

Konfigurieren der Integration von ISE 2.4 und FMC 6.2.3 pxGrid

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren der ISE](#)

[Schritt 1: pxGrid-Services aktivieren](#)

[Schritt 2: Konfigurieren der ISE zur Genehmigung aller zertifikatbasierten pxGrid-Konten](#)

[Schritt 3: ISE MNT-Administratorzertifikat und pxGrid-Zertifizierungsstellenzertifikate exportieren](#)

[Konfigurieren von FMC](#)

[Schritt 4: Neuen Bereich zu FMC hinzufügen](#)

[Schritt 5: FMC CA-Zertifikat generieren](#)

[Schritt 6: Extrahieren Sie das Zertifikat und den privaten Schlüssel mithilfe von OpenSSL aus dem generierten Zertifikat.](#)

[Schritt 7. Zertifikat auf FMC installieren](#)

[Schritt 8: FMC-Zertifikat in ISE importieren](#)

[Schritt 9. Konfigurieren der pxGrid-Verbindung auf FMC](#)

[Überprüfung](#)

[Verifizierung in der ISE](#)

[Verifizierung in FMC](#)

[Fehlerbehebung](#)

Einleitung

Dieses Dokument beschreibt den Konfigurationsprozess für die Integration der ISE pxGrid Version 2.4 und FMC Version 6.2.3.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

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

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

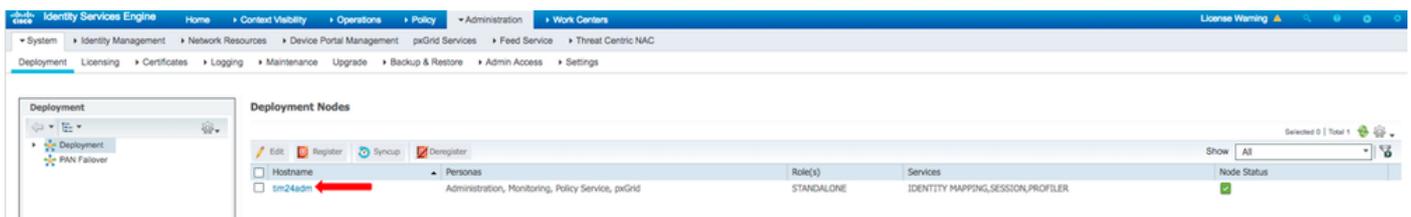
- Standalone ISE 2.4
- FMCv 6.2.3
- Active Directory 2012R2
- Identity Services Engine (ISE) pxGrid Version 2.4
- FirePOWER Management Center (FMC) Version 6.2.3

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Konfigurieren der ISE

Schritt 1: pxGrid-Services aktivieren

1. Melden Sie sich bei der ISE Admin-GUI an, und navigieren Sie zu **Administration > Deployment**.
2. Wählen Sie den ISE-Knoten für pxGrid persona aus.



3. Aktivieren Sie pxGrid Service und klicken Sie auf **Speichern**, wie im Bild angezeigt.

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 ⓘ

Include Node in Node Group: None ⓘ

Enable Profiling Service ⓘ

Enable Threat Centric NAC Service ⓘ

Enable SXP Service ⓘ

Enable Device Admin Service ⓘ

Enable Passive Identity Service ⓘ

pxGrid ⓘ

Save Reset

4. Überprüfen Sie, ob die pxGrid-Dienste über die CLI ausgeführt werden.

Hinweis: Der Vorgang dauert bis zu 5 Minuten, bis die pxGrid-Dienste vollständig gestartet sind und den HA-Status (High Availability) ermitteln, wenn mehr als ein pxGrid-Knoten verwendet wird.

