

使用外部CA將ISE 3.3與WSA整合

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[A部分：思科身分識別服務引擎3.3憑證組態](#)

[步驟 1:生成anISEServer pxGrid證書](#)

[步驟 2:使用外部CA建立ISE伺服器pxGrid證書](#)

[步驟 3:將CA根證書匯入ISE信任儲存](#)

[步驟 4:將ISE證書繫結到證書簽名請求\(CSR\)。](#)

[B部分：正在將CA根證書新增到WSA證書信任庫](#)

[整合](#)

[A部分：為ISE整合啟用WSA並為WSA客戶端證書生成CSR。](#)

[B部分：使用外部CA簽署WSA客戶端CSR](#)

[C部分：將WSA客戶端證書繫結到證書簽名請求\(CSR\)並整合。](#)

[驗證](#)

[疑難排解](#)

[問題](#)

[解決方案](#)

[已知瑕疵](#)

簡介

本文檔介紹使用pxGrid連線將ISE 3.3與思科安全網路裝置(WSA)整合的過程。

必要條件

需求

思科建議瞭解以下主題：

- 身分識別服務引擎
- Cisco Secure Web Appliance (WSA)
- 平台交換網格(pxGrid)
- TLS/SSL證書。
- Windows Server 2016上的PKI

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 身分識別服務引擎(ISE)版本3.3補丁4
- 思科安全Web裝置版本15.2.0-116
- Windows server 2016作為外部證書頒發機構(CA)伺服器。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

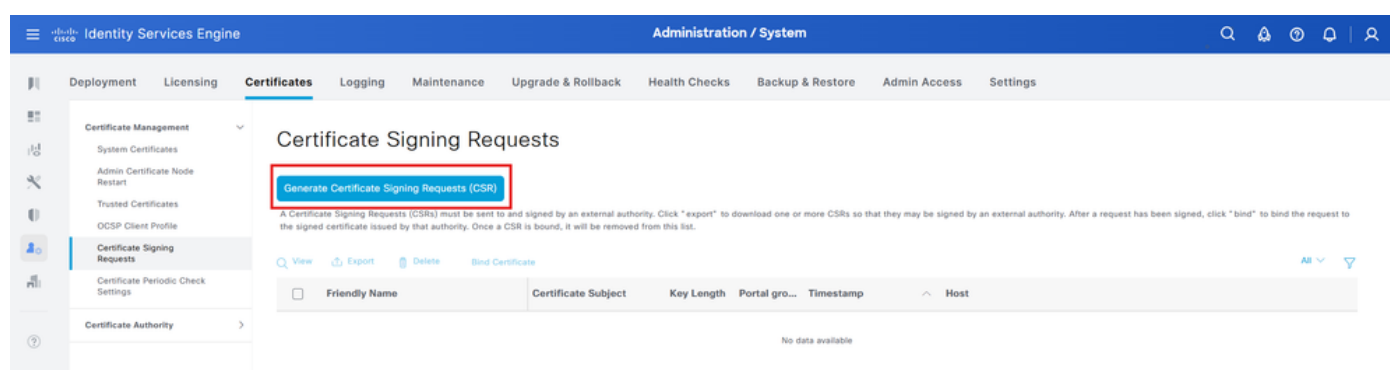
設定

A部分：思科身分識別服務引擎3.3憑證組態

步驟 1:生成anISEServer pxGrid證書

為ISE伺服器pxGrid證書生成CSR:

- 1.登入思科身分識別服務引擎(ISE)GUI。
- 2.導航到管理>系統>證書>證書管理>證書簽名請求。
- 3.選擇產生憑證簽署請求(CSR)。



- 4.選擇「使用證書」作為欄位。
5. SelectISE 節點為其生成證書。
- 6.根據需要填寫其他證書詳細資訊。
7. ClickGenerate。

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.導覽至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

