외부 CA를 사용하여 ISE 3.3을 WSA와 통합

목차

소개

이 문서에서는 pxGrid 연결을 사용하여 ISE 3.3을 Cisco WSA(Secure Web Appliance)와 통합하는 절차에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- ISE(Identity Services Engine)
- Cisco WSA(Secure Web Appliance)
- 플랫폼 교환 그리드(pxGrid)
- TLS/SSL 인증서
- Windows Server 2016의 PKI

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ISE(Identity Services Engine) 버전 3.3 패치 4
- Cisco Secure Web Appliance 버전 15.2.0-116
- 외부 CA(Certificate Authority) 서버로서의 Windows Server 2016.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

섹션 A: Cisco Identity Services Engine 3.3 인증서 구성

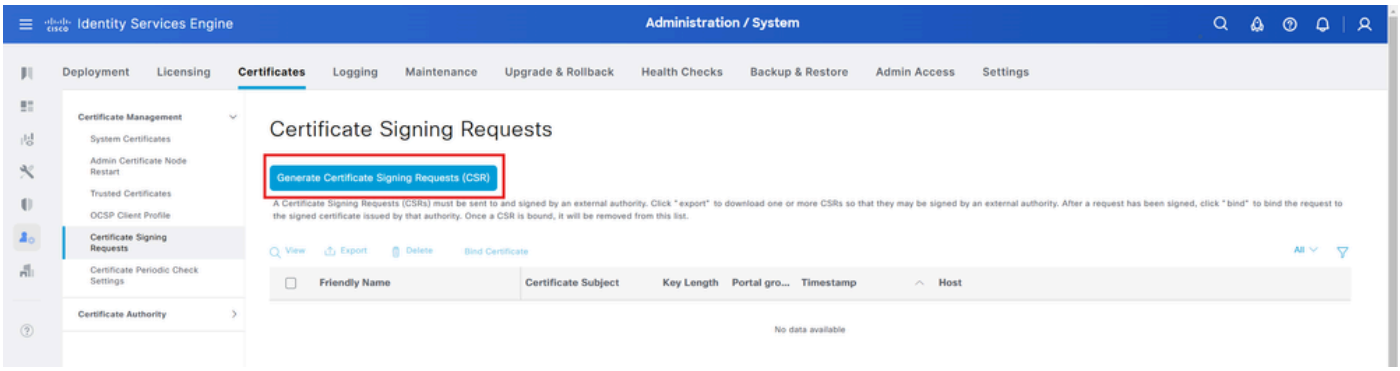
1단계: ISEServer pxGrid 인증서 생성

ISE 서버 pxGrid 인증서에 대한 CSR을 생성합니다.

1. Cisco ISE(Identity Services Engine) GUI에 로그인합니다.

2.Administration(관리) > System(시스템) > Certificates(인증서) > Certificate Management(인증서 관리) > Certificate Signing Requests(인증서 서명 요청)로 이동합니다.

3. CSR(Certificate Signing Request) 생성을 선택합니다.



4. 인증서는 필드에 사용됨을 선택합니다.

5. 인증서가 생성되는 ISE 노드를 선택합니다.

6. 그 밖에 필요한 증명서의 내용을 적는 행위

7. 생성을 클릭합니다.

