

Integración de ISE 3.3 con WSA mediante CA externa

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Sección A: Configuración del certificado de Cisco Identity Services Engine 3.3](#)

[Paso 1: Generar un certificado ISEServer pxGrid](#)

[Paso 2: Creación de un certificado pxGrid de servidor ISE mediante una CA externa](#)

[Paso 3: Importar el certificado raíz de la CA en el almacén de confianza de ISE](#)

[Paso 4: Enlace del certificado de ISE a la solicitud de firma de certificado \(CSR\).](#)

[Sección B: Adición de un certificado raíz de CA al almacén de confianza de certificados de WSA](#)

[Integración](#)

[Sección A: Habilite WSA para la integración con ISE y genere CSR para el certificado de cliente WSA.](#)

[Sección B: Firmar una CSR de cliente WSA mediante una CA externa](#)

[Sección C: Enlazar el certificado de cliente WSA a la solicitud de firma de certificado \(CSR\) e integrarlo.](#)

[Verificación](#)

[Resolución de problemas](#)

[Problema](#)

[Solución](#)

[Defectos conocidos](#)

Introducción

Este documento describe los procedimientos para integrar ISE 3.3 con Cisco Secure Web Appliance (WSA) mediante conexiones pxGrid.

Prerequisites

Requirements

Cisco recomienda conocimientos sobre los siguientes temas:

- Identity Services Engine
- Dispositivo Cisco Secure Web Appliance (WSA)
- Platform Exchange Grid (pxGrid)
- Certificados TLS/SSL.
- PKI en Windows Server 2016

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- parche 4 de Identity Services Engine (ISE) versión 3.3
- Cisco Secure Web Appliance versión 15.2.0-116
- Windows Server 2016 como servidor de la Autoridad de certificación externa (CA).

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

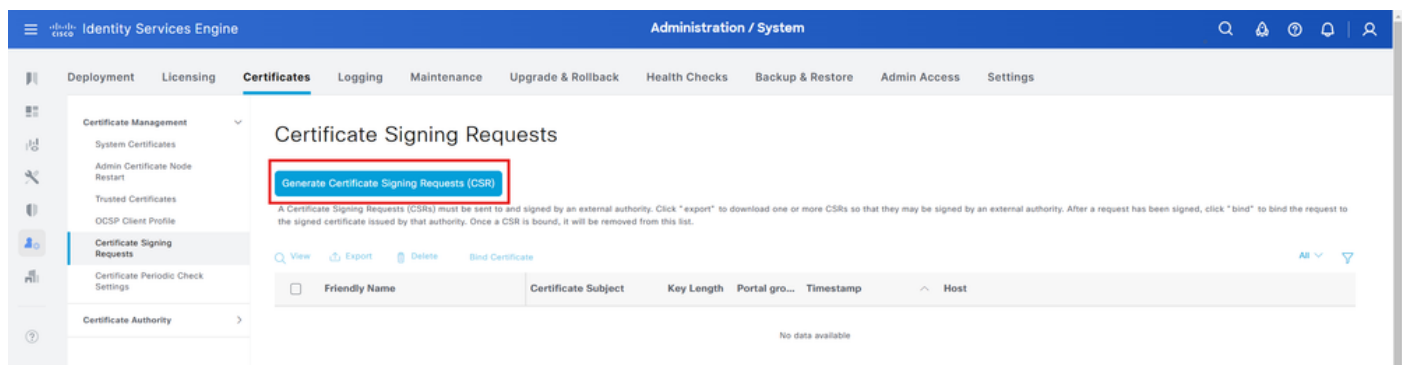
Configurar

Sección A: Configuración del certificado de Cisco Identity Services Engine 3.3

Paso 1: Generar un certificado ISEServer pxGrid

Generar una CSR para un certificado pxGrid de servidor ISE:

1. Inicie sesión en la GUI de Cisco Identity Services Engine (ISE).
2. Navegue hasta Administración > Sistema > Certificados > Administración de certificados > Solicitudes de firma de certificados.
3. Seleccione Generar solicitud de firma de certificado (CSR).



4. Seleccione pxGridin para el campo Certificate(s) is used for (Se utiliza para).
5. Seleccione el nodo ISE para el que se genera el certificado.
6. Llenar otros detalles de certificados según sea necesario.
7. Haga clic en Generar.

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

La plantilla de certificado pxGrid utilizada necesita la autenticación de cliente y la autenticación de servidor en el campo Uso mejorado de clave.

