

Geïntegreerde ISE 3.3 met WSA met behulp van externe CA

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Deel A: Cisco Identity Services Engine 3.3 certificaatconfiguratie](#)

[Stap 1: Genereert een ISEServer-pxGrid-certificaat](#)

[Stap 2: Een ISE-servercertificaat met NetGrid maken met een externe CA](#)

[Stap 3: Het CA Root Certificate importeren in de ISE Trust Store](#)

[Stap 4: Binding van het ISE-certificaat aan het verzoek tot ondertekening van het certificaat \(CSR\).](#)

[Deel B: CA Root Certificate toevoegen aan WSA Certificate Trust Store](#)

[Integratie](#)

[Deel A: Schakel WSA in voor ISE-integratie en genereer CSR voor WSA-clientcertificaat.](#)

[Deel B: Onderteken een WSA-client CSR met een externe CA](#)

[Deel C: Binding van het WSA-clientcertificaat aan het CSR-certificaat \(Certificate Signing Verzoek\) en integratie.](#)

[Verifiëren](#)

[Probleemoplossing](#)

[Probleem](#)

[Oplossing](#)

[Bekende gebreken](#)

Inleiding

Dit document beschrijft procedures om ISE 3.3 te integreren met Cisco Secure Web Applicatie (WSA) met behulp van pxGrid-verbindingen.

Voorwaarden

Vereisten

Cisco raadt kennis over deze onderwerpen aan:

- Identity Services Engine
- Cisco Secure Web Applicatie (WSA)
- Platform Exchange Grid (pxGrid)
- TLS-/SSL-certificaten.
- PKI op Windows-server 2016

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Identity Services Engine (ISE) versie 3.3 patch 4
- Cisco Secure Web Applicatie versie 15.2.0-16
- Windows-server 2016 als een externe certificeringsinstantie (CA)-server.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

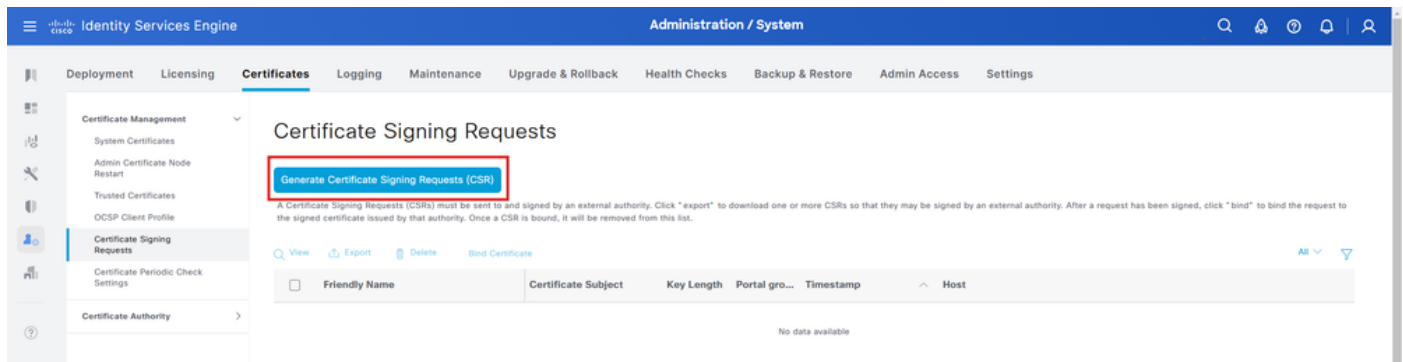
Configureren

Deel A: Cisco Identity Services Engine 3.3 certificaatconfiguratie

Stap 1: Genereert een ISEserver pxGrid-certificaat

Een CSR genereren voor een ISE-server pxGrid-certificaat:

1. Log in Cisco Identity Services Engine (ISE) GUI.
2. Navigatie to **Administration > Systeem > Certificaten > Certificaatbeheer > Certificaatondertekeningaanvragen**.
3. Selecteer **Generate Certificate Signing Verzoek (CSR)**.



4. Select **pxGrid** in het certificaat (de certificaten) wordt gebruikt voor het veld.
5. Selecteer ISE-knooppunt waarvoor het certificaat wordt gegenereerd.
6. Indien nodig andere gegevens van het certificaat invullen.
7. Klik op **Generate**.

