

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

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Sezione A: Configurazione certificato Secure Network Analytics \(Stealthwatch\)](#)

[Parte I - Generazione di un CSR per il certificato client PxGrid di Secure Network Analytics](#)

[Parte II - Creazione di un certificato client pxGrid Secure Network Analytics tramite una CA esterna](#)

[PARTE III - Aggiunta del certificato client pxGrid di Secure Network Analytics a Gestione](#)

[PARTE IV - Importazione del certificato radice CA nell'archivio di attendibilità del manager](#)

[Sezione B: Configurazione certificato Cisco Identity Services Engine 3.3](#)

[PARTE I - Generazione di un certificato PxGrid per un server ISE](#)

[PARTE II - Creazione di un certificato PxGrid per un server ISE tramite una CA esterna](#)

[PARTE III - Importazione del certificato radice CA nell'ISE Trust Store](#)

[PARTE IV - Associazione del certificato ISE alla richiesta di firma del certificato \(CSR\)](#)

[Integrazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Problema di risoluzione DNS](#)

[Soluzione](#)

[Errore CA sconosciuto o certificato attendibile mancante](#)

[Soluzione](#)

[Difetti noti](#)

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.



Risk



Monitor



Investigate



Report



Configure

Configure

X

Detection

Host Group Management

Alarm Severity

Policy Management

Response Management

Network Scanners

Analytics

Alerts

Global

Central Management

User Management

Manager

UDP Director

External Lookup

System

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.

Microsoft Active Directory Certificate Services -- Avaste-ISE

Certificate Issued

The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

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.

Welcome

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

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

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

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

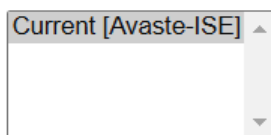
2. Selezionare il formato Base 64, quindi fare clic su Scarica certificato CA.

3. Salvare il certificato come CA_Root.cer.

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

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

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

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

4. 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.

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

Inventory / Appliance Configuration

Appliance Configuration - Manager

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

Cancel Apply Settings

Configuration Menu

Appliance Network Services **General**

☐ Enable FIPS Encryption Libraries

☐ Enable Common Criteria Encryption Libraries

SMTP Configuration

SMTP Server

Port

From Email

User Name

Password

Encryption Type

☒ SMTPS ☐ STARTTLS ☐ Un-Encrypted

External Services

If you enable a service, make sure you enable it on the other required appliances. Refer to the tooltip for requirements.

☒ Enable Cisco Security Cloud Control

☒ Enable Customer Success Metrics

☒ Enable Threat Feed

Feed Confidence Level

7

DoDIN Notifications

☐ Enable

To Email *

Backup Configuration Encryption

Make sure you save your password. If you lose your password, you can change it. However, you will not be able to restore a backup configuration file without the password.

☐ Enable Encryption

Backup Configuration Password

Confirm Password

Trust Store

Add New

Friendly Name	Issued To	Issued By	Valid From	Valid To	Serial Number	Key Length	Actions
yy1nde2owmzmdus5ndc2m2r2mu...ert	Secure Network Analytics	Secure Network Analytics	2024-06-20 20:17:15	2029-06-21 20:17:15	403cd116b1af4d3b71e9060afdbba...	4096	Delete
fc751new.www.cisco.com	Secure Network Analytics	Secure Network Analytics	2024-06-23 12:14:09	2029-06-24 12:14:09	14e60739401a8e204c7f03b12279...	4096	Delete
AWS	Amazon	Amazon	2015-05-26 05:30:00	2038-01-17 05:30:00	66c9cf998f8c0a39e2f0788a43e69...	2048	Delete

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

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.

Add Certification Authority Certificate

Friendly Name *

AVASTEROOTCA

Certificate File *

AVASTE_ROOT.cer

Select file...

Cancel Add Certificate

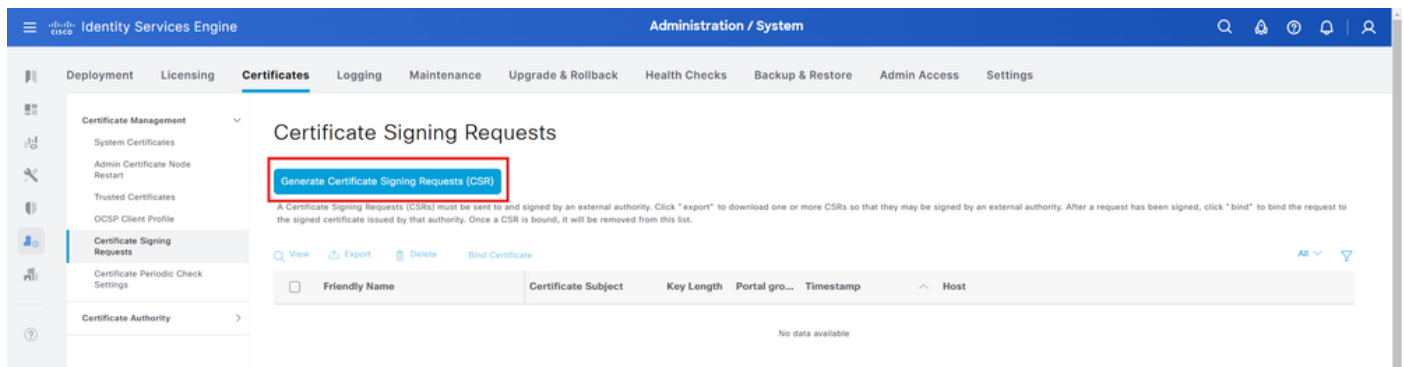
13. Fare clic su Applica impostazioni per salvare le modifiche.

