

Integration von ISE 3.3 mit WSA über externe Zertifizierungsstelle

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Abschnitt A: Cisco Identity Services Engine 3.3-Zertifikatkonfiguration](#)

[Schritt 1: ISE-Server pxGrid-Zertifikat generieren](#)

[Phase 2: Erstellen eines ISE-Server pxGrid-Zertifikats mit einer externen Zertifizierungsstelle](#)

[Schritt 3: Importieren des CA-Stammzertifikats in den ISE-Vertrauensspeicher](#)

[Schritt 4: Binden des ISE-Zertifikats an die Zertifikatsignierungsanforderung \(Certificate Signing Request, CSR\)](#)

[Abschnitt B: Hinzufügen eines CA-Stammzertifikats zum WSA-Zertifikatvertrauensspeicher](#)

[Integration](#)

[Abschnitt A: Aktivieren Sie WSA für die ISE-Integration, und generieren Sie CSR für das WSA-Client-Zertifikat.](#)

[Abschnitt B: Signieren eines WSA-Client-CSR mithilfe einer externen Zertifizierungsstelle](#)

[Abschnitt C: Bindung des WSA-Clientzertifikats an die Zertifikatsanforderung \(Certificate Signing Request, CSR\) und Integration](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Problem](#)

[Lösung](#)

[Bekannte Fehler](#)

Einleitung

In diesem Dokument werden Verfahren zur Integration von ISE 3.3 in die Cisco Secure Web Appliance (WSA) unter Verwendung von pxGrid-Verbindungen beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt Fachwissen in folgenden Bereichen:

- Identity Services Engine
- Cisco Secure Web Appliance (WSA)
- Platform Exchange Grid (pxGrid)
- TLS/SSL-Zertifikate

- PKI auf Windows Server 2016

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Identity Services Engine (ISE) Version 3.3 Patch 4
- Cisco Secure Web Appliance Version 15.2.0-116
- Windows Server 2016 als CA-Server (External Certificate Authority)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

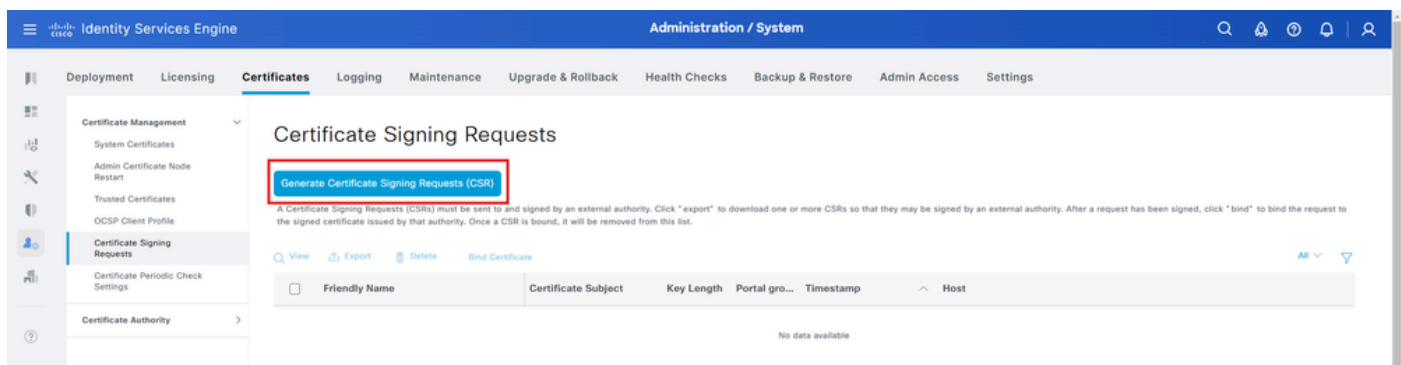
Konfigurieren

Abschnitt A: Zertifikatskonfiguration der Cisco Identity Services Engine 3.3

Schritt 1: ISEServer pxGrid-Zertifikat generieren

Generieren Sie einen CSR für ein pxGrid-Zertifikat des ISE-Servers:

1. Melden Sie sich an der Cisco Identity Services Engine (ISE)-GUI an.
2. Navigieren Sie zu Administration > System > Certificates > Certificate Management > Certificate Signing Requests.
3. Wählen Sie CSR (Certificate Signing Request) generieren.