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

Voor het gebruik van certificaatsjabloon pxGrid zijn zowel clientverificatie als serververificatie in het veld Uitgebreid sleutelgebruik nodig.

6. Download het gegenereerde certificaat in Base-64-formaat en Opslaan als 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](#)

Stap 3: Het CA Root Certificate importeren in de ISE Trust Store

1. Navigeren naar MS Active Directory Certificate Service startpagina en selecteer Een CA-certificaat, certificaatketen of CRL downloaden.

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](#)

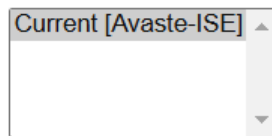
2. Selecteer Base-64formaat en klik Download CA certificaat.

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](#)

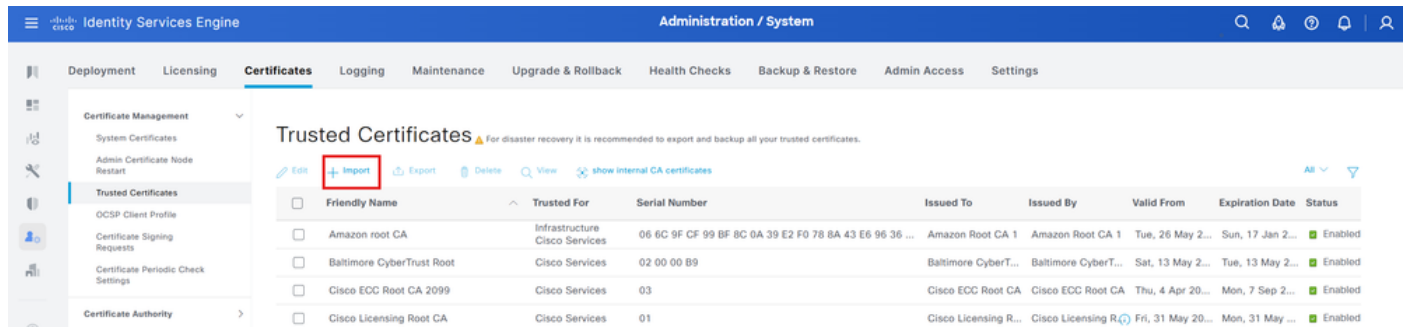
[Download latest base CRL](#)

[Download latest delta CRL](#)

3. Het certificaat opslaan als CA_Root.cer.

4. Log in op Cisco Identity Services Engine (ISE) GUI.

5. Selecteer Beheer > Systeem > Certificaten > Certificaatbeheer > Betrouwbare certificaten.



The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System interface. The 'Certificates' tab is selected in the left sidebar. 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 CF 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. Selecteer Importeren > certificaatbestand en Importeer het basiscertificaat.

7. Zorg ervoor dat het selectievakje Vertrouwen voor verificatie in ISE is geselecteerd.

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. Klik op Indienen.

Stap 4: Binding van het ISE-certificaat aan het verzoek tot ondertekening van het certificaat (CSR).

1. Log in Cisco Identity Services Engine (ISE) GUI.

2. Selecteer Beheer > Systeem > Certificaten > Certificaatbeheer > Aanvragen voor certificaatondertekening.

3. Selecteer de MVO die in de vorige sectie is gegenereerd en klik vervolgens op Bindcertificaat.

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.

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. Kies op het formulier Bind CA Signed Certificate het eerder gegenereerde ISE_pxGrid.cer certificaat.

5. Geef het certificaat een vriendschappelijke naam en klikSubmit.

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. Klik op Ja als het systeem het certificaat moet vervangen.

