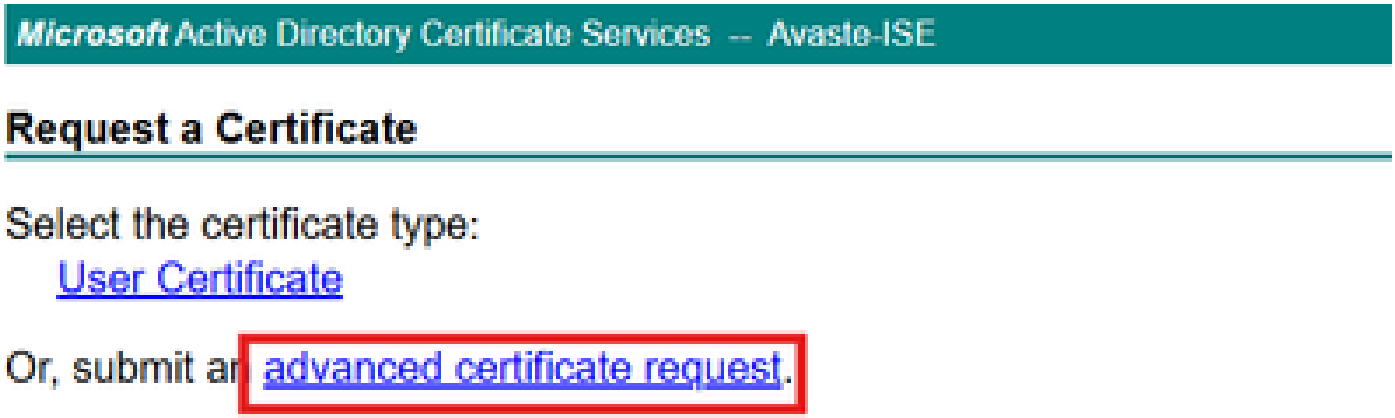
PARTE II - Creazione di un certificato PxGrid per un server ISE tramite una CA esterna

1. Passare a Servizio certificati Microsoft Active Directory, https://server/certsrv/, dove server è IP o DNS del server MS.