4. Select pxGrid in das Zertifikat (die Zertifikate) wird für Feld verwendet.
5. Wählen Sie ISE-Knoten, für den das Zertifikat generiert wird.
6. Füllen Sie ggf. weitere Zertifikatdetails ein.
7. Klicken Sie auf Generieren.

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

Die verwendete Zertifikatvorlage pxGrid erfordert sowohl die Client- als auch die Serverauthentifizierung im Feld "Enhanced Key Usage" (Erweiterte Schlüsselerwendung).

6. Laden Sie das generierte Zertifikat im Base-64-Format herunter und speichern Sie es 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](#)

Schritt 3: Importieren des CA-Stammzertifikats in den ISE-Vertrauensspeicher

1. Navigieren Sie zur Startseite des MS Active Directory-Zertifikatdienst und wählen Sie Zertifizierungsstellenzertifikat, Zertifikatskette oder Zertifikatssperrliste herunterladen.

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](#)

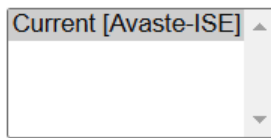
2. Select Base-64format, und klicken Sie dann auf CA-Zertifikat herunterladen.

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](#)

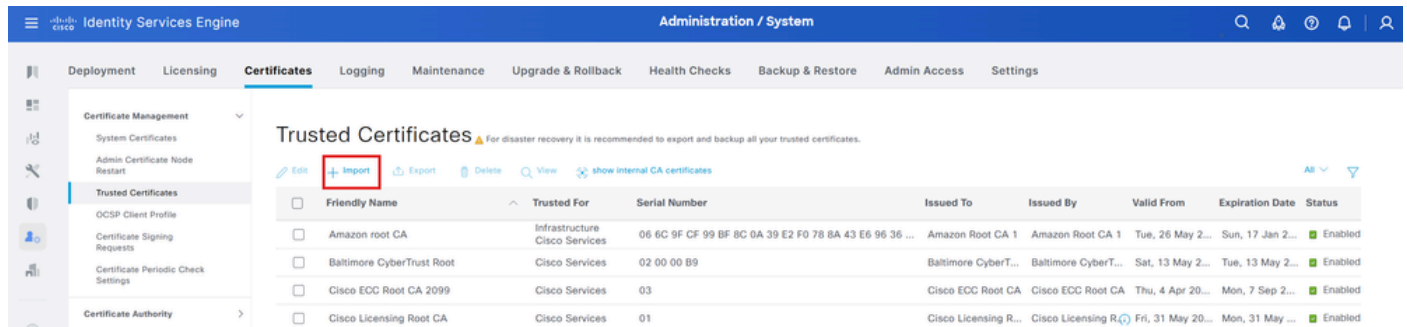
[Download latest base CRL](#)

[Download latest delta CRL](#)

3. Speichern Sie das Zertifikat als CA_Root.cer.

4. Melden Sie sich an der Cisco Identity Services Engine (ISE)-GUI an.

5. Wählen Sie Administration > System > Certificates > Certificate Management > Trusted Certificates aus.



Trusted Certificates For disaster recovery it is recommended to export and backup all your trusted certificates.

[Edit](#)
[+ Import](#)
[Export](#)
[Delete](#)
[View](#)
[show internal CA certificates](#)

☐	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 E5 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. Wählen Sie Importieren > Zertifikatsdatei und importieren Sie das Stammzertifikat.

7. Stellen Sie sicher, dass das Kontrollkästchen Bei Authentifizierung innerhalb der ISE vertrauen aktiviert ist.

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. Klicken Sie auf Senden.

Schritt 4: Binden des ISE-Zertifikats an die Zertifikatsignierungsanforderung (Certificate Signing Request, CSR).

1. Melden Sie sich an der Cisco Identity Services Engine (ISE)-GUI an.

2. Wählen Sie Administration > System > Certificates > Certificate Management > Certificate Signing Requests.

3. Wählen Sie den im vorherigen Abschnitt generierten CSR aus, und klicken Sie dann auf Zertifikat binden.

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. Wählen Sie auf dem Formular "Bind CA Signed Certificate" das zuvor generierte Zertifikat ISE_pxGrid.cer aus.

5. Geben Sie dem Zertifikat einen Anzeigenamen, und klicken Sie dann auf Senden.

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. ClickYesif wird vom System aufgefordert, das Zertifikat zu ersetzen.

