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

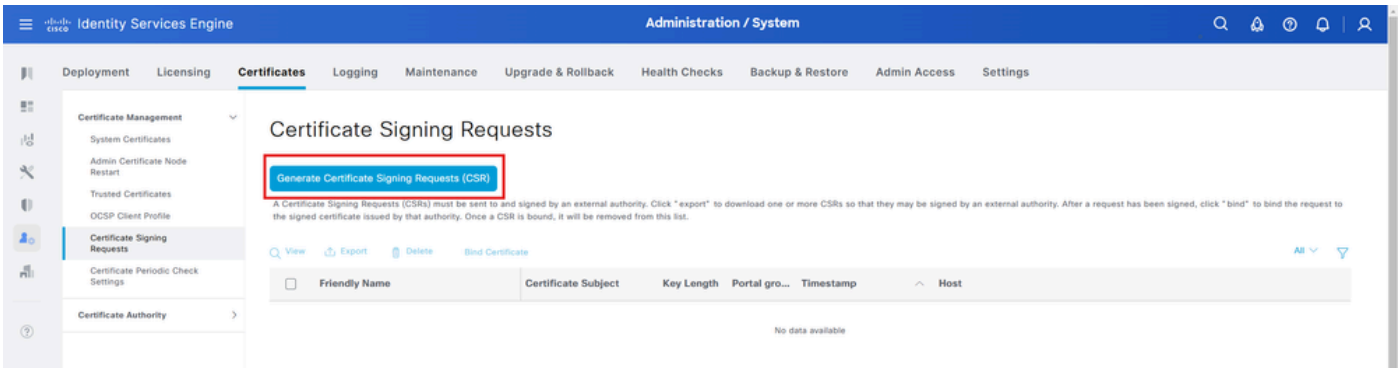
Paso 1: Generar un certificado ISEServer pxGrid

Generar una CSR para un certificado pxGrid de servidor ISE:

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

2.Navegue hastaAdministración > 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

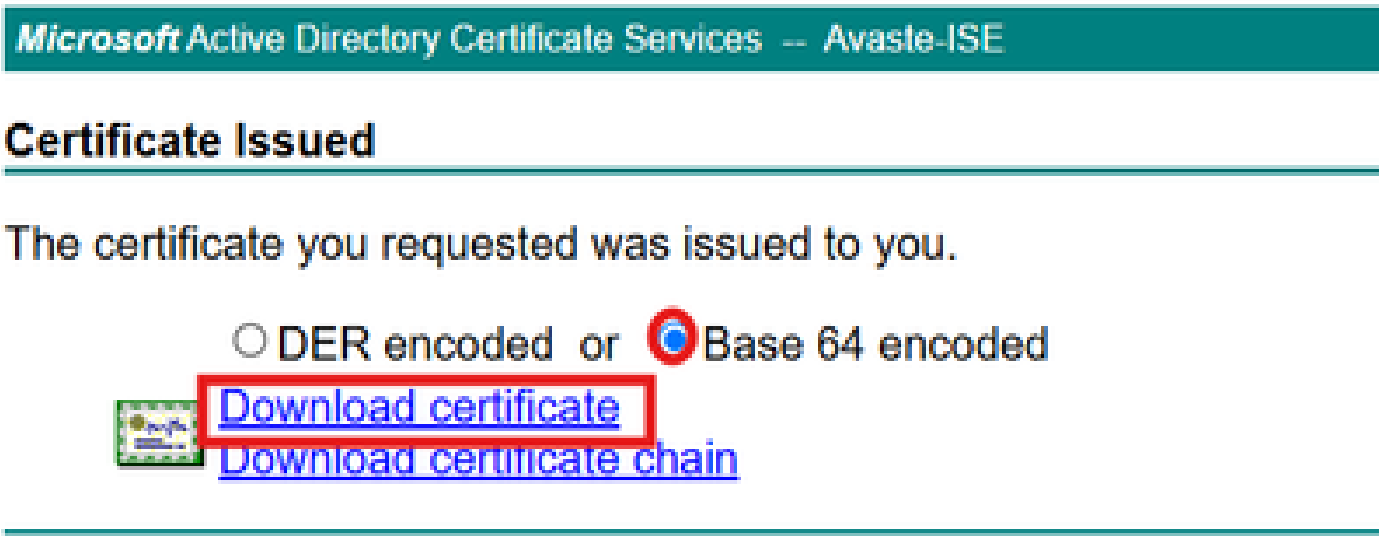
* Key Length: 4096

* Digest to Sign With: SHA-384

Certificate Policies

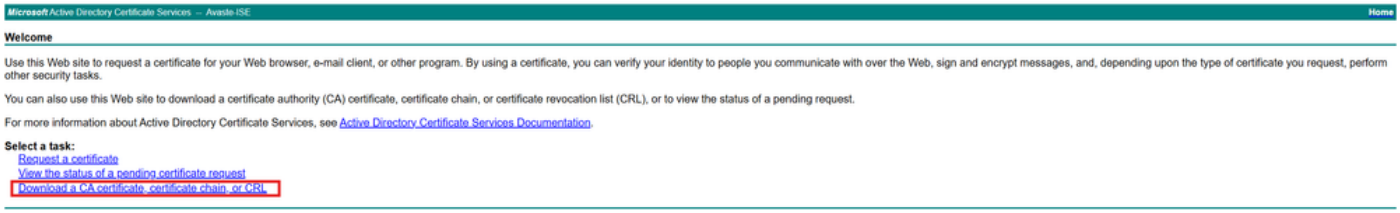
La plantilla de certificado pxGrid utilizada necesita la autenticación de cliente y la autenticación de servidor en el campo Uso mejorado de clave.