5. SSH in die CLI des ISE-pxGrid-Knotens integrieren und den Anwendungsstatus überprüfen.

```
# 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. Zugreifen Sie auf die ISE-Admin-GUI, und überprüfen Sie, ob die Dienste online sind und funktionieren. Navigieren Sie zu **Administration > pxGrid Services**.

7. Unten auf der Seite zeigt ISE "Connected to pxGrid <pxGrid node FQDN>" an.

Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log
ise-rest-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-20752a2982d...		Capabilities(0 Pub, 6 Sub)	Online (DHPP)		Certificate	View
fresightstest-freepower-20752a...		Capabilities(0 Pub, 0 Sub)	Offline (DHPP)		Certificate	View

Schritt 2: Konfigurieren der ISE zur Genehmigung aller zertifikatbasierten pxGrid-Konten

1. Navigieren Sie zu **Administration > pxGrid Services > Settings**.
2. Aktivieren Sie das Kontrollkästchen "Neue zertifikatbasierte Konten automatisch genehmigen", und klicken Sie auf **Speichern**.

PxGrid Settings

Automatically approve new certificate-based accounts

Allow password based account creation

Use Default Save

Test

Connected to pxGrid tim24adm.rtpaaa.net

Hinweis: Der Administrator muss die FMC-Verbindung zur ISE manuell genehmigen, wenn diese Option nicht aktiviert ist.

Schritt 3: ISE MNT-Administratorzertifikat und pxGrid-Zertifizierungsstellenzertifikate exportieren

1. Navigieren Sie zu **Administration > Certificates > System Certificates**.
2. Erweitern Sie den Knoten Primary Monitoring (MNT) (Primäre Überwachung), wenn dieser Knoten nicht im Knoten Primary Administration (Primäre Verwaltung) aktiviert ist.
3. Wählen Sie das Zertifikat mit dem Feld Used-By "Admin".

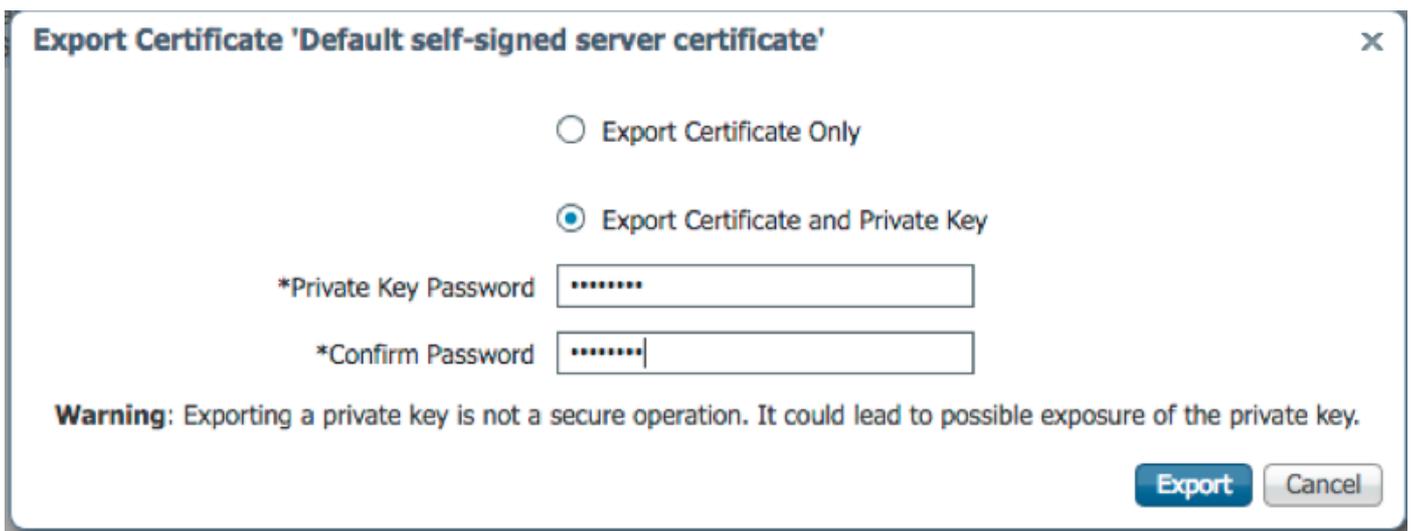
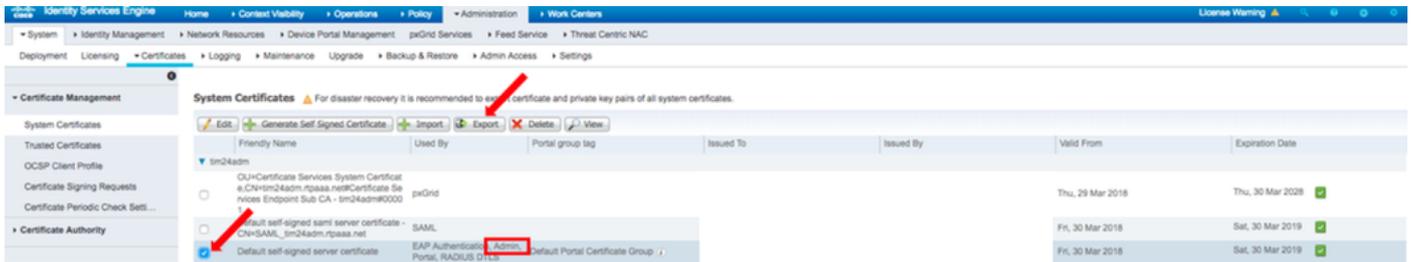
Hinweis: In diesem Leitfaden wird das ISE-Standardzertifikat mit Selbstsignatur für Administratoren verwendet. Wenn Sie ein von der Zertifizierungsstelle signiertes Administratorzertifikat verwenden, exportieren Sie die Stammzertifizierungsstelle, die das Administratorzertifikat auf dem ISE MNT-Knoten signiert hat.

4. Klicken Sie auf **Exportieren**.

5. Wählen Sie die Option zum Exportieren des Zertifikats und des privaten Schlüssels.

6. Legen Sie einen Verschlüsselungsschlüssel.

7. Exportieren und speichern Sie die Datei, wie im Bild dargestellt.

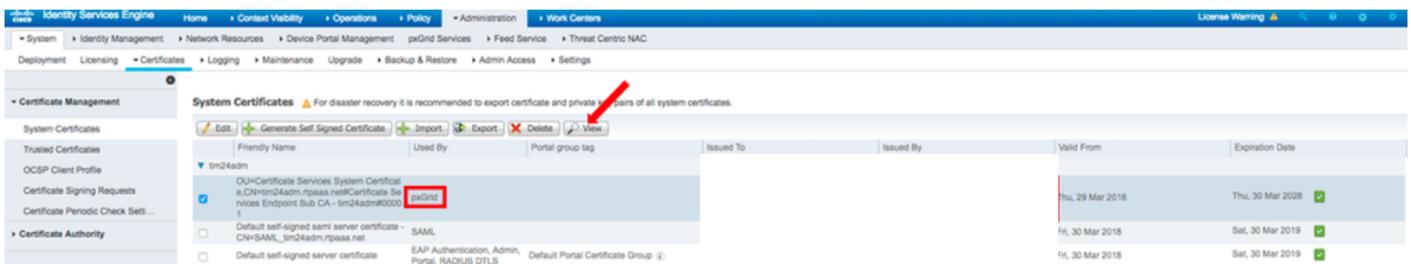


9. Kehren Sie zum Bildschirm ISE-Systemzertifikate zurück.

10. Bestimmen Sie das Feld Ausgestellt von im Zertifikat mit der Verwendung "pxGrid" in der Spalte "Verwendet von".

Hinweis: In älteren Versionen der ISE handelte es sich um ein selbstsigniertes Zertifikat. Ab Version 2.2 wird dieses Zertifikat jedoch standardmäßig von der internen ISE-Zertifizierungsstellenkette ausgestellt.

11. Wählen Sie das Zertifikat aus, und klicken Sie auf **Anzeigen**, wie im Bild dargestellt.



