

FMC 7.2.4 통합으로 ISE 3.2 구성 및 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[통합을 위해 ISE를 준비합니다.](#)

[통합을 위해 FMC를 준비합니다.](#)

[ISE와 FMC 간에 pxGrid 연결을 설정합니다.](#)

[확인](#)

[FMC에 대한 검증](#)

[ISE에서 검증](#)

[문제 해결](#)

[FMC에서 트러블슈팅을 수행합니다.](#)

[ISE에서 트러블슈팅을 수행합니다.](#)

[일반적인 문제](#)

[PxGrid 가입자 클라이언트는 ISE에서 승인되지 않습니다.](#)

[PxGrid ISE 인증서 체인이 완료되지 않았습니다.](#)

[참조](#)

소개

이 문서에서는 Platform Exchange Grid 연결을 사용하여 Identity Services Engine을 방화벽 관리 센터와 통합하는 절차에 대해 설명합니다.

사전 요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- Identity Services Engine(ISE)
- 플랫폼 교환 그리드
- FMC(Firewall Management Center)
- TLS/SSL 인증서

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ISE(Identity Services Engine) 버전 3.2 패치 3
- Firewall Management Center 버전 7.2.4

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.

배경 정보.

이 문서에서는 pxGrid 버전 2를 사용하여 FMC와 ISE를 통합하는 솔루션을 제공합니다.

Cisco FMC(Firepower Management Center)는 Next Generation Firewall 및 Intrusion Prevention System을 위한 중앙 집중식 플랫폼으로서 정책 관리, 위협 탐지, 사고 대응을 제공합니다.

Cisco Identity Services Engine은 AAA(Authentication, Authorization, and Accountability) 및 정책 시행 서비스를 제공하여 엔드포인트에 대한 보안 액세스를 제공하는 포괄적인 솔루션입니다.

pxGrid(Platform Exchange Grid)를 사용하면 멀티벤더 교차 플랫폼 네트워크 간에 정보를 교환할 수 있습니다.

이러한 통합을 통해 안전한 모니터링, 위협 탐지, 공유된 정보를 기반으로 네트워크 정책을 설정할 수 있습니다.

PxGrid 프레임워크는 2가지 버전을 가지고 있습니다. 사용할 버전은 검토해야 하는 ISE 버전 및 패치에 따라 다릅니다.

버전 ISE 3.1부터 모든 pxGise의 rid 연결은 pxgrid 버전을 기반으로 합니다. 2 .

PxGrid 버전 1.

T이 프레임워크의 첫 번째 버전 (pxGrid v1) show application status ise 명령을 통해 확인된 서비스 기능 때문에 특징이 있습니다. 표시됩니다.

pxGrid 기능이 노드에서 활성화되면 pxGrid가 표시됩니다 기능 실행 중 상태.

```
ise/admin# show application status ise
ISE PROCESS NAME                STATE                PROCESS ID
-----
Database Listener                running              3688
Database Server                  running              41 PROCESSES
Application Server                running              6041
Profiler Database                 running              4533
AD Connector                      running              6447
M&T Session Database              running              2363
M&T Log Collector                 running              6297
M&T Log Processor                 running              6324
Certificate Authority Service     running              6263
pxGrid Infrastructure Service      disabled
pxGrid Publisher Subscriber Service disabled
pxGrid Connection Manager         disabled
pxGrid Controller                 disabled
Identity Mapping Service          disabled
```

PxGrid 버전 1 서비스 가용성.

이 플랫폼 버전에서는 pxGrid 프로세스가 실행 중인 하나의 pxGrid 노드만 있고 나머지 pxGrid 노드는 대기 상태인 것으로 알려져 있습니다.

이러한 노드는 실행 관련 서비스가 있는 pxGrid 노드의 상태를 지속적으로 모니터링하고 있습니다.

이 경우 기본 pxGrid 노드에 프로모션이 있었고 다른 pxGrid 노드는 해당 pxGrid 서비스를 활성화했습니다.

그러나 이는 장애 조치가 발생했을 때의 다운타임을 나타냅니다.

pxgrid의 첫 번째 버전은 협업 및 음성 인프라에 사용되는 기술 집합인 XMPP(Extensible Messaging and Presence Protocol)의 통신을 기반으로 했습니다.

pxGrid v1 연결에서 공유하는 항목은 다음과 같습니다.

- 세션 디렉터리
- 엔드포인트 프로파일 메타데이터
- Trustsec 메타데이터
- 엔드포인트 보호 기능
- 적응형 네트워크 제어
- MDM_Offline 항목
- 신원
- SXP

PxGrid 버전 2.

이 문서에서는 PxGrid 버전 2의 사용에 대해 설명합니다. 이 플랫폼은 ISE 및 WebSocket 프로토콜에서 REST 작업을 사용하여 작동하며, 이를 통해 데이터 모델에서 개선, 확장성, 성능 및 유연성이 향상됩니다.

이 버전에서는 show application status ise 명령을 사용하여 이전 버전에서와 같이 실행 중인 pxgrid 기능을 볼 수 없습니다.

pxGrid 기능을 검토하기 위해 어떤 메커니즘을 확인해야 하는지 알아보려면 이 문서의 ISE에 대한 검증 섹션을 참조하십시오.

이 버전에서는 활성 pxGrid 노드로 구성하는 모든 pxGrid 노드가 있습니다. 이들은 언제든지 정보 교환에 참여할 수 있습니다.

버전 1에서는 한 노드만 pxGrid의 서비스 가용성을 실행 중인 것으로 유지했습니다.

pxGrid v2 연결에서 공유하는 항목은 다음과 같습니다.

- 세션 디렉터리
- Radius 실패
- 프로파일러 컨피그레이션
- 시스템 상태
- MDM

- ANC 상태
- 트러스트섹(TrustSec)
- TrustSec 컨피그레이션
- TrustSec SXP
- 엔드포인트 자산.

pxGrid의 구성 요소를 플랫폼으로 사용합니다.

PxGrid 컨트롤러(ISE): pxGrid를 사용하는 각 참가자를 신뢰해야 합니다.

클라이언트: 다른 주제의 구독자 및 게시자가 될 수 있습니다.

게시자: 컨트롤러와 정보를 공유하는 클라이언트입니다.

가입자: 주제의 정보를 사용하는 클라이언트입니다.

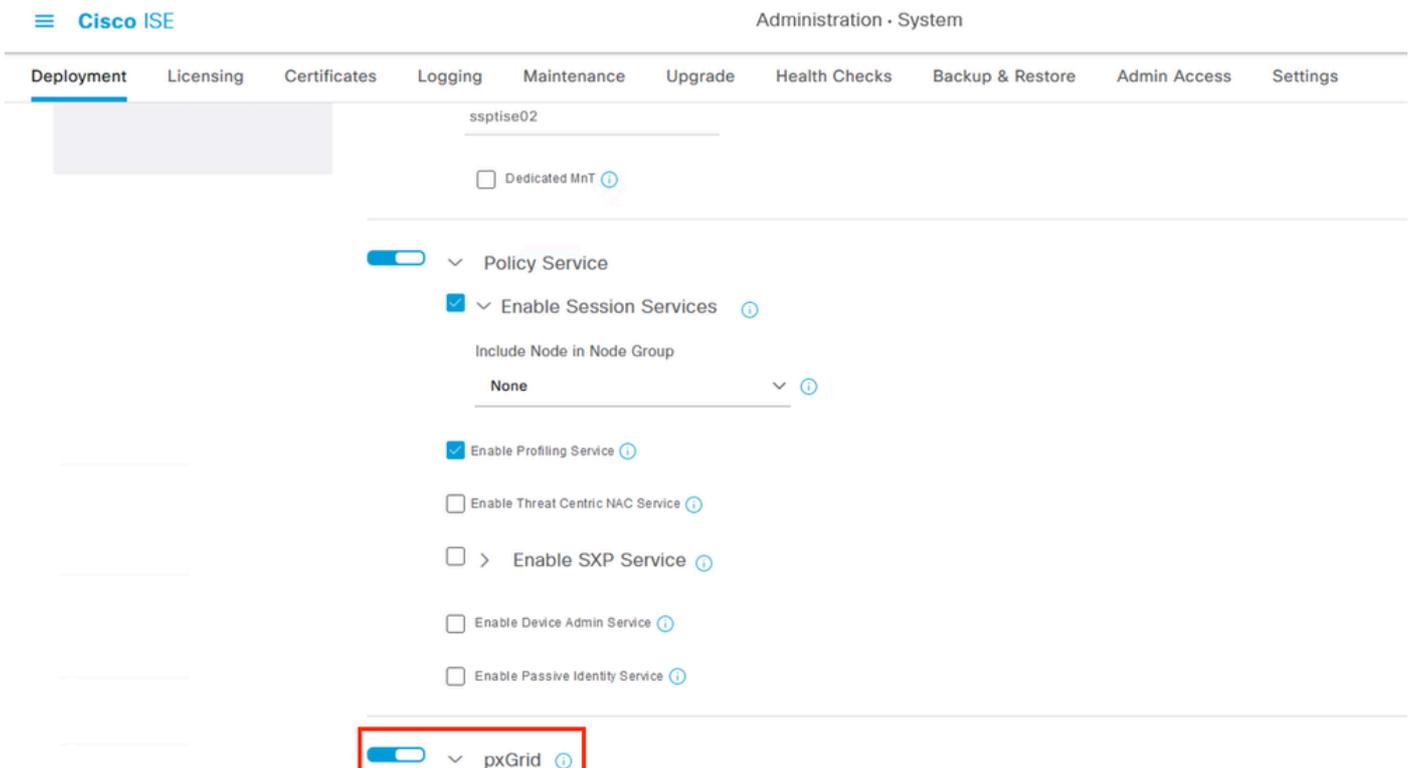
이러한 통합을 통해 ISE에서 공유하는 정보 및 게시된 항목(엔드포인트 활동과 관련)을 기반으로 FMC에서 콘텐츠 정책을 생성할 수 있습니다.

구성

통합을 위해 ISE를 준비합니다.

1단계. Administration(관리) > System(시스템) > Deployment(구축) 메뉴에서 pxGrid 페르소나를 실행하도록 ISE 노드를 구성합니다.

노드를 선택하고 pxGrid 기능을 활성화합니다.



노드에서 ISE pxGrid 서비스를 활성화합니다.

2단계. pxGrid 기능을 사용하여 노드를 활성화한 후 연결된 내부 클라이언트와 관련된 Websockets의 상태를 검토합니다.

Administration > pxGrid Services > WebSocket으로 이동합니다. IP 주소 127.0.0.1을 통해 ISE 서비스를 직접 가리키는 클라이언트를 확인합니다.

The screenshot shows the 'Websocket Clients' table in the Cisco ISE Administration interface. The table lists various clients with their connection details and status.

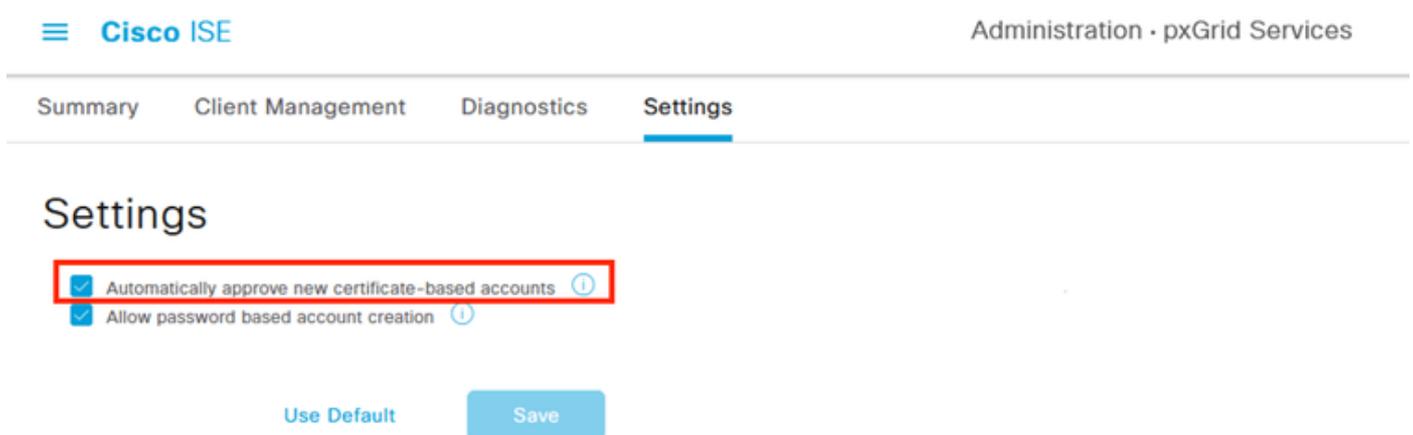
Client Name	Connect To	Session Id	Certificate	Subscriptions	Publications	IP Address	Status
-ise-fanout-ssptise01	ssptise01	ssptise01:0	CN=ssptise01.ss...	/topic/wildcard	/topic/com.cisco.ise.pxgrid...	127.0.0.1	Connected
-ise-fanout-ssptise02	ssptise01	ssptise01:1	CN=ssptise02.ss...	/topic/distributed	/topic/distributed	10.4.49.42	Connected
-ise-fanout-ssptise01	ssptise01	ssptise01:2	CN=ssptise01.ss...	/topic/distributed		10.4.49.41	Connected
-ise-fanout-ssptise02	ssptise02	ssptise02:9	CN=ssptise02.ss...	/topic/wildcard	/topic/com.cisco.ise.pxgrid...	127.0.0.1	Connected
-ise-mnt-ssptise02	ssptise02	ssptise02:11	CN=ssptise02.ss...	/topic/com.cisco.ise.sessio...	/topic/com.cisco.ise.sessio...	10.4.49.42	Connected
-ise-admin-ssptise02	ssptise02	ssptise02:12	CN=ssptise02.ss...		/topic/com.cisco.ise.pxgrid...	10.4.49.42	Connected
-ise-mnt-ssptise01	ssptise02	ssptise02:13	CN=ssptise01.ss...	/topic/com.cisco.ise.sessio...	/topic/com.cisco.ise.sessio...	10.4.49.41	Connected
-ise-admin-ssptise01	ssptise02	ssptise02:14	CN=ssptise01.ss...	/topic/com.cisco.ise.pxgrid...	/topic/com.cisco.ise.pxgrid...	10.4.49.41	Connected

ISE의 내부 WebSockets

3단계. 메뉴 Administration(관리) > pxGrid Services(pxGrid 서비스) > Settings(설정)로 이동하고 새 인증서 기반 어카운트를 자동으로 승인하는 옵션을 선택합니다.

이 단계는 선택 사항이지만 pxGrid 연결의 경우 이 확인란을 활성화하는 것이 좋습니다.

나중에 수동으로 FMC를 가입자로 수락할 수 있습니다.