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

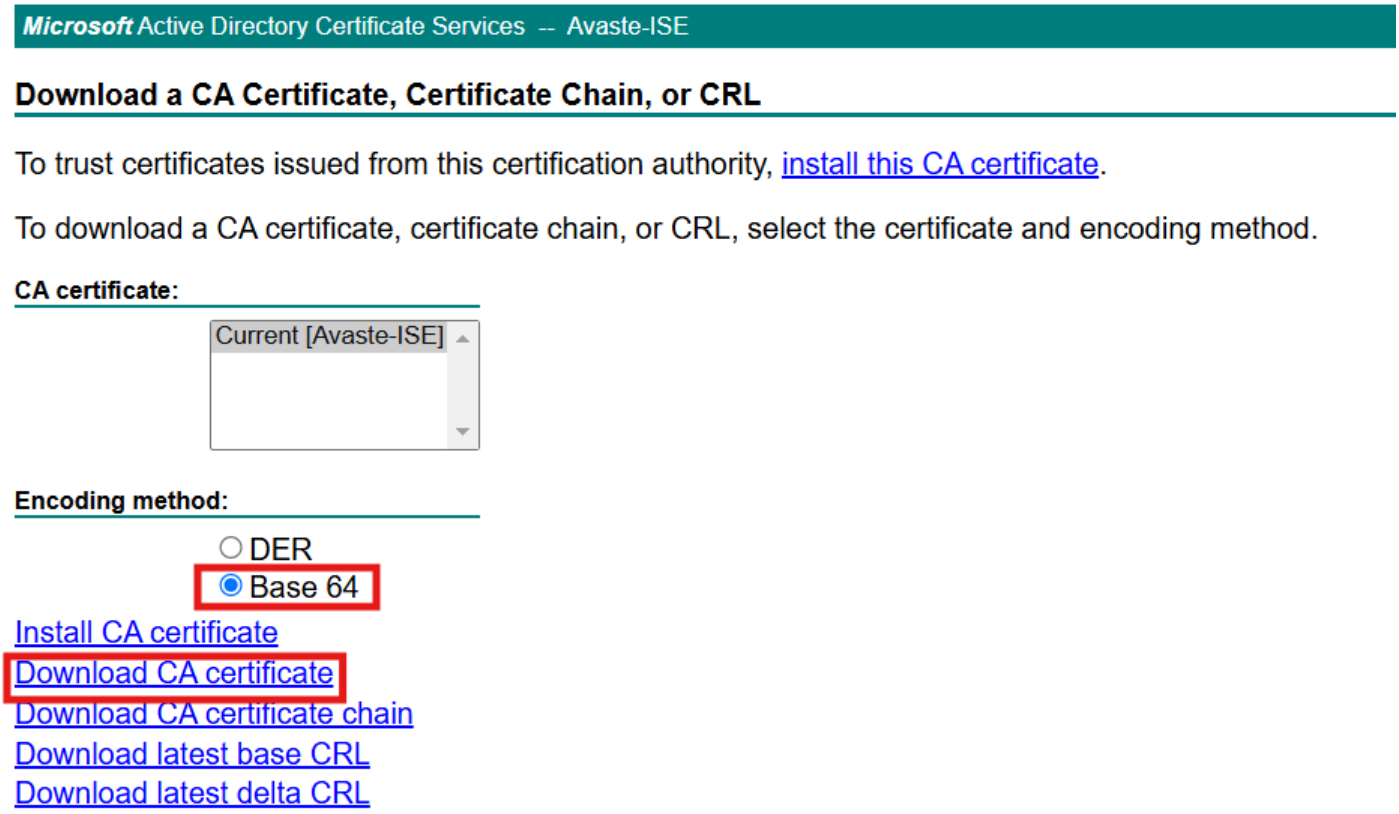


Paso 3: Importar el certificado raíz de la CA en el almacén de confianza de ISE

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.



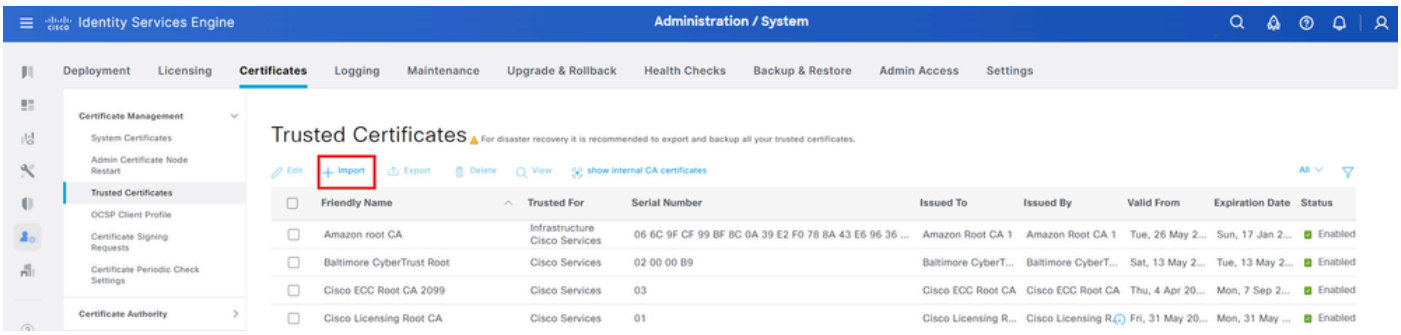
2. Seleccione el formato Base-64y, a continuación, haga clic en Descargar certificado CA.



3.Guarde el certificado como CA_Root.cer.

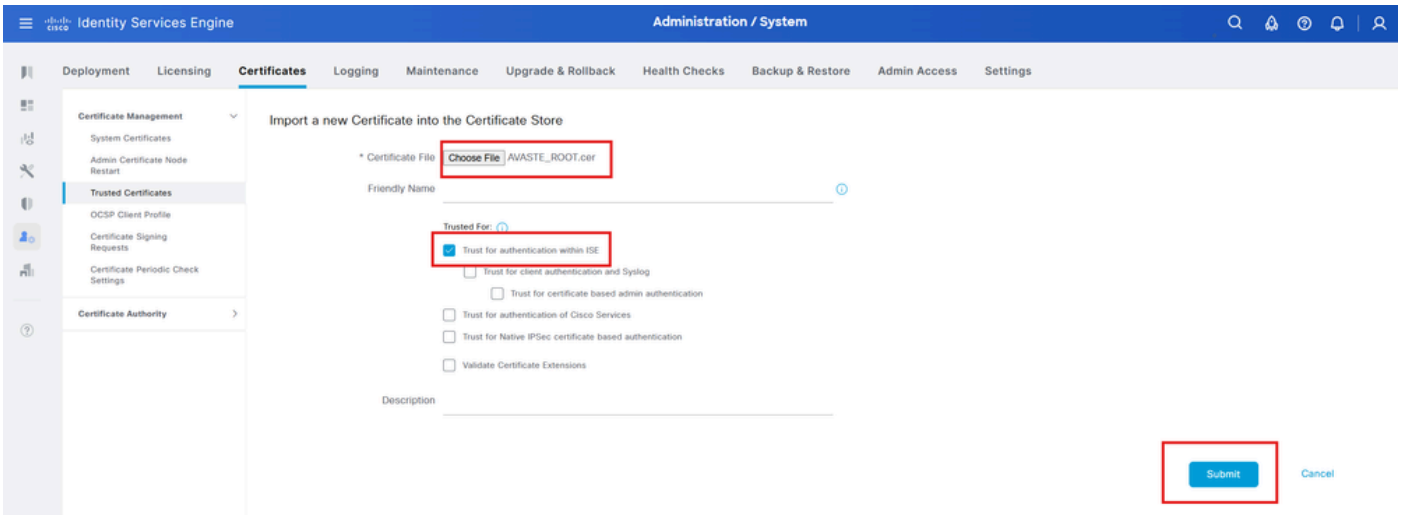
4.Inicie sesión en la GUI de Cisco Identity Services Engine (ISE).

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



6. Seleccione Importar > Archivo de certificado eImporte el certificado raíz.

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



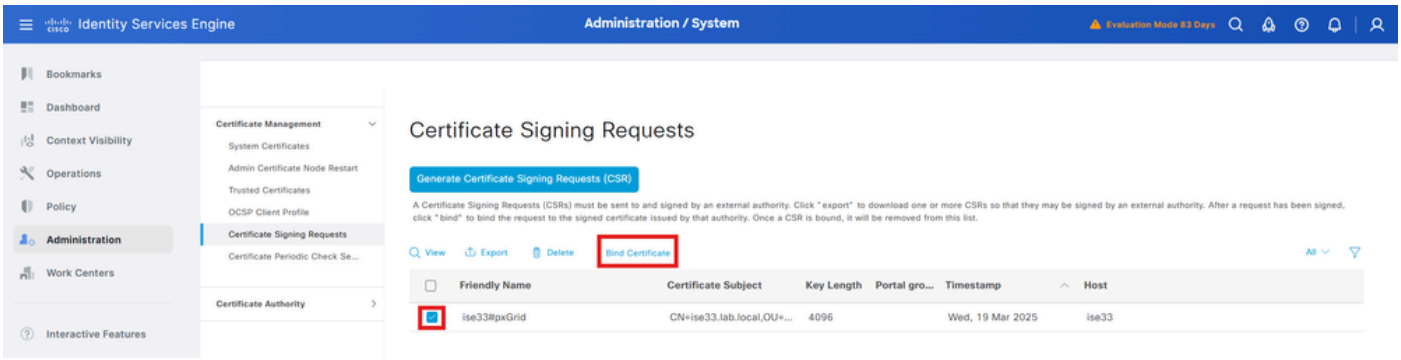
8. Haga clic en Enviar.

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).

