

使用外部CA将ISE 3.3与WSA集成

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[A 部分：思科身份服务引擎3.3证书配置](#)

[步骤 1：生成anISEServer pxGrid证书](#)

[步骤 2：使用外部CA创建ISE服务器pxGrid证书](#)

[步骤 3：将CA根证书导入ISE信任存储](#)

[步骤 4：将ISE证书绑定到证书签名请求\(CSR\)。](#)

[B 部分：将CA根证书添加到WSA证书信任库](#)

[集成](#)

[A 部分：启用WSA for ISE集成并为WSA客户端证书生成CSR。](#)

[B 部分：使用外部CA签署WSA客户端CSR](#)

[C 部分：将WSA客户端证书绑定到证书签名请求\(CSR\)并集成。](#)

[验证](#)

[故障排除](#)

[问题](#)

[解决方案](#)

[已知缺陷](#)

简介

本文档介绍使用pxGrid连接将ISE 3.3与思科安全Web设备(WSA)集成的过程。

先决条件

要求

思科建议了解以下主题：

- 身份服务引擎
- 思科安全Web设备(WSA)
- 平台交换网格(pxGrid)
- TLS/SSL证书。
- Windows Server 2016上的PKI

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 身份服务引擎(ISE)版本3.3补丁4
- 思科安全Web设备版本15.2.0-116
- Windows server 2016作为外部证书颁发机构(CA)服务器。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

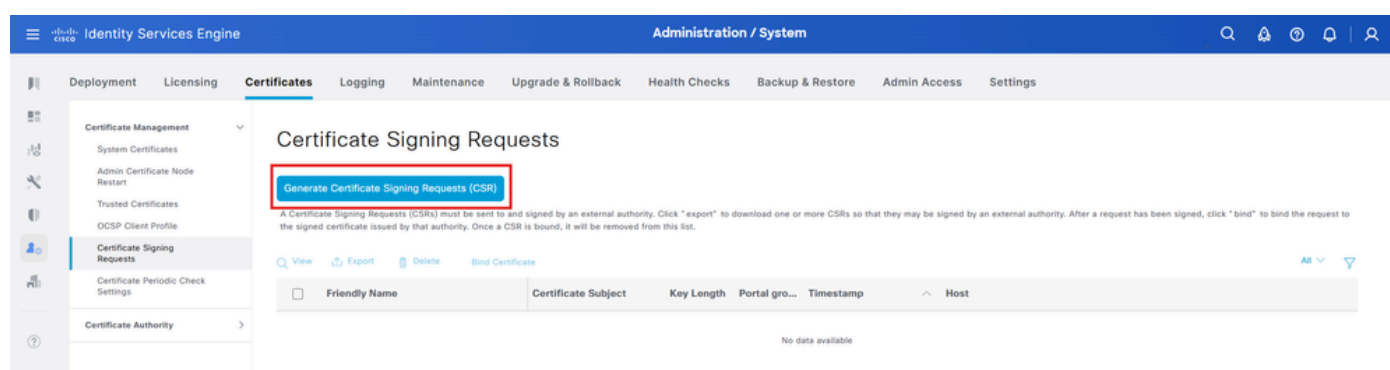
配置

A 部分：思科身份服务引擎3.3证书配置

步骤 1：生成anISEServer pxGrid证书

为ISE服务器pxGrid证书生成CSR:

- 1.登录思科身份服务引擎(ISE)GUI。
- 2.Navigate to Administration > System > Certificates > Certificate Management > Certificate Signing Requests。
- 3.选择生成证书签名请求(CSR)。



- 4.选择Certificate(s)is used for field.
5. Select ISE节点为其生成证书。
- 6.根据需要填写其他证书详细信息。
- 7.单击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