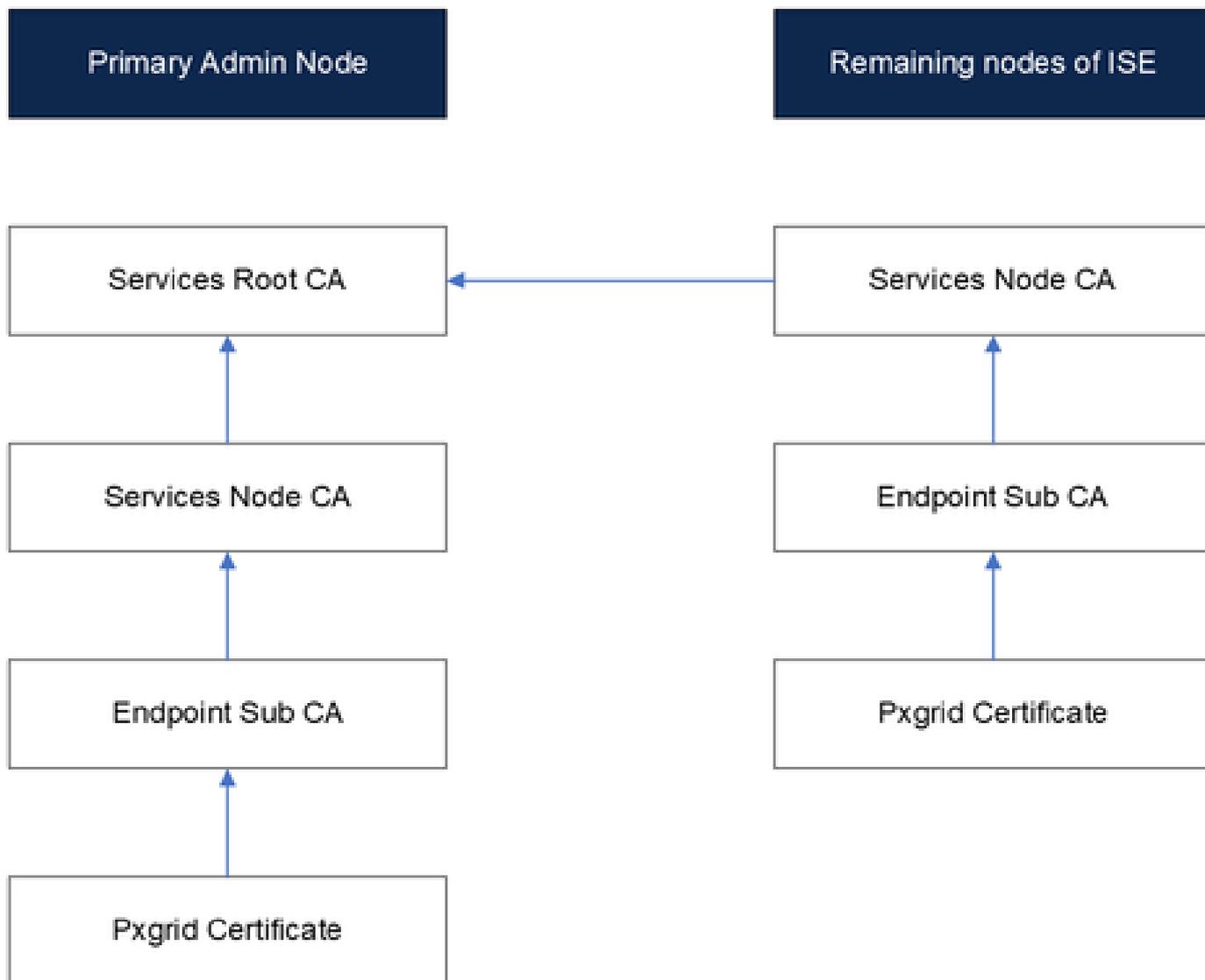
pxGrid 인증서 기반 어카운트에 대한 자동 승인을 활성화합니다.

4단계. Administration(관리) > System(시스템) > System Certificates(시스템 인증서)에서 해당 환경의 pxGrid 기능과 관련된 인증서를 검토합니다.

동일한 루트 CA(Certificate Authority)에서 서명한 구축의 모든 노드에 동일한 pxGrid 인증서가 있는

것이 좋습니다

이 시나리오에서는 생성된 내부 ISE 인증서를 사용합니다. 이 버전의 ISE에서는 루트 CA가 PAN 노드에 해당합니다.



ISE의 내부 인증서 다이어그램



참고: ISE에서 생성된 인증서의 내부 구조에 대한 자세한 내용은 ISE [내부 인증 기관 서비스 이해를 참조하십시오.](#)

System Certificates									
For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.									
Edit + Generate Self Signed Certificate + Import Export Delete View									
Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status		
CA - ssp1se01 (1000001)									
<input type="checkbox"/> CN=ssp1se01.ssp1sec.mex, O=U-Certificate Services System Certificate/Certificate Services Endpoint Sub CA - ssp1se01#00002	pxGrid		ssp1se01.ssp1sec.mex	Certificate Services Endpoint Sub CA - ssp1se01	Fri, 30 Jun 2023	Sat, 1 Jul 2028	Active		
<input type="checkbox"/> ise01_External_CA	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group	ssp1se01.ssp1sec.mex	ssp1sec-CXLABS-WIN2K22D-CA-2	Mon, 3 Jul 2023	Wed, 2 Jul 2025	Active		
<input checked="" type="checkbox"/> ssp1se02									
<input type="checkbox"/> Default self-signed saml server certificate - CN=SAML_ssp1se01.ssp1sec.mex	SAML		SAML_ssp1se01.ssp1sec.mex	SAML_ssp1se01.ssp1sec.mex	Sat, 1 Jul 2023	Thu, 29 Jun 2028	Active		
<input type="checkbox"/> ise02_External_CA	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group	ssp1se02.ssp1sec.mex	ssp1sec-CXLABS-WIN2K22D-CA-2	Mon, 3 Jul 2023	Wed, 2 Jul 2025	Active		
<input type="checkbox"/> CN=ssp1se02.ssp1sec.mex, O=U-ISE Messaging Services/Certificate Services Endpoint Sub CA - ssp1se02#00004	ISE Messaging Service		ssp1se02.ssp1sec.mex	Certificate Services Endpoint Sub CA - ssp1se02	Sat, 1 Jul 2023	Sun, 2 Jul 2028	Active		
<input type="checkbox"/> CN=ssp1se02.ssp1sec.mex, O=U-Certificate Services System Certificate/Certificate Services Endpoint Sub CA - ssp1se02#00003	pxGrid		ssp1se02.ssp1sec.mex	Certificate Services Endpoint Sub CA - ssp1se02	Sat, 1 Jul 2023	Sun, 2 Jul 2028	Active		

분산 구축의 PxGrid 인증서

5단계. pxGrid 인증서의 상태를 확인합니다.

이전 메뉴에서 노드 pxGrid 인증서의 확인란을 선택한 다음 보기 옵션을 선택합니다.

출력은 여기에 pxGrid 인증서에 표시된 것과 같습니다.

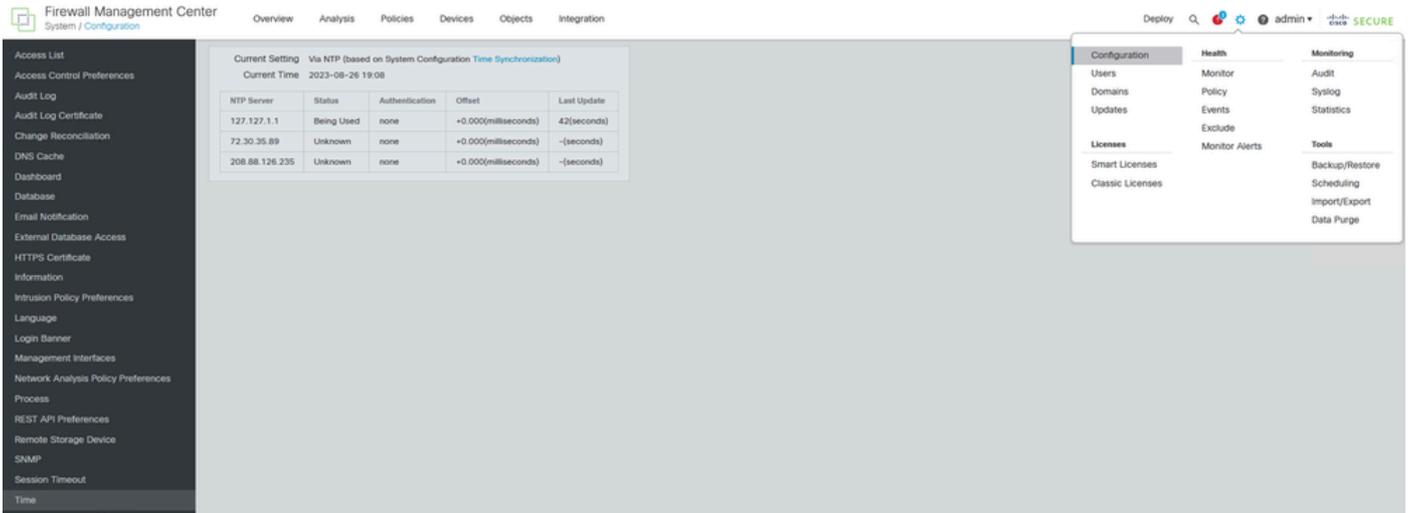
The screenshot shows a 'Certificate Hierarchy' window. At the top, it lists the hierarchy: Certificate Services Root CA - ssp1se01, Certificate Services Node CA - ssp1se02, and Certificate Services Endpoint Sub CA - ssp1se02. Below this, a specific certificate is highlighted: ssp1se02.ssp1sec.mex. A red box highlights the text 'Certificate status is good'. Under the 'Details' section, the 'Issued To' field is expanded to show: Common Name (CN) ssp1se02.ssp1sec.mex, Organization Unit (OU) Certificate Services System Certificate, Organization (O), City (L), State (ST), and Country (C). The background shows the 'System Certificates' table with the 'ssp1se02' section expanded.

pxGrid 인증서 확인.

통합을 위해 FMC를 준비합니다.

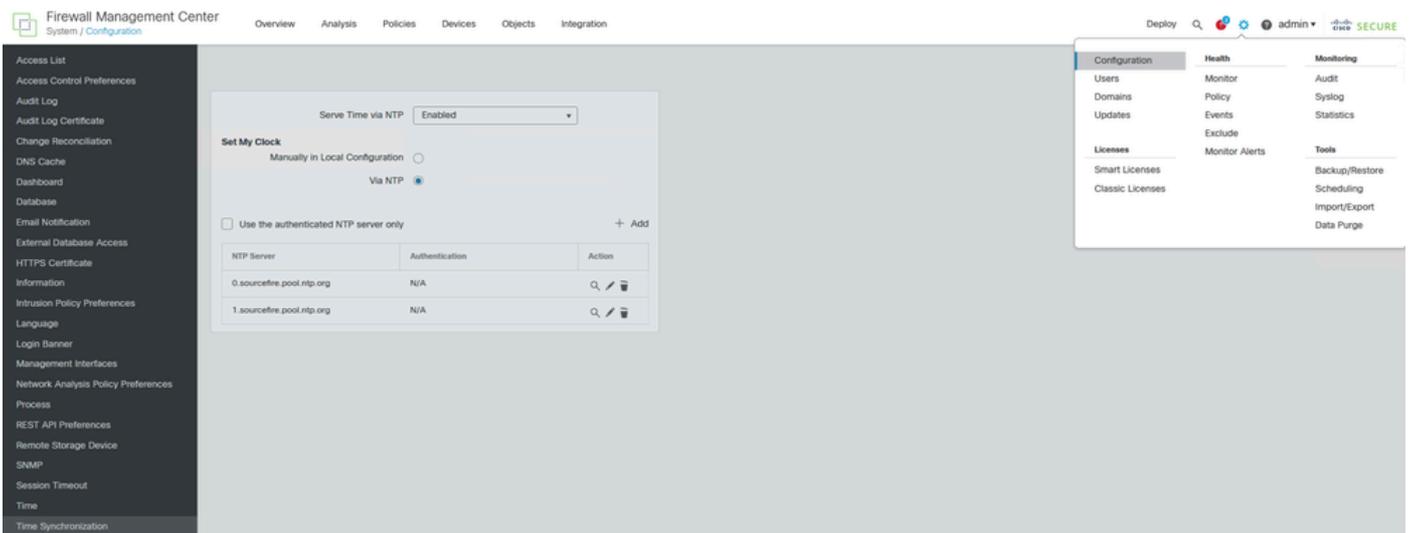
1단계.FMC 내부 시간이 최신.

로 이동합니다 System(시스템) > Configuration(구성) > Time FMC에 구성된 시간이 최신.



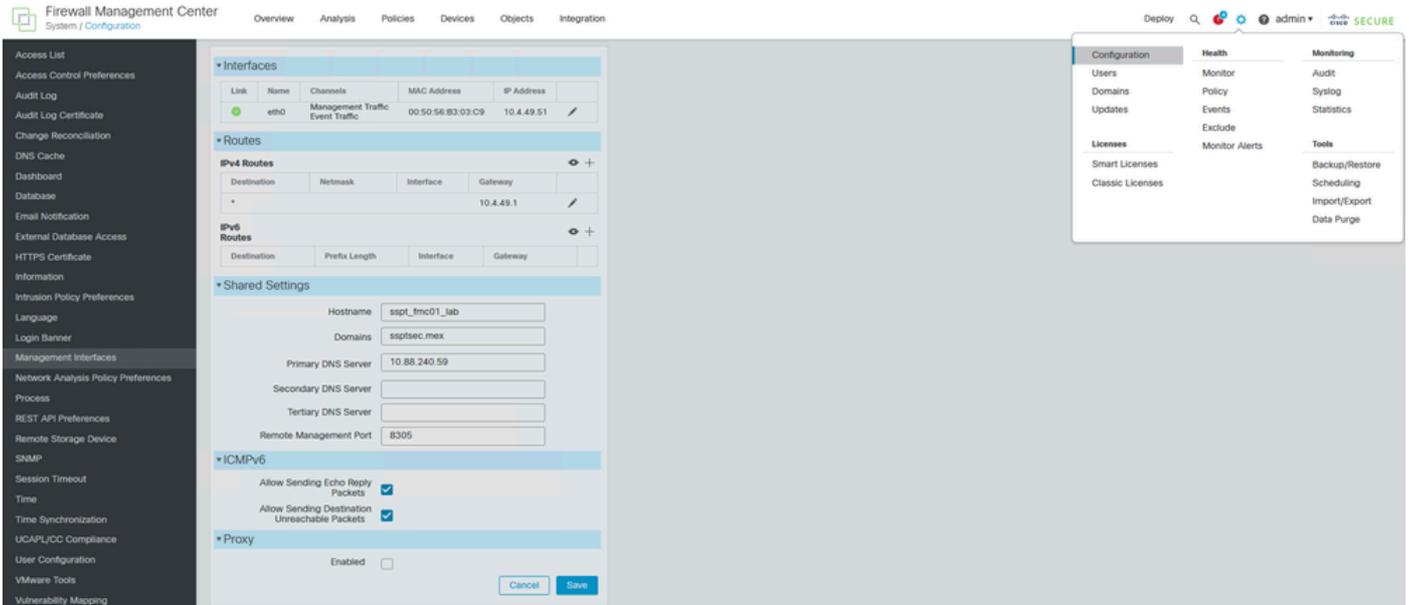
FMC가 최신 상태인지 확인하는 중입니다.

