

ISE 2.4 및 FMC 6.2.3 pxGrid 통합 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[ISE 구성](#)

[1단계. pxGrid 서비스 활성화](#)

[2단계. 모든 pxGrid 인증서 기반 계정을 승인하도록 ISE 구성](#)

[3단계. ISE MNT 관리자 인증서 및 pxGrid CA 인증서 내보내기](#)

[FMC 구성](#)

[4단계. FMC에 새 영역 추가](#)

[5단계. FMC CA 인증서 생성](#)

[6단계. OpenSSL을 사용하여 생성된 인증서에서 인증서 및 개인 키 추출](#)

[7단계. FMC에 인증서 설치](#)

[8단계. ISE로 FMC 인증서 가져오기](#)

[9단계. FMC에서 pxGrid 연결 구성](#)

[다음을 확인합니다.](#)

[ISE에서 확인](#)

[FMC에서 확인](#)

[문제 해결](#)

소개

이 문서에서는 ISE pxGrid 버전 2.4 및 FMC 버전 6.2.3의 통합을 위한 컨피그레이션 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ISE 2.4
- FMC 6.2.3
- Active Directory/LDAP(Lightweight Directory Access Protocol)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 독립형 ISE 2.4

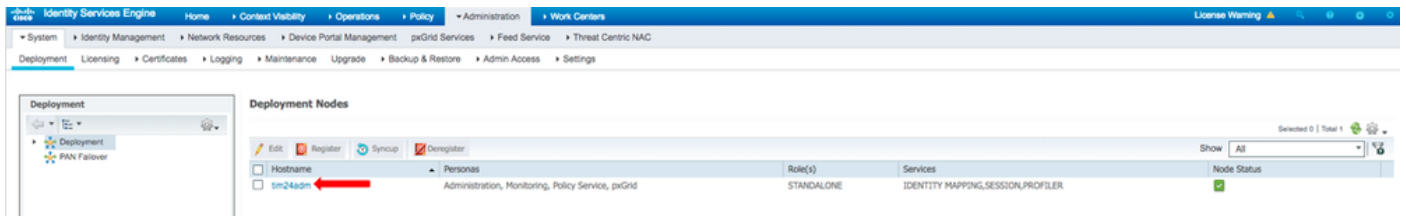
- FMCv 6.2.3
- Active Directory 2012R2
- ISE(Identity Services Engine) pxGrid 버전 2.4
- Firepower Management Center(FMC) 버전 6.2.3

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.

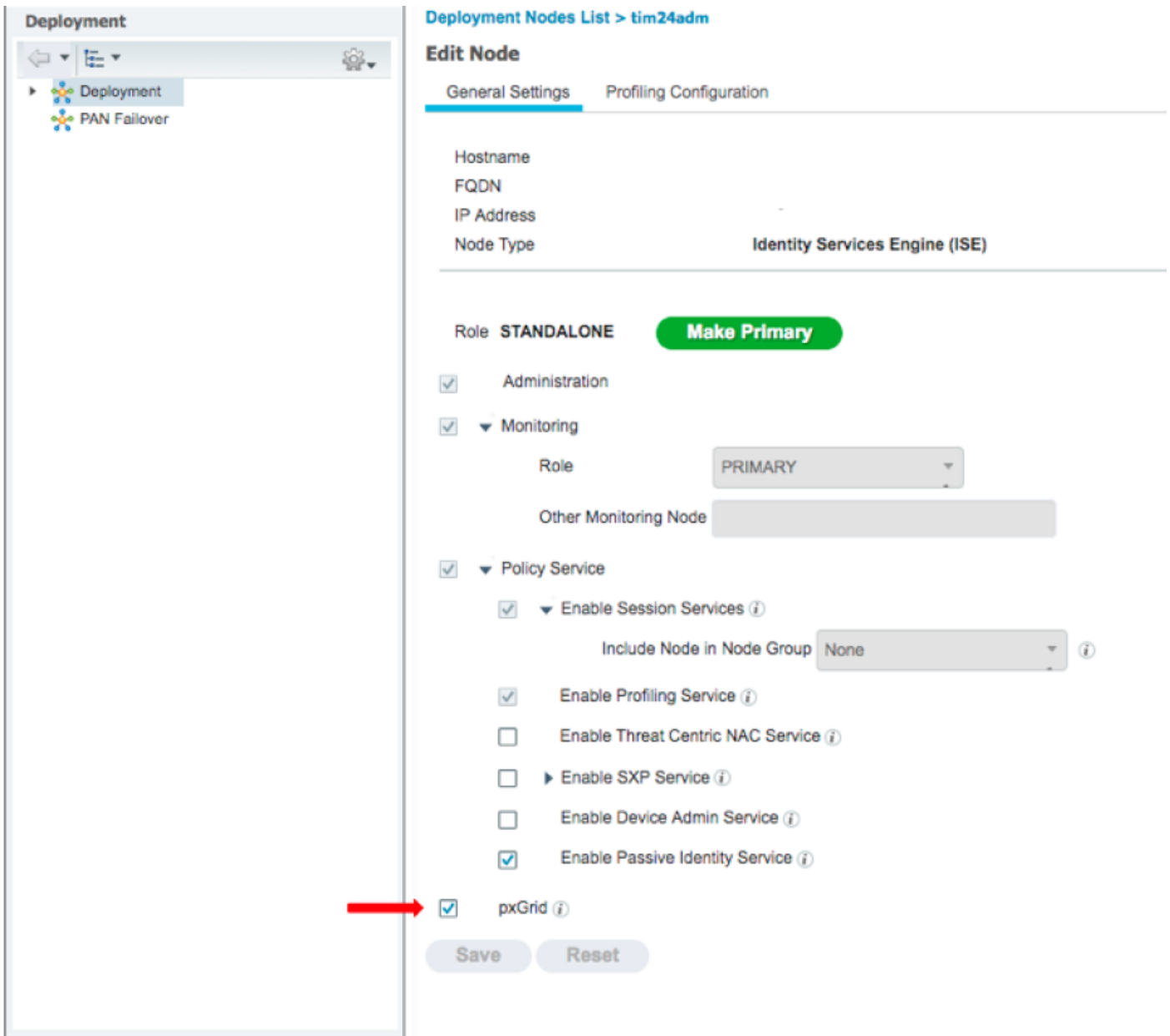
ISE 구성

1단계. pxGrid 서비스 활성화

1. ISE Admin GUI에 로그인하고 Administration(관리) > Deployment(구축)로 이동합니다.
2. pxGrid 페르소나에 사용할 ISE 노드를 선택합니다.



3. pxGrid 서비스를 활성화하고 그림과 같이 **Save(저장)**를 클릭합니다.



