Integrare ISE 3.3 con WSA utilizzando una CA esterna

Sommario

Introduzione

In questo documento vengono descritte le procedure per integrare ISE 3.3 con Cisco Secure Web Appliance (WSA) utilizzando le connessioni pxGrid.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Identity Services Engine
- Cisco Secure Web Appliance (WSA)
- Piattaforma Exchange Grid (pxGrid)
- 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
- Cisco Secure Web Appliance versione 15.2.0-116
- Windows Server 2016 come server CA (Certification Authority) 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 Cisco Identity Services Engine 3.3

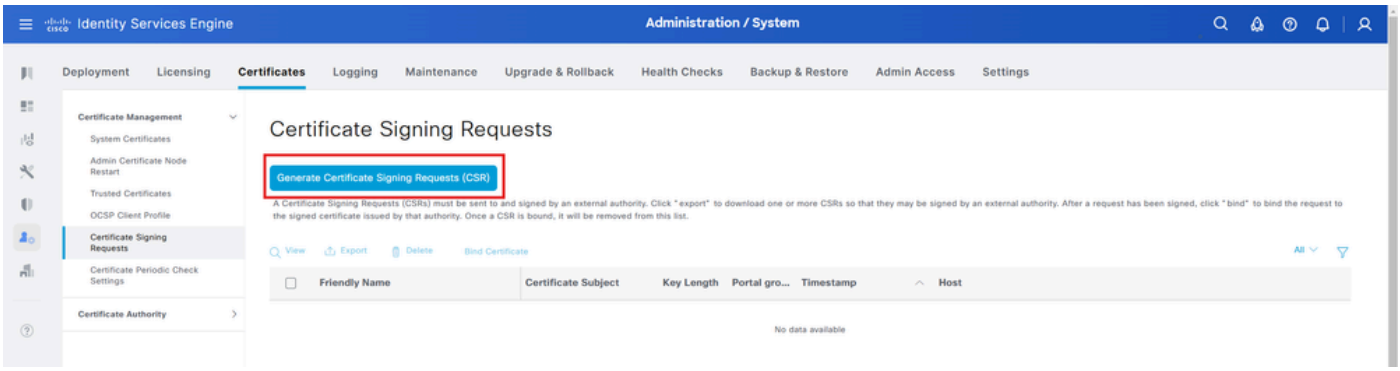
Passaggio 1: Genera un certificato ISEServer pxGrid

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 del certificato (CSR).



4. Selezionare pxGrid nel campo Certificati.

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

6.Inserire i dettagli relativi agli altri certificati, se necessario.

7. Fare clic su Genera.

Usage

Certificate(s) will be used for: pxGrid

Allow Wildcard Certificates

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
ise33	ise33#pxGrid

Subject

Common Name (CN): $FQDN$

Organizational Unit (OU): AAA

Organization (O): Cisco

City (L): Bangalore

State (ST): KA

Country (C): IN

Subject Alternative Name (SAN)

DNS Name	ise33.lab.local
IP Address	10.127.197.128

* Key type: RSA

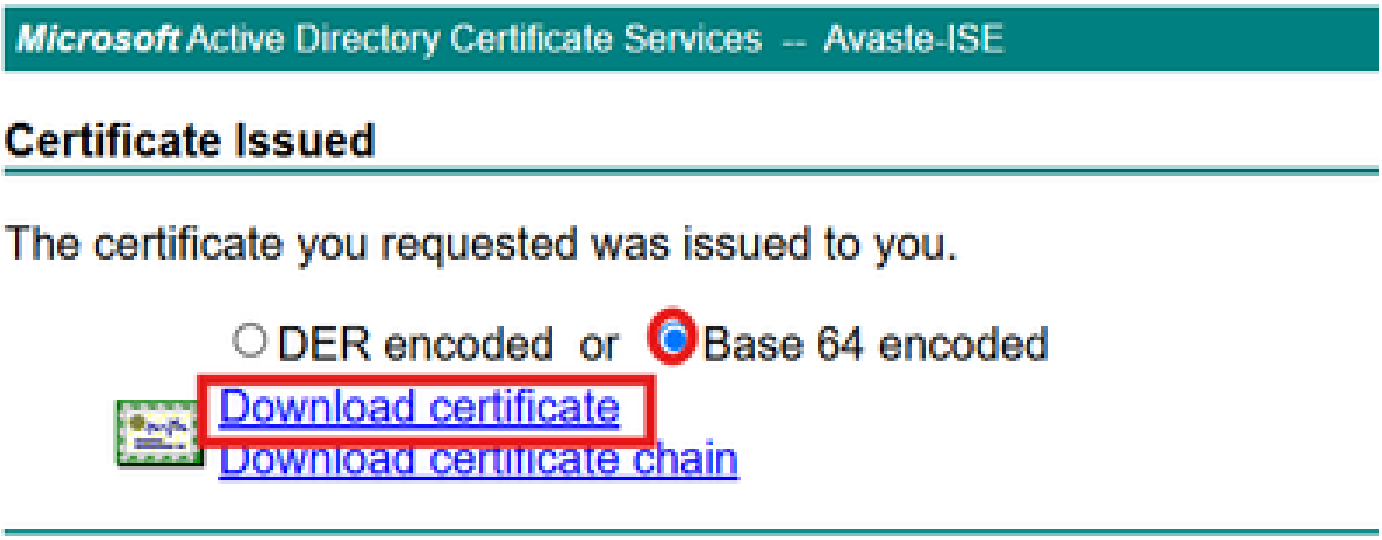
* Key Length: 4096

* Digest to Sign With: SHA-384

Certificate Policies

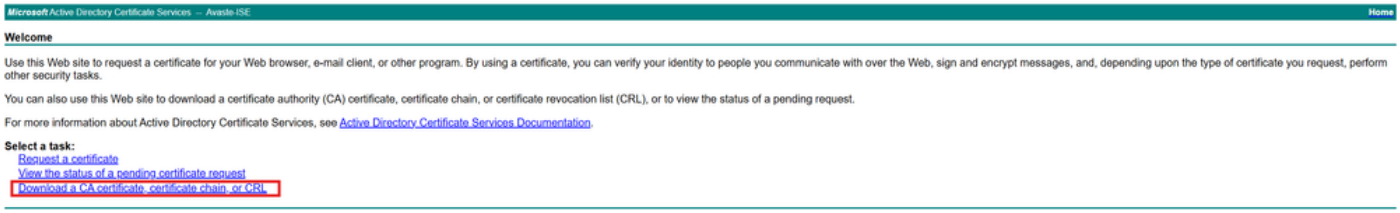
Il modello di certificato pxGrid utilizzato richiede sia l'autenticazione client che l'autenticazione server nel campo Utilizzo chiave avanzato.