2. Fare clic su Richiedi certificato.

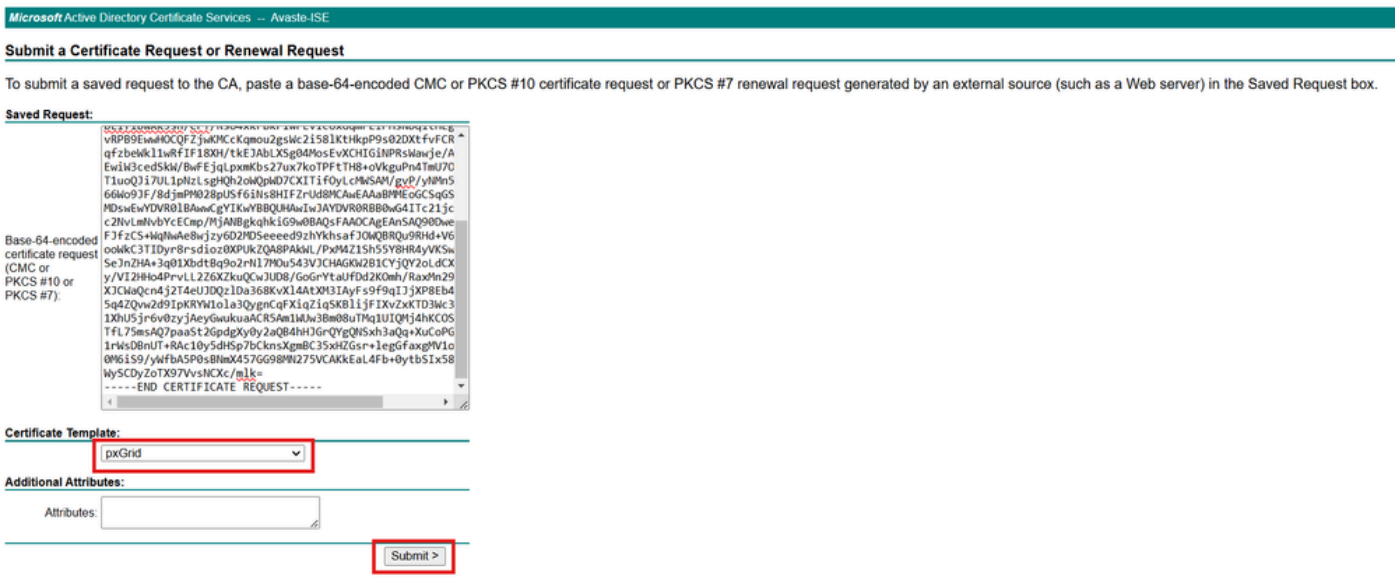


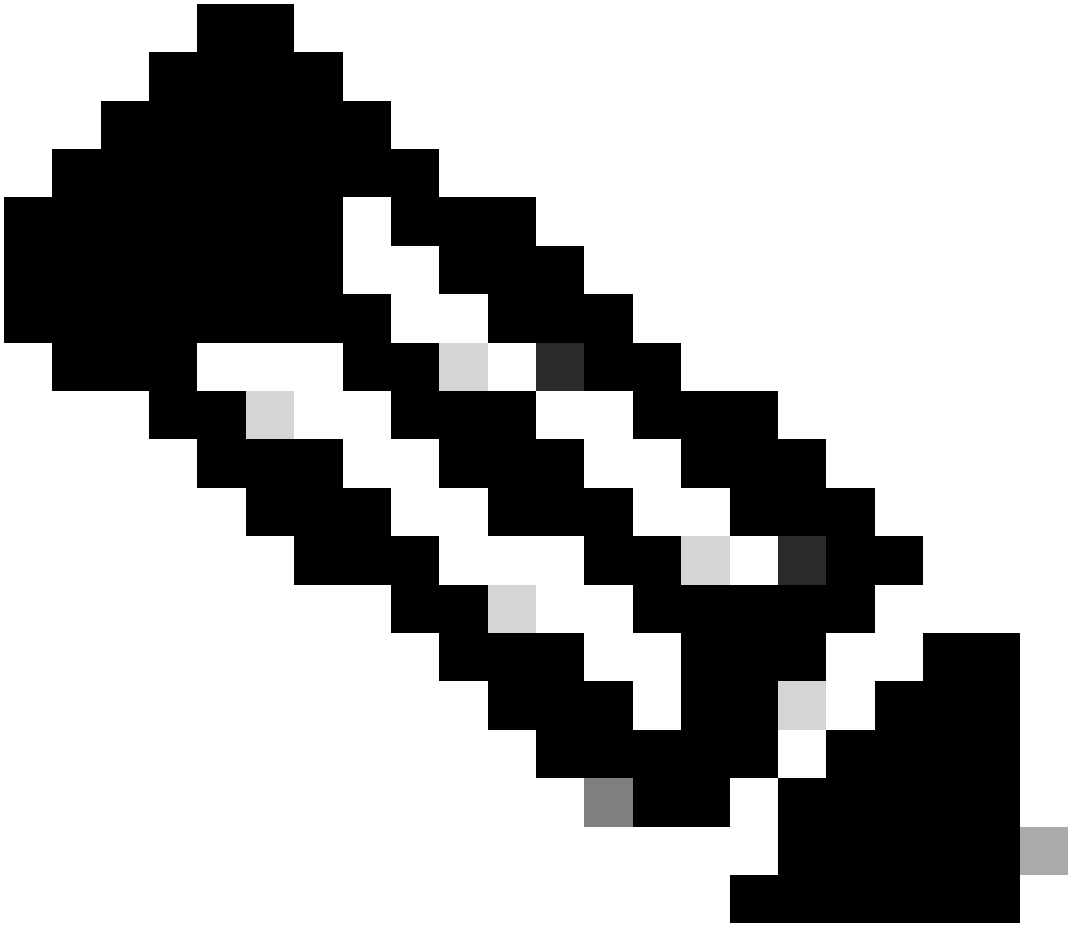
3. Scegliere di sottomettere una richiesta avanzata di certificati.



4. Copiare il contenuto del CSR generato nella sezione precedente nel campo Richiesta salvata.

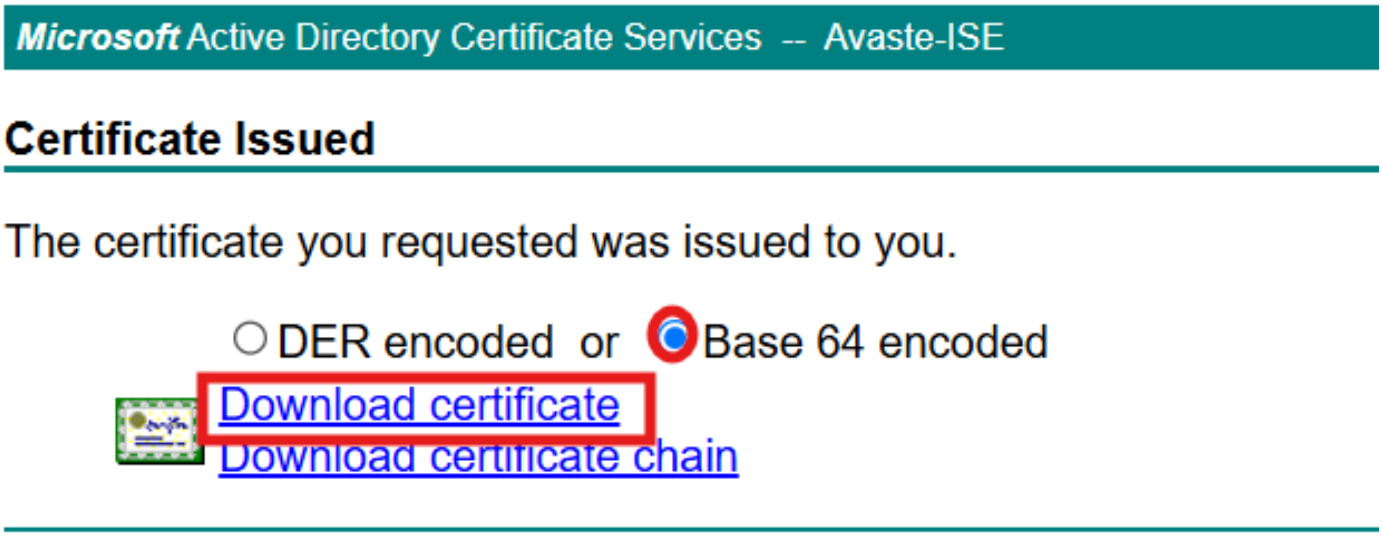
5. Selezionare pxGrid come modello di certificato, quindi fare clic su Sottometti.





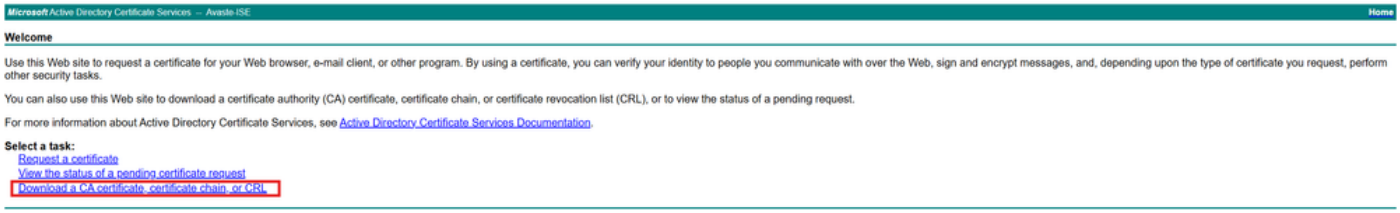
Nota: Il modello di certificato pxGrid utilizzato richiede sia l'autenticazione client che l'autenticazione server nel campo "Utilizzo chiavi avanzato".