FMC 시간이 업데이트되지 않은 경우 NTP가 제대로 구성되었는지 확인합니다 및 에서 동기화. NTP는 System(시스템) > Configuration(구성) > Time(시간) > + Add(추가).



FMC에서 시간 동기화.

2단계. 로 이동합니다 System(시스템) > Configuration(구성) > 관리 인터페이스 > 공유 설정 최소 100% 이상의 기본 DNS 서버 필드 포함 유효한 DNS 서버 IP.



FMC의 DNS 컨피그레이션

3단계. FMC 호스트 이름이 구성되었는지 확인합니다.

로 이동합니다 System(시스템) > Configuration(컨피그레이션) > Management Interface(관리 인터페이스) > Shared Settings(공유 설정) Cisco가 호스트 이름 필드에 FMC 호스트 이름이 포함되어 있습니다.

이 섹션의 이전 단계를 검토하면서 이 단계를 확인할 수 있습니다.

ISE와 FMC 간에 pxGrid 연결을 설정합니다.

1단계. Administration(관리) > pxGrid Services(pxGrid 서비스) > Client Management(클라이언트 관리) > Certificates(인증서) 메뉴로 이동합니다.

첫 번째 옵션에서 I want to Generate single certificate (without certificate signing request)(인증서 서명 요청 없이 단일 인증서를 생성하겠습니다)를 선택합니다.

Common Name (CN) 섹션에서 ISE가 인증서를 발급할 FMC의 FQDN을 입력합니다.

설명을 입력합니다.

SAN(Subject Alternative Name) 섹션에서 연결할 FMC의 FQDN과 IP 주소를 입력합니다.

Certificate Download Format(인증서 다운로드 형식)의 맨 아래에 있는 드롭다운 메뉴에서 Certificate in Privacy Enhanced Electronic Mail (PEM) format(프라이버시 강화 전자 메일(PEM) 형식의 인증서) 옵션을 선택합니다.

입력 PKCSS PEM 형식(인증서 체인 포함).

나중에 FMC에서 이 비밀번호를 사용할 때 Certificate Password(인증서 비밀번호)에 비밀번호를 입력하고 저장합니다.

비밀번호를 확인한 다음 생성을 선택합니다.

Summary Client Management Diagnostics Settings

Clients
Policy
Groups
Certificates
pxGrid Cloud Connection
pxGrid Cloud Policy

Certificates

Generate pxGrid Certificates

I want to*
Generate a single certificate (withou...v

Common Name (CN)*
sspt_fmc01_lab.ssptsec.mex

Description
testing lab

Certificate Template pxGrid_Certificate_Template ⓘ

Subject Alternative Name (SAN)
FQDN sspt_fmc01_lab.ssptsec.mex -- +

Subject Alternative Name (SAN)
IP address 10.4.49.51 -- +

Certificate Download Format*
Certificate in Privacy Enhanced Elect...v ⓘ

Certificate Password*
***** ⓘ

Confirm Password*

Reset **Create**

pxGrid 인증서 생성의 예

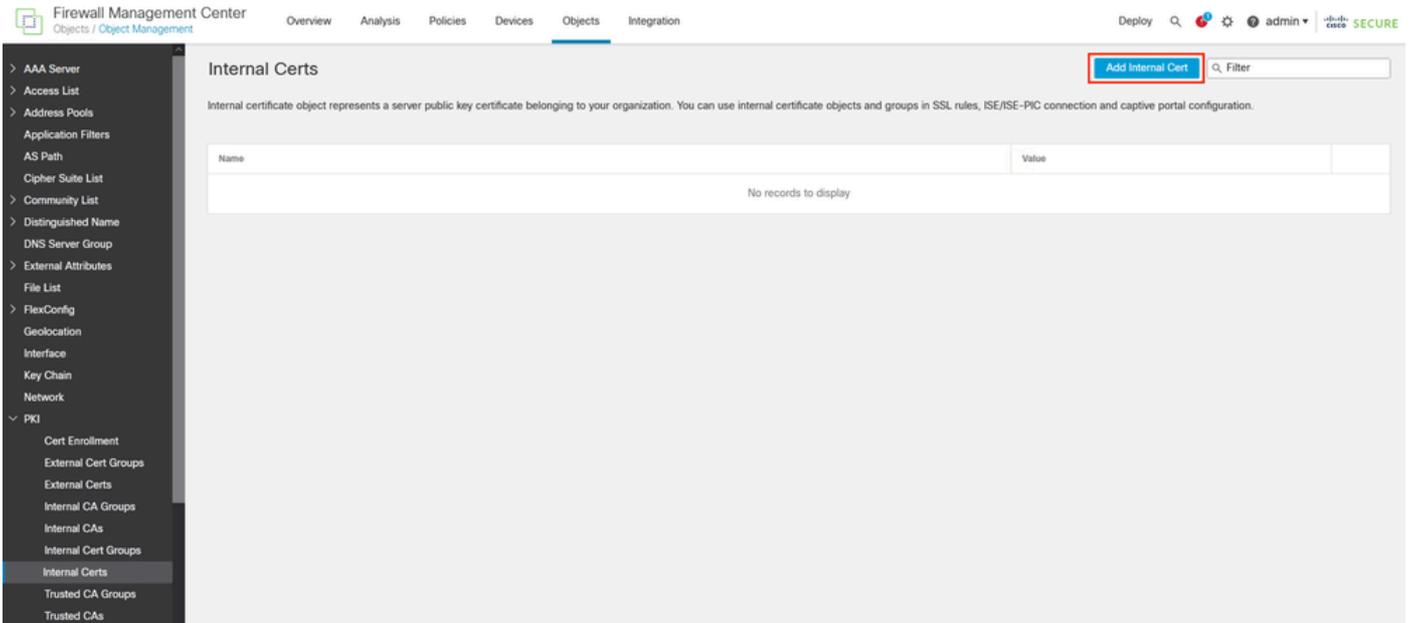
2단계. zip 파일이 컴퓨터에 다운로드됩니다. 파일 압축을 풀고 해당 환경에서 다음 파일이 있는지 확인합니다.

Name	Date modified	Type	Size
CertificateServicesEndpointSubCA-ssptise01_	21/08/2023 04:55	Security Certificate	3 KB
CertificateServicesNodeCA-ssptise01_	21/08/2023 04:55	Security Certificate	2 KB
CertificateServicesRootCA-ssptise01_	21/08/2023 04:55	Security Certificate	2 KB
sspt_fmc01_lab.ssptsec.mex_sspt_fmc01_lab.ssptsec.mex	21/08/2023 04:55	Security Certificate	2 KB
sspt_fmc01_lab.ssptsec.mex_sspt_fmc01_lab.ssptsec.mex.key	21/08/2023 04:55	KEY File	2 KB

ISE에서 생성된 PxGrid 인증서

3단계. FMC에서 Objects(개체) > Objects Management(개체 관리) > PKI > Internal Certs(내부 인증서) 메뉴로 이동합니다.

Add Internal Cert(내부 인증서 추가) 옵션을 선택합니다.



FMC 인증서를 내부 인증서로 추가합니다.

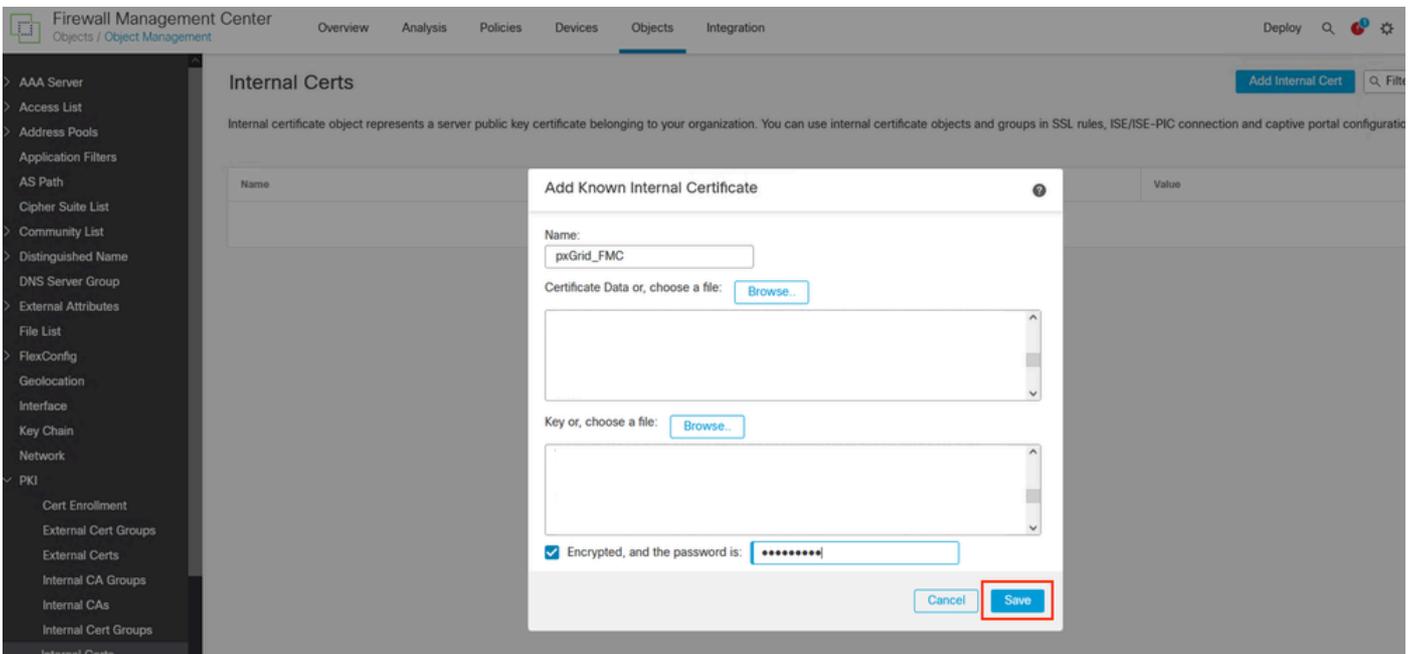
4단계. FMC에 할당된 인증서의 이름을 지정합니다.

Certificate Data(인증서 데이터) 섹션에서 ISE에서 FMC에 대해 생성한 인증서를 찾아봅니다.

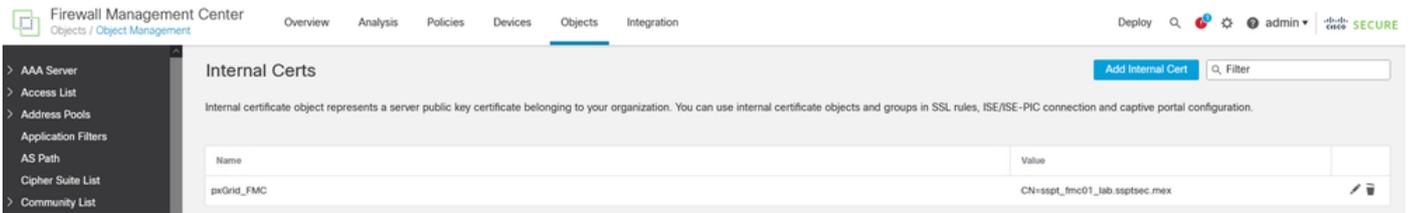
다음 필드를 채우려면 확장자 .key가 있는 파일을 찾습니다.

Encrypted(암호화됨) 옵션을 선택하고 ISE에서 인증서를 생성할 때 사용한 비밀번호를 입력합니다.

설정 저장.



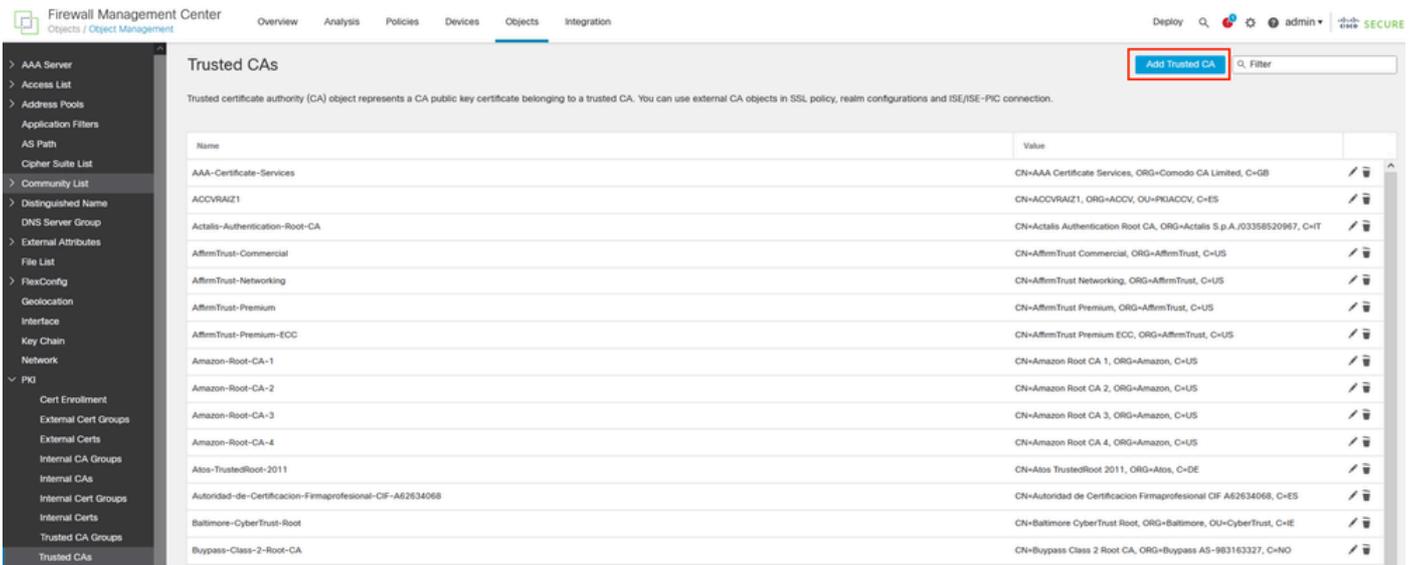
ISE에서 생성한 FMC 인증서 내보내기



FMC 인증서

5단계. Objects(개체) > Objects Management(개체 관리) > PKI > Trusted CAs(신뢰할 수 있는 CA) 메뉴로 이동합니다.

Add Trusted CAs(신뢰할 수 있는 CA 추가)를 선택합니다.

