

Integrate ISE 3.3 with WSA Using External CA

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Section A: Cisco Identity Services Engine 3.3 Certificate Configuration](#)

[Step 1: Generate an ISE Server pxGrid Certificate](#)

[Step 2: Create an ISE Server pxGrid Certificate Using an External CA](#)

[Step 3: Import the CA Root Certificate into the ISE Trust Store](#)

[Step 4: Binding the ISE certificate to the Certificate Signing Request \(CSR\).](#)

[Section B: Adding CA Root Certificate to WSA Certificate Trust Store](#)

[Integration](#)

[Section A: Enable WSA for ISE integration and generate CSR for WSA Client Certificate.](#)

[Section B: Sign an WSA client CSR Using an External CA](#)

[Section C: Binding the WSA client certificate to the Certificate Signing Request \(CSR\) and integrating.](#)

[Verify](#)

[Troubleshooting](#)

[Problem](#)

[Solution](#)

[Known Defects](#)

Introduction

This document describes procedures to integrate ISE 3.3 with Cisco Secure Web Appliance (WSA) using pxGrid connections.

Prerequisites

Requirements

Cisco recommends knowledge in these topics:

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

Components Used

The information in this document is based on these software and hardware versions:

- Identity Services Engine (ISE) version 3.3 patch 4
- Cisco Secure Web Appliance version 15.2.0-116

- Windows server 2016 as an External Certificate Authority (CA) server.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

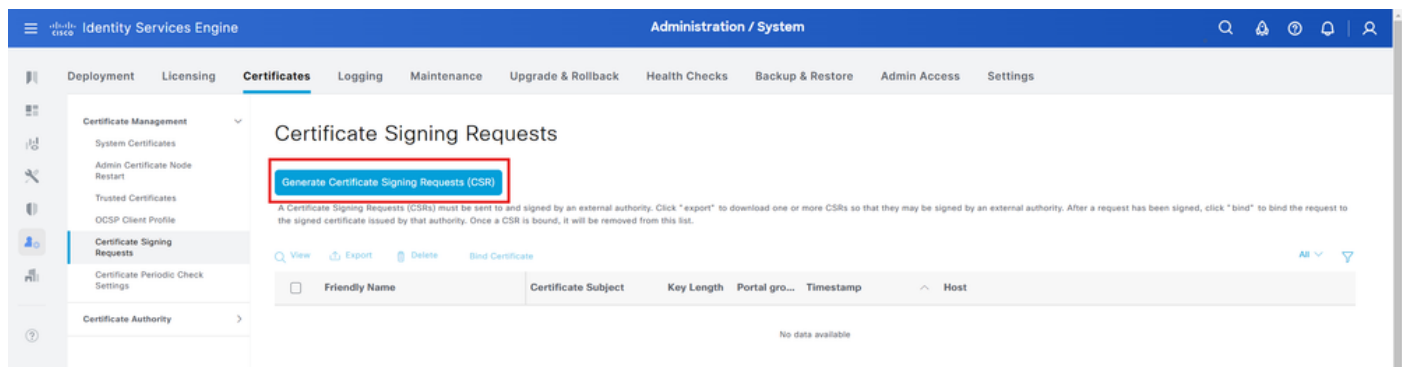
Configure

Section A: Cisco Identity Services Engine 3.3 Certificate Configuration

Step 1: Generate an ISE Server pxGrid Certificate

Generate a CSR for an ISE server pxGrid certificate:

1. **Log into** Cisco Identity Services Engine (ISE) GUI.
2. **Navigate to** **Administration > System > Certificates > Certificate Management > Certificate Signing Requests**.
3. Select **Generate Certificate Signing Request (CSR)**.



4. Select **pxGrid** in the Certificate(s) is used for field.
5. Select **ISE node** for which the certificate is generated.
6. **Fill in** other certificates details as necessary.
7. Click **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

: Certificate Template pxGrid used needs both Client authentication and server authentication in the Enhanced Key Usage field.

6. **Download** the generated certificate in **Base-64** format and **Save** it as 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](#)

Step 3: Import the CA Root Certificate into the ISE Trust Store

1. **Navigate** to MS Active Directory Certificate Service home page and select **Download a CA certificate, certificate chain, or 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](#)

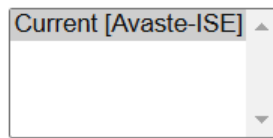
2. Select **Base-64** format, then click **Download** CA certificate.

