

Integrare ISE 3.3 con WSA utilizzando una CA esterna

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

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

[Passaggio 1: Genera un certificato ISEServer pxGrid](#)

[Passaggio 2: Creare un certificato PxGrid per un server ISE utilizzando una CA esterna](#)

[Passaggio 3: Importazione del certificato radice CA nell'archivio di attendibilità ISE](#)

[Passaggio 4: Associazione del certificato ISE alla richiesta di firma del certificato \(CSR\).](#)

[Sezione B: Aggiunta del certificato radice CA all'archivio di certificati attendibili WSA](#)

[Integrazione](#)

[Sezione A: Abilitare WSA per l'integrazione ISE e generare CSR per il certificato client WSA.](#)

[Sezione B: Firmare un CSR client WSA utilizzando una CA esterna](#)

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

[Verifica](#)

[Risoluzione dei problemi](#)

[Problema](#)

[Soluzione](#)

[Difetti noti](#)

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.

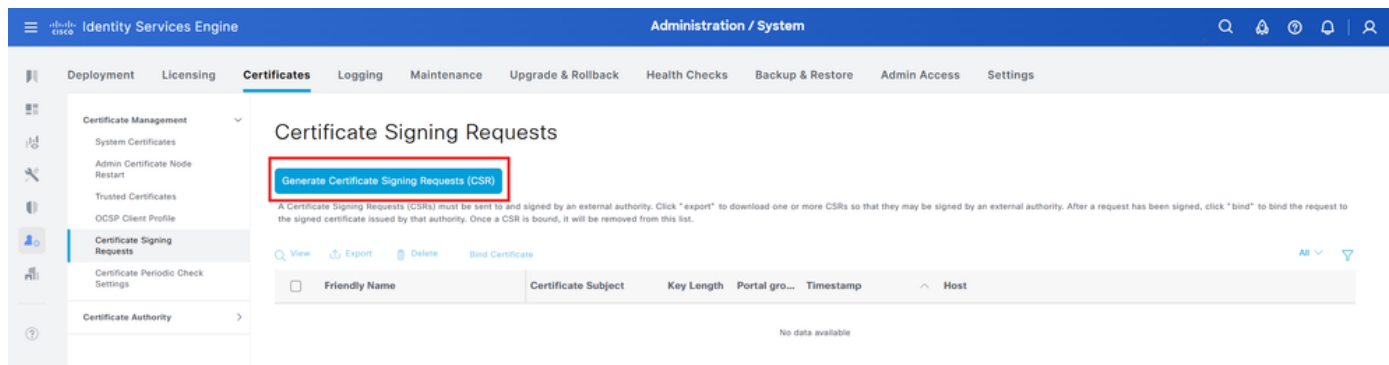
Configurazione

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.

Microsoft Active Directory Certificate Services -- Avast-ISE

Certificate Issued

The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

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

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

Microsoft Active Directory Certificate Services -- Avast-ISE

Home

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](#)

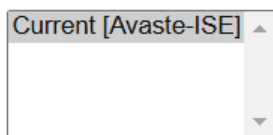
2. Selezionare il formato Base-64, quindi fare clic su Scarica certificato CA.

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](#)

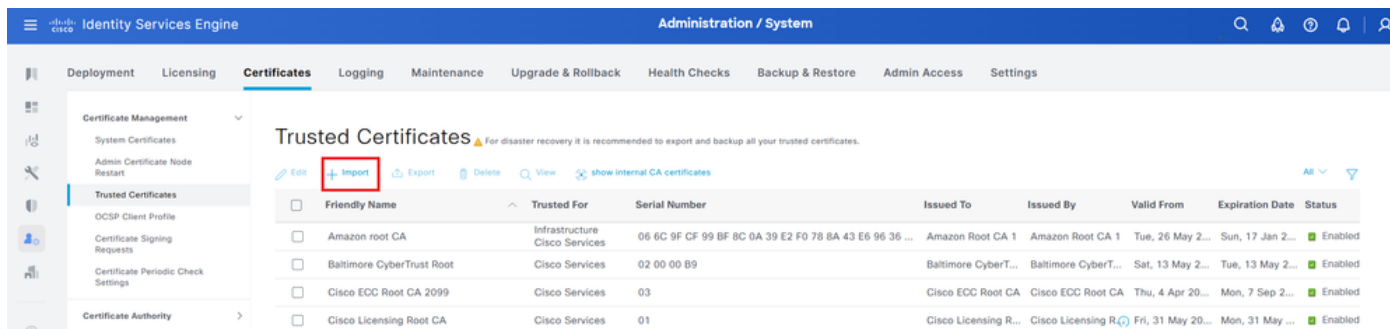
[Download latest base CRL](#)

[Download latest delta CRL](#)

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.