6.Descargue el certificado generado en formato Base-64yGuárdelo como 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](#)

Paso 3: Importar el certificado raíz de la CA en el almacén de confianza de ISE

1.Navegue hasta la página de inicio del Servicio de certificados de Active Directory de MS y seleccione Descargar un certificado de CA, cadena de certificados o 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](#)

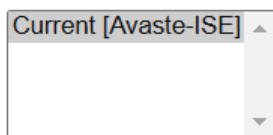
2. Seleccione el formato Base-64y, a continuación, haga clic en Descargar certificado CA.

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](#)

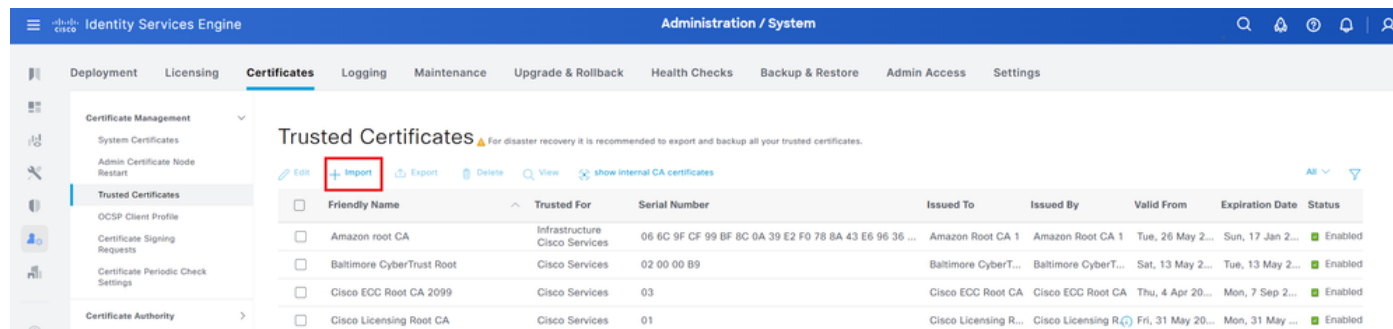
[Download latest base CRL](#)

[Download latest delta CRL](#)

3. Guarde el certificado como CA_Root.cer.

4. Inicie sesión en la GUI de Cisco Identity Services Engine (ISE).

5. Seleccione Administración > Sistema > Certificados > Administración de certificados > Certificados de confianza.



The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System interface. The left sidebar contains a navigation menu with 'Certificates' selected. The main content area displays 'Trusted Certificates' with a table of existing certificates. The 'Import' button is highlighted with a red box.

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. Seleccione Importar > Archivo de certificado elImporte el certificado raíz.

7. Asegúrese de que la casilla de verificación Confiar en la autenticación de ISE esté activada.

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. Haga clic en Enviar.

Paso 4: Enlace del certificado de ISE a la solicitud de firma de certificado (CSR).

1. Inicie sesión en la GUI de Cisco Identity Services Engine (ISE).

2. Seleccione Administración > Sistema > Certificados > Administración de certificados > Solicitudes de firma de certificado.

3. Seleccione el CSR generado en la sección anterior y, a continuación, haga clic en Enlazar certificado.

Identity Services Engine Administration / System Evaluation Mode 83 Days

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.

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. En el formulario de certificado firmado de CA de enlace, seleccione el certificado ISE_pxGrid.cer generado anteriormente.

5. Asigne un nombre descriptivo al certificado y, a continuación, haga clic en Enviar.

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

- Haga clic en Sí si el sistema solicita la sustitución del certificado.
- Seleccione Administración > Sistema > Certificados > Certificados del sistema.
- Puede ver el certificado pxGrid creado firmado por la CA externa en la lista.

System Certificates For disaster recovery it is recommended to export certificate and private key pairs of all 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 - ise33lab0005	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

Sección B: Adición de un certificado raíz de CA al almacén de confianza de certificados de WSA

Agregar certificado raíz de CA al almacén de confianza de WSA:

- Inicie sesión en la GUI del dispositivo de seguridad web (WSA).
- Navegue hasta Red > Administración de certificados > Administrar certificados raíz de confianza.