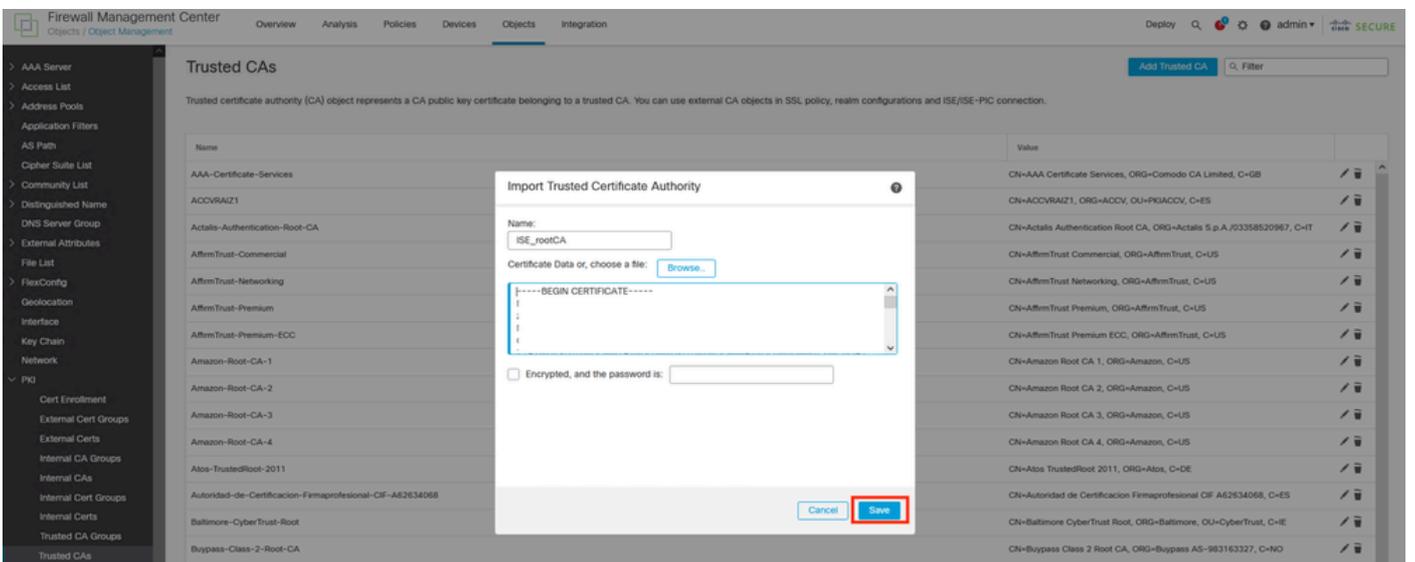


ISE rootCA를 신뢰할 수 있는 인증서로 추가합니다.

6단계. 인증 기관의 이름을 지정합니다.

ISE 파일에서 다운로드한 ISE rootCA를 찾아 선택합니다.

컨피그레이션을 저장합니다.



ISE rootCA를 내보냅니다.

7단계. Integration(통합) > Other Integrations(기타 통합) > Identity Sources(ID 소스) 메뉴로 이동합니다.

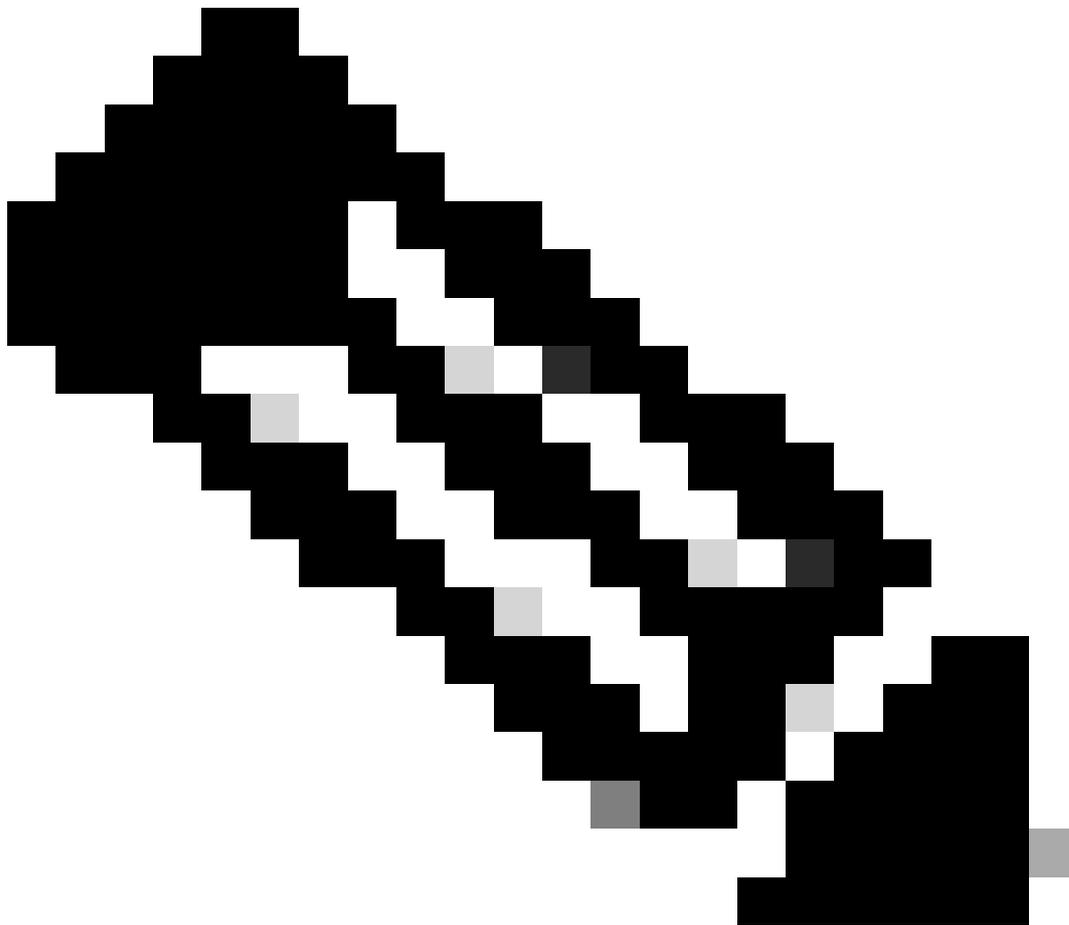
서비스 유형에서 선택: Identity Services Engine,

기본 노드가 되는 pxGrid 노드의 IP 주소 또는 FQDN을 입력합니다.

보조 pxGrid 노드에 대해 이 절차를 반복합니다.

드롭다운 메뉴에서 pxGrid 클라이언트 인증서 섹션에 대해 ISE에서 생성한 pxGrid 인증서를 선택합니다.

MNT 서버 CA 및 pxGrid 서버 CA 섹션에서 마지막 단계에서 내보낸 ISE rootCA를 선택합니다.



참고: pxGrid 서버 CA는 pxGrid 노드의 pxGrid에서 사용 중인 인증서의 루트 Certificate Authority에 해당합니다.

MNT 서버 CA는 MNT 노드의 pxGrid에서 사용 중인 인증서의 인증 기관에 해당합니다.

(선택 사항) ISE에서 세션 디렉토리 및 SXP 주제에 가입할 수 있습니다.

설정 저장.

Service Type:
 None Identity Services Engine

Primary Host Name/IP Address*
10.4.49.41

Secondary Host Name/IP Address
10.4.19.42

pxGrid Client Certificate*
pxGrid_FMC

MNT Server CA*
ISE_rootCA

pxGrid Server CA*
ISE_rootCA

ISE Network Filter
ex. 10.89.31.0/24

Subscribe To:
 Session Directory Topic
 SXP Topic

Test

FMC에서 ISE를 ID 소스로 설정

확인.

FMC에 대한 검증

메뉴에서 컨피그레이션을 저장하기 전에 Integration > Other Integrations > Identity Sources > Identity Services Engine으로 이동합니다. pxGrid 링크에 대한 설정을 테스트할 수 있습니다.

Service Type:
 None Identity Services Engine

Primary Host Name/IP Address*
10.4.49.41

Secondary Host Name/IP Address
10.4.49.42

pxGrid Client Certificate*
pxGrid_FMC

MNT Server CA*
ISE_rootCA

pxGrid Server CA*
ISE_rootCA

ISE Network Filter
ex. 10.89.31.0/24

Subscribe To:
 Session Directory Topic
 SXP Topic

Test

Status

ISE connection status:
Primary host: Success
Secondary host: Success

Additional Logs

Primary host:
[INFO]: PXGrid v2 is enabled
[INFO]: pxgrid 2.0: account activate succeeded
[INFO]: Successful connection to
ssptise02.ssptsec.mex:8910

OK

PxGrid가 성공적으로 통신했습니다.

Primary host:

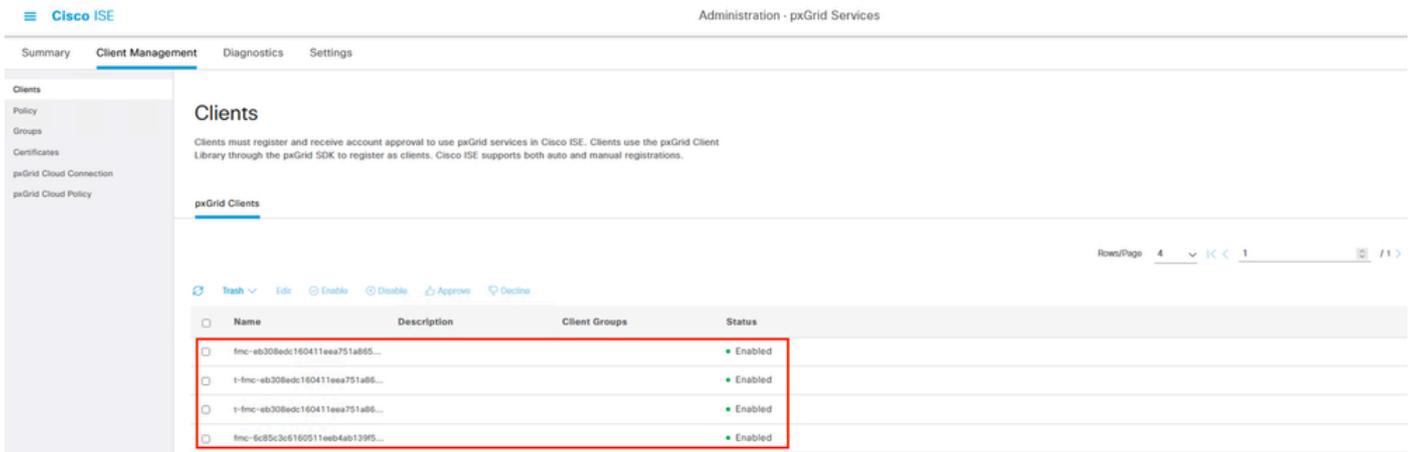
```
[INFO]: PXGrid v2 is enabled
[INFO]: pxgrid 2.0: account activate succeeded
[INFO]: Successful connection to ssptise02.ssptsec.mex:8910
[INFO]: Successful connection to ssptise01.ssptsec.mex:8910
[INFO]: These ISE Services are up: SessionDirectory, SXP, EndpointProfile, SecurityGroups, AdaptiveNetwork
[INFO]: All requested ISE Services are online.
```

Secondary host:

```
[INFO]: PXGrid v2 is enabled
[INFO]: pxgrid 2.0: account activate succeeded
[INFO]: Successful connection to ssptise02.ssptsec.mex:8910
[INFO]: Successful connection to ssptise01.ssptsec.mex:8910
[INFO]: These ISE Services are up: SessionDirectory, SXP, EndpointProfile, SecurityGroups, AdaptiveNetwork
[INFO]: All requested ISE Services are online.
```

ISE에서 검증.

FMC pxGrid 클라이언트가 ISE에 성공적으로 통합되면 당신 를 참조하십시오.의 Administration(관리) > pxGrid Services(pxGrid 서비스) > Client Management(클라이언트 관리) > Clients(클라이언트) 메뉴) fmc라는 이름의 클라이언트가 포함되어 있으며 활성화됨.



The screenshot shows the Cisco ISE Administration interface for pxGrid Services. The 'Client Management' tab is active, and the 'Clients' section is displayed. A table lists pxGrid Clients with columns for Name, Description, Client Groups, and Status. Four clients are listed, all with a status of 'Enabled'. The first row is highlighted with a red border.

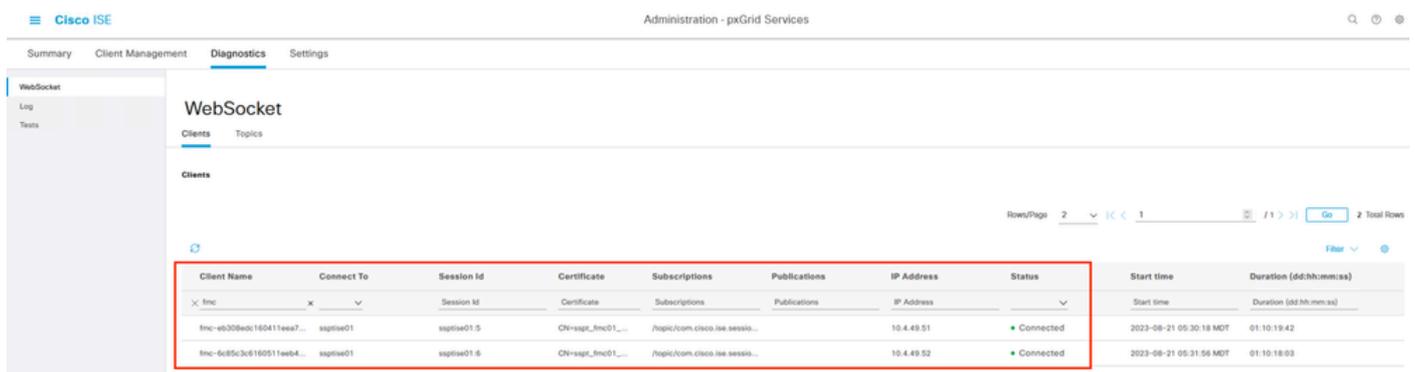
Name	Description	Client Groups	Status
fmc-eb308edc160411ea751a86...			Enabled
t-fmc-eb308edc160411ea751a86...			Enabled
t-fmc-eb308edc160411ea751a86...			Enabled
fmc-6c85c3c6160511eb4ab139f5...			Enabled

사용 가능한 PxGrid 클라이언트 및 활성화

참고: 접두사가 "t-fmc"로 시작되는 pxGrid 클라이언트는 FMC의 테스트 버튼을 통해 사용 됩니다.

또한 administration(관리) > pxGrid Services(pxGrid 서비스) > Diagnostics(진단) > WebSocket(WebSocket) 메뉴로 이동할 경우 그런 다음 Cisco의 FMC

FMC가 포함된 시나리오에서는 고가용성, 그런 다음 이 예에 표시된 대로 기본 및 보조 유닛이 표시 됩니다.