8. Selecteer Beheer > Systeem > Certificaten > Systeemcertificaten.

9. In de lijst ziet u het gemaakte pxGrid-certificaat dat is ondertekend door de externe CA.

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 Endpoint Sub CA - ise33r00005	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

Deel B: CA Root Certificate toevoegen aan WSA Certificate Trust Store

CA Root Certificate toevoegen aan WSA Trusted Store:

1. Log in op Web Security Applicatie (WSA) GUI.

2. Navigeer naar netwerk > certificaatbeheer > Trusted Root-certificaten beheren.

Network

System

Interfaces

Transparent Redirection

Routes

DNS

High Availability

Internal SMTP Relay

Upstream Proxy

External DLP Servers

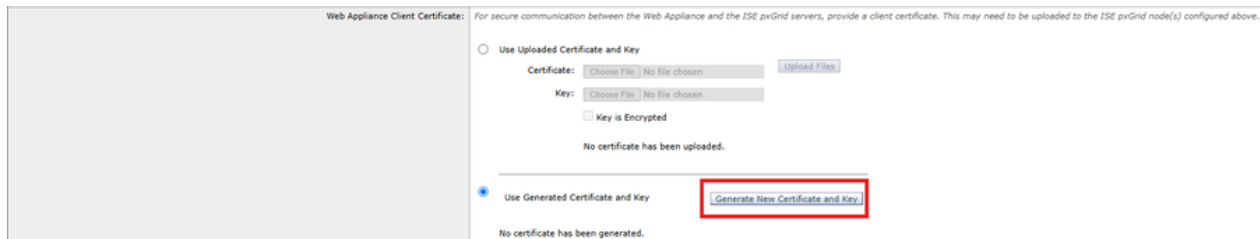
Web Traffic Tap

Certificate Management

Cloud Services Settings

Er kunnen slechts twee pxGrid-knooppunten per ISE-implementatie zijn. Dit fungeert als een PxGrid Active-Standby configuratie; slechts één ISE+pxGrid-knooppunt kan tegelijkertijd actief zijn. In een pxGrid Active-stand-by configuratie wordt alle informatie doorgegeven via de PAN, waar de tweede ISE+pxGrid-knooppunt inactief blijft.

8. Blader naar het gedeelte Clientcertificaat voor Web Appliance en klik op Nieuw certificaat en nieuwe sleutel genereren.