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

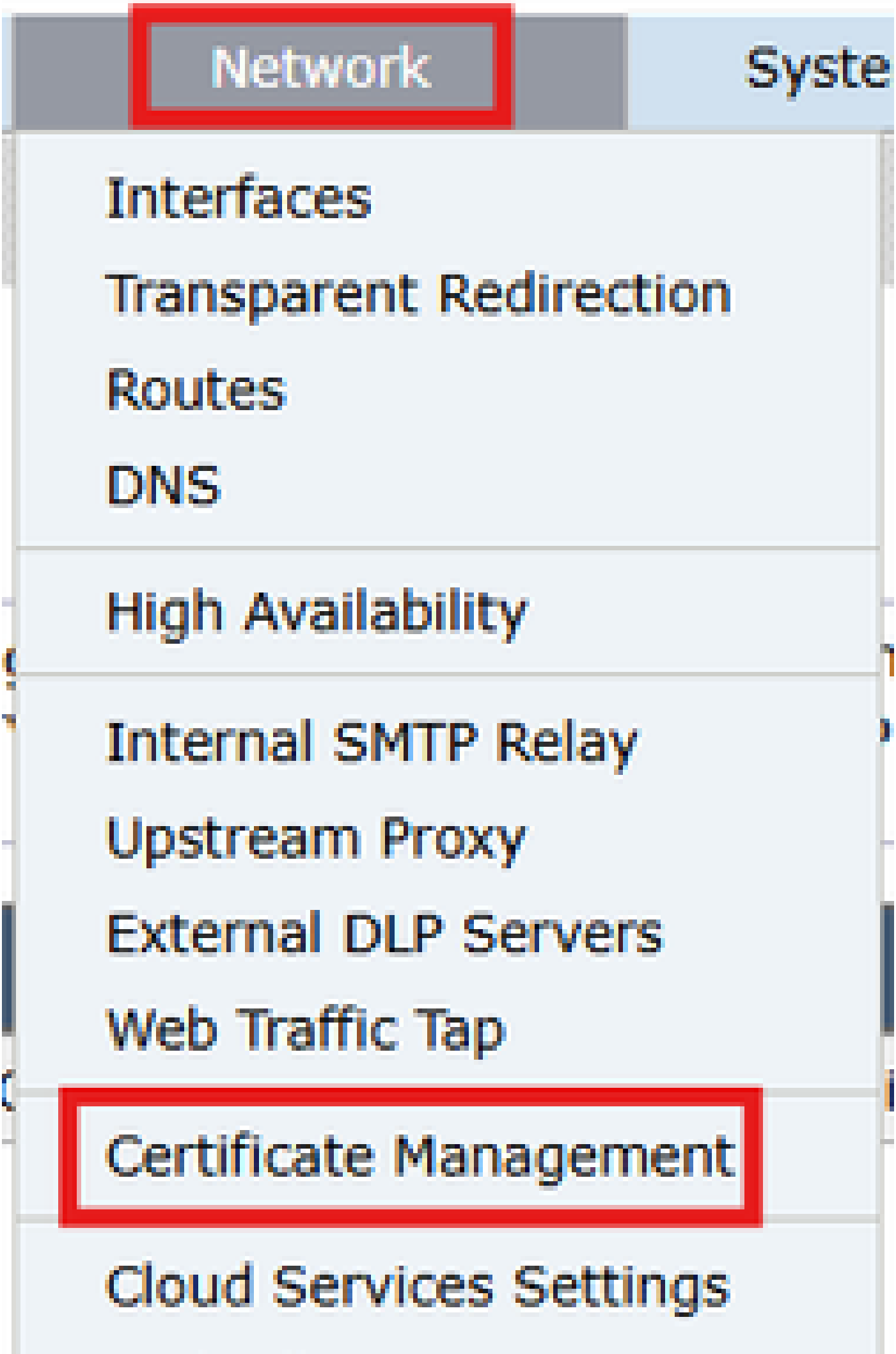
* Key type: RSA

* Key Length: 4096

* Digest to Sign With: SHA-384

Certificate Policies

2. Network(네트워크) > Certificate Management(인증서 관리) > Manage Trusted Root Certificates(신뢰할 수 있는 루트 인증서 관리)로 이동합니다.

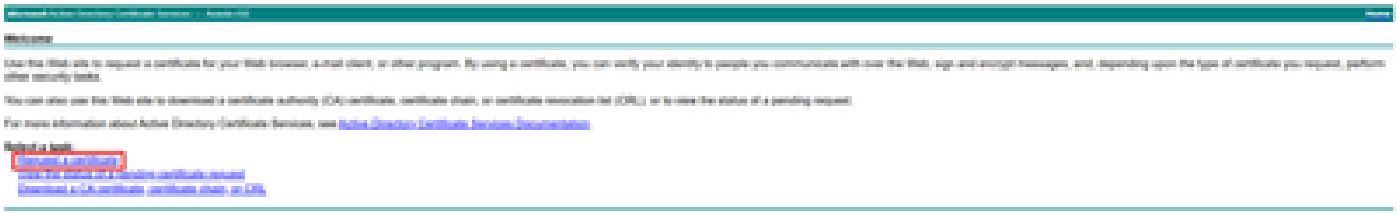

Network
Syste
Interfaces
Transparent Redirection
Routes
DNS
High Availability