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

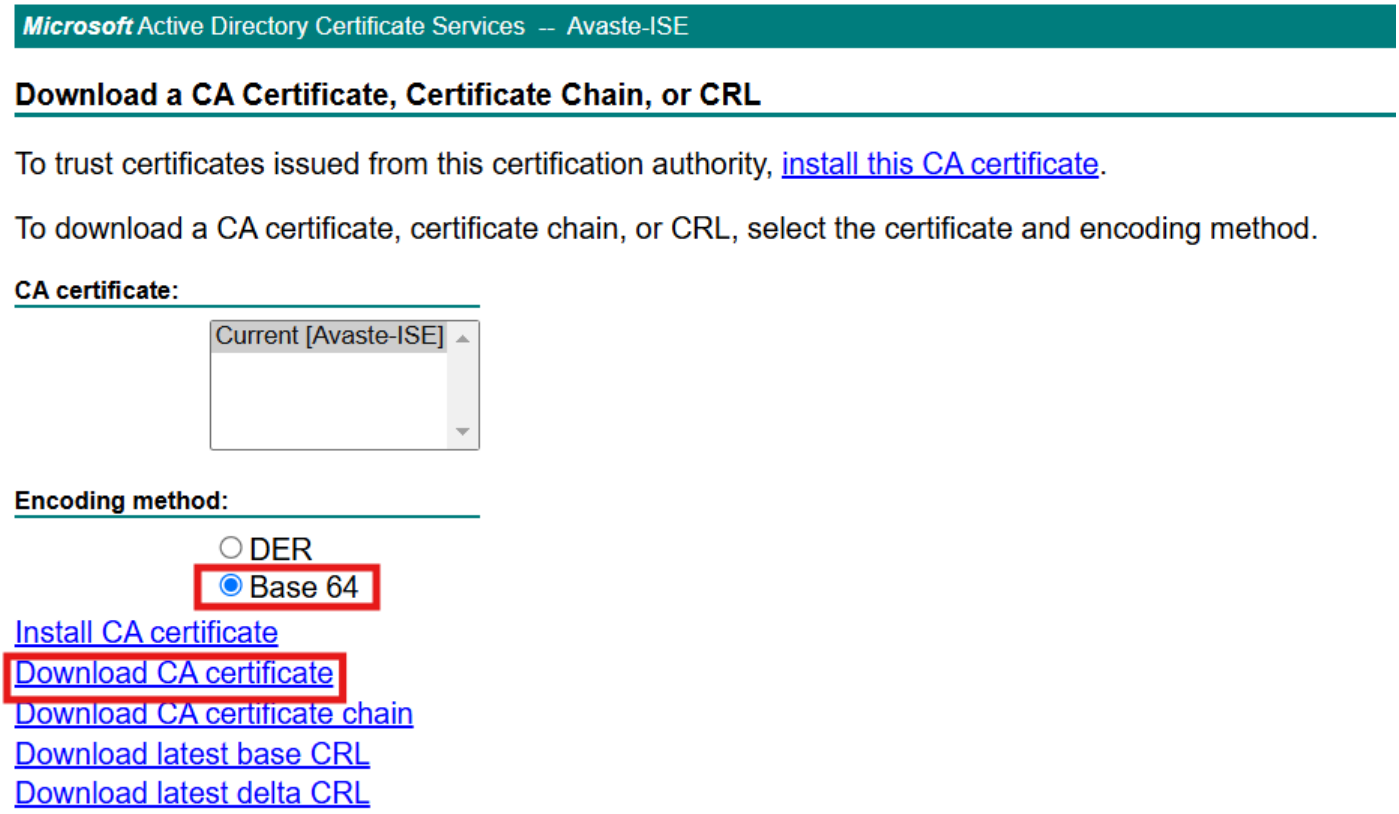


Passaggio 3: Importazione del certificato radice CA nell'archivio di attendibilità ISE

1. Passare alla home page di Servizi certificati Microsoft Active Directory e selezionareScarica un certificato CA, una catena di certificati o un CRL.



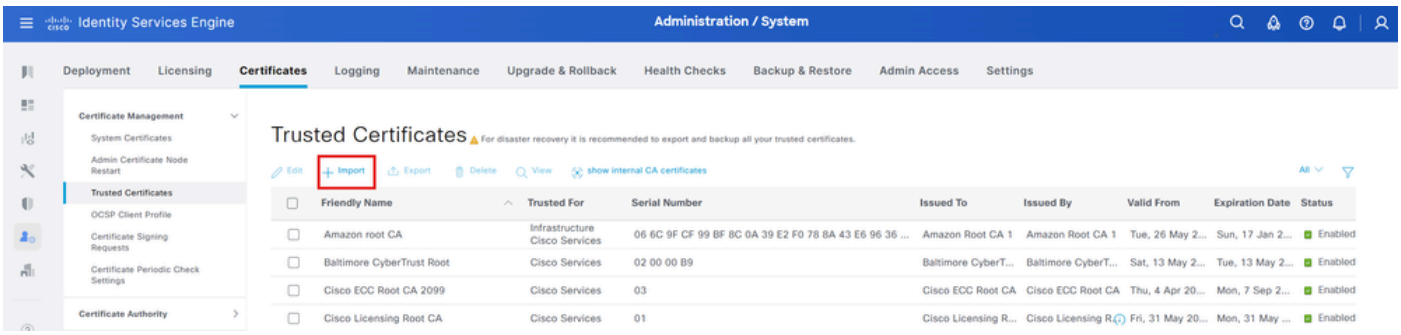
2. Selezionare il formato Base-64, quindi fare clic su Scarica certificato CA.



3.Salvare il certificato come CA_Root.cer.

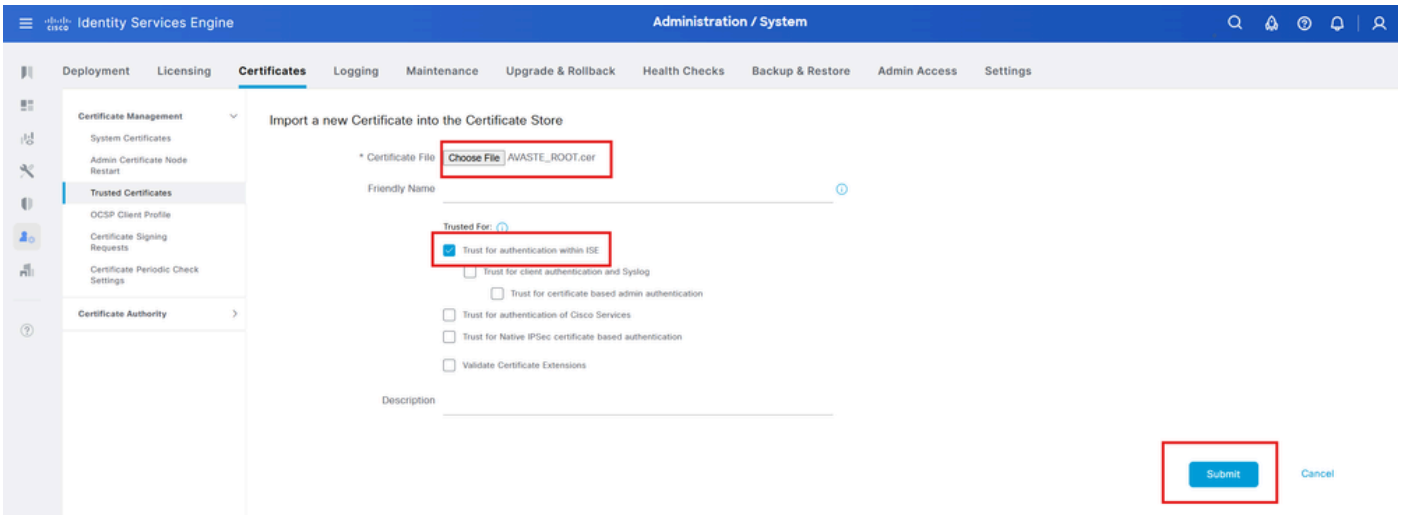
4.Accedere all'interfaccia utente di Cisco Identity Services Engine (ISE).

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



6. SelezionareImporta > File di certificato eImporta il certificato radice.

7. Verificare che la casella di controllo Trust for authentication within ISE sia selezionata.



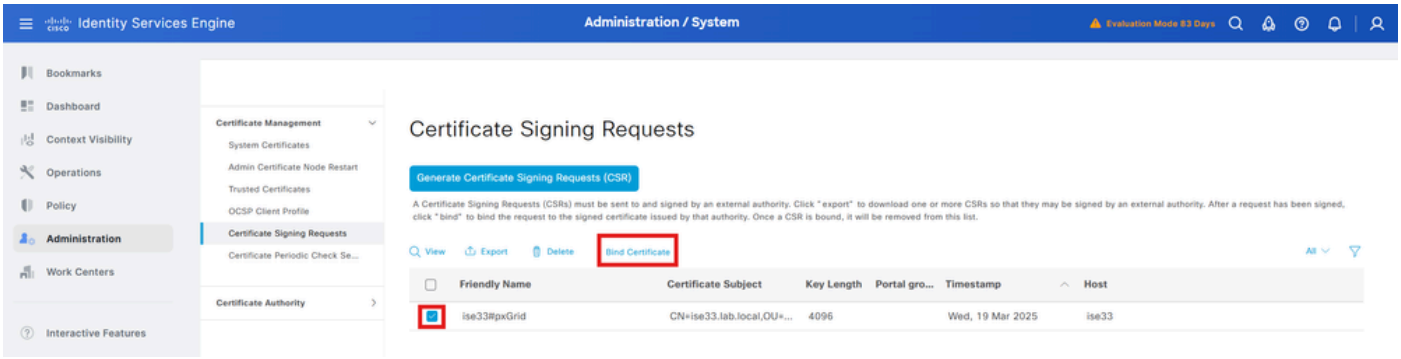
8. Fare clic su Sottometti.

Passaggio 4: Associazione del certificato ISE alla richiesta di firma del certificato (CSR).