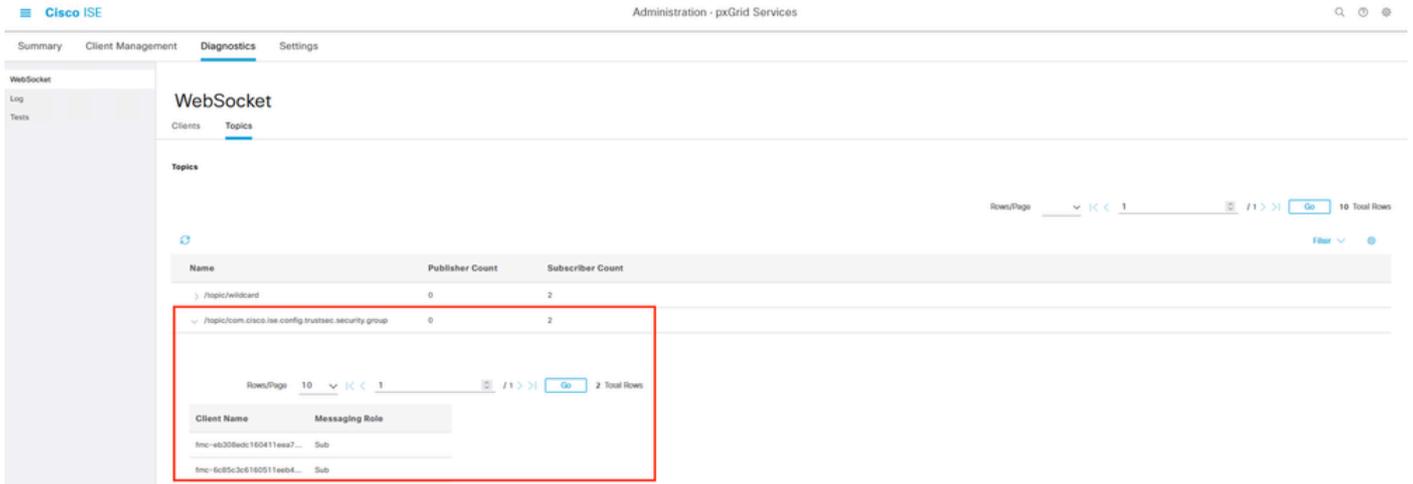


Client Name	Connect To	Session Id	Certificate	Subscriptions	Publications	IP Address	Status	Start time	Duration (dd:hh:mm:ss)
fmc-eb308edc160411ea47...	x	sxpria01	Session Id	Certificate	Subscriptions	Publications	IP Address	Start time	Duration (dd:hh:mm:ss)
fmc-eb308edc160411ea47...	x	sxpria01	sxpria01.5	CN=aspt_fmc01...	/topic/com.cisco.ise.sessio...	10.4.49.51	Connected	2023-08-21 05:30:18 MDT	01:10:19.42
fmc-6d5c3d160511ea4...	x	sxpria01	sxpria01.6	CN=aspt_fmc01...	/topic/com.cisco.ise.sessio...	10.4.49.52	Connected	2023-08-21 05:31:56 MDT	01:10:18.03

ISE에서 사용할 수 있는 WebSockets.

다음 탭에서 이 메뉴에서 지명 Topics, 다음을 수행할 수 있습니다. fmc 가입자가 ISE에서 게시한 pxGrid 주제에 추가되었는지 확인합니다.

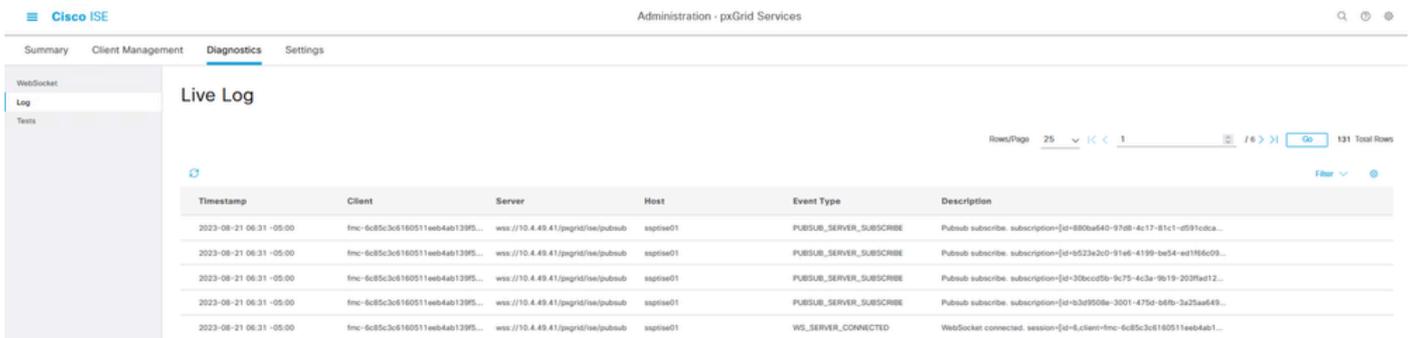
예를 들어, 보안 그룹 위치 당신 두 FMC 모두 가입 및 수신 관련 정보 수신 SGT ISE에서 게시했습니다.



pxGrid 가입자당 항목 수

메뉴 Administration(관리) > pxGrid Services(pxGrid 서비스) > Diagnostics(진단) > Log(로그), 중요한 이벤트 pxGrid 통신에서 관련(활성화된 기능이 활성화된 노드에 해당)이 표시됩니다.

통합과 관련된 정보를 보여 줍니다.



PxGrid 라이브 로그

문제 해결

FMC에서 트러블슈팅을 수행합니다.

FMC가 호스트 이름으로 자체 호스트 이름 및 ISE 노드를 확인할 수 있는지 확인합니다.

예를 들면 다음과 같습니다.

<#root>

```
> expert
admin@sspt_fmc01_lab:~$ ping sspt_fmc01_lab

PING sspt_fmc01_lab (10.4.49.51) 56(84) bytes of data.
64 bytes from sspt_fmc01_lab (10.4.49.51): icmp_seq=1 ttl=64 time=0.029 ms
64 bytes from sspt_fmc01_lab (10.4.49.51): icmp_seq=2 ttl=64 time=0.071 ms
64 bytes from sspt_fmc01_lab (10.4.49.51): icmp_seq=3 ttl=64 time=0.055 ms
^C
--- sspt_fmc01_lab ping statistics ---
3 packets transmitted, 3 received,
0% packet loss, time 27ms

admin@sspt_fmc01_lab:~$ ping ssptise01
PING ssptise01.ssptsec.mex (10.4.49.41) 56(84) bytes of data.
64 bytes from ssptise01.ssptsec.mex (10.4.49.41): icmp_seq=1 ttl=64 time=0.586 ms
64 bytes from ssptise01.ssptsec.mex (10.4.49.41): icmp_seq=2 ttl=64 time=0.646 ms
64 bytes from ssptise01.ssptsec.mex (10.4.49.41): icmp_seq=3 ttl=64 time=0.743 ms
^C
--- ssptise01.ssptsec.mex ping statistics ---
3 packets transmitted, 3 received,
0% packet loss, time 82ms
rtt min/avg/max/mdev = 0.586/0.658/0.743/0.068 ms
admin@sspt_fmc01_lab:~$
admin@sspt_fmc01_lab:~$ ping ssptise02

PING ssptise02.ssptsec.mex (10.4.49.42) 56(84) bytes of data.
64 bytes from ssptise02.ssptsec.mex (10.4.49.42): icmp_seq=1 ttl=64 time=0.588 ms
64 bytes from ssptise02.ssptsec.mex (10.4.49.42): icmp_seq=2 ttl=64 time=0.609 ms
64 bytes from ssptise02.ssptsec.mex (10.4.49.42): icmp_seq=3 ttl=64 time=0.628 ms
^C
--- ssptise02.ssptsec.mex ping statistics ---
3 packets transmitted, 3 received
, 0% packet loss, time 45ms
rtt min/avg/max/mdev = 0.588/0.608/0.628/0.025 ms
```

다음을 확인합니다. ADI 프로세스가 실행 중입니다.

```
<#root>
```

```
>
```

```
expert
```

```
sudo suadmin@sspt_fmc01_lab:~$
```

```
sudo su
```

```
root@sspt_fmc01_lab:/Volume/home/admin#
```

```
pmtool status | grep adi
```

adi (normal) - Running 7911

EFMC에서 ISE로의 통신이 port TCPP 8910이 허용됩니다. FMC에서 CLI Cisco는 구성 a tcpdump 패킷 캡처를 통해 양방향 통신을 확인합니다.

```
<#root>
```

```
>
```

```
expert
```

```
sudo suadmin@sspt_fmc01_lab:~$
```

```
sudo su
```

```
root@sspt_fmc01_lab:/Volume/home/admin#
```

```
tcpdump -i any tcp and port 8910
```

```
22:34:08.415370 IP
```

```
sspt_fmc01_lab.46248 > ssptise01.ssptsec.mex.8910
```

```
: Flags [S], seq 3033526171, win 29200, options [mss 1460,sackOK,TS val 2701166399 ecr 0,nop,wscale 7],  
22:34:08.415840 IP
```

```
ssptise01.ssptsec.mex.8910 > sspt_fmc01_lab.46248
```

```
: Flags [S.], seq 3024877968, ack 3033526172, win 28960, options [mss 1460,sackOK,TS val 2268665064 ecr  
22:34:08.415894 IP
```

```
sspt_fmc01_lab.46248 > ssptise01.ssptsec.mex.8910
```

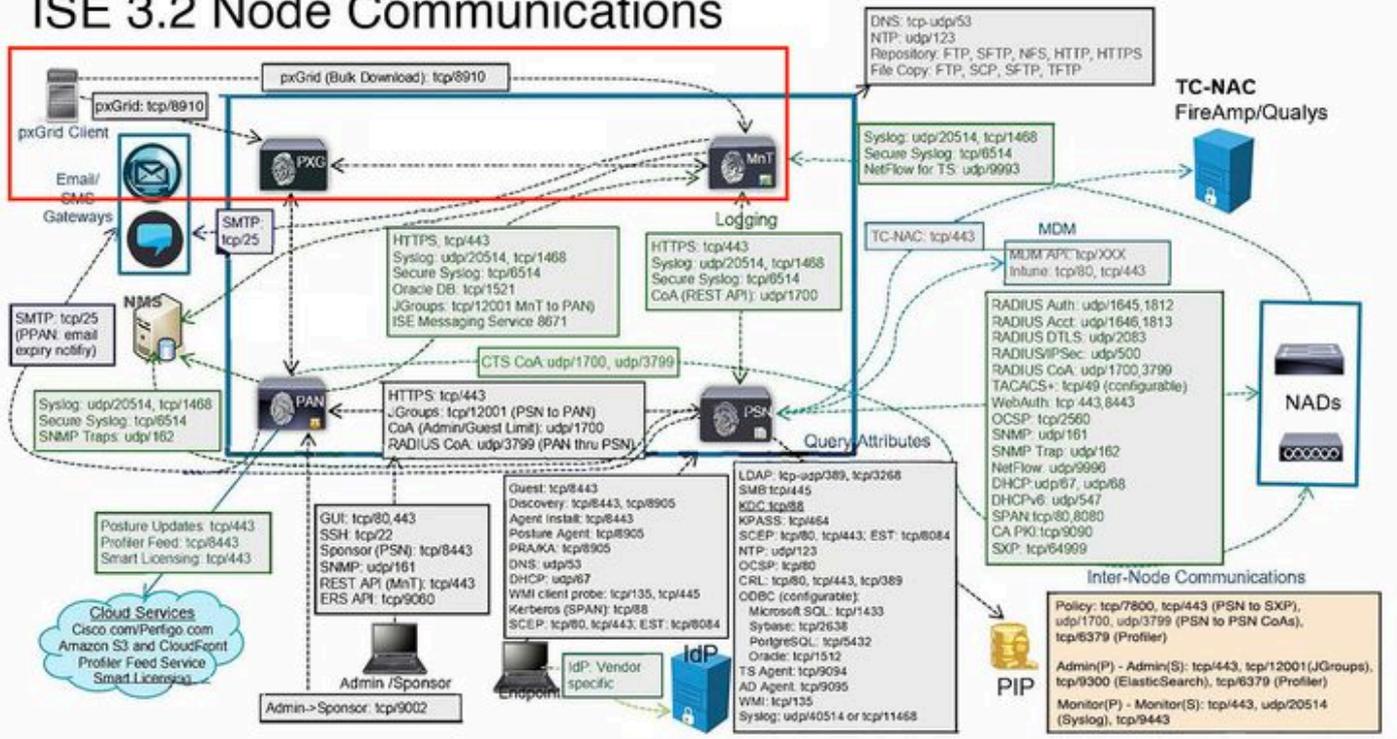
```
: Flags [.], ack 1, win 229, options [nop,nop,TS val 2701166400 ecr 2268665064], length 0  
[...]
```

ISE에서 트러블슈팅을 수행합니다.

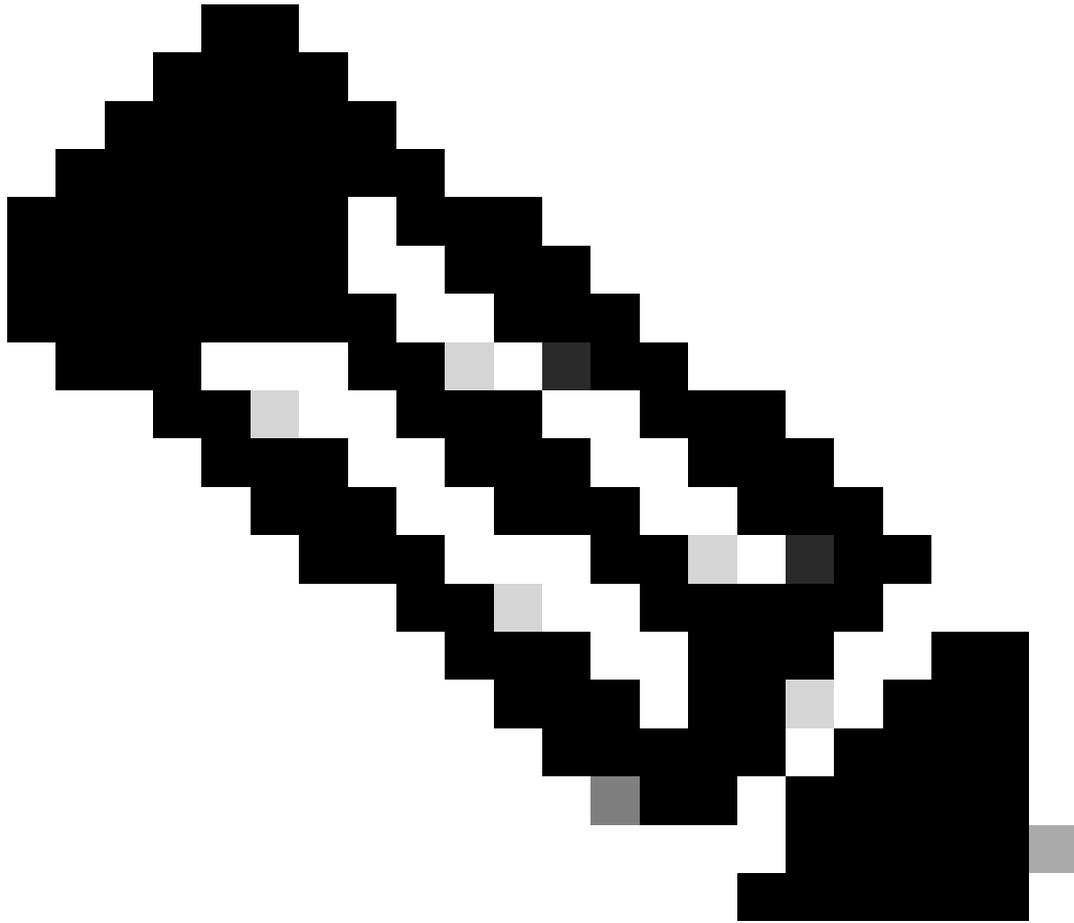
포트 8910의 통신 확인 운영 중입니다.

pxGrid 클라이언트에서 사용하는 포트입니다. 를 사용하여 정보의 대량 다운로드를 위해 pxGrid 노드 및 MnT 노드와 통신할 수 있습니다.

