Integratie van ISE 2.4 en FMC 6.2.3 pxGrid configureren

Inhoud

Inleiding **Voorwaarden** Vereisten Gebruikte componenten ISE configureren Stap 1. PxGrid-services inschakelen Stap 2. Configureer ISE om alle PxGrid op certificaat gebaseerde accounts goed te keuren Stap 3. Exporteren ISE MNT Admin-certificaat en PxGrid CA-certificaten **FMC** configureren Stap 4. Voeg een nieuw domein toe aan FMC Stap 5. VCC CA-certificaat genereren Stap 6. Het certificaat en de privésleutel uit het gegenereerde certificaat halen met behulp van OpenSSL Stap 7. Certificaat in het VCC installeren Stap 8. Importeer het FMC-certificaat in ISE Stap 9. PxGrid Connection op FMC configureren Verifiëren Verificatie in ISE Verificatie in het VCC Problemen oplossen

Inleiding

In dit document wordt het configuratieproces beschreven voor de integratie van ISE pxGrid versie 2.4 en FMC versie 6.2.3.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ISE-lijnkaart 2.4
- VCC 6.2.3
- Active Directory/Lichtgewicht Directory Access Protocol (LDAP)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Standalone ISE 2.4
- VCCv 6.2.3
- Active Directory 2012R2
- Identity Services Engine (ISE) PxGrid versie 2.4
- Firepower Management Center (FMC) versie 6.2.3

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

ISE configureren

Stap 1. PxGrid-services inschakelen

- 1. Log in de ISE Admin GUI, navigeer naar Beheer > Implementatie.
- 2. Selecteer het ISE-knooppunt dat voor pxGrid-personen moet worden gebruikt.



3. Schakel de pxGrid-service in en klik op **Opslaan** zoals in de afbeelding.

Deployment	Deployment Nodes List > tim24adm
()E-	Edit Node
Argenter Argenter	General Settings Profiling Configuration
	Hostname
	FQDN
	Node Type Identity Services Engine (ISE)
	Role STANDALONE Make Primary
	Administration
	V V Monitoring
	Role PRIMARY *
	Other Monitoring Node
	Policy Service
	Enable Session Services (i)
	Include Node in Node Group None 👻 👔
	Enable Profiling Service (j)
	Enable Threat Centric NAC Service (i)
	Enable SXP Service (i)
	Enable Device Admin Service ()
	Enable Passive Identity Service (i)
	→ pxGrid 👔
	Save Reset

4. Controleer dat de pxGrid-services vanaf de CLI worden uitgevoerd.

Opmerking: Het proces vereist tot 5 minuten voor de pxGrid-services om de status Hoge beschikbaarheid (HA) volledig te starten en te bepalen als er meer dan één pxGrid-knooppunt in gebruik is.

5. SSH naar de ISE-pxGrid-knooppunt CLI en controleer de toepassingsstatus.

```
# 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. Open de ISE-beheerdersgids en controleer of de services online zijn en goed functioneren. Ga naar **Beheer > PxGrid Services**.

7. Onder aan de pagina geeft ISE Connected to pxGrid <pxGrid knooppunt FQDN> weer.

-de-ti- cisce Identity Services Engine Home + Context	Visibility Operations Policy Admi	istration + Work Centers				License Warning 🔺 🔍 🔍 🔿 🔿
System Identity Management Network Resources	Device Portal Management pxGrid Services	Feed Service Threat Centre	ic NAC			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					
	Ociete + SRefresh 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	
□ ▶ 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	
Connected to syGrid Em24adm strease net						

Stap 2. Configureer ISE om alle PxGrid op certificaat gebaseerde accounts goed te keuren

1. Ga naar Beheer > PxGrid-services > Instellingen.

2. Schakel het vakje "Automatisch nieuwe op certificaten gebaseerde accounts goedkeuren" in en klik op **Opslaan**.

cisco	Identity Services Engin	ne Home	► Context Visibility	Operations	Policy	 Administration 	Work Centers
▶ Sy	stem Identity Manager	ment I Network	Resources + Device	e Portal Management	pxGrid Serv	vices + Feed Se	rvice + Threat Centric NAC
All	Clients Web Clients	Capabilities Li	ve Log Settings	Certificates Perr	nissions		
F	xGrid Settings						
	Automatically approve ne Allow password based ac	w certificate-based	accounts				
	Use Default Save						
	Test						
Conne	cted to pxGrid tim24adm.rtp	aaa.net					

Opmerking: de beheerder moet de FMC-verbinding met ISE handmatig goedkeuren als deze optie niet is ingeschakeld.