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

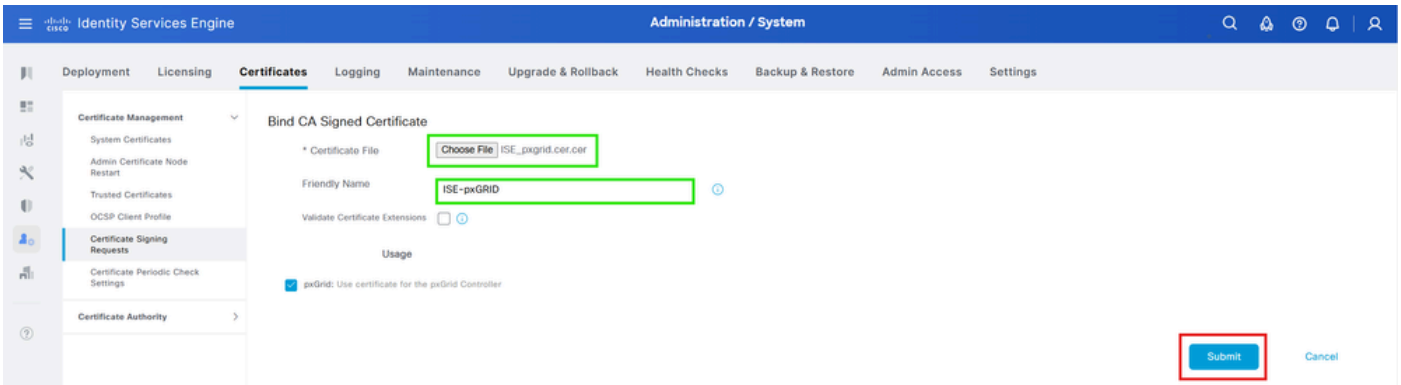
2. Selezionare Amministrazione > Sistema > Certificati > Gestione certificati > Richieste di firma del certificato.

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



4. Nel modulo Binding CA Signed Certificate scegliere il certificato ISE_pxGrid.cer generato in precedenza.

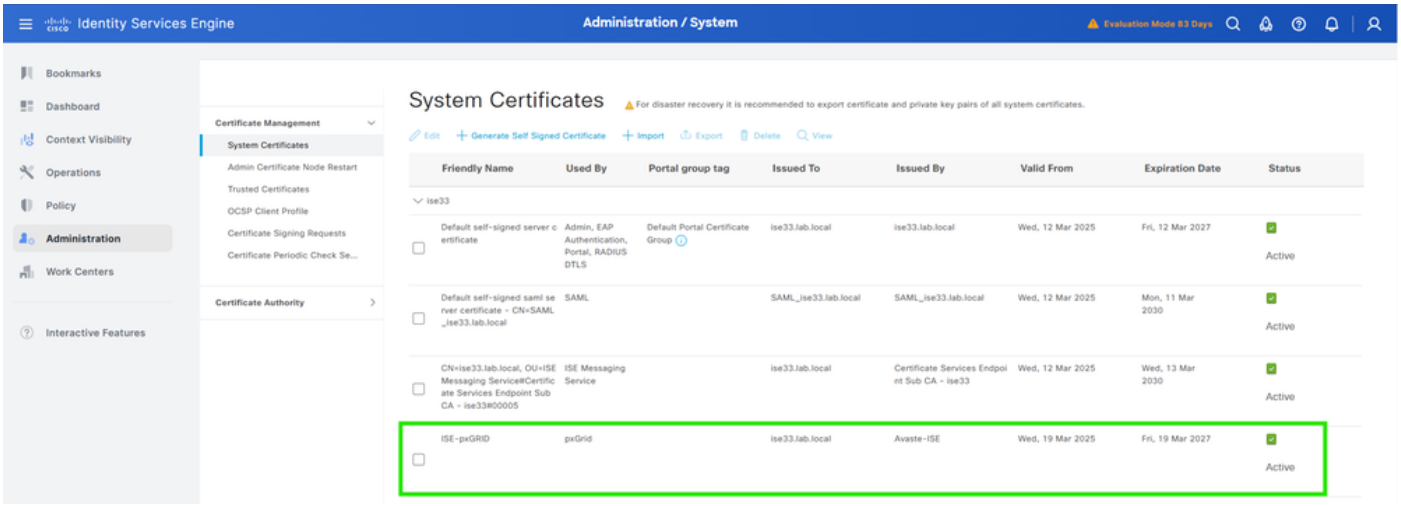
5. Assegnare al certificato un nome descrittivo, quindi fare clic su Invia.



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

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

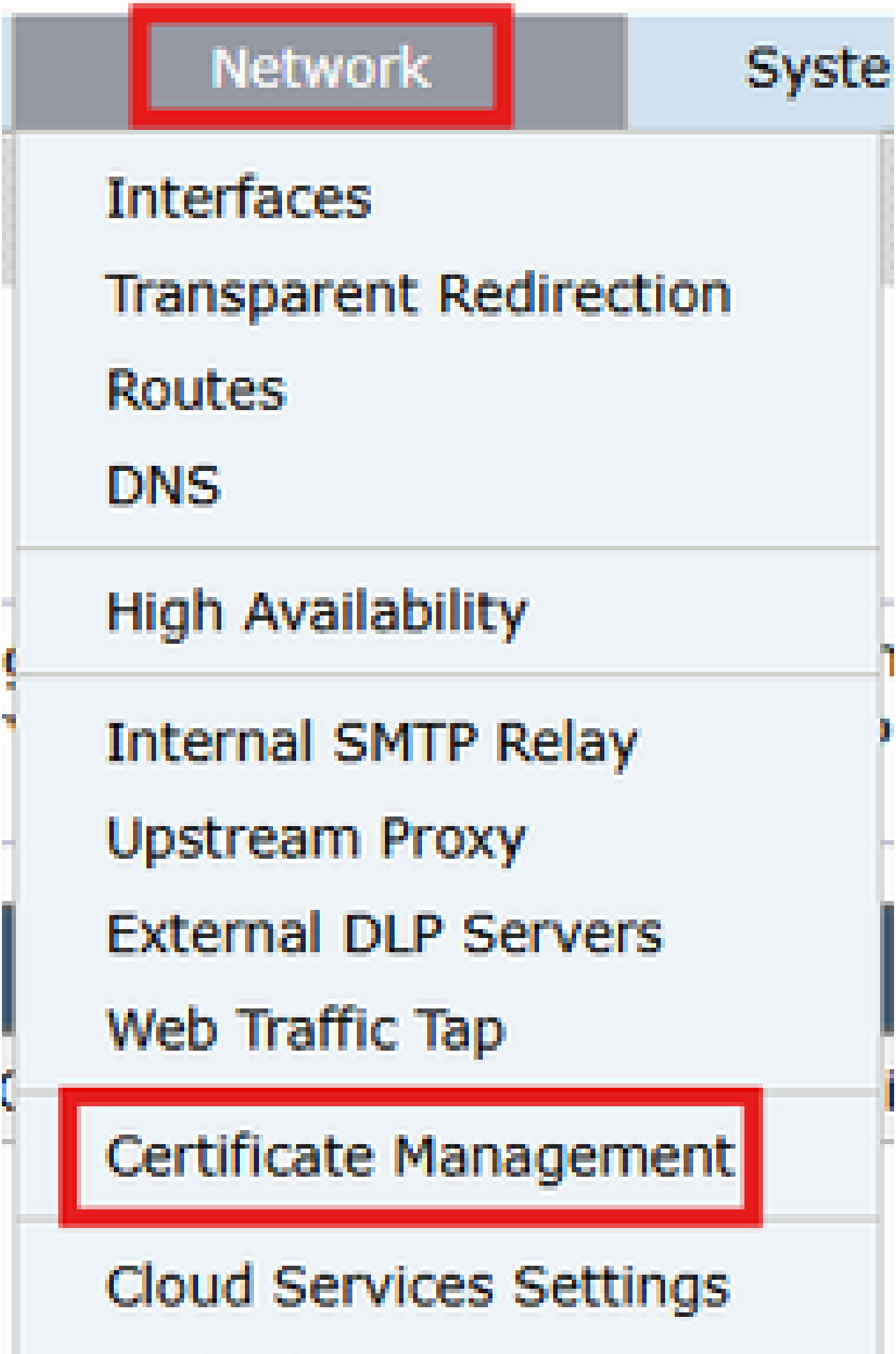
9. È possibile visualizzare nell'elenco il certificato pxGrid creato firmato dalla CA esterna.



Sezione B: Aggiunta del certificato radice CA all'archivio di certificati attendibili WSA

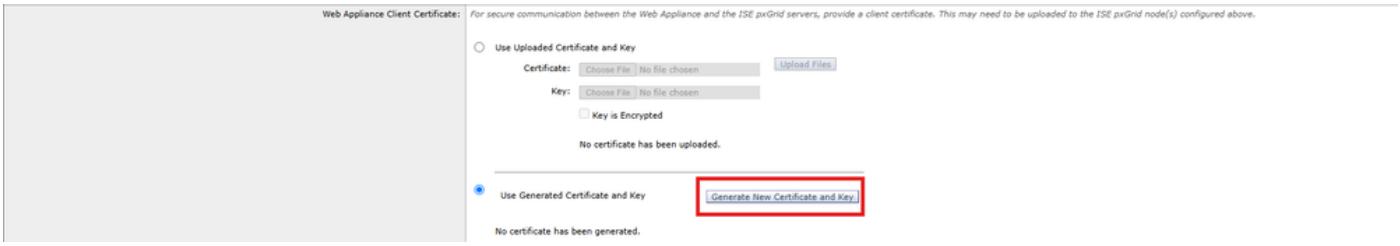
Aggiungi certificato radice CA all'archivio attendibile WSA:

1.Accedere alla GUI di Web Security Appliance (WSA).
2. Passare a Rete > Gestione certificati > Gestisci certificati radice attendibili.