Internal SMTP Relay
Upstream Proxy
External DLP Servers
Web Traffic Tap
Certificate Management
Cloud Services Settings

언급된 변경 사항을 제출 및 커밋하지 않고 서명된 인증서를 직접 업로드하고 커밋을 수행할 경우 통합 과정에서 문제가 발생할 수 있습니다.

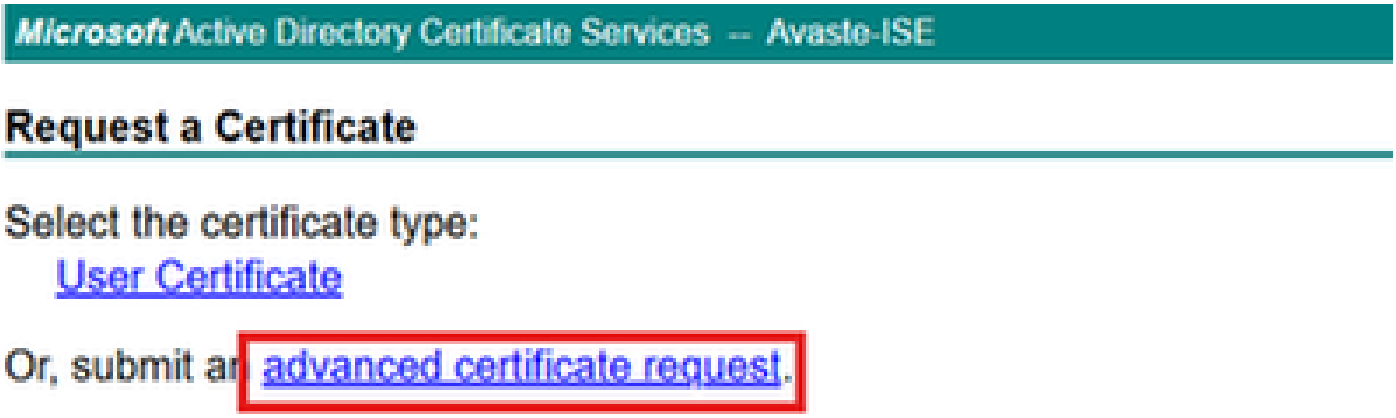
섹션 B: 외부 CA를 사용하여 WSA 클라이언트 CSR 서명

1.MS Active Directory Certificate Service(MS Active Directory 인증서 서비스)https://server/certsrv/으로 이동합니다. 여기서 server는 MS 서버의 IP 또는 DNS입니다.

2. 인증서 요청을 클릭합니다.