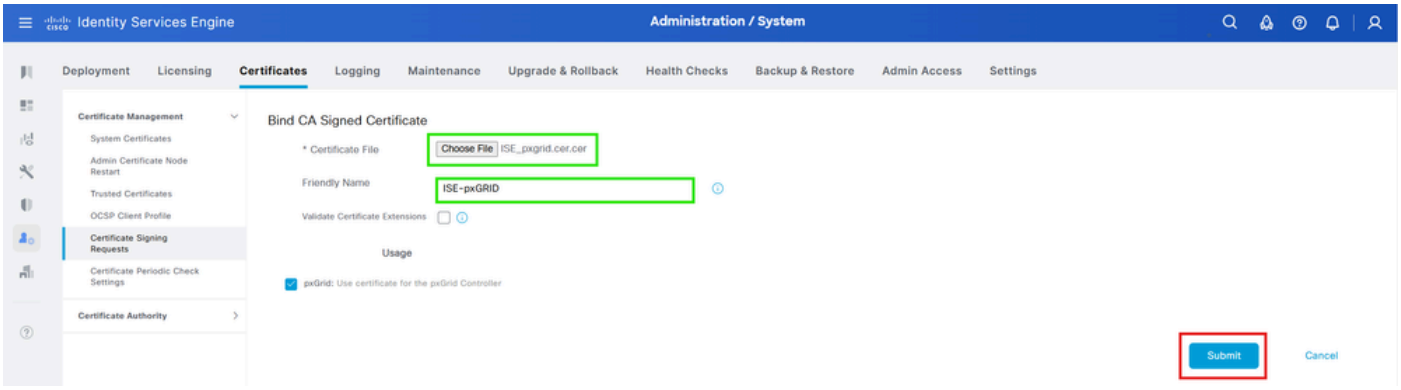
2. Seleccione Administración > Sistema > Certificados > Administración de certificados > Solicitudes de firma de certificado.

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



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

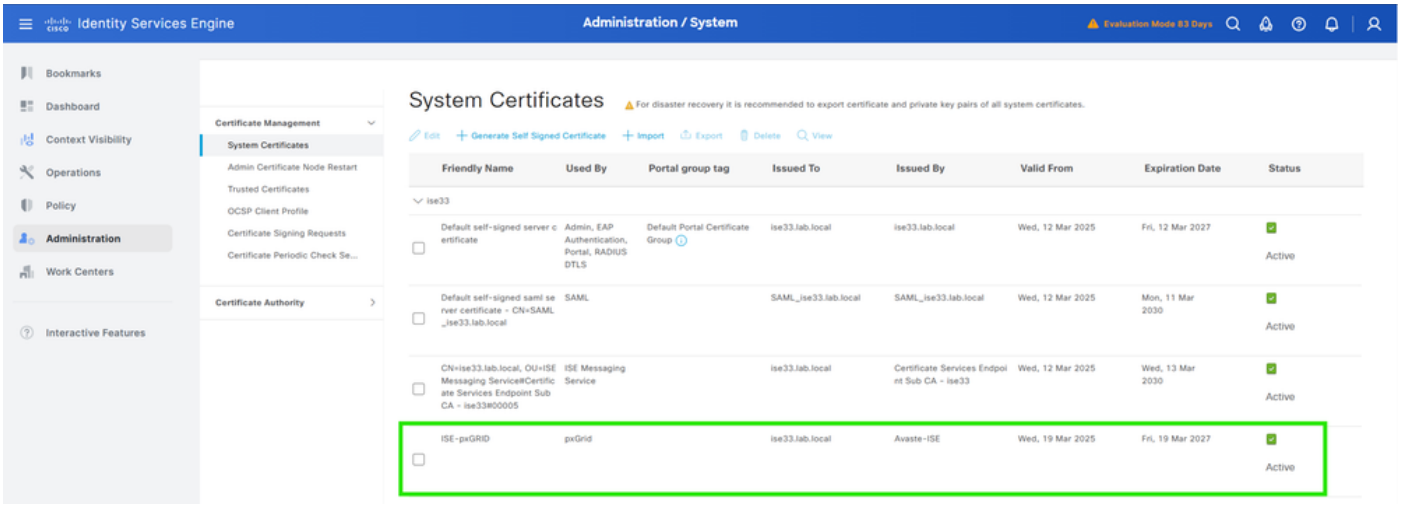
5. Asigne un nombre descriptivo al certificado y, a continuación, haga clic en Enviar.



7. Haga clic en Sí si el sistema solicita la sustitución del certificado.

8. Seleccione Administración > Sistema > Certificados > Certificados del sistema.

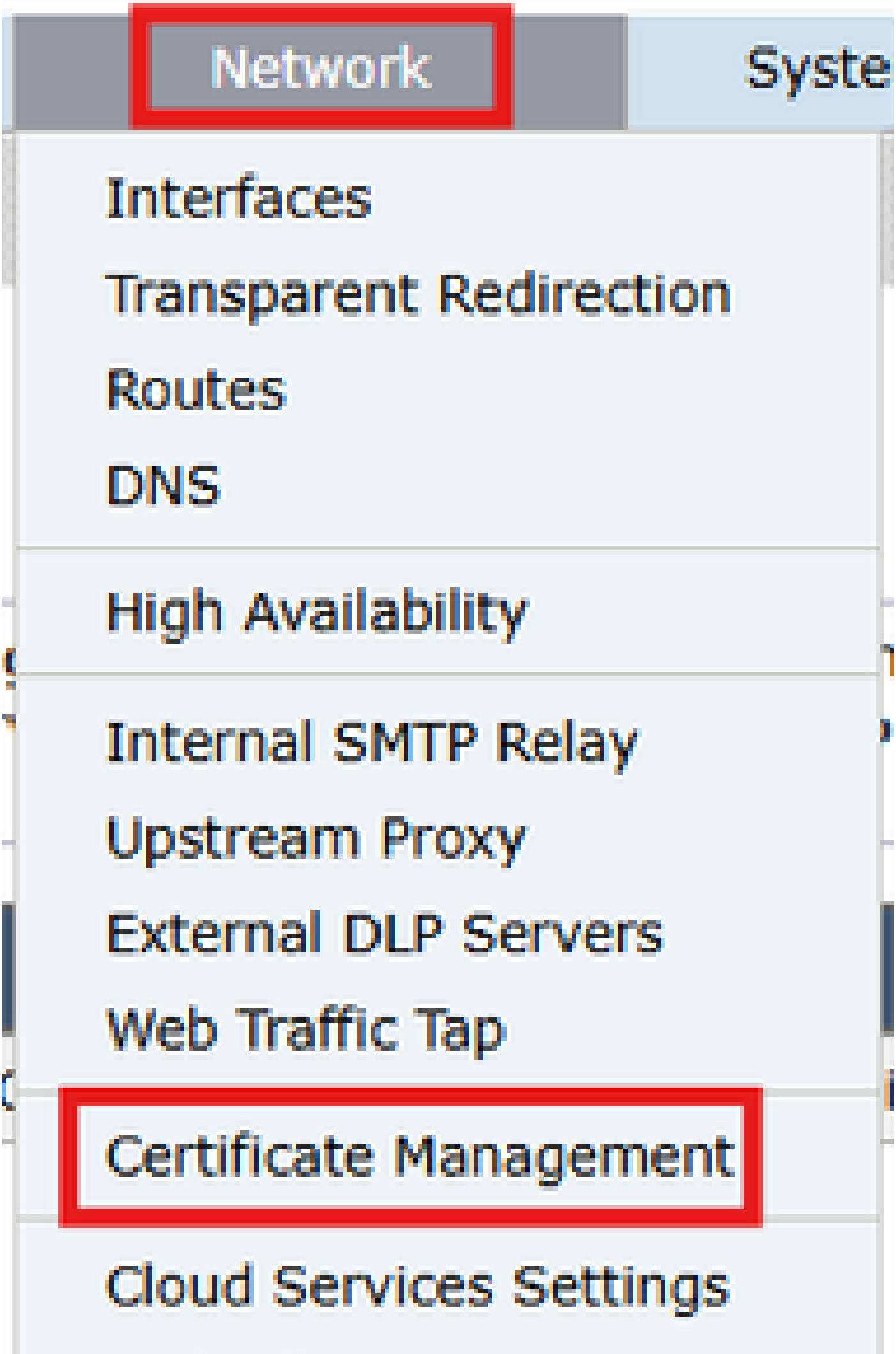
9. Puede ver el certificado pxGrid creado firmado por la CA externa en la lista.