6. Scaricare il certificato generato in formato Base-64 e salvarlo come ISE_pxGrid.cer.

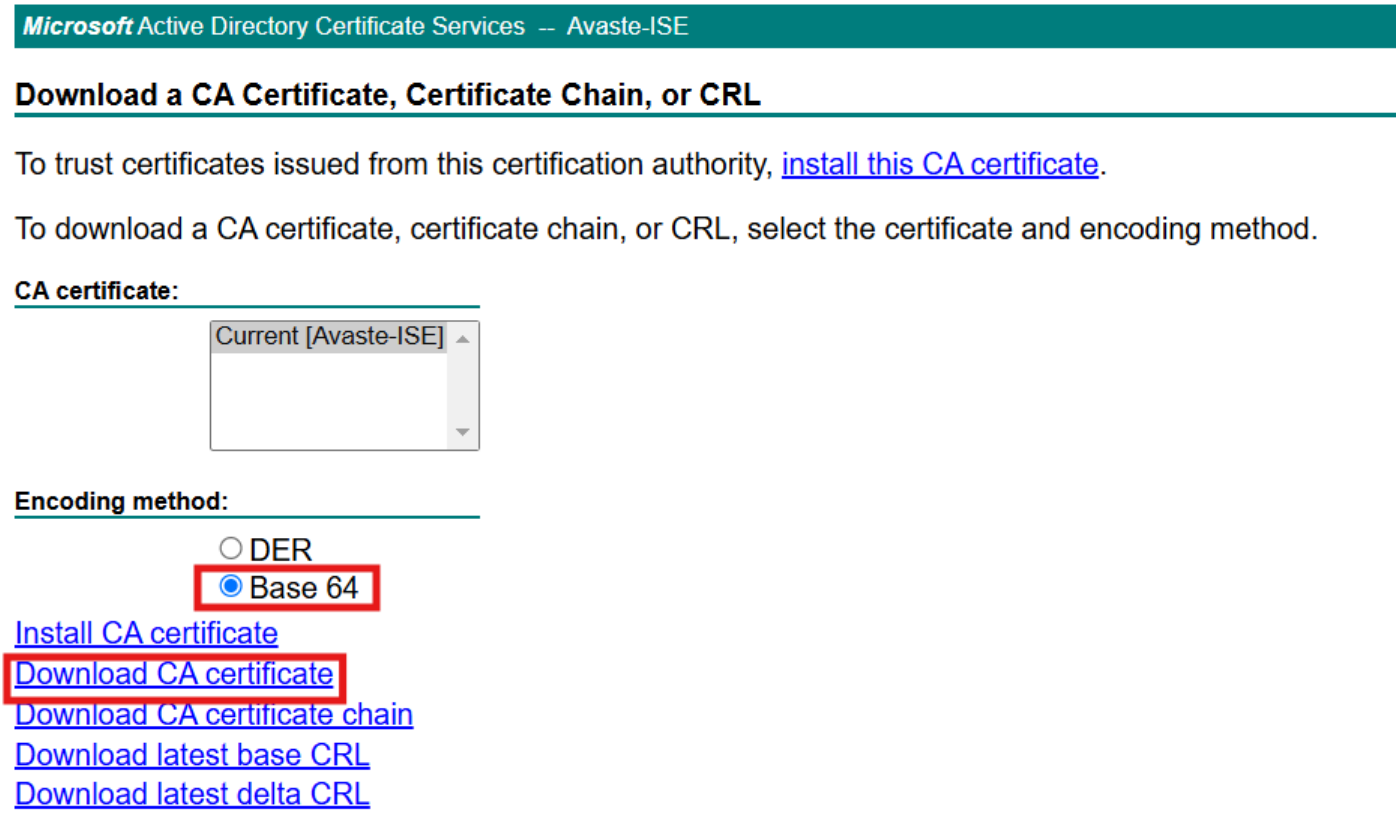


PARTE III - Importazione del certificato radice CA nell'ISE Trust Store

1. Passare alla home page del servizio certificati MS Active Directory e selezionare Scarica un certificato CA, una catena di certificati o un elenco di revoche di certificati.



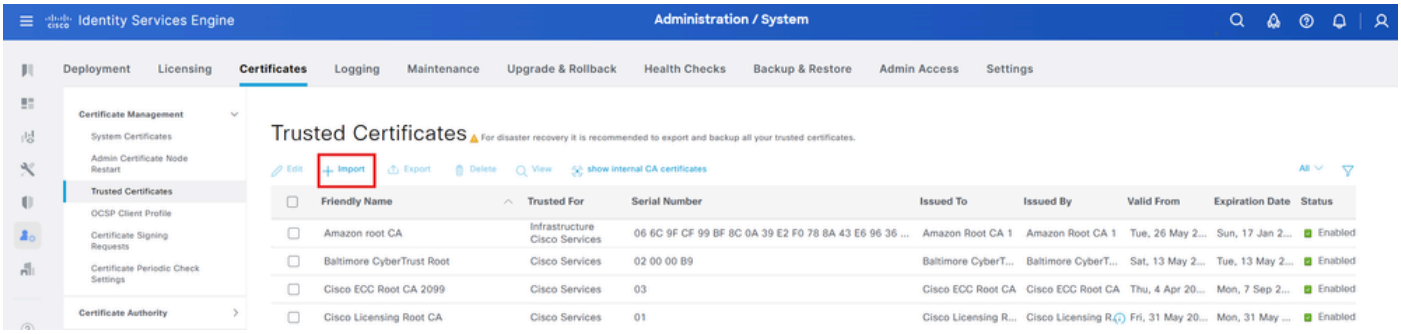
2. Selezionare il formato Base-64, quindi fare clic su Scarica certificato CA.



