

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:

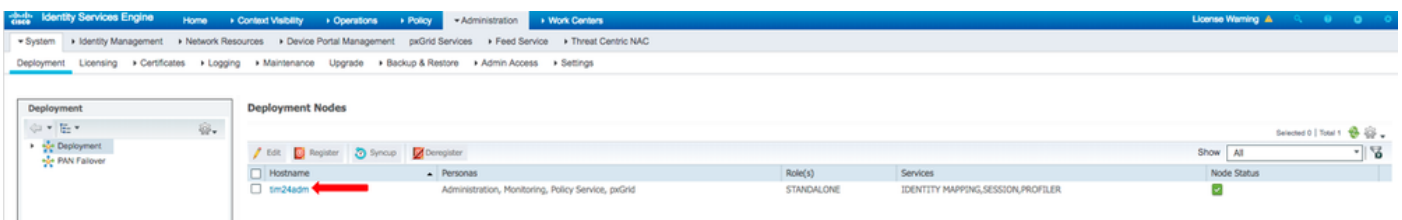
- Standalone ISE 2.4
- VCCv 6.2.3
- Active Directory 2012R2
- Identity Services Engine (ISE) PxGrid versie 2.4
- Firepower Management Center (FMC) versie 6.2.3

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 Nodes List > tim24adm

Edit Node

General Settings | Profiling Configuration

Hostname
FQDN
IP Address
Node Type: Identity Services Engine (ISE)

Role: STANDALONE **Make Primary**

Administration

Monitoring

Role: PRIMARY

Other Monitoring Node

Policy Service

Enable Session Services (i)

Include Node in Node Group: None (i)

Enable Profiling Service (i)

Enable Threat Centric NAC Service (i)

Enable SXP Service (i)

Enable Device Admin Service (i)

Enable Passive Identity Service (i)

pxGrid (i)

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.

Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log
ise-mnt-tim24adm		Capabilities(2 Pub, 1 Sub)	Online (DHPP)	Internal	Certificate	View
ise-fincut-tim24adm		Capabilities(0 Pub, 0 Sub)	Online (DHPP)	Internal	Certificate	View
ise-pubsub-tim24adm		Capabilities(0 Pub, 0 Sub)	Online (DHPP)	Internal	Certificate	View
ise-bridge-tim24adm		Capabilities(0 Pub, 4 Sub)	Online (DHPP)	Internal	Certificate	View
ise-admin-tim24adm		Capabilities(4 Pub, 2 Sub)	Online (DHPP)	Internal	Certificate	View
iseagent-freepower-20762a2962d...		Capabilities(0 Pub, 6 Sub)	Online (DHPP)		Certificate	View
freesightstest-freepower-20762a...		Capabilities(0 Pub, 0 Sub)	Offline (DHPP)		Certificate	View

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**.

PxGrid Settings

Automatically approve new certificate-based accounts

Allow password based account creation

Use Default Save

Test

Connected to pxGrid tim24adm.rtpaaa.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".