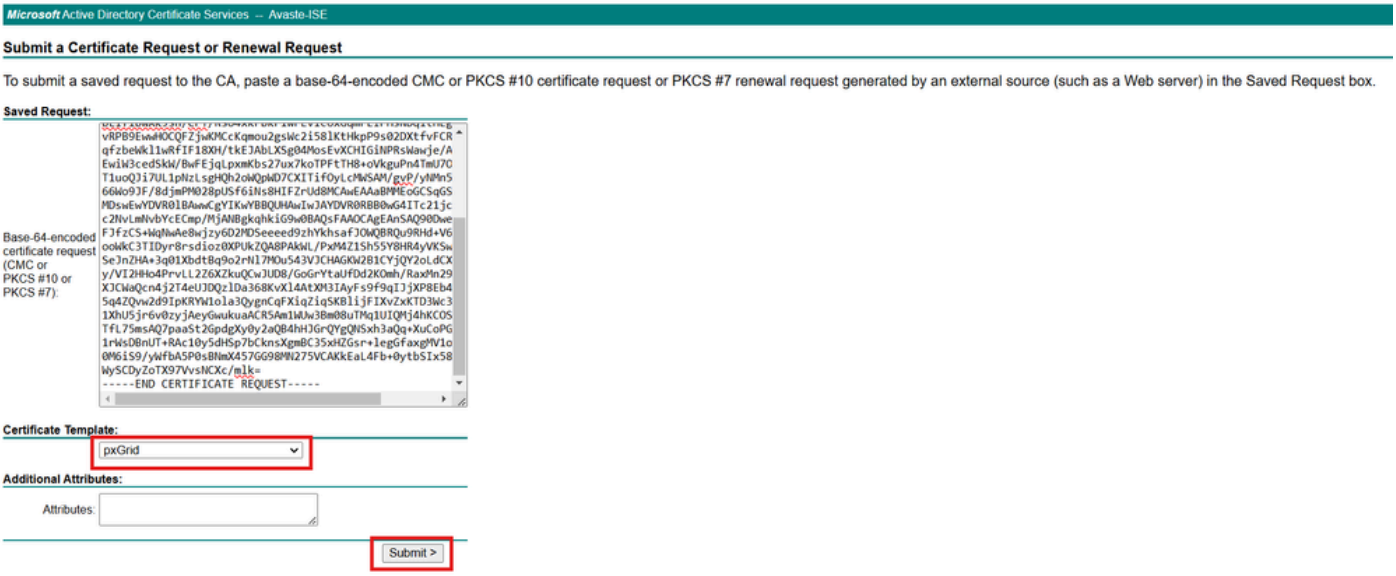


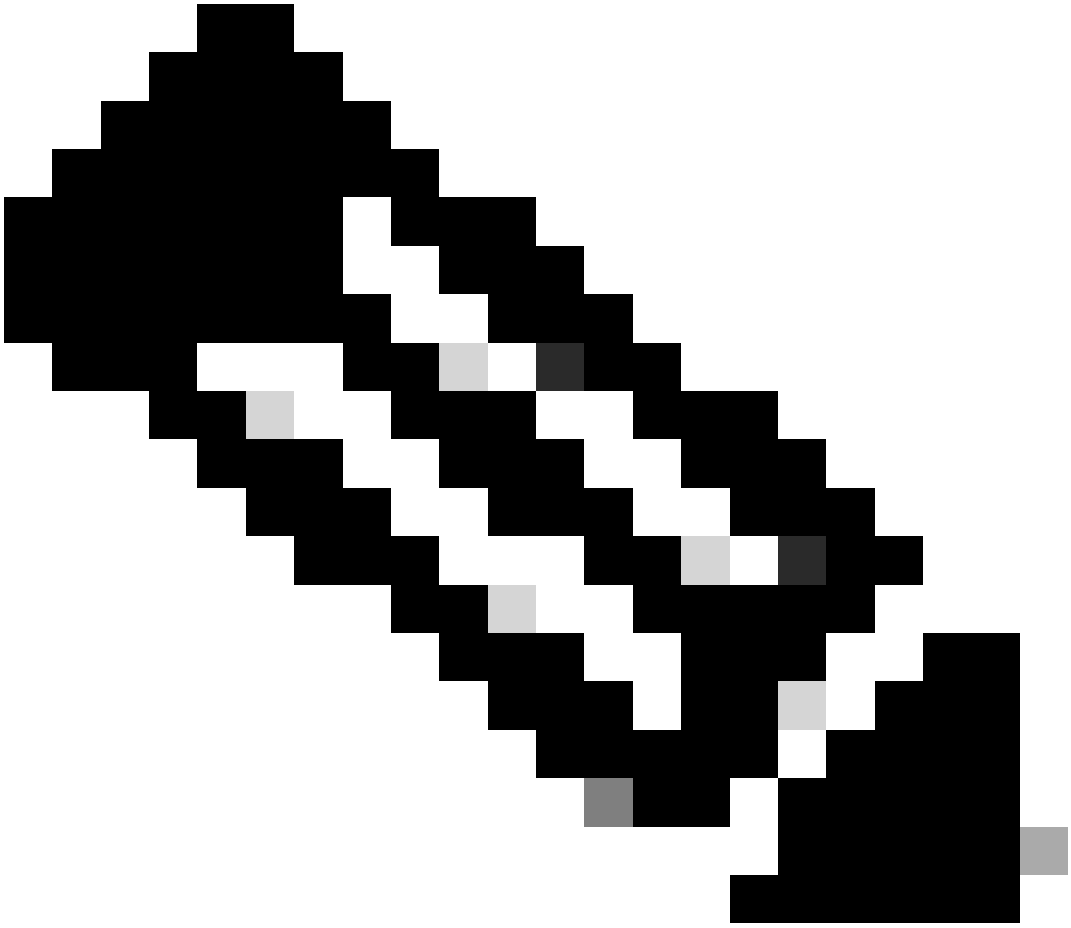
3. 고급 인증서 요청을 실행하도록 선택합니다.