3. Salvare il certificato come CA_Root.cer.

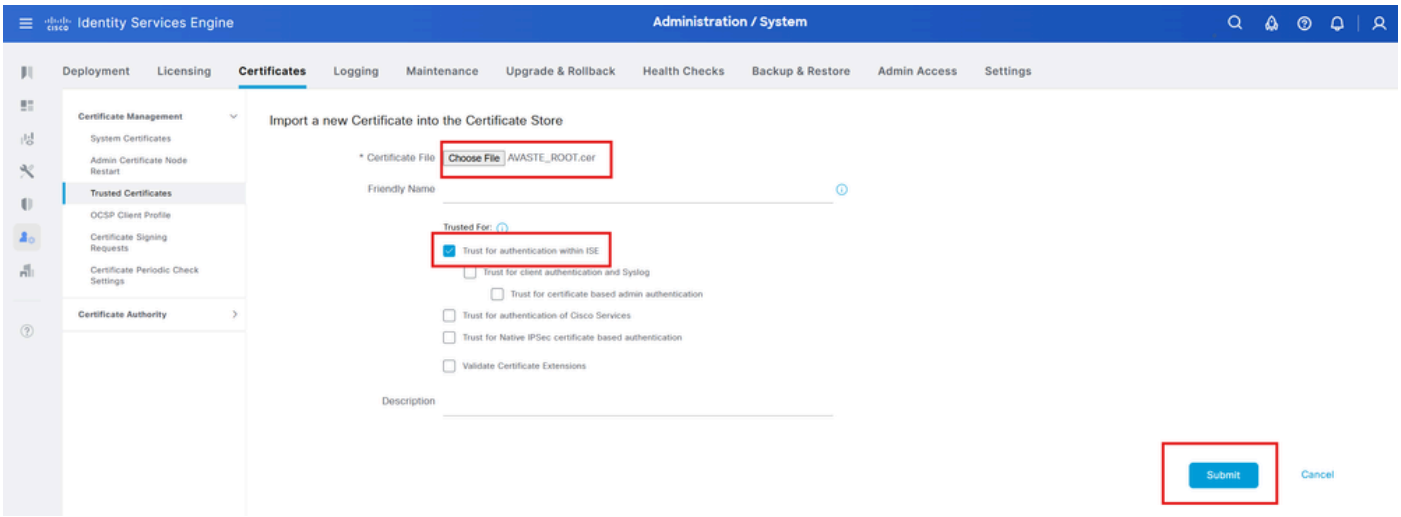
4. Accedere all'interfaccia utente di Cisco Identity Services Engine (ISE).

5. Selezionare Amministrazione > Sistema > Certificati > Gestione certificati > Certificati attendibili.



6. Selezionare Importa > File certificato e Importa il certificato radice.

7. Verificare che la casella di controllo Considera attendibile per l'autenticazione all'interno di ISE sia selezionata.



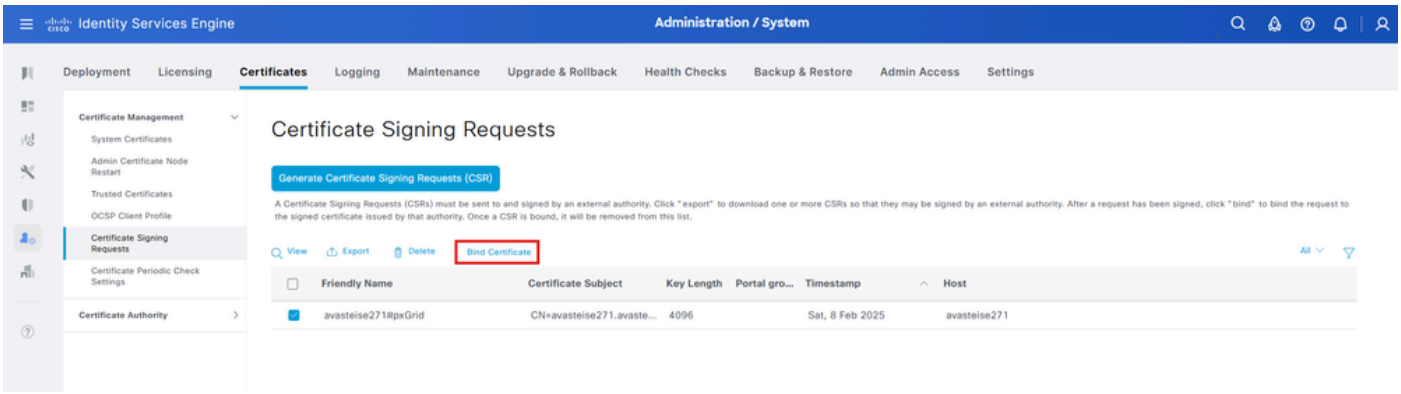
8. Fare clic su Sottometti.

PARTE IV - Associazione del certificato ISE alla richiesta di firma del certificato (CSR)

1. Accedere all'interfaccia utente di Cisco Identity Services Engine (ISE).

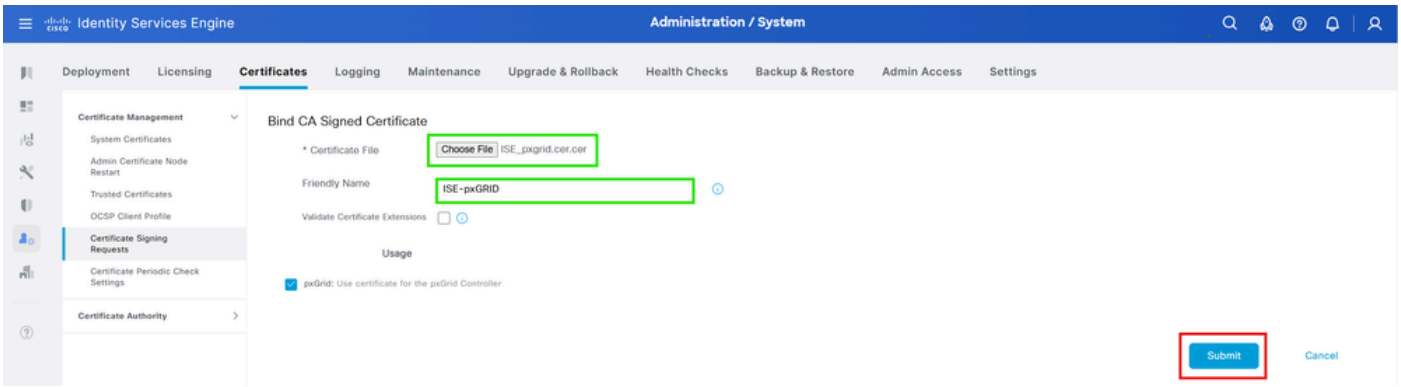
2. Selezionare Amministrazione > Sistema > Certificati > Gestione certificati > Richieste di firma del certificato.