ISE 3.2 Node Communications



ISE 환경의 PxGrid 상호 작용



참고: 이 경우 pxGrid 클라이언트는 pxGrid 노드 및 보조 MNT(SMNT) 노드에 통신하여 정보의 (대량 다운로드)를 가져옵니다. SMNT에서 장애가 발생할 경우 기본 MNT를 통해 정보를 검색합니다.

lpxGrid 클라이언트와의 통신이 유지되는 ISE 노드에서 다음을 검토할 수 있습니다 이 포트: 열기 또는 에 연결된 소켓이 있는 경우 해당 포트.

```
#show ports | include 8910  
tcp: (output omitted), :::8910,
```

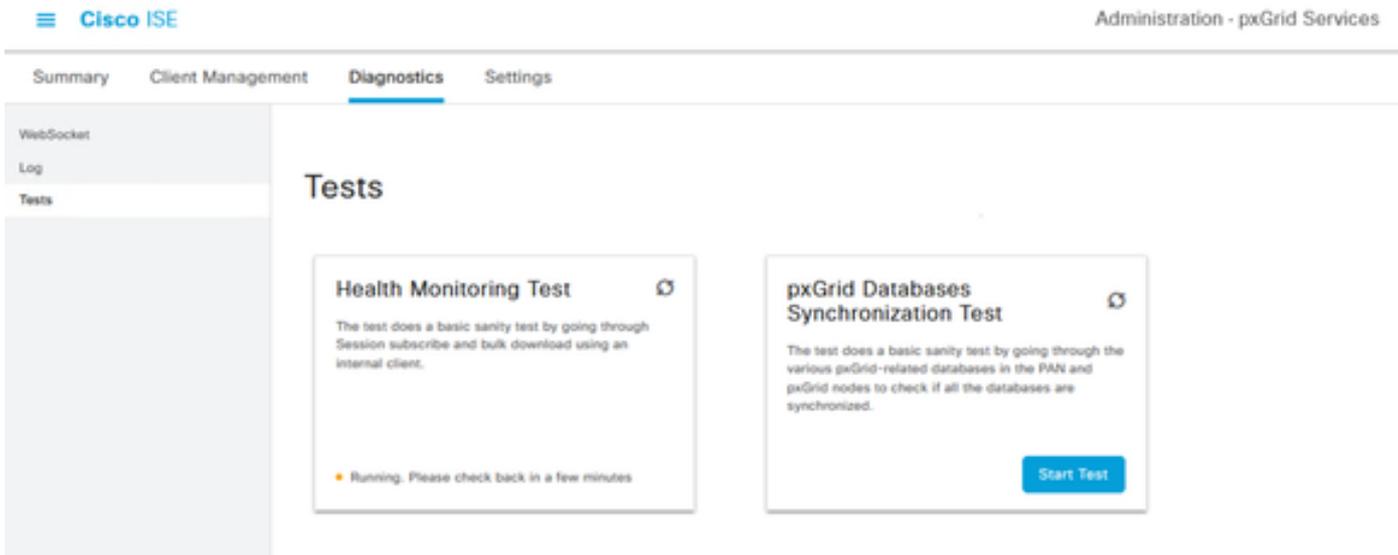
ISE에서는 pxGrid 구현의 전반적인 상태를 진단하는 2가지 테스트를 사용할 수 있습니다.

그것들은 메뉴에 있습니다 관리 > pxGrid 서비스 > 진단 > 테스트

이 섹션에 표시된 테스트는 ISE에서 내부적으로 수행됩니다.

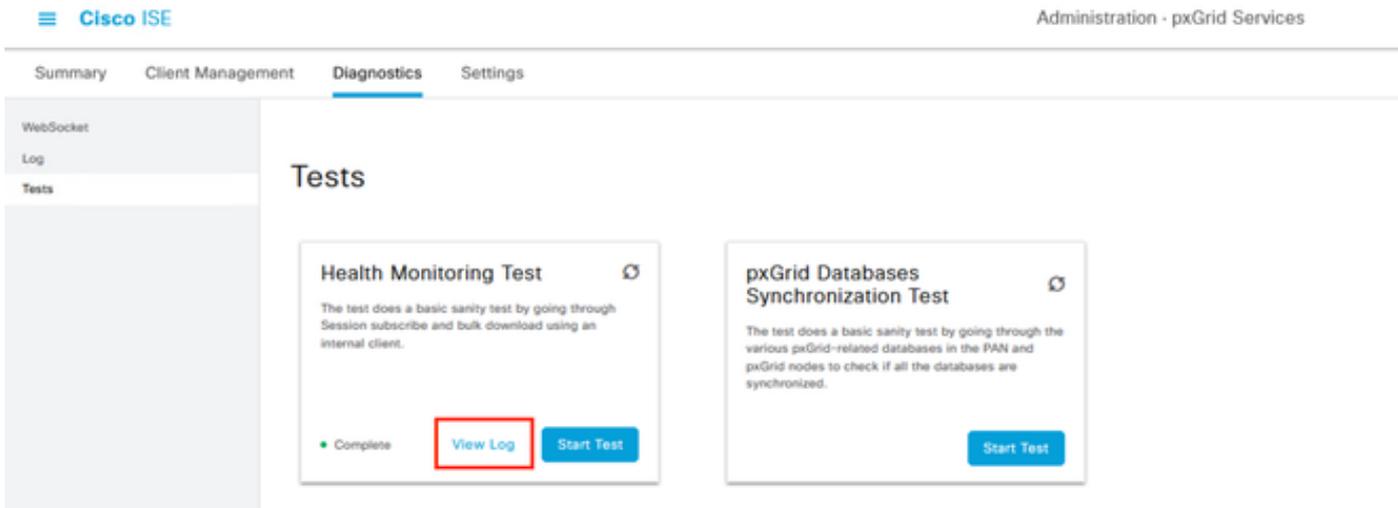
상태 모니터링 테스트 pxGrid 서비스 모양을 검토합니다.위로 클라이언트가 세션 디렉터리, 서비스 및 pxGrid 컨트롤러에서 게시한 주제에 액세스할 수 있는지 평가합니다.

다음을 선택합니다. 선택 시작하기 테스트 로그가 수집될 때까지 기다립니다.



PxGrid 상태 모니터링 테스트입니다.

테스트가 완료되면 선택 로그 보기. 이 예에서는 로그의 내용입니다 이(가):



상태 모니터링 테스트 검토

```

22-Aug-2023 17:03:13 [INFO] ***** pxGrid Session Directory Test *****
22-Aug-2023 17:03:13 [INFO] ----- Starting Connection Test -----
22-Aug-2023 17:03:14 [INFO] pxGrid Node: ssptise01.ssptsec.mex
22-Aug-2023 17:03:14 [INFO] wsPubsubServiceName=com.cisco.ise.pubsub
22-Aug-2023 17:03:14 [INFO] sessionTopic=/topic/com.cisco.ise.session
22-Aug-2023 17:03:14 [INFO] sessionRestBaseUrل=https://ssptise01.ssptsec.mex:8910/pxgrid/mnt/sd
22-Aug-2023 17:03:14 [INFO] wsUrل=wss://ssptise02.ssptsec.mex:8910/pxgrid/ise/pubsub
22-Aug-2023 17:03:15 [INFO] ----- Connection Test Completed -----
22-Aug-2023 17:03:15 [INFO] ----- Starting Download Test -----
22-Aug-2023 17:03:15 [INFO] Downloading sessions since 2023-08-21T17:03:15.273-06:00
22-Aug-2023 17:03:15 [INFO] Response status=200
22-Aug-2023 17:03:15 [INFO] Number of sessions read: 0
    
```

```

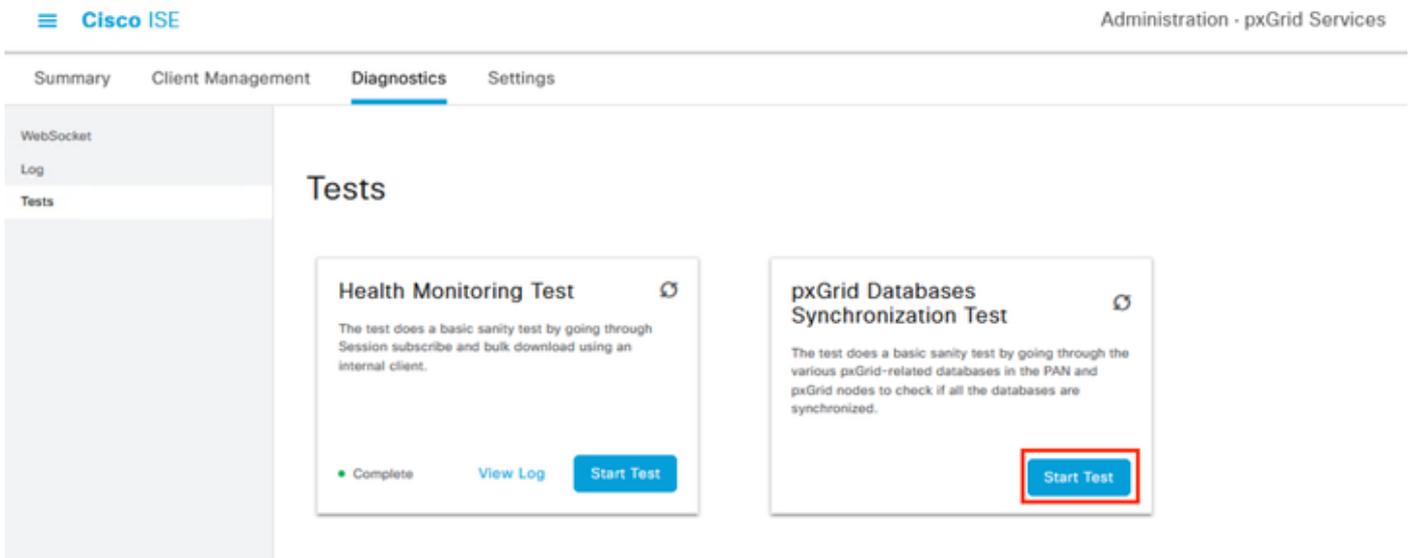
22-Aug-2023 17:03:15 [INFO] ----- Download Test Completed -----
22-Aug-2023 17:03:15 [INFO] ----- Starting Subscribe Test -----
22-Aug-2023 17:03:16 [INFO] STOMP CONNECT host=ssptise02.ssptsec.mex
22-Aug-2023 17:03:16 [INFO] STOMP SUBSCRIBE topic=/topic/com.cisco.ise.session
22-Aug-2023 17:03:16 [INFO] STOMP CONNECTED version=1.2
22-Aug-2023 17:07:16 [INFO] A total of 0 notifications were received.
22-Aug-2023 17:07:16 [INFO] STOMP RECEIPT id=77
22-Aug-2023 17:07:19 [INFO] ----- Subscribe Test Completed -----
22-Aug-2023 17:07:19 [INFO] ***** pxGrid Session Directory Test Complete *****

```

PxGrid 데이터베이스 동기화 테스트는 다음을 확인합니다. 정보 데이터베이스 내에서 PAN 노드와 pxGrid 노드 간에 올바르게 동기화됩니다.

따라서 pxGrid 가입자에게 전송되는 정보는 다음과 같습니다 정확합니다.

다음을 선택합니다. 선택 테스트 시작 결과가 나올 때까지 기다립니다.



PxGrid 데이터베이스 동기화 테스트입니다.

생성된 로그에서 이 출력을 얻었습니다.

```

ssptise01.ssptsec.mex : In Sync
ssptise02.ssptsec.mex : In Sync

```

```

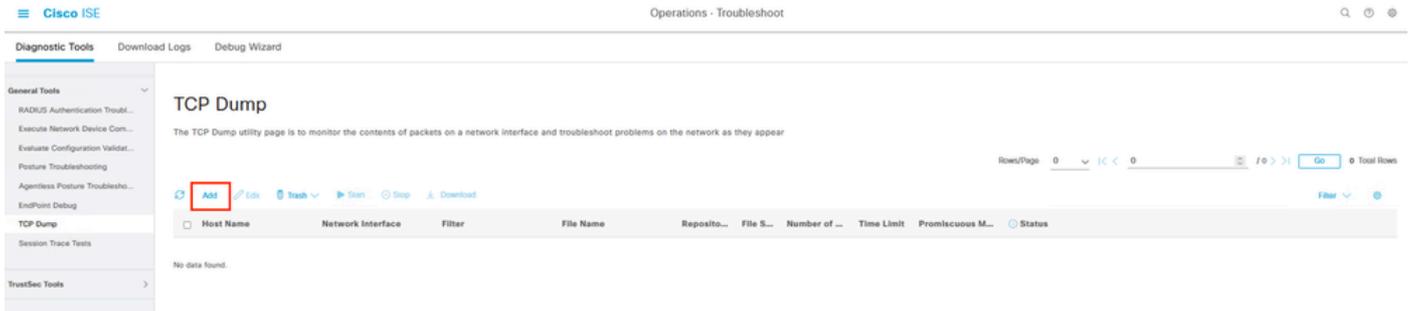
Primary PAN : ssptise01.ssptsec.mex
pxGrid Nodes : ssptise01.ssptsec.mex ssptise02.ssptsec.mex

```

캡처 수집 기본 FMC 노드를 가리키는 pxGrid 노드에서

메뉴로 이동 Operations(운영) > Troubleshoot(문제 해결) > Diagnostic Tools(진단 도구) > TCP Dump,

다음을 선택합니다. 선택 수신 추가 새로운 캡처.