Network

System

Interfaces

Transparent Redirection

Routes

DNS

High Availability

Internal SMTP Relay

Upstream Proxy

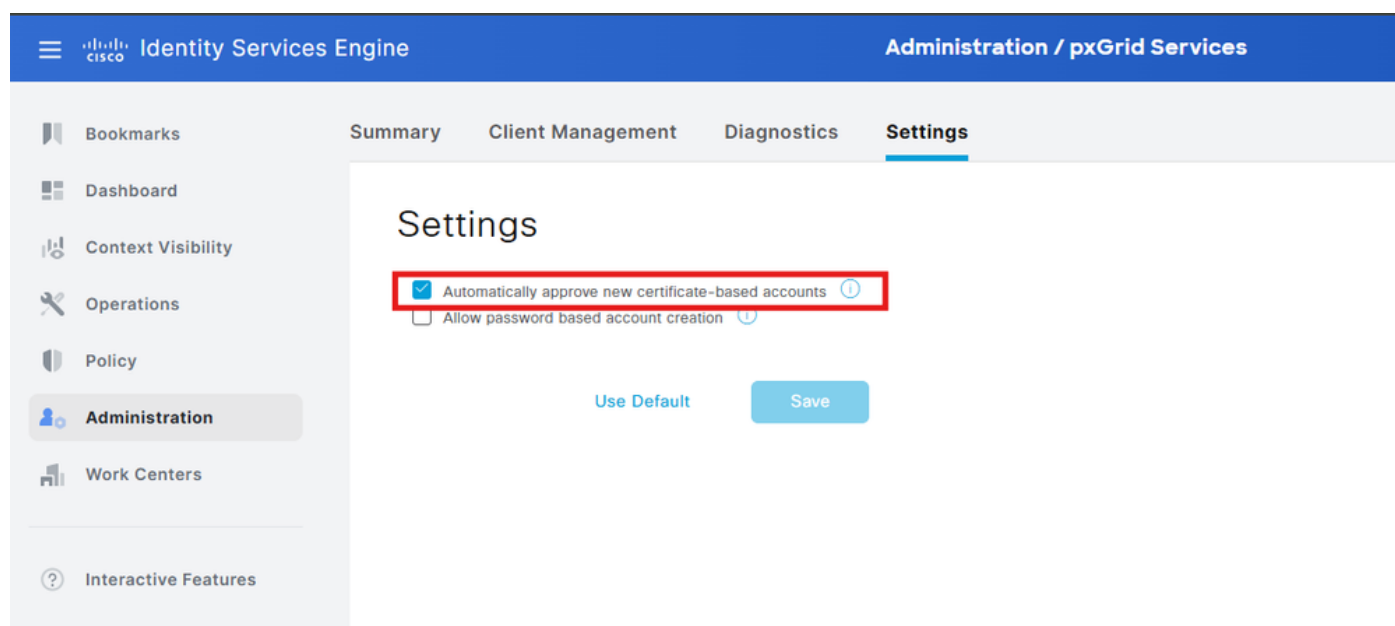
External DLP Servers

Web Traffic Tap

Certificate Management

Cloud Services Settings

Apruebe automáticamente las nuevas cuentas basadas en certificados para que la solicitud del cliente se apruebe automáticamente y guarde.



Sección A: Habilite WSA para la integración con ISE y genere CSR para el certificado de cliente WSA.

1. Inicie sesión en la GUI del dispositivo de seguridad web (WSA).

2. Navegue hasta Red > Servicios de identificación > Motor de servicios de identificación.

Network

System

Interfaces

Transparent Redirection

Routes

DNS

High Availability

Internal SMTP Relay

Upstream Proxy

External DLP Servers

Web Traffic Tap

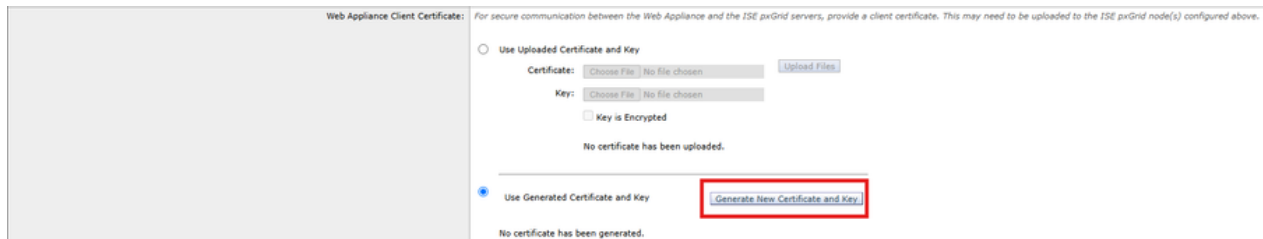
Certificate Management

Cloud Services Settings

Umbrella Settings

Solo puede haber dos nodos pxGrid por implementación de ISE. Esto sirve como una configuración pxGrid Active-Standby; solo puede haber un nodo de ISE+pxGrid activo a la vez. En una configuración pxGrid Active-Standby, toda la información pasa a través de PPAN, donde el segundo nodo de ISE+pxGrid permanece inactivo.