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](#)

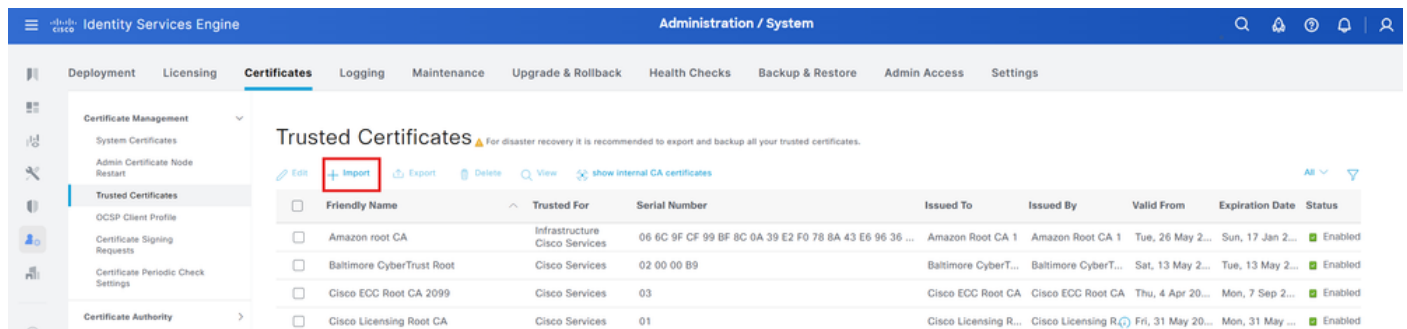
[Download latest base CRL](#)

[Download latest delta CRL](#)

3. Save the certificate as CA_Root.cer.

4. Log into Cisco Identity Services Engine (ISE) GUI.

5. Select **Administration > System > Certificates > Certificate Management > Trusted Certificates**.



The screenshot shows the Cisco Identity Services Engine (ISE) GUI. The top navigation bar includes 'Administration / System'. The left sidebar shows the 'Certificates' menu with 'Trusted Certificates' selected. The main content area displays a table of 'Trusted 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. Select **Import > Certificate file** and **Import** the root certificate.

7. Ensure the **Trust for authentication within ISE** check box is selected.

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. Click **Submit**.

Step 4: Binding the ISE certificate to the Certificate Signing Request (CSR).

1. **Log** into Cisco Identity Services Engine (ISE) GUI.

2. Select **Administration > System > Certificates > Certificate Management > Certificate Signing Requests**.

3. Select the CSR generated in the previous section, then click **Bind Certificate**.

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
☒	ise33@pxGrid	CN=ise33.lab.local,OU=...	4096		Wed, 19 Mar 2025	ise33

4. On the Bind CA Signed Certificate form, **choose** the ISE_pxGrid.cer certificate generated previously.

5. Give the certificate a friendly name, then click **Submit**.

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. Click **Yes** if the system asks to replace the certificate.

8. Select **Administration > System > Certificates > System Certificates**.

9. You can see the created pxGrid certificate signed by the external CA in the list.

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 table of certificates. The table has columns: Friendly Name, Used By, Portal group tag, Issued To, Issued By, Valid From, Expiration Date, and Status. The 'ISE-pxGRID' certificate is highlighted with a green box. It is issued by 'Avast-ISE' and is currently 'Active'.

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, CN=ISE Messaging Service 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	Avast-ISE	Wed, 19 Mar 2025	Fri, 19 Mar 2027	Active

Section B: Adding CA Root Certificate to WSA Certificate Trust Store

Add CA Root Certificate to WSA Trusted Store:

1. **Log** into Web Security Appliance (WSA) GUI.
2. **Navigate** to **Network > Certificate Management > Manage Trusted Root Certificates**.

Network

System

Interfaces

Transparent Redirection

Routes

DNS

High Availability

Internal SMTP Relay

Upstream Proxy

External DLP Servers

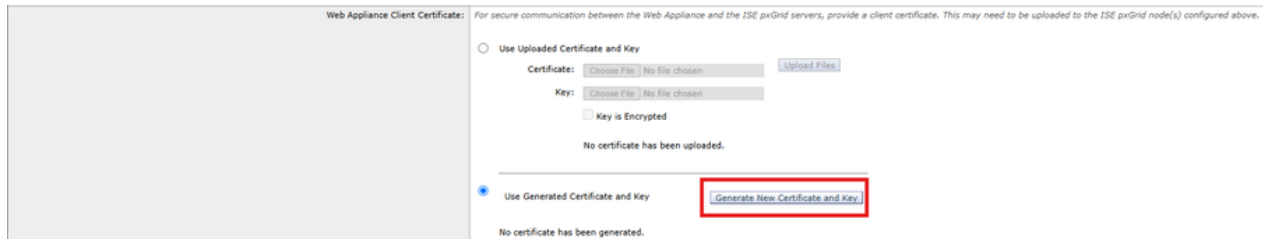
Web Traffic Tap

Certificate Management

Cloud Services Settings

: There can be only two pxGrid nodes per ISE deployment. This serves as a pxGrid Active-Standby configuration; only one ISE+pxGrid node can be active at a time. In a pxGrid Active-Standby configuration, all information is passed through the PPAN, where the second ISE+pxGrid node remains inactive.