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.

Usage

Certificate(s) will be used forpxGrid

Allow Wildcard Certificates

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☒ avasteise271	avasteise271#pxGrid

Subject

Common Name (CN)
SFQDNS

Organizational Unit (OU)
AAA

Organization (O)
Cisco

City (L)
Bangalore

State (ST)
KA

Country (C)
IN

Subject Alternative Name (SAN)

DNS Name

avasteise271.avaste.local

IP Address

10.127.197.128

* Key type

RSA

* Key Length

4096

* Digest to Sign With

SHA-384

Certificate Policies

Generate

Cancel

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

×

Successfully generated CSR(s)

Certificate Signing request(s) generated:

avasteise271#pxGrid

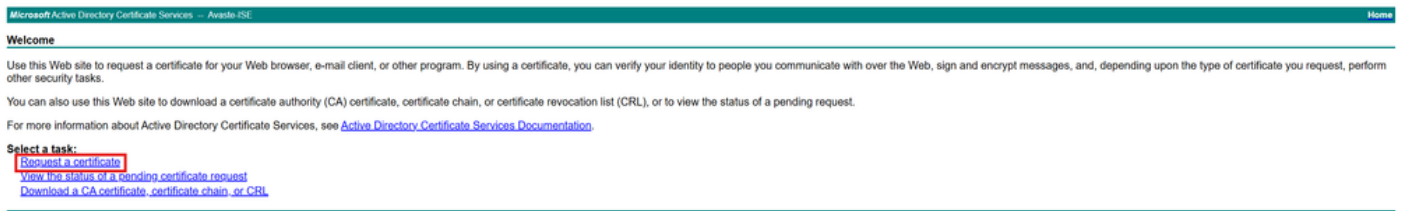
Click Export to download CSR(s) or OK to return to list of CSR(s) screen

OK

Export

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.

