Konfigurieren der Integration von ISE 2.4 und FMC 6.2.3 pxGrid

Inhalt

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:

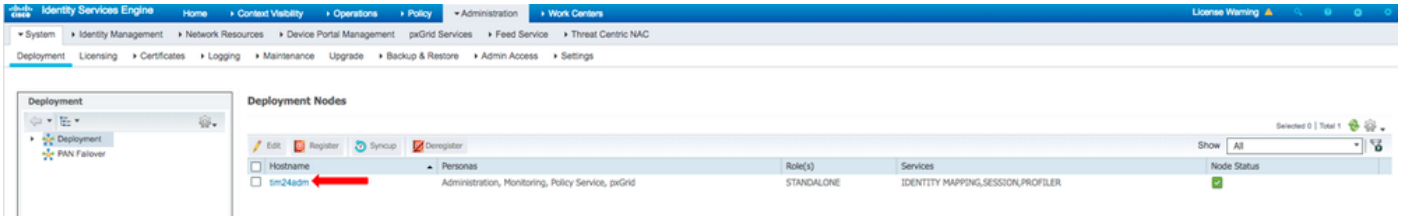
- Standalone ISE 2.4
- FMCv 6.2.3
- Active Directory 2012R2
- Identity Services Engine (ISE) pxGrid Version 2.4
- FirePOWER Management Center (FMC) Version 6.2.3

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.

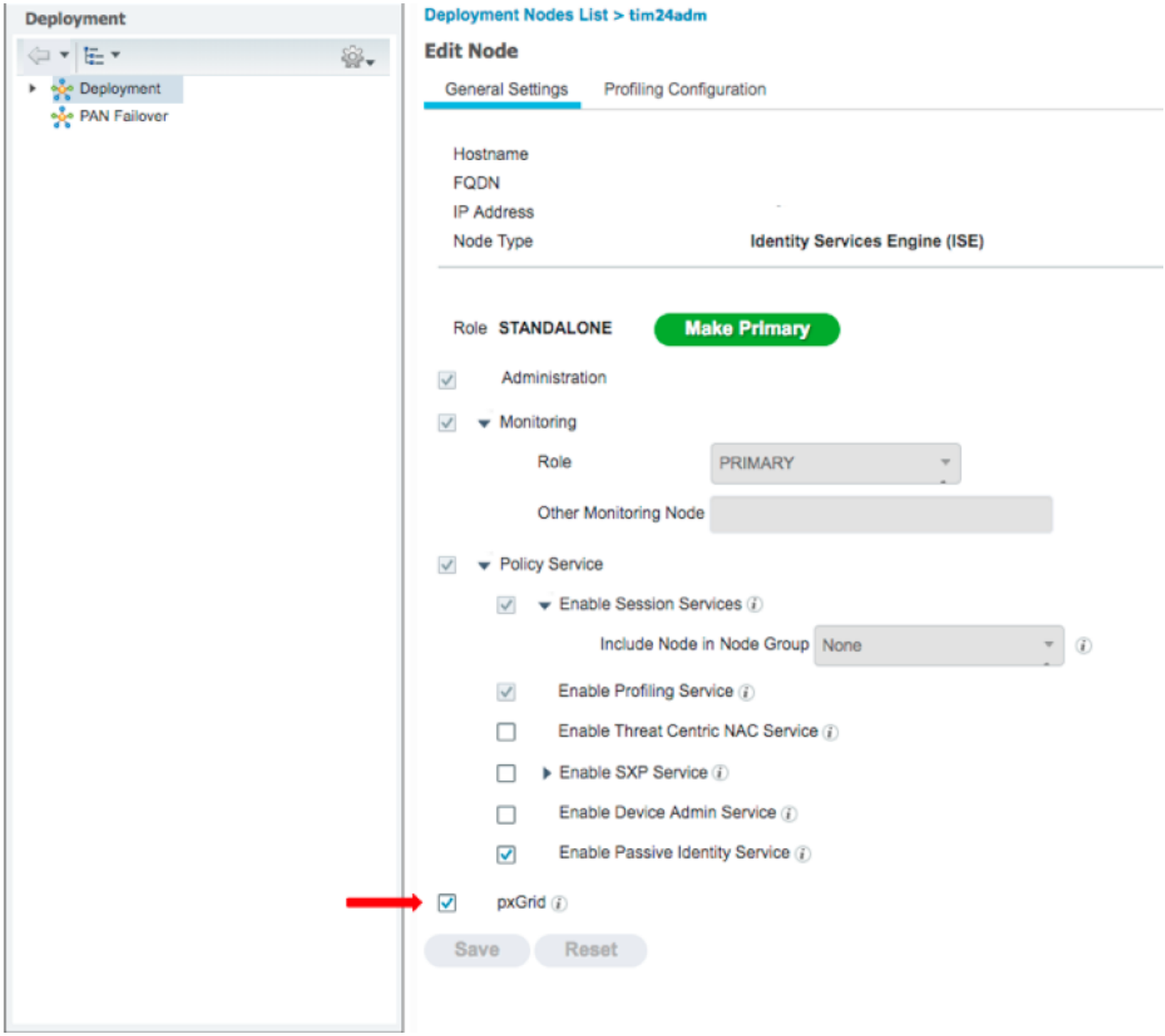
Konfigurieren der ISE

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.



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

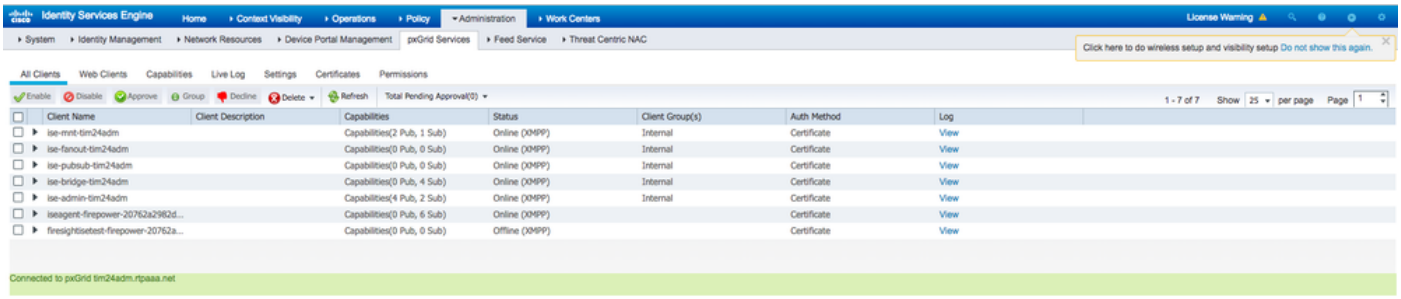
Hinweis: Der Vorgang dauert bis zu 5 Minuten, bis die pxGrid-Dienste vollständig gestartet sind und den HA-Status (High Availability) ermitteln, wenn mehr als ein pxGrid-Knoten verwendet wird.

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**.

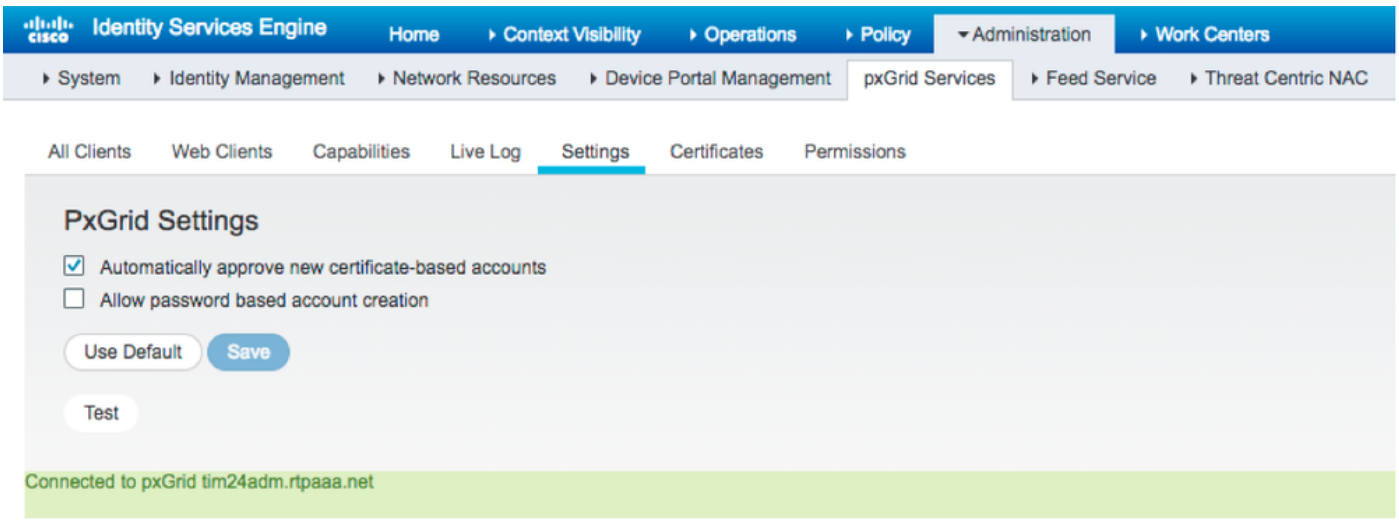
7. Unten auf der Seite zeigt ISE **"Connected to pxGrid <pxGrid node FQDN>" an**.



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**.



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".

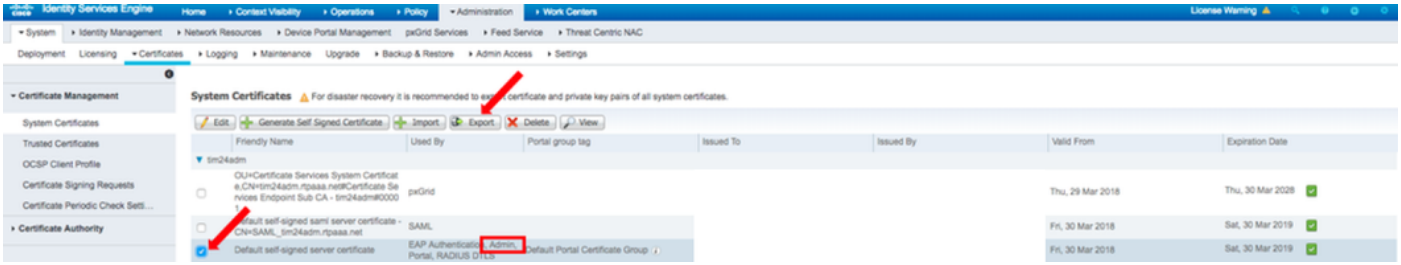
Hinweis: In diesem Leitfaden wird das ISE-Standardzertifikat mit Selbstsignatur für Administratoren verwendet. Wenn Sie ein von der Zertifizierungsstelle signiertes Administratorzertifikat verwenden, exportieren Sie die Stammzertifizierungsstelle, die das Administratorzertifikat auf dem ISE MNT-Knoten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

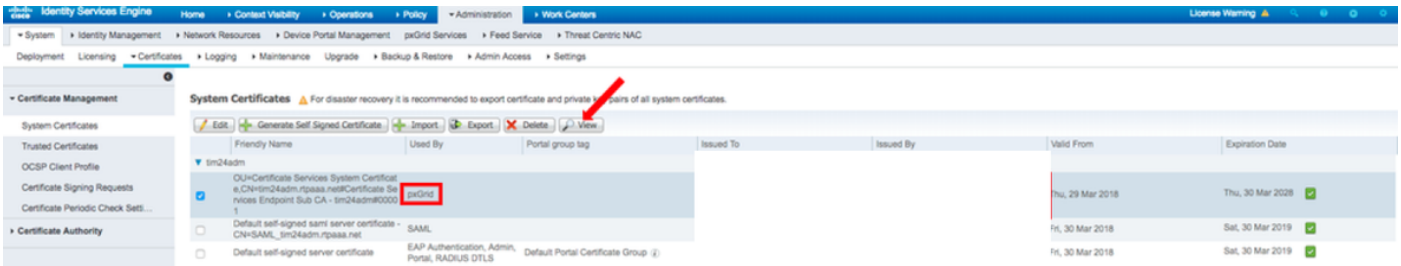


9. Kehren Sie zum Bildschirm ISE-Systemzertifikate zurück.

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

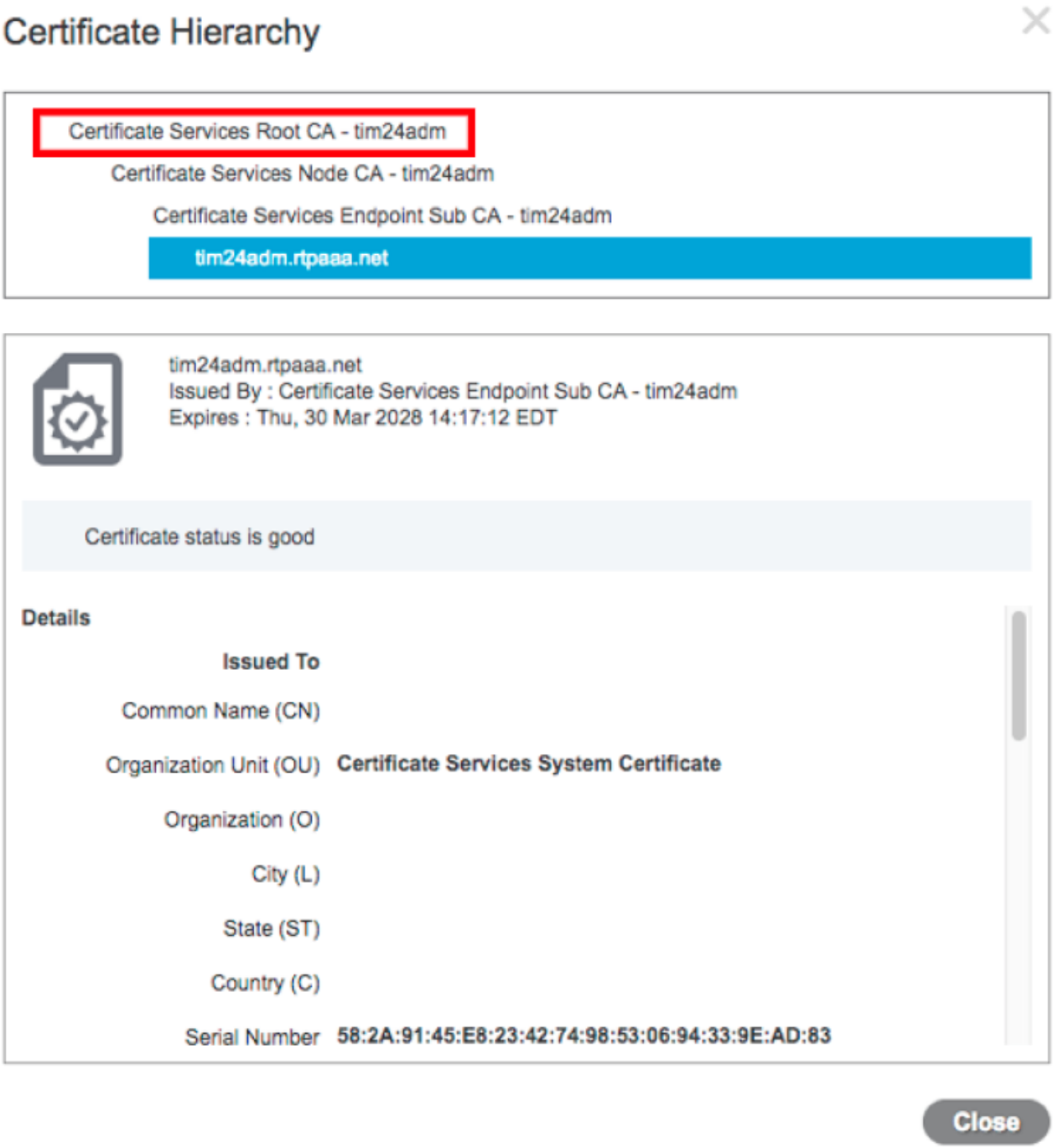
> **Hinweis**: In älteren Versionen der ISE handelte es sich um ein selbstsigniertes Zertifikat. Ab Version 2.2 wird dieses Zertifikat jedoch standardmäßig von der internen ISE-Zertifizierungsstellenkette ausgestellt.

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.

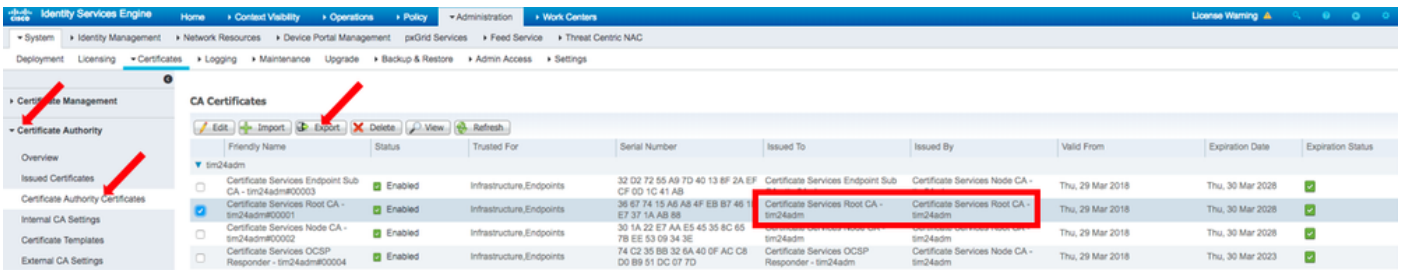


---

14. Erweitern Sie das Menü der ISE-Zertifizierungsstelle.

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

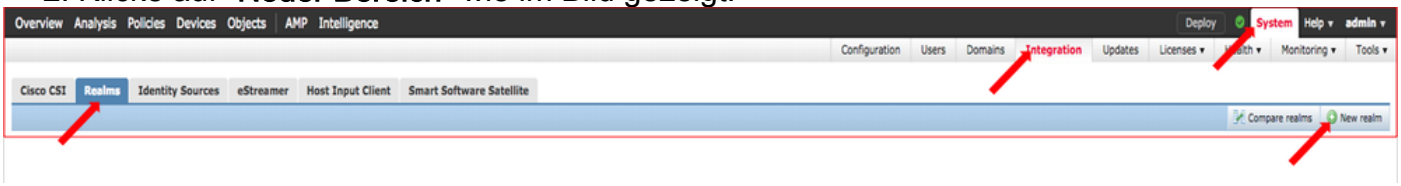
16. Wählen Sie das identifizierte Stammzertifikat aus, und klicken Sie auf **Exportieren.** Speichern Sie dann das Zertifikat der pxGrid-Stammzertifizierungsstelle, wie im Bild dargestellt.



Konfigurieren von FMC

Schritt 4: Neuen Bereich zu FMC hinzufügen

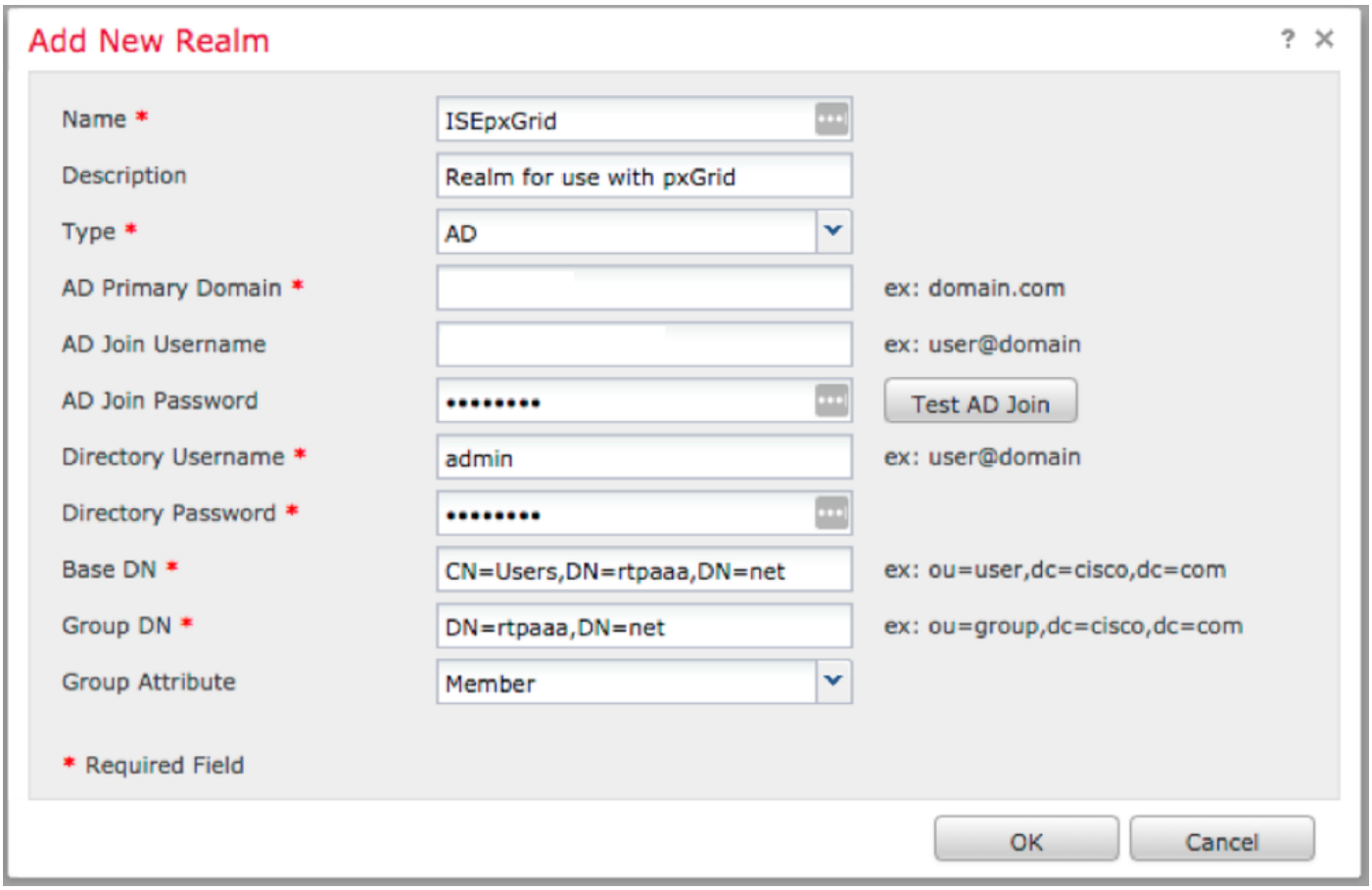
1. Rufen Sie die FMC-GUI auf, und navigieren Sie zu **System > Integration > Realms**.
2. Klicke auf "**Neuer Bereich**" wie im Bild gezeigt.



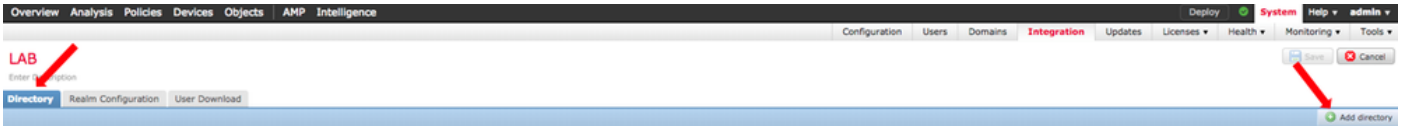
3. Füllen Sie das Formular aus und klicken Sie auf die Schaltfläche Active Directory (AD)-Join testen.

> **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**.



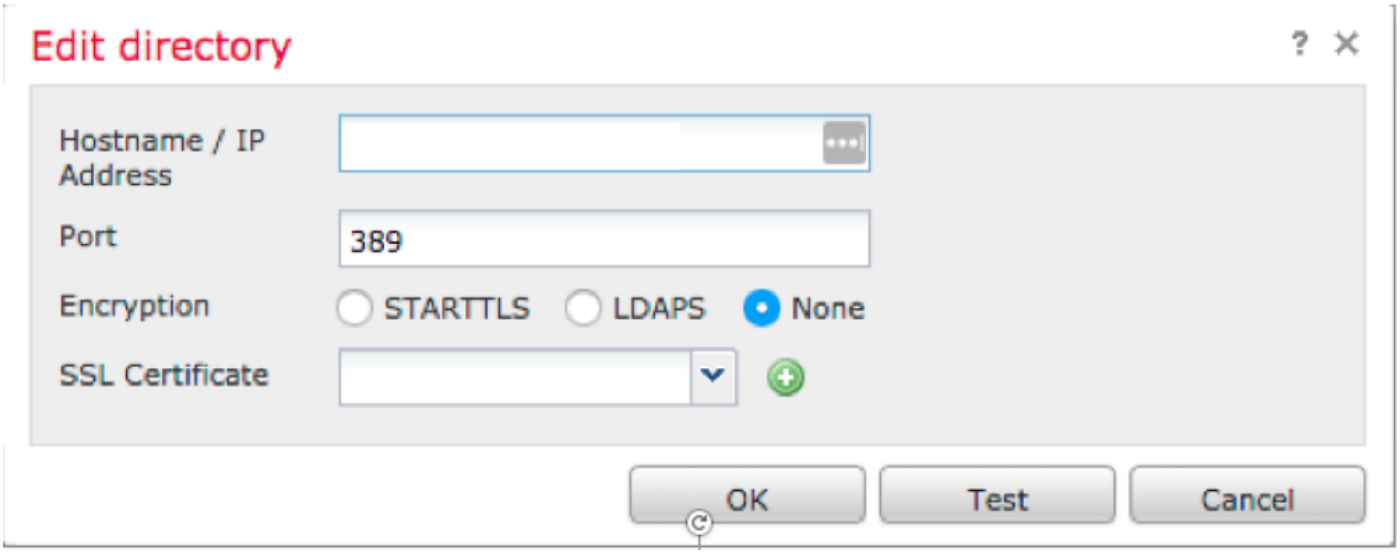
5. Klicken Sie auf die Registerkarte **Verzeichnis** und dann auf **Verzeichnis hinzufügen,** wie im Bild dargestellt.

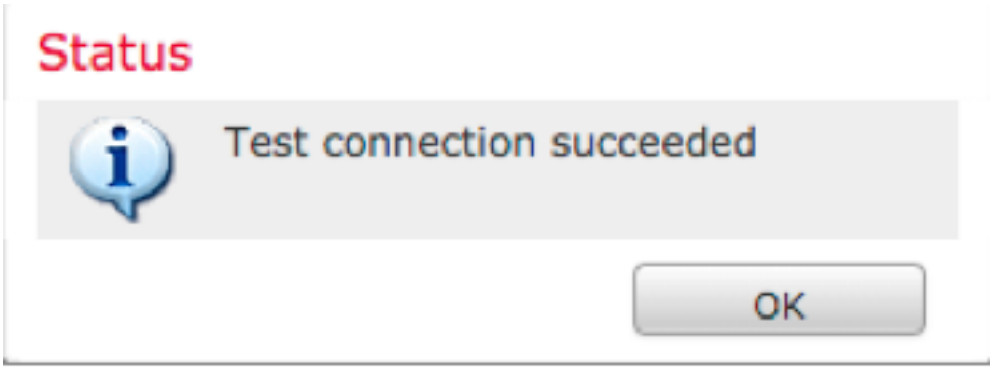


6. Konfigurieren Sie IP/Hostname und Testverbindung.

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

7. Klicken Sie auf **OK**.





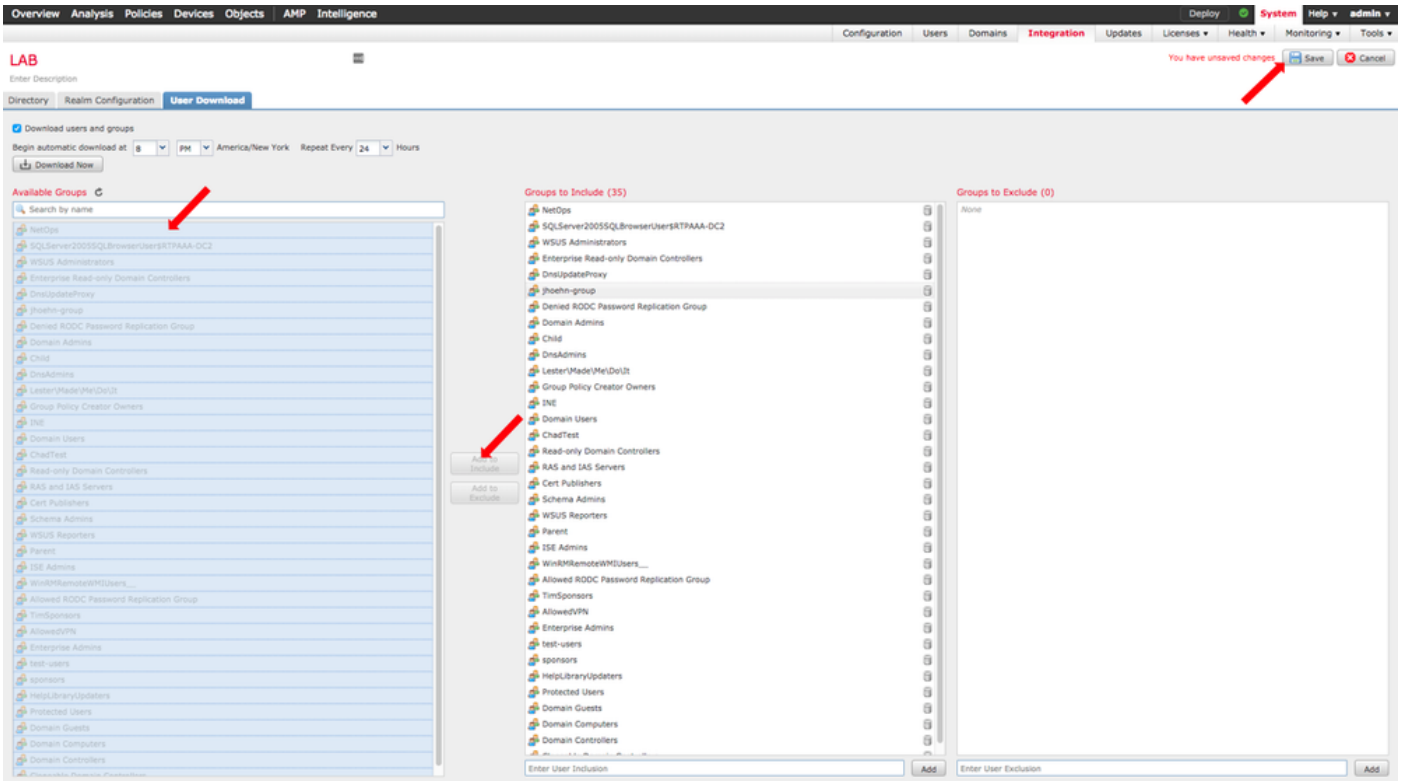
8. Klicken Sie auf die Registerkarte **Benutzerdownload**.

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

10. Klicken Sie auf Jetzt herunterladen

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

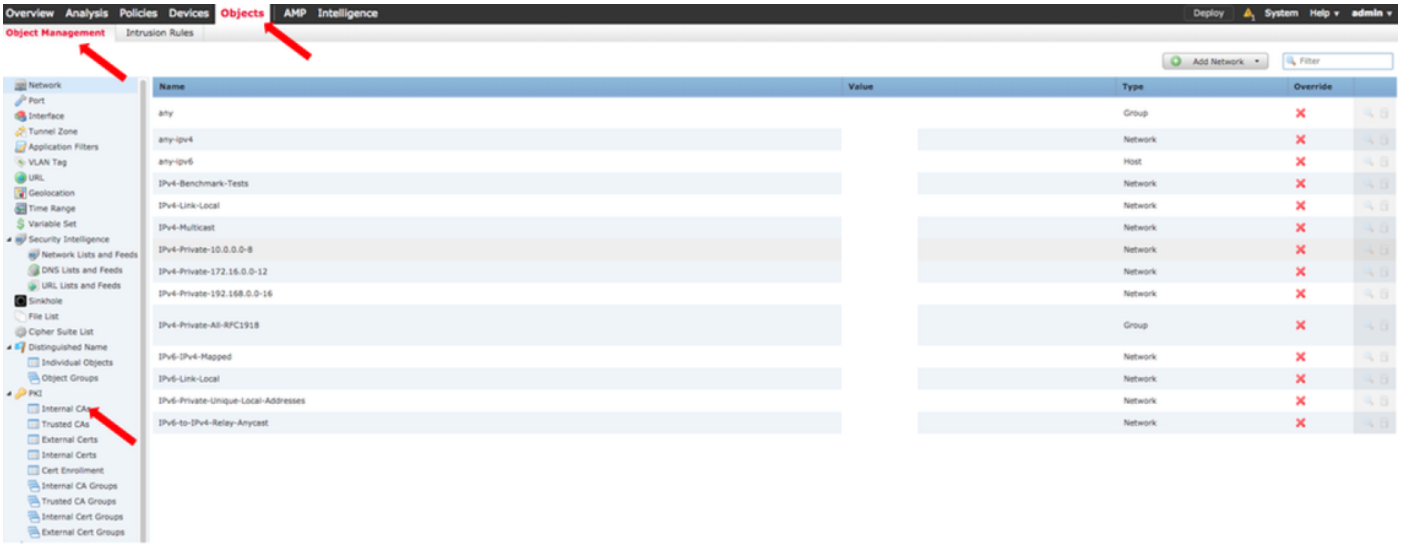
12. Speichern Sie die **Bereichskonfiguration**.



13. Aktivieren Sie den Realm-Status.