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

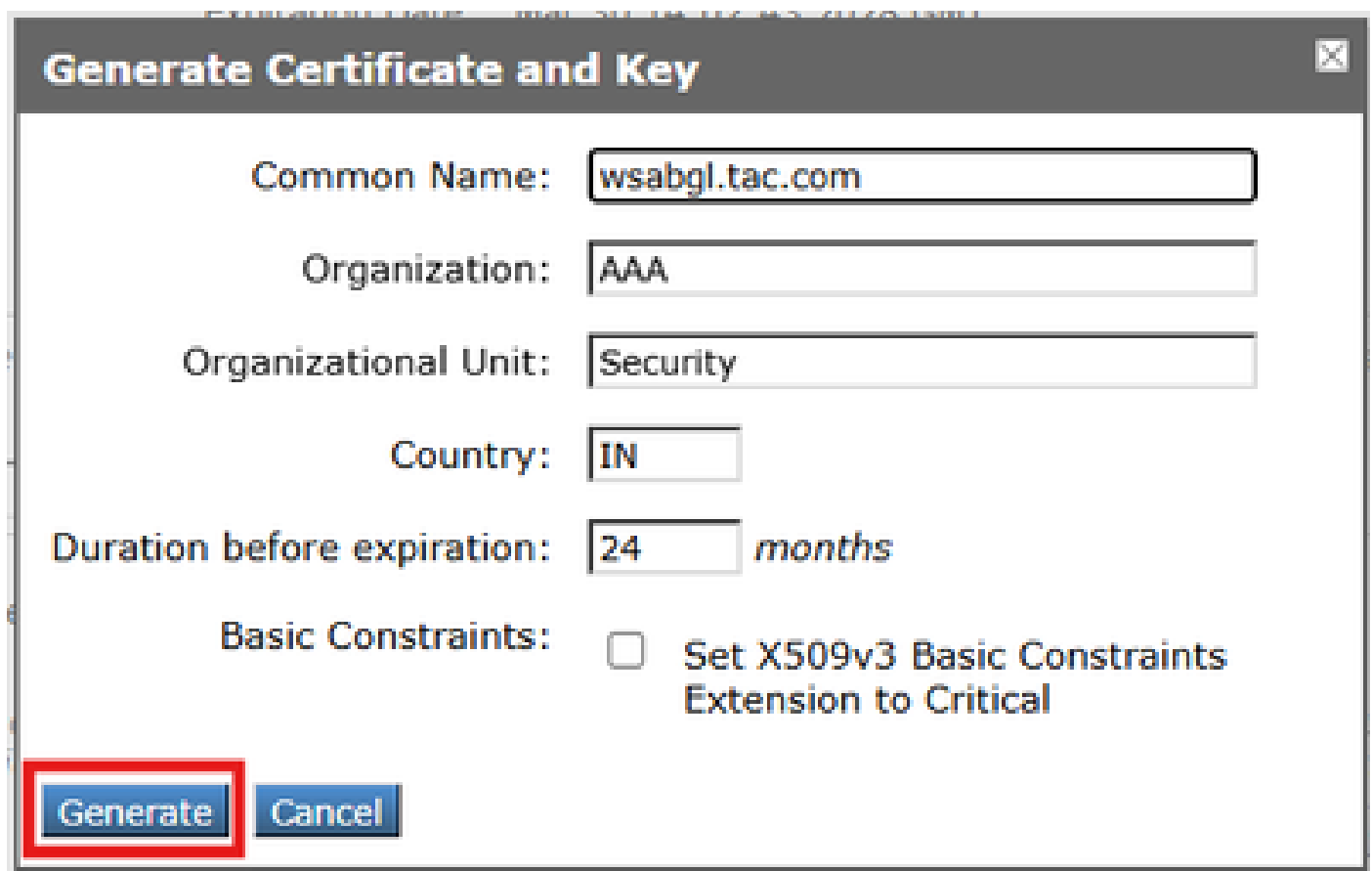
☐ Key is Encrypted

No certificate has been uploaded.

☒ Use Generated Certificate and Key

No certificate has been generated.

9. Vul certificaatgegevens in zoals nodig en klik op Generate.



Generate Certificate and Key

Common Name:

Organization:

Organizational Unit:

Country:

Duration before expiration: months

Basic Constraints: ☐ Set X509v3 Basic Constraints Extension to Critical



Opmerking: De duur van het certificaat moet een geheel getal tussen 24 en 60 maanden zijn en het land moet een landencode van twee tekens volgens ISO zijn (alleen hoofdletters).

10. Klik op Aanvraag voor ondertekening van certificaat downloaden.

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: wsabgl.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. Klik op Indienen.

12. Klik op Wijzigingen vastleggen om de wijzigingen toe te passen.

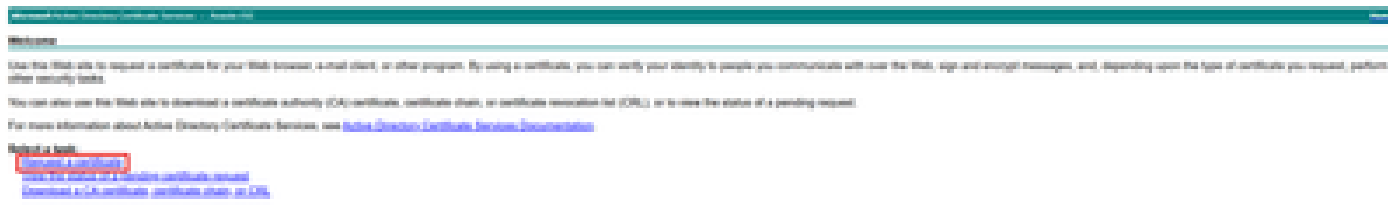


Waarschuwing: Als u geen vermelde wijzigingen indient en doorvoert en het ondertekende certificaat direct uploadt en uitvoert, kunt u problemen tijdens de integratie onder ogen zien.