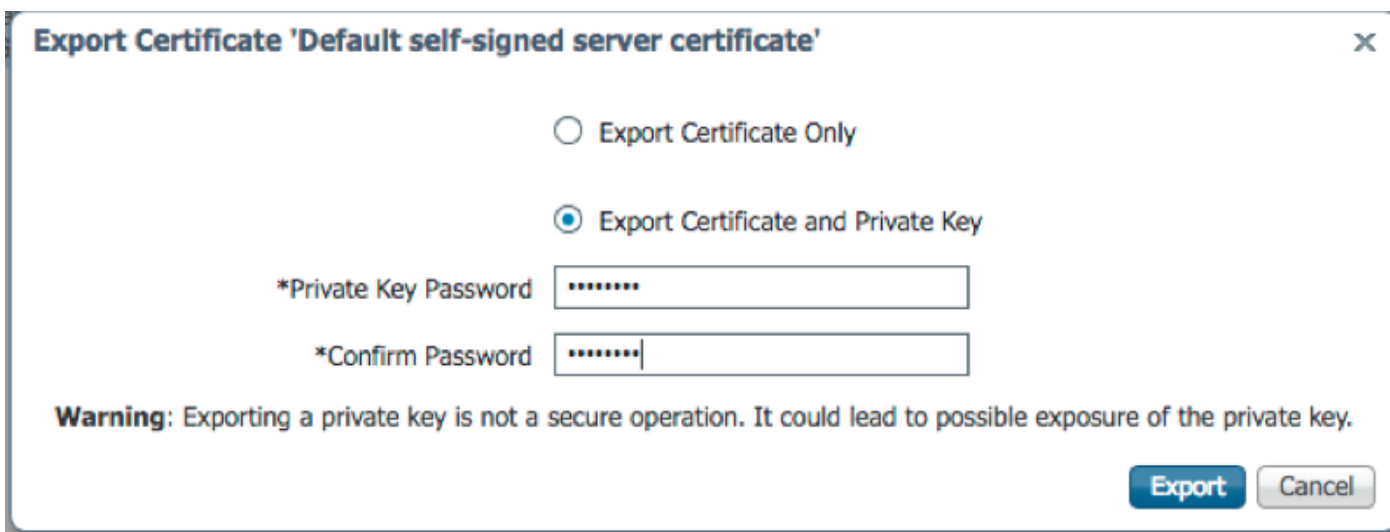
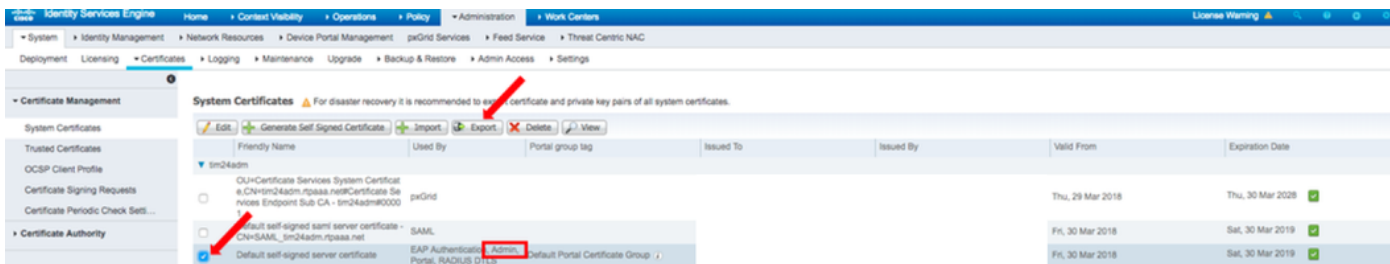
Opmerking: deze handleiding maakt gebruik van het standaard ISE-zelfondertekende certificaat voor gebruik van Admin. Als u een certificaat gebruikt dat is ondertekend door een certificeringsinstantie (CA), exporteert u de root-CA die het beheercertificaat heeft ondertekend naar de ISE MNT-knooppunt.

4. Klik op **Exporteren**.

5. Kies de optie om Certificaat en Private Key te exporteren.

6. Stel een coderingsleutel in.

7. Het bestand exporteren en opslaan zoals in de afbeelding.

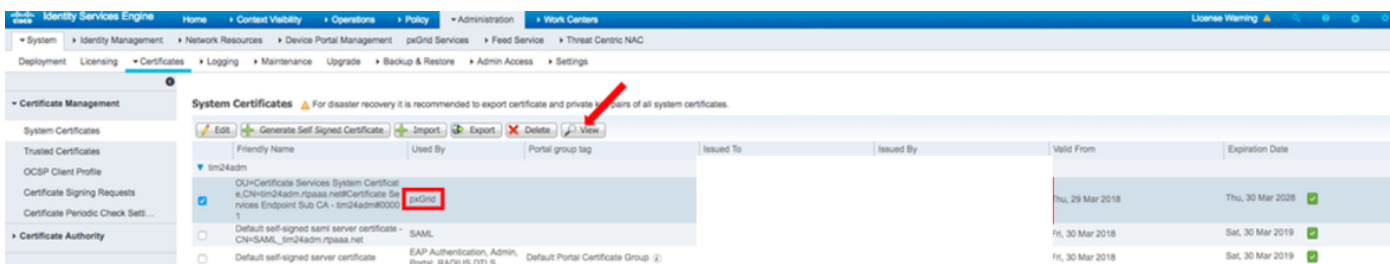


9. Ga terug naar het scherm ISE-systeemcertificaten.

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.



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 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. Breid het menu van de ISE-certificeringsinstantie uit.