3. Selezionare il CSR generato nella sezione precedente, quindi fare clic su Associa certificato.



4. Nel modulo Certificato firmato CA, scegliere il certificato ISE_pxGrid.cer generato in precedenza.

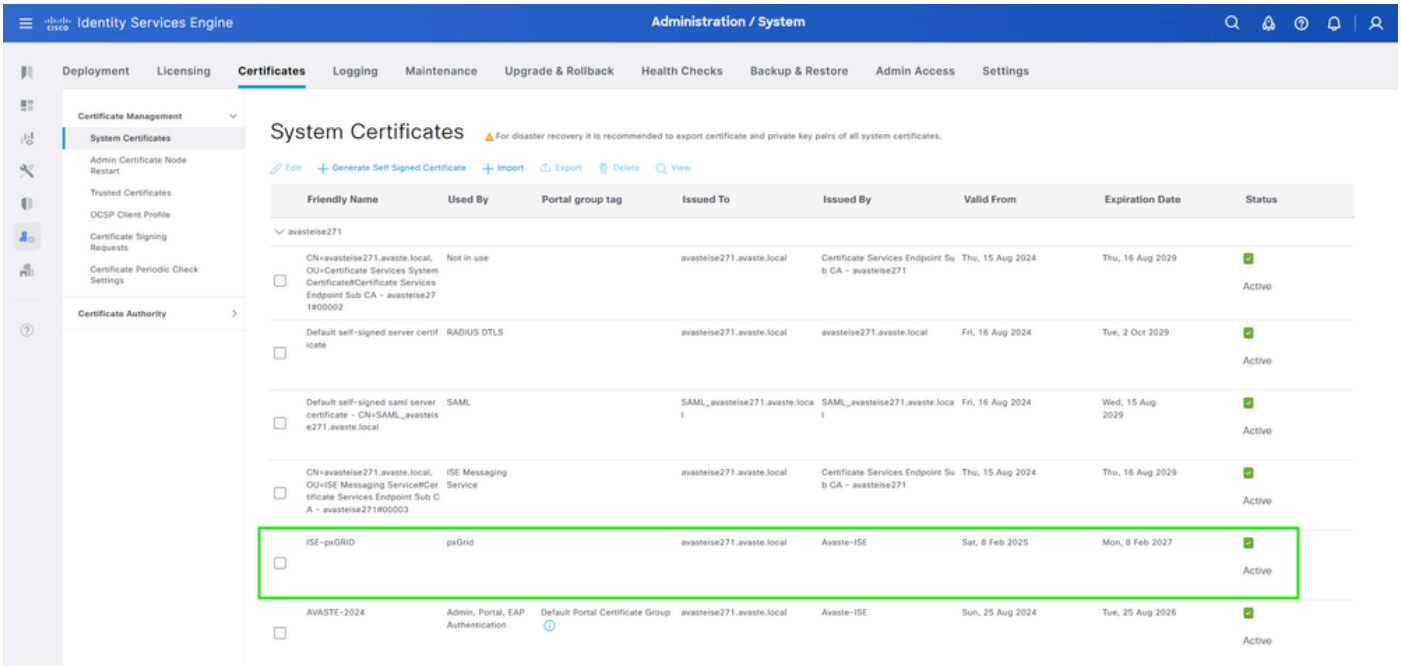
5. Assegnare al certificato un nome descrittivo, quindi fare clic su Invia.



7. Fare clic su Sì se il sistema chiede di sostituire il certificato.

8. Selezionare Amministrazione > Sistema > Certificati > Certificati di sistema.

9. È possibile visualizzare nell'elenco il certificato pxGrid creato firmato dalla CA esterna.

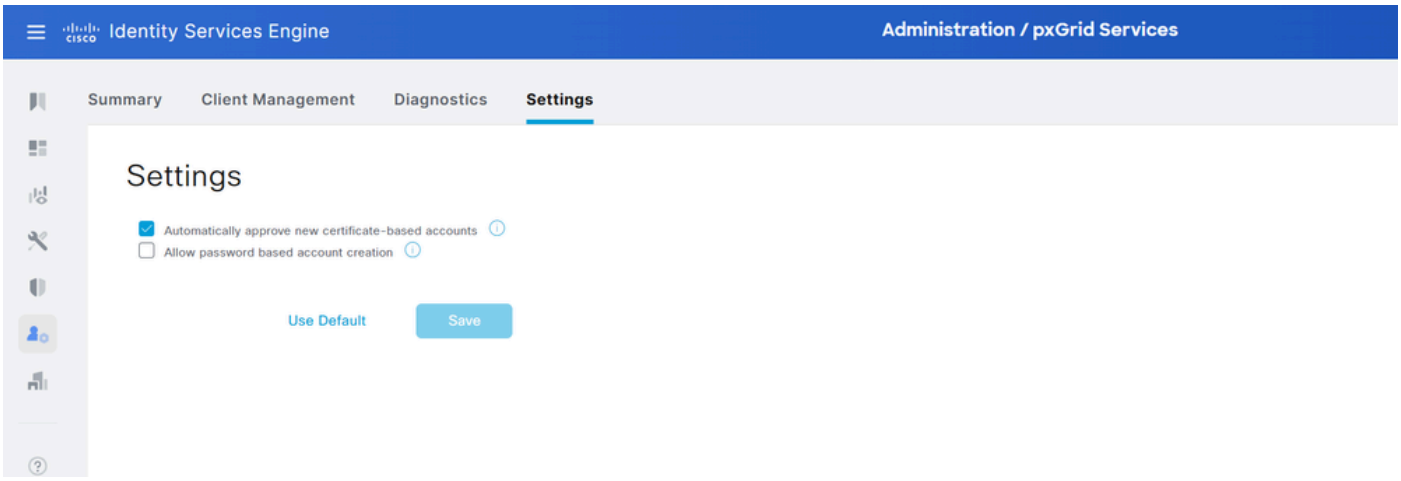


I certificati sono stati distribuiti. Procedere con l'integrazione.