Friendly Name	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Status
☐ Amazon root CA	Infrastructure Cisco Services	06 6C 9F 9F 99 BF 8C 0A 39 E2 F0 78 8A 43 E6 96 36 ...	Amazon Root CA 1	Amazon Root CA 1	Tue, 26 May 2...	Sun, 17 Jan 2...	Enabled
☐ Baltimore CyberTrust Root	Cisco Services	02 00 00 B9	Baltimore CyberT...	Baltimore CyberT...	Sat, 13 May 2...	Tue, 13 May 2...	Enabled
☐ Cisco ECC Root CA 2099	Cisco Services	03	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 20...	Mon, 7 Sep 2...	Enabled
☐ Cisco Licensing Root CA	Cisco Services	01	Cisco Licensing R...	Cisco Licensing R...	Fri, 31 May 20...	Mon, 31 May ...	Enabled

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

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

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

Import a new Certificate into the Certificate Store

* Certificate File **Choose File** AWASTE_ROOT.cer

Friendly Name

Trusted For

- ☒ Trust for authentication within ISE
- ☐ Trust for client authentication and Syslog
- ☐ Trust for certificate based admin authentication
- ☐ Trust for authentication of Cisco Services
- ☐ Trust for Native IPsec certificate based authentication
- ☐ Validate Certificate Extensions

Description

Submit Cancel

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.

Identity Services Engine Administration / System

Bookmarks

- Dashboard
- Context Visibility
- Operations
- Policy
- Administration**
- Work Centers
- Interactive Features

Certificate Management

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

Certificate Authority

Certificate Signing Requests

Generate Certificate Signing Requests (CSR)

A Certificate Signing Requests (CSRs) 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 gro...	Timestamp	Host
☒	ise33rpxGrid	CN=ise33.lab.local,OU=...	4096		Wed, 19 Mar 2025	ise33

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.

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.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System page. The left sidebar contains navigation links: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (selected), Work Centers, and Interactive Features. The main content area is titled 'System Certificates' and includes a warning: 'For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.' Below this, there are buttons for Edit, Generate Self Signed Certificate, Import, Export, Delete, and View. A table lists the system certificates:

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
Default self-signed server certificate	Admin, EAP Authentication, Portal, RADIUS, DTLS	Default Portal Certificate Group	ise33.lab.local	ise33.lab.local	Wed, 12 Mar 2025	Fri, 12 Mar 2027	Active
Default self-signed saml server certificate - CN=SAML_ise33.lab.local	SAML		SAML_ise33.lab.local	SAML_ise33.lab.local	Wed, 12 Mar 2025	Mon, 11 Mar 2030	Active
CN=ise33.lab.local, OU=ISE Messaging Service, Certificate Services Endpoint Sub CA - ise33m00005	ISE Messaging Service		ise33.lab.local	Certificate Services Endpoint Sub CA - ise33	Wed, 12 Mar 2025	Wed, 13 Mar 2030	Active
ISE-pxGRID	pxGrid		ise33.lab.local	Avaste-ISE	Wed, 19 Mar 2025	Fri, 19 Mar 2027	Active