4.이전 섹션에서 생성된 CSR의 내용을 Saved Request(저장된 요청) 필드에 복사합니다.

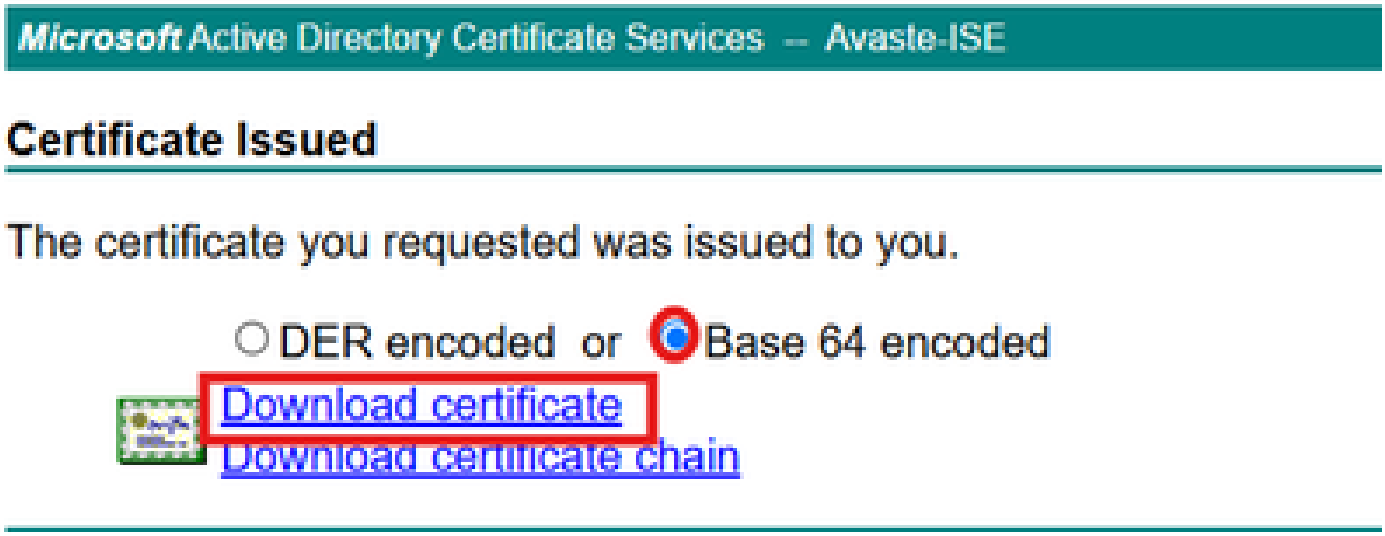
5. 인증서 템플릿에서 pxGridas를 선택한 다음 제출을 클릭합니다.