Microsoft Active Directory Certificate Services -- Avasto-ISE

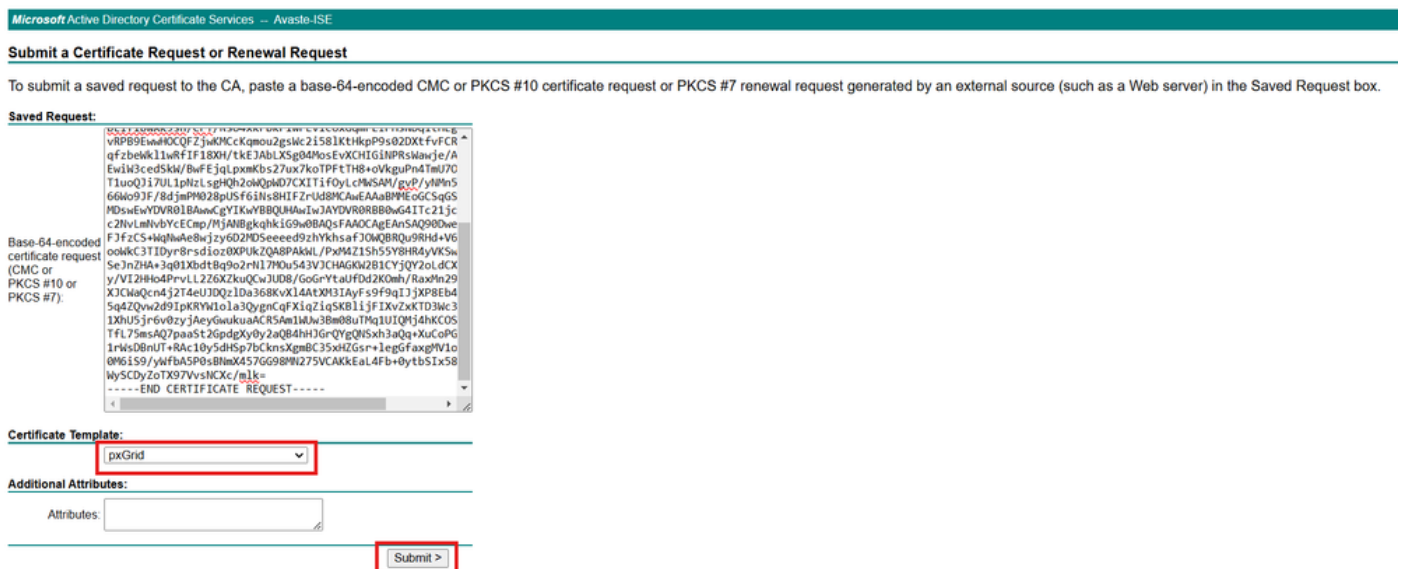
Request a Certificate

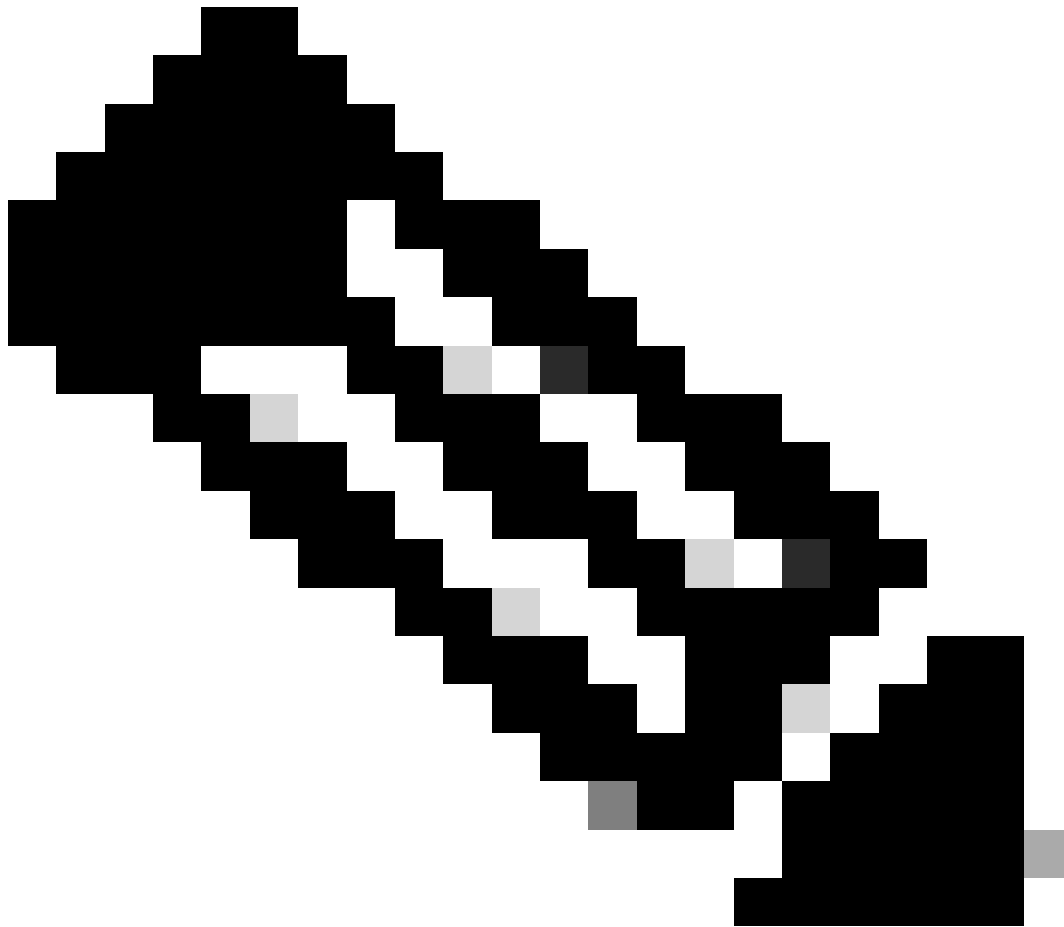
Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#).

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.

Certificate Issued

The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded

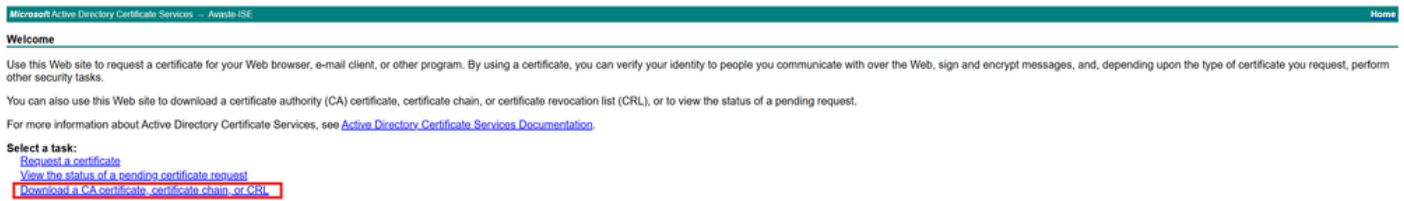


[Download certificate](#)

[Download certificate chain](#)

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.