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

System

Interfaces

Transparent Redirection

Routes

DNS

High Availability

Internal SMTP Relay

Upstream Proxy

External DLP Servers

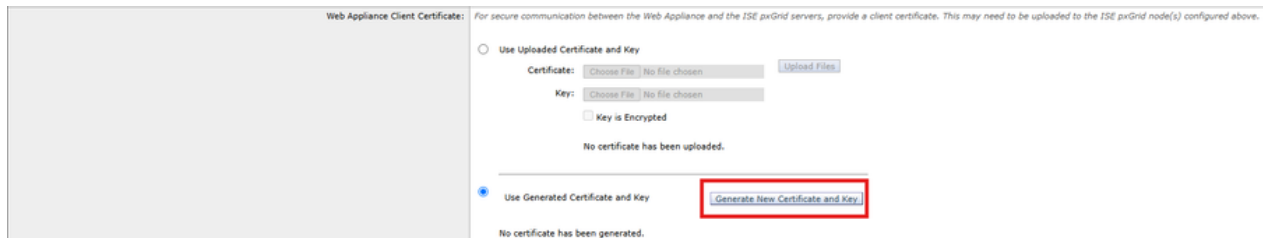
Web Traffic Tap

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.



Web Appliance Client Certificate: For secure communication between the Web Appliance and the ISE pxGrid servers, provide a client certificate. This may need to be uploaded to the ISE pxGrid node(s) configured above.