2.导航到网络>证书管理>管理受信任的根证书。

Network

System

Interfaces

Transparent Redirection

Routes

DNS

High Availability

Internal SMTP Relay

Upstream Proxy

External DLP Servers

Web Traffic Tap

Certificate Management

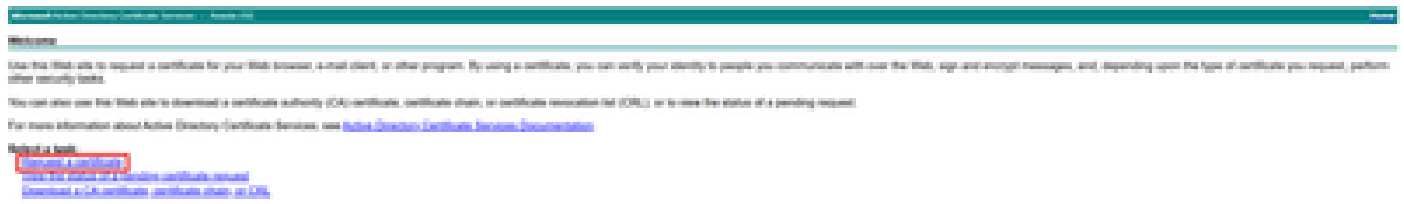
Cloud Services Settings

如果不提交和提交上述更改，并直接上传签名证书并执行提交，则可能会在集成期间遇到问题。

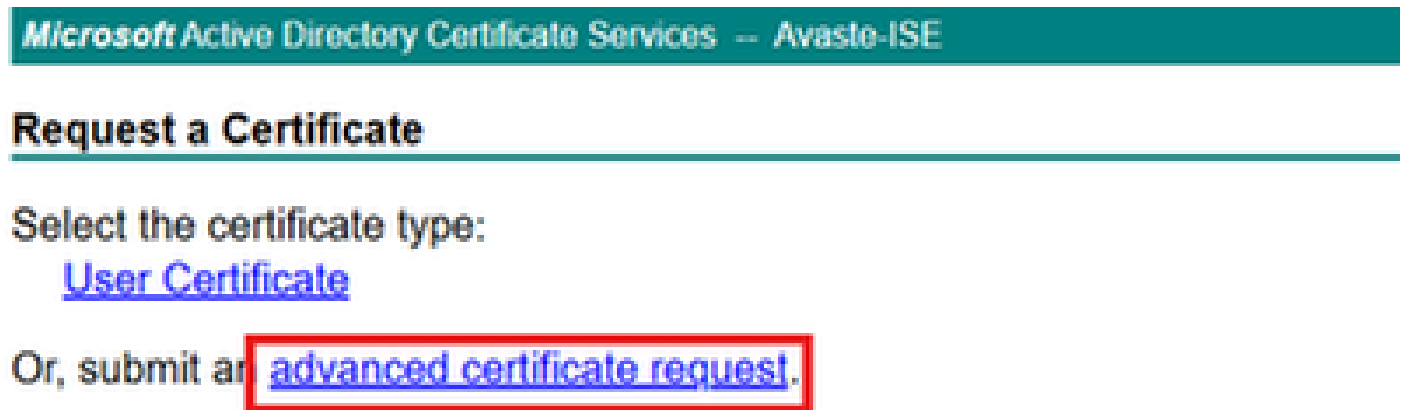
B 部分：使用外部CA签署WSA客户端CSR