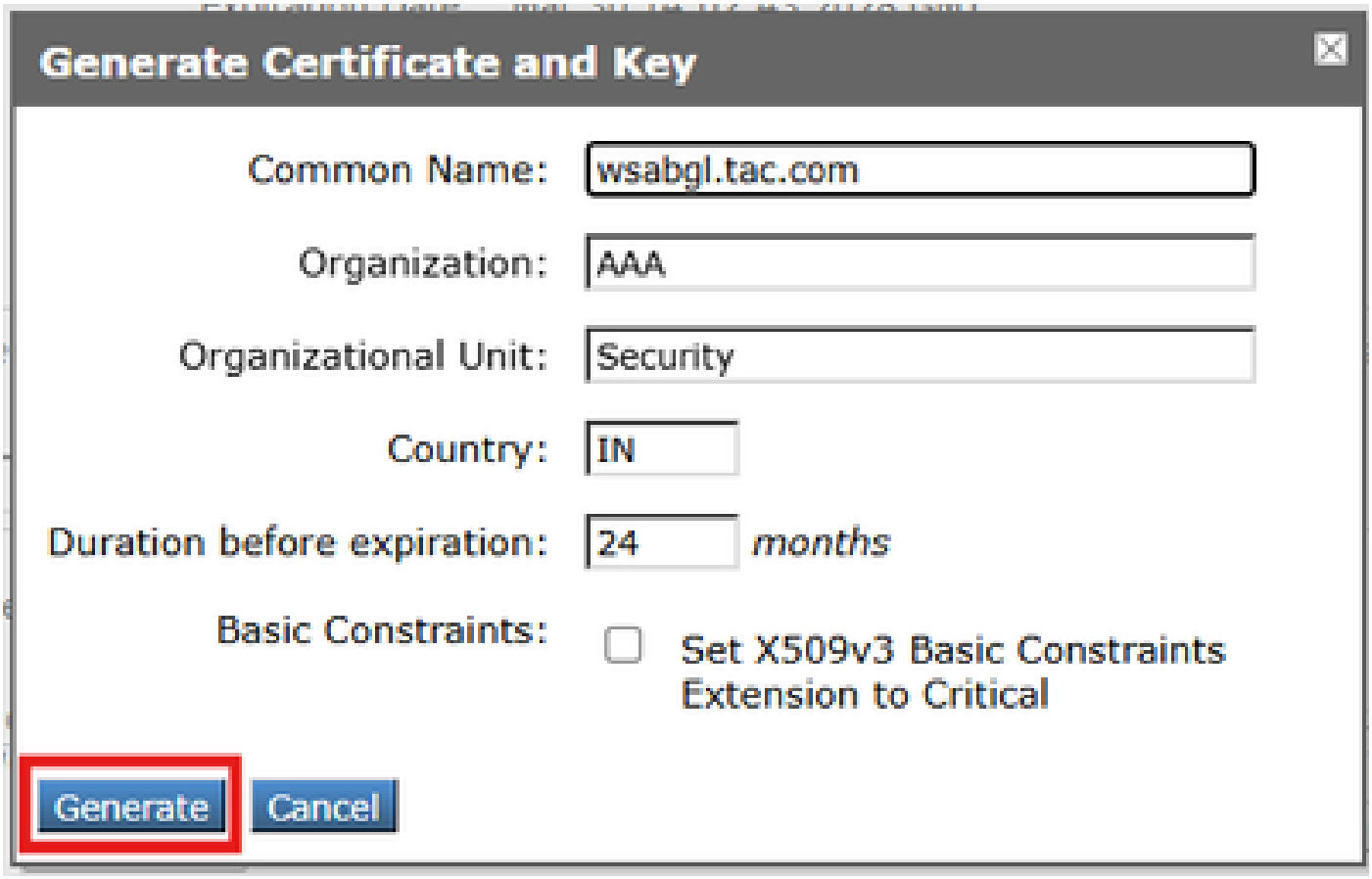

Network
Syste
Interfaces
Transparent Redirection
Routes
DNS
High Availability
Internal SMTP Relay
Upstream Proxy
External DLP Servers
Web Traffic Tap
Certificate Management
Cloud Services Settings

Per ogni implementazione ISE possono esistere solo due nodi pxGrid. Questa configurazione funziona come una configurazione di standby attivo di pxGrid; può essere attivo un solo nodo ISE+pxGrid alla volta. In una configurazione pxGrid Active-Standby, tutte le informazioni vengono passate attraverso il PAN, dove il secondo nodo ISE+pxGrid rimane inattivo.