8. **Scroll** to the Web Appliance Client Certificate section and click **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

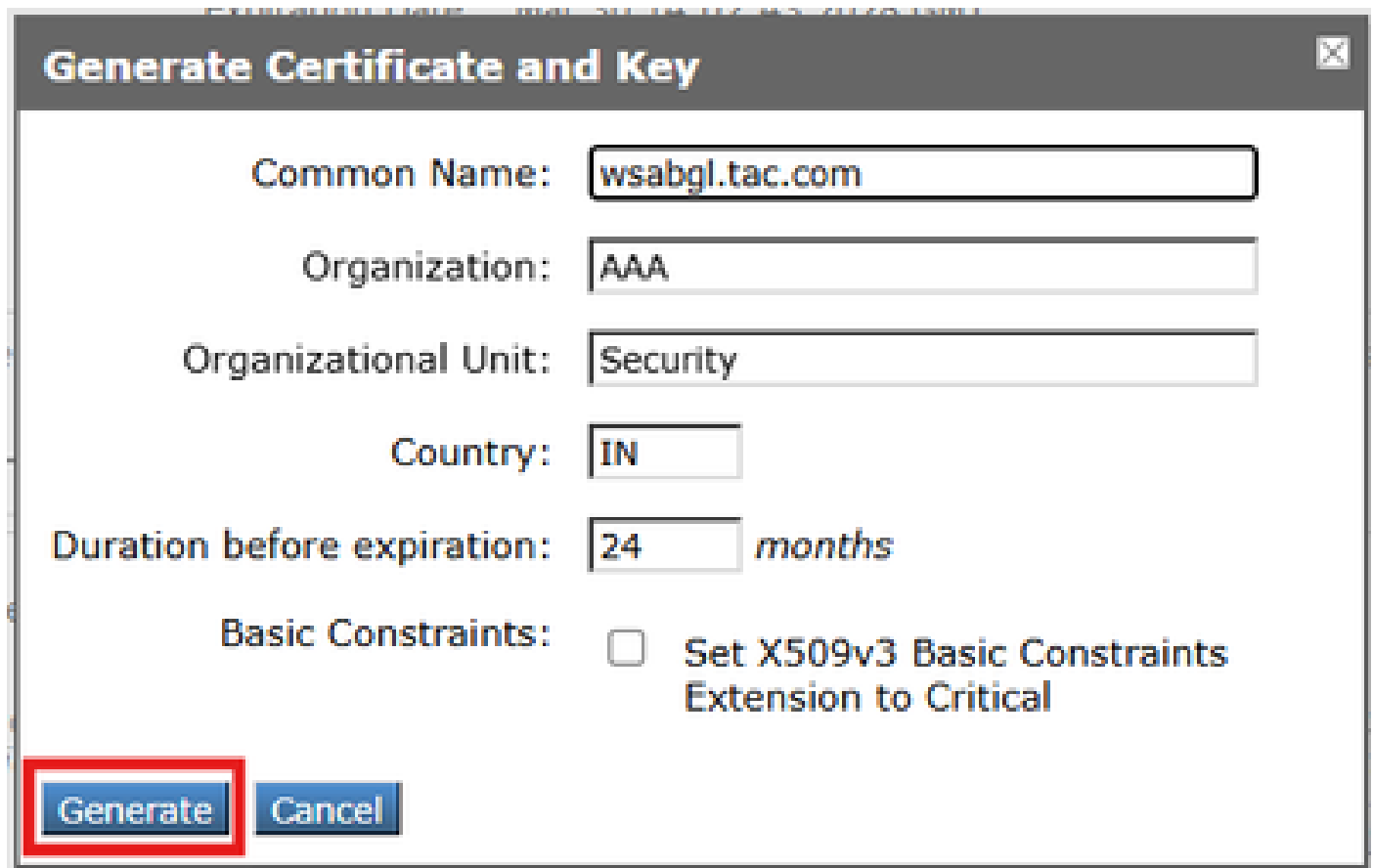
☐ Key is Encrypted

No certificate has been uploaded.