☐ Use Uploaded Certificate and Key

Certificate: No file chosen

Key: No file chosen

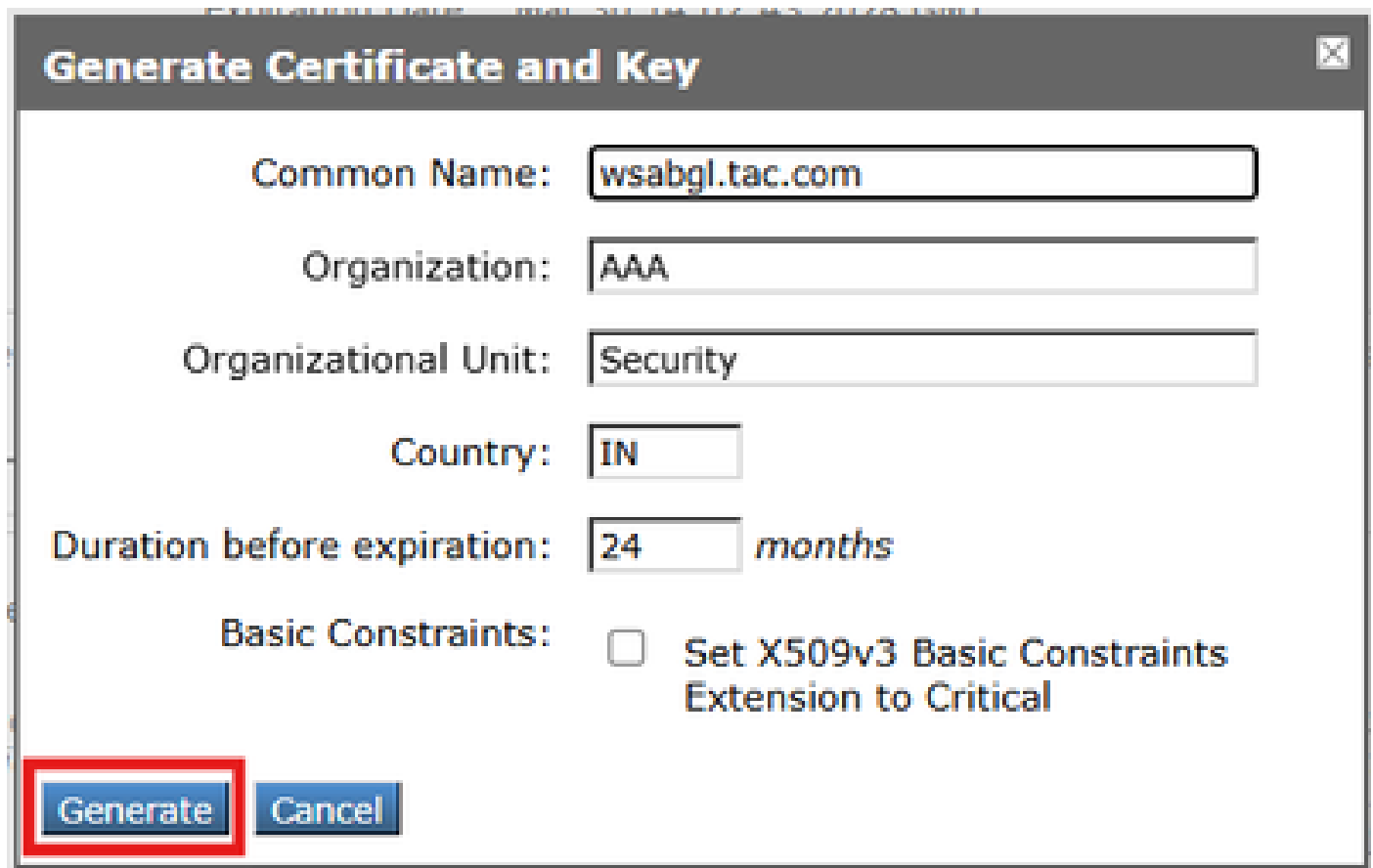
☐ Key is Encrypted

No certificate has been uploaded.

☒ Use Generated Certificate and Key

No certificate has been generated.

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