8. Scorrere fino alla sezione Certificato client Web Appliance e fare clic su Genera nuovo certificato e chiave.

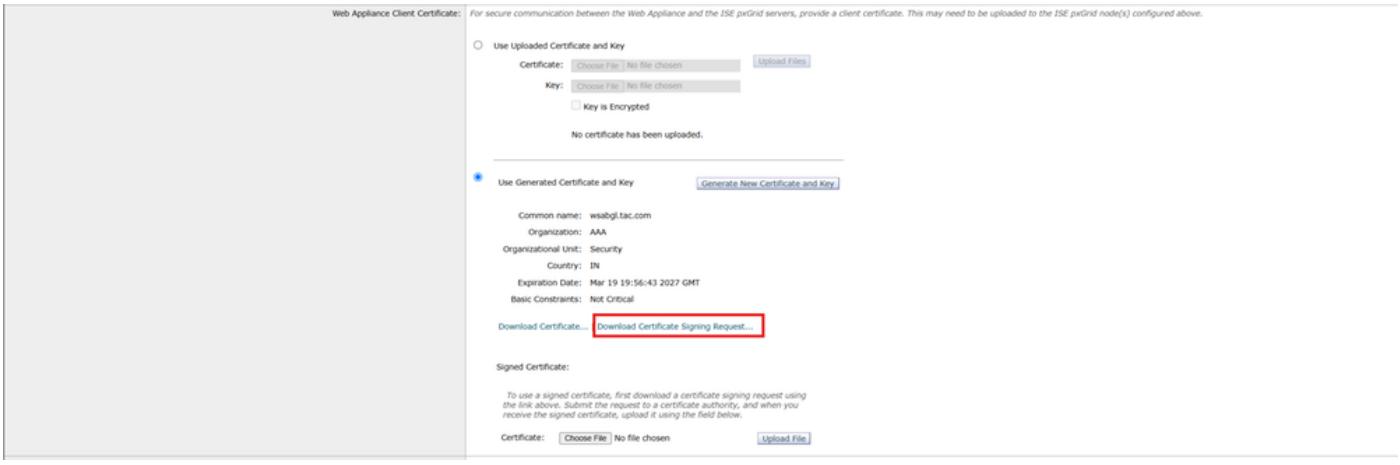


9. Inserire i dettagli del certificato come necessario e fare clic su Genera.



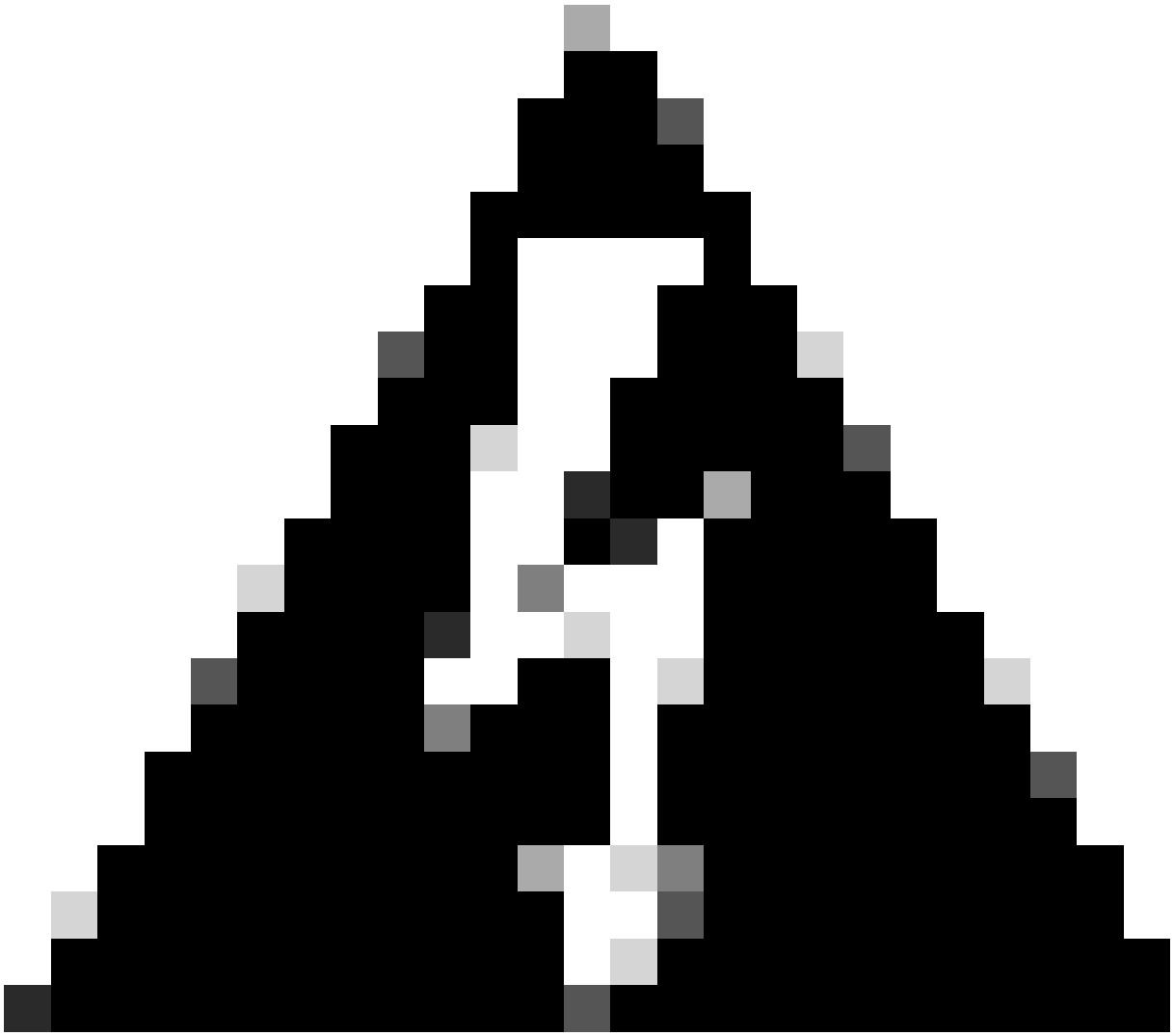
Nota: La durata del certificato deve essere un numero intero compreso tra 24 e 60 mesi e il paese deve essere un codice ISO a due caratteri del paese (solo lettere maiuscole).

10. Fare clic su Scarica richiesta di firma certificato.



11. Fare clic su Sottometti.

12. Fare clic su Commit delle modifiche per applicare le modifiche.

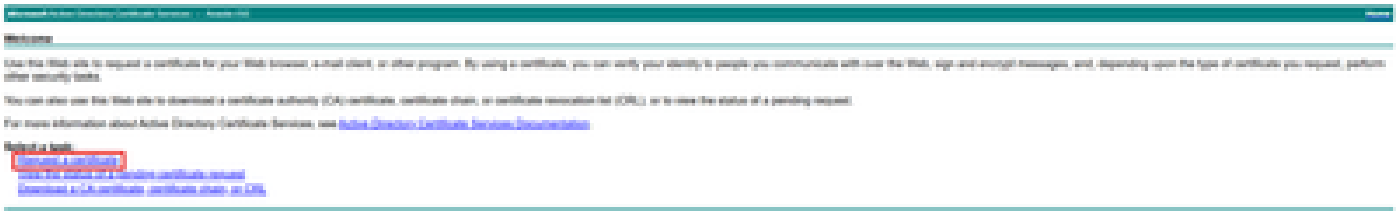


Avviso: Se non si inviano ed eseguono il commit delle modifiche indicate e non si carica direttamente il certificato firmato e non si esegue il commit, è possibile che si verifichino problemi durante l'integrazione.

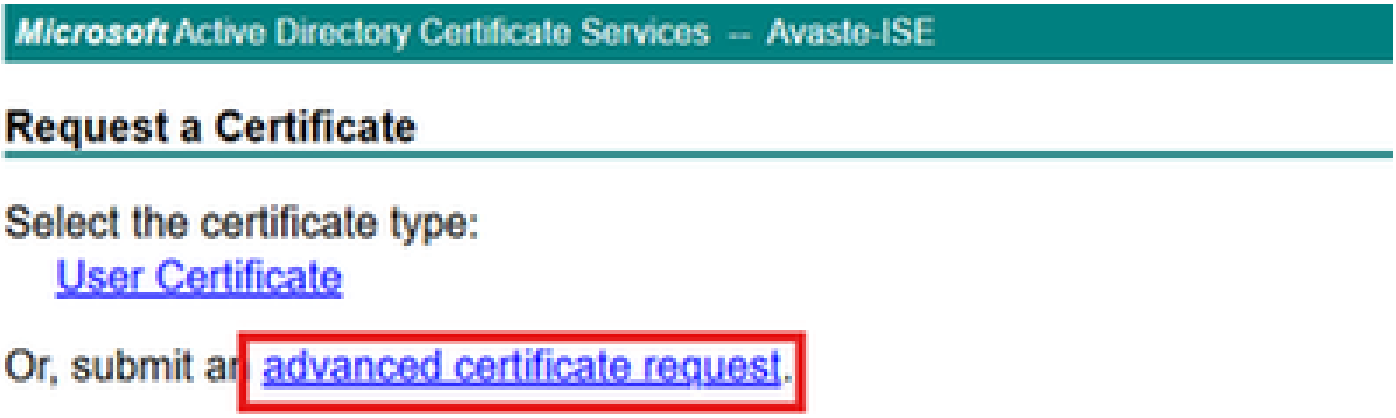
Sezione B: Firmare un CSR client WSA utilizzando una CA esterna