8. Desplácese a la sección Web Appliance Client Certificate y haga clic en Generate New Certificate and Key.



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

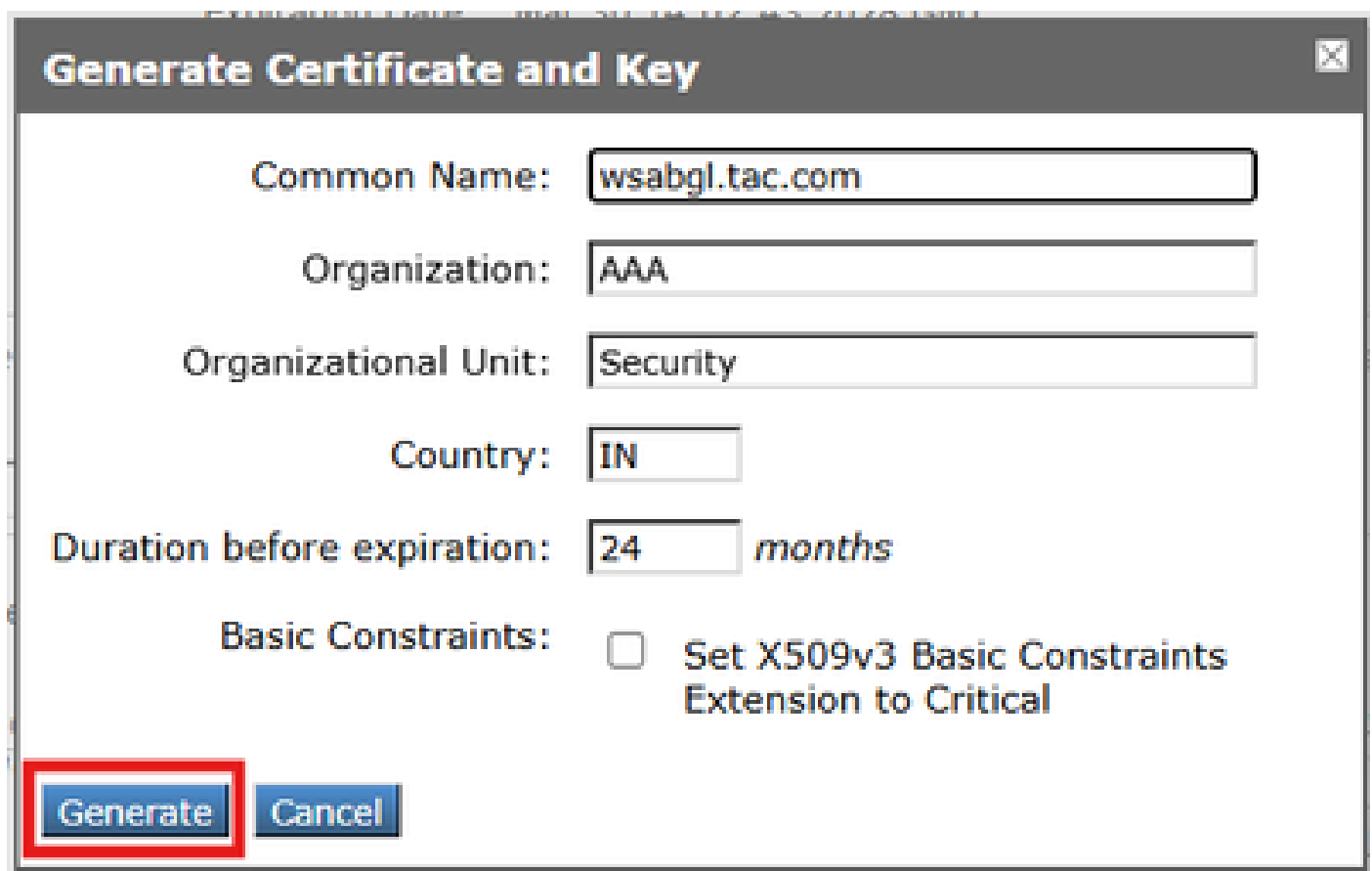
☐ Key is Encrypted

No certificate has been uploaded.

☒ Use Generated Certificate and Key

No certificate has been generated.

