# 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 <u>9단계. FMC에서 pxGrid 연</u>결 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 대 해 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 디바 이스는 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.

Deployment		Deployment Nodes List > tim24adm									
(= • E •	- <u>Si</u>	Edit Node									
Opployment     PAN Failover		General Settings Profiling Configuration Hostname FQDN									
		IP Address									
		Node Type Identity Services Engine (ISE)									
		Role       STANDALONE       Make Primary         Image: Administration       Image: Administration         Image: Administration       Image: Administration									
		pxond ()									
		Save Reset									

4. pxGrid 서비스가 CLI에서 실행되는지 확인합니다.

**참고**: 둘 이상의 pxGrid 노드가 사용 중인 경우, pxGrid 서비스가 완전히 시작되고 HA(고가용 성) 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 과리 CLUICH ON HILA THE STORE
```

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**.

-dusts Identity Services Engine Home + Co	ntext Visibility + Operations + Policy • Adm	nistration + Work Centers				License Warning 🔺 🔍 😑 🔿 🔿
System      Identity Management      Network Resource	roes	Feed Service     Threat Centric N	AC			Click here to do wireless setup and visibility setup Do not show this again. $ imes$
All Clients Web Clients Capabilities Live Log	Settings Certificates Permissions					
🖋 Enable 🖉 Disable 🙄 Approve 😝 Group 🌻 Decl	int 🔞 Delete 👻 🎨 Refresh 🛛 Total Pending Approval(0)	•				1-7 of 7 Show 25 v per page Page 1 🗘
Client Name Client Descrip	ption Capabilities	Status	Client Group(s)	Auth Method	Log	
ise-mnt-tim24adm	Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate	View	
Ise-fanout-tim24adm	Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View	
ise-pubsub-tim24adm	Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View	
Ise-bridge-tim24adm	Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate	View	
Ise-admin-tim24adm	Capabilities(4 Pub, 2 Sub)	Online (XMPP)	Internal	Certificate	View	
iseagent-firepower-20762a2982d	Capabilities(0 Pub, 6 Sub)	Online (XMPP)		Certificate	View	
Firesightisetest-firepower-20762a	Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		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.

cisco Iden	tity Services Engine	Home → Co	ntext Visibility	<ul> <li>Operations</li> </ul>	▶ Policy	→ Adminis	stration V	Vork Centers
System	Identity Management	Network Resource	ces Device	e Portal Management	pxGrid S	ervices	Feed Service	Threat Centric NAC
All Clients	Web Clients Cap	abilities Live Log	Settings	Certificates Per	missions			
PxGri	d Settings							
Auto	matically approve new ce v password based accour	rtificate-based account creation	nts					
Use D	efault 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 인증서 에 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.

dentity Services Engine	Home + Context Visibility + Operations +	Policy   Administration	Work Centers				License Warning 📥 🔍 😣 😋 🗢			
System      Identity Management	Network Resources	pxGrid Services + Feed Service	ce							
Deployment Licensing Certificate	s + Logging + Maintenance Upgrade + Baci	up & Restore + Admin Access	Settings							
0	_	/								
* Certificate Management	System Certificates 🛕 For disaster recovery i	is recommended to explicit certification	ate and private key pairs of all syste	m certificates.						
System Certificates	📝 Edit 🕂 Generate Self Signed Certificate	- Import 🚱 Export 🗶 De	iete 🔎 View							
Trusted Certificates	Friendly Name	Used By Pr	ortal group tag	Issued To	Issued By	Valid From	Expiration Date			
OCSP Client Profile	▼ tim24adm									
Certificate Signing Requests Certificate Periodic Check Setti	e.CN+tim24adm.rtpaaa.net#Certificate Se vices Endpoint Sub CA - tim24adm#0000	pxGrid				Thu, 29 Mar 2018	Thu, 30 Mar 2028 🛃			
Certificate Authority	<ul> <li>Mault self-signed sami server certificate</li> <li>Chr/SAML tim24artm rbass net</li> </ul>	SAML				Fri, 30 Mar 2018	Sat, 30 Mar 2019 2			
	Default self-signed server certificate	EAP Authentication, Admin, De	fault Portal Certificate Group 👔			Fri, 30 Mar 2018	Sat, 30 Mar 2019 🛃			
		Forae, POUNUS UTLS								
	Export Certificate Only     Export Certificate and Private Key									
	*Private Ke	y Password								
	*Confir	n Paceword								
	Comm	II Fassword								
Warning	Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private key.									