15. Selecteer **certificaten van de certificeringsinstantie**.

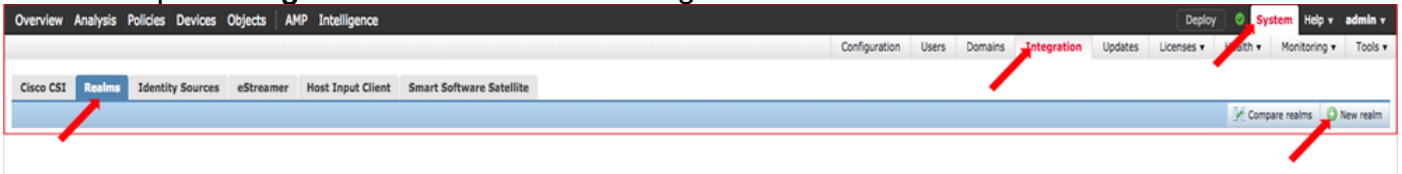
16. Selecteer het basiscertificaat dat is geïdentificeerd en klik op **Exporteren**. Sla vervolgens het CA-certificaat van de PxGrid Root op zoals in de afbeelding.

Friendy Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiration Status
tim24adm								
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	✓
Certificate Services Root CA - tim24adm00001	Enabled	Infrastructure.Endpoints	36 67 74 15 A6 A8 4F EB B7 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	✓
Certificate Services Node CA - tim24adm00002	Enabled	Infrastructure.Endpoints	30 1A 22 E7 AA E5 45 35 8C 65 78 EE 03 09 34 3E	Certificate Services Node CA - tim24adm	Certificate Services Root CA - tim24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2028	✓
Certificate Services OCSP Responder - tim24adm00004	Enabled	Infrastructure.Endpoints	74 C2 35 B8 32 6A 40 DF 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.



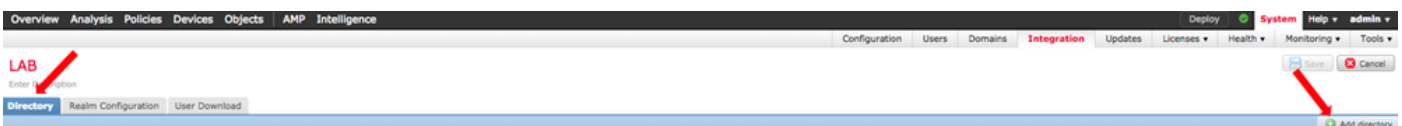
3. Vul het formulier in en klik op de knop Active Directory (AD) testen.

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**.

A screenshot of the 'Add New Realm' dialog box. The fields are filled with the following values: Name: ISEpxGrid; Description: Realm for use with pxGrid; Type: AD; AD Primary Domain: (empty); AD Join Username: (empty); AD Join Password: (masked with dots); Directory Username: admin; Directory Password: (masked with dots); Base DN: CN=Users, DN=rtpaaa, DN=net; Group DN: DN=rtpaaa, DN=net; Group Attribute: Member. A 'Test AD Join' button is visible. At the bottom, there are 'OK' and 'Cancel' buttons. A legend at the bottom left indicates that fields with an asterisk are required.

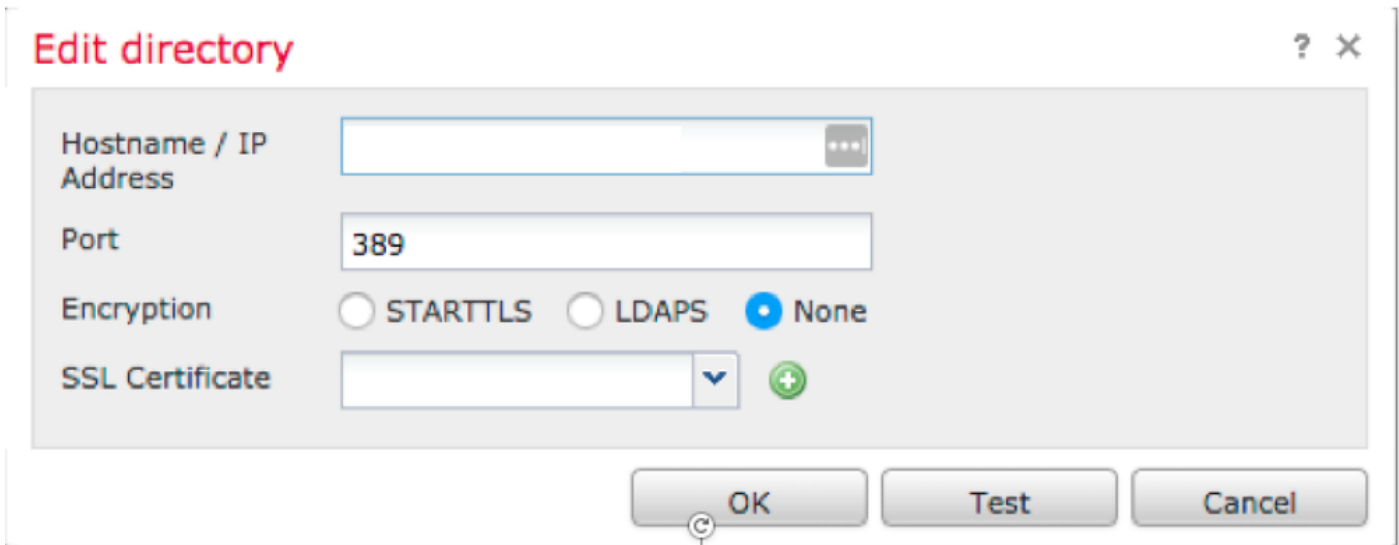
5. Klik op het tabblad **Directory** en klik vervolgens op **Map toevoegen** zoals in de afbeelding.