9. Rellene los detalles del certificado según sea necesario y haga clic en Generar.



Generate Certificate and Key

Common Name:

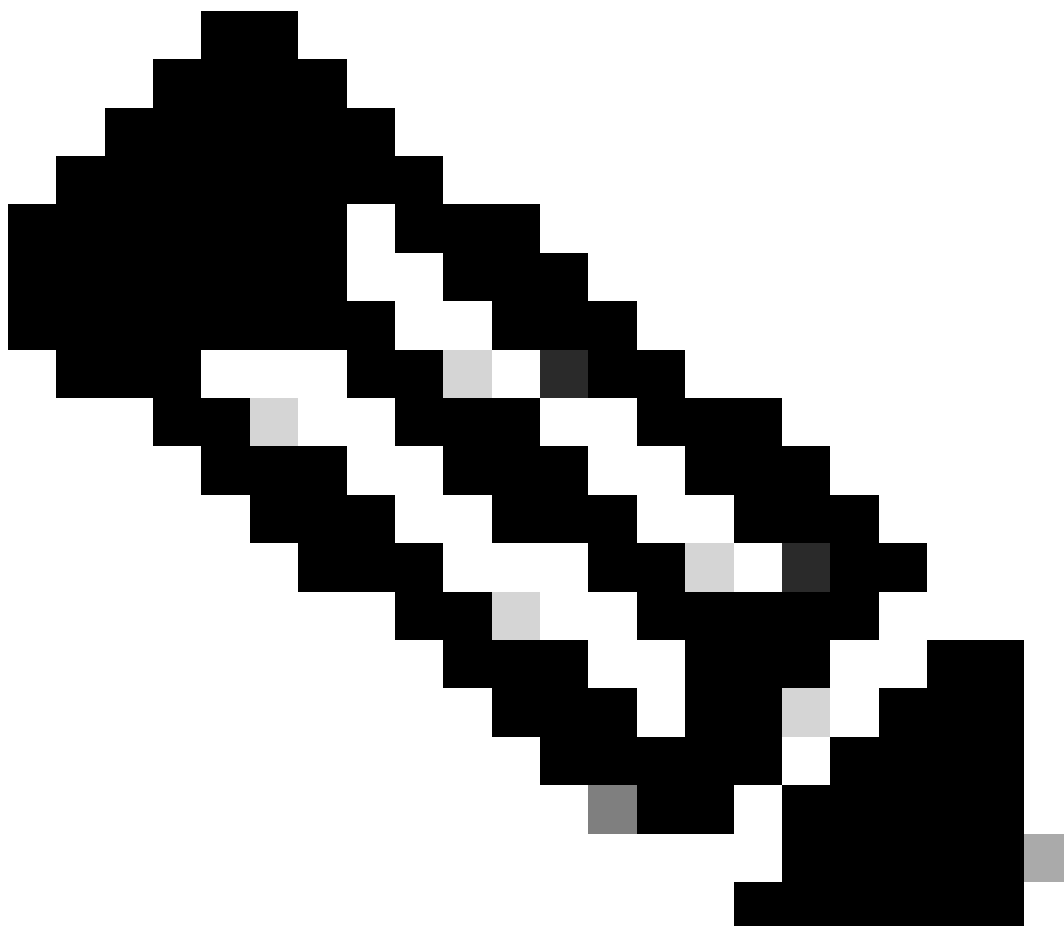
Organization:

Organizational Unit:

Country:

Duration before expiration: months

Basic Constraints: ☐ Set X509v3 Basic Constraints Extension to Critical



Nota: La duración del certificado debe ser un número entero entre 24 y 60 meses y el país debe ser un código de país ISO de dos caracteres (sólo letras mayúsculas).

10. Haga clic en Descargar solicitud de firma de certificado.

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. Haga clic en Enviar.

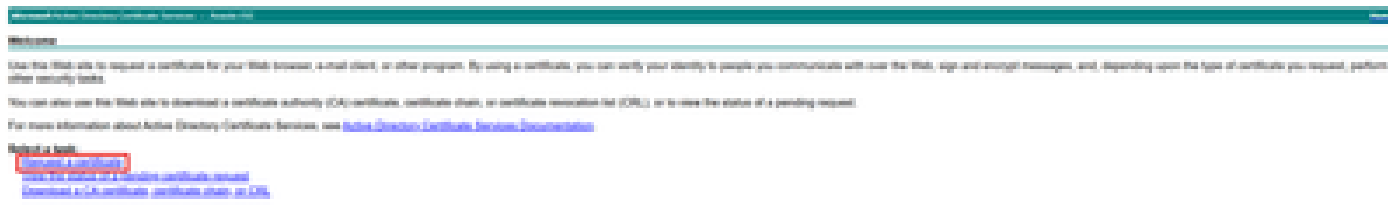
12. Haga clic en Registrar Cambios para aplicar los cambios.