						E	cport Cancel			

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 **보기**를 클릭합니다.

Hude Identity Services Engine	Home + Context Visibility + Operations	Policy      Administration      Work Cer	ten			License Warning 🔺 🤍 😐 🔿 🔿
* System + Identity Management	Network Resources	pxGrid Services + Feed Service + Thr	at Centric NAC			
Deployment Licensing Certificate	s + Logging + Maintenance Upgrade + Ba	ckup & Restore + Admin Access + Setting	5			
0						
Certificate Management	System Certificates 🛕 For disaster recovery	it is recommended to export certificate and privi	te is pairs of all system certificates.			
System Certificates	🖊 Edit 🛛 🕂 Generate Self Signed Certificate	🕂 Import. 🕃 Export. 🗙 Delete 🔎	len -			
Trusted Certificates	Friendly Name	Used By Portal group t	ag Issued To	Issued By	Valid From	Expiration Date
OCSP Client Profile	▼ tim24adm					
Certificate Signing Requests	OU=Certificate Services System Certific e,CN=tim24adm.rtpaaa.net#Certificate 5	et Se pxGrid			Tru, 29 Mar 2018	Thu, 30 Mar 2028 🛃
Certificate Periodic Check Set5	1					
Certificate Authority	<ul> <li>Default self-signed sami server certification</li> <li>CN=SAML_tim24adm.rtpaaa.net</li> </ul>	• SAML			Fri, 30 Mar 2018	Sat, 30 Mar 2019 🗾
	<ul> <li>Default self-signed server certificate</li> </ul>	EAP Authentication, Admin, Portal, RADIUS DTLS Default Portal	Certificate Group (g)		Fri, 30 Mar 2018	Sat, 30 Mar 2019 🛃

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

13. 이미지에 표시된 대로 인증서 보기 창을 닫습니다.

Certificate Services Root CA Certificate Services Not	A - tim24adm de CA - tim24adm	
Certificate Services	Endpoint Sub CA - tim24adm	
tim24adm.rtpa	aa.net	
tim24adm.rtpaaa Issued By : Certif Expires : Thu, 30	net icate Services Endpoint Sub CA - tim24adm 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.

dentity Services Engine	Home	+ Context Visibility + Operatio	ns + Policy - A	dministration + Work Centers					License Warning 🔺 👘	
System       Identity Management	Network	Resources + Device Portal Manag	ement pxGrid Service	s + Feed Service + Threat Cent	ric NAC					
Deployment Licensing - Certificate	es + Lo	ogging + Maintenance Upgrade	Backup & Restore	Admin Access Settings						
0										
Certifiete Management	CAC	ertificates								
- Certificate Authority		Edit 🕂 Import 🕃 Export 🗙	Delete 🔎 View 🔮	Refresh						
Outries		Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiration Status
Charlien	V Sr	m24adm								
Issued Certificates	0	Certificate Services Endpoint Sub C& . tim24artm#000003	Enabled	Infrastructure,Endpoints	32 D2 72 55 A9 7D 40 13 8F 2A EF	Certificate Services Endpoint Sub	Certificate Services Node CA -	Thu, 29 Mar 2018	Thu, 30 Mar 2028	
Certificate Authority Certificates	-	Certificate Services Root CA -	Ecobled	Infeasts where Endoniets	36 67 74 15 A6 A8 4F EB B7 46 1	Certificate Services Root CA -	Certificate Services Root CA -	Thu: 20 Mar 2018	Thu: 20 Mar 2028	
Internal CA Settings	•	tim24adm#00001	Enabled	intrastructure, Enopoints	E7 37 1A AB 88	tim24adm	tim24adm	Thu, 29 Mar 2016	Thu, 30 Mar 2028	
Certificate Templates		Certificate Services Node CA - tim24adm#00002	Enabled	Infrastructure,Endpoints	30 1A 22 E7 AA E5 45 35 8C 65 78 EE 53 09 34 3E	tim24adm	tim24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2028	<b>9</b>
External CA Settings		Certificate Services OCSP Responder - tim24adm#00004	Enabled	Infrastructure,Endpoints	74 C2 35 BB 32 6A 40 0F AC C8 D0 B9 51 DC 07 7D	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 > Realms로 이동합니다.