12. Bestimmen Sie das Zertifikat der obersten Ebene (Root). In diesem Fall ist dies "Certificate Services Root CA - tim24adm".

13. Schließen Sie das Fenster Zertifikatsansicht wie im Bild dargestellt.

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)

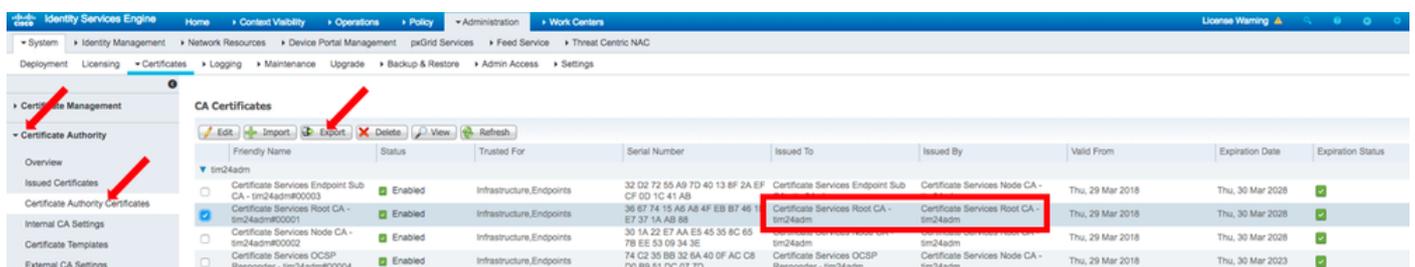
Serial Number **58:2A:91:45:E8:23:42:74:98:53:06:94:33:9E:AD:83**

Close

14. Erweitern Sie das Menü der ISE-Zertifizierungsstelle.

15. Wählen Sie **Zertifikate der Zertifizierungsstelle** aus.

16. Wählen Sie das identifizierte Stammzertifikat aus, und klicken Sie auf **Exportieren**. Speichern Sie dann das Zertifikat der pxGrid-Stammzertifizierungsstelle, wie im Bild dargestellt.



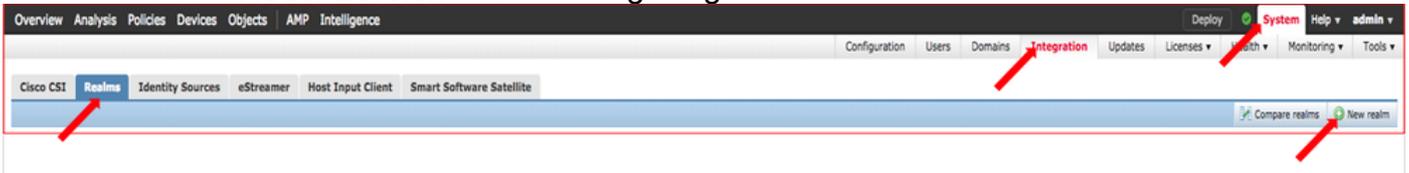
The screenshot shows the 'CA Certificates' management page in the Identity Services Engine. The left sidebar has 'Certificate Management' expanded, with 'Certificate Authority' and 'Certificates' selected. The main area shows a table of certificates. The 'Certificate Services Root CA - tim24adm' entry is selected, and its details are shown in a red box. The 'Export' button is also highlighted with a red arrow.

Friendly 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 E7 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 E5 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	✓

Konfigurieren von FMC

Schritt 4: Neuen Bereich zu FMC hinzufügen

1. Rufen Sie die FMC-GUI auf, und navigieren Sie zu **System > Integration > Realms**.
2. Klicke auf "Neuer Bereich" wie im Bild gezeigt.



3. Füllen Sie das Formular aus und klicken Sie auf die Schaltfläche Active Directory (AD)-Join testen.

Hinweis: Der AD-Join-Benutzername muss das Format des Benutzerprinzipalnamens (UPN) aufweisen, da der Test andernfalls fehlschlägt.

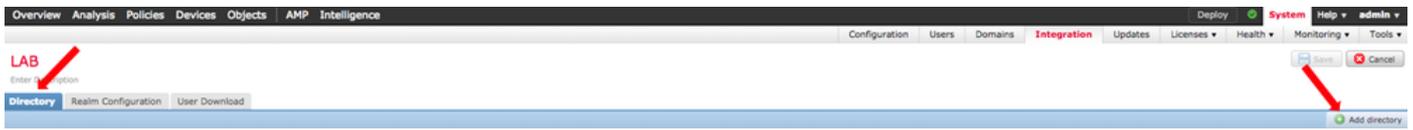
4. Wenn der Test AD Join erfolgreich war, klicken Sie auf **OK**.

A screenshot of the 'Add New Realm' form in the FMC GUI. The form contains the following fields and 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

There are example values for several fields: ex: domain.com, ex: user@domain, ex: user@domain, ex: ou=user,dc=cisco,dc=com, ex: ou=group,dc=cisco,dc=com. A 'Test AD Join' button is visible next to the AD Join Username field. At the bottom, there are 'OK' and 'Cancel' buttons. A legend indicates that a red asterisk (*) denotes a required field.

5. Klicken Sie auf die Registerkarte **Verzeichnis** und dann auf **Verzeichnis hinzufügen**, wie im Bild dargestellt.



6. Konfigurieren Sie IP/Hostname und Testverbindung.

Hinweis: Wenn der Test fehlschlägt, überprüfen Sie die Anmeldeinformationen auf der Registerkarte Realm Configuration (Bereichskonfiguration).

7. Klicken Sie auf OK.



8. Klicken Sie auf die Registerkarte **Benutzerdownload**.



9. Falls noch nicht ausgewählt, Benutzer- und Gruppdownload aktivieren

10. Klicken Sie auf Jetzt herunterladen