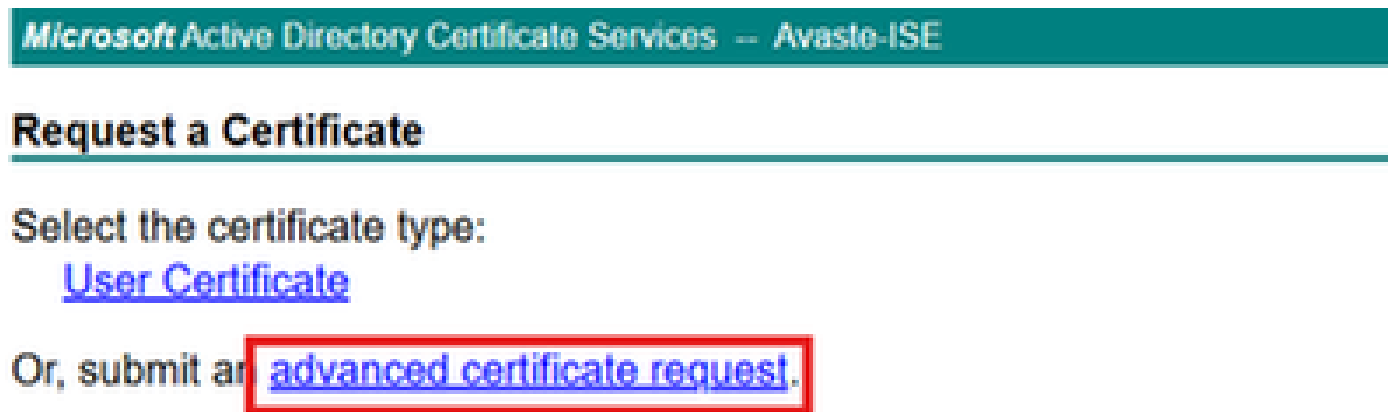
Advertencia: Si no envía y confirma los cambios mencionados y carga directamente el certificado firmado y realiza la confirmación, puede enfrentarse a problemas durante la integración.

Sección B: Firmar una CSR de cliente WSA mediante una CA externa

1. Navegue hasta Servicio de certificados de Active Directory de MS, <https://server/certsrv/>, donde el servidor es IP o DNS de su servidor MS.
2. Haga clic en Solicitar un certificado.

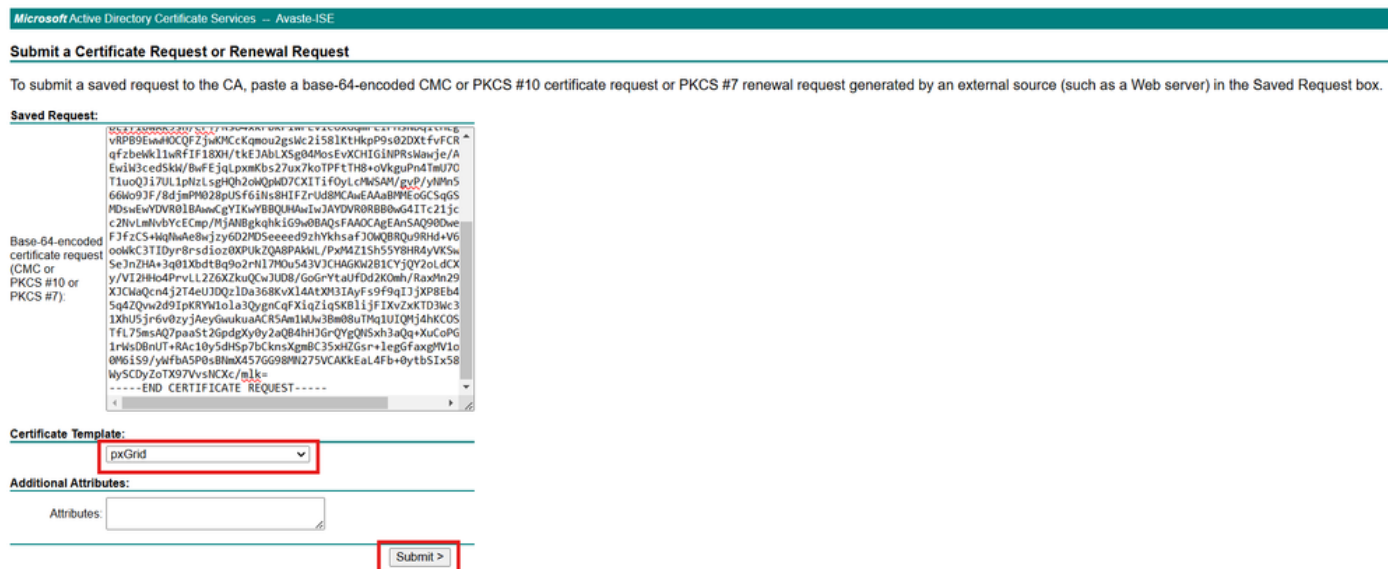


3. Seleccione esta opción para ejecutar una solicitud de certificado avanzada.



4. Copie el contenido del CSR generado en la sección anterior en el campo Solicitud guardada.

5. Seleccione pxGrid como la plantilla de certificado y, a continuación, haga clic en Enviar.





Nota: Nota: La plantilla de certificado pxGrid utilizada necesita la autenticación de cliente y la autenticación de servidor en el campo Uso mejorado de clave.