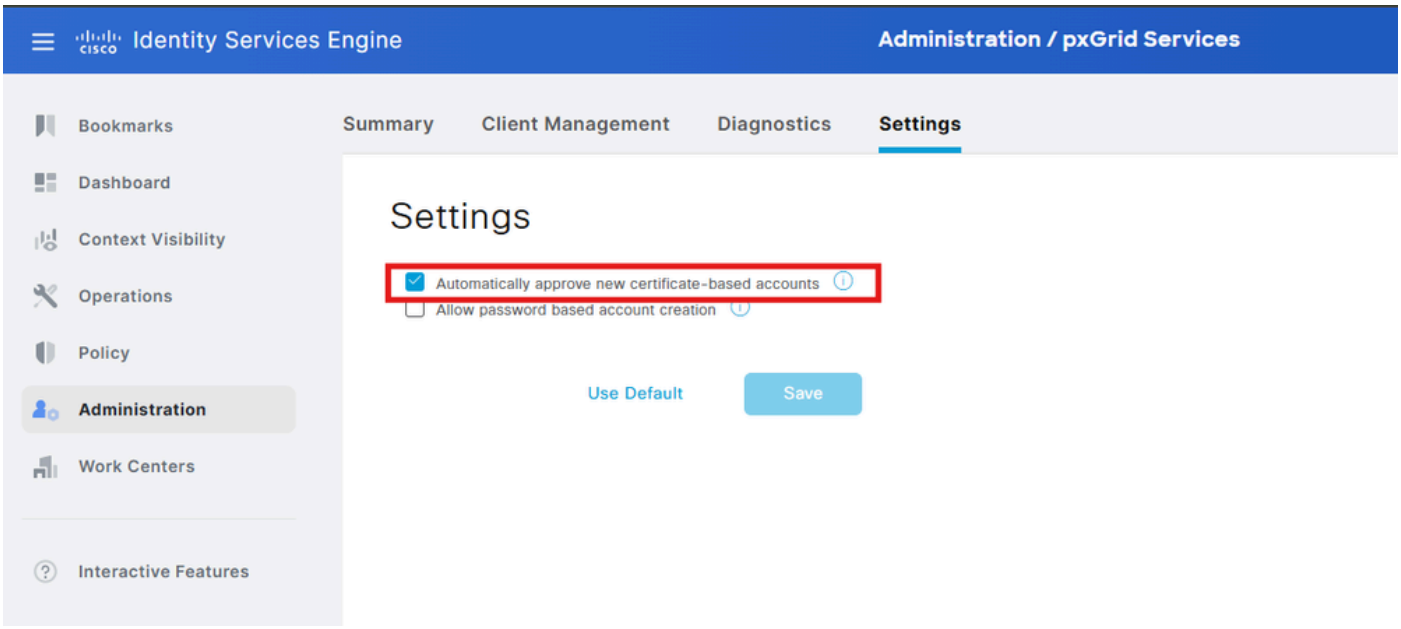
Sección B: Adición de un certificado raíz de CA al almacén de confianza de certificados de WSA

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

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


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

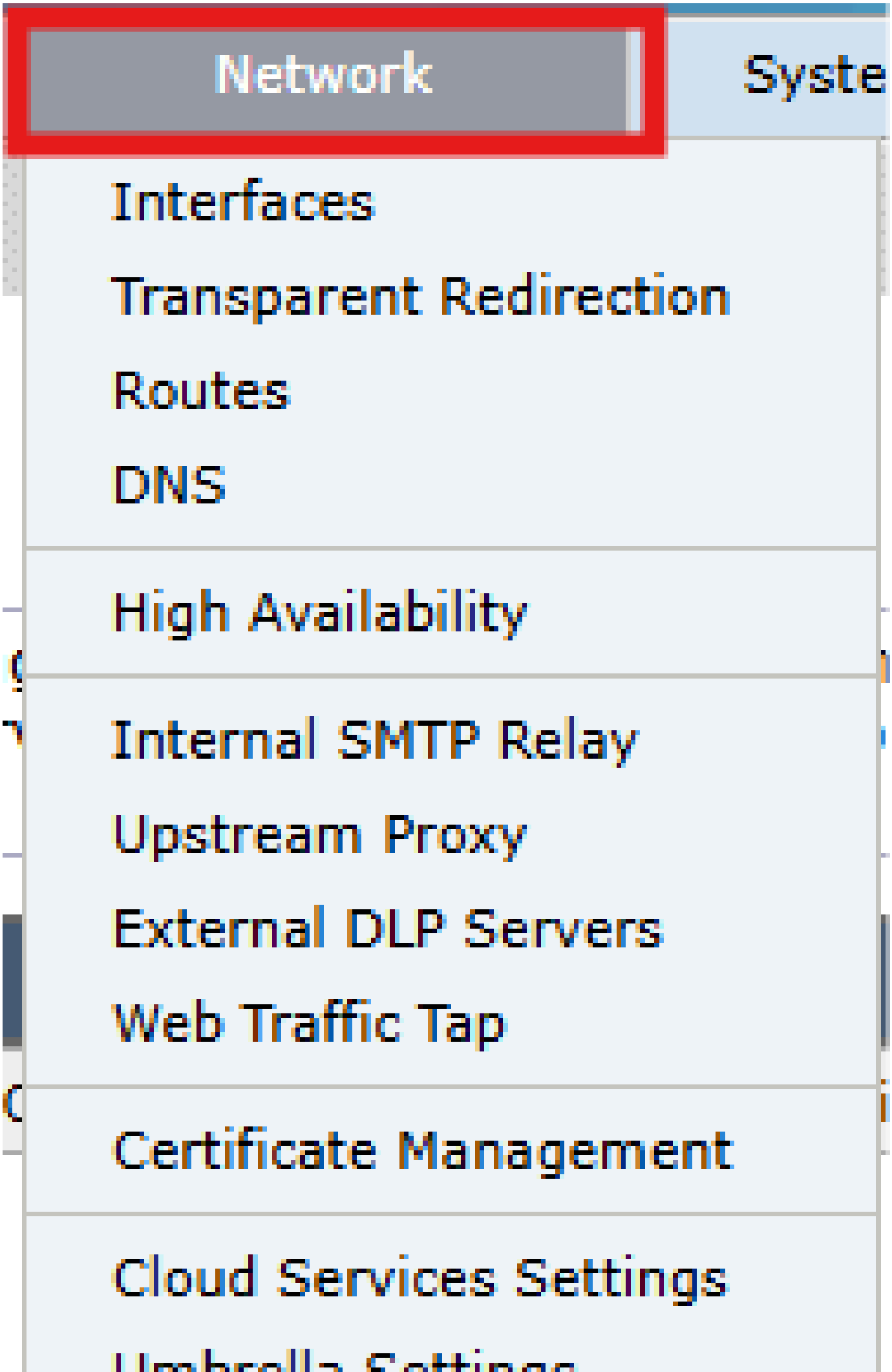
Apruebe automáticamente las nuevas cuentas basadas en certificados para que la solicitud del cliente se apruebe automáticamente y guarde.



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

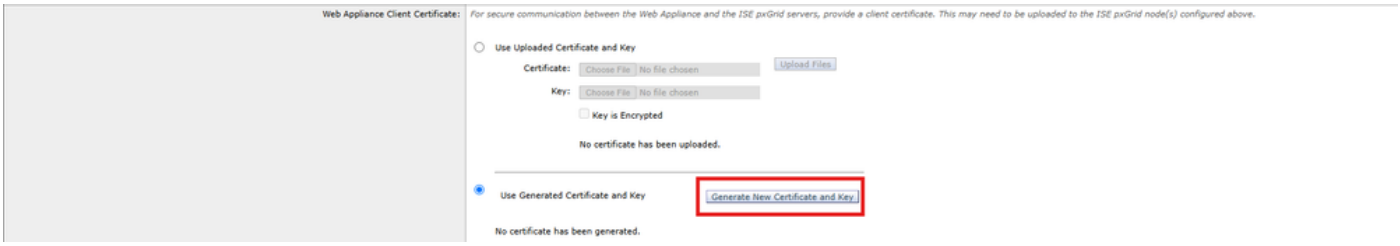
1.Inicie sesión en la GUI del dispositivo de seguridad web (WSA).