Enter Description

Directory

Realm Configuration

User Download

 Download users and groups

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

Download Now

11. Fügen Sie nach dem Ausfüllen der Liste die gewünschten Gruppen hinzu, und wählen Sie **Zu Einschließen hinzufügen** aus.

12. Speichern Sie die **Bereichskonfiguration**.

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

Download Now

Available Groups

Search by name

Groups to Include (35)

Groups to Exclude (0)

Save Cancel

You have unsaved changes

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/Mel/Del/It
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

Enter User Inclusion Add

Enter User Exclusion Add

13. Aktivieren Sie den Realm-Status.

Overview Analysis Policies Devices Objects AMP Intelligence

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

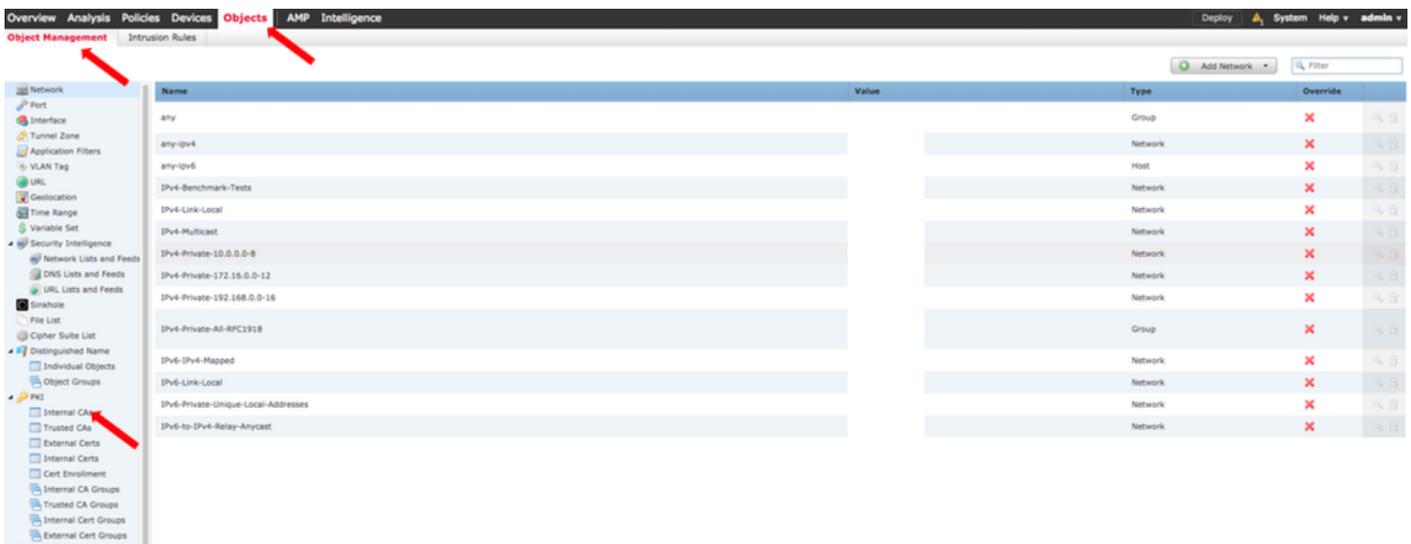
Cisco CSI Realms Identity Sources eStreamer Host Input Client Smart Software Satellite

Name	Description	Domain	Type	Base DN	Group DN	Group Attribute	Status
LAB		Global	AD	DC=rt2aaa,DC=net	CN=Users,DC=rt2aaa,DC=	member	On

Compare realms New realm

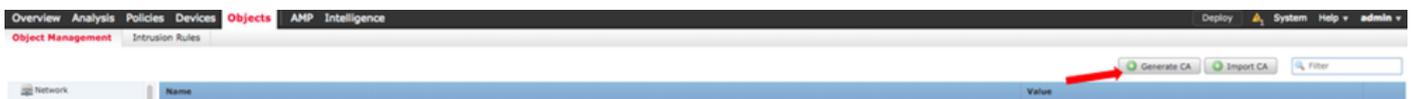
Schritt 5: FMC CA-Zertifikat generieren

1. Navigieren Sie zu **Objekte > Objektverwaltung > Interne Zertifizierungsstellen**, wie im Bild dargestellt.



2. Klicken Sie auf **Zertifizierungsstelle erstellen**.

3. Füllen Sie das Formular aus und klicken Sie auf **Selbstsignierte Zertifizierungsstelle erstellen**.



Generate Internal Certificate Authority ? X

Name:

Country Name (two-letter code):

State or Province:

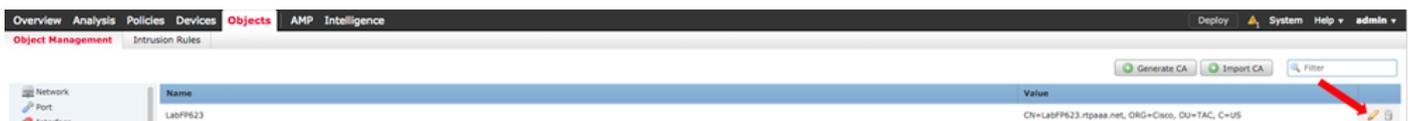
Locality or City:

Organization:

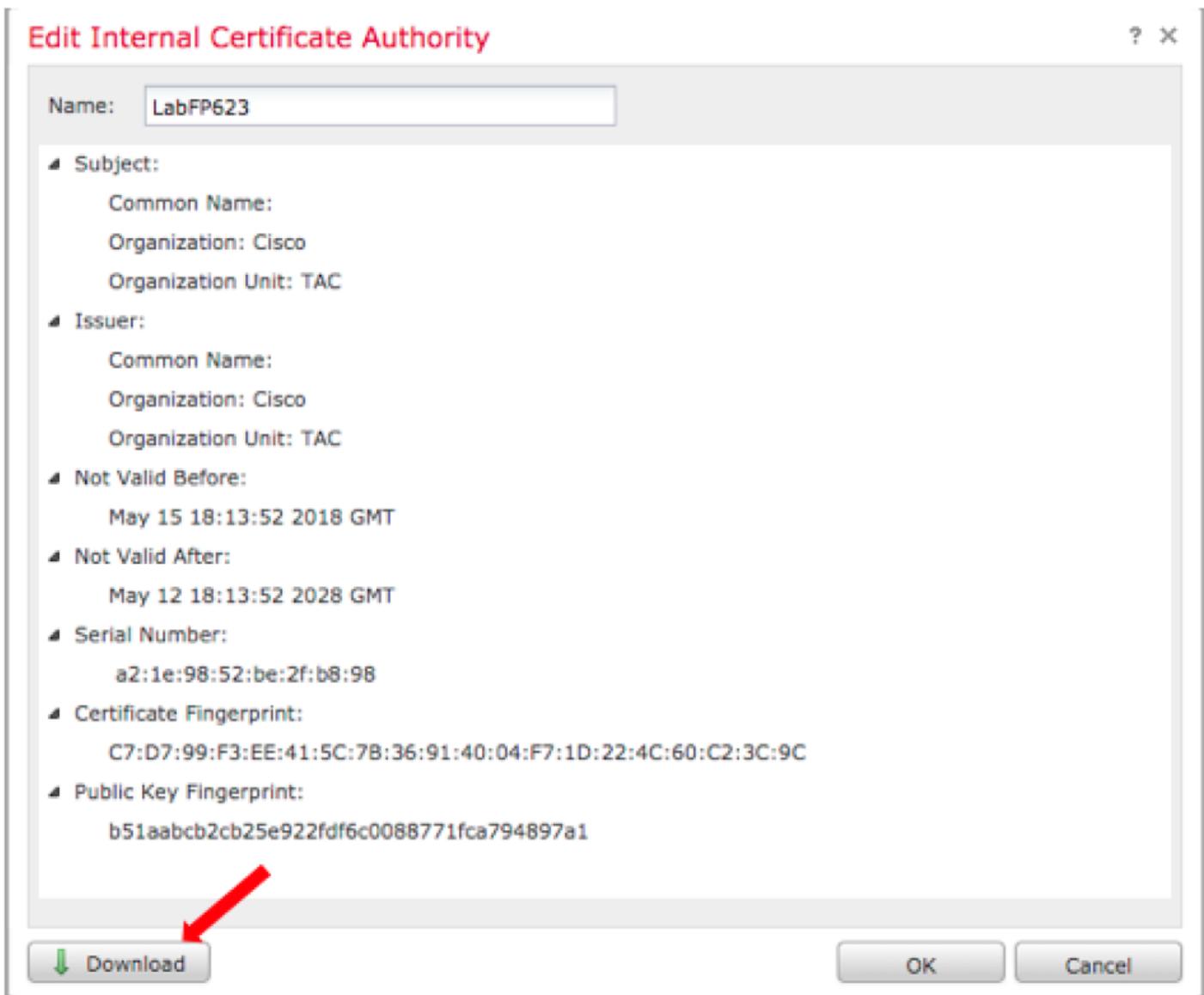
Organizational Unit (Department):

Common Name:

4. Klicken Sie nach Abschluss der Generierung auf den Bleistift rechts neben dem generierten CA-Zertifikat, wie im Bild gezeigt.



5. Klicken Sie auf **Herunterladen**.



6. Konfigurieren und bestätigen Sie das Verschlüsselungskennwort, und klicken Sie auf **OK**.

7. Speichern Sie die Datei Public-Key Cryptography Standards (PKCS) p12 auf Ihrem lokalen Dateisystem.

Schritt 6: Extrahieren Sie das Zertifikat und den privaten Schlüssel mithilfe von OpenSSL aus dem generierten Zertifikat.

Dies erfolgt entweder auf dem Root des FMC oder auf jedem Client, der OpenSSL-Befehle ausführen kann. In diesem Beispiel wird eine Standard-Linux-Shell verwendet.

1. Verwenden Sie **openssl**, um das Zertifikat (CER) und den privaten Schlüssel (PVK) aus der p12-Datei zu extrahieren.

2. Extrahieren Sie die CER-Datei, und konfigurieren Sie dann den Zertifikatexportschlüssel von der Zertifikatgenerierung auf 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. Extrahieren Sie die PVK-Datei, konfigurieren Sie den Zertifikatexportschlüssel, legen Sie dann einen neuen PEM-Kennsatz fest, und bestätigen Sie ihn.