Stap 3. Exporteren ISE MNT Admin-certificaat en PxGrid CA-certificaten

1. Navigeer naar **Beheer > Certificaten > Systeemcertificaten**.

2. Breid het knooppunt voor primaire bewaking (MNT) uit als dit niet is ingeschakeld voor het knooppunt voor primair beheer.

3. Selecteer het certificaat met het veld Gebruikte-by "Admin".

Opmerking: deze handleiding maakt gebruik van het standaard ISE-zelfondertekende certificaat voor gebruik van Admin. Als u een certificaat gebruikt dat is ondertekend door een certificeringsinstantie (CA), exporteert u de root-CA die het beheercertificaat heeft ondertekend naar de ISE MNT-knooppunt.

4. Klik op Exporteren.

- 5. Kies de optie om Certificaat en Private Key te exporteren.
- 6. Stel een coderingssleutel in.
- 7. Het bestand exporteren en opslaan zoals in de afbeelding.



9. Ga terug naar het scherm ISE-systeemcertificaten.

10. Bepaal het veld Uitgegeven door op het certificaat met behulp van het "pxGrid"-gebruik in de kolom Gebruikt door.

Opmerking: In oudere versies van ISE was dit een zelfondertekend certificaat, maar vanaf 2.2 wordt dit certificaat standaard afgegeven door de interne ISE CA-keten.

1. Selecteer het certificaat en klik op Weergeven zoals in de afbeelding.

ence Identity Services Engine	Home	nationa + Policy + Administra	Ion Work Centers				License Warning 🔺 🧠 😐 😋 🔍
System Identity Management	Network Resources Device Portal M	anagement pxGrid Services + Fe	ed Service + Threat Centric NAC				
Deployment Licensing - Certificate	+ Logging + Maintenance Upgra	ide + Backup & Restore + Admir	Access + Settings				
0							
Certificate Management	System Certificates 🛕 For disas	ter recovery it is recommended to expo	rt certificate and private in pairs of all syste	m certificates.			
System Certificates	🕖 Edit 🛛 🕂 Generate Self Signed C	ertificate 🕂 Import 🖗 Export	X Delete				
Trusted Certificates	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date
OCSP Client Profile	▼ tim24adm						
Certificate Signing Requests	e,CN=tim24adm.rtpaaa.net#	tem Certificat Certificate Se nxDrid				Dui: 29 Mar 2018	Thu, 30 Mar 2028
Certificate Periodic Check Set5	rvices Endpoint Sub CA - tim 1	24adm#0000					-
Certificate Authority	 Default self-signed sami serv CN=SAML_tim24adm.rtpasa 	er certificate - SAML				Fri, 30 Mar 2018	Sat, 30 Mar 2019 🛃
	 Default self-signed server cer 	tificate EAP Authentication, Ad Portal, RADIUS DTLS	min, Default Portal Certificate Group (j)			Fri, 30 Mar 2018	Sat, 30 Mar 2019

- 12. Bepaal het basiscertificaat. In dit geval is het "Certificate Services Root CA tim24adm".
- 13. Sluit het venster voor de certificaatweergave zoals in de afbeelding.

Certificate Services Root CA	A - tim24adm	
Certificate Services No	de CA - tim24adm	
Certificate Services	s 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. Breid het menu van de ISE-certificeringsinstantie uit.

15. Selecteer certificaten van de certificeringsinstantie.

16. Selecteer het basiscertificaat dat is geïdentificeerd en klik op **Exporteren.** Sla vervolgens het CA-certificaat van de PxGrid Root op zoals in de afbeelding.