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

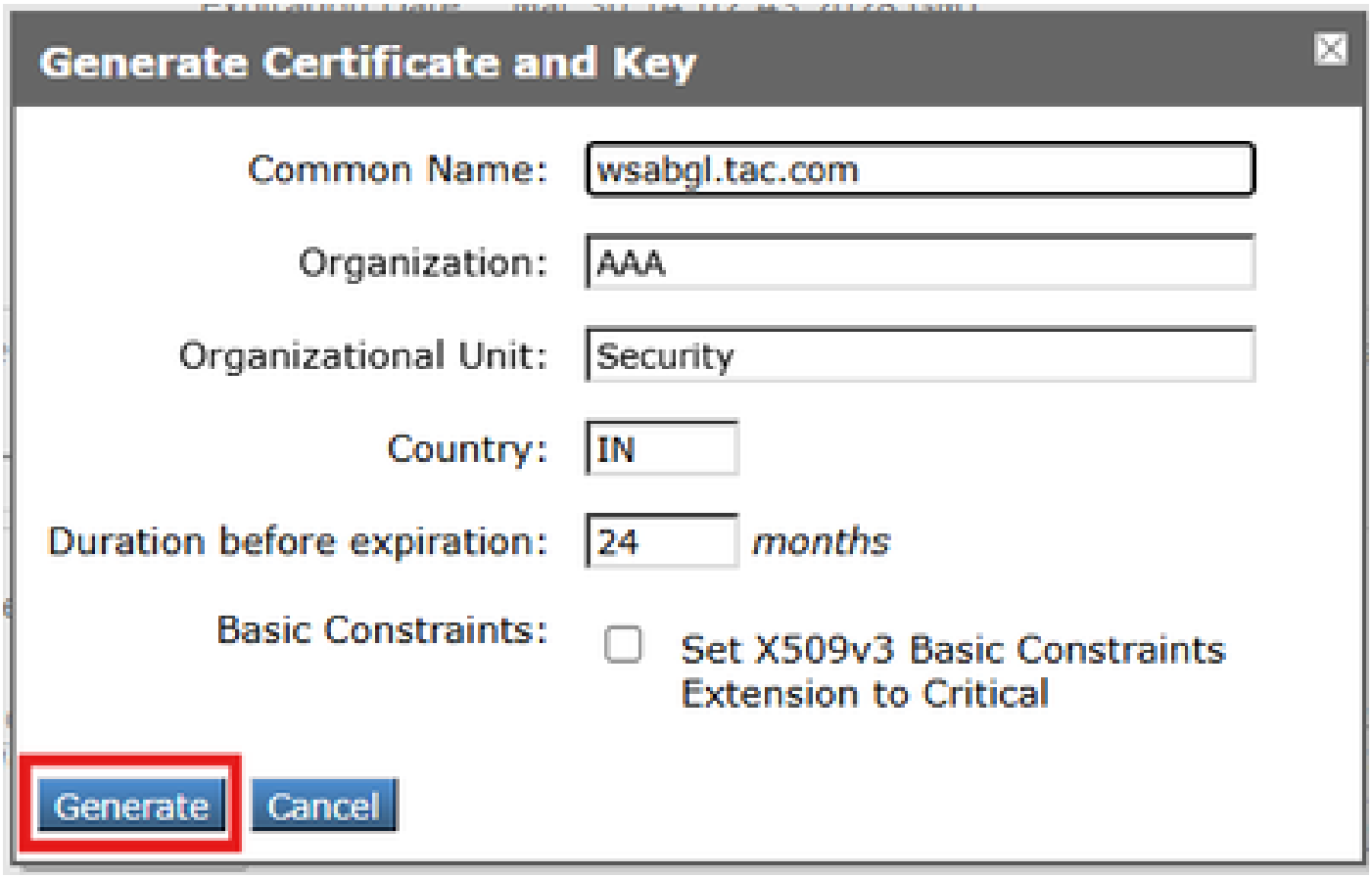

Network
Syste
Interfaces
Transparent Redirection
Routes
DNS
High Availability
Internal SMTP Relay
Upstream Proxy
External DLP Servers
Web Traffic Tap
Certificate Management
Cloud Services Settings

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.

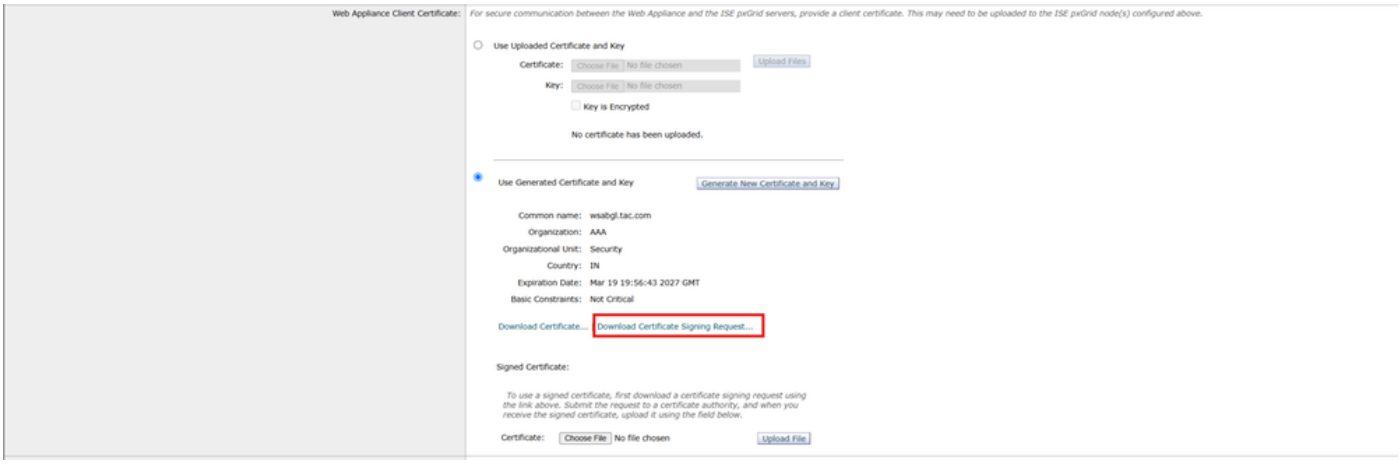


9. Rellene los detalles del certificado según sea necesario y haga clic en Generar.



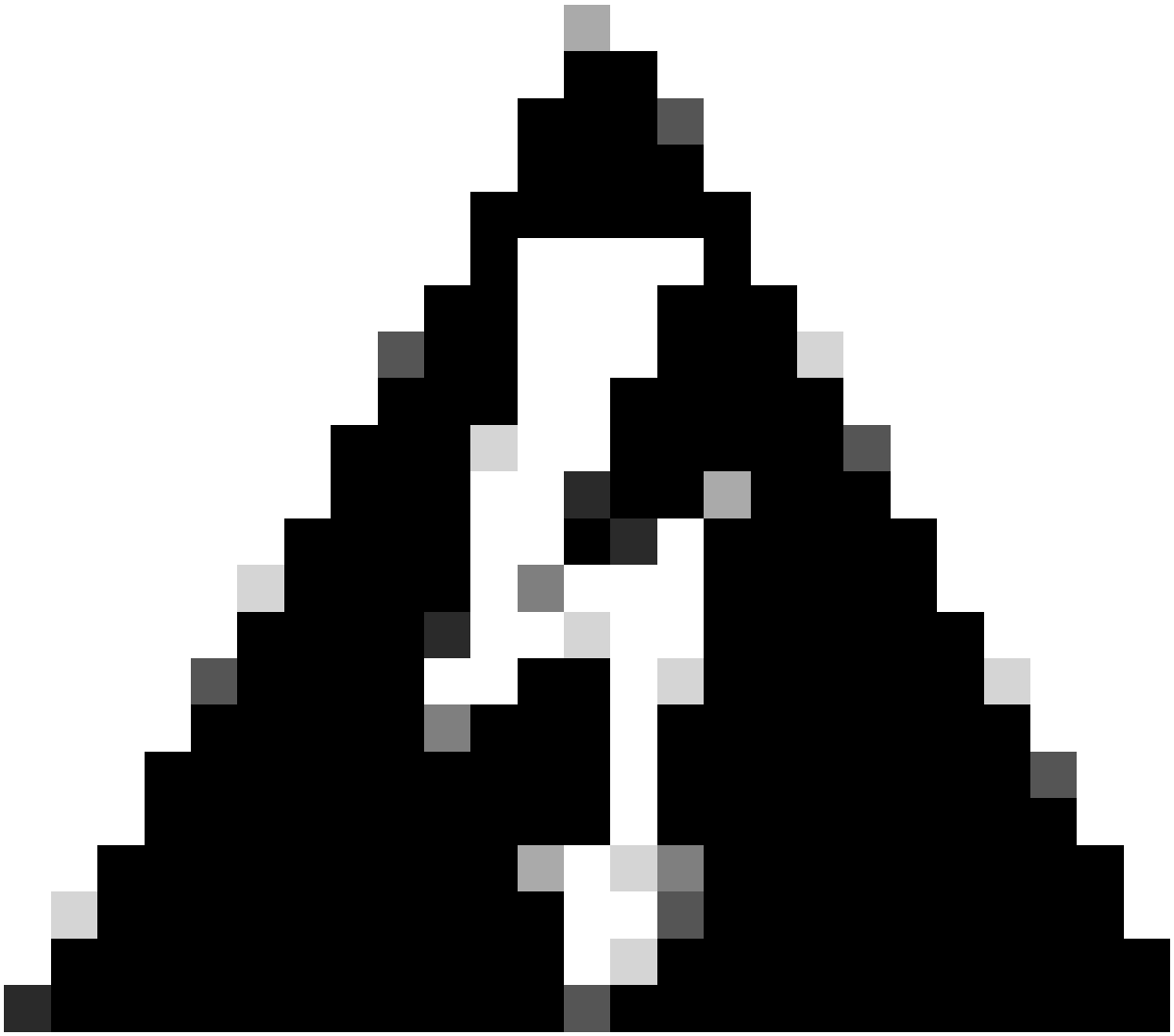
Nota: La duración del certificado debe ser un número entero entre 24 y 60 meses y el país debe ser un código de país ISO de dos caracteres (sólo letras mayúsculas).