```
~$ openssl pkcs12 -nocerts -in <filename.p12> -out <filename.pvk>
```

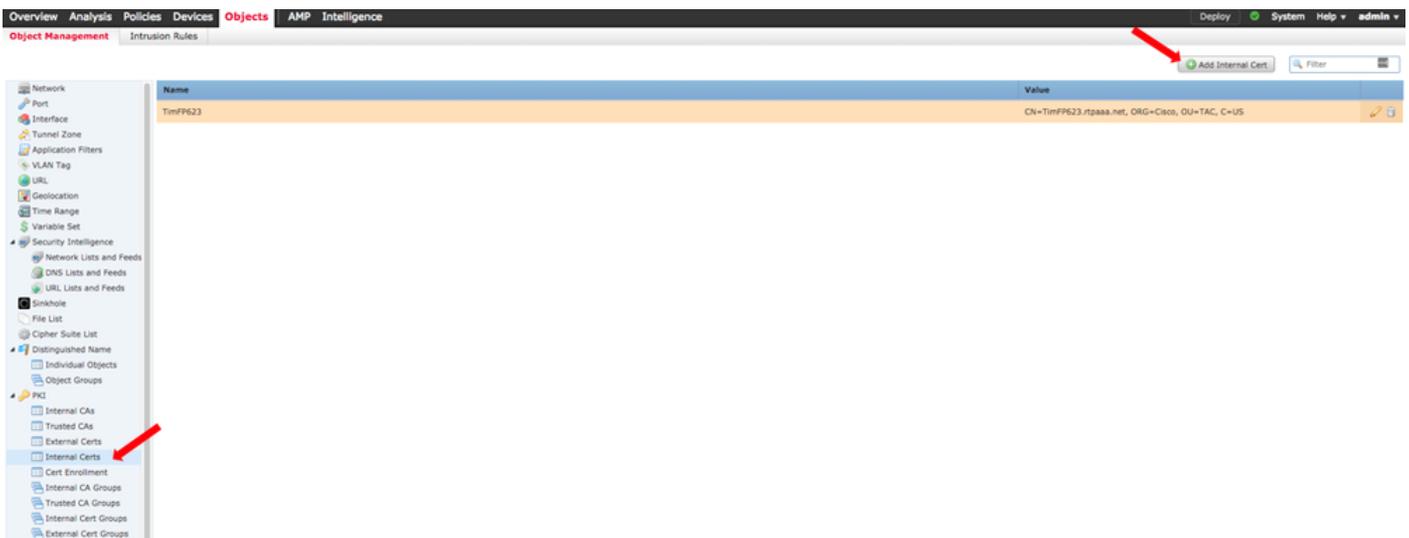
Password: Last login: Tue May 15 18:46:41 UTC 2018 Enter Import Password: MAC verified OK

4. Diese PEM-Phrase wird im nächsten Schritt benötigt.

Schritt 7. Zertifikat auf FMC installieren

1. Navigieren Sie zu **Objekte > Objektverwaltung > PKI > Interne Zertifikate**.

2. Klicken Sie auf **Internes Zertifikat hinzufügen**, wie im Bild dargestellt.



3. Konfigurieren Sie einen Namen für das interne Zertifikat.

4. Navigieren Sie zum Speicherort der CER-Datei, und wählen Sie sie aus. Wählen Sie nach dem Ausfüllen der Zertifikatsdaten die zweite Option aus.

5. Durchsuchen Sie **Option** und wählen Sie die PVK-Datei.

6. Löschen Sie alle führenden "Bag-Attribute" und alle nachfolgenden Werte im Abschnitt PVK. Das PVK beginnt mit -----BEGIN ENCRYPTED PRIVATE KEY und endet mit -----END ENCRYPTED PRIVATE KEY.

Hinweis: Sie können nicht auf **OK** klicken, wenn der PVK-Text Zeichen außerhalb der vor- und nachgestellten Bindestriche enthält.

7. Aktivieren Sie das Kontrollkästchen **Encrypted (Verschlüsselt)**, und konfigurieren Sie das Kennwort, das beim Exportieren des PVK in Schritt 6 erstellt wurde.

8. Klicken Sie auf **OK**.

Add Known Internal Certificate



Name:

Certificate Data or, choose a file:

```
-----BEGIN CERTIFICATE-----
MIIDFTCCAmWgAwIBAgIJAKIemFK+L7iYMA0GCSqGSIb3DQEBCwUAMGQxCzAJBgNV
BAYTAIVTMQswCQYDVQQIDAJOQzEMMAoGA1UEBwwDUIRQM4wDAYDVQQKDAVDAxNj
bzEMMAoGA1UECwwDVEFDMRwwGgYDVQQDDDBNMYWJGUDYyMy5ydHBhYWEubmV0MB4X
DTE4MDUxNTE4MTM1MloXDTI4MDUxMjE4MTM1MlowZDELMAkGA1UEBhMCVVMxZAJ
BgNVBAGMAK5DMQwwCgYDVQQHDANSVFAXDjAMBgNVBAoMBUNpc2NvMQwwCgYDVQQQL
DANUQUxHDAaBgNVBAMME0xhYkZQNjIzLnJ0cGFhYS5uZXQwgwEIMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQMjtS5IUIFIZkZK/TSGtkOCmuivTK5kk1WzAy6
D7Gm/c69cXw/VfIPWnSBzhEkiRTyspmTMdyf/4TJvUmUH60h1O8/8dZeqJOzbjon
-----
```

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="">

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABGkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQI5uV3MsiHZsICAggA
MBQGCCqGSIb3DQMHBABGVM1+xHLIASCBMjjJxkffXUNUcdB22smybvWotwbcRrt
xL0qjEStmwuyExVp+TWC3AyIJN1DE7/rRssjRAqsnSOxIvDGmg0dVsvnbqZwjFP
74POu/O2Vy99iFoVgW2q9DyXyL/h64TH9CZtwLKIOGOeEunNKpamDnpfyN8QC4DC
fXvNZ8jNG4HrEcFmnnij0EwJ0QT8Jn5gAUj+AIPMe32zPqwocCRNYrRXMVM9+Jwp
-----
```