8. Wählen Sie Administration > System > Certificates > System Certificates aus.

9. Sie können das erstellte pxGrid-Zertifikat in der Liste sehen, das von der externen Zertifizierungsstelle signiert wurde.

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

Abschnitt B: Hinzufügen eines CA-Stammzertifikats zum WSA-Zertifikatvertrauensspeicher

CA-Stammzertifikat zum vertrauenswürdigen WSA-Speicher hinzufügen:

1. Melden Sie sich bei der Web Security Appliance (WSA) GUI an.
2. Navigieren Sie zu Netzwerk > Zertifikatsverwaltung > Vertrauenswürdige Stammzertifikate verwalten.

Network

System

Interfaces

Transparent Redirection

Routes

DNS

High Availability

Internal SMTP Relay

Upstream Proxy

External DLP Servers

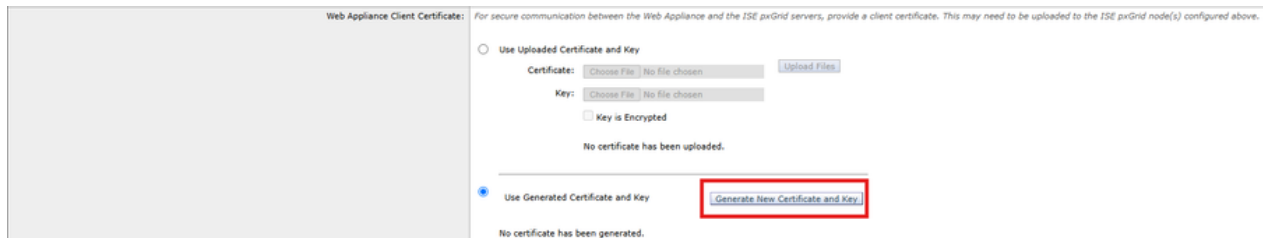
Web Traffic Tap

Certificate Management

Cloud Services Settings

Pro ISE-Bereitstellung können nur zwei pxGrid-Knoten vorhanden sein. Dies dient als pxGrid-Aktiv/Standby-Konfiguration. Es kann jeweils nur ein ISE+pxGrid-Knoten aktiv sein. In einer pxGrid-Aktiv/Standby-Konfiguration werden alle Informationen über das PPAN weitergeleitet, wobei der zweite ISE+pxGrid-Knoten inaktiv bleibt.

8. Blättern Sie zum Abschnitt "Zertifikat des Web-Appliance-Clients", und klicken Sie auf Neues Zertifikat und neuen Schlüssel generieren.