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**.



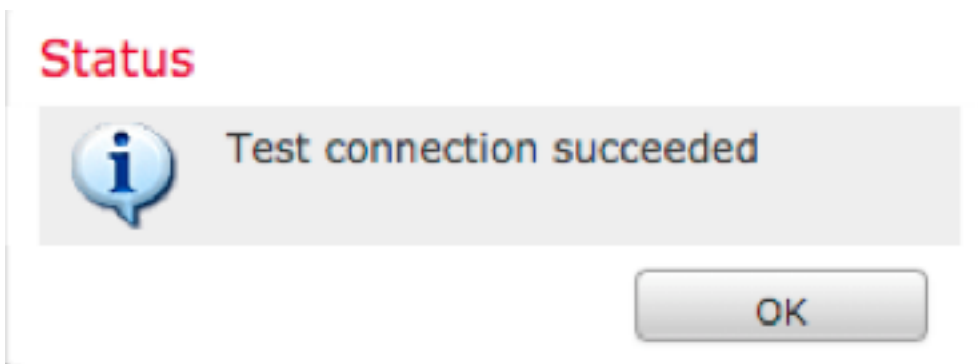
Edit directory ? X

Hostname / IP Address


Port

Encryption STARTTLS LDAPS None

SSL Certificate



Status

 Test connection succeeded

8. Klik op het tabblad **Gebruikersdownload**.



9. Indien nog niet geselecteerd, gebruiker en groep downloaden inschakelen

10. Klik op Nu downloaden

Enter Description

Directory

Realm Configuration

User Download

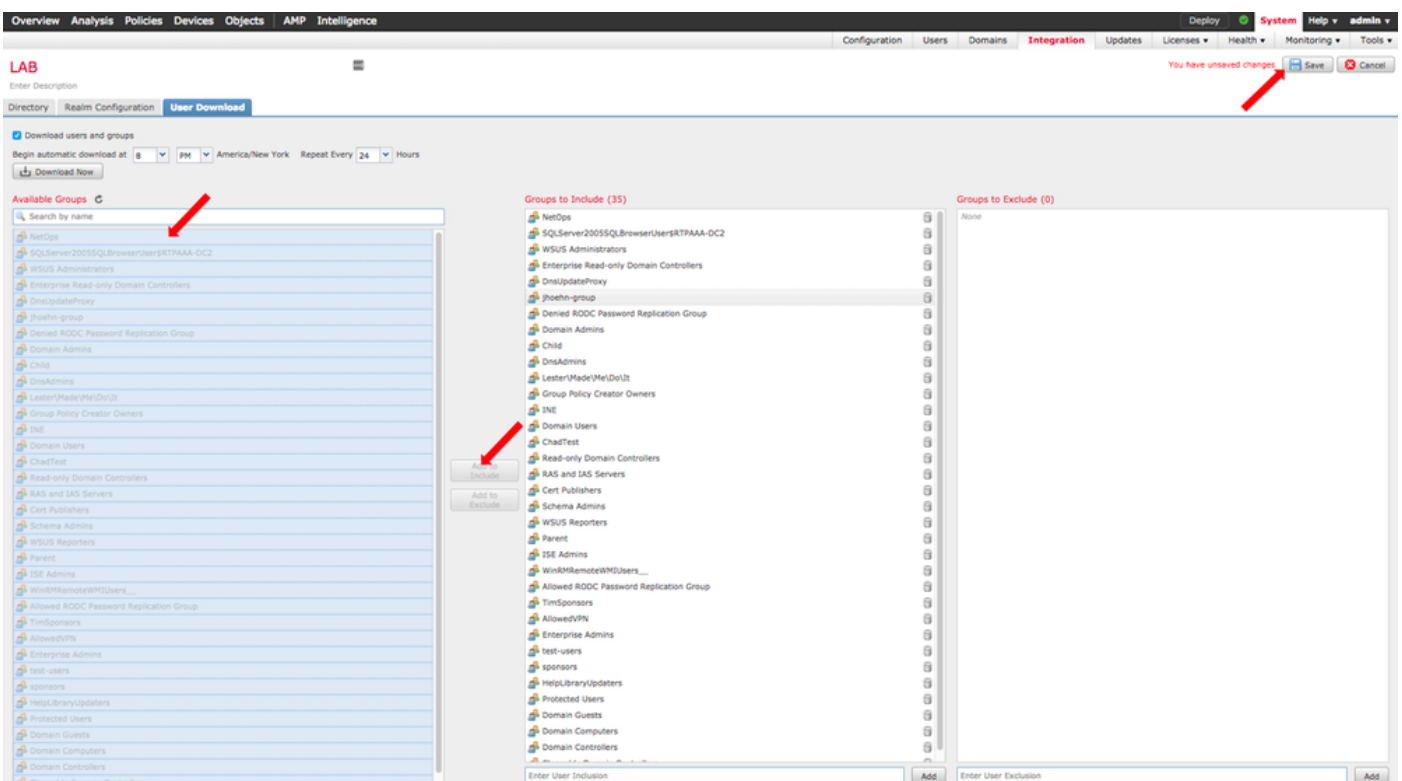
 Download users and groups

Begin automatic download at 8 PM America/New York Repeat Every 24 Hours



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

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 8 PM America/New York Repeat Every 24 Hours



Available Groups

Search by name

NetOps
SQLServer2005SQLBrowserUsersRTPAAA-DC2
WSUS Administrators
Enterprise Read-only Domain Controllers
DnsUpdateProxy
joheln-group
Denied RODC Password Replication Group
Domain Admins
Child
Child
DnsAdmins
Lester/Mede/Her/Dir3