참고: 참고: 사용된 인증서 템플릿 pxGrid에는 Enhanced Key Usage(고급 키 사용) 필드에 클라이언트 인증과 서버 인증이 모두 필요합니다.

6.생성된 인증서를 Base-64 형식으로 다운로드하고 WSA-Client.cer로 저장합니다.



섹션 C: WSA 클라이언트 인증서를 CSR(Certificate Signing Request)에 바인딩하고 통합합니다.

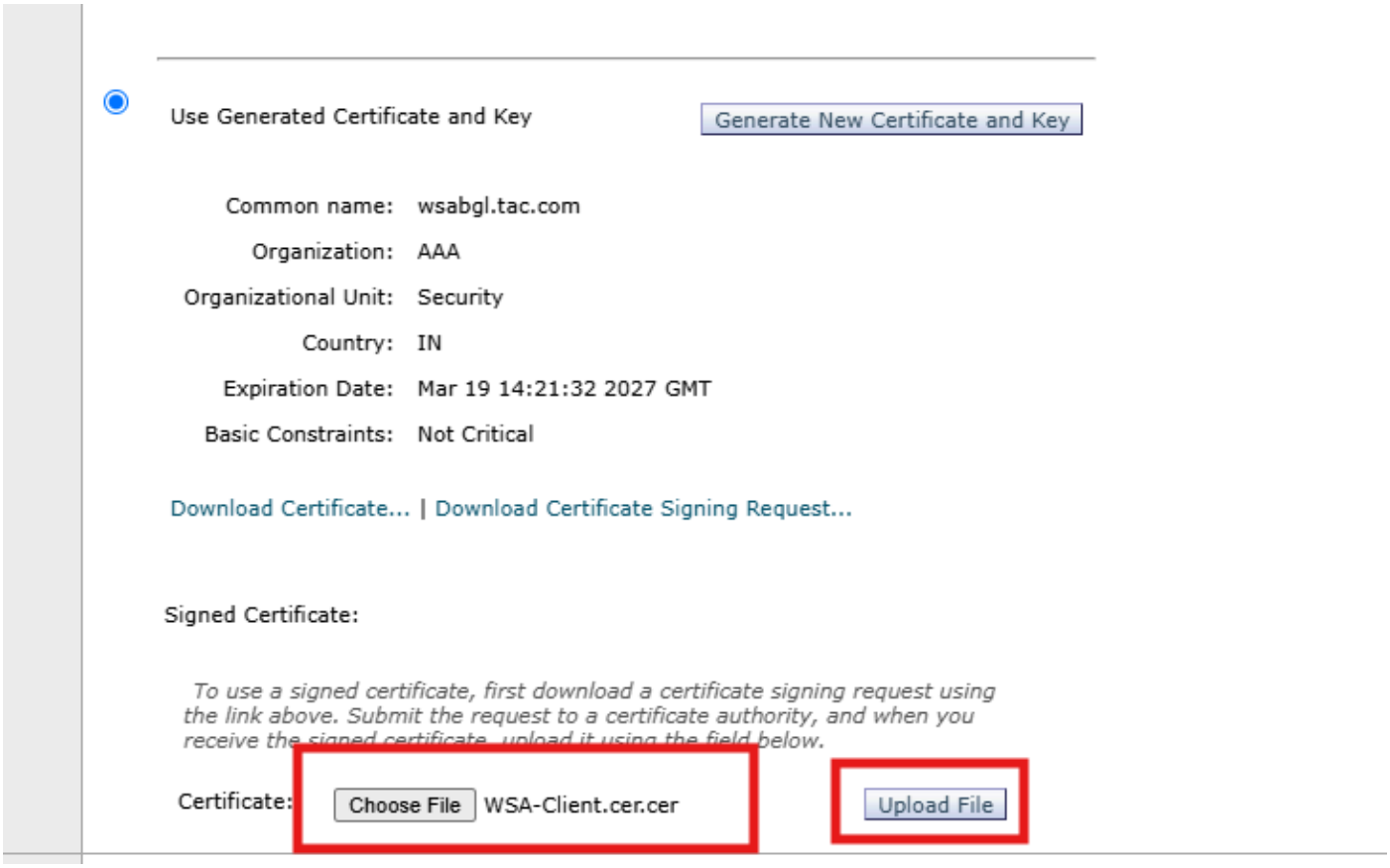
1.WSA(Web Security Appliance) GUI로 이동합니다.