Download a CA Certificate, Certificate Chain, or CRL

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

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

CA certificate:

Current [Avaste-ISE] ▲
▼

Encoding method:

☐ DER

☒ Base 64

[Install CA certificate](#)

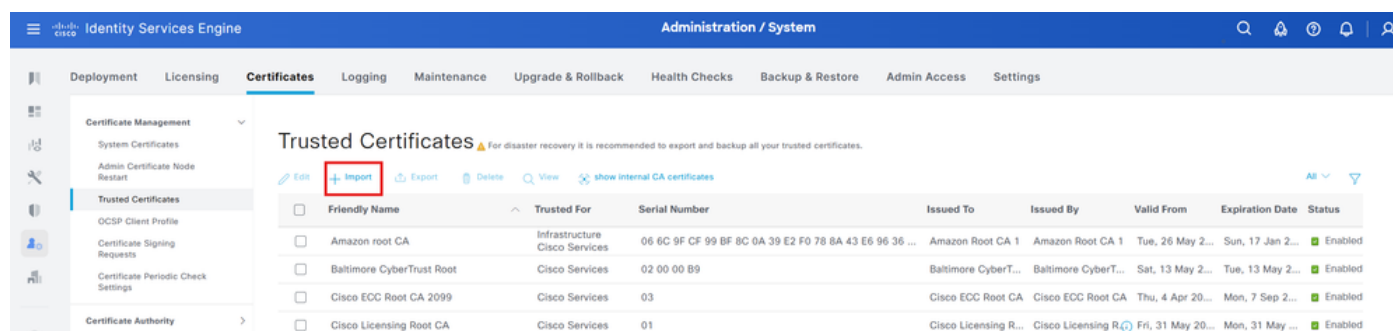
[Download CA certificate](#)

[Download CA certificate chain](#)

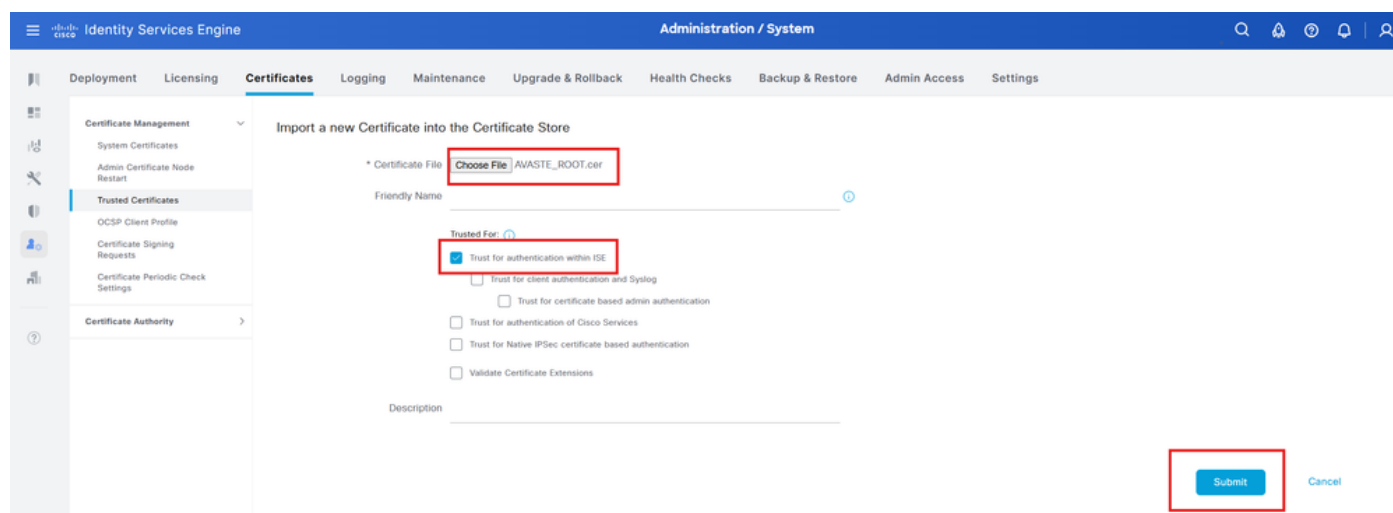
[Download latest base CRL](#)

[Download latest delta CRL](#)

3. 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.

Identity Services Engine Administration / System

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

Certificate Management

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

Certificate Signing Requests

Generate Certificate Signing Requests (CSR)

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

View Export Delete **Bind Certificate**

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

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.

Identity Services Engine Administration / System

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

Certificate Management

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

Bind CA Signed Certificate

* Certificate File **Choose File** ISE_pxgrid.cer.cer

Friendly Name **ISE-pxGRID**

Validate Certificate Extensions ☐

Usage

☒ pxGrid: Use certificate for the pxGrid Controller

Submit Cancel

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.