- 2. 이미지에 표시된 대로 New Realm(새 영역)을 클릭합니다.

Overview	Analysis	Policies	Devices	Objects	AMP 1	Intelligence		•	í							Deploy	🛛 🔍 Sy	stem Help v	admin v
											Configuration	Users	Domains	Integration	Updates	Licenses v	ii aith 🔻	Monitoring	Tools •
	_															1			
Cisco CSI	Realms	Identit	y Sources	eStream	er Hos	st Input Client	Smart Software Satellite												
																	Comp	pare realms	New realm

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		
Туре *	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 확 인합니다.

1

## 7. 확인을 **클릭합니다**.

Edit directory		? ×
Hostname / IP Address	••••	
Port	389	
Encryption	◯ STARTTLS ◯ LDAPS 💿 None	
SSL Certificate	<ul> <li>✓ ②</li> </ul>	
	ОК Test Ca	incel
Status		
Test	connection succeeded	

8. **사용자 다운로드 탭**을 클릭합니다.

Overview Analysis Policies Devices Objects AMP Intelligence						Deploy	🕘 🔍 Sys	tem Help v	admin +
	Configuration	Users	Domains	Integration	Updates	Licenses •	Health +	Monitoring •	Tools •
LAB								Save (	Cancel
Directory Realm Configuration User Download									

OK

9. 아직 선택하지 않은 경우 사용자 및 그룹 다운로드를 활성화합니다

10. 지금 다운로드를 클릭합니다

Enter Description

Directory	Realm Configuration	User Download
Downloa	ad users and groups	America/New York Repeat Event DA Y Hours
Down	load Now	

••••|

11. 목록이 채워지면 원하는 그룹을 추가하고 포함에 **추가를 선택합니다**.

#### 12. 영역 구성을 **저장합니다**.

Overview Analysis Policies Devices Objects AMP Intelligence								Deploy O System Help v admir
			Configuration	Users	Domains	Integration	Updates	Licenses • Health • Monitoring • Tool
LAB E								You have unsaved changes_ 🔚 Save 🛛 😫 Cano
Enter Description								
Directory Realm Configuration User Download								•
Obwinload users and groups								
Begin automatic download at R Y PM Y America/New York Repeat Every 24 Y Hours								
s <sup>4</sup> s Download Now								
Available Groups C		Groups to Include (35)			Groups to Ex	clude (0)		
Search by name		A NetOps		8	None			
A NetOps	1	SQLServer2005SQLBrowserUsersRTPAAA-DC2		8				
SQLServer2005SQLBrowserUserSRTPAAA-DC2		A WSUS Administrators		8				
A WSUS Administrators		A Enterprise Read-only Domain Controllers		8				
A Enterprise Read-only Domain Controllers		A DnsUpdateProxy		8				
A DnsUpdateProxy		af jhoehn-group		8				
A jhoehis-group		A Denied RODC Password Replication Group		8				
A Denied RODC Password Replication Group		af Domain Admins		8				
A Domain Admins		af Child		8				
A Child		a DnsAdmins		8				
A DasAdmins		a Lester\Made\Me\Do\It		8				
A Lester/Made/Me/DoUt		af Group Policy Creator Owners		8				
A Group Policy Creator Owners		af INE		8				
A INE		🖌 🍰 Domain Users		8				
🔗 Domain Users		de ChadTest		8				
A ChadTest		Acad-only Domain Controllers		8				
A Read-only Domain Controllers	Include	a RAS and IAS Servers		8				
As and LAS Servers	Add to	der Cert Publishers		8				
🔗 Cert Publishers	Exclude	🝰 Schema Admins		8				
🝰 Schema Admins		A WSUS Reporters		8				
🝰 WSUS Reporters		af Parent		8				
🔗 Parent		a 15E Admins		8				
🔗 ISE Admins		WinRMRemoteWMIUsers		8				
A WinRMRemoteWMIUsers		Allowed RODC Password Replication Group		8				
Allowed RODC Password Replication Group		2 TimSponsors		8				
A TimSponsors		AllowedVPN		8				
Allowed/PN		Enterprise Admins		8				
🔗 Enterprise Admins		🛃 test-users		8				
🝰 test-users		a sponsors		8				
🝰 sponsors		A HelpLibraryUpdaters		8				
A HelpLibraryUpdaters		Protected Users		8				
AP Protected Users		2 Domain Guests		8				
🔗 Domain Guests		Domain Computers		8				
A Domain Computers		Domain Controllers		8.0				
A Domain Controllers		Enter Dart stan		-	Enter Herr De	and		
A Channella Deservic Controllers		Einer Aber Hinngebu		ADD	Lenter user Ex	Crossed11		Add

13. 영역 상태를 사용으로 설정합니다.

Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence									Deploy	🕘 🗢 Sy	stem Help	• admin •
										Configuration	Users	Domains 1	Integration	Updates	Licenses +	Health +	Monitoring	• Tools •
Cisco CSI	Realms	Identit	y Sources	eStreame	r H	lost Input Client	Smart Software Satellite											
																Comp	pare realms	O New realm
Name								Description	Domain	Туре		Base DN	Group	DN	Group Atte	ibute	State	
LAB									Global	AD		DC=rtpaaa,DC=ne	t CN+U	sers,DC=rtpaaa,	.DC+ member			± 🥒 🐚 🕄

## 5단계. FMC CA 인증서 생성

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

Overview Analysis Polici	es Devices Objects AMP Intelligence		Deploy 🔺 Syst	tem Help v I	edmin v
Object Management Intru	sion Rules				
			Add Network •	G Filter	
2 Network	Name	Value	Туре	Override	
Port G Interface	any		Group	×	۹.8
Application Filters	any-ipv4		Network	×	
🛞 VLAN Tag	any-ipv6		Host	×	
Geolocation	IPv4-Benchmark-Tests		Network	×	
Time Range	1Pv4-Unix-Local		Network	×	
\$ Variable Set	1Pv4-Multicast		Network	×	
<ul> <li>Security Intelligence</li> <li>Network Lists and Feeds</li> </ul>	1Pv4-Private-10.0.0.0-8		Network	×	
DNS Lists and Feeds	IPv4-Private-172.16.0.0-12		Network	×	
URL Lists and Feeds	IPv4-Private-192.168.0.0-16		Network	×	
File List	1Pv4-Private-Al-RPC1918		Group	×	
Distinguished Name     Individual Objects	1Pu6-IPu6-Mapped		Network	×	
Cobject Groups	1Pv6-Link-Local		Network	×	
PKI Internal Chart	1Pv6-Private-Unique-Local-Addresses		Network	×	
Trusted CAs	1Pv6-to-1Pv4-Relay-Anycast		Network	×	
External Certs     Internal Certs     Cert Enroliment     Internal CA Groups     Internal CA Groups     Internal Cert Groups     External Cert Groups					

#### 2. **CA** 생성**을 클릭합니다**.

3. 양식을 작성하고 Generate **self-signed CA를 클릭합니다**.

Overview Analysis	Policies Devices	Objects AMP Intelligence				Deploy 🗛 System Help + admin +
<b>Object Management</b>	Intrusion Rules					
					Generate CA	O Import CA
Retwork	Name				Value	
			•		1	
		Generate Internal Certificate	Authority	? X		
		Name:	LabFP623	3		
		Country Name (two-letter code):	US			
		State or Province:	NC			
		Locality or City:	RTP			
		Organization:	Cisco			
		Organizational Unit (Department):	TAC			
		Common Name:				
			•			
		Generate CSR	Generate self-signed CA	Cancel		

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



5. 다운로드를 **클릭합니다**.

lame:	LabFP623		
Subje	ct:		
Co	mmon Name:		
Or	ganization: Cisco		
Or	ganization Unit: TAC		
Issue	r:		
Co	mmon Name:		
Or	ganization: Cisco		
Or	ganization Unit: TAC		
Not V	alid Before:		
Ma	by 15 18:13:52 2018 GMT		
Not V	alid After:		
Ma	ay 12 18:13:52 2028 GMT		
Serial	Number:		
a	2:1e:98:52:be:2f:b8:98		
Certif	icate Fingerprint:		
C7	D7:99:F3:EE:41:5C:7B:36:91:40:04:F7:1D:22:4C:60:C2:3C:9C		
Public	: Key Fingerprint:		
b5	1aabcb2cb25e922fdf6c0088771fca794897a1		
Dow	nload	OK	Cancel

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 예에 서는 표준 Linux 셸을 사용합니다.