Generate Certificate and Key

Common Name:

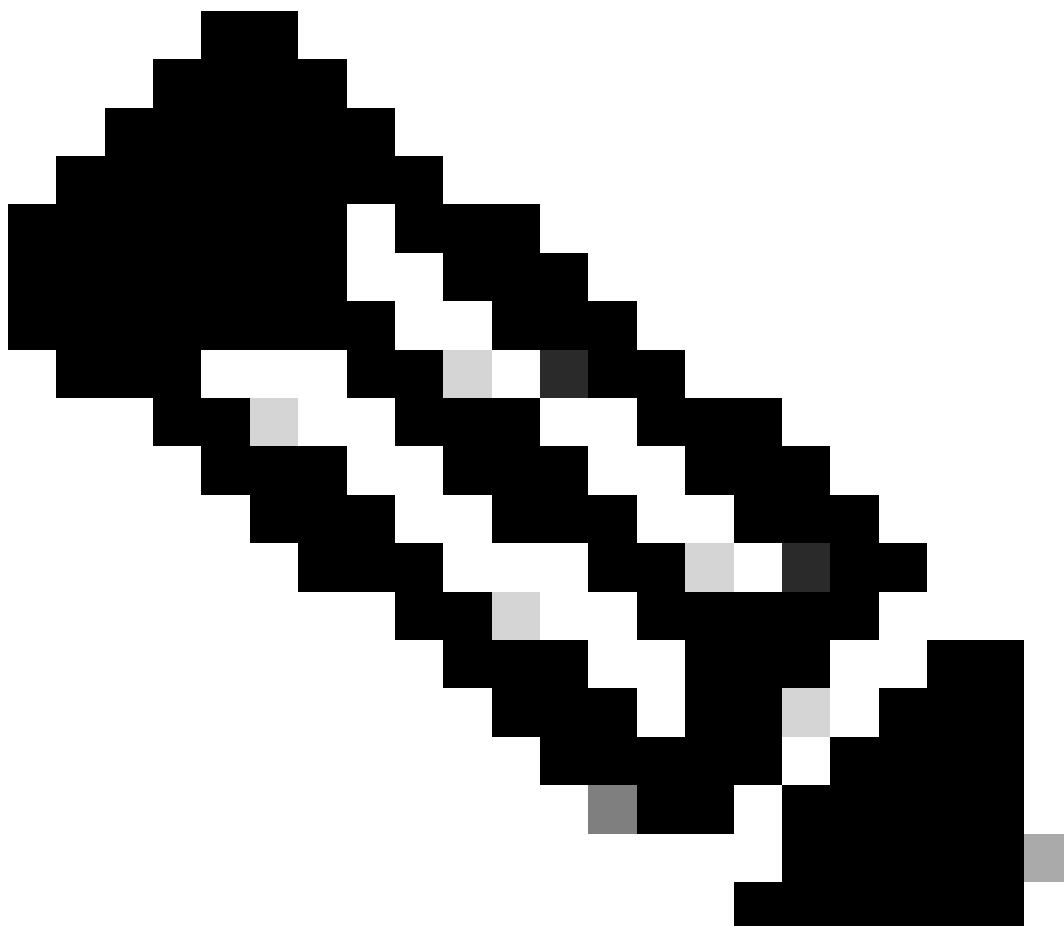
Organization:

Organizational Unit:

Country:

Duration before expiration: months

Basic Constraints: ☐ Set X509v3 Basic Constraints Extension to Critical



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.