Identity Services Engine Administration / System

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

Certificate Management

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

System Certificates

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

Edit + Generate Self Signed Certificate + Import Export Delete View

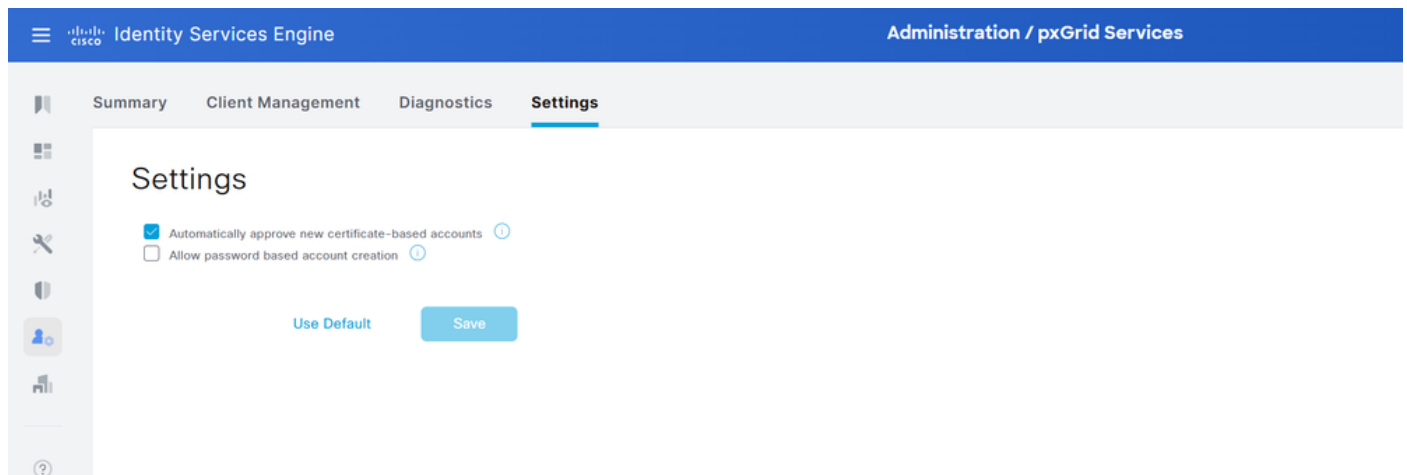
☐	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
☒	avasteise271							
☐	CN=avasteise271.avaste.local, OU=Certificate Services System, Certificate Services Endpoint Sub CA - avasteise271@00002	Not in use		avasteise271.avaste.local	Certificate Services Endpoint Sub CA - avasteise271	Thu, 15 Aug 2024	Thu, 16 Aug 2029	Active
☐	Default self-signed server certificate	RADIUS DTLS		avasteise271.avaste.local	avasteise271.avaste.local	Fri, 16 Aug 2024	Tue, 2 Oct 2029	Active
☐	Default self-signed saml server certificate - CN=SAML_avasteise271.avaste.local	SAML		SAML_avasteise271.avaste.local	SAML_avasteise271.avaste.local	Fri, 16 Aug 2024	Wed, 15 Aug 2029	Active
☐	CN=avasteise271.avaste.local, OU=ISE Messaging Service Certificate Services Endpoint Sub CA - avasteise271@00003	ISE Messaging Service		avasteise271.avaste.local	Certificate Services Endpoint Sub CA - avasteise271	Thu, 15 Aug 2024	Thu, 16 Aug 2029	Active
☐	ISE-pxGRID	pxGrid		avasteise271.avaste.local	Avaste-ISE	Sat, 8 Feb 2025	Mon, 8 Feb 2027	Active
☐	AVASTE-2024	Admin, Portal, EAP Authentication	Default Portal Certificate Group	avasteise271.avaste.local	Avaste-ISE	Sun, 25 Aug 2024	Tue, 25 Aug 2026	Active

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

Integrazione

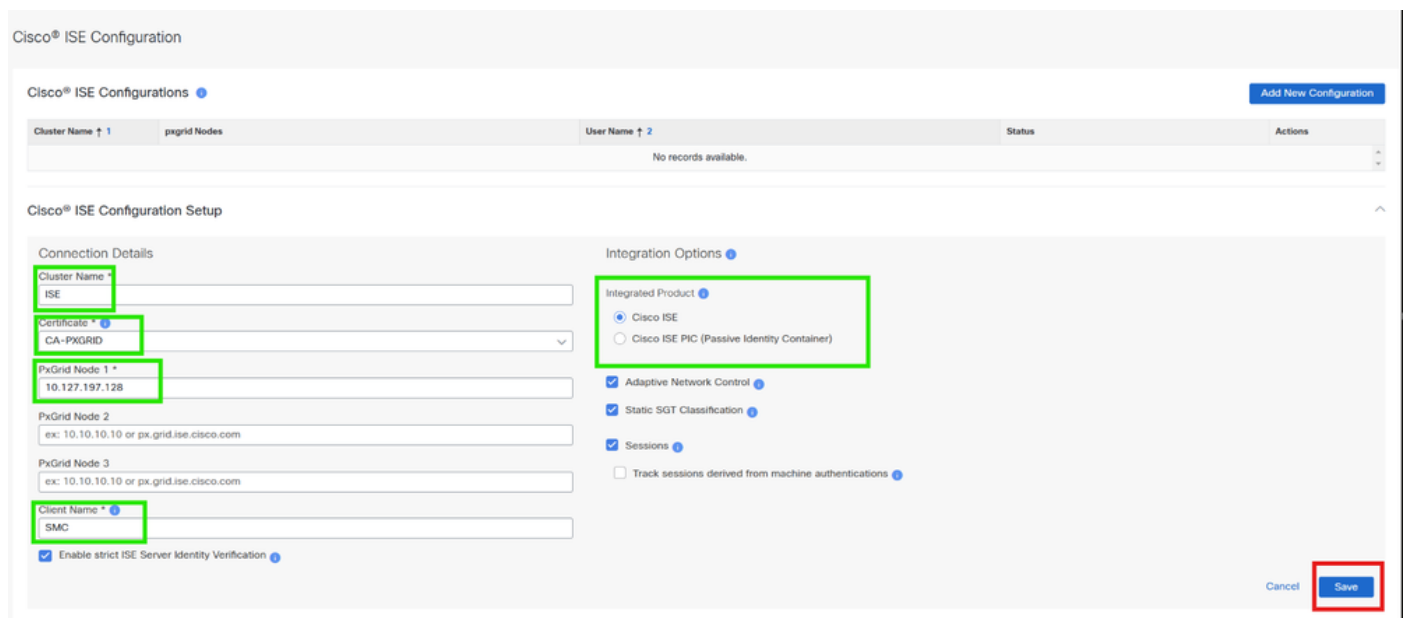
Prima di procedere all'integrazione, assicurarsi che:

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.

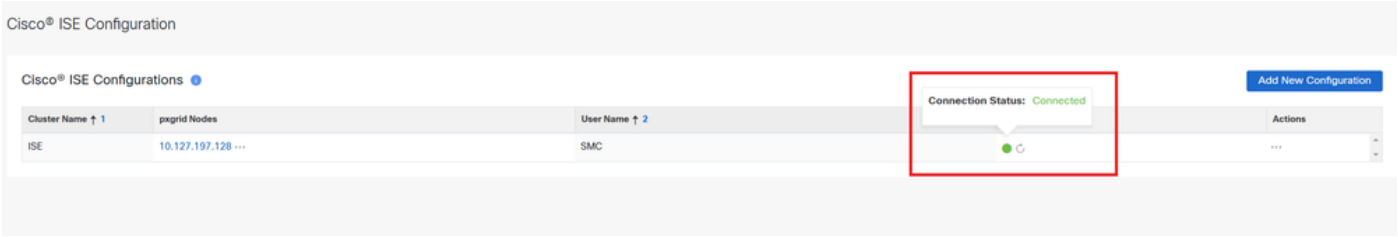


Verifica

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

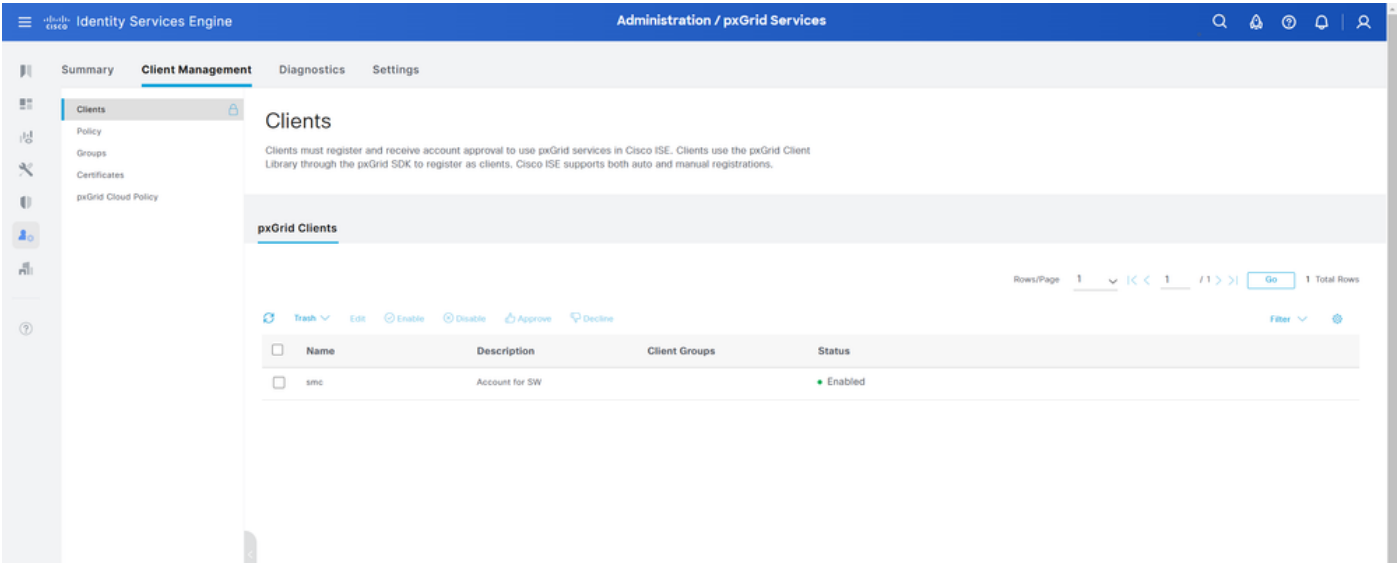
1. Tornare alla pagina di configurazione ISE in Web App e aggiornare la pagina.
2. Confermare che l'indicatore di stato del nodo situato accanto al campo Indirizzo IP applicabile sia verde, per indicare