1. openssl을 사용하여 p12 파일에서 인증서(CER) 및 개인 키(PVK)를 추출합니다.

2. CER 파일을 추출한 다음 FMC의 인증서 생성에서 인증서 내보내기 키를 구성합니다.

~\$ openssl pkcsl2 -nokeys -clcerts -in <filename.pl2> -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 pkcsl2 -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.

Overview Analysis	Policies Device	S Objects AMP I	ntelligence					Deploy	System Hel	p v admin v
<b>Object Management</b>	Intrusion Rules			 	 					
										-
								Add Internal 0	ert Filter	-
Retwork	Name					Value				
J <sup>ar</sup> Port	TimFP623					CN+TimEP623.r	toaaa.net. ORG+Cir	co. OU+TAC. C+US		2 =
😋 Interface										
Tunnel Zone										
Application Filters										
S VLAN Tag										
UKL Contraction										
Ceolocation										
C Variable Est										
A Security Intelligence										
Network Lists and	Feeds									
ONS Lists and Fee	nds									
URL Lists and Feed	ds									
Sinkhole										
Tile List										
Opher Suite List										
a 📢 Distinguished Name										
Individual Objects	5									
Cobject Groups										
a 🔑 PKI										
Internal CAs										
Trusted CAs										
External Certs										
Internal Certs										
Cert Enrollment										
Internal CA Groups	96									
Trusted CA Groups	15									
E Internal Cert Grou	ups									

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(암호화됨) 상자를 선택하고 6단계에서 PVK를 내보낼 때 생성된 비밀번호를 구성합니다.

8. 확인을 **클릭합니다**.

#### Add Known Internal Certificate

Name: TZfpcert									
Certificate Data or, choose a file: Browse									
BEGIN CERTIFICATE MIIDfTCCAmWgAwIBAgIJAKIemFK+L7iYMA0GCSqGSIb3DQEBCwUAMGQxCzAJBgNV BAYTAIVTMQswCQYDVQQIDAJOQzEMMAoGA1UEBwwDUIRQMQ4wDAYDVQQKDAVDaXNj bzEMMAoGA1UECwwDVEFDMRwwGgYDVQQDDBNMYWJGUDYyMy5ydHBhYWEubmV0MB4X DTE4MDUxNTE4MTM1MloXDTI4MDUxMjE4MTM1MlowZDELMAkGA1UEBhMCVVMxCzAJ BgNVBAgMAk5DMQwwCgYDVQQHDANSVFAxDjAMBgNVBAoMBUNpc2NvMQwwCgYDVQQL DANUQUMxHDAaBgNVBAMME0xhYkZQNjIzLnJ0cGFhYS5uZXQwggEiMA0GCSqGSIb3 DQEBAQUAA4IBDwAwggEKAoIBAQDMjtS5lUIFiZkZK/TSGtkOCmuivTK5kk1WzAy6 D7Gm/c69cXw/VfIPWnSBzhEkiRTyspmTMdyf/4TJvUmUH60h108/8dZeqJOzbjon									
Bag Attributes localKeyID: C7 D7 99 F3 EE 41 5C 7B 36 91 40 04 F7 1D 22 4C 60 C2 3C Key Attributes: <no attributes=""> MIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQI5uV3MsiHZsIC MBQGCCqGSIb3DQMHBAhgGVm1+xHLIASCBMjjJxkffXUNUcdB22smybvWotw xL0qjEStmwuyExVp+TWC3AyIJN1DE7/rRssjRAqsnSOxIvDGmg0dVsvnbbqZwj 74POu/O2Vy99iFoVgW2q9DyXyL/h64TH9CZtwLKIOGOeEunNKpamDnpfyN8Q fXvNZ91NG4HrEcFmnnij0EwJ0QT8Jn5gAUj+AIPMe32zPqwoccRNYrRXMVM9+</no>	9C ← DELETE AggA bcRrt iFP C4DC Jwp								
Encrypted, and the password is:									
	OK Cancel								
cfCJU2QGI4jT0SorN4u2Lk+S+Qd1s7Ii2wIQMWKPI2R9UGv1tyM6HTPCGoCo6VDI acClCUAsecVrYY081GKTVVJ3bWgWfPtR3OH12YCA2whcCKcG50MByB4tjhHN036q O/g= END_ENCRYPTED_PRIVATE_KEY ← DELETE									
Encrypted, and the password is:									
	OK Cancel								