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

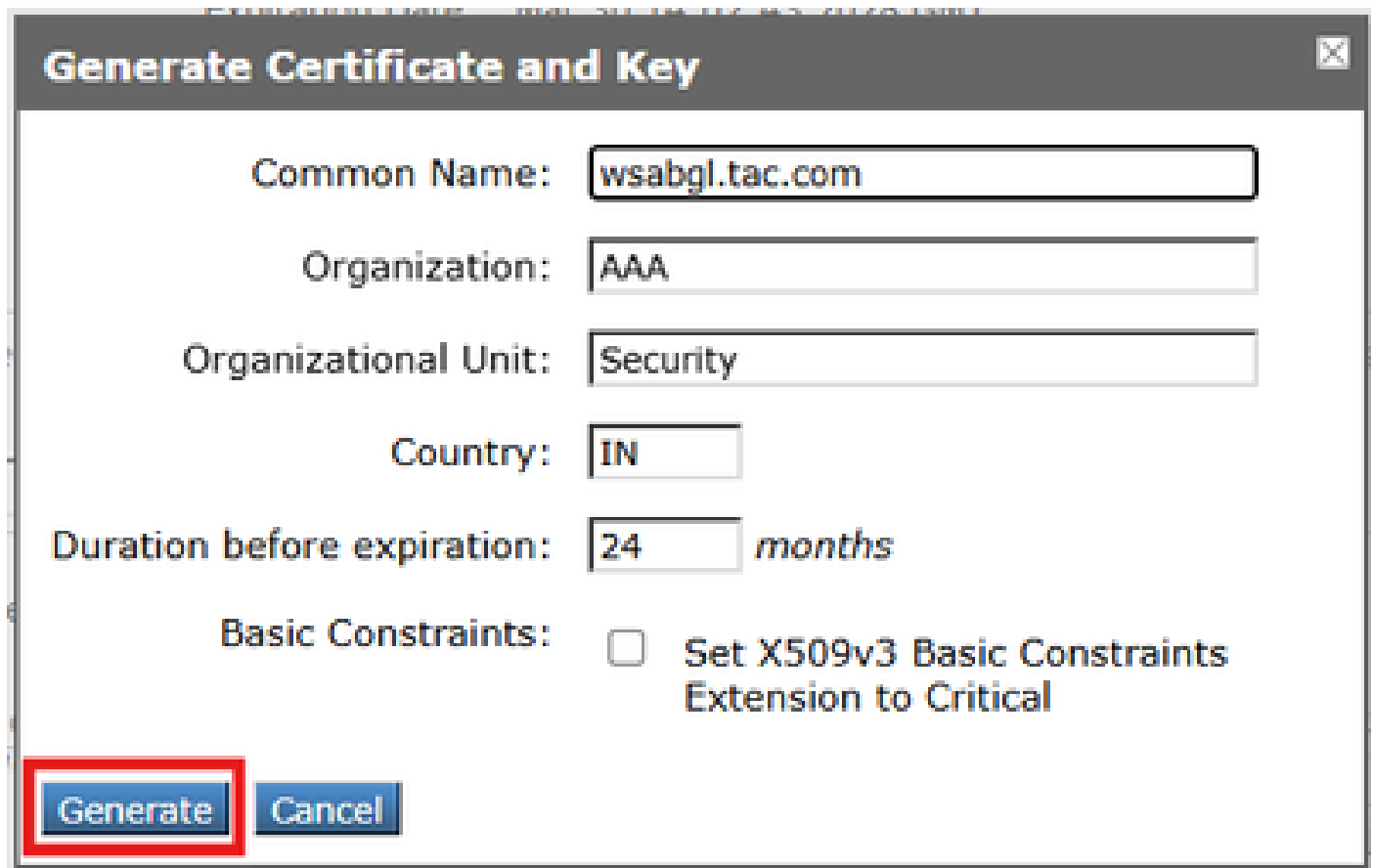
☐ Key is Encrypted

No certificate has been uploaded.

☒ Use Generated Certificate and Key

No certificate has been generated.

9. Geben Sie bei Bedarf Zertifikatdetails ein, und klicken Sie auf Generieren.



Generate Certificate and Key

Common Name:

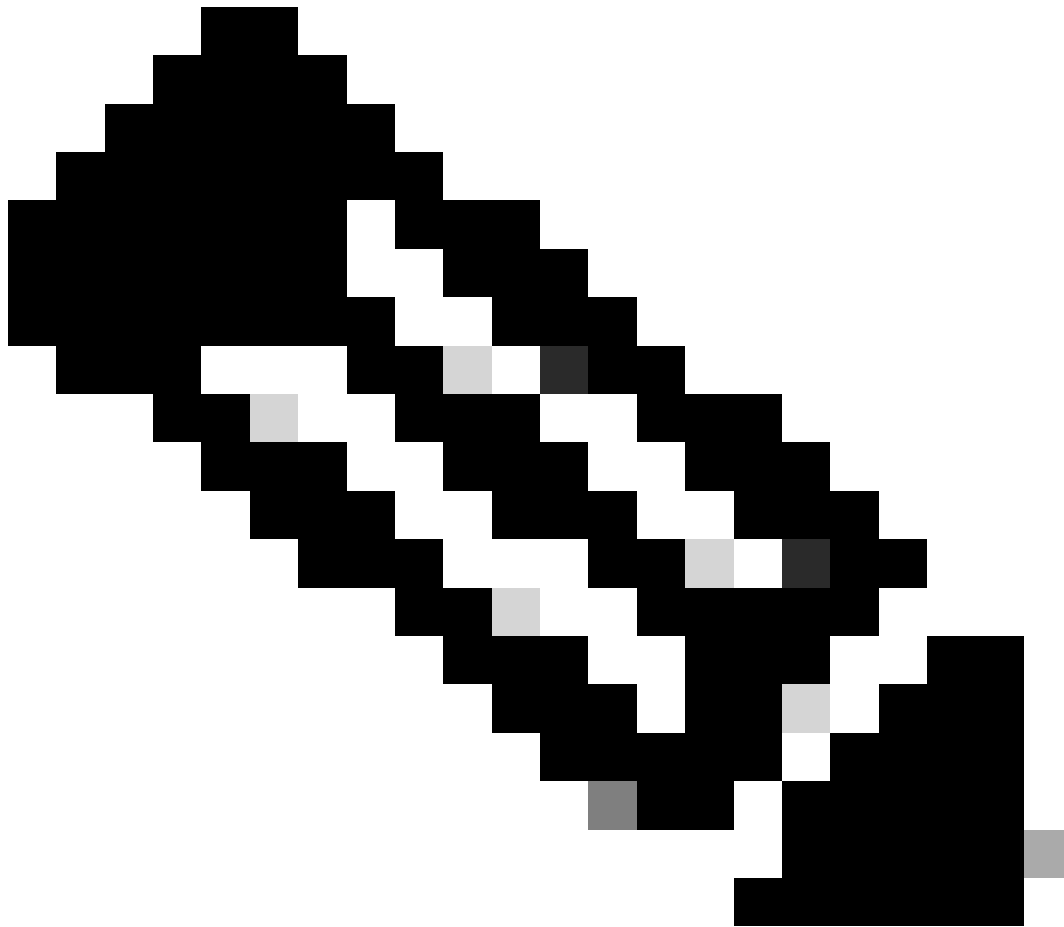
Organization:

Organizational Unit:

Country:

Duration before expiration: months

Basic Constraints: ☐ Set X509v3 Basic Constraints Extension to Critical



Anmerkung: Die Dauer des Zertifikats muss eine ganze Zahl zwischen 24 und 60 Monaten sein, und das Land muss ein ISO-Ländercode mit zwei Zeichen sein (nur Großbuchstaben).

10. Klicken Sie auf Zertifikatsignierungsanforderung herunterladen.

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... **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: No file chosen

11. Klicken Sie auf Senden.

12. Klicken Sie auf Änderungen bestätigen, um die Änderungen anzuwenden.

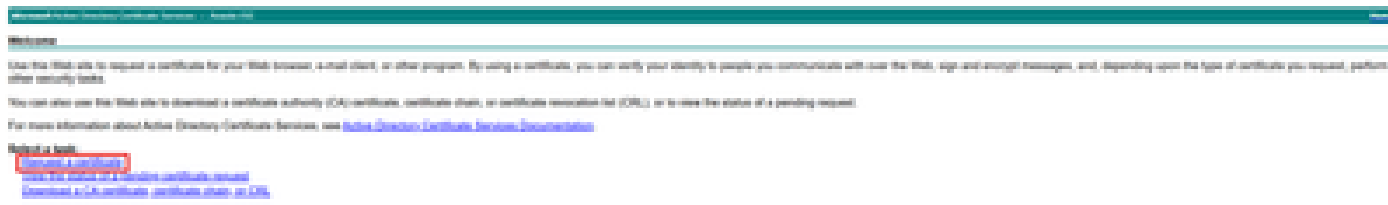


Warnung: Wenn Sie die erwähnten Änderungen nicht übermitteln und bestätigen und das signierte Zertifikat direkt hochladen und bestätigen, können Sie während der Integration Probleme bekommen.

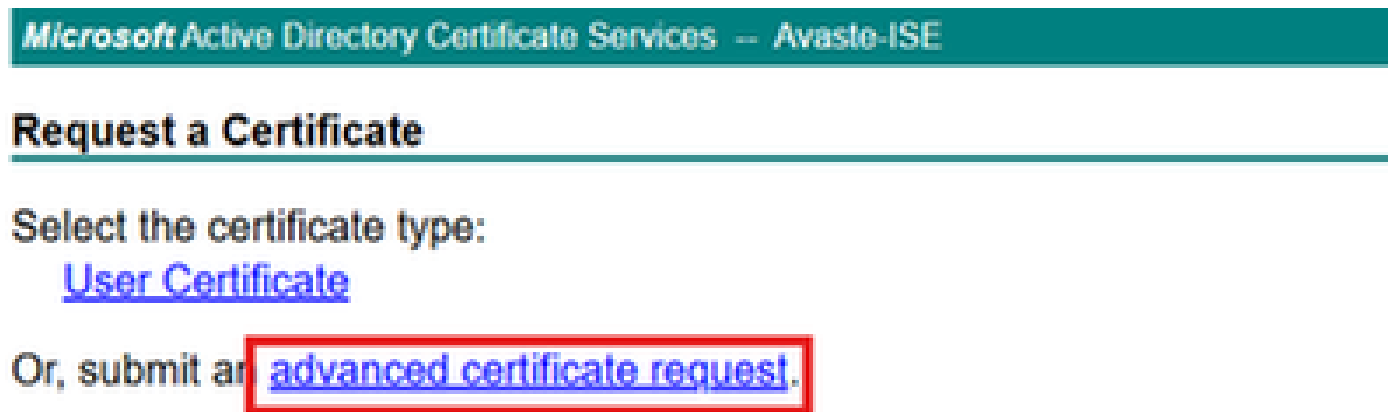
Abschnitt B: Signieren eines WSA-Client-CSR mithilfe einer externen Zertifizierungsstelle