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



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

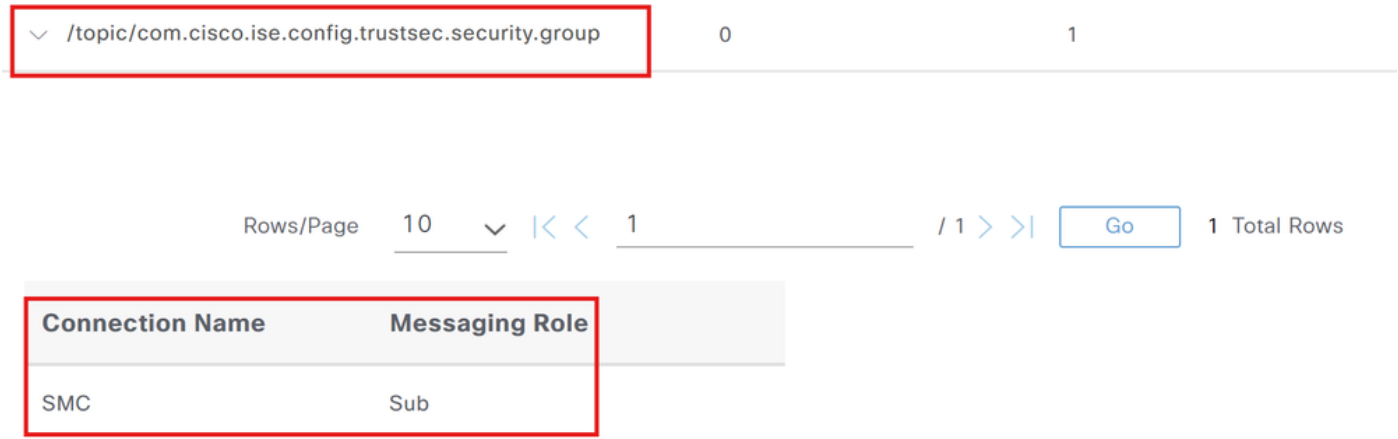
Questo genera SMC come client pxgrid con lo stato Abilitato.



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

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

Rows/Page

10

▼

<<

<

1

/ 1 >

>>

Go

2 Total Rows

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

Argomento sui binding ISE SXP

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

Rows/Page

10

▼

<<

<

1

/ 1 >

>>

Go

1 Total Rows

Connection Name	Messaging Role
SMC	Sub

Cisco ISE Pxgrid-server.log 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 -:::