Integrazione

Prima di procedere all'integrazione, assicurarsi che:

Per Cisco ISE in Amministrazione > pxGrid Services > Impostazioni e controllo Approva automaticamente nuovi account basati su certificato per le richieste del client da approvare e salvare automaticamente.

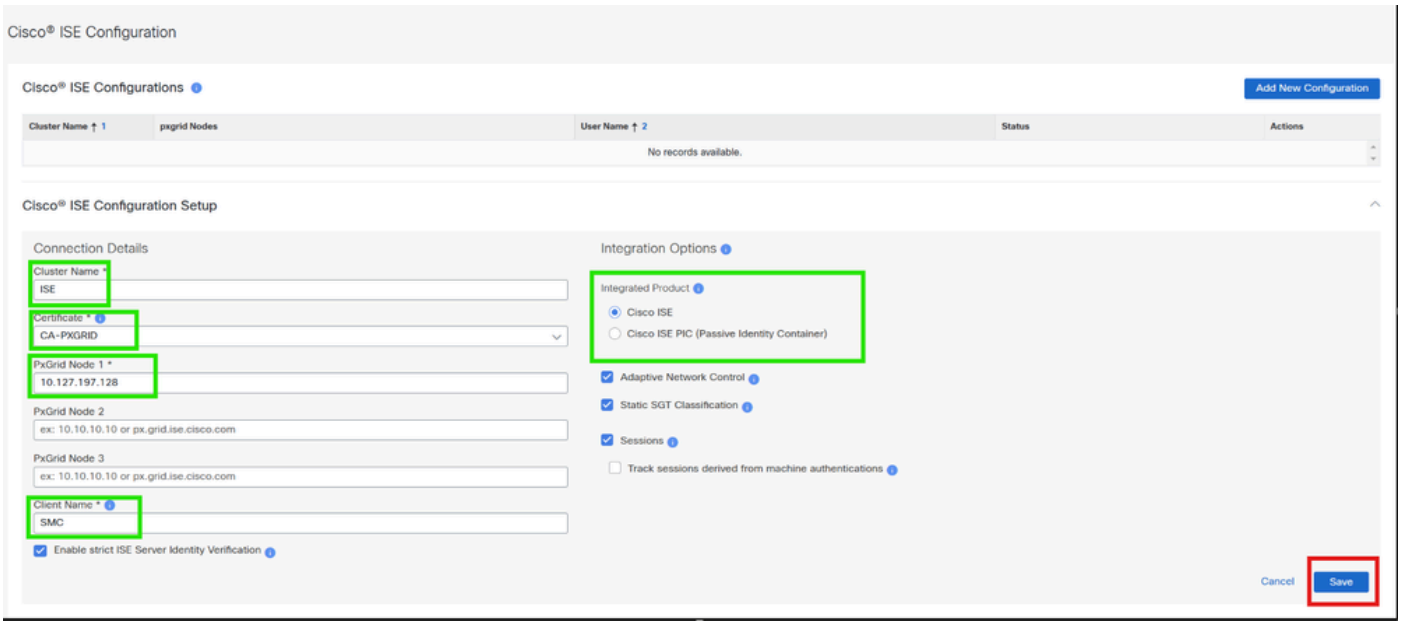


In Stealthwatch Management Console (SMC), per aprire la pagina di configurazione ISE:

1. Selezionare Configure > Integrations > Cisco ISE.

2. Nell'angolo superiore destro della pagina, fare clic su Aggiungi nuova configurazione.

3. Immettere il nome del cluster, selezionare il certificato & prodotto di integrazione, il nodo pxGrid IP e fare clic su Salva.



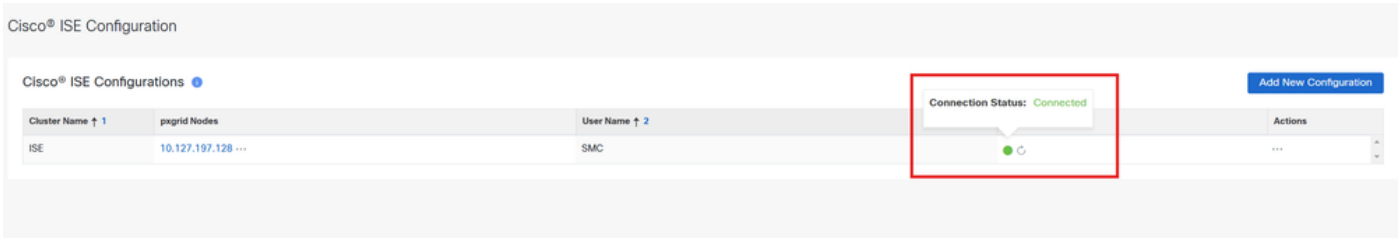
Verifica

Aggiornare la pagina Configurazione ISE in Stealthwatch Management Console (SMC).