Encrypted, and the password is:

```
cfCJU2QGI4jT0SorN4u2Lk+S+Qd1s7Ii2wIQMWKPI2R9UGv1tyM6HTPCGoCo6VDI
acCICUasecVrYY081GKTVVJ3bWgWfPtR3OH12YCA2whcCKcG50MByB4tjhHN036q
O/g=
-----END ENCRYPTED PRIVATE KEY-----
</no> ← DELETE
```

Encrypted, and the password is:

Schritt 8: FMC-Zertifikat in ISE importieren

1. Öffnen Sie die ISE-GUI, und navigieren Sie zu **Administration > System > Certificates > Trusted Certificates**.

2. Klicken Sie auf **Importieren**.

Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiration Status
Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 89	Baltimore CyberTrust Ro...	Baltimore CyberTrust Ro...	Fri, 12 May 2000	Mon, 12 May 2025	✓
Cisco CA Manufacturing	Disabled	Endpoints Infrastructure	6A 69 67 83 00 00	Cisco Manufacturing CA	Cisco Root CA 2048	Fri, 10 Jun 2005	Mon, 14 May 2029	✓
Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure	02	Cisco Manufacturing CA...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037	✓
Cisco Root CA 2048	Disabled	Endpoints Infrastructure	5F FB 78 28 28 54	Cisco Root CA 2048	Cisco Root CA 2048	Fri, 14 May 2004	Mon, 14 May 2029	✓
Cisco Root CA M2	Enabled	Endpoints Infrastructure	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037	✓
Default self-signed server certificate	Enabled	Endpoints Infrastructure	5A BE 7E D8 00 00...	tm24adm.rtpaaa.net	tm24adm.rtpaaa.net	Fri, 30 Mar 2018	Sat, 30 Mar 2019	✓
DigiCert root CA	Enabled	Endpoints Infrastructure	02 AC 5C 26 6A 08...	DigiCert High Assurance...	DigiCert High Assurance...	Thu, 9 Nov 2006	Sun, 9 Nov 2031	✓
DigiCert SHA2 High Assurance Server CA	Enabled	Endpoints Infrastructure	04 E1 E7 A4 DC 5C...	DigiCert SHA2 High Ass...	DigiCert High Assurance	Tue, 22 Oct 2013	Sun, 22 Oct 2028	✓
DST Root CA X3 Certificate Authority	Enabled	Cisco Services	44 AF B0 80 D6 A3...	DST Root CA X3	DST Root CA X3	Sat, 30 Sep 2000	Thu, 30 Sep 2021	✓
HydrantID SSL ICA G2	Enabled	Cisco Services	75 17 16 77 83 00...	HydrantID SSL ICA G2	QuoVadis Root CA 2	Tue, 17 Dec 2013	Sun, 17 Dec 2023	✓
QuoVadis Root CA 2	Enabled	Cisco Services	05 09	QuoVadis Root CA 2	QuoVadis Root CA 2	Fri, 24 Nov 2006	Mon, 24 Nov 2031	✓
Thawte Primary Root CA	Enabled	Cisco Services	34 4E D5 57 20 D5...	thawte Primary Root CA	thawte Primary Root CA	Thu, 16 Nov 2006	Wed, 16 Jul 2036	✓
TimFP623	Enabled	Endpoints Infrastructure	8E F9 42 3D 25 A5...	TimFP623.rtpaaa.net	TimFP623.rtpaaa.net	Tue, 15 May 2018	Fri, 12 May 2028	✓
VeriSign Class 3 Public Primary Certification Authority	Enabled	Cisco Services	18 DA D1 9E 26 7D...	VeriSign Class 3 Public ...	VeriSign Class 3 Public ...	Tue, 7 Nov 2006	Wed, 16 Jul 2036	✓
VeriSign Class 3 Secure Server CA - G3	Enabled	Cisco Services	6E CC 7A A5 A7 03...	VeriSign Class 3 Secure ...	VeriSign Class 3 Public ...	Sun, 7 Feb 2010	Fri, 7 Feb 2020	✓