1. Navigieren Sie zu MS Active Directory Certificate Service, <https://server/certsrv/>, wobei server die IP-Adresse oder der DNS des MS-Servers ist.

2. ClickRequest ein Zertifikat.

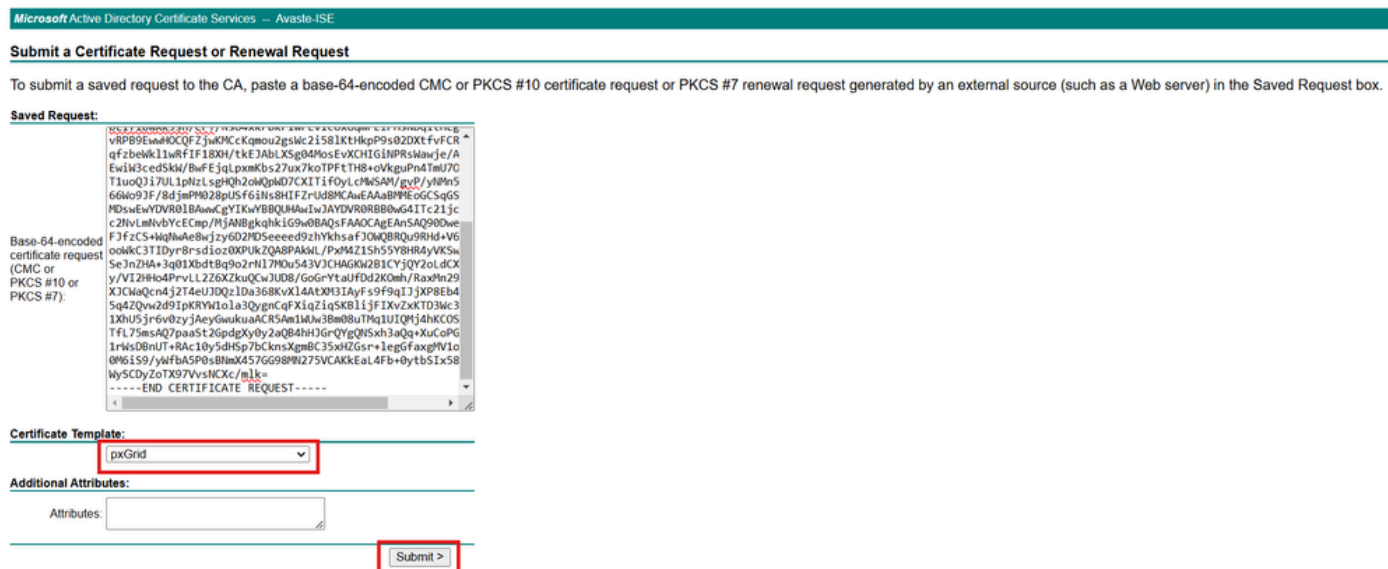


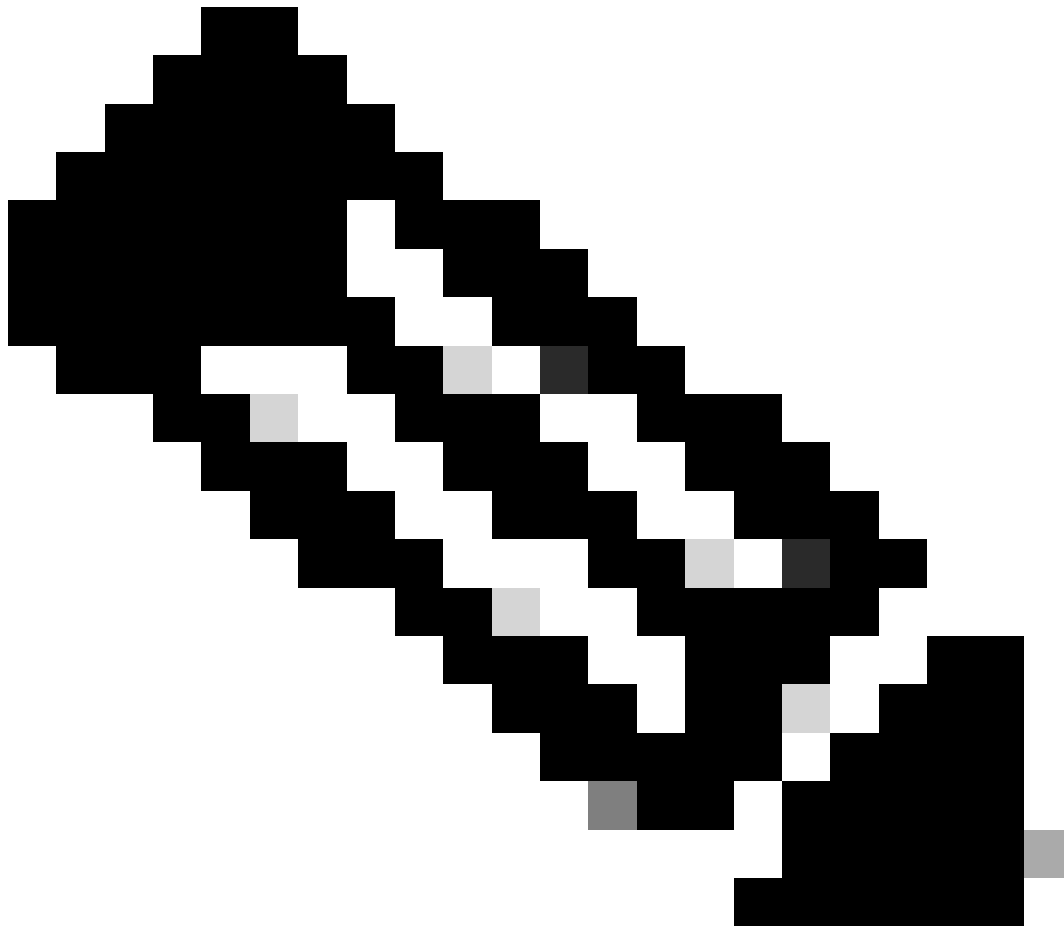
3. Wählen Sie diese Option, um eine Anforderung für ein erweitertes Zertifikat zu senden.



4. Kopieren Sie den Inhalt des im vorherigen Abschnitt erstellten CSR in das Feld "Gespeicherte Anforderung".

5. Wählen Sie pxGrids Zertifikatvorlage aus, und klicken Sie dann auf Senden.





Anmerkung: Anmerkung: Die verwendete Zertifikatvorlage pxGrid erfordert sowohl die Client- als auch die Serverauthentifizierung im Feld "Enhanced Key Usage" (Erweiterte Schlüsselerwendung).

6. Laden Sie das generierte Zertifikat im Base-64-Format herunter und speichern Sie es 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](#)

Abschnitt C: Bindung des WSA-Clientzertifikats an die Zertifikatsanforderung (Certificate Signing Request, CSR) und Integration

1. Navigieren Sie zur Web Security Appliance (WSA)-GUI.
2. Navigieren Sie zu Netzwerk > Identifikationsservices > Identifikationsservice-Engine.
3. Klicken Sie auf Einstellungen bearbeiten.
4. Navigieren Sie zum Abschnitt Web Appliance Client Certificate.
5. Under the signed certificate section, Upload the signed certificate 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: WSA-Client.cer.cer

6. Klicken Sie auf Senden.

7. Klicken Sie auf Änderungen bestätigen, um die Änderungen anzuwenden.

8. Klicken Sie auf Einstellungen bearbeiten.

9. Scrollen Sie zu Kommunikation mit ISE-Knoten testen und klicken Sie auf Test starten, was folgendermaßen aussehen kann:

Testen der Kommunikation mit ISE-Knoten

Testen der Kommunikation mit ISE-Knoten

```
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.
```

Überprüfung

Navigieren Sie auf der Cisco ISE zu Administration > pxGrid Services > Client Management > Clients.