1. Tornare alla pagina di configurazione ISE in Web App e aggiornare la pagina.

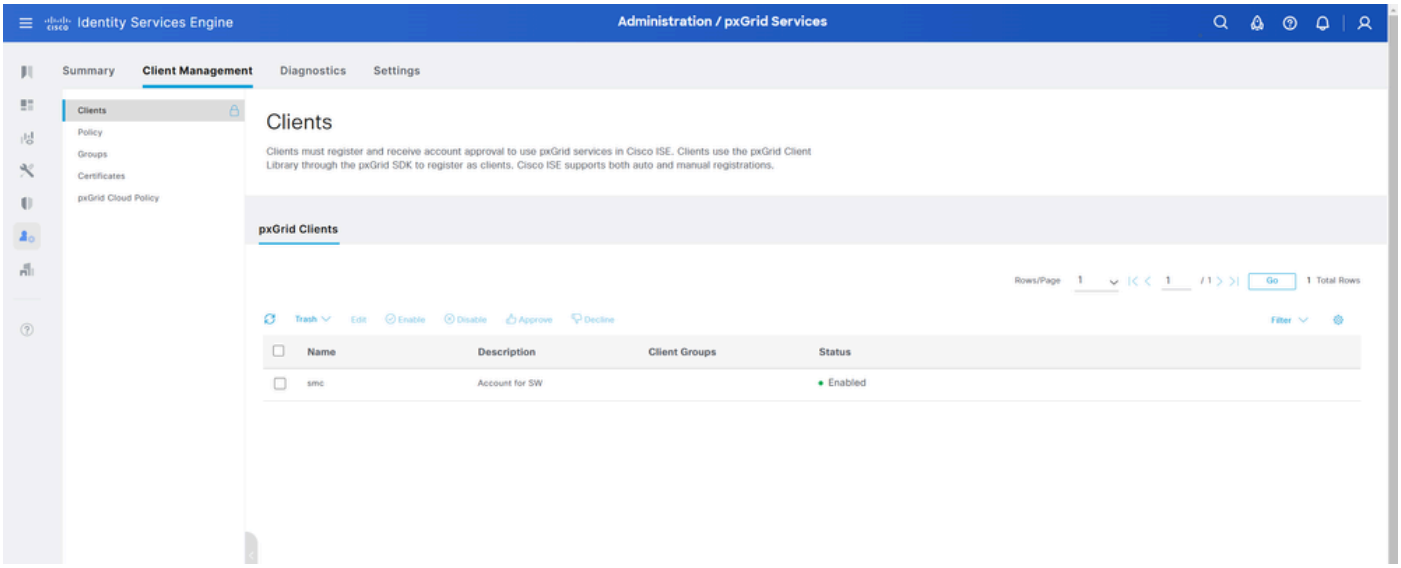
2. Confermare che l'indicatore di stato del nodo situato accanto al campo Indirizzo IP applicabile sia verde, per indicare

che è stata stabilita una connessione al cluster ISE o ISE-PIC.



In Cisco ISE, selezionare Administration > pxGrid Services > Client Management > Client.

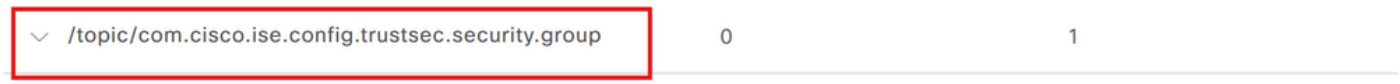
Questo genera SMC come client pxgrid con lo stato Abilitato.

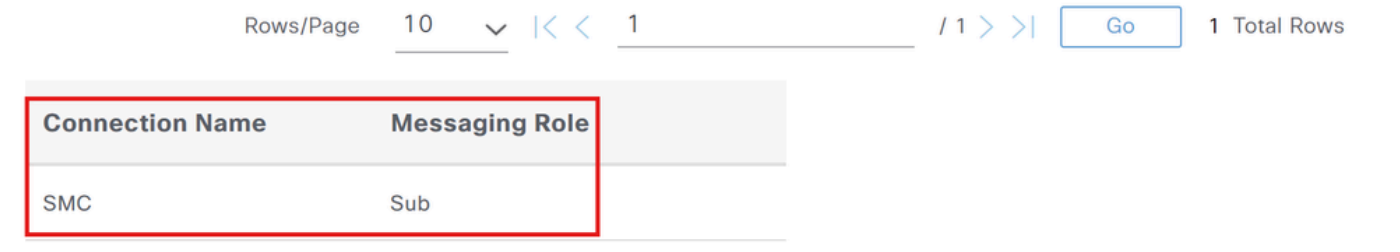


Per verificare l'abbonamento all'argomento su Cisco ISE, selezionare Administration > pxGrid Services > Diagnostics > Websocket > Topics

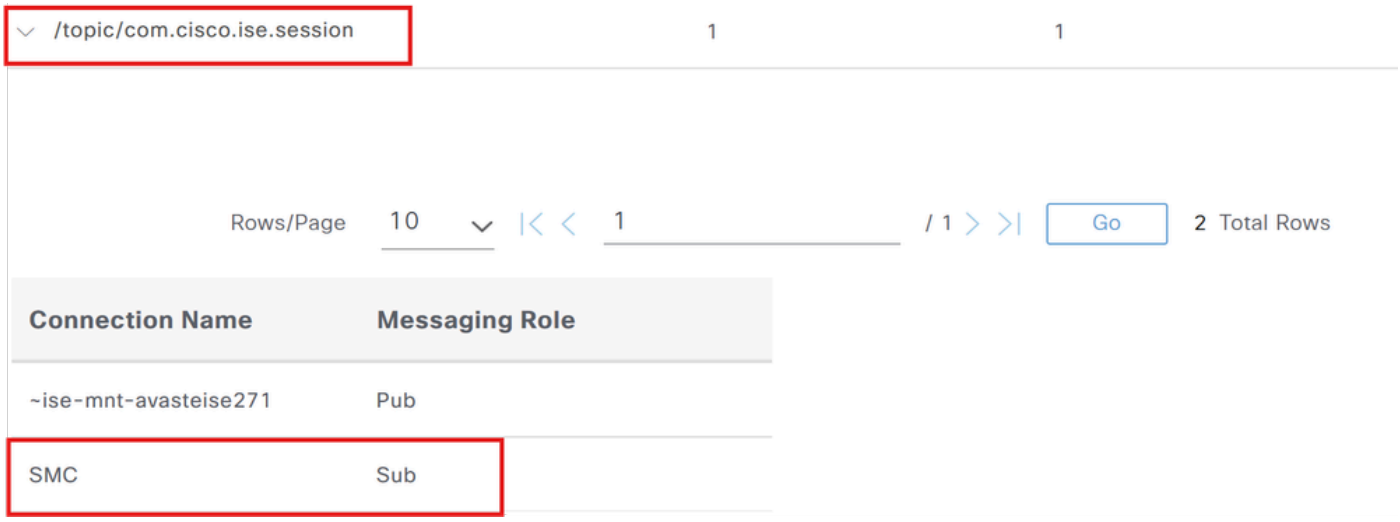
In questo modo viene creato un SMC sottoscritto a questi argomenti.