use Identity Services Engine	Home	Context Visibility Operation	ns + Policy +A	dministration + Work Centers					License Warning 🔺 👘	A 0 0 0
System Identity Management	Network	Resources + Device Portal Manag	ement pxGrid Service	s + Feed Service + Threat Cent	ric NAC					
Deployment Licensing Certificate	rs ⊁Lo	gging + Maintenance Upgrade	Backup & Restore	Admin Access Settings						
0										
Certificate Management	CAC	ertificates								
- Certificate Authority	1	Edit 👍 Import 🕼 Export 🗶	Delete 🔎 View 🔮	Refresh						
Outries A		Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiration Status
Oneman	V Sr	n24adm								
Issued Certificates	0	Certificate Services Endpoint Sub CA - tim24adm#00003	Enabled	Infrastructure,Endpoints	32 D2 72 55 A9 7D 40 13 8F 2A EF CF 0D 1C 41 A8	Certificate Services Endpoint Sub	Certificate Services Node CA -	Thu, 29 Mar 2018	Thu, 30 Mar 2028	2
Certificate Authority Certificates		Certificate Services Root CA -	Enabled	Infrastructure,Endpoints	36 67 74 15 A5 A8 4F EB B7 46 1	Certificate Services Root CA -	Certificate Services Root CA -	Thu, 29 Mar 2018	Thu, 30 Mar 2028	
Internal CA Settings	-	Certificate Services Node CA -			30 1A 22 E7 AA E5 45 35 8C 65		umpresent			-
Certificate Templates		tim24adm#00002	Enacied	inmastructure,Endpoints	78 EE 53 09 34 3E	tim24adm	tim24adm	1 nu, 29 Mar 2018	Thu, 30 Mar 2028	×.
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 configureren

Stap 4. Voeg een nieuw domein toe aan FMC

- 1. Open de FMC GUI en navigeer naar **System > Integration > Realms**.
- 2. Klik op Nieuw gebied zoals in de afbeelding.

															_		
Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence								Deploy	🛛 🔍 Sys	tem Help v	admin v
									Configuration	Users	Domains	Integration	Updates	Licenses v	Haith •	Monitoring •	Tools •
														•			
Cisco CSI	Realms	Identi	ty Sources	eStream	er He	ost Input Client	Smart Software Satellite										
	/														🔀 Comp	are realms	New realm
-																	

3. Vul het formulier in en klik op de knop Active Directory (AD) testen.

Opmerking: de AD Join Gebruikersnaam moet in UPN-formaat (User Principal Name) zijn of de test mislukt.

4. Als de Test AD Join succesvol is, klikt u op OK.

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. Klik op het tabblad Directory en klik vervolgens op Map toevoegen zoals in de afbeelding.



6. Configureer IP/Hostname en test verbinding.

N.B.: Als de test mislukt, controleert u de referenties op het tabblad Real Configuration.

7. Klik op **OK**.

Edit directory	? ×
Hostname / IP Address	
Port 389	
Encryption O STARTTLS O LDAPS O None	
SSL Certificate 🗸 🗿	
OKTest	Cancel
Status	
Test connection succeeded	
ОК	

8. Klik op het tabblad Gebruikersdownload.

Overview Analysis Policies Devices Objects AMP Intelligence						Deploy	🕘 🔍 Syr	stem Help v	admin +
	Conf	lguration Users	Domains	Integration	Updates	Licenses •	Health •	Monitoring •	Tools •
LAB Enter Description								Save	Cancel
Directory Realm Configuration User Download									

- 9. Indien nog niet geselecteerd, gebruiker en groep downloaden inschakelen
- 10. Klik op Nu downloaden



11. Zodra de lijst is ingevuld, kunt u de gewenste groepen toevoegen en **op Toevoegen om op te nemen** selecteren.