3. Klicken Sie auf **Choose File (Datei auswählen)**, und wählen Sie die FMC CER-Datei von Ihrem lokalen System aus.

Optional: Konfigurieren Sie einen Anzeigenamen.

4. Aktivieren Sie **Vertrauenswürdig** für die Authentifizierung in der ISE.

Optional: Konfigurieren Sie eine Beschreibung.

5. Klicken Sie auf **Senden**, wie in der Abbildung dargestellt.

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

Schritt 9. Konfigurieren der pxGrid-Verbindung auf FMC

1. Navigieren Sie zu **System > Integration > Identity Sources (System > Integration > Identitätsquellen)**, wie im Bild dargestellt.



2. Klicken Sie auf **ISE**.

3. Konfigurieren Sie die IP-Adresse oder den Hostnamen des ISE pxGrid-Knotens.

4. Wählen Sie das + rechts neben pxGrid Server CA.

5. Benennen Sie die Server-CA-Datei, und navigieren Sie zur pxGrid-Stammsignaturzertifizierungsstelle, die in Schritt 3 erfasst wurde, und klicken Sie auf **Speichern**.

6. Wählen Sie das + rechts neben der MNT Server-CA.

7. Benennen Sie die Server-CA-Datei, und navigieren Sie zu dem in Schritt 3 erfassten Admin-Zertifikat, und klicken Sie auf **Speichern**.

8. Wählen Sie die Datei **FMC CER** aus der Dropdown-Liste.

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 ex. 10.89.31.0/24, 192.168.8.0/24, ...

* Required Field

9. Klicken Sie auf **Test**.

10. Wenn der Test erfolgreich ist, klicken Sie auf **OK**, dann oben rechts auf dem Bildschirm **Speichern**.

Status

i ISE connection status:
Primary host: Success

[Additional Logs](#)

Hinweis: Wenn Sie zwei ISE pxGrid-Knoten ausführen, ist es normal, dass ein Host Erfolgreich und einer Fehler zeigt, da pxGrid nur auf jeweils einem ISE-Knoten aktiv ausgeführt wird. Es hängt von der Konfiguration ab, ob auf dem primären Host Fehler und auf dem sekundären Host Erfolg angezeigt wird. Dies hängt davon ab, welcher Knoten in der ISE der aktive pxGrid-Knoten ist.

Überprüfung

Verifizierung in der ISE

1. Öffnen Sie die ISE-GUI, und navigieren Sie zu **Administration > pxGrid Services**.

Bei Erfolg werden in der Client-Liste zwei Verbindungen mit Firepower aufgelistet. Eine für das tatsächliche FMC (iseagent-hostname-33bytes) und eine für das Testgerät (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, 2 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

Die Verbindung iseagent-firepower zeigt sechs (6) Subs an und wird online angezeigt.

Die Verbindung firesightisetest-firepower zeigt null (0) U-Boote an und ist offline.

In der erweiterten Ansicht des iseagent-firepower-Clients werden die sechs Abonnements angezeigt.

Capability Name	Capability Version	Messaging Role	Message Filter
<input type="radio"/> AdaptiveNetworkControl	1.0	Sub	
<input type="radio"/> Core	1.0	Sub	
<input type="radio"/> EndpointProfileMetaData	1.0	Sub	
<input type="radio"/> EndpointProtectionService	1.0	Sub	
<input type="radio"/> SessionDirectory	1.0	Sub	
<input type="radio"/> TrustSecMetaData	1.0	Sub	

Hinweis: Aufgrund des Cisco-Fehlers [IDCSCvo75376](#) gibt es eine Hostnamensbeschränkung, und der Bulk-Download schlägt fehl. Die Testtaste am FMC zeigt einen Verbindungsfehler an. Dies betrifft 2.3p6, 2.4p6 und 2.6. Es wird empfohlen, 2.3 Patch 5 oder 2.4 Patch 5 so lange auszuführen, bis ein offizieller Patch veröffentlicht wird.

Verifizierung in FMC

1. Öffnen Sie die FMC-GUI, und navigieren Sie zu **Analyse > Benutzer > Aktive Sitzungen**.

Alle über die Sitzungsverzeichnisfunktion in der ISE veröffentlichten aktiven Sitzungen werden in der Tabelle "Aktive Sitzungen" des FMC angezeigt.

Login Time	Last Seen	User	Authentication Type	Current IP	Realm	Username	First Name	Last Name	E-Mail	Department	Phone	Discovery 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\javoerman@lab.com)	Passive Authentication		LAB					users (doaaa)		LDAP	firepower

Im FMC CLI-Sudo-Modus zeigt die **adi_cli-Sitzung** die Informationen der Benutzersitzung an, die von der ISE an das FMC gesendet wurden.

```
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.
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.