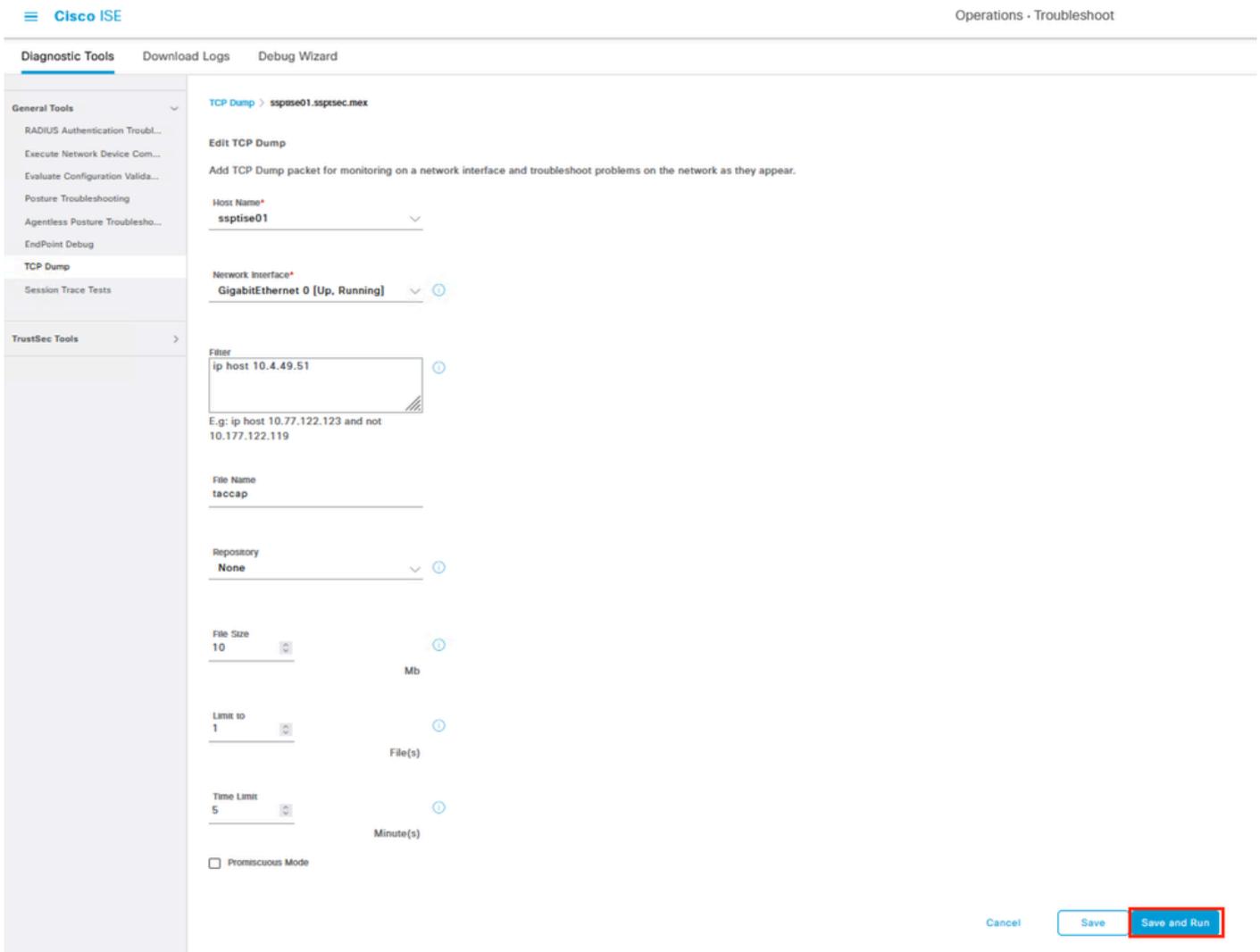
ISE에서 패킷 캡처 생성

캡처에 대한 매개변수를 구성합니다.

수신 호스트 이름, fmc에서 선택한 주 pxGrid 노드를 선택합니다.

필터 이 트래픽의 구문 ip 호스트 <FMC IP>

캡처 이름 지정 그리고 진행 수신 저장 및 실행.



패킷 캡처 컨피그레이션의 예

다른 창의 FMC 메뉴에서 Integration(통합) > Other Integrations(기타 통합) > Identity(ID) 소스, pxGrid 채널을 통해 ISE와의 연결을 테스트합니다.

W테스트 결과가 나오면 진행 수신 초꼭대기 ISE의 캡처.

The screenshot shows the Cisco ISE interface for the 'TCP Dump' utility. The 'Stop' button is highlighted with a red box. The table below shows the configuration for the dump:

Host Name	Network Interface	Filter	File Name	Repository	File S...	Number of ...	Time Limit	Promiscuous M...	Status
ssptise01.asptsec.mex	GigabitEthernet 0 [Up, Run...	ip host 10.4.49.51	taccap		10	1	5	false	RUNNING

ISE에서 패킷 캡처를 중지합니다.

다운로드 분석을 캡처하고 시작합니다. 이 시나리오에서는 참조 역할을 할 수 있는 작업 연결의 캡처를 표시합니다.

10.4.49.51	10.4.49.41	TCP	74	47508	→	8910	[SYN]	Seq=0	Win=29200	Len=0	MSS=1460	SACK_PERM	TSval=2738457626	TSecr=0	WS=128	
10.4.49.41	10.4.49.51	TCP	74	8910	→	47508	[SYN, ACK]	Seq=0	Ack=1	Win=28968	Len=0	MSS=1460	SACK_PERM	TSval=2305956319	TSecr=2738457626	WS=128
10.4.49.51	10.4.49.41	TCP	66	47508	→	8910	[ACK]	Seq=1	Ack=1	Win=29312	Len=0	TSval=2738457627	TSecr=2305956319			
10.4.49.51	10.4.49.41	TLSv1.2	389				Client Hello									
10.4.49.41	10.4.49.51	TCP	66	8910	→	47508	[ACK]	Seq=1	Ack=324	Win=30080	Len=0	TSval=2305956319	TSecr=2738457627			
10.4.49.41	10.4.49.51	TCP	7306	8910	→	47508	[ACK]	Seq=1	Ack=324	Win=30080	Len=7240	TSval=2305956341	TSecr=2738457627	[TCP segment of a reassembled PDU]		
10.4.49.41	10.4.49.51	TLSv1.2	462				Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done									
10.4.49.51	10.4.49.41	TCP	66	47508	→	8910	[ACK]	Seq=324	Ack=7637	Win=44544	Len=0	TSval=2738457650	TSecr=2305956341			
10.4.49.51	10.4.49.41	TLSv1.2	1783				Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message									
10.4.49.41	10.4.49.51	TCP	66	8910	→	47508	[ACK]	Seq=7637	Ack=2041	Win=33536	Len=0	TSval=2305956345	TSecr=2738457653			
10.4.49.41	10.4.49.51	TLSv1.2	72				Change Cipher Spec									
10.4.49.41	10.4.49.51	TLSv1.2	111				Encrypted Handshake Message									
10.4.49.51	10.4.49.41	TCP	66	47508	→	8910	[ACK]	Seq=2041	Ack=7688	Win=44544	Len=0	TSval=2738457658	TSecr=2305956349			
10.4.49.51	10.4.49.41	TLSv1.2	99				Application Data									
10.4.49.41	10.4.49.51	TCP	66	8910	→	47508	[ACK]	Seq=7688	Ack=2074	Win=33536	Len=0	TSval=2305956391	TSecr=2738457658			
10.4.49.51	10.4.49.41	TLSv1.2	615				Application Data, Application Data									
10.4.49.41	10.4.49.51	TCP	66	8910	→	47508	[ACK]	Seq=7688	Ack=2623	Win=36480	Len=0	TSval=2305956391	TSecr=2738457659			
10.4.49.41	10.4.49.51	TLSv1.2	515				Application Data									
10.4.49.41	10.4.49.51	TLSv1.2	100				Application Data									
10.4.49.51	10.4.49.41	TCP	66	47508	→	8910	[ACK]	Seq=2623	Ack=8171	Win=47488	Len=0	TSval=2738457708	TSecr=2305956400			
10.4.49.51	10.4.49.41	TCP	66	47508	→	8910	[FIN, ACK]	Seq=2623	Ack=8171	Win=47488	Len=0	TSval=2738457708	TSecr=2305956400			
10.4.49.41	10.4.49.51	TLSv1.2	97				Encrypted Alert									
10.4.49.41	10.4.49.51	TCP	66	8910	→	47508	[FIN, ACK]	Seq=8202	Ack=2624	Win=36480	Len=0	TSval=2305956401	TSecr=2738457708			

ISE와 FMC 간의 PxGrid 통신

또한 ISE에서는 px와 관련된 디버그를 수집할 수 있습니다그리드 처리.

메뉴 탐색 작업 이 >> 디버그 마법사 > 디버그 문제 해결 로그 컨피그레이션, 분석할 해당 ISE 노드를 선택한 다음 편집.

The screenshot shows the Cisco ISE interface for the 'Debug Wizard'. The 'Edit' button is highlighted with a red box. The 'Node List' table below shows the configuration for the debug:

Node Name	Replication Role
ssptise01	PRIMARY
ssptise02	SECONDARY

ISE에서 디버깅할 노드 선택

표시된 구성 요소를 필터링하고 로그 수준: pxgrid 디버그 구성 요소 수신 진행 분석 기능을 제공합니다

저장 구성합니다.

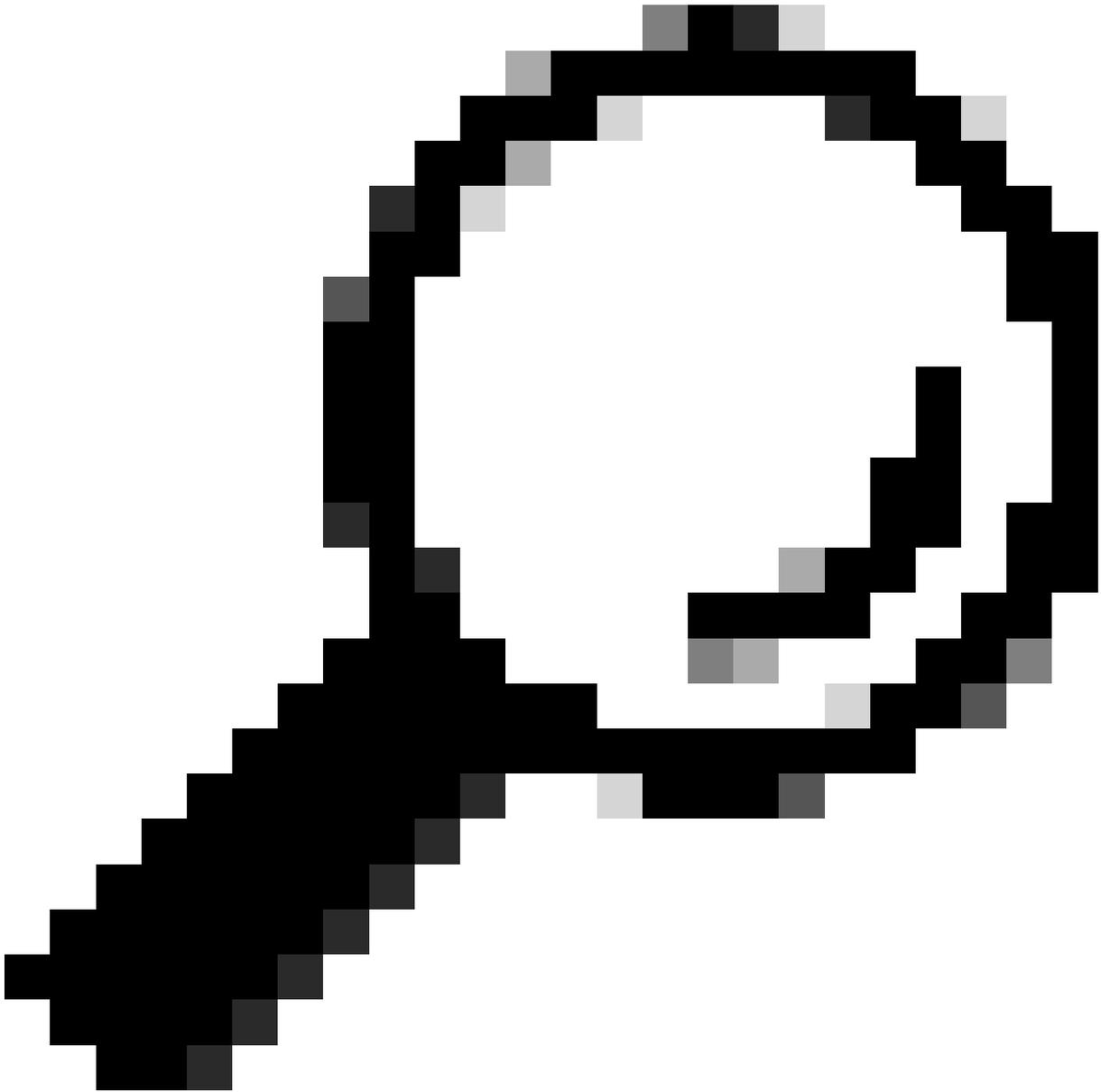
The screenshot shows the Cisco ISE interface for configuring debug levels. The page title is "Debug Level Configuration" and it is part of the "Debug Wizard" under "Diagnostic Tools". The node is identified as "ssptise01.sspsec.mex". There are buttons for "Edit" and "Reset to Default". A table lists the components and their current log levels:

Component Name	Log Level	Description	Log file Name
pxgrid	DEBUG	pxGrid messages	pxgrid-server.log
pxGrid Cloud	INFO	pxGrid Cloud messages	pxcloud.l Save Cancel
pxGrid Direct	INFO	pxGrid Direct backend and UI log messages	ise-pxgriddirect.log, pxgriddirect.log

pxGrid 구성 요소를 디버그 레벨로 변경합니다.

분석할 동작을 재현한 다음 진행 - pxgrid-server.log 파일에 수집된 로그를 분석합니다. 기타 로그 ISE 노드에서 문제 해결을 검토할 수 있는 항목은 다음과 같습니다.

```
#show logging application | include pxgrid  
ise-pxgriddirect.log  
pxgrid/pxgrid-server.log  
pxgrid/pxgrid-test.log  
pxgrid/pxgrid_dbsync_summary.log  
pxgrid/pxgrid_internal_dbsync_summary.log  
pxgriddirect.log
```

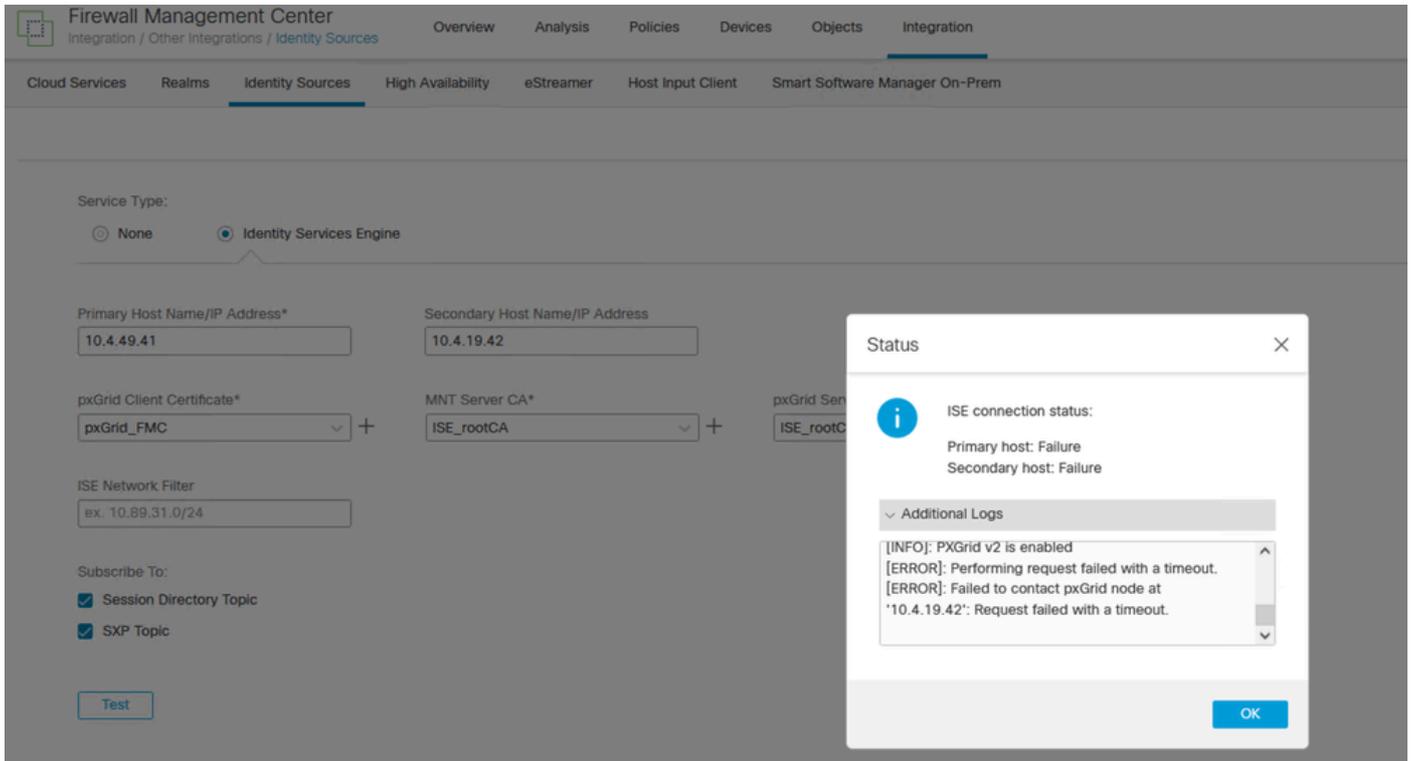


팁: 추가 로그 수집 권장 사항을 보려면 [ISE 3.x 버전에서 디버그를 활성화하는 방법을 비디오에서 검토하십시오.](#)

일반적인 문제.