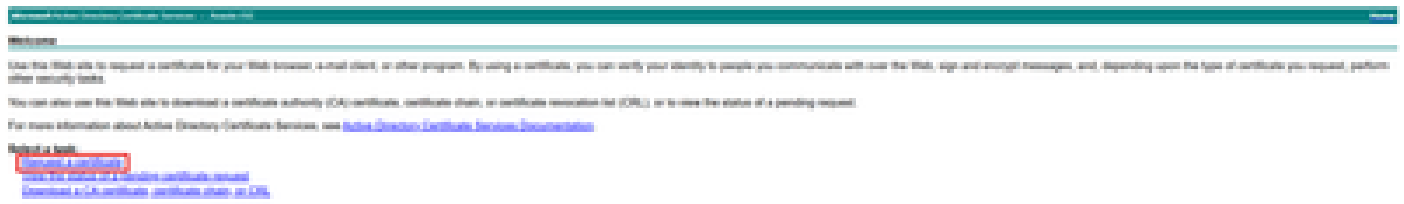
Cloud Services Settings

如果不提交和提交上述更改，並直接上傳簽名證書並執行提交，則整合過程中可能會遇到問題。

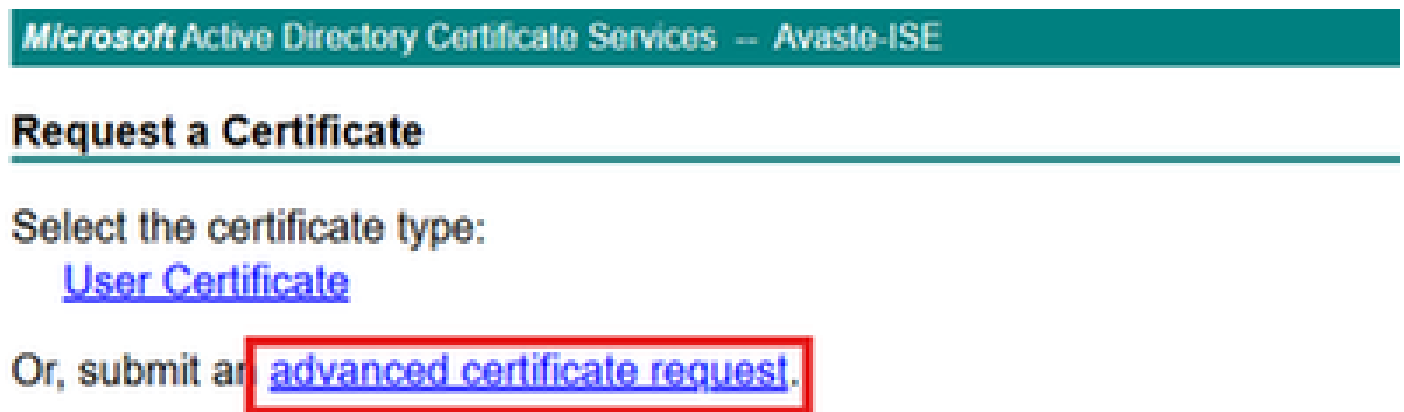
B部分：使用外部CA簽署WSA客戶端CSR

1. 導覽至MS Active Directory Certificate Service, <https://server/certsrv/>，其中伺服器是MS伺服器的IP或DNS。