Group Policy Creator Owners
INE
Domain Users
ChadTest
ChadTest
Read-only Domain Controllers
RAS and IAS Servers
Cert Publishers
Schema Admins
WSUS Reporters
Parent
ISE Admins
WinRMRemoteWMIUsers_
Allowed RODC Password Replication Group
TimSponsors
AllowedVPN
Enterprise Admins
test-users
sponsors
HelpLibraryUpdaters
Protected Users
Domain Guests
Domain Computers
Domain Controllers

Groups to Include (35)

NetOps
SQLServer2005SQLBrowserUsersRTPAAA-DC2
WSUS Administrators
Enterprise Read-only Domain Controllers
DnsUpdateProxy
joheln-group
Denied RODC Password Replication Group
Domain Admins
Child
Child
DnsAdmins
Lester/Mede/Her/Dir3
Group Policy Creator Owners
INE
Domain Users
ChadTest
Read-only Domain Controllers
RAS and IAS Servers
Cert Publishers
Schema Admins
WSUS Reporters
Parent
ISE Admins
WinRMRemoteWMIUsers_
Allowed RODC Password Replication Group
TimSponsors
AllowedVPN
Enterprise Admins
test-users
sponsors
HelpLibraryUpdaters
Protected Users
Domain Guests
Domain Computers
Domain Controllers

Groups to Exclude (0)