6.Descargue el certificado generado en formato Base-64yGuárdelo como WSA-Client.cer.

Certificate Issued

The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

Sección C: Enlazar el certificado de cliente WSA a la solicitud de firma de certificado (CSR) e integrarlo.

1. Navegue hasta la GUI del dispositivo de seguridad web (WSA).
2. Navegue hasta Red > Servicios de identificación > Motor de servicios de identificación.
3. Haga clic en Editar configuración.
4. Vaya a la sección Certificado de cliente de dispositivo web.
5. En la sección certificado firmado, cargue el certificado firmado 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. Haga clic en Submit.

7. Haga clic en Commit Changes para aplicar los cambios.

8. Haga clic en Editar configuración.

9. Desplácese hasta Probar comunicación con nodos ISE y haga clic en Iniciar prueba, que puede resultar de la siguiente manera:

Comunicación de prueba con nodos ISE

Comunicación de prueba con nodos 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.
```

Verificación

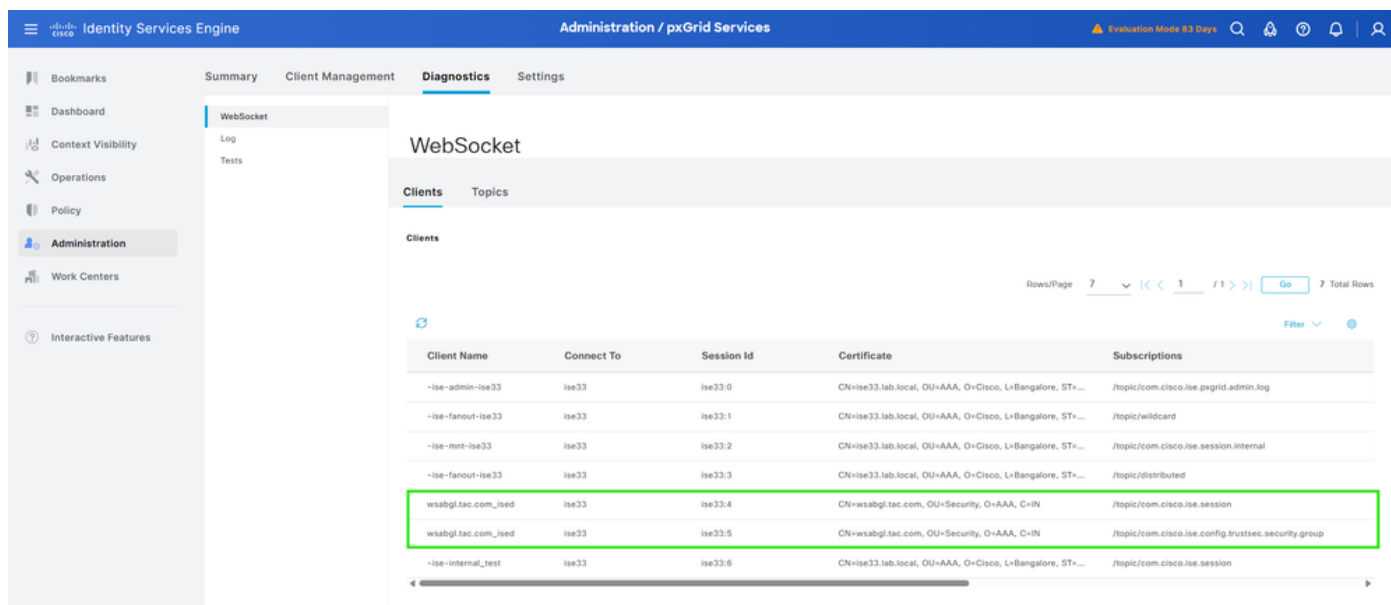
En Cisco ISE, vaya a Administración > Servicios pxGrid > Administración de clientes > Clientes.

Esto genera el WSA como un cliente pxgrid con el status Enabled.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar indicates 'Administration / pxGrid Services'. The left sidebar shows the 'Administration' menu. The main content area is titled 'Clients' and displays a table of 'pxGrid Clients'. The table has columns for Name, Description, Client Groups, and Status. A single client is listed: 'wsabgltac.com_iseid' with a description of 'ISEID' and a status of 'Enabled'. The 'Enabled' status is highlighted with a green box. The table also includes a checkbox for each client and a 'Filter' button.

Name	Description	Client Groups	Status
☐ wsabgltac.com_iseid	ISEID		☒ Enabled

Para verificar la suscripción a los temas en Cisco ISE, vaya a Administración > Servicios pxGrid > Diagnósticos > Websocket > Clientes:



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 Pxgrid-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. subscri
TRACE [WsIseClientConnection-804][[]] cpm.pxgrid.ws.client.WsEndpoint -:::-- Send. session=[id=34eae1
```