1.导航到MS Active Directory证书服务,https://server/certsrv/，其中服务器是MS服务器的IP或DNS。

2.单击请求证书。

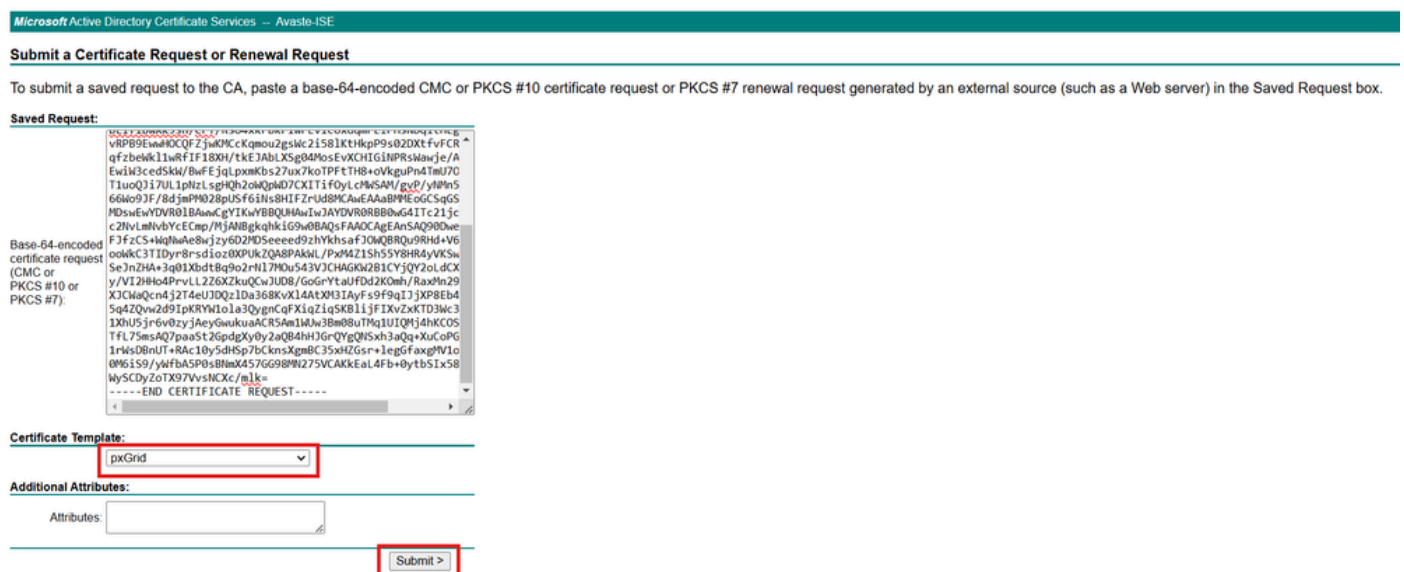


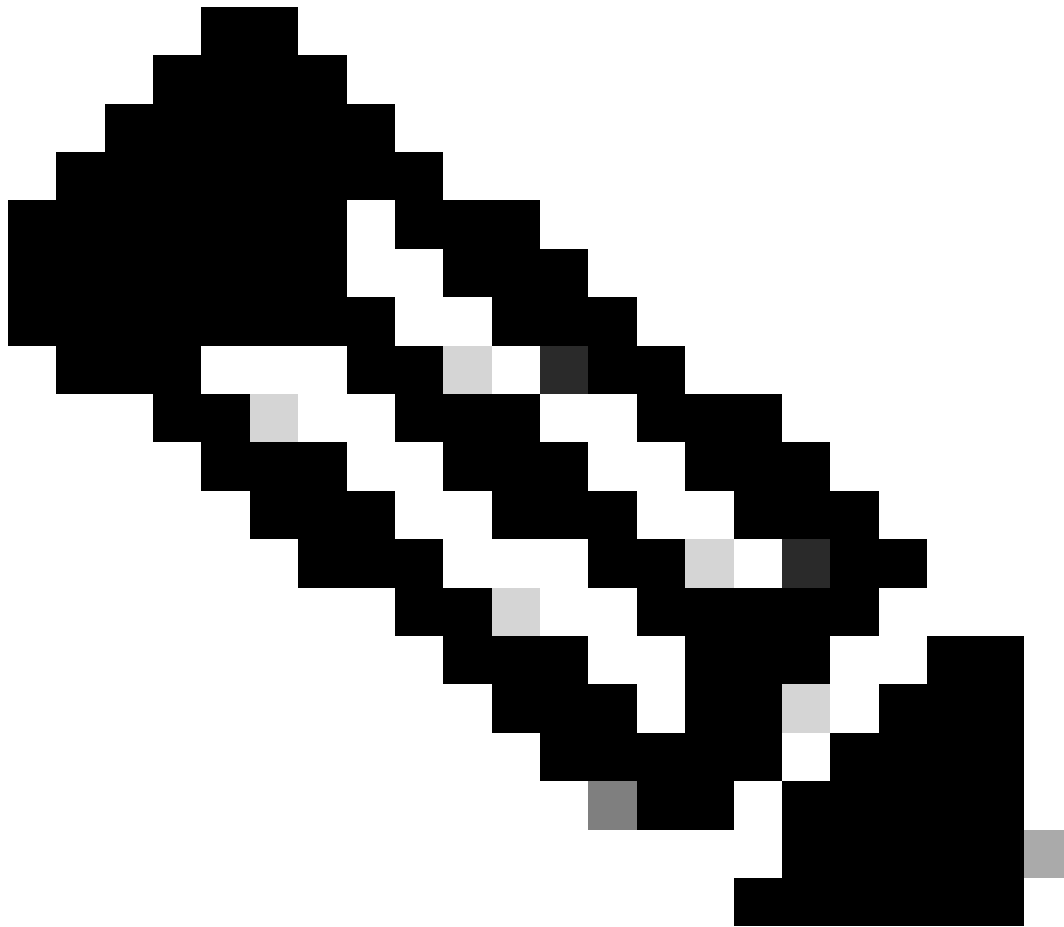
3.选择提交高级证书请求。



4.将上一部分中生成的CSR的内容复制到“保存的请求”(Saved Request)字段中。

5.选择Certificate Template，然后单击Submit。





注意：注意：使用的证书模板pxGrid需要在Enhanced Key Usage字段中同时进行客户端身份验证和服务器身份验证。

6. 下载生成的证书inBase-64format，并另存为WSA-Client.cer。

Certificate Issued

The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