Web Appliance Client Certificate: For secure communication between the Web Appliance and the ISE pxGrid servers, provide a client certificate. This may need to be uploaded to the ISE pxGrid node(s) configured above.

☐ Use Uploaded Certificate and Key

Certificate: No file chosen

Key: No file chosen

☐ Key is Encrypted

No certificate has been uploaded.

☒ Use Generated Certificate and Key

Common name: wsibgl.tac.com

Organization: AAA

Organizational Unit: Security

Country: IN

Expiration Date: Mar 19 19:56:43 2027 GMT

Basic Constraints: Not Critical

Download Certificate...

Signed Certificate:

To use a signed certificate, first download a certificate signing request using the link above. Submit the request to a certificate authority, and when you receive the signed certificate, upload it using the field below.

Certificate: No file chosen

11. Fare clic su Sottometti.

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

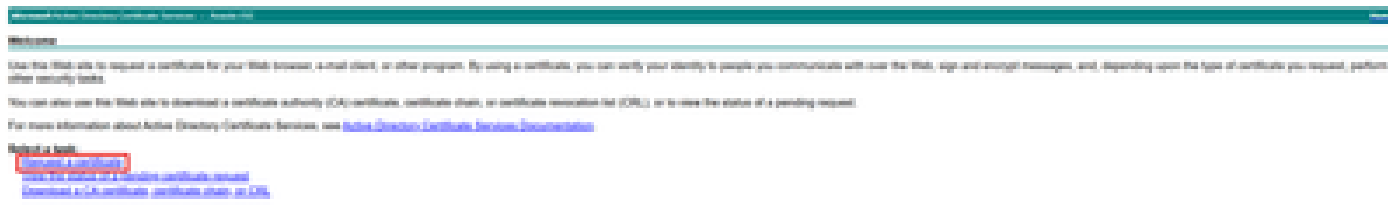


Avviso: Se non si inviano ed eseguono il commit delle modifiche indicate e non si carica direttamente il certificato firmato e non si esegue il commit, è possibile che si verifichino problemi durante l'integrazione.

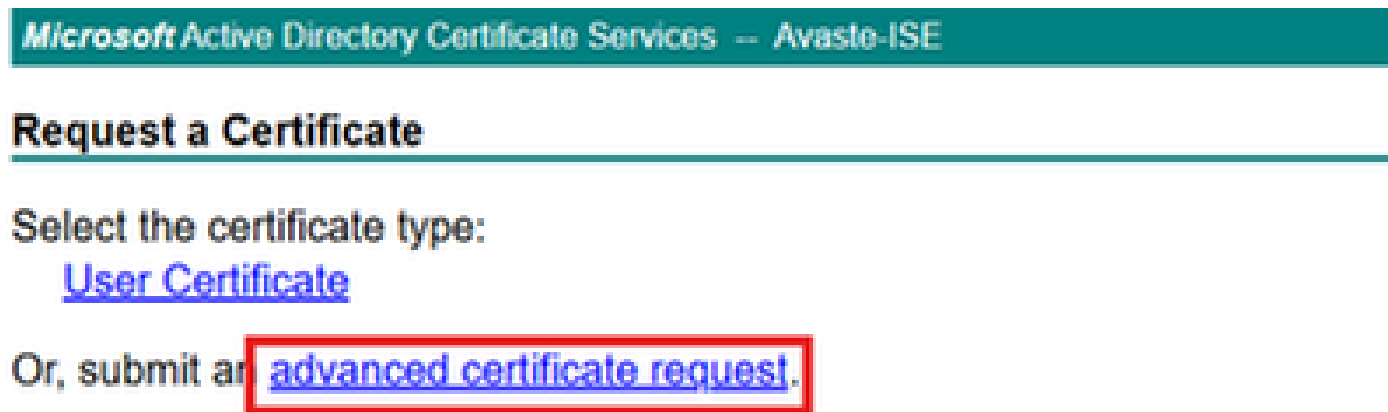
Sezione B: Firmare un CSR client WSA utilizzando una CA esterna

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.