12. Sla de gebiedsconfiguratie op.

Overview Analysis Policies Devices Objects AMP Intelligence								Deploy 🥝 S	ystem Help v admin v
			Configuration	Users	Domains	Integration	Updates	Licenses • Health •	Monitoring Tools
IAB E								You have unsaved chang	Save 🖸 Cancel
LAD -									
Enter Description									
Directory Realm Configuration User Dowmload								-	
Ownload users and groups									
Begin automatic download at B Y PM Y America/New York Repeat Every 24 Y Hours									
d Download Now									
Available Groups C		Groups to Include (35)			Groups to Ex	clude (0)			
Search by name		A NetOps		8	None				
A NetOps		SQLServer2005SQLBrowserUsersRTPAAA-DC2		8					
A SQLServer2005SQLBrowserUserSRTPAAA-OC2		A WSUS Administrators		8					
A WSUS Administrators		A Enterprise Read-only Domain Controllers		8					
A Enterprise Read-only Domain Controllers		af DnsUpdateProxy		8					
A DnsUpdateProxy		🝰 jhoehn-group		8					
🝰 jhoehn-group		A Denied RODC Password Replication Group		8					
A Denied RODC Password Replication Group		🝰 Domain Admins		8					
🔗 Domain Admins		af Child		8					
🔗 Child		af DnsAdmins		8					
A DosAdmins		▲ Lester\Made\Me\Do\It		8					
A Lester/Made/Me\Do\Jt		af Group Policy Creator Owners		8					
A Group Policy Creator Owners		af INE		8					
₽ INE		🖌 💣 Domain Users		8					
🔗 Domain Users		de ChadTest		8					
🔗 ChadTest		Acad-only Domain Controllers		8					
A Read-only Domain Controllers	Include	AS and IAS Servers		8					
AS and IAS Servers	Add to	de Cert Publishers		8					
A Cert Publishers	Exclude	🛃 Schema Admins		8					
🔗 Scheme Admins		A WSUS Reporters		8					
A WSUS Reporters		af Parent		8					
A Parent		af 15E Admins		8					
🔗 ISE Admins		WinRMRemoteWMIUsers		8					
A WinAMRemoteWHIUsers		Allowed RODC Password Replication Group		8					
Allowed RODC Password Replication Group		2 TimSponsors		8					
🔗 TimSponsors		AllowedVPN		8					
Allowed VPN		Enterprise Admins		8					
🔗 Enterprise Admins		🛃 test-users		8					
🝰 test-users		a sponsors		8					
🔗 sponsors		A HelpLibraryUpdaters		8					
🝰 HelpLibraryUpdaters		Protected Users		8					
🔗 Protected Users		Pomain Guests		8					
🔗 Domain Guests		Domain Computers		8					
🝰 Domain Computers		Domain Controllers		8.0					
🝰 Domain Controllers		Enter Derivities		-	Enter Herr Do	rhuston.			
A Classifie Densis Controllers		Eine Ant Intransi			Lenver Oper Ex				Add

13. Schakel de Real State in.

Overview	Analysis I	Policies Devices	Objects Al	4P Intelligence									Deploy	ି 🍳 🔊	rstem Help	v admin v
								Configuration	Users	Domains	Integration	Updates	Licenses +	Health •	Monitoring	 Tools •
Cisco CSI	Realms	Identity Sources	eStreamer	Host Input Client	Smart Software Satellite											
														Com	pare realms	New realm
Name						Description	Domain	Туре		Base DN	Group	DN	Group Atte	ribute	State	
LAB							Global	AD		DC=rtpaaa,DC=n	et CN+U	sers, DC=rtpaaa,	,DC+ member			± 🥒 🐚 🖯

Stap 5. VCC CA-certificaat genereren

1. Navigeer naar **Objecten > Objectbeheer > Interne CA's** zoals in de afbeelding.

Overview Analysis Polici	es Devices Objects AMP Intelligence		Deploy	🔺 System Help 🔹	admin +
Object Management Intro	usion Rules				
			O Add Netwo	vik •	
Retwork	Name	Value	Type	Override	
Port Interface	any		Group	×	4.8
Application Filters	any-ipu4		Network	×	
S VLAN Tag	any-ipv6		Host	×	
Geolocation	IPv4-Benchmark-Tests		Network	×	
Time Range	1Pv4-Link-Local		Network	×	
\$ Variable Set	1Pv4-Multicast		Network	×	
Network Lists and Feeds	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	×	
C File List	Dv4-Private-A3-87C1918		Group	×	
Distinguished Name Individual Objects	IPv4-IPv4-Mapped		Network	×	
Cobject Groups	IPv6-Link-Local		Network	×	
A PKI	IPv6-Private-Unique-Local-Addresses		Network	×	
Trusted CAs	IPv6-to-IPv4-Relay-Anycast		Network	×	
External Certs Internal Certs Cert Enrolment Internal CA Groups Internal CA Groups Internal Cert Groups Internal Cert Groups External Cert Groups					

- 2. Klik op Generate CA.