C 部分：将WSA客户端证书绑定到证书签名请求(CSR)并集成。

- 1.导航至网络安全设备(WSA)GUI。
- 2.导航至网络>标识服务>标识服务引擎。
- 3.单击Edit Settings。
- 4.导航至Web设备客户端证书部分。
- 5.在签名证书部分下，上传签名证书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.单击Submit。

7.单击Commit Changes以应用更改。

8.单击“编辑设置”。

9.滚动到测试与ISE节点的通信，然后单击开始测试，结果可能如下所示：

测试与ISE节点的通信

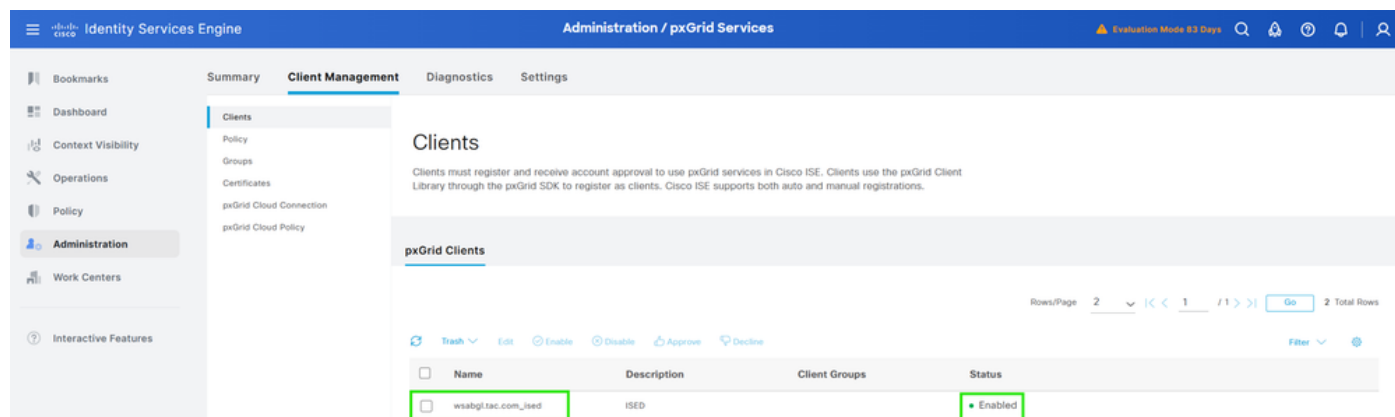
测试与ISE节点的通信

```
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.
```