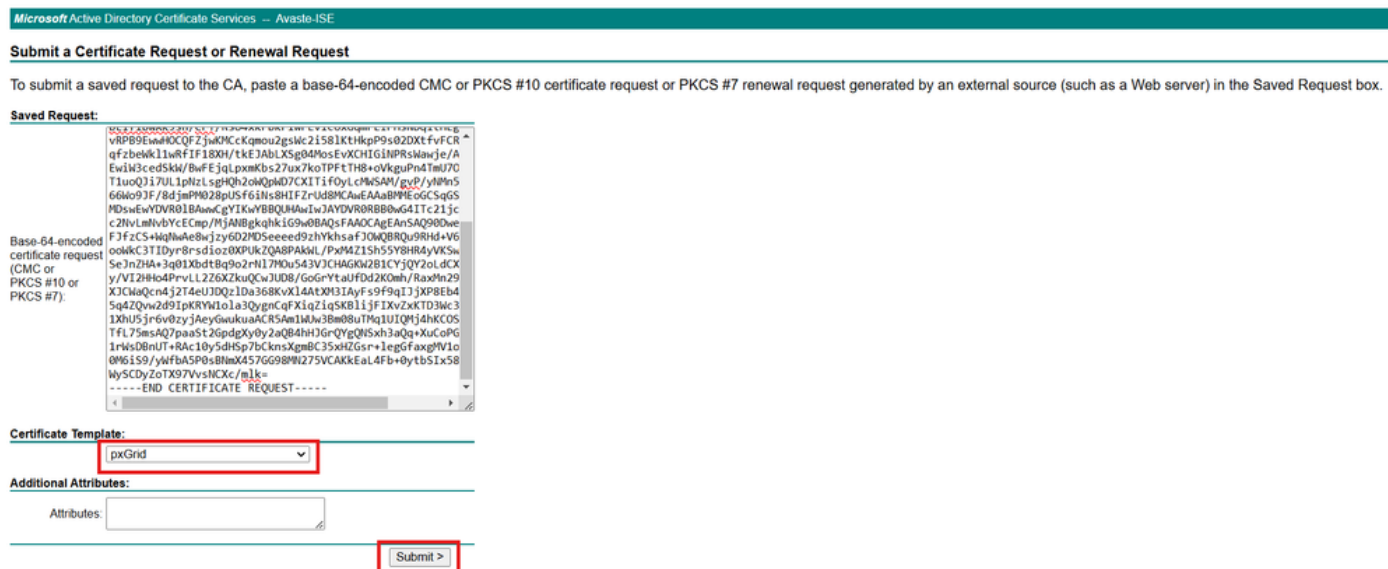


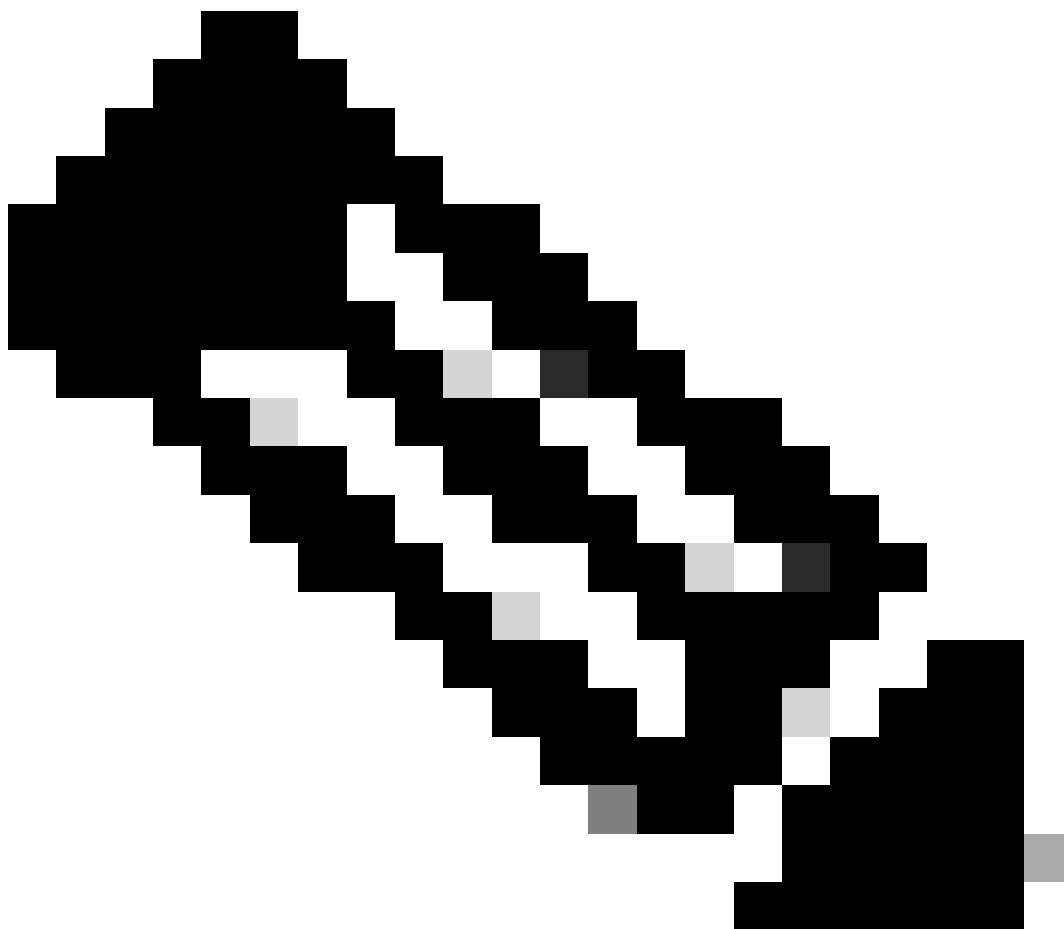
3. Scegliere di sottomettere una richiesta avanzata di certificati.



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

5. Selezionare pxGrids 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.

Certificate Issued

The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

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

☒

Use Generated Certificate and Key

Generate New Certificate and Key

Common name: wsabgl.tac.com

Organization: AAA

Organizational Unit: Security

Country: IN

Expiration Date: Mar 19 14:21:32 2027 GMT

Basic Constraints: Not Critical

[Download Certificate...](#) | [Download Certificate Signing Request...](#)

Signed Certificate:

To use a signed certificate, first download a certificate signing request using the link above. Submit the request to a certificate authority, and when you receive the signed certificate, upload it using the field below.

Certificate:

Choose File

WSA-Client.cer.cer

Upload File

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.