Dadurch wird die WSA als pxgrid-Client mit dem Status Enabled generiert.

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 shows a table of 'pxGrid Clients'. The table has columns for Name, Description, Client Groups, and Status. One client is listed: 'wsabglzsc.com_iseid' with description 'ISEID' and status 'Enabled'. The status 'Enabled' is highlighted with a green box.

Name	Description	Client Groups	Status
wsabglzsc.com_iseid	ISEID		Enabled

Um das Themenabonnement auf der Cisco ISE zu überprüfen, navigieren Sie zu Administration >pxGrid Services > Diagnostics > WebSocket > Clients:

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
```

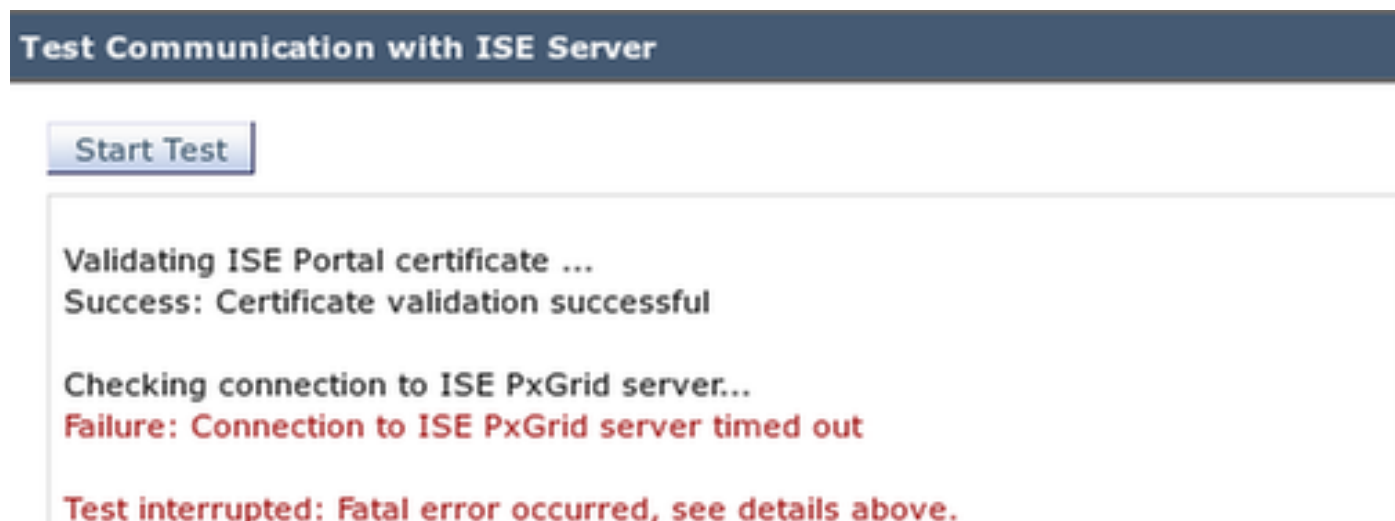


```
TRACE [Thread-10][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::::- Received frame=[command=S
TRACE [Thread-10][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::::- Authorized to send (cached
```

Fehlerbehebung

Problem

Unbekanntes CA-Problem. Auf der WSA schlägt der Test für die ISE-Verbindung mit Fehler fehl. Fehler:
Zeitüberschreitung bei der Verbindung mit dem ISE-PxGrid-Server.



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
```

Der Grund für den Fehler wird bei der Paketerfassung deutlich.

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

Lösung

1. Stellen Sie sicher, dass das signierte Web-Appliance-Zertifikat erfolgreich an die WSA gebunden ist und die Änderungen bestätigt wurden.
2. Stellen Sie sicher, dass der Aussteller oder das Zertifikat der Stammzertifizierungsstelle des WSA-Client-Zertifikats Teil des Trusted Store auf der Cisco ISE ist.

Bekannte Fehler

Cisco Bug-ID	Beschreibung
Cisco Bug-ID: 23986	Pxgrid getUserGroups API-Anforderung gibt eine leere Antwort zurück.
Cisco Bug-ID: 77321	Die WSA empfängt SIDs anstelle von AD-Gruppen von der ISE.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.