## 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**.

rise Identity Services Engine	Home   Context Visibility   Operations   Policy	Administrat	ion Vork Centers							License Warning 🔺	S 0	0
System + Identity Management +	Network Resources	id Services + Fe	ed Service + Threat Cent	tric NAC								
Deployment Licensing - Certificates	s + Logging + Maintenance Upgrade + Backup & F	Restore + Admin	Access + Settings									
0												
Certificate Management	Trusted Certificate											
System Certificates	/Edit -Import @Export XDelete DView									Show All		- 8
Trusted Certificates	Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiration Status			
OCSP Client Profile	Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust Ro	Baltimore CyberTrust Ro	Fri, 12 May 2000	Mon, 12 May 2025				
Certificate Signing Requests	Cisco CA Manufacturing	Disabled	Endpoints Infrastructure	6A 69 67 B3 00 00	Cisco Manufacturing CA	Cisco Root CA 2048	Fri, 10 Jun 2005	Mon, 14 May 2029	<b>1</b>			
Certificate Periodic Check Sets	Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure	02	Cisco Manufacturing CA	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037	<b>1</b>			
Certificate Authority	Cisco Root CA 2048	Disabled	Infrastructure Endpoints	SF F8 78 28 28 54	Cisco Root CA 2048	Cisco Root CA 2048	Fri, 14 May 2004	Mon, 14 May 2029	2			
	Cisco Root CA M2	Enabled	Endpoints Infrastructure	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037	<b>2</b>			
	Default self-signed server certificate	Enabled	Endpoints Infrastructure	5A BE 7E D8 00 00	tim24adm.rtpaaa.net	tim24adm.rtpaaa.net	Fri, 30 Mar 2018	Sat, 30 Mar 2019	2			
	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	<b>2</b>			
	DigiCert SHA2 High Assurance Server CA	Enabled	Endpoints Infrastructure	04 E1 E7 A4 DC SC	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 80 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 D0	HydrantID SSL ICA G2	QuoVadis Root CA 2	Tue, 17 Dec 2013	Sun, 17 Dec 2023	2			
	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	<b>1</b>			
	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	2			
	TimFP623	Enabled	Infrastructure Endpoints	BE F9 42 3D 25 AS	TimFP623.rtpaaa.net	TimFP623.rtpaaa.net	Tue, 15 May 2018	Fri, 12 May 2028	<b>1</b>			
	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	<b>2</b>			
	VeriSign Class 3 Secure Server CA - G3	Enabled	Cisco Services	6E CC 7A A5 A7 03	VeriSign Class 3 Secure	VeriSign Class 3 Public	Sun, 7 Feb 2010	Fri, 7 Feb 2020				

3. **파일 선택**을 클릭하고 로컬 시스템에서 FMC CER 파일을 선택합니다.

선택 사항: 식별 이름을 구성합니다.

4. ISE **내**에서 **Trust**(신뢰)를 선택합니다.

선택 사항: 설명을 구성합니다.

5. 이미지에 표시된 대로 제출을 클릭합니다.

#### Import a new Certificate into the Certificate Store

* Certificate File	Choose File TZfpcert.cer	
Friendly Name		<i>i</i>
\[         \]     \[         \[         \]     \[	Trusted For: 🥡	
	✓ Trust for authentication within ISE	
	Trust for client authentication and Syslog	
	Trust for authentication of Cisco Services	
	Validate Certificate Extensions	
Description		
<b>`</b>	Submit Cancel	

## 9단계. FMC에서 pxGrid 연결 구성

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



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 **클릭** 합니다.

8. 드롭다운 목록에서 FMC CER 파일을 선택합니다.

192.168.8.0/24,

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

Status		
٩	ISE connection status: Primary host: Success	
- 👻 Ad	ditional Logs	
		ок

**참고**: 두 개의 ISE pxGrid 노드를 실행하는 경우, pxGrid가 한 번에 하나의 ISE 노드에서만 활 발하게 실행되므로 하나의 호스트가 Success(성공)를 표시하고 하나는 Failure(실패)를 표시 하는 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(iseagenthostname-33bytes)용, 다른 하나는 테스트 디바이스(firesightisetest-hostname-33bytes)용.