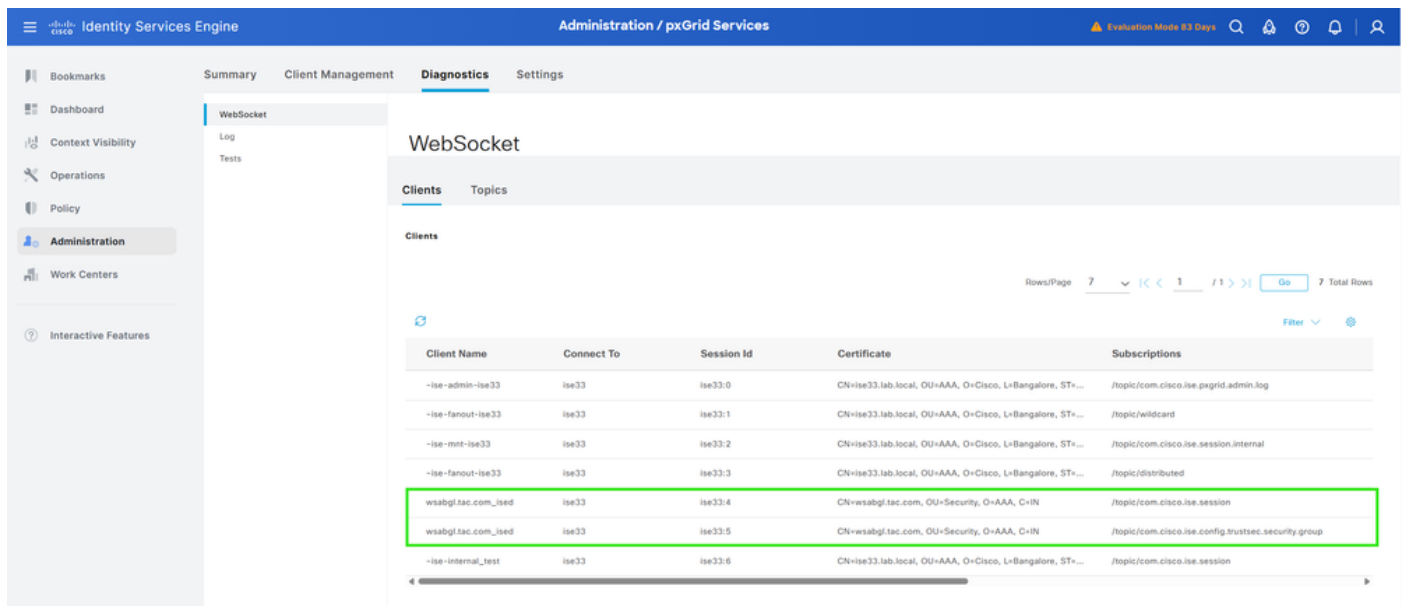
In questo modo il WSA viene generato come client pxgrid con statusEnabled.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar indicates 'Administration / pxGrid Services'. The left sidebar shows the 'Administration' menu. The main content area is titled 'Clients' and includes a sub-section 'pxGrid Clients'. Below this, there is a table with the following columns: Name, Description, Client Groups, and Status. The table contains one entry: 'wsa@tac.com_iseif' with description 'ISEF' and status 'Enabled'. The 'Enabled' status is highlighted with a green box. The table also includes a checkbox for each row and a 'Filter' button.

Name	Description	Client Groups	Status
☐ wsa@tac.com_iseif	ISEF		☒ Enabled

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

Websocket > Client:



Administration / pxGrid Services					
Identity Services Engine					
Evaluation Mode 63 Days					
Bookmarks Summary Client Management Diagnostics Settings					
WebSocket					
Log Tests					
Clients Topics					
Clients					
Rows/Page 7 < < 1 / 1 > > Go 7 Total Rows					
Filter					
Client Name	Connect To	Session Id	Certificate	Subscriptions	
-ise-admin-ise33	ise33	ise33:0	CN=ise33.lab.local, OU=AAA, O=Cisco, L=Bangalore, ST=...	/topic/com.cisco.ise.pxgrid.admin.log	
-ise-fanout-ise33	ise33	ise33:1	CN=ise33.lab.local, OU=AAA, O=Cisco, L=Bangalore, ST=...	/topic/wildcard	
-ise-mnt-ise33	ise33	ise33:2	CN=ise33.lab.local, OU=AAA, O=Cisco, L=Bangalore, ST=...	/topic/com.cisco.ise.session.internal	
-ise-fanout-ise33	ise33	ise33:3	CN=ise33.lab.local, OU=AAA, O=Cisco, L=Bangalore, ST=...	/topic/distributed	
wsabgl.tac.com_ised	ise33	ise33:4	CN=wsabgl.tac.com, OU=Security, O=AAA, C=IN	/topic/com.cisco.ise.session	
wsabgl.tac.com_ised	ise33	ise33:5	CN=wsabgl.tac.com, OU=Security, O=AAA, C=IN	/topic/com.cisco.ise.config.trustsec.security.group	
-ise-internal_test	ise33	ise33:6	CN=ise33.lab.local, OU=AAA, O=Cisco, L=Bangalore, ST=...	/topic/com.cisco.ise.session	

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\u003d
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 (cached

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.

Test Communication with ISE Server

Start Test

Validating ISE Portal certificate ...

Success: Certificate validation successful

Checking connection to ISE PxGrid server...

Failure: Connection to ISE PxGrid server timed out

Test interrupted: Fatal error occurred, see details above.

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).