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

2. Fare clic su Richiedi certificato.

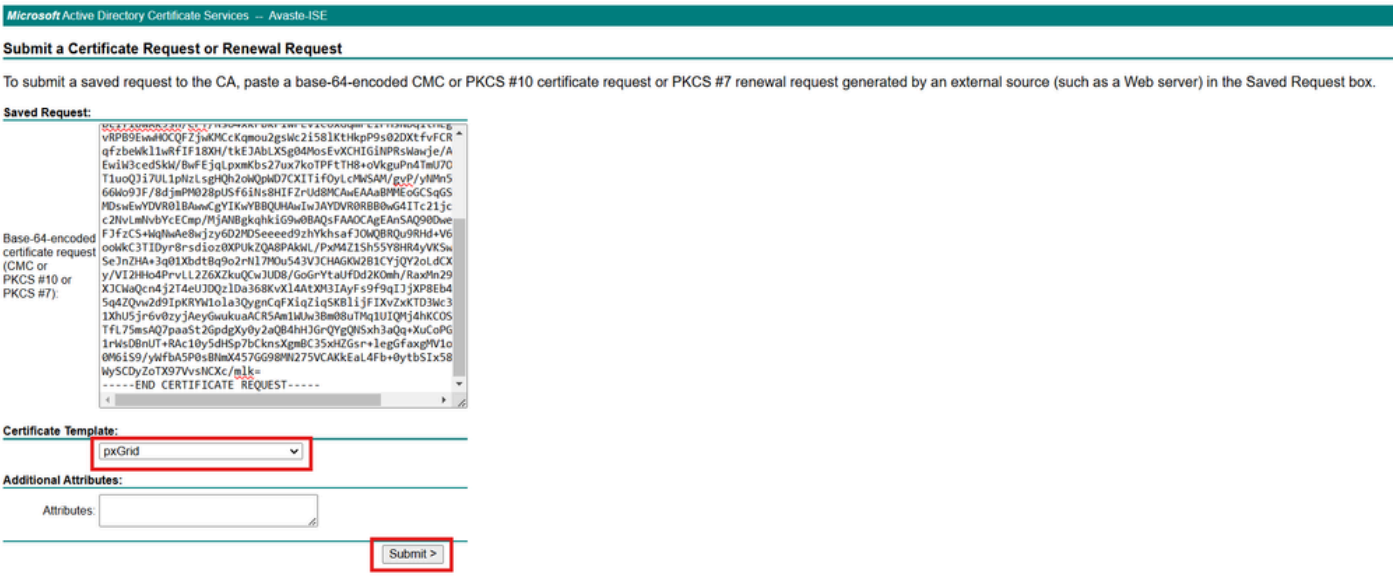


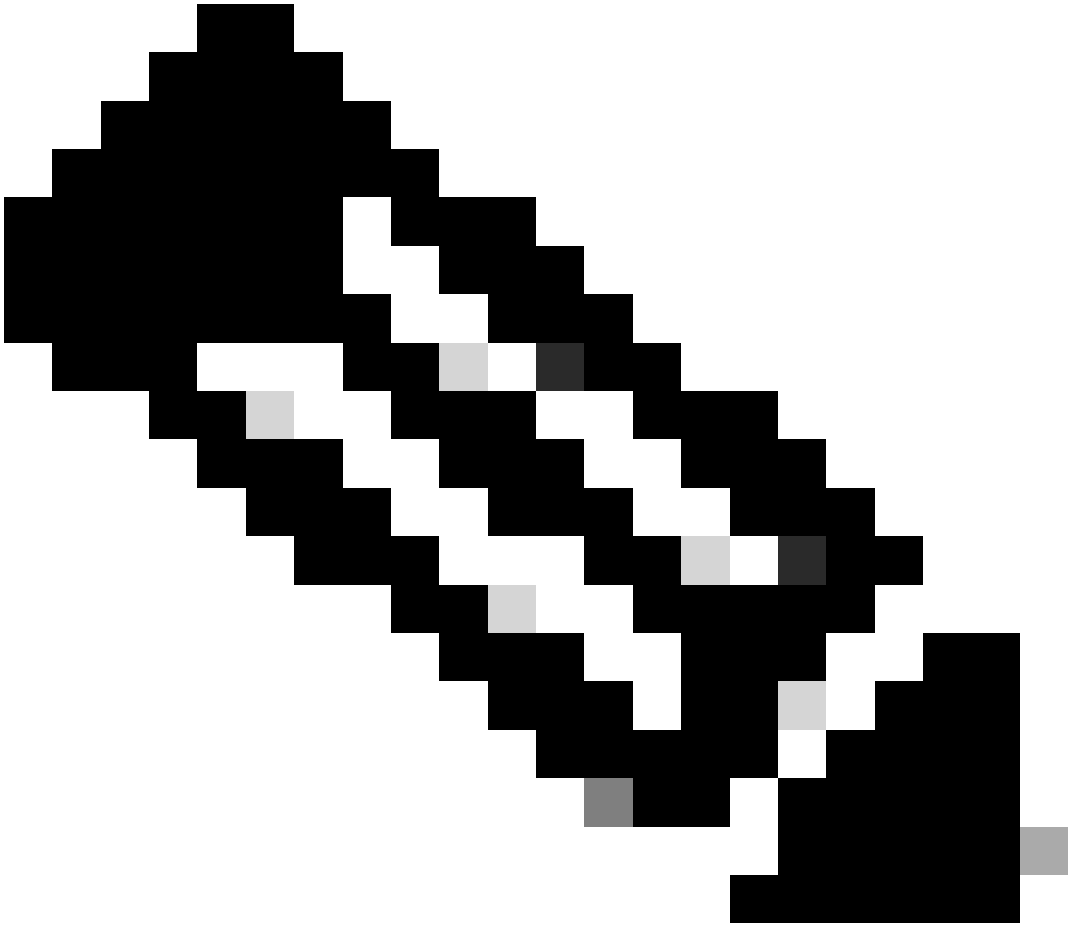
3. Scegliere di sottomettere una richiesta avanzata di certificati.



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

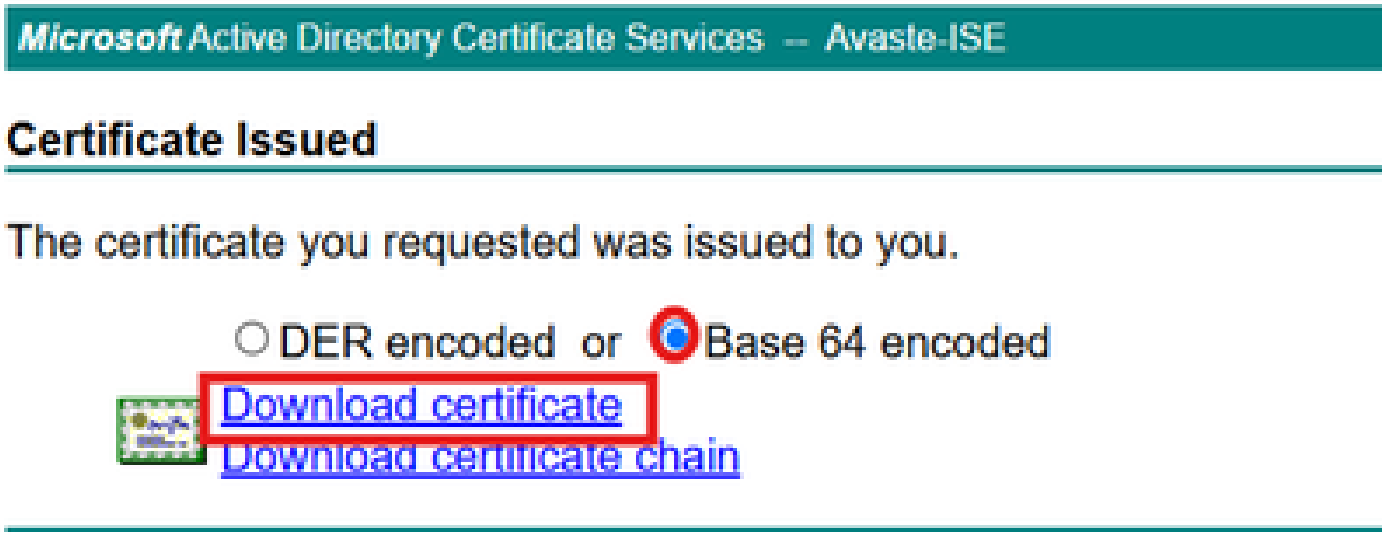
5. Selezionare pxGridas theCertificate Template, quindi fare clic su Invia.





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

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



Sezione C: Associazione del certificato client WSA alla richiesta di firma del certificato (CSR) e integrazione.

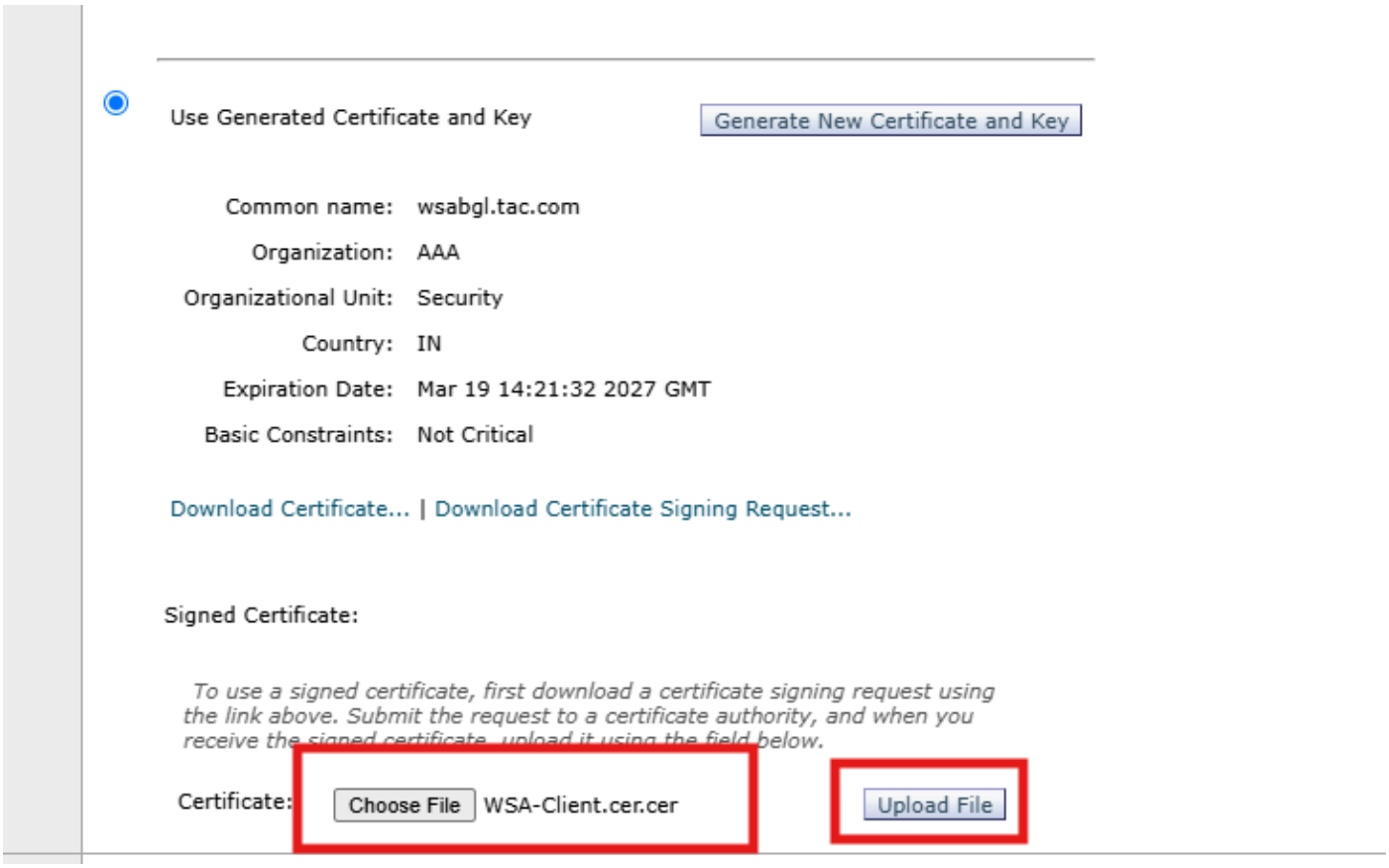
1.Passare alla GUI di Web Security Appliance (WSA).