None

Enter User Inclusion Add

Enter User Exclusion Add

You have unsaved changes Save Cancel

13. Schakel de Real State in.



Overview Analysis Policies Devices Objects AMP Intelligence

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

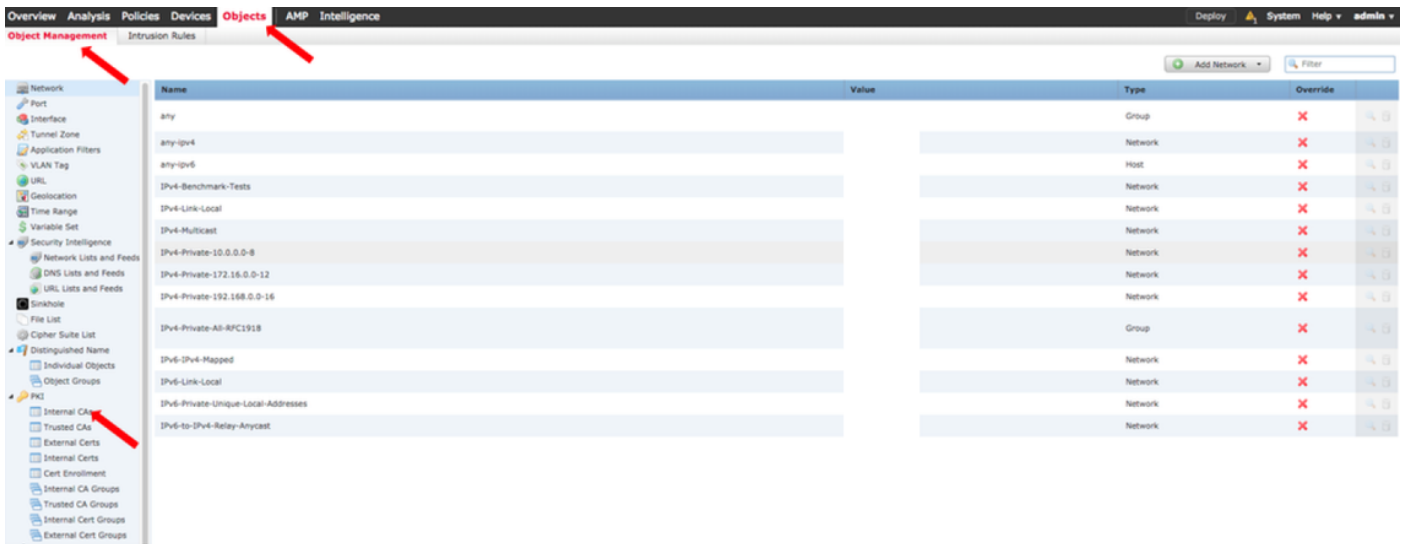
Cisco CSI Realms Identity Sources eStreamer Host Input Client Smart Software Satellite

Compare realms New realm

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"/>

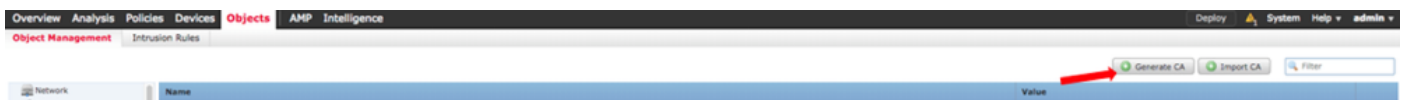
Stap 5. VCC CA-certificaat genereren

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



2. Klik op **Generate CA**.

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



Generate Internal Certificate Authority

Name:

Country Name (two-letter code):

State or Province:

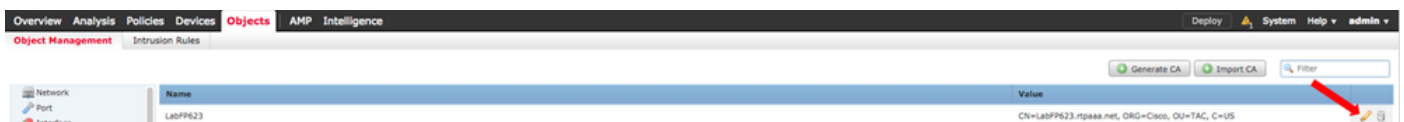
Locality or City:

Organization:

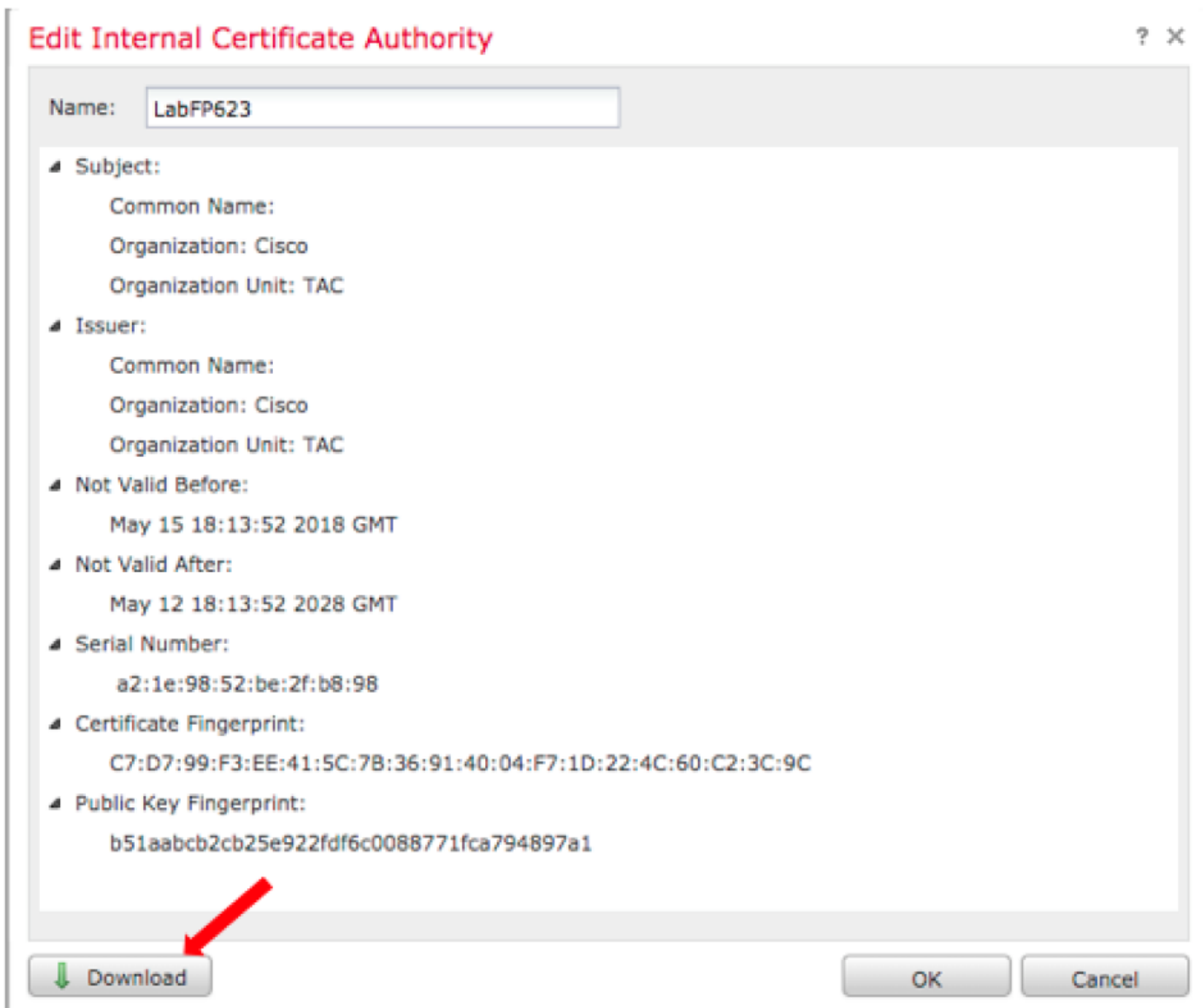
Organizational Unit (Department):

Common Name:

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



5. Klik op **Downloaden**.



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 cert-generatie op FMC.

```
~$ 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. 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>
```

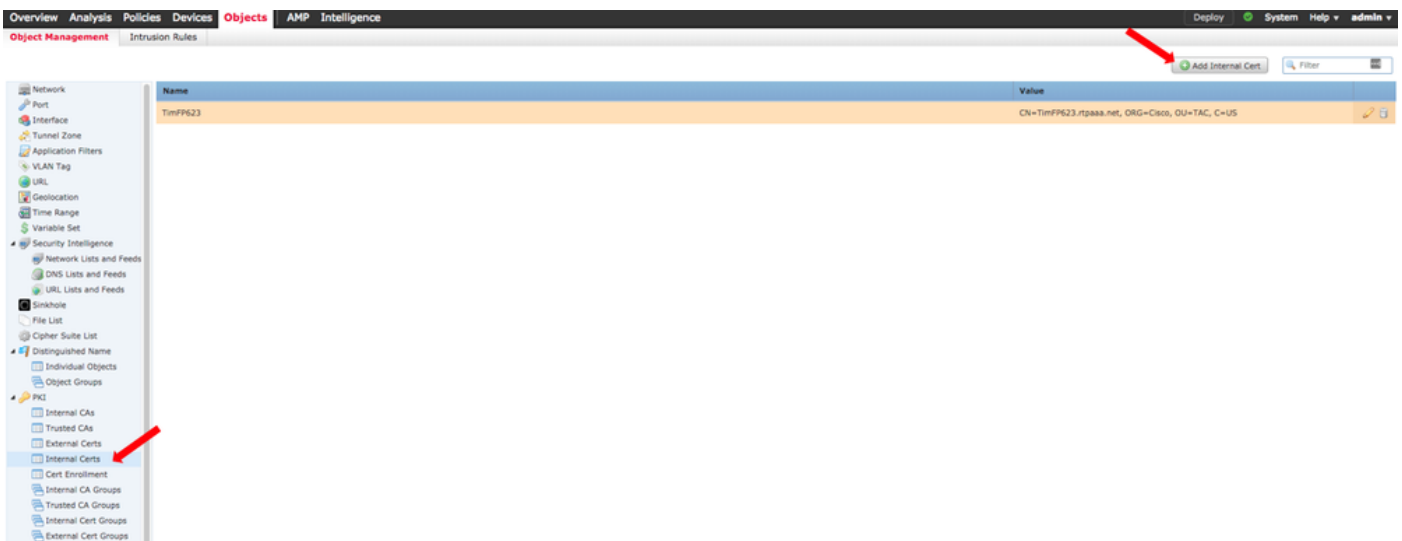
Password: Last login: Tue May 15 18:46:41 UTC 2018 Enter Import Password: MAC verified OK