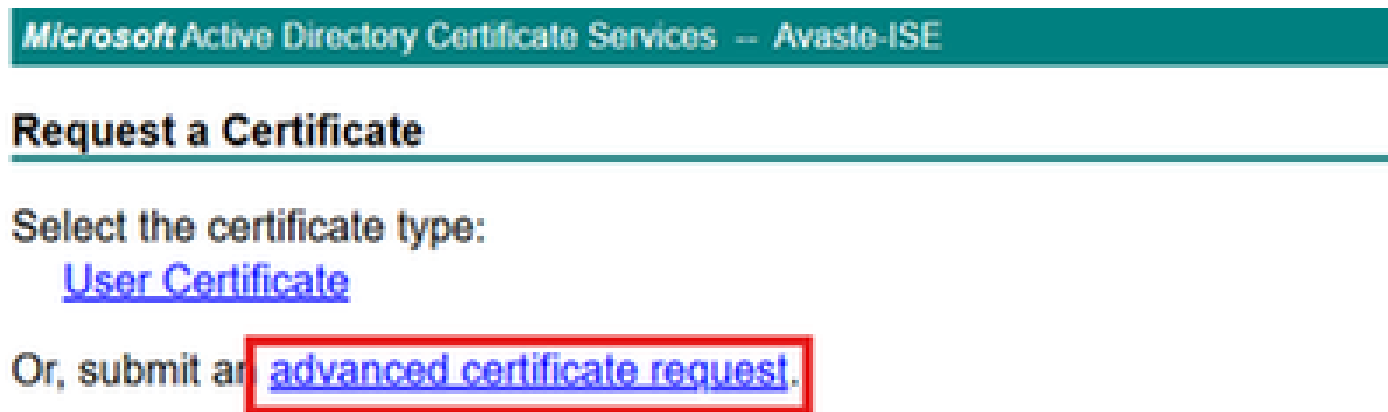
Deel B: Onderteken een WSA-client CSR met een externe CA

1. Navigeren naar MS Active Directory Certificate Service, <https://server/certsrv/>, waar de server IP of DNS van uw MS-server is.