- 3. Vul het formulier in en klik op Generate self-signed CA.

Overview Analysis	Policies	Devices	Objects AMP Intelligence						Deploy 🔺 Sy	stem Help + a	dmin v
Object Management	Intrusio	n Rules									
							_	Generate CA	O Import CA	🔍 Filter	
Network		Name					Value				
			Generate Internal Certificate	Authority		? ×					
			Name:	LabFP623	83						
			Country Name (two-letter code):	US							
			State or Province:	NC	_						
			State of Frovince.	NC							
			Locality or City:	RTP							
			Oranaization		_						
			organization.	Cisco							
			Organizational Unit (Department):	TAC							
			Common Name:		-						
			common Name.								
			Concernto CCD	Concepts colf signed CA							
			Generate CSK	Generate self-signed CA	Cance	81					

4. Zodra de generatie voltooid is, klikt u op het potlood rechts van het gegenereerde CAcertificaat zoals in de afbeelding.

Overview Analysis	Policies Devices Objects A	MP Intelligence	Deploy 💧	System Help +	admin +
Object Management	Intrusion Rules				
			Generate CA Generate CA	A Filter	
Network	Name		Value		
Port A Interface	LabFP623		CN+LabFP623.rtpaaa.net, ORG+Cisco, OU+TAC, C+US		/ 8

5. Klik op Downloaden.

lame:	LabFP623	
Subje	ct:	
Co	ommon Name:	
Or	ganization: Cisco	
Or	ganization Unit: TAC	
Issue	r:	
Co	ommon Name:	
Or	ganization: Cisco	
Or	ganization Unit: TAC	
Not V	alid Before:	
Ma	ay 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	Cancel

6. Configureer en bevestig het coderingswachtwoord en klik op OK.

7. Sla het bestand Public-Key Cryptography Standards (PKCS) p12 op in uw lokale bestandssysteem.

Stap 6. Het certificaat en de privésleutel uit het gegenereerde certificaat halen met behulp van OpenSSL

Dit gebeurt op basis van het FMC of op elke client die OpenSSL-opdrachten kan uitvoeren. Dit voorbeeld gebruikt een standaard Linux shell.

1. Gebruik **openssl** om het certificaat (CER) en de persoonlijke sleutel (PVK) uit het p12-bestand te extraheren.

2. Extraheer het CER-bestand en configureer vervolgens de certificaatexportsleutel uit de certgeneratie op FMC.

~\$ openssl pkcs12 -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. Extraheer het PVK-bestand, configureer de exportsleutel voor het certificaat, stel vervolgens een nieuwe PEM-wachtwoordzin in en bevestig.

~\$ openssl pkcs12 -nocerts -in <filename.p12> -out <filename.pvk>
Password: Last login: Tue May 15 18:46:41 UTC 2018 Enter Import Password: MAC verified OK
4. Deze PEM-zin is nodig in de volgende stap.

Stap 7. Certificaat in het VCC installeren

- 1. Ga naar Objecten > Objectbeheer > PKI > Interne certs.
- 2. Klik op Interne waarschuwing toevoegen zoals in de afbeelding.

Overview Analysis	Policies De	evices Objects AMP Intelligence	Deploy 🔮 Sys	stem Help + admin +
Object Management	Intrusion Ru	les		
			Add Internal Cert	🔍 Filter 🔛
Retwork	Nam	•	Value	
P Port	Test		CHUTHERING AND AN OCCUPANTIC CUIE	2 -
🥵 Interface	THE P	1963	CH-INFFEESTQUEETING, OKG-CIGO, OG-INC, C-05	¥ 0
nnei Zone				
Application Filters				
S VLAN Tag				
URL .				