4. pxGrid 서비스가 CLI에서 실행되는지 확인합니다.

참고: 둘 이상의 pxGrid 노드가 사용 중인 경우, pxGrid 서비스가 완전히 시작되고 HA(고가용성) 상태를 확인하려면 이 프로세스에 최대 5분이 필요합니다.

5. ISE pxGrid 노드 CLI에 SSH를 적용하고 애플리케이션 상태를 확인합니다.

```
# show application status ise | in pxGrid
pxGrid Infrastructure Service running 24062
pxGrid Publisher Subscriber Service running 24366
pxGrid Connection Manager running 24323
pxGrid Controller running 24404
#
```

6. ISE 관리 GUI에 액세스하여 서비스가 온라인 상태이고 작동하는지 확인합니다. Administration(관리) > **pxGrid Services(pxGrid 서비스)**로 이동합니다.

7. ISE는 페이지 하단에 Connected to pxGrid <pxGrid node FQDN>을 표시합니다.

Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log
ise-mnt-tim24adm		Capabilities(2 Pub, 1 Sub)	Online (OKPP)	Internal	Certificate	View
ise-fincut-tim24adm		Capabilities(0 Pub, 0 Sub)	Online (OKPP)	Internal	Certificate	View
ise-pubsub-tim24adm		Capabilities(0 Pub, 0 Sub)	Online (OKPP)	Internal	Certificate	View
ise-bridge-tim24adm		Capabilities(0 Pub, 4 Sub)	Online (OKPP)	Internal	Certificate	View
ise-admin-tim24adm		Capabilities(4 Pub, 2 Sub)	Online (OKPP)	Internal	Certificate	View
iseagent-freepower-20762a2982d...		Capabilities(0 Pub, 6 Sub)	Online (OKPP)		Certificate	View
fireightsitest-freepower-20762a...		Capabilities(0 Pub, 0 Sub)	Offline (OKPP)		Certificate	View

2단계. 모든 pxGrid 인증서 기반 계정을 승인하도록 ISE 구성

1. Administration(관리) > pxGrid Services(pxGrid 서비스) > Settings(설정)로 이동합니다.
2. "새 인증서 기반 계정을 자동으로 승인" 확인란을 선택하고 저장을 클릭합니다.

PxGrid Settings

Automatically approve new certificate-based accounts
 Allow password based account creation

Use Default Save

Test

Connected to pxGrid tim24adm.rtpaaa.net

참고: 이 옵션이 활성화되지 않은 경우 관리자는 ISE에 대한 FMC 연결을 수동으로 승인해야 합니다.

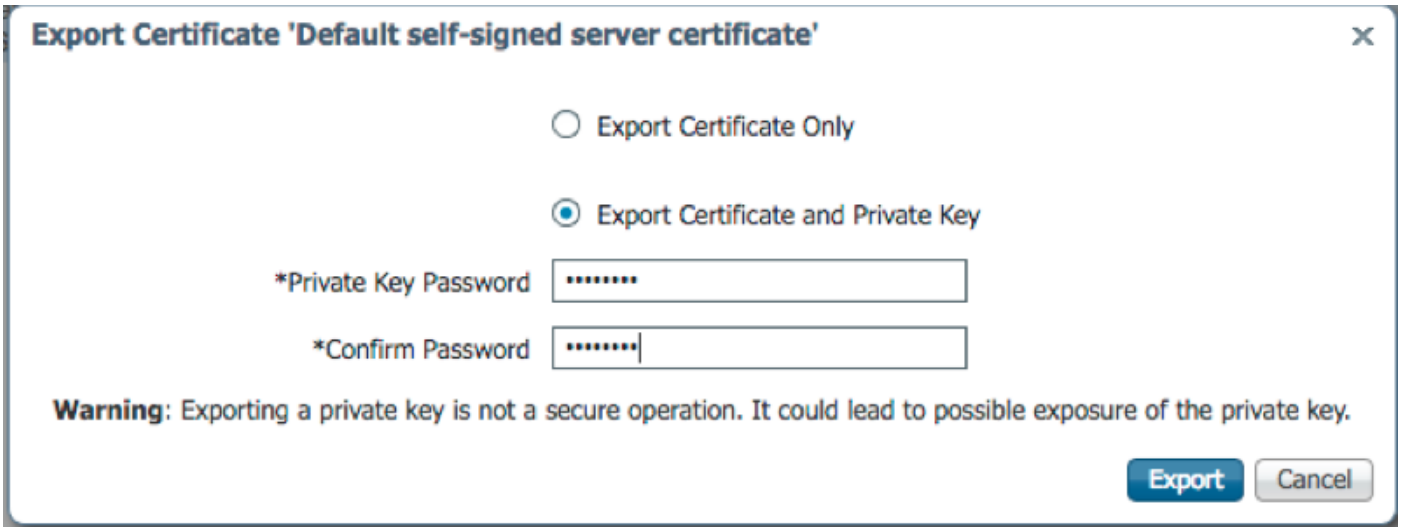
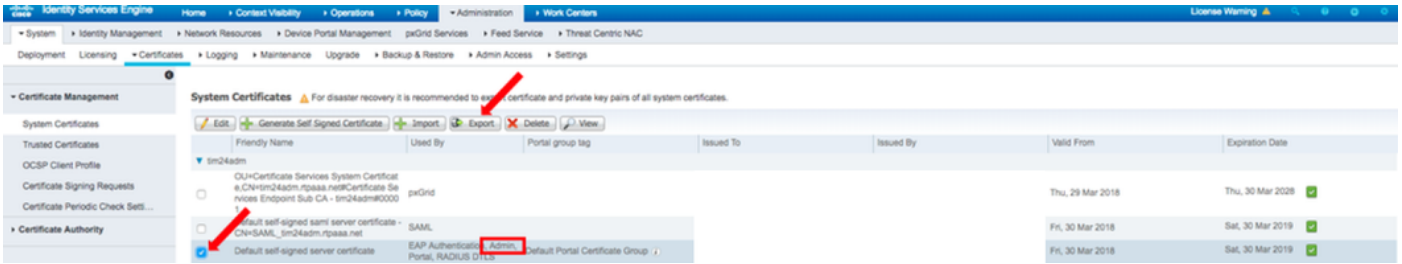
3단계. ISE MNT 관리자 인증서 및 pxGrid CA 인증서 내보내기

1. Administration > Certificates > System Certificates로 이동합니다.
2. 기본 관리 노드에서 활성화되지 않은 경우 MNT(기본 모니터링) 노드를 확장합니다.
3. Used-By "Admin" 필드가 있는 인증서를 선택합니다.