2. Passare a Rete > Servizi di identificazione > Motore servizio di identificazione.

3. Fare clic su Modifica impostazioni.

4. Passare alla sezione Certificato client Web Appliance.

5.Nella sezione Certificato firmato, caricare il certificato firmato WSA-Client.cer



6. Fare clic su Submit (Invia).

7. Fare clic su Commit Changes per applicare le modifiche.

8.Fare clic su Modifica impostazioni.

9.Scorrere fino a Test comunicazione con i nodi ISE e fare clic su Start Test, che può avere il seguente risultato:

Test della comunicazione con i nodi ISE

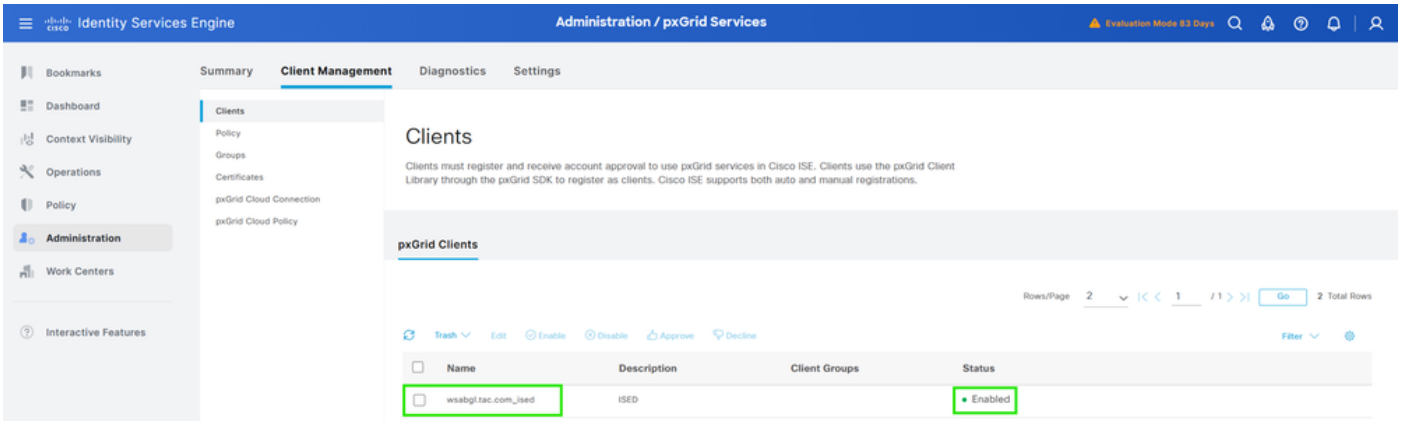
Test della comunicazione con i nodi ISE

```
Checking DNS resolution of ISE pxGrid Node hostname(s) ...
Success: Resolved '10.127.197.128' address: 10.127.197.128
Validating WSA client certificate ...
Success: Certificate validation successful
Validating ISE pxGrid Node certificate(s) ...
Success: Certificate validation successful
Checking connection to ISE pxGrid Node(s) ...
Trying primary PxGrid server...
SXP not enabled.
ERS not enabled.
Preparing TLS connection...
Completed TLS handshake with PxGrid successfully.
Trying download user-session from (https://ise33.lab.local:8910)...
Failure: Failed to download user-sessions.
Trying download SGT from (https://ise33.lab.local:8910)...
Able to Download 17 SGTs.
Skipping all SXP related service requests as SXP is not configured.
Success: Connection to ISE pxGrid Node was successful.
Test completed successfully.
```

Verifica

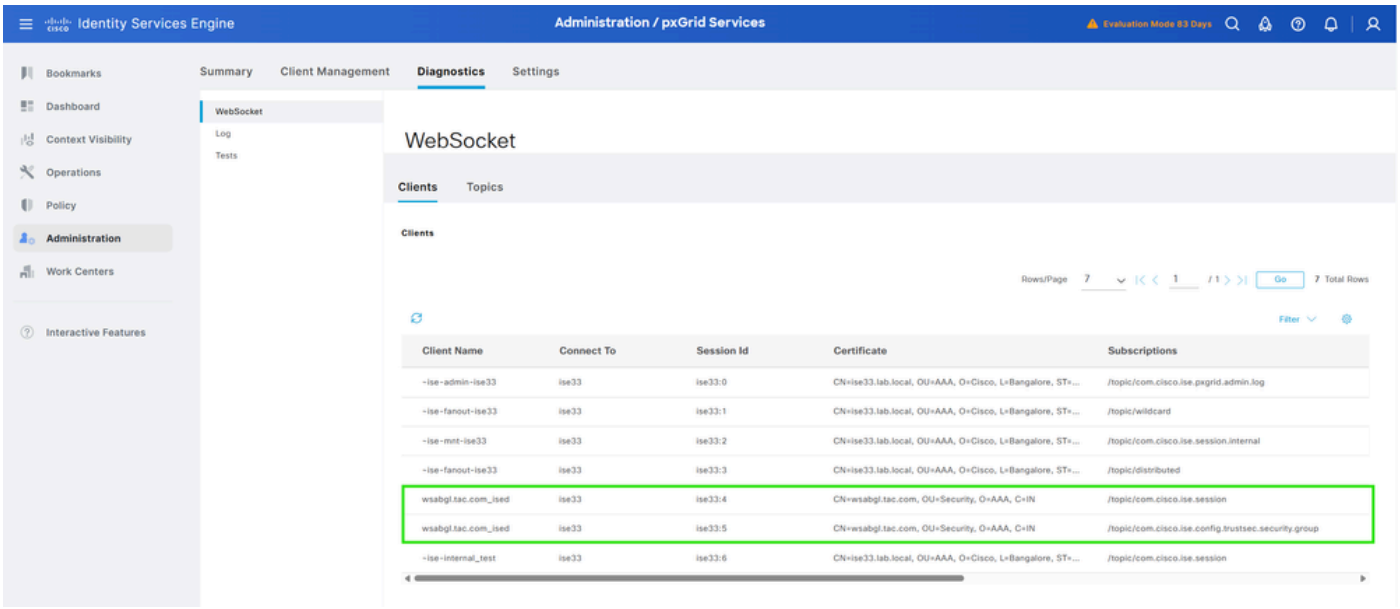
In Cisco ISE, selezionare Administration > pxGrid Services > Client Management > Client.

In questo modo il WSA viene generato come client pxgrid con statusEnabled.



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

Websocket > Client:



Cisco ISE Pixgrid-server.log TRACE level.reference.