"wsabgl.lab.local_ised

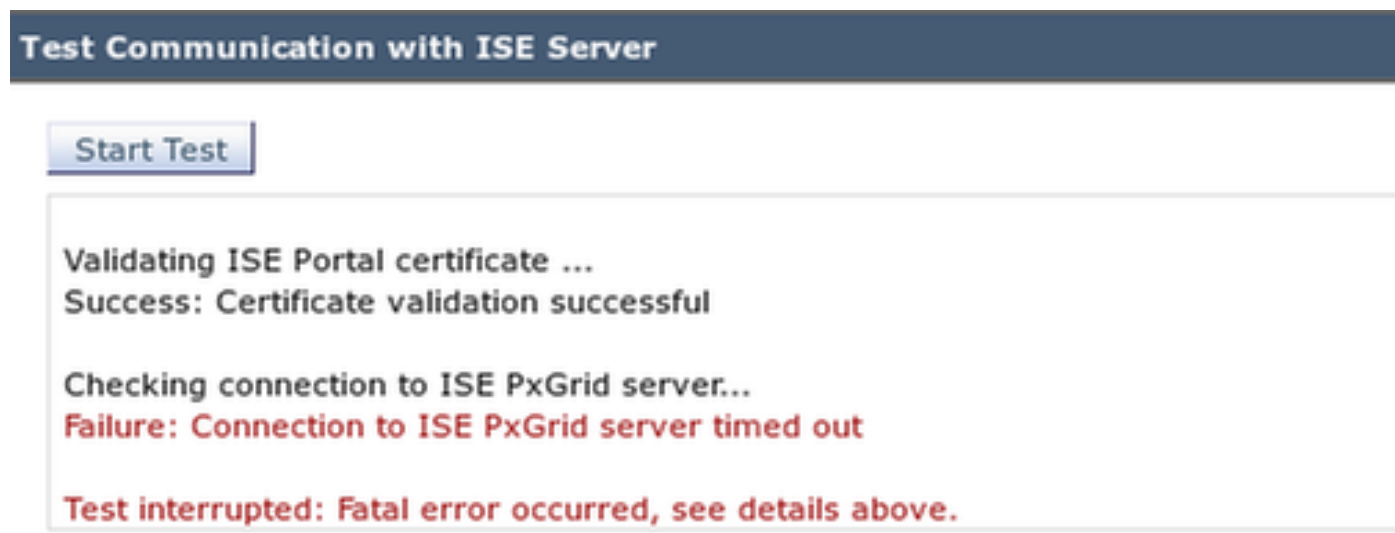
```
", "server": "wss://ise33.lab.local:8910/pxgrid/ise/pubsub", "message": "Pubsub subscribe. subscription\u003d
TRACE [Thread-3][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::-- Received frame=[command=SE
TRACE [Thread-3][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::-- Authorized 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 (cache
```

Resolución de problemas

Problema

Problema de CA desconocido. En WSA, la prueba de conexión ISE falla con un error. Falla: Se ha agotado el tiempo de espera de la conexión al servidor PxGrid de ISE.



Cisco ISE Pxgrid-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 razón de la falla se puede ver con las capturas de paquetes,

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

Solución

1. Asegúrese de que el certificado firmado por el dispositivo web esté enlazado correctamente en el WSA y de que se hayan confirmado los cambios.
2. Asegúrese de que el emisor o el certificado de CA raíz del certificado de cliente WSA forme parte del almacén de confianza en Cisco ISE.

Defectos conocidos

ID de falla de funcionamiento de Cisco	Descripción
ID de bug de Cisco 23986	La solicitud API getUserGroups de Pxgrid devuelve una respuesta vacía.
ID de bug de Cisco 77321	WSA recibe SID en lugar de grupos de AD de ISE.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).