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



11. Haga clic en Enviar.

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

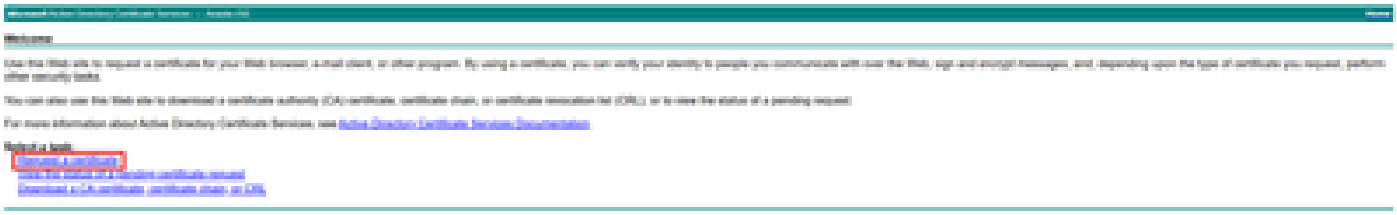


Advertencia: Si no envía y confirma los cambios mencionados y carga directamente el certificado firmado y realiza la confirmación, puede enfrentarse a problemas durante la integración.

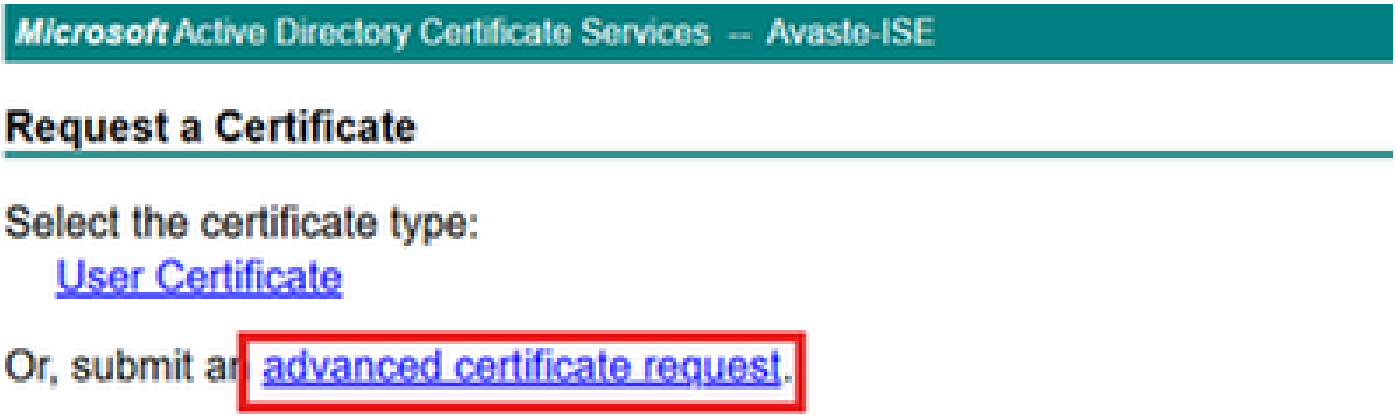
Sección B: Firmar una CSR de cliente WSA mediante una CA externa

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.