Geolocation				
Time Range				
Ş Variable Set				
 Security Intelligence 				
Network Lists and	reeds			
ONS Lists and Feed	15			
URL Lists and Feed	5			
Sinkhole				
C File List				
Optionulated Name				
Tedividual Objects				
Chiert Cerups				
A PKI				
Internal CAs				
Trusted CAs				
External Certs				
Internal Certs				
Cert Enrollment				
E Internal CA Groups				
Trusted CA Groups				
Enternal Cert Group	25			
External Cert Grou	25			

3. Configureer een naam voor het interne certificaat.

4. Blader naar de locatie van het CER-bestand en selecteer dit. Zodra de certificaatgegevens zijn ingevuld, selecteert u de tweede.

5. Bladeren **door optie** en selecteer het PVK-bestand.

6. Verwijder eventuele belangrijke "eigenschappen van de tas" en eventuele waarden achter de afbeelding in het PVK-gedeelte. De PVK begint met -----START ENCRYPTED PRIVATE KEY— en eindigt met -----END ENCRYPTED PRIVATE KEY—.

N.B.: U kunt niet op **OK** klikken als de PVK-tekst tekens bevat die niet onder de regelafstand en de bijbehorende koppeltekens vallen.

7. Controleer het vakje Encrypted en configureer het wachtwoord dat is gegenereerd toen de PVK in Stap 6 is geëxporteerd.

8. Klik op OK.

Add Known Internal Certificate

Name: TZfpcert
Certificate Data or, choose a file: Browse
BEGIN CERTIFICATE MIIDfTCCAmWgAwIBAgIJAKIemFK+L7iYMA0GCSqGSIb3DQEBCwUAMGQxCzAJBgNV BAYTAIVTMQswCQYDVQQIDAJOQzEMMAoGA1UEBwwDUIRQMQ4wDAYDVQQKDAVDaXNj bzEMMAoGA1UECwwDVEFDMRwwGgYDVQQDDBNMYWJGUDYyMy5ydHBhYWEubmV0MB4X DTE4MDUxNTE4MTM1MloxDTI4MDUxMjE4MTM1MlowZDELMAkGA1UEBhMCVVMxCzAJ BgNVBAgMAk5DMQwwCgYDVQQHDANSVFAxDjAMBgNVBAoMBUNpc2NvMQwwCgYDVQQL DANUQUMxHDAaBgNVBAMME0xhYkZQNjIzLnJ0cGFhYS5uZXQwggEiMA0GCSqGSIb3 DQEBAQUAA4IBDwAwggEKAoIBAQDMjtS5IUIFiZkZK/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 9C Key Attributes: <no attributes=""> MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQI5uV3MsiHZsICAggA MBQGCCqGSIb3DQMHBAhgGVm1+xHLIASCBMjjJxkffXUNUcdB22smybvWotwbcRrt xL0qjEStmwuyExVp+TWC3AyIJN1DE7/rRssjRAqsnSOxIvDGmg0dVsvnbbqZwjFP 74POu/O2Vy99iFoVgW2q9DyXyL/h64TH9CZtwLKIOGOeEunNKpamDnpfyN8QC4DC fXvNZ9/NG4HrEcFmnnij0EwJ0QT8Jn5gAUj+AIPMe32zPqwoccRNYrRXMVM9+Jwp</no>
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

Stap 8. Importeer het FMC-certificaat in ISE

1. Open de ISE GUI en navigeer naar Beheer > Systeem > Certificaten > Betrouwbare certificaten.