2. Network(네트워크) > Identification Services(식별 서비스) > Identification Service Engine(식별 서비스 엔진)으로 이동합니다.

3.설정 편집을 클릭합니다.

4.Web Appliance Client Certificate(웹 어플라이언스 클라이언트 인증서) 섹션으로 이동합니다.

5. signed certificate(서명된 인증서) 섹션에서 서명된 인증서 WSA-Client.cer을 업로드합니다



6. 제출을 클릭합니다.

7. Commit Changes(변경 사항 커밋)를 클릭하여 변경 사항을 적용합니다.

8.설정 편집을 클릭합니다.

9.Test Communication with ISE Nodes(ISE 노드와의 통신 테스트)로 스크롤하고 Start Test(테스트 시작)를 클릭합니다. 다음 결과가 나타날 수 있습니다.

ISE 노드와의 통신 테스트

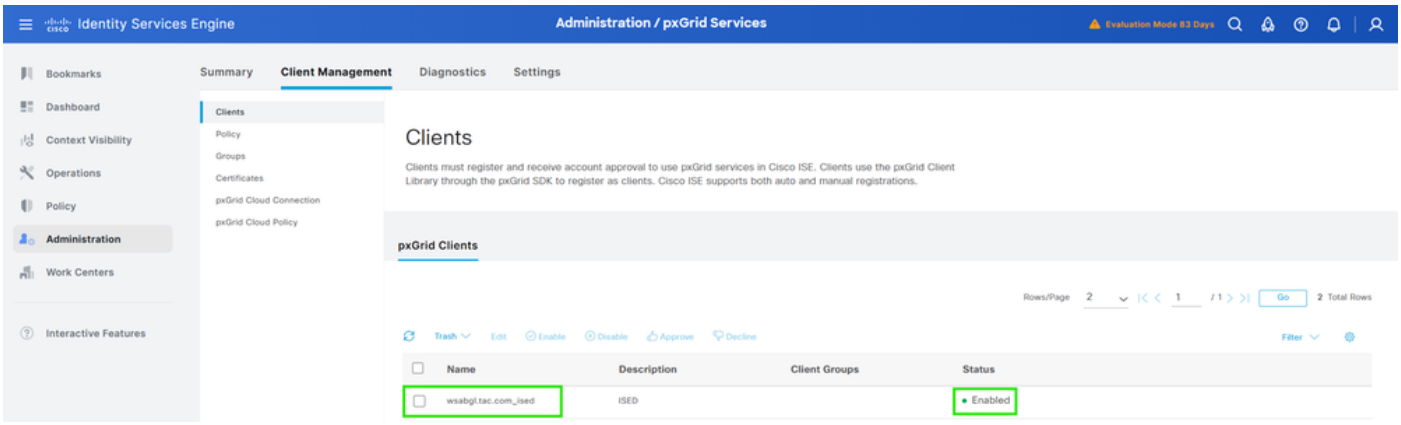
ISE 노드와의 통신 테스트

```
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.
```