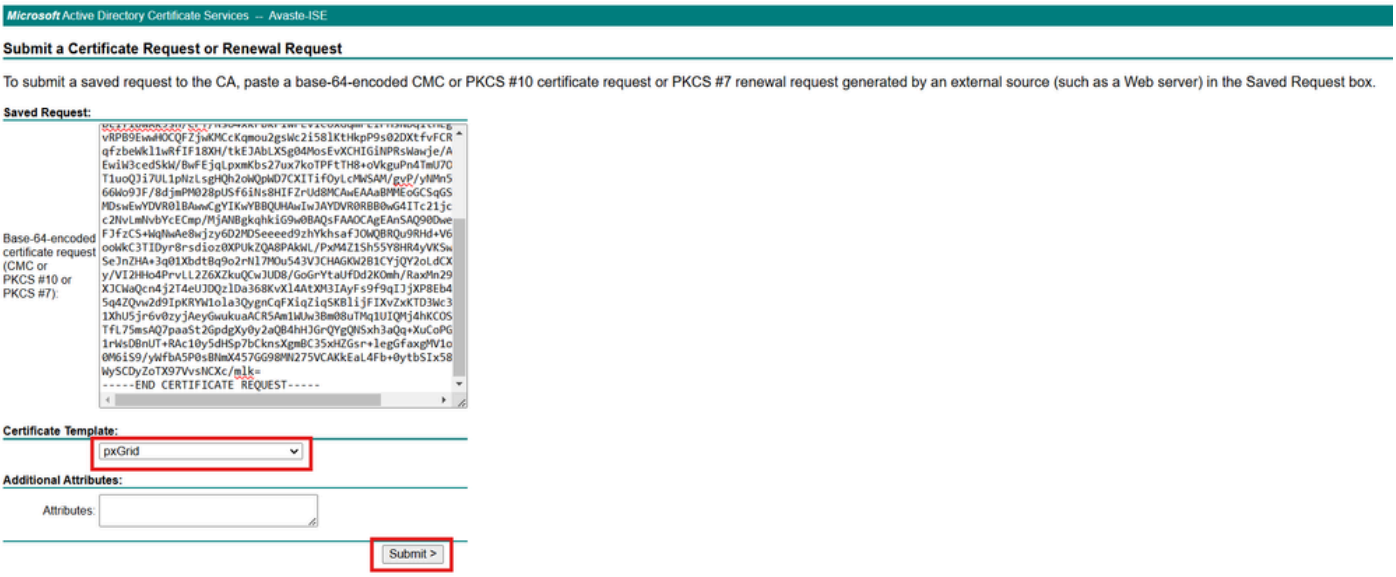


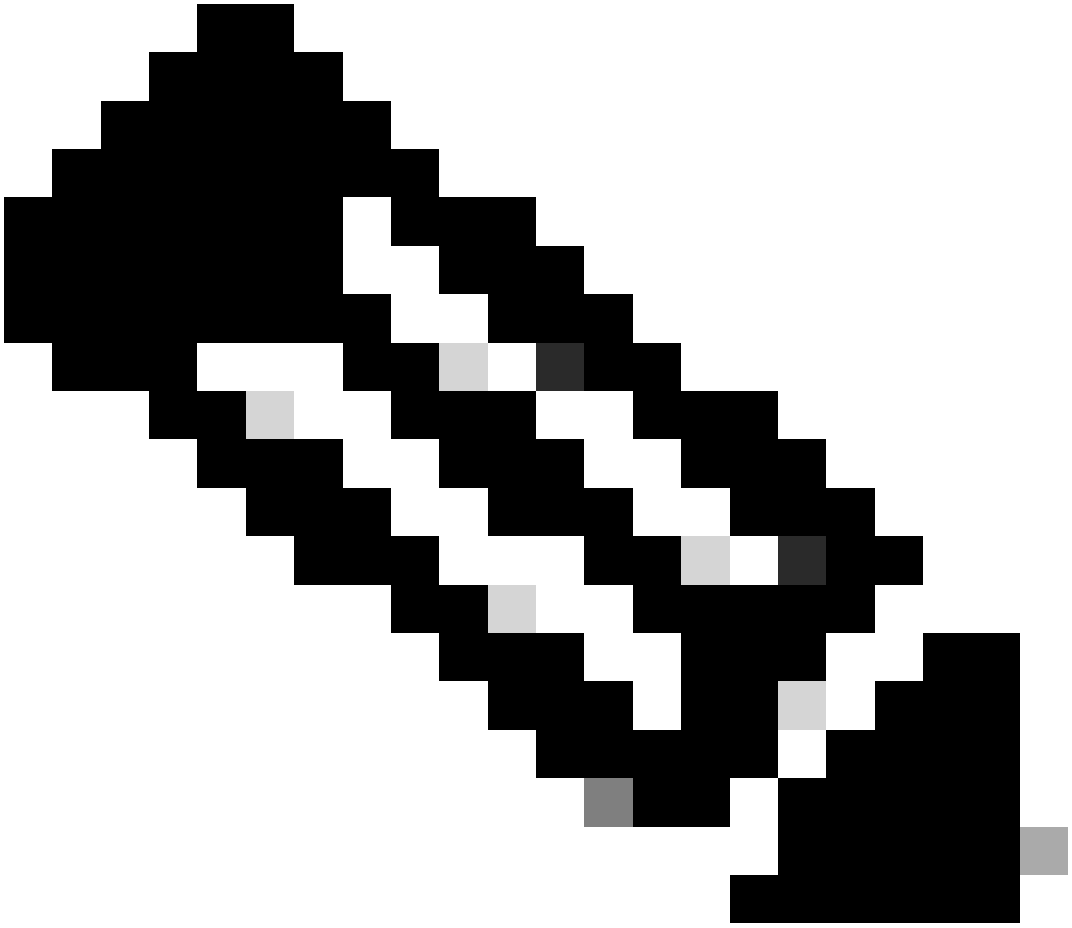
3. Seleccione esta opción para ejecutar una solicitud de certificado avanzada.



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

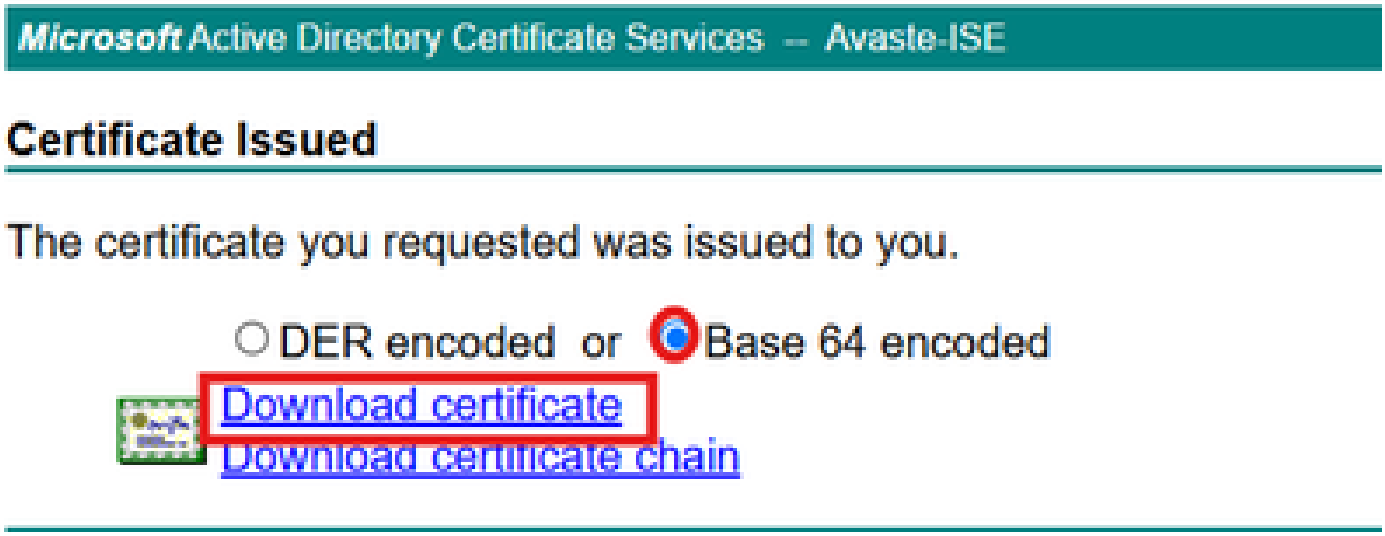
5. Seleccione pxGrid como la plantilla de certificado y, a continuación, haga clic en Enviar.





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.



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

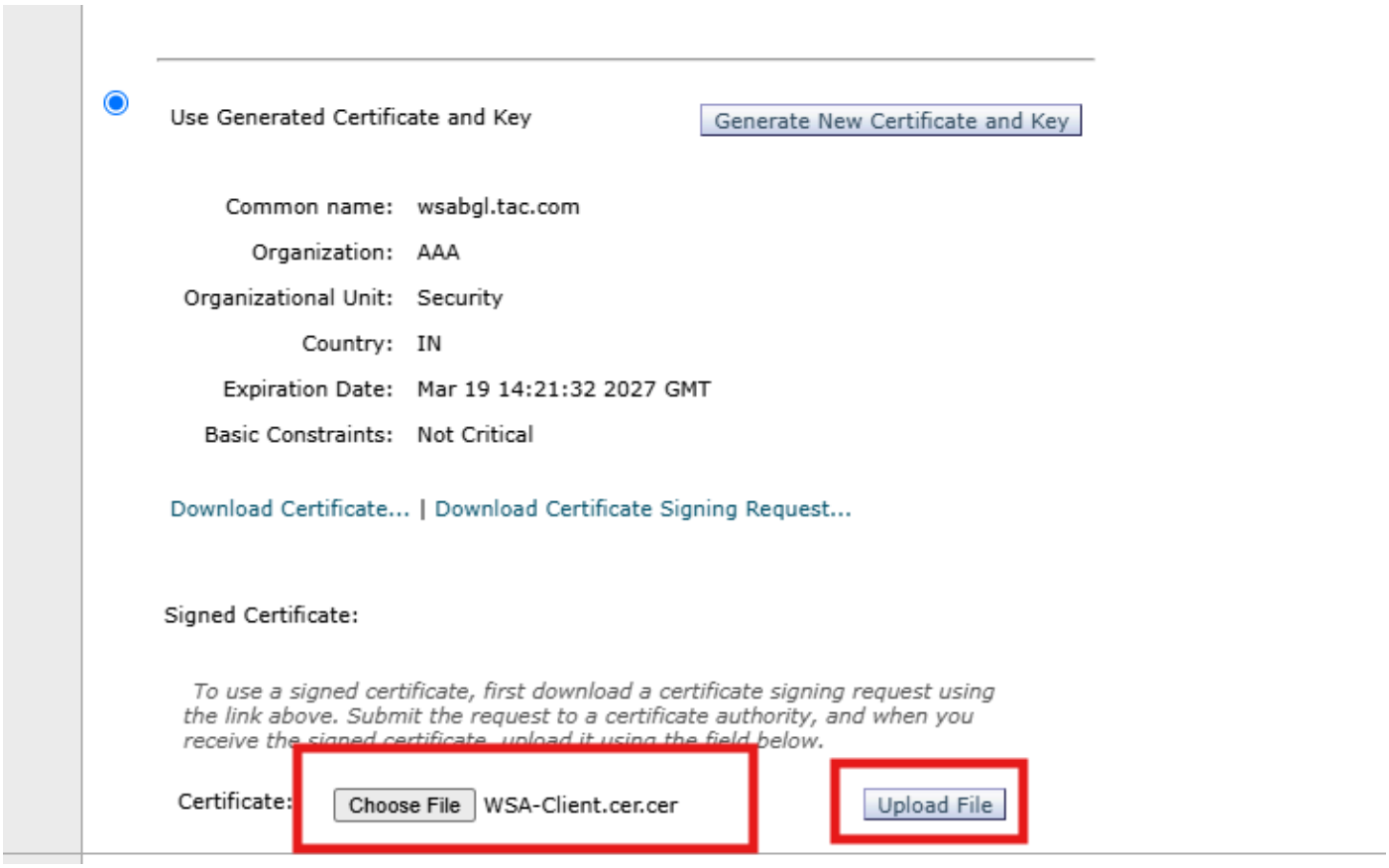
1.Navegue hasta la GUI del dispositivo de seguridad web (WSA).