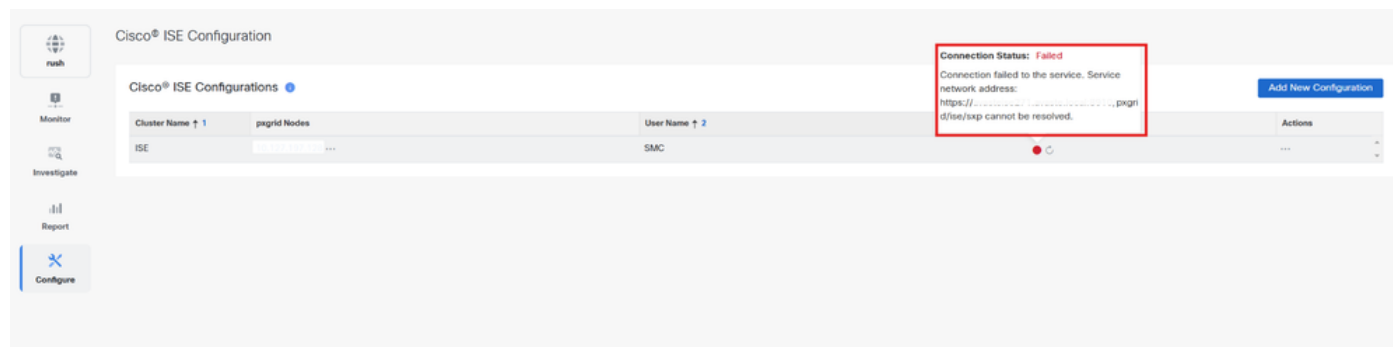
] from=[id=7,client=~ise-admin-avasteise271,server=wss://avasteise271.avaste.local:8910/pxgr
2025-02-08 18:07:11,324 TRACE [sub-sender-0][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionSender -:::

```

Risoluzione dei problemi

Problema di risoluzione DNS

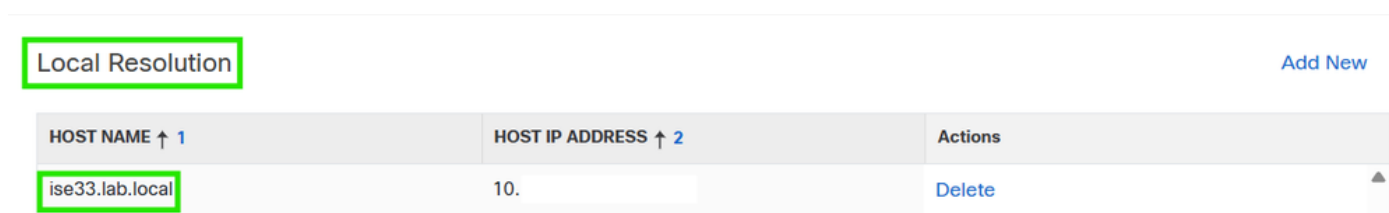
Viene visualizzato il messaggio di errore "Connection Status; Connessione non riuscita al servizio. Indirizzo di rete del servizio: <https://sehostnameme.domain.com:891pxgridiisessxpxp> non può essere risolto":



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:

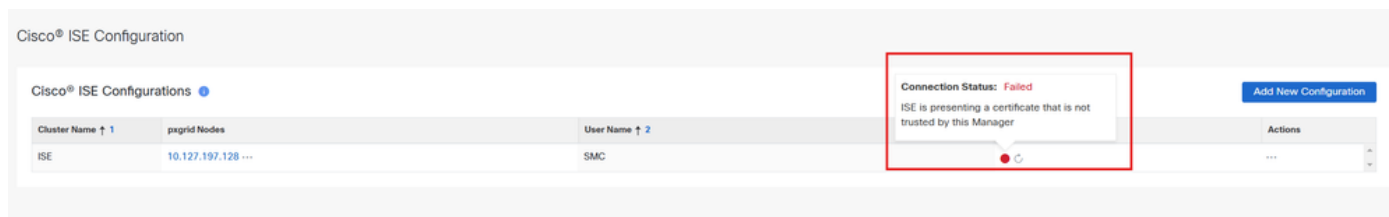
1. Accedere a Stealthwatch Management Console (SMC).
2. Dal menu principale, selezionare Configura > Globale > Gestione centrale.
3. Nella pagina Magazzino, fare clic sull'icona (Ellissi) per il Responsabile.
4. Scegliere Modifica configurazione accessorio.
5. Scheda Network Services e aggiungere una voce di risoluzione locale per questo FQDN ISE.



Local Resolution			Add New
HOST NAME ↑ 1	HOST IP ADDRESS ↑ 2	Actions	
ise33.lab.local	10.	Delete	

Errore CA sconosciuto o certificato attendibile mancante

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



Cisco® ISE Configurations				Add New Configuration
Cluster Name ↑ 1	pxgrid Nodes	User Name ↑ 2	Actions	
ISE	10.127.197.128 ...	SMC	...	

Un riferimento al log simile può essere visto nel file SMCMsvcvise-client.log. Percorso: catlancopepe/var/logs/containsvcvise-client.log

```
snasmc1 docker/svc-ise-client[1453]: java.util.concurrent.ExecutionException: javax.net.ssl.SSLException
snasmc1 docker/svc-ise-client[1453]: at java.base/java.util.concurrent.CompletableFuture.reportGet(CompletableFuture.java:396)
snasmc1 docker/svc-ise-client[1453]: at java.base/java.util.concurrent.CompletableFuture.get(CompletableFuture.java:2061)
snasmc1 docker/svc-ise-client[1453]: at org.springframework.web.socket.client.jetty.JettyWebSocketClient.doHandshake(JettyWebSocketClient.java:100)
snasmc1 docker/svc-ise-client[1453]: at java.base/java.util.concurrent.FutureTask.run(FutureTask.java:284)
snasmc1 docker/svc-ise-client[1453]: at java.base/java.lang.Thread.run(Thread.java:829)
snasmc1 docker/svc-ise-client[1453]: Caused by: javax.net.ssl.SSLException: org.bouncycastle.tls.TlsFatalAlert(40): The certificate is not trusted by the peer
snasmc1 docker/svc-ise-client[1453]: at org.bouncycastle.jssse.provider.ProvSSLSessionImpl.unwrap(ProvSSLSessionImpl.java:100)
snasmc1 docker/svc-ise-client[1453]: at java.base/java.net.ssl.SSLEngine.unwrap(SSLEngine.java:637)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection.unwrap(SslConnection.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection$DecryptedEndPoint.fill(SslConnection$DecryptedEndPoint.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.client.http.HttpReceiverOverHTTP.process(HttpReceiverOverHTTP.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.client.http.HttpReceiverOverHTTP.receive(HttpReceiverOverHTTP.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.client.http.HttpChannelOverHTTP.receive(HttpChannelOverHTTP.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.AbstractConnection$ReadCallback.succeeded(AbstractConnection$ReadCallback.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.FillInterest.fillable(FillInterest.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection$DecryptedEndPoint.onFillable(SslConnection$DecryptedEndPoint.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection.onFillable(SslConnection.java:100)
```

```
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection$2.succeeded(SslConnection$2.java:10)
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(SelectableChannelEndPoint$1.java:10)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.util.thread.QueuedThreadPool.runJob(QueuedThreadPool.java:10)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.util.thread.QueuedThreadPool$Runner.run(QueuedThreadPool$Runner.java:10)
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).