验证

在Cisco ISE上，导航到管理>pxGrid服务>客户端管理>客户端。

这会将WSA生成为statusEnabled的pxgrid客户端。

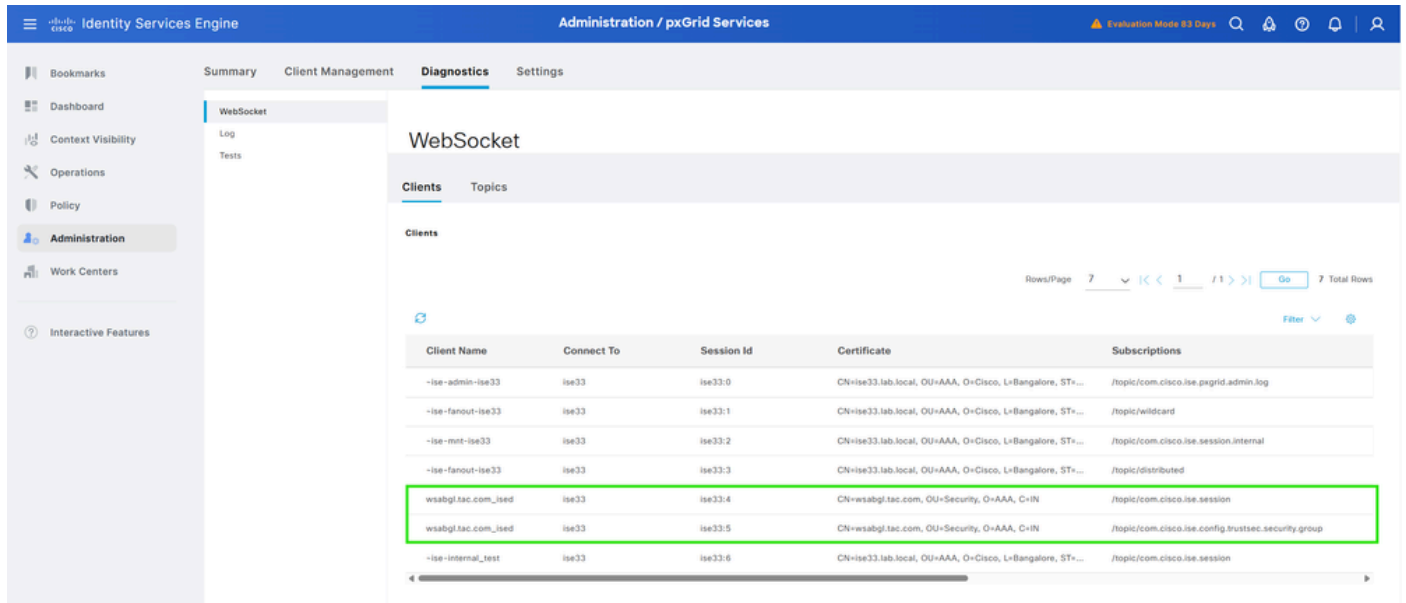


The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar indicates 'Administration / pxGrid Services'. The left sidebar shows the 'Administration' menu. The main content area is titled 'Clients' and displays a table of 'pxGrid Clients'. The table has columns for 'Name', 'Description', 'Client Groups', and 'Status'. A single client is listed: 'wsa@gt.tac.com_iseif' with a description of 'ISEF' and a status of 'Enabled'. The 'Status' column shows a green checkmark next to the word 'Enabled'.