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



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

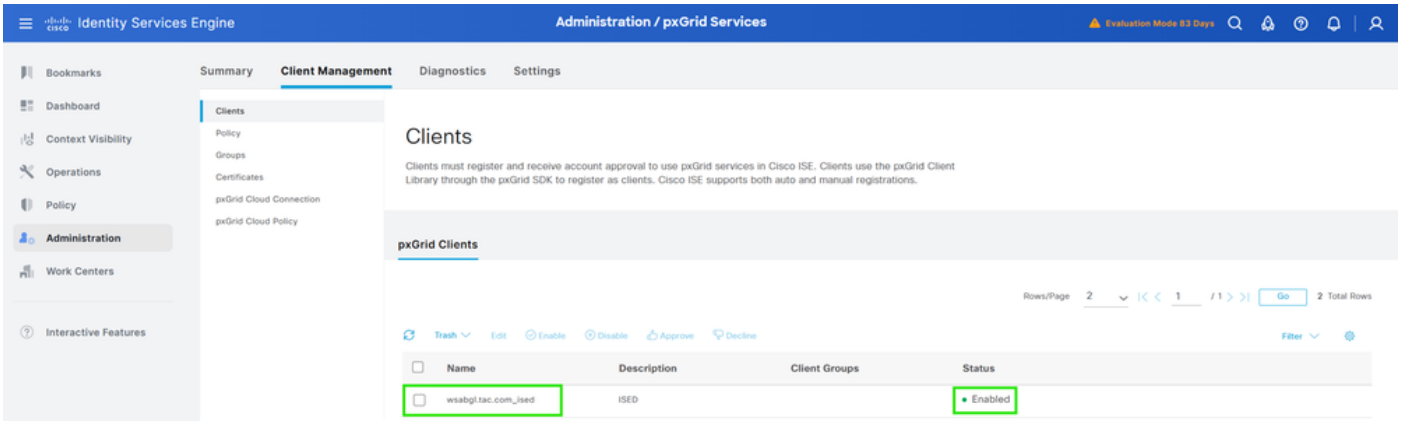
Comunicación de prueba con nodos ISE

```
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.
```

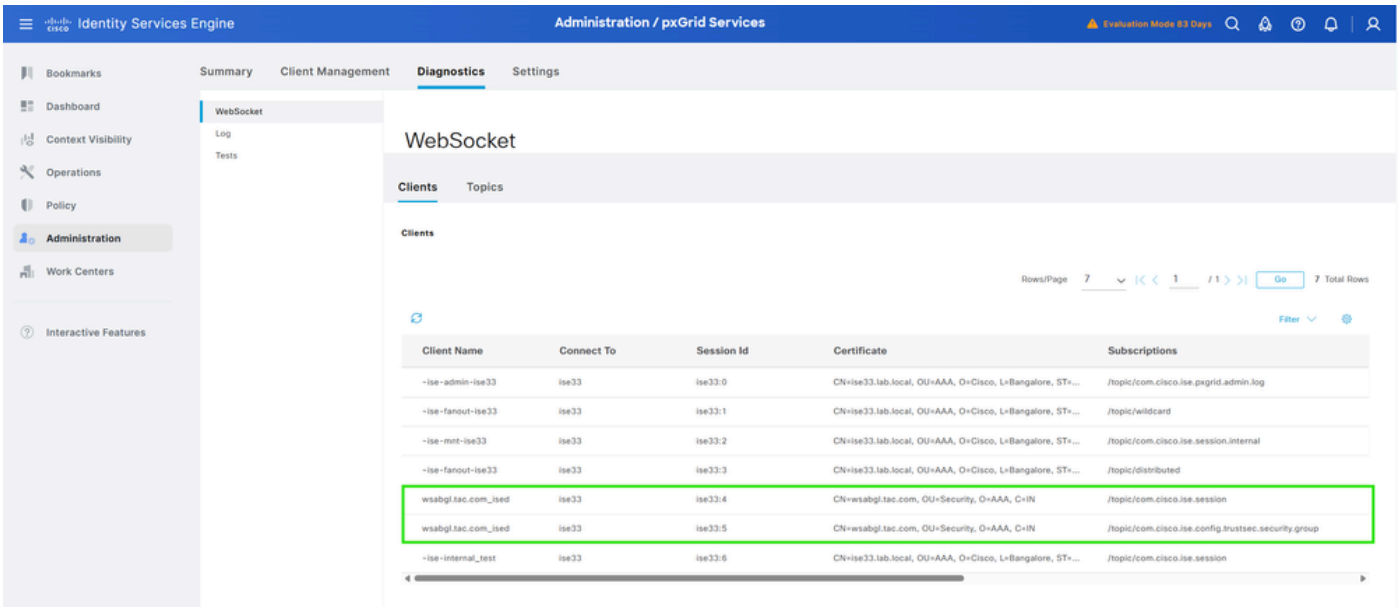
Verificación

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

Esto genera el WSA como un cliente pxgrid con el statusEnabled.



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



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. 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
```

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.
```

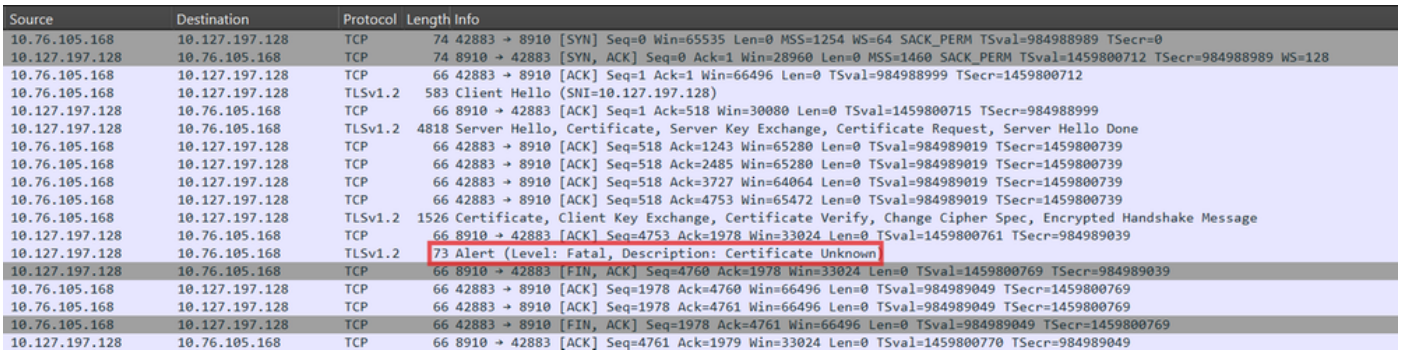
unable to find valid certification path to requested target principle=CN=wsabgl.lab.local, OU=Security,

```
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).