2. Klik op Certificaat aanvragen.

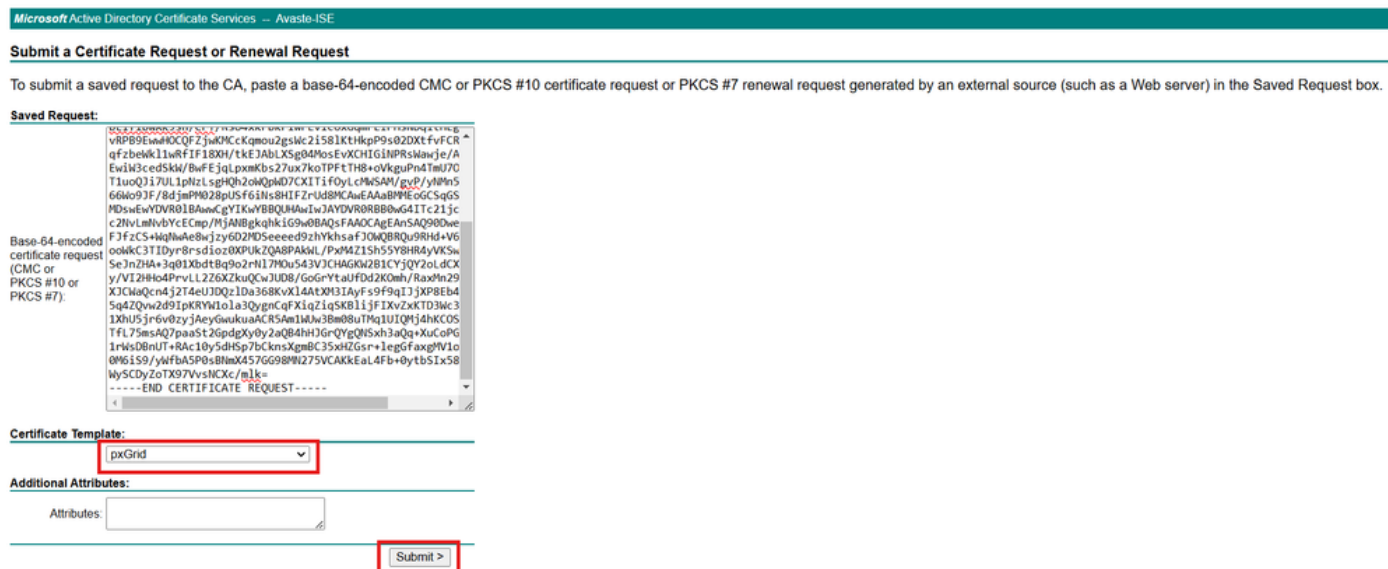


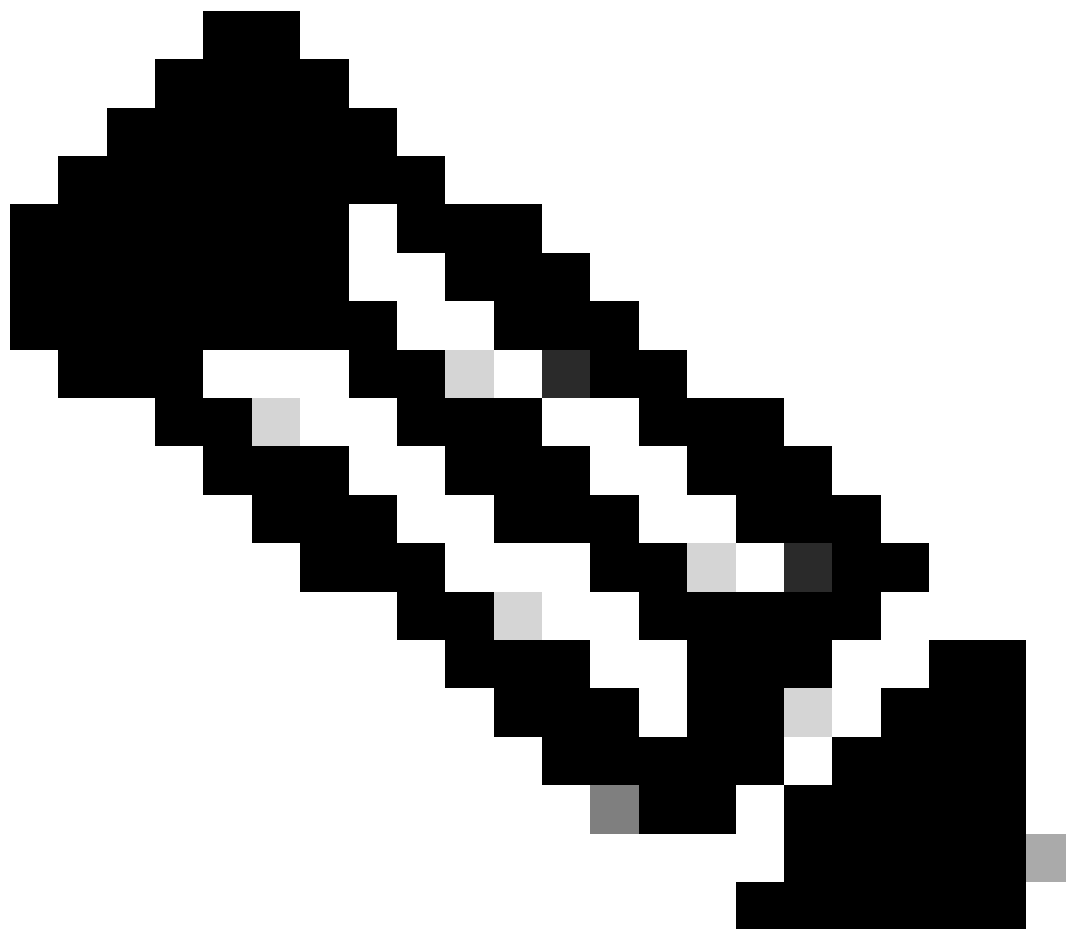
3. Kies om een geavanceerde certificaataanvraag in te dienen.



4. Kopieer de inhoud van de MVO gegenereerd in de vorige sectie naar het veld Opgeslagen aanvraag.

5. Selecteer pxGrids de certificaatsjabloon en klik Indienen.





Opmerking: Opmerking: Voor het gebruik van certificaatsjabloon pxGrid zijn zowel clientverificatie als serververificatie in het veld Uitgebreid sleutelgebruik nodig.

6. Download het gegenereerde certificaat in Base-64-formaat en Opslaan als WSA-Client.cer.

Certificate Issued

The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

Deel C: Binding van het WSA-clientcertificaat aan het CSR-certificaat (Certificate Signing Verzoek) en integratie.