Identity Services Engine	Home + Context Visibility	Operations      Policy      Admin	istration + Work Centers				License Warming 🔺 🔍 😑 🥥 🗢					
System      Identity Management	System + Identity Management + Network Resources + Device Portal Management pxGird Sarvices + Feed Sarvice + Treat Centric NAC											
All Clients Web Clients Capabilities Live Log Settings Certificates Permissions												
✓Enable ⊘Disable ②Approve	😝 Group 👎 Decline 🔞 Delete 🕶	Refresh Total Pending Approval(0)	•				1-7 of 7 Show 25 + per page Page 1 +					
Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log						
0		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate	View						
		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View						
		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View						
		Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate	View						
П		Canabilities(4 Pub. 2 Sub)	Online (XMPP)	Internal	Certificate	Vew						
		Capabilities(0 Pub, 6 Sub)	Online (XMPP)		Certificate	View						
		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate	View						

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.

<ul> <li>iseagent-firepower-20762a2982d</li> </ul>	Ca	pabilities(0 Pub, 6 Sub) O	nline (XMPP)		Certificate	View		
	Cap	ability Detail			1 - 6 of 6	Show 25 👻 per page	Page 1	¢
		Capability Name	Capability Version	Messaging Role	Message Filter			
	0	AdaptiveNetworkControl	1.0	Sub				
	0	Core	1.0	Sub				
	0	EndpointProfileMetaData	1.0	Sub				
	0	EndpointProtectionService	1.0	Sub				_
	0	SessionDirectory	1.0	Sub				
	0	TrustSecMetaData	1.0	Sub				

**참고**: Cisco 버그 IDCSCvo<u>75376으로</u> 인해 호스트 이름 제한이 있으며 대량 다운로드가 실패 합니다. FMC의 테스트 단추에 연결 오류가 표시됩니다. 이는 2.3p6, 2.4p6 및 2.6에 영향을 줍 니다. 현재 권고하는 내용은 정식 패치가 나올 때까지 2.3 패치 5나 2.4 패치 5를 실행하는 것 이다.

## 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

Overview Analysis Policies Devices Objects   AHP Intelligence Depicy   © System Help + admin +																
Contex	it Expl	orer Connection	s • Intrusions •	Files • Hosts •	Users + Activ	e Sessions Vulnerabil	ties • Correlatio	n • Custom	• Lookup •	Search						
Boskmark This Page: Report Designer															signer Dashboard View Bookn	harks Search +
Active Sessions																
							Info     No device <u>Click here</u>	s registered. to register a dev	óze.	×						
Table V	fiew o	Active Sessions >	Active Sessions													
<ul> <li>Search</li> </ul>	th Cons	traints (Edit Search)														Disabled Columns
Jump		•														
	•	Login Time ×	Last Seen ×	<u>User</u> ×		Authentication Type ×	<u>Current IP</u> ×	Realm ×	<u>Username</u> ×	First Name >	Last Name ×	E-Mail ×	Department ×	Phone ×	Discovery Application ×	Device ×
4 0	2	018-05-15 13:26:21	2018-05-15 13:27:36	🗏 xiao vao (LAB\xia	VBO. LDAP)	Passive Authentication		LAB					users (rtoaaa)		LDAP	firecower
4 0	2	018-05-15 12:35:54	2018-05-15 12:35:54	admin admin (LAB	Nadmin, LDAP)	Passive Authentication		LAB					users.(ctoasa)		LDAP	firecower
4 0	2	018-05-15 11:27:14	2018-05-15 11:27:14	tom (LAB\tom, LD	AP1	Passive Authentication		LAB					users (rtoaaa)		LDAP	firecower
4 0	2	018-05-15 11:20:30	2018-05-15 11:20:30	Stark kent (LAB)su	(PAGL_nam_LDAP)	Passive Authentication		LAB					users.(rtoaaa)		LDAP	firequier
< < P	hage 🔤	of 1 >>  Display	ring rows 1-4 of 4 rows													
Vie	view ew All	Logout														

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 번 역 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.