2. ClickRequest證書。

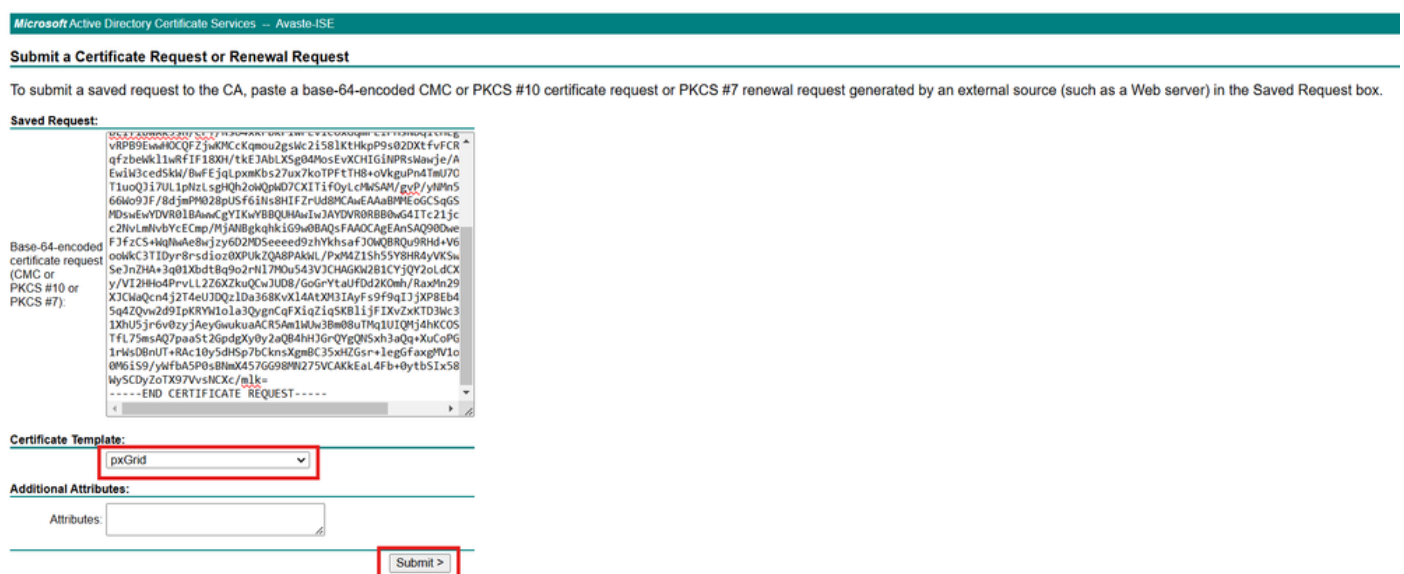


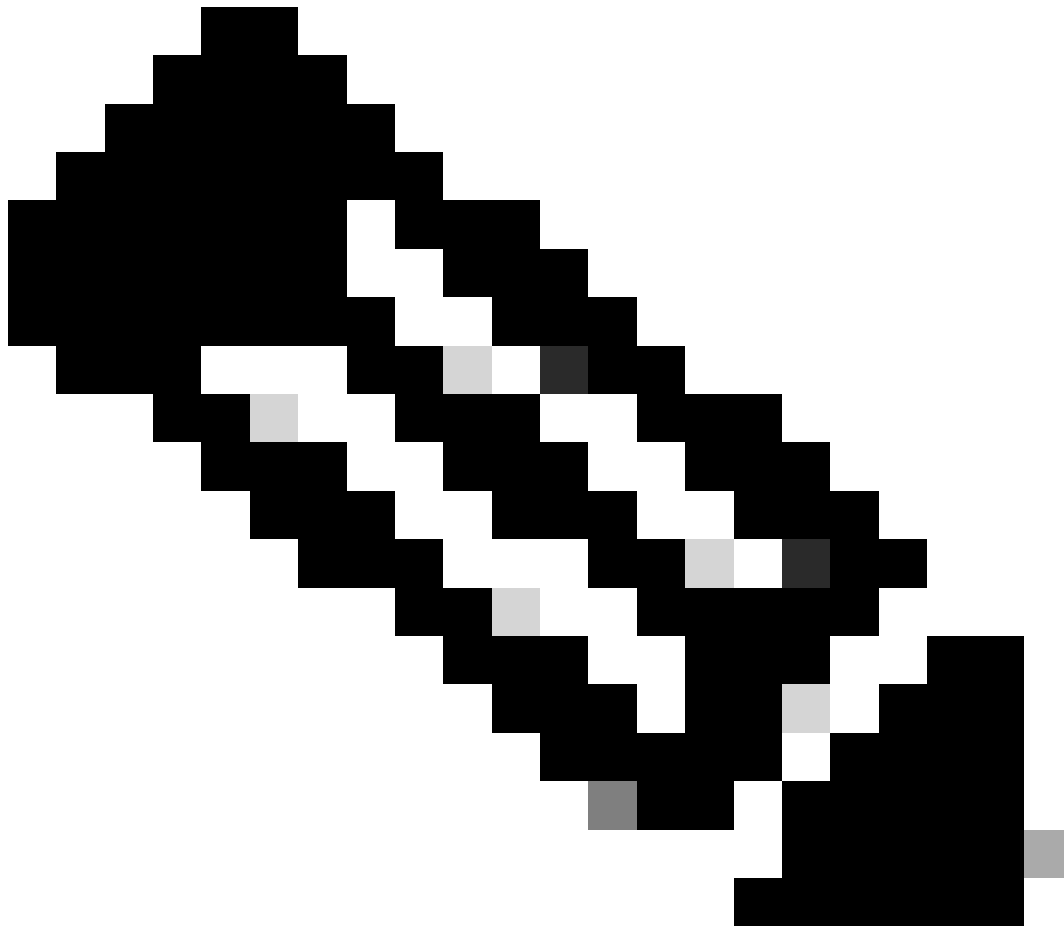
3. 選擇提交高級證書請求。



4. 將上一節中生成的CSR的內容複製到「儲存的請求」欄位中。

5. 選擇pxGrids證書模板，然後單擊Submit。





附註：附註：使用的證書模板pxGrid需要在Enhanced Key Usage欄位中同時進行客戶端身份驗證和伺服器身份驗證。

6. 下載生成的證書inBase-64format，並將其另存為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：將WSA客戶端證書繫結到證書簽名請求(CSR)並整合。