<#root>

```
{"timestamp":1742395398803,"level":"INFO","type":"WS_SERVER_CONNECTED","host":"ise33","client":"
```

wsabgl.lab.local_ised

```
","server":"wss://ise33.lab.local:8910/pxgrid/ise/pubsub","message":"WebSocket connected. session\u003d
TRACE [Thread-8][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistributor -:::::- Drop. exclude=[id=3,cl
DEBUG [Thread-8][[]] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::::- Authenticating null
DEBUG [Thread-8][[]] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::::- Certs up to date. user=~ise-pu
DEBUG [Thread-8][[]] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::::- preAuthenticatedPrincipal = ~i
DEBUG [Thread-8][[]] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::::- X.509 client authentication ce
DEBUG [Thread-8][[]] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::::- Authentication
```

success

```
: PreAuthenticatedAuthenticationToken [Principal=org.springframework.security.core.userdetails.User [Us
DEBUG [Thread-8][[]] cisco.cpm.pxgridwebapp.data.AuthzDaoImpl -:::::- requestNodeName=wsabgl.lab.local
DEBUG [Thread-13][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistributor -:::::- Adding subscription=[
INFO [Thread-13][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::::- Pubsub subscribe. subscrip
TRACE [WsIseClientConnection-804][[]] cpm.pxgrid.ws.client.WsEndpoint -:::::- Send. session=[id=34eae1
```

"wsabgl.lab.local_ised

```
","server":"wss://ise33.lab.local:8910/pxgrid/ise/pubsub","message":"Pubsub subscribe. subscription\u00
TRACE [Thread-3][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::::- Received frame=[command=SE
TRACE [Thread-3][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::::- Authorized to send (cached
TRACE [Thread-3][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistributor -:::::- Distribute from=[id=0,
TRACE [Thread-3][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistributor -:::::- Distribute distributed
TRACE [Thread-3][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistributor -:::::- Distribute distributed
TRACE [sub-sender-1][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionSender -:::::- Send. subscription=[id=
TRACE [sub-sender-0][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionSender -:::::- Send. subscription=[id=
DEBUG [Grizzly(1)][[]] cpm.pxgrid.ws.client.WsSubscriber -:::::- onStompMessage session=[id=34eae17d-5
DEBUG [Grizzly(1)][[]] cpm.pxgrid.ws.client.WsSubscriber -:::::- onStompMessage session=[id=4b4d7de4-b
TRACE [Grizzly(1)][[]] cpm.pxgrid.ws.client.WsEndpoint -:::::- Send. session=[id=dd1d138d-a640-4f4f-bd
TRACE [Grizzly(1)][[]] cpm.pxgridwebapp.ws.distributed.FanoutDistributor -:::::- DownstreamHandler sen
TRACE [Thread-10][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::::- Received frame=[command=S
```

```
TRACE [Thread-10][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::::- Authorized to send (cache
```

Risoluzione dei problemi

Problema

Problema CA sconosciuto. Su WSA il test per la connessione ISE non riesce con un errore. Errore: Timeout della connessione al server ISE PxGrid.

Cisco ISE Pixgrid-server.log TRACE level.reference.

<#root>

ERROR

```
 [Thread-8][[]] cisco.cpm.pxgrid.cert.LoggingTrustManagerWrapper -:::::- checkClientTrusted exception.
```

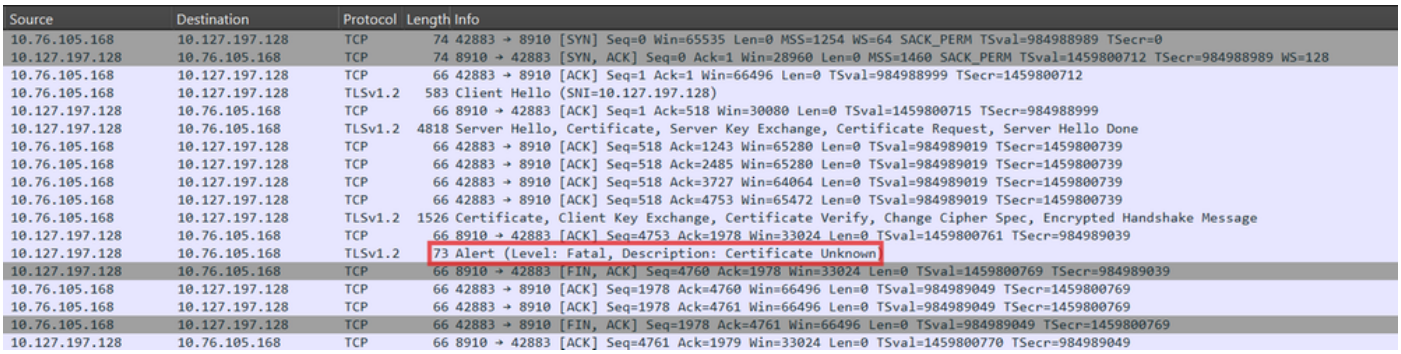
unable to find valid certification path to requested target principle=CN=wsabgl.lab.local, OU=Security,

```
TRACE [WsIseClientConnection-804][[]] cpm.pxgrid.ws.client.WsEndpoint -:::::- Send. session=[id=34eae1
TRACE [Thread-9][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::::- Received frame=[command=SE
TRACE [Thread-9][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::::- Authorized to send (cached
TRACE [Thread-9][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistributor -:::::- Distribute from=[id=0,
```

unable to find valid certification path to requested target

```
 principle\u003dCN\u003dwsabgl.lab.local, OU\u003dSecurity, O\u003dAAA, C\u003dIN"}
TRACE [Thread-9][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistributor -:::::- Distribute distributed
TRACE [Thread-9][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistributor -:::::- Distribute distributed
TRACE [sub-sender-1][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionSender -:::::- Send. subscription=[id=
DEBUG [Grizzly(2)][[]] cpm.pxgrid.ws.client.WsSubscriber -:::::- onStompMessage session=[id=4b4d7de4-b
TRACE [Grizzly(2)][[]] cpm.pxgrid.ws.client.WsEndpoint -:::::- Send. session=[id=dd1d138d-a640-4f4f-bd
```

La causa del problema può essere individuata con le acquisizioni dei pacchetti,



Source	Destination	Protocol	Length	Info
10.76.105.168	10.127.197.128	TCP	74	42883 → 8910 [SYN] Seq=0 Win=65535 Len=0 MSS=1254 WS=64 SACK_PERM TSval=984988989 TSecr=0
10.127.197.128	10.76.105.168	TCP	74	8910 → 42883 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=1459800712 TSecr=984988989 WS=128
10.76.105.168	10.127.197.128	TCP	66	42883 → 8910 [ACK] Seq=1 Ack=1 Win=66496 Len=0 TSval=984988999 TSecr=1459800712
10.76.105.168	10.127.197.128	TLSv1.2	583	Client Hello (SNI=10.127.197.128)
10.127.197.128	10.76.105.168	TCP	66	8910 → 42883 [ACK] Seq=1 Ack=518 Win=30080 Len=0 TSval=1459800715 TSecr=984988999
10.127.197.128	10.76.105.168	TLSv1.2	4818	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
10.76.105.168	10.127.197.128	TCP	66	42883 → 8910 [ACK] Seq=518 Ack=1243 Win=65280 Len=0 TSval=984989019 TSecr=1459800739
10.76.105.168	10.127.197.128	TCP	66	42883 → 8910 [ACK] Seq=518 Ack=2485 Win=65280 Len=0 TSval=984989019 TSecr=1459800739
10.76.105.168	10.127.197.128	TCP	66	42883 → 8910 [ACK] Seq=518 Ack=3727 Win=64064 Len=0 TSval=984989019 TSecr=1459800739
10.76.105.168	10.127.197.128	TCP	66	42883 → 8910 [ACK] Seq=518 Ack=4753 Win=65472 Len=0 TSval=984989019 TSecr=1459800739
10.76.105.168	10.127.197.128	TLSv1.2	1526	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
10.127.197.128	10.76.105.168	TCP	66	8910 → 42883 [ACK] Seq=4753 Ack=1978 Win=33024 Len=0 TSval=1459800761 TSecr=984989039
10.127.197.128	10.76.105.168	TLSv1.2	73	Alert (Level: Fatal, Description: Certificate Unknown)
10.127.197.128	10.76.105.168	TCP	66	8910 → 42883 [FIN, ACK] Seq=4760 Ack=1978 Win=33024 Len=0 TSval=1459800769 TSecr=984989039
10.76.105.168	10.127.197.128	TCP	66	42883 → 8910 [ACK] Seq=1978 Ack=4760 Win=66496 Len=0 TSval=984989049 TSecr=1459800769
10.76.105.168	10.127.197.128	TCP	66	42883 → 8910 [ACK] Seq=1978 Ack=4761 Win=66496 Len=0 TSval=984989049 TSecr=1459800769
10.76.105.168	10.127.197.128	TCP	66	42883 → 8910 [FIN, ACK] Seq=1978 Ack=4761 Win=66496 Len=0 TSval=984989049 TSecr=1459800769
10.127.197.128	10.76.105.168	TCP	66	8910 → 42883 [ACK] Seq=4761 Ack=1979 Win=33024 Len=0 TSval=1459800770 TSecr=984989049

Soluzione

1. Verificare che il certificato firmato da Web Appliance sia stato associato correttamente al WSA e che sia stato eseguito il commit delle modifiche.

2. Verificare che l'autorità emittente o il certificato CA radice del certificato client WSA faccia parte di Trusted Store in Cisco ISE.

Difetti noti

ID bug Cisco	Descrizione
Cisco, ID bug 23986	La richiesta API getUserGroups di Pxgrid ha restituito una risposta vuota.
Cisco ID bug 7321	WSA riceve SID anziché gruppi AD da ISE.

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).