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.



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 koppelttekens 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:

Certificate Data or, choose a file:

```
-----BEGIN CERTIFICATE-----
MIIDFTCCAmWgAwIBAgIJAKIemFK+L7iYMA0GCSqGSIb3DQEBCwUAMGQxCzAJBgNV
BAYTAIVTMQswCQYDVQQIDAJOQzEMMAoGA1UEBwwDUIRQM4wDAYDVQQKDAVDAxNj
bzEMMAoGA1UECwwDVEFDMRwwGgYDVQQDDDBNMYWJGUDYyMy5ydHBhYWEubmV0MB4X
DTE4MDUxNTE4MTM1MloXDTI4MDUxMjE4MTM1MlowZDELMAkGA1UEBhMCVVMxZzAJ
BgNVBAGMAK5DMQwwCgYDVQQHDANSVFAXDjAMBgNVBAoMBUNpc2NvMQwwCgYDVQQQL
DANUQUxHDAaBgNVBAMME0xhYkZQNjIzLnJ0cGFhYS5uZXQwgwEIMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQMjtS5IUIFIZkZK/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:

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**.

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 0B ...	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 A7 03 ...	VeriSign Class 3 Secure ...	VeriSign Class 3 Public ...	Sun, 7 Feb 2010	Fri, 7 Feb 2020	✓

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 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

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

pxGrid Server CA * +

MNT Server CA * +

FMC Server Certificate * +

ISE Network Filter

* Required Field

9. Klik op **Test**.

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

Status

ISE connection status:
Primary host: Success

Additional Logs

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 ISE-knooppunt 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).

Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log
		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
		Capabilities(4 Pub, 3 Sub)	Online (XMPP)	Internal	Certificate	View
		Capabilities(0 Pub, 6 Sub)	Online (XMPP)	Internal	Certificate	View
		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)	Internal	Certificate	View

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.

Capability Name	Capability Version	Messaging Role	Message Filter
AdaptiveNetworkControl	1.0	Sub	
Core	1.0	Sub	
EndpointProfileMetaData	1.0	Sub	
EndpointProtectionService	1.0	Sub	
SessionDirectory	1.0	Sub	
TrustSecMetaData	1.0	Sub	

Opmerking: vanwege Cisco-bug [IDCSCvo75376](#) 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.

Login Time	Last Seen	User	Authentication Type	Current IP	Realm	Username	First Name	Last Name	E-Mail	Department	Phone	Discoverx Application	Device
2018-05-15 13:26:21	2018-05-15 13:27:36	xiao yao (LAB\yao@lab.com)	Passive Authentication		LAB					users (doaaa)		LDAP	firepower
2018-05-15 12:35:54	2018-05-15 12:35:54	admin admin (LAB\admin@lab.com)	Passive Authentication		LAB					users (doaaa)		LDAP	firepower
2018-05-15 11:27:14	2018-05-15 11:27:14	tom (LAB\tom@lab.com)	Passive Authentication		LAB					users (doaaa)		LDAP	firepower
2018-05-15 11:20:30	2018-05-15 11:20:30	clark kent (LAB\javeerman@lab.com)	Passive Authentication		LAB					users (doaaa)		LDAP	firepower

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.