2. Klik op Importeren.

dentity Services Engine	Home + Context Visibility + Operations + Policy	- Administra	Son Vork Centers							License Warning 🔺	<u> </u>	0 0	0
System + Identity Management +	Network Resources	id Services + Fe	ed Service + Threat Cent	tric NAC									
Deployment Licensing - Certificates	Logging Maintenance Upgrade Backup &	Restore + Admir	Access + Settings										
0													
Certificate Management	Trusted Certificat												
System Certificates	/Edit 📲 Import 😨 Export 🗙 Delete 🔎 View									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 89	Baltimore CyberTrust Ro	Baltimore CyberTrust Ro	Fri, 12 May 2000	Mon, 12 May 2025	1				
Certificate Signing Requests	Cisco CA Manufacturing	O Disabled	Endpoints Infrastructure	6A 69 67 B3 00 00	Cisco Manufacturing CA	Cisco Root CA 2048	Fri, 10 Jun 2005	Mon, 14 May 2029	1				
Certificate Periodic Check Setti	Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure	02	Cisco Manufacturing CA	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037					
Certificate Authority	Cisco Root CA 2048	Disabled	Infrastructure Endpoints	5F F8 78 28 28 54	Cisco Root CA 2048	Cisco Root CA 2048	Fri, 14 May 2004	Mon, 14 May 2029					
avgr Solating Sciences Registry How • Contact V • System • Identify Management > Network Resources Deployment Licensing • Certificates > Logging Management System Certificates Identify Management > Identify Management / Identify Management / Identify Management System Certificates Identify Management / Identify Management / Identify Management / Identify	Cisco Root CA M2	Enabled	Endpoints Infrastructure	01	Cisco Root GA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037	1				
	Default self-signed server certificate	Enabled	Endpoints Infrastructure	SA BE 7E D8 00 00	tim24adm.rtpaaa.net	tim24adm.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	1				
	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	1				
	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	Infrastructure Endpoints	BE F9 42 3D 25 AS	TimFP623.rtpaaa.net	TimFP623.rtpaaa.net	Tue, 15 May 2018	Fri, 12 May 2028	1				
	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 AS A7 03	VeriSign Class 3 Secure	VeriSign Class 3 Public	Sun, 7 Feb 2010	Fri, 7 Feb 2020	1				

3. Klik op Kies bestand en selecteer het FMC CER-bestand van uw lokale systeem.

Optioneel: Een vriendschappelijke naam instellen.

4. Controleer vertrouwen op verificatie binnen ISE.

Optioneel: een beschrijving instellen.

5. Klik op Indienen zoals in de afbeelding.

Import a new Certificate into the C	ertificate Store	
* Certificate File	Choose File TZfpcert.cer	
Friendly Name		i
	Trusted For: (j)	
	✓ Trust for authentication within ISE	
	Trust for client authentication and Syslog	
	Trust for authentication of Cisco Services	
	Validate Certificate Extensions	
Description		
<u>}</u>	Submit Cancel	

Stap 9. PxGrid Connection op FMC configureren

1. Navigeer naar Systeem > Integratie > Identiteitsbronnen zoals in de afbeelding.



- 2. Klik op ISE.
- 3. Configureer het IP-adres of de hostnaam van de ISE-pxGrid-knooppunt.
- 4. Selecteer de + rechts van de PxGrid Server CA.

5. Geef het server CA-bestand een naam en blader vervolgens naar de pxGrid Root Signing CA die is verzameld in Stap 3. en klik op **Opslaan**.

6. Selecteer + rechts van MNT Server CA.

7. Geef het CA-bestand van de server een naam en blader vervolgens naar het Admin-certificaat dat in Stap 3 is verzameld en klik op **Opslaan**.

8. Selecteer het FMC CER-bestand in de vervolgkeuzelijst.

Identity Sources		
Service Type	None Identity Services Engine	User Agent
Primary Host Name/IP Address * Secondary Host Name/IP Address	<ise address="" ip="" node="" pxgrid=""></ise>	
pxGrid Server CA *	ISE24InternalRoot	▼ ③
MNT Server CA *	ISE24SelfSigned	▼ ②
FMC Server Certificate *	TimFP623	v ()
ISE Network Filter		ex. 10.89.31.0/24, 192.168.8.0/24,
* Required Field	Test	

9. Klik op Test.

10. Als de test succesvol is, klikt u op **OK** en vervolgens **Opslaan** rechtsboven op het scherm.

Status



Opmerking: wanneer u twee ISE pxGrid-knooppunten gebruikt, is het normaal dat één host Success toont en één die de failliet laat zien, omdat pxGrid alleen actief op één ISEknooppunt tegelijk werkt. Het hangt van de configuratie af of welke Primaire gastheer Mislukking zou kunnen tonen en de Secundaire gastheer Succes zou kunnen tonen. Dit is allemaal afhankelijk van welke knooppunt in ISE de actieve pxGrid-knooppunt is.

Verifiëren

Verificatie in ISE

1. Open de ISE GUI en navigeer naar Beheer > PxGrid-services.

Indien geslaagd, worden twee verbindingen van de vuurkracht vermeld in de cliëntlijst. Een voor het feitelijke FMC (iseagent-hostname-33bytes) en een voor het testapparaat (firesightisetest-hostname-33bytes).