참고: 이 설명서에서는 기본 ISE 셀프 서명 인증서를 관리자 용도로 사용합니다. CA(Certificate Authority) 서명 관리 인증서를 사용하는 경우 ISE MNT 노드에서 관리 인증서에 서명한 루트 CA를 내보냅니다.

4. 익스포트를 클릭합니다.
5. 인증서 및 개인 키 내보내기 옵션을 선택합니다.
6. 암호화 키를 설정합니다.

7. 이미지에 표시된 대로 파일을 내보내고 저장합니다.

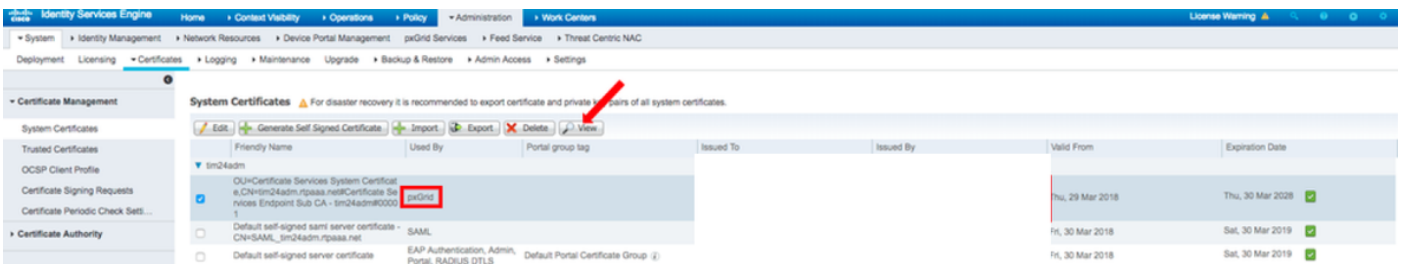


9. ISE 시스템 인증서 화면으로 돌아갑니다.

10. Used By 열에 "pxGrid" 사용량이 있는 인증서의 Issued By 필드를 확인합니다.

참고: 이전 버전의 ISE에서는 자체 서명 인증서였지만 2.2 이상부터는 기본적으로 내부 ISE CA 체인이 이 인증서를 발급합니다.

11. 인증서를 선택하고 이미지에 표시된 대로 보기를 클릭합니다.



12. 최상위(루트) 인증서를 확인합니다. 이 경우에는 "Certificate Services Root CA - tim24adm"입니다.

13. 이미지에 표시된 대로 인증서 보기 창을 닫습니다.

Certificate Hierarchy



Certificate Services Root CA - tim24adm
Certificate Services Node CA - tim24adm
Certificate Services Endpoint Sub CA - tim24adm

tim24adm.rtpaaa.net

tim24adm.rtpaaa.net
Issued By : Certificate Services Endpoint Sub CA - tim24adm
Expires : Thu, 30 Mar 2028 14:17:12 EDT

Certificate status is good

Details

Issued To

Common Name (CN)

Organization Unit (OU) **Certificate Services System Certificate**

Organization (O)

City (L)

State (ST)

Country (C)

Serial Number **58:2A:91:45:E8:23:42:74:98:53:06:94:33:9E:AD:83**

Close

14. ISE Certificate Authority 메뉴를 확장합니다.

15. 인증 기관 인증서를 선택합니다.

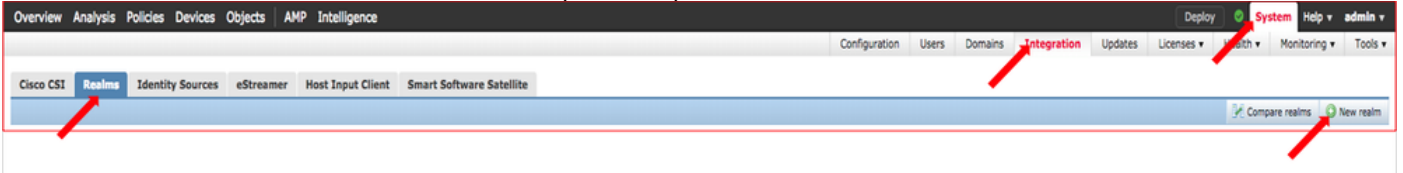
16. 식별된 루트 인증서를 선택하고 내보내기를 클릭합니다. 그런 다음 그림과 같이 pxGrid 루트 CA 인증서를 저장합니다.

Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiration Status
tim24adm								
<input type="checkbox"/> Certificate Services Endpoint Sub CA - tim24adm00003	Enabled	Infrastructure.Endpoints	32 D2 72 55 A9 7D 40 13 8F 2A EF CF 03 10 41 A8	Certificate Services Endpoint Sub	Certificate Services Node CA - tim24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2028	✔
<input checked="" type="checkbox"/> Certificate Services Root CA - tim24adm00001	Enabled	Infrastructure.Endpoints	36 67 74 15 A6 A8 4F EB 87 46 1 E7 37 1A A8 B8	Certificate Services Root CA - tim24adm	Certificate Services Root CA - tim24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2028	✔
<input type="checkbox"/> Certificate Services Node CA - tim24adm00002	Enabled	Infrastructure.Endpoints	30 1A 22 E7 AA E5 45 35 8C 65 78 E5 03 09 34 3E	Certificate Services Node CA - tim24adm	Certificate Services Root CA - tim24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2028	✔
<input type="checkbox"/> Certificate Services OCSP Responder - tim24adm00004	Enabled	Infrastructure.Endpoints	74 C2 35 B8 32 6A 40 DF AC C8 D0 B9 51 DC 07 D	Certificate Services OCSP Responder - tim24adm	Certificate Services Node CA - tim24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2023	✔

FMC 구성

4단계. FMC에 새 영역 추가

1. FMC GUI에 액세스하여 **System > Integration > Realms**로 이동합니다.
2. 이미지에 표시된 대로 **New Realm(새 영역)**을 클릭합니다.



3. 양식을 작성하고 Test Active Directory (AD) Join 버튼을 클릭합니다.

참고: AD 조인 사용자 이름은 UPN(User Principal Name) 형식이어야 합니다. 그렇지 않으면 테스트가 실패합니다.

4. AD 조인 테스트가 성공하면 확인을 클릭합니다.

Add New Realm

Name * ISEpxGrid

Description Realm for use with pxGrid

Type * AD

AD Primary Domain * ex: domain.com

AD Join Username ex: user@domain

AD Join Password ***** Test AD Join

Directory Username * admin ex: user@domain

Directory Password * *****

Base DN * CN=Users, DN=rtpaaa, DN=net ex: ou=user, dc=cisco, dc=com

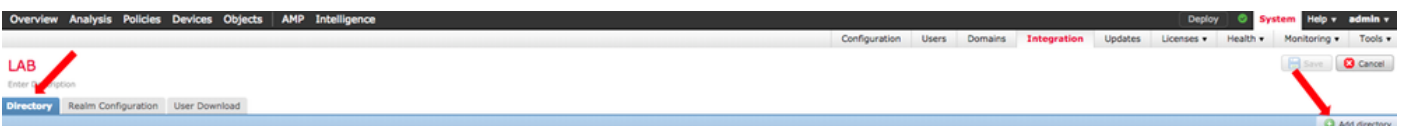
Group DN * DN=rtpaaa, DN=net ex: ou=group, dc=cisco, dc=com

Group Attribute Member

* Required Field

OK Cancel

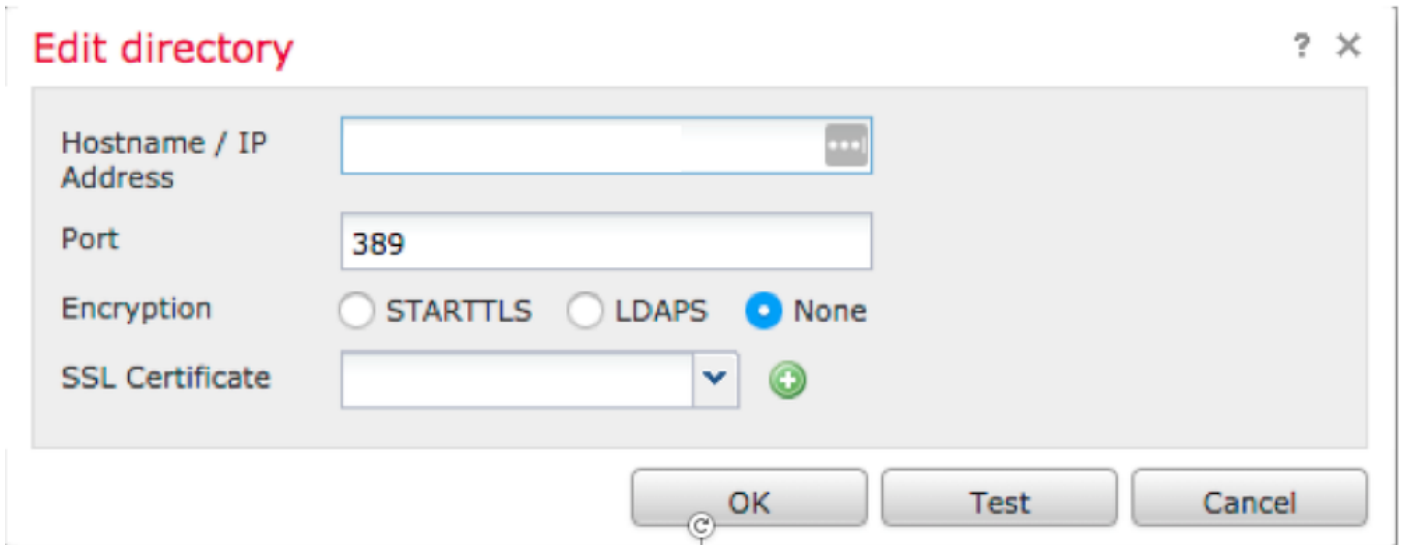
5. 디렉토리 탭을 클릭한 다음 이미지에 표시된 대로 디렉토리 추가를 클릭합니다.



6. IP/호스트 이름을 구성하고 연결을 테스트합니다.

참고: 테스트가 실패할 경우 Realm Configuration(영역 컨피그레이션) 탭에서 자격 증명을 확인합니다.

7. 확인을 클릭합니다.



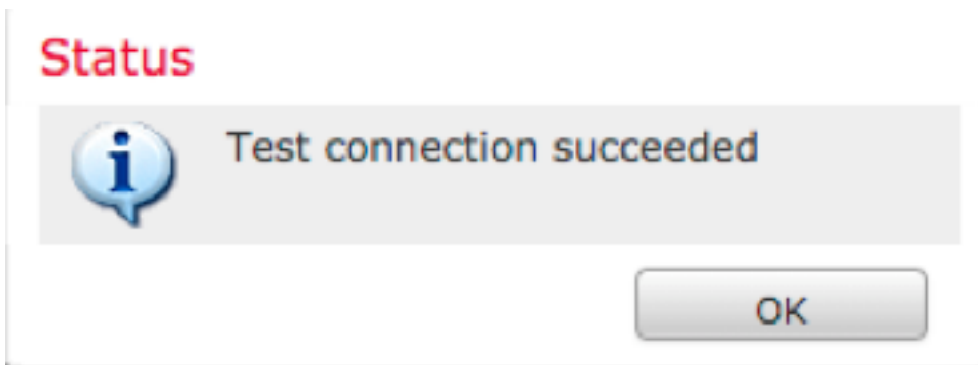
Edit directory ? X

Hostname / IP Address

Port

Encryption STARTTLS LDAPS None

SSL Certificate



Status

Test connection succeeded

8. 사용자 다운로드 탭을 클릭합니다.



9. 아직 선택하지 않은 경우 사용자 및 그룹 다운로드를 활성화합니다

10. 지금 다운로드를 클릭합니다

Enter Description

Directory Realm Configuration **User Download**

Download users and groups

Begin automatic download at America/New York Repeat Every Hours

11. 목록이 채워지면 원하는 그룹을 추가하고 포함에 추가를 선택합니다.

12. 영역 구성을 저장합니다.

Overview Analysis Policies Devices Objects AMP Intelligence

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

LAB

Enter Description

Directory Realm Configuration **User Download**

Download users and groups

Begin automatic download at America/New York Repeat Every Hours

Available Groups

Groups to Include (35)

Groups to Exclude (0)

13. 영역 상태를 사용으로 설정합니다.

Overview Analysis Policies Devices Objects AMP Intelligence

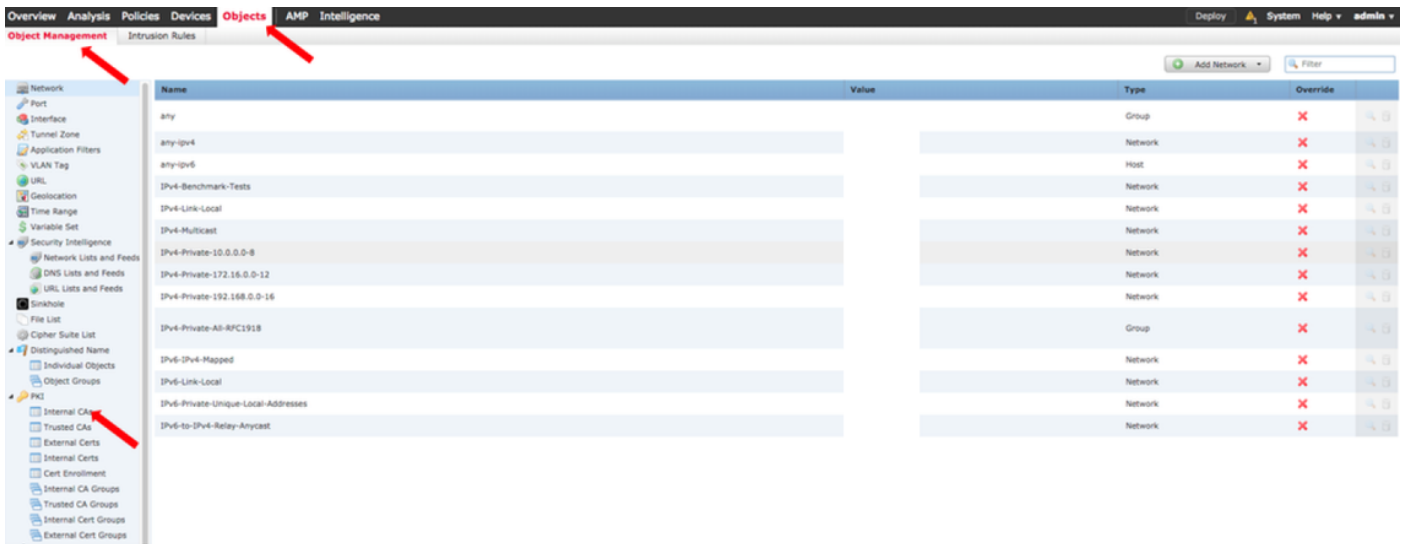
Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

Cisco CSI Realms Identity Sources eStreamer Host Input Client Smart Software Satellite

Name	Description	Domain	Type	Base DN	Group DN	Group Attribute	State
LAB		Global	AD	DC=rt2aaa,DC=net	CN=Users,DC=rt2aaa,DC=	member	<input checked="" type="checkbox"/>

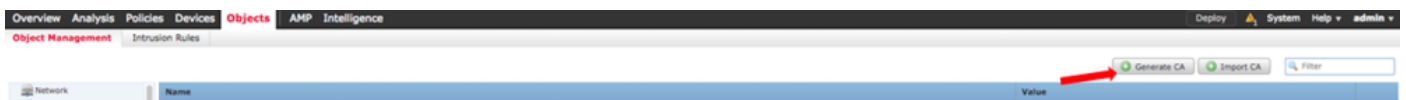
5단계. FMC CA 인증서 생성

1. 이미지에 표시된 대로 Objects(개체) > Object Management(개체 관리) > Internal CAs(내부 CA)로 이동합니다.



2. CA 생성을 클릭합니다.

3. 양식을 작성하고 Generate self-signed CA를 클릭합니다.



Generate Internal Certificate Authority ? X

Name:

Country Name (two-letter code):

State or Province:

Locality or City:

Organization:

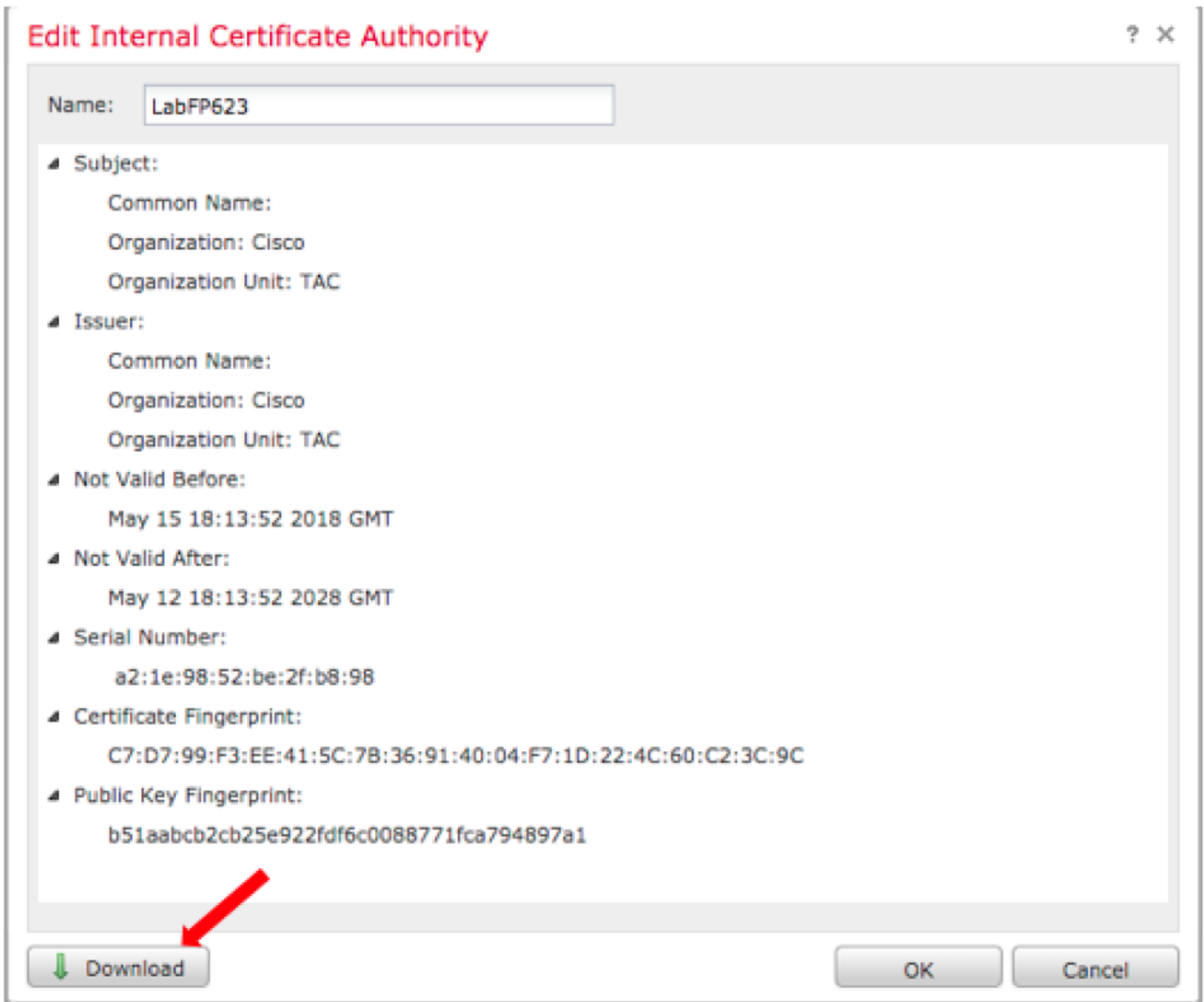
Organizational Unit (Department):

Common Name:

4. 생성이 완료되면 이미지에 표시된 대로 생성된 CA 인증서 오른쪽의 연필을 클릭합니다.



5. 다운로드를 클릭합니다.



6. 암호화 비밀번호를 구성하고 확인한 후 확인을 클릭합니다.

7. PKCS(Public-Key Cryptography Standards) p12 파일을 로컬 파일 시스템에 저장합니다.

6단계. OpenSSL을 사용하여 생성된 인증서에서 인증서 및 개인 키 추출

이는 FMC의 루트 또는 OpenSSL 명령을 사용할 수 있는 모든 클라이언트에서 수행됩니다. 이 예에서는 표준 Linux 셸을 사용합니다.

1. **openssl**을 사용하여 p12 파일에서 인증서(CER) 및 개인 키(PVK)를 추출합니다.
2. CER 파일을 추출한 다음 FMC의 인증서 생성에서 인증서 내보내기 키를 구성합니다.

```
~$ openssl pkcs12 -nokeys -clcerts -in <filename.p12> -out <filename.cer>  
Password:  
Last login: Tue May 15 18:46:41 UTC 2018  
Enter Import Password:  
MAC verified OK
```

3. PVK 파일을 추출하고 인증서 내보내기 키를 구성한 다음 새 PEM 암호를 설정하고 확인합니다.

```
~$ openssl pkcs12 -nocerts -in <filename.pl2> -out <filename.pvk>
```

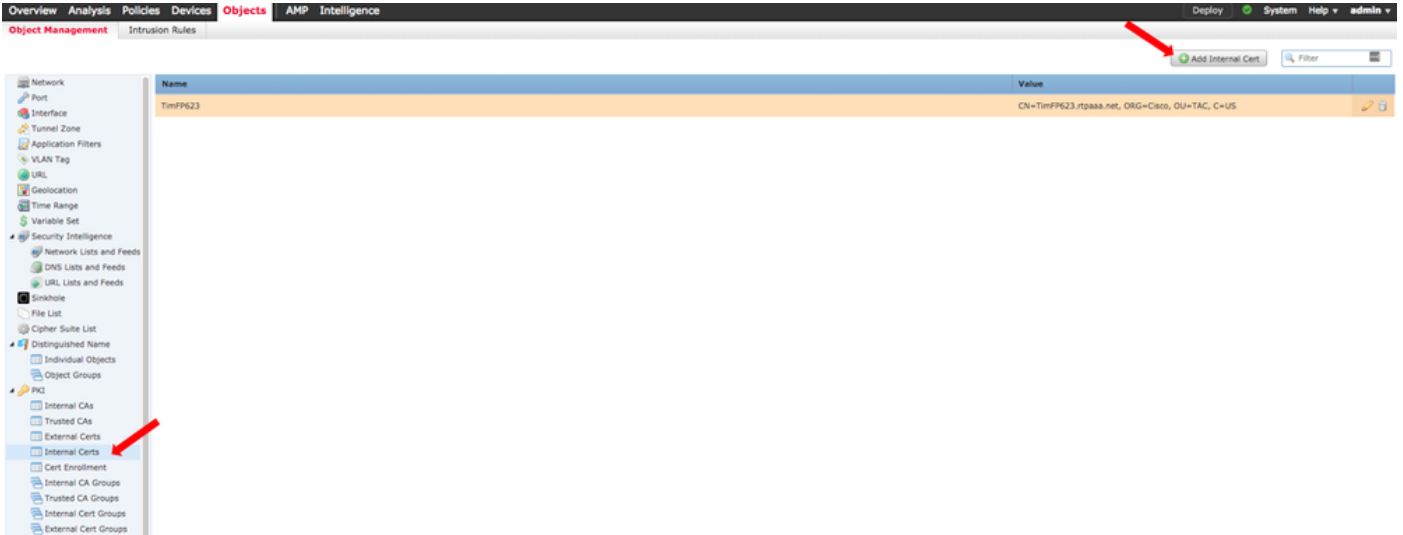
Password: Last login: Tue May 15 18:46:41 UTC 2018 Enter Import Password: MAC verified OK

4. 이 PEM 구문은 다음 단계에서 필요합니다.

7단계. FMC에 인증서 설치

1. 객체 > 객체 관리 > PKI > 내부 인증서로 이동합니다.

2. 이미지에 표시된 대로 Add Internal Cert(내부 인증서 추가)를 클릭합니다.



3. 내부 인증서의 이름을 구성합니다.

4. CER 파일의 위치로 이동하여 선택합니다. Certificate Data(인증서 데이터)가 채워지면 두 번째 항목을 선택합니다.

5. 옵션을 찾아보고 PVK 파일을 선택합니다.

6. PVK 섹션에서 임의의 선행 "백 속성" 및 임의의 후행 값을 삭제합니다. PVK는 -----BEGIN ENCRYPTED PRIVATE KEY-----로 시작하고 -----END ENCRYPTED PRIVATE KEY-----로 끝납니다

참고: PVK 텍스트에 선행 및 후행 하이픈을 제외한 문자가 있으면 확인을 클릭할 수 없습니다

7. Encrypted(암호화된) 상자를 선택하고 6단계에서 PVK를 내보낼 때 생성된 비밀번호를 구성합니다.

8. 확인을 클릭합니다.

Add Known Internal Certificate

? X

Name:

Certificate Data or, choose a file:

```
-----BEGIN CERTIFICATE-----
MIIDFTCCAmWgAwIBAgIJAKIemFK+L7iYMA0GCSqGSIb3DQEBCwUAMGQxCzAJBgNV
BAYTAIVTMQswCQYDVQQIDAJOQzEMMAoGA1UEBwwDUIRQM4wDAYDVQQKDAVDAxNj
bzEMMAoGA1UECwwDVEFDMRwwGgYDVQQDDDBNMYWJGUDYyMy5ydHBhYWEubmV0MB4X
DTE4MDUxNTE4MTM1MlloXDTI4MDUxMjE4MTM1MlowZDELMAkGA1UEBhMCVVMxZzAJ
BgNVBAGMAK5DMQwwCgYDVQQHDANSVFAXDjAMBgNVBAoMBUNpc2NmMQwwCgYDVQQQL
DANUQUxHDAaBgNVBAMME0xhYkZQNjIzLnJ0cGFhYS5uZXQwggeEIMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQMjt5S5UIFIZkZK/TSGtkOCmuivTK5kk1WzAy6
D7Gm/c69cXw/VfIPWnSBzhEkiRTyspmTMdyf/4TJvUmUH60h1O8/8dZeqJOzbjon
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABGkqhkiG9w0BBQwwMzAbBgkqhkiG9w0BBQwwDgQI5uV3MsiHZsICAggA
MBQGCCqGSIb3DQMHBABGvm1+xHLIASCBMjjJxkffXUNUcdB22smybvWotwbcRrt
xL0qjEStmwuyExVp+TWC3AyIJN1DE7/rRssjRAqsnSOxIvDGmg0dVsvnbqZwjFP
74POu/O2Vy99iFoVgW2q9DyXyL/h64TH9CZtwLKIOGOeEunNKpamDnpfyN8QC4DC
fXvNZ8jNG4HrEcFmnnij0EwJ0QT8Jn5gAUj+AIPMe32zPqwocCRNYrRXMVM9+Jwp
-----END ENCRYPTED PRIVATE KEY-----
</no>
```

Key or, choose a file:

Bag Attributes
localKeyID: C7 D7 99 F3 EE 41 5C 7B 36 91 40 04 F7 1D 22 4C 60 C2 3C 9C ← DELETE
Key Attributes: <no attributes="">

Encrypted, and the password is:

Encrypted, and the password is:

8단계. ISE로 FMC 인증서 가져오기

1. ISE GUI에 액세스하여 Administration(관리) > System(시스템) > Certificates(인증서) > Trusted Certificates(신뢰할 수 있는 인증서)로 이동합니다.

2. 임포트를 클릭합니다.

Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiration Status
Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 89	Baltimore CyberTrust Ro...	Baltimore CyberTrust Ro...	Fri, 12 May 2000	Mon, 12 May 2025	✓
Cisco CA Manufacturing	Disabled	Endpoints Infrastructure	6A 69 67 83 00 00	Cisco Manufacturing CA	Cisco Root CA 2048	Fri, 10 Jun 2005	Mon, 14 May 2029	✓
Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure	02	Cisco Manufacturing CA...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037	✓
Cisco Root CA 2048	Disabled	Endpoints Infrastructure	5F FB 78 28 28 54	Cisco Root CA 2048	Cisco Root CA 2048	Fri, 14 May 2004	Mon, 14 May 2029	✓
Cisco Root CA M2	Enabled	Endpoints Infrastructure	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037	✓
Default self-signed server certificate	Enabled	Endpoints Infrastructure	5A BE 7E D8 00 00...	tm24adm.rtpaaa.net	tm24adm.rtpaaa.net	Fri, 30 Mar 2018	Sat, 30 Mar 2019	✓
DigICert root CA	Enabled	Endpoints Infrastructure	02 AC 5C 26 6A 08	DigICert High Assurance...	DigICert High Assurance...	Thu, 9 Nov 2006	Sun, 9 Nov 2031	✓
DigICert SHA2 High Assurance Server CA	Enabled	Endpoints Infrastructure	04 E1 E7 A4 DC 5C...	DigICert SHA2 High Ass...	DigICert High Assurance...	Tue, 22 Oct 2013	Sun, 22 Oct 2028	✓
DST Root CA X3 Certificate Authority	Enabled	Cisco Services	44 AF B0 80 D6 A3...	DST Root CA X3	DST Root CA X3	Sat, 30 Sep 2000	Thu, 30 Sep 2021	✓
HydrantID SSL ICA G2	Enabled	Cisco Services	75 17 16 77 83 00...	HydrantID SSL ICA G2	QuoVadis Root CA 2	Tue, 17 Dec 2013	Sun, 17 Dec 2023	✓
QuoVadis Root CA 2	Enabled	Cisco Services	05 09	QuoVadis Root CA 2	QuoVadis Root CA 2	Fri, 24 Nov 2006	Mon, 24 Nov 2031	✓
Thawte Primary Root CA	Enabled	Cisco Services	34 4E D5 57 20 D5...	thawte Primary Root CA	thawte Primary Root CA	Thu, 16 Nov 2006	Wed, 16 Jul 2036	✓
TimFP623	Enabled	Endpoints Infrastructure	8E F9 42 3D 25 A5...	TimFP623.rtpaaa.net	TimFP623.rtpaaa.net	Tue, 15 May 2018	Fri, 12 May 2028	✓
VeriSign Class 3 Public Primary Certification Authority	Enabled	Cisco Services	18 DA D1 9E 26 7D...	VeriSign Class 3 Public ...	VeriSign Class 3 Public ...	Tue, 7 Nov 2006	Wed, 16 Jul 2036	✓
VeriSign Class 3 Secure Server CA - G3	Enabled	Cisco Services	6E CC 7A A5 47 03...	VeriSign Class 3 Secure ...	VeriSign Class 3 Public ...	Sun, 7 Feb 2010	Fri, 7 Feb 2020	✓

3. 파일 선택을 클릭하고 로컬 시스템에서 FMC CER 파일을 선택합니다.

선택 사항: 식별 이름을 구성합니다.

4. ISE 내에서 Trust(신뢰)를 선택합니다.

선택 사항: 설명을 구성합니다.

5. 이미지에 표시된 대로 제출을 클릭합니다.

Import a new Certificate into the Certificate Store

* Certificate File TZfpcert.cer

Friendly Name

Trusted For: Trust for authentication within ISE

Trust for client authentication and Syslog

Trust for authentication of Cisco Services

Validate Certificate Extensions

Description

9단계. FMC에서 pxGrid 연결 구성

1. 이미지에 표시된 대로 System > Integration > Identity Sources로 이동합니다.



2. ISE를 클릭합니다.

3. ISE pxGrid 노드의 IP 주소 또는 호스트 이름을 구성합니다.

4. pxGrid Server CA 오른쪽의 +를 선택합니다.

5. 서버 CA 파일의 이름을 지정한 다음 3단계에서 수집된 pxGrid 루트 서명 CA를 찾은 다음 저장을 클릭합니다.

6. MNT 서버 CA 오른쪽의 +를 선택합니다.

7. 서버 CA 파일의 이름을 지정한 다음 3단계에서 수집한 관리자 인증서를 찾은 다음 저장을 클릭합니다.

8. 드롭다운 목록에서 FMC CER 파일을 선택합니다.

Identity Sources

Service Type: None Identity Services Engine User Agent

Primary Host Name/IP Address * <ISE pxGRID Node IP ADDRESS>

Secondary Host Name/IP Address

pxGrid Server CA * ISE24InternalRoot +

MNT Server CA * ISE24SelfSigned +

FMC Server Certificate * TimFP623 +

ISE Network Filter ex. 10.89.31.0/24, 192.168.8.0/24, ...

* Required Field Test

9. 테스트를 클릭합니다.

10. 테스트가 성공하면 화면 오른쪽 상단에서 확인, 저장을 차례로 클릭합니다.

Status

ISE connection status:
Primary host: Success

Additional Logs

OK

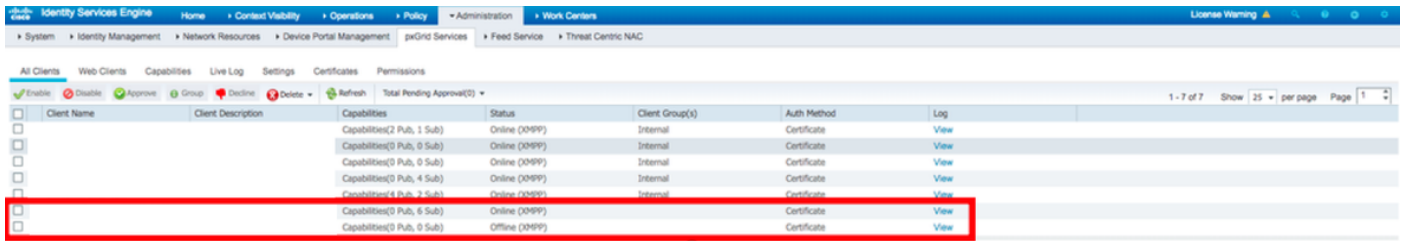
참고: 두 개의 ISE pxGrid 노드를 실행하는 경우, pxGrid가 한 번에 하나의 ISE 노드에서만 활발하게 실행되므로 하나의 호스트가 Success(성공)를 표시하고 하나는 Failure(실패)를 표시하는 것이 일반적입니다. 어떤 기본 호스트가 Failure(실패)를 표시하고 보조 호스트가 Success(성공)를 표시할지 여부에 따라 달라집니다. 이는 모두 ISE의 어떤 노드가 액티브 pxGrid 노드인지에 따라 달라집니다.

다음을 확인합니다.

ISE에서 확인

1. ISE GUI를 열고 Administration(관리) > pxGrid Services(pxGrid 서비스)로 이동합니다.

성공하면 클라이언트 목록에 두 개의 Firepower 연결이 나열됩니다. 하나는 실제 FMC(iseagent-hostname-33bytes)용, 다른 하나는 테스트 디바이스(firesightisetest-hostname-33bytes)용.



iseagent-firepower 연결에는 6개의 하위 탭이 표시되고 온라인으로 나타납니다.

firesightisetest-firepower 연결은 0개의 서브셋을 표시하고 오프라인으로 나타납니다.

iseagent-firepower 클라이언트의 확장된 보기에는 6개의 서브스크립션이 표시됩니다.

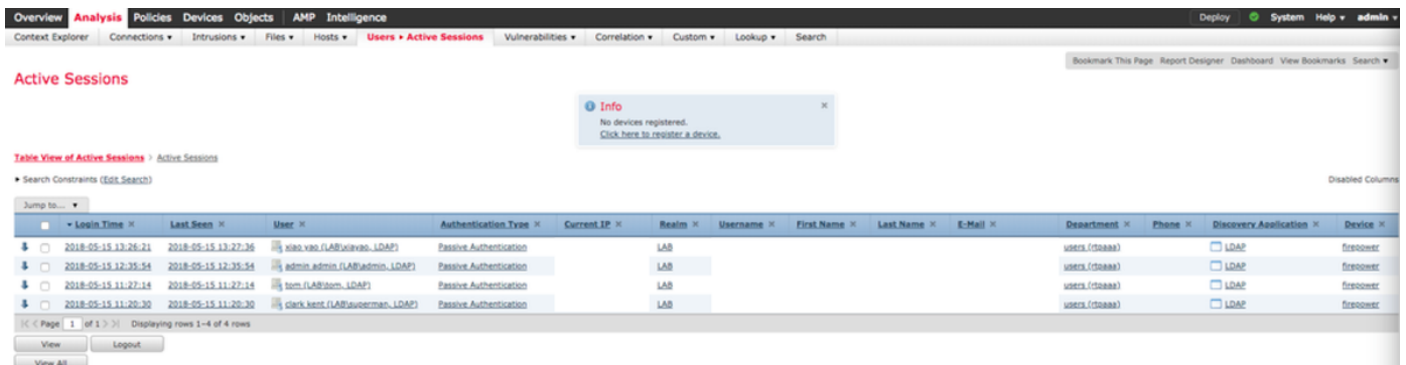


참고: Cisco 버그 ID CSCvo75376으로 인해 호스트 이름 제한이 있으며 대량 다운로드가 실패합니다. FMC의 테스트 단추에 연결 오류가 표시됩니다. 이는 2.3p6, 2.4p6 및 2.6에 영향을 줍니다. 현재 권고하는 내용은 정식 패치가 나올 때까지 2.3 패치 5나 2.4 패치 5를 실행하는 것입니다.

FMC에서 확인

1. FMC GUI를 열고 Analysis(분석) > Users(사용자) > Active Sessions(활성 세션)로 이동합니다.

ISE의 세션 디렉토리 기능을 통해 게시된 모든 활성 세션은 FMC의 활성 세션 테이블에 표시됩니다.



FMC CLI 하위 모드에서 'adi_cli session'은 ISE에서 FMC로 전송된 사용자 세션 정보를 표시합니다.


```
ssh admin@<FMC IP ADDRESS>
Password:
Last login: Tue May 15 19:03:01 UTC 2018 from dhcp-172-18-250-115.cisco.com on ssh
Last login: Wed May 16 16:28:50 2018 from dhcp-172-18-250-115.cisco.com
```

Copyright 2004-2018, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

```
Cisco Fire Linux OS v6.2.3 (build 13)
Cisco Firepower Management Center for VMWare v6.2.3 (build 83)
```

```
admin@firepower:~$ sudo -i
Password:
Last login: Wed May 16 16:01:01 UTC 2018 on cron
root@firepower:~# adi_cli session
```

```
received user session: username tom, ip ::ffff:172.18.250.148, location_ip ::ffff:10.36.150.11,
realm_id 2, domain rtpaaa.net, type Add, identity Passive.
received user session: username xiayao, ip ::ffff:10.36.148.98, location_ip ::, realm_id 2,
domain rtpaaa.net, type Add, identity Passive.
received user session: username admin, ip ::ffff:10.36.150.24, location_ip ::, realm_id 2,
domain rtpaaa.net, type Add, identity Passive.
received user session: username administrator, ip ::ffff:172.18.124.200, location_ip ::,
realm_id 2, domain rtpaaa.net, type Add, identity Passive.
```

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

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.