Argomento Trustsec SGT

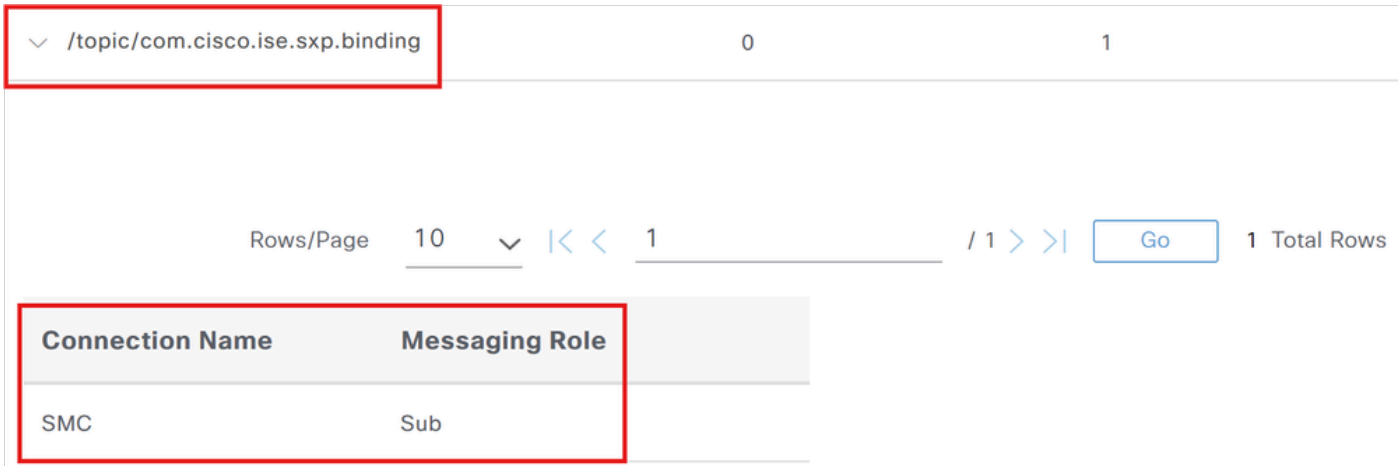




Argomento relativo alla directory di sessione ISE



Argomento sui binding ISE SXP



Cisco ISE Pxgrid-server.log nel livello TRACE.

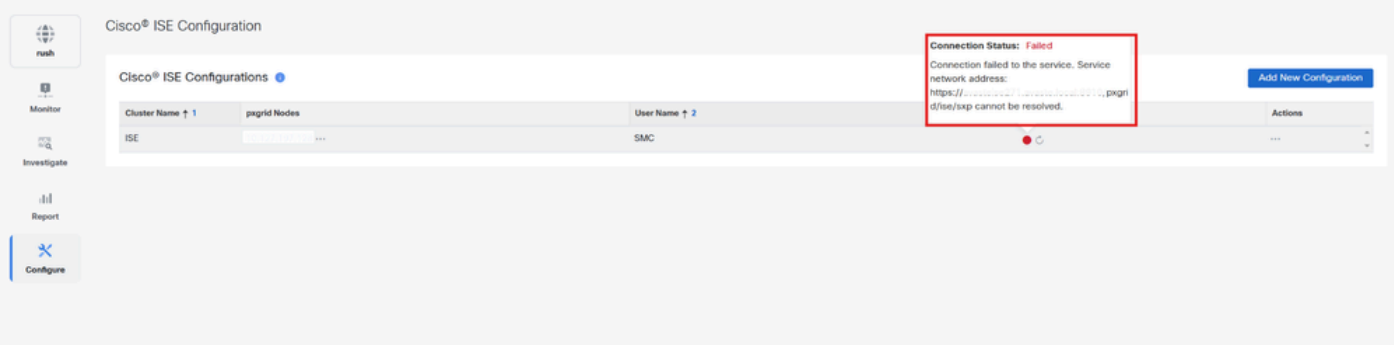
```
2025-02-08 18:07:11,086 TRACE  [pxgrid-http-pool15][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribu
2025-02-08 18:07:11,087 TRACE  [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint
2025-02-08 18:07:11,102 TRACE  [pxgrid-http-pool19][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint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



        ] 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.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 -::::::



          ] 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 -::::::
```

Risoluzione dei problemi

Problema di risoluzione DNS

Viene visualizzato il messaggio di errore "Connection Status; Connessione non riuscita al servizio. Indirizzo di rete del servizio: https:isehostnameme.domain.com:891pxgridiisessxpxp non può essere resolto":



Soluzione

Idealmente, questo problema deve essere risolto sul server DNS per le ricerche dirette e inverse per questo FQDN ISE. Tuttavia, è possibile aggiungere una soluzione temporanea per la risoluzione locale:

1. Accedere a Stealthwatch Management Console (SMC).

2. Dal menu principale, selezionare Configura > Globale > Gestione centrale.

3. Nella pagina Magazzino, fare clic sull'icona (Ellissi) per il Responsabile.

4. Scegliere Modifica configurazione accessorio.

5. Scheda Network Services e aggiungere una voce di risoluzione locale per questo FQDN ISE.

Errore CA sconosciuto o certificato attendibile mancante

Viene visualizzato il messaggio di errore "ISE sta presentando un certificato non considerato attendibile da questo manager":

Un riferimento al log simile può essere visto nel file SMCMsvcvisese-client.log. Percorso: 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.
```

Soluzione

1. Accedere a Stealthwatch Management Console (SMC).

2. Dal menu principale, selezionare Configura > Globale > Gestione centrale.

3. Nella pagina Magazzino, fare clic sull'icona (puntini di sospensione) per il Responsabile.

4. Scegliere Modifica configurazione accessorio.

5. Selezionare la scheda Generale.

6. Accedere alla sezione Trust Store e verificare che l'emittente del certificato Pxgridid di Cisco ISE sia parte del Trust Store.

Difetti noti

ID bug	Descrizione
ID bug Cisco 1819	ISE sta selezionando una crittografia non supportata per il pacchetto Hello del server ITLS
ID bug Cisco 01634	Impossibile mettere in quarantena i dispositivi utilizzando la condizione EPS

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).