☒ Use Generated Certificate and Key

No certificate has been generated.

9. **Fill in** certificate details as necessary and **Click Generate**.



Generate Certificate and Key

Common Name:

Organization:

Organizational Unit:

Country:

Duration before expiration: months

Basic Constraints: ☐ Set X509v3 Basic Constraints Extension to Critical



Note: Duration of certificate must be an integer between 24 and 60 months and Country must be a ISO two character country code (uppercase letters only).

10. Click Download Certificate Signing Request.

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. Click Submit.

12. Click **Commit Changes** to Apply the changes.

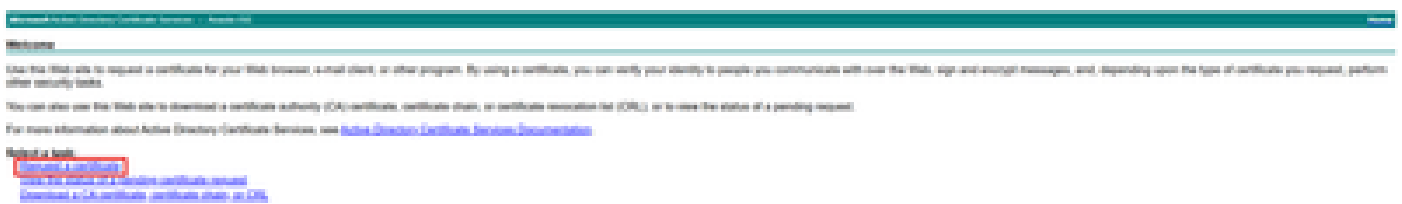


Warning: If you do not submit and commit mentioned changes and directly upload the signed certificate and perform commit, you can face issues during the integration.

Section B: Sign an WSA client CSR Using an External CA

1. Navigate to **MS Active Directory Certificate Service**, <https://server/certsrv/>, where server is IP or DNS of your MS Server.

2. Click **Request a certificate**.



3. Choose to submit an **advanced certificate request**.

User Certificate

Or, submit an [advanced certificate request](#).

- Microsoft Active Directory Certificate Services – Avast-ISE

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

[illegible]

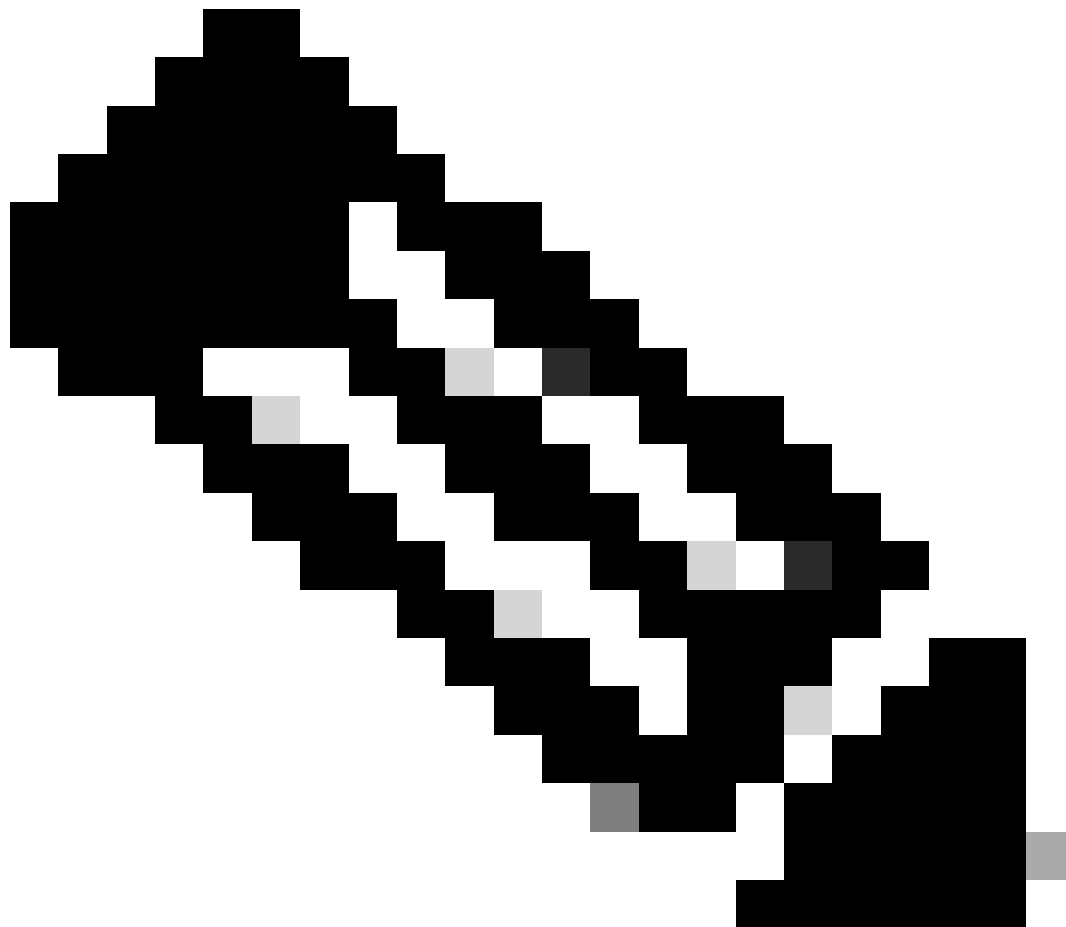
Certificate Template:

pxGrid

Additional Attributes:

Attributes

Submit >



Note: Note: Certificate Template pxGrid used needs both Client authentication and server authentication in the Enhanced Key Usage field.

6. **Download** the generated certificate in **Base-64** format and **Save** it as WSA-Client.cer.

Microsoft Active Directory Certificate Services -- Avaste-ISE

Certificate Issued

The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

Section C: Binding the WSA client certificate to the Certificate Signing Request (CSR) and integrating.

1. **Navigate** to Web Security Appliance (WSA) GUI.
2. **Navigate** to **Network > Identification Services > Identification Service Engine**.
3. Click **Edit Settings**.
4. **Navigate** to **Web Appliance Client Certificate** section.
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. Click **Submit**.
7. Click **Commit Changes** to Apply the changes.
8. Click **Edit Settings**.
9. **Scroll** to **Test Communication with ISE Nodes** and click **Start Test**, which can result as follows:

Test Communication with ISE Nodes

Test Communication with ISE Nodes

```
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.
```

Verify

On Cisco ISE, navigate to **Administration > pxGrid Services > Client Management > Clients**.

This generates the WSA as a pxgrid client with the status **Enabled**.

The screenshot shows the Cisco ISE Administration interface for pxGrid Services. 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 'Administration / pxGrid Services' and includes tabs for Summary, Client Management (selected), Diagnostics, and Settings. Under Client Management, there are sub-tabs for Clients, Policy, Groups, Certificates, pxGrid Cloud Connection, and pxGrid Cloud Policy. The 'Clients' sub-tab is active, displaying a table of pxGrid Clients. The table has columns for Name, Description, Client Groups, and Status. A single client is listed: 'wsabgl.tac.com_ised' with description 'ISED' and status 'Enabled'. The status is highlighted with a green box.

Name	Description	Client Groups	Status
wsabgl.tac.com_ised	ISED		Enabled

To verify topic subscription on Cisco ISE, navigate to **Administration > pxGrid Services > Diagnostics > Websocket > Clients**:

The screenshot shows the Cisco ISE Administration interface for pxGrid Services. The left sidebar is the same as the previous screenshot. The main content area is titled 'Administration / pxGrid Services' and includes tabs for Summary, Client Management, Diagnostics (selected), and Settings. Under Diagnostics, there are sub-tabs for WebSocket, Log, and Tests. The 'WebSocket' sub-tab is active, displaying a table of WebSocket Clients. The table has columns for Client Name, Connect To, Session Id, Certificate, and Subscriptions. The last two rows of the table are highlighted with a green box.

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,~1
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 (cache
```

Troubleshooting

Problem

Unknown CA Issue, On the WSA the test for ISE connection fails with error. Failure: Connection to ISE PxGrid server timed out.

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
```

The reason for the failure can be seen with packet captures,

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	TLSh1.2	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	TLSh1.2	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	TLSh1.2	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	TLSh1.2	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

Solution

1. Ensure the Web Appliance signed certificate is bind successfully on the WSA and changes have been committed.
2. Ensure the issuer or the Root CA certificate of WSA Client certificate is part of Trusted Store on Cisco ISE.

Known Defects

Cisco Bug ID	Description
Cisco bug ID 23986	Pxgrid getUserGroups API request return empty response.
Cisco bug ID 77321	WSA receives SIDs instead of AD groups from ISE.