1. Navigatie naar Web Security Applicatie (WSA) GUI.
2. Navigeren naar netwerk > Identificatiediensten > Identification Service Engine.
3. Klik op Instellingen bewerken.
4. Navigeer naar het gedeelte Clientcertificaat voor Web Applicatie.
5. Upload onder het gedeelte ondertekende certificaten het ondertekende certificaat 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. Klik op Indienen.

7. Klik op Wijzigingen vastleggen om de wijzigingen toe te passen.

8. Klik op Instellingen bewerken.

9. Scroll naar Test Communication met ISE-knooppunten en klik op Start Test, dat als volgt kan resulteren:

Communicatie testen met ISE-knooppunten

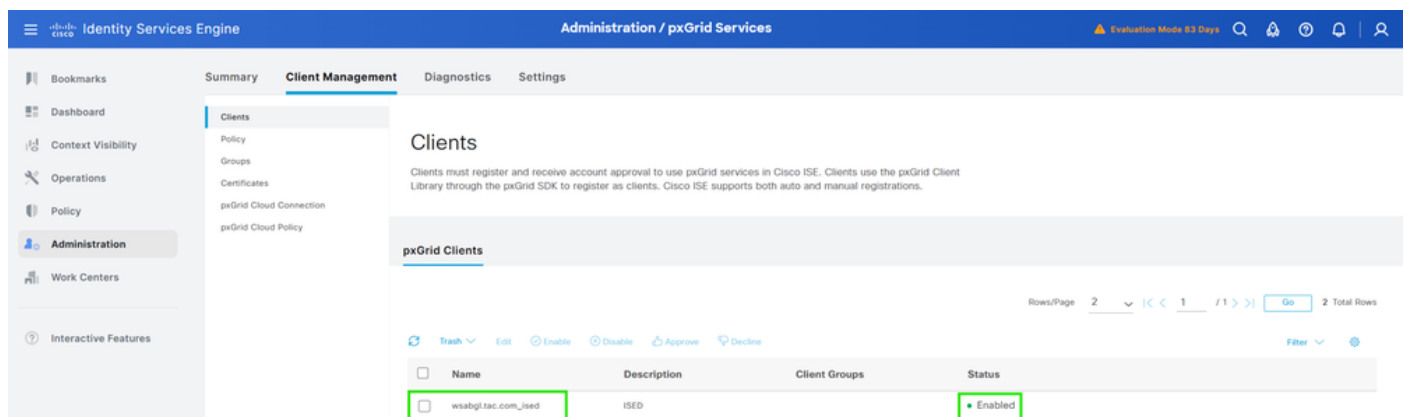
Communicatie testen met ISE-knooppunten

```
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.
```

Verifiëren

Ga op Cisco ISE naar Beheer > PxGrid Services > Clientbeheer > Clients.

Dit genereert de WSA als een pxgrid-client met de 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 includes a sub-header 'pxGrid Clients'. Below this, there is a table with the following columns: Name, Description, Client Groups, and Status. A single client is listed: 'wsabgi-tac.com_iseif' with the description 'ISED' and the status 'Enabled'. The status 'Enabled' is highlighted with a green box.

Name	Description	Client Groups	Status
wsabgi-tac.com_iseif	ISED		Enabled

Om het abonnement op een onderwerp van Cisco ISE te verifiëren, navigeer naar Beheer > PxGrid-services >

Diagnostiek > Websocket > Clients:

Administration / pxGrid Services					
Evaluation Mode 63 Days					
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 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\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
```

Probleemoplossing

Probleem

Onbekende CA-probleem, op de WSA de test voor ISE-verbinding mislukt met fout. Falen: Time out van verbinding met ISE PxGrid-server.

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 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
```

De reden voor de fout kan met pakketopnamen worden gezien,

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

Oplossing

1. Zorg ervoor dat het door de Web Appliance ondertekende certificaat met succes op de WSA is gekoppeld en dat de wijzigingen zijn doorgevoerd.
2. Zorg ervoor dat de emittent of het Root CA-certificaat van het WSA-clientcertificaat deel uitmaakt van Trusted Store op Cisco ISE.

Bekende gebreken

Cisco bug-ID	Beschrijving
23986 van Cisco-bug-id	PxGrid GetUserGroups API-verzoek om lege respons terug te sturen.
77321 van Cisco-bug-id	WSA ontvangt SID's in plaats van AD-groepen van ISE.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.