Name	Description	Client Groups	Status
wsa@gt.tac.com_iseif	ISEF		Enabled

要验证思科ISE上的主题订用，请导航到管理(Administration)>pxGrid服务(pxGrid Services)>诊断(Diagnostics)>

Websocket >客户端(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. subscrip
TRACE [WsIseClientConnection-804][ ] cpm.pxgrid.ws.client.WsEndpoint -:::- Send. session=[id=34eae1
```

"wsabgl.lab.local_ised

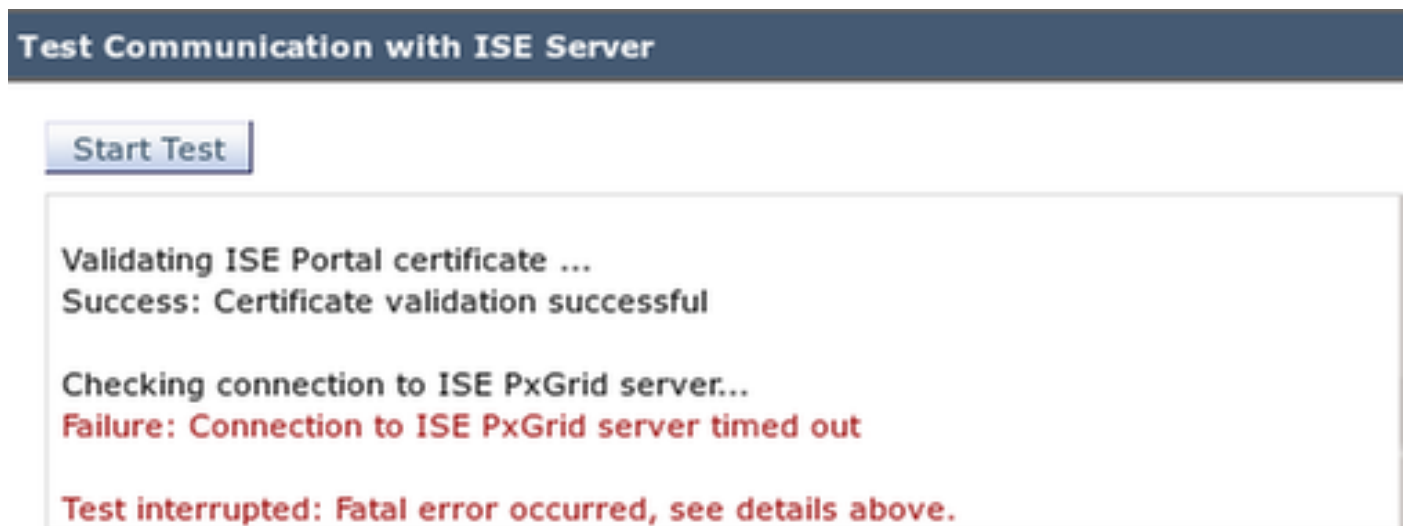
```
", "server":"wss://ise33.lab.local:8910/pxgrid/ise/pubsub", "message":"Pubsub subscribe. subscription\u003d
TRACE [Thread-3][ ] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::- Received frame=[command=SE
TRACE [Thread-3][ ] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::- Authorized to send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

故障排除

问题

未知的CA问题，在WSA上，ISE连接的测试失败并出现错误。故障：与ISE PxGrid服务器的连接超时。



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

故障原因可以通过数据包捕获看到，

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

解决方案

- 1.确保在WSA上成功绑定Web设备签名证书，并且已提交更改。
- 2.确保WSA客户端证书的颁发者或根CA证书是思科ISE上受信任存储的一部分。

已知缺陷

Cisco Bug ID	描述
思科漏洞ID 23986	Pxgrid getUserGroups API请求返回空响应。
思科漏洞ID 77321	WSA从ISE接收SID而不是AD组。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。