-them Identity Services Engine	Home Context Visibility	Operations Policy Admin	istration Work Centers				Licen	se Warning 🔺 🔍 🕴	0 0		
System Identity Management	t Network Resources Device Pr	ortal Management pxGrid Services	Feed Service Threat Centric	NAC							
All Clients Web Clients Capabilities Live Log Settings Certificates Permissions											
√Enable ØDisable ØApprove	🖯 Group 👎 Decline 🚯 Delete 🕶	Refresh Total Pending Approval(0)					1 - 7 of 7	Show 25 + per page	Page 1 0		
Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log					
		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate	Vew					
		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	Vew					
		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	Vew					
		Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate	View					
		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	Vew					

De iseagent-firepower verbinding toont zes (6) subs en verschijnt online.

De verbinding met de vuurbestendigste vuurkracht geeft nul (0) subs weer en wordt offline weergegeven.

Uitgebreide weergave van de iseagent-firepower client geeft de zes abonnementen weer.

 iseagent-firepower-20762a2982d 	Ca	apabilities(0 Pub, 6 Sub) Or	nline (XMPP)		Certificate		View			
	Cap	pability Detail			1 - 6 of 6	Show 3	25 🔻 per page	Page	1 ;	ŧ.
		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						
										1

Opmerking: vanwege Cisco-bug <u>IDCSCvo75376</u> er is een hostname beperking en bulk downloaden mislukt. De testknop op het VCC geeft een storing in de connectiviteit weer. Dit betreft 2.3p6, 2.4p6 en 2.6. De huidige aanbeveling is om 2,3 pleister of 2,4 pleister 5 te gebruiken totdat een officiële pleister wordt afgegeven.

Verificatie in het VCC

1. Open de FMC GUI en navigeer naar **Analysis > Gebruikers > Actieve sessies**.

Alle actieve sessies die via de Session Directory-mogelijkheid in ISE worden gepubliceerd, worden weergegeven in de tabel Actieve sessies op FMC.

Ov	Overview Analysis Policies Devices Objects AMP Intelligence [Depicy] © System Help + admits														edmin v					
Cor	text Explore	r Connection	s • Intrusions •	Files • Hosts	 Users + Acti 	ve Sessions Vulner	abilities •	Correlation •	Custom	Lookup •	Search									
															Bookmark This Pa	ige Report Des	ligner Dasht	oard View Bo	okmarks S	arch v
A	tive Se	ssions																		
								O Info			~									
								No devices req	istered.											
								Click here to re	oister a devic	e.										
Tel	ie View of As	tive Sessions > (Active Sessions																	
• 5	earch Constrai	nts (Edit Search)																	Disable	Columns
3	uma ta																			
	- L0	oin Time ×	Last.Seen ×	User ×		Authentication Type	× Surre	ent.IP ×	Realm ×	Username ×	First Name	× Last Name ×	E-Mail ×		Department ×	Phone ×	Discovery	Application	× De	lice ×
- 4	2018	-05-15 13:26:21	2018-05-15 13:27:36	iteo vao (LAB	xiavao, LDAP)	Passive Authentication			AB						users (rtoaaa)		LDAP		fires	ower
4	2018	-05-15 12:35:54	2018-05-15 12:35:54	admin admin (LABLadmin_LDAP)	Passive Authentication			AB						users.(rtoaaa)		LDAP		fired	ower
4	2018	-05-15 11:27:14	2018-05-15 11:27:14	tom (LAB\tom	LDAP	Passive Authentication			AB						users (rtoaaa)		LDAP		fired	ower
4	2018	-05-15 11:20:30	2018-05-15 11:20:30	slark kent (LA	Superman, LDAP)	Passive Authentication			AB.						users.(toaaa)		D LDAP		fired	ower
K	< Page 1	of 1 >> Display	ing rows 1-4 of 4 rows																	
	View	Logout]																	
	View All)																		

Vanuit de FMC CLI sudo-modus geeft de 'adi_cli sessie' de informatie weer van de

gebruikerssessie die van ISE naar FMC is gestuurd.

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.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.