- 1.導航至網路安全裝置(WSA)GUI。
- 2.導覽至網路>識別服務>識別服務引擎。
- 3.按一下Edit Settings。
- 4.導覽至Web Appliance Client Certificate 部分。
- 5.在signed certificate部分下，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:

Choose File WSA-Client.cer.cer

Upload File

6.按一下Submit。

7.按一下提交更改以應用更改。

8.單擊「編輯設定」。

9.滾動到測試與ISE節點的通訊，然後按一下開始測試，結果如下：

測試與ISE節點的通訊

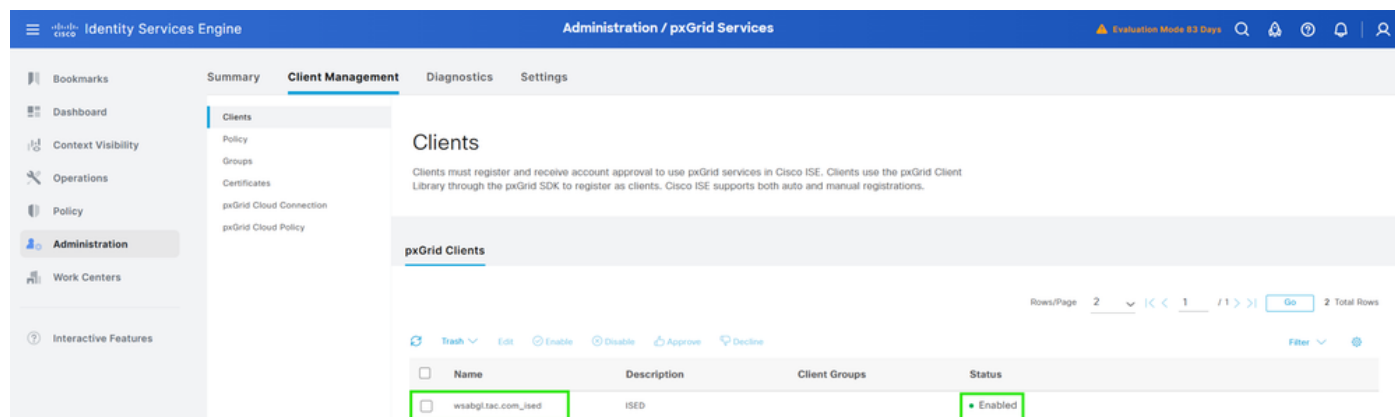
測試與ISE節點的通訊

```
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.
```

驗證

在Cisco ISE上，導航到管理>pxGrid Services >客戶端管理>客戶端。

這會將WSA生成為statusEnabled的pxgrid客戶端。



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 includes a sub-header 'pxGrid Clients'. Below this, there is a table with the following columns: Name, Description, Client Groups, and Status. The table contains one entry: 'wsa@gl.tac.com_iseif' with a description of 'ISEP' and a status of 'Enabled'. The status is highlighted with a green box.

Name	Description	Client Groups	Status
wsa@gl.tac.com_iseif	ISEP		Enabled

要驗證思科ISE上的主題訂閱，請導覽至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-mint-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 (cache
```

疑難排解

問題

未知CA問題，在WSA上，ISE連線測試失敗，出現錯誤。失敗：與ISE PxGrid伺服器的連線超時。

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
```

使用封包擷取可以看出失敗的原因，

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

解決方案

- 1.確保Web裝置簽名證書在WSA上成功繫結且已提交更改。
- 2.確保WSA客戶端證書的頒發者或根CA證書是思科ISE上的受信任儲存的一部分。

已知瑕疵

思科錯誤 ID	說明
思科錯誤ID 23986	Pxgrid getUserGroups API請求返回空響應。
思科錯誤ID 77321	WSA從ISE接收SID而不是AD組。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。