PxGrid 가입자 클라이언트는 ISE에서 승인되지 않습니다.

이 활용 사례의 경우 FMC 테스트 pxGrid 버튼과 관련된 출력에 다음 동작이 표시됩니다.



FMC pxGrid 연결에 실패했습니다.

Primary host:

```
[INFO]: PXGrid v2 is enabled
[ERROR]: pxgrid 2.0: failed account activation. accountState=PENDING
[ERROR]: Failed to contact pxGrid node at '10.4.49.41': pxgrid2.0: Could not activate account
```

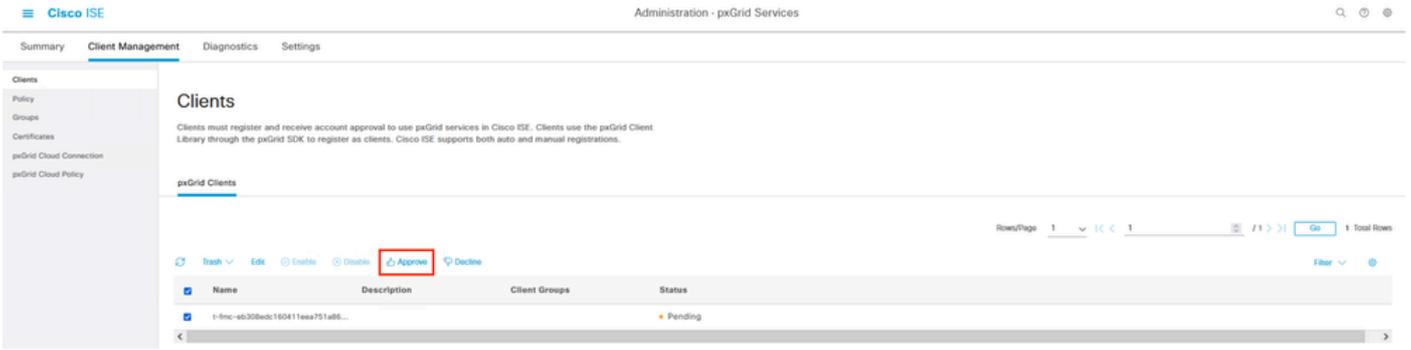
Secondary host:

```
[INFO]: PXGrid v2 is enabled
[ERROR]: Performing request failed with a timeout.
[ERROR]: Failed to contact pxGrid node at '10.4.19.42': Request failed with a timeout.
```

ISE에서 Administration(관리) > PxGrid Services(PxGrid 서비스) > Client Management(클라이언트 관리) > Clients(클라이언트)의 메뉴에서 FMC(pxGrid 클라이언트)가 승인 대기 중임을 나타내는 동작을 확인합니다.

승인 버튼을 선택하고, 다음 창에서 선택을 확인한 후 통합을 다시 시도합니다.

이번에는 통합이 성공했습니다.



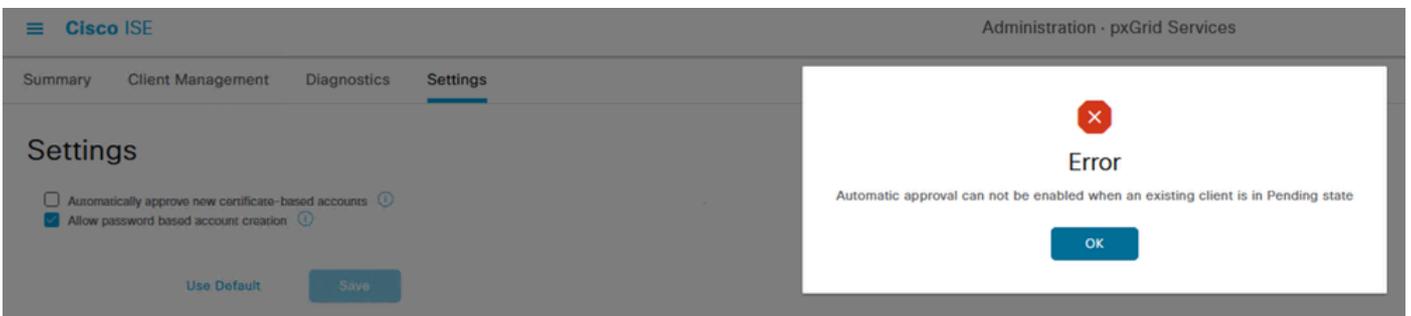
FMC 클라이언트가 보류 중 상태입니다.



pxGrid 클라이언트의 승인 확인

인증서 기반 pxGrid 클라이언트의 자동 승인을 활성화하려는 경우 주의하십시오.

이전 페이지에서 클라이언트를 승인/거부합니다(이 경보가 나타날 수 있음).



pxGrid 클라이언트 승인과 관련된 오류입니다.

PxGrid ISE 인증서 사슬 불완전해.

이 시나리오에서 Administration(관리) > System(시스템) > Certificate(인증서) 메뉴로 이동하면 pxgrid 인증서를 선택하고 View(보기) 옵션을 선택합니다.

인증서에 문제가 있는 경우 이러한 관련 오류가 발생할 수 있습니다.

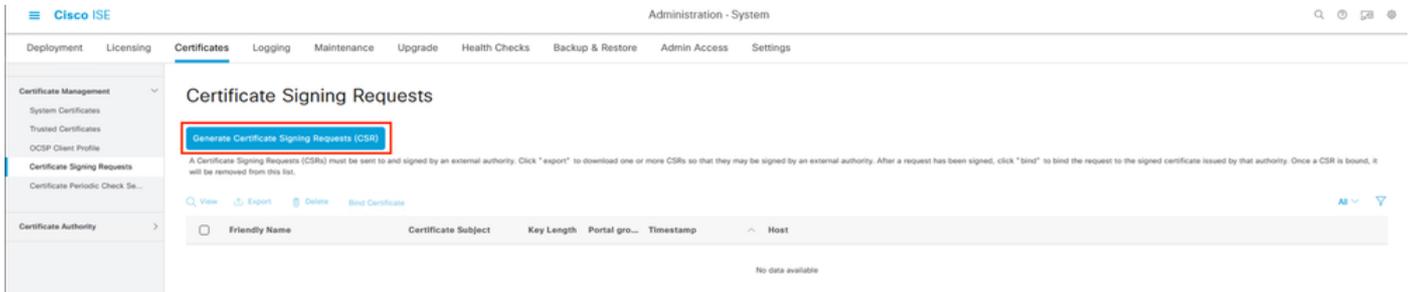
 Certificate trust chain is incomplete

인증서 체인과 관련된 오류가 발생했습니다.

T확인해야 할 첫 번째 단계는 ISE 루트 CA가 완전한지 여부입니다View(보기) 옵션을 클릭합니다.

계층 구조에 인증서가 없는 경우 전체 ISE 구축 루트 CA를 발급할 수 있습니다.

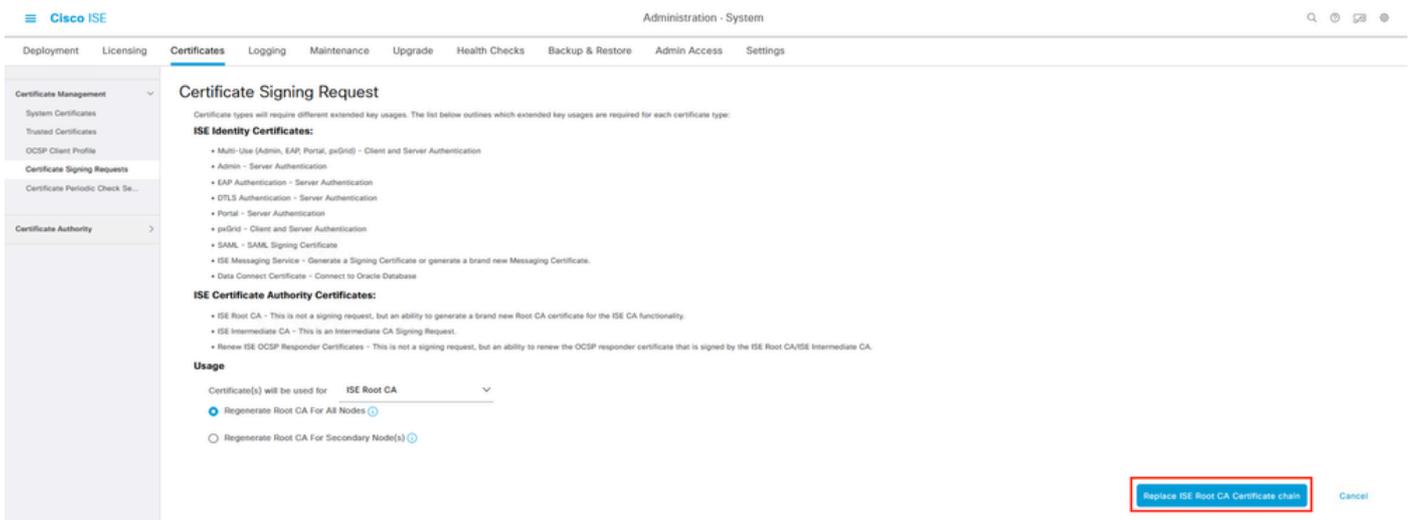
B메뉴 관리 > 시스템 > 인증서 > 인증서 관리 > 인증서 서명 요청 (CSR) 및 단추를 선택합니다.



ISE에서 CSR 생성

이 메뉴에서 사용 ISE 루트 CA 모든 노드에 대해 ISE 루트 CA를 재생성합니다.

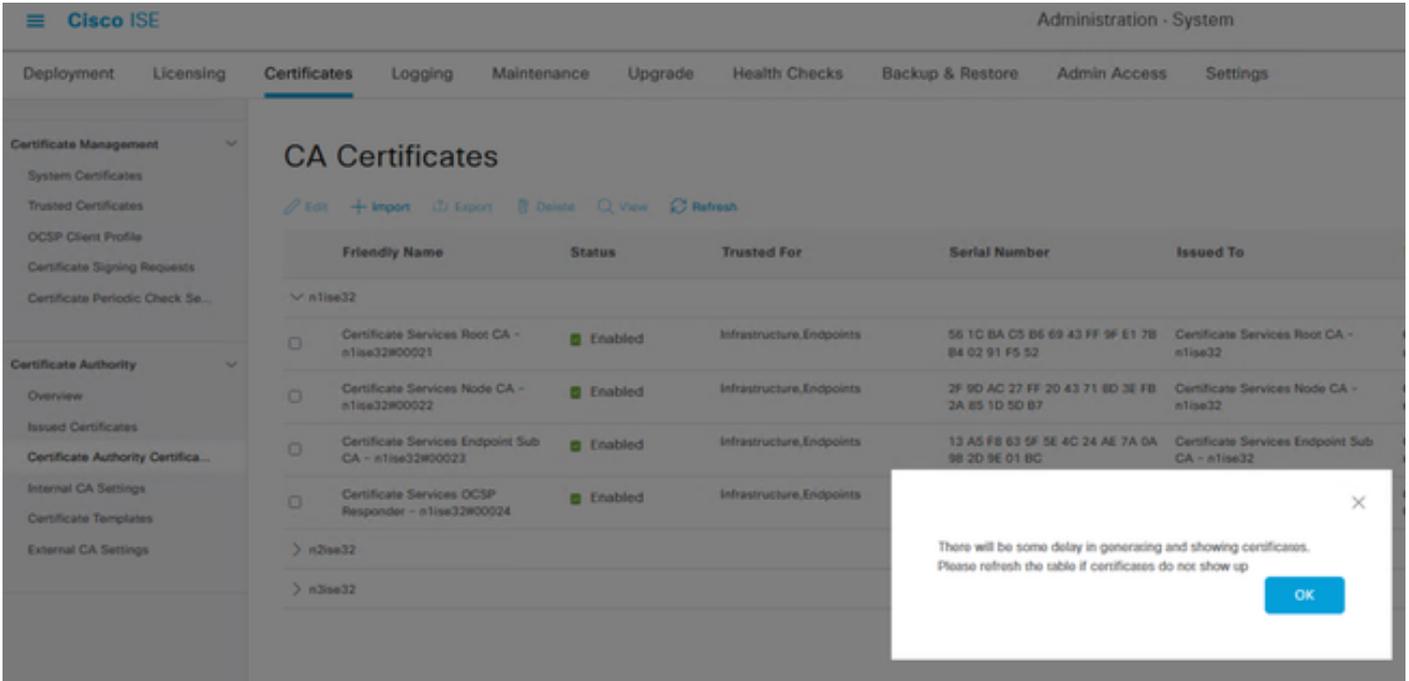
단추를 계속 진행합니다. ISE 루트 CA 인증서 체인 교체.



Certificate Signing Request 구성

IMP의 모든 노드에서 인증서가 생성될 때까지 기다립니다실행.

완료되면 ISE는 다음 알림을 표시합니다.



인증서 생성 확인

px가Grid 인증서 신뢰 체인이 완료되었습니다. 옵션을 선택하여 보기 시스템 인증서에 있습니다.

참조.

[PxGrid Cisco 개발자 페이지](#)

[Cisco Identity Services Engine 관리자 가이드, 릴리스 3.2, 장: Cisco pxGrid입니다.](#)

[Cisco Identity Services Engine 설치 설명서, 릴리스 3.2, 장: Cisco ISE 포트 참조](#)

[Cisco Identity Services Engine CLI 참조 가이드, 릴리스 2.4](#)

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.