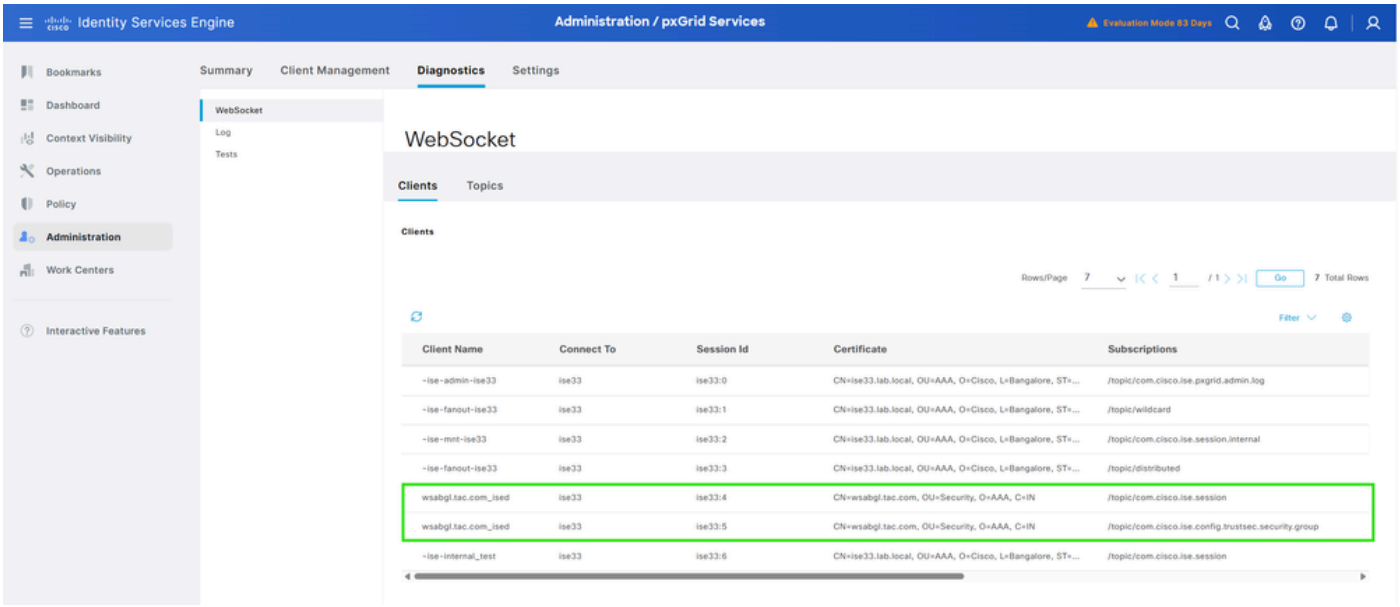
다음을 확인합니다.

Cisco ISE에서 Administration(관리) > pxGrid Services(pxGrid 서비스) > Client Management(클라이언트 관리) > Clients(클라이언트)로 이동합니다.

그러면 WSA가 statusEnabled의 pxgrid 클라이언트로 생성됩니다.



Cisco ISE에서 항목 등록을 확인하려면 Administration(관리) >pxGrid Services(pxGrid 서비스) > Diagnostics(진단) > Websocket(웹소켓) > Clients(클라이언트)로 이동합니다.



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\u00
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
```

문제 해결

문제

알 수 없는 CA 문제, WSA에서 ISE 연결 테스트가 오류로 인해 실패합니다. 실패: ISE PxGrid 서버에 대한 연결 시간이 초과되었습니다.

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
```

실패 이유는 패킷 캡처,

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

솔루션

1. 웹 어플라이언스 서명 인증서가 WSA에서 성공적으로 바인딩되었고 변경 사항이 커밋되었는지 확인합니다.

2. 발급자 또는 WSA 클라이언트 인증서의 루트 CA 인증서가 Cisco ISE의 신뢰할 수 있는 저장소에 속하는지 확인합니다.

알려진 결함

Cisco 버그 ID	설명
Cisco 버그 ID 23986	Pxgrid getUserGroups API 요청이 빈 응답을 반환합니다.
Cisco 버그 ID 77321	WSA는 ISE에서 AD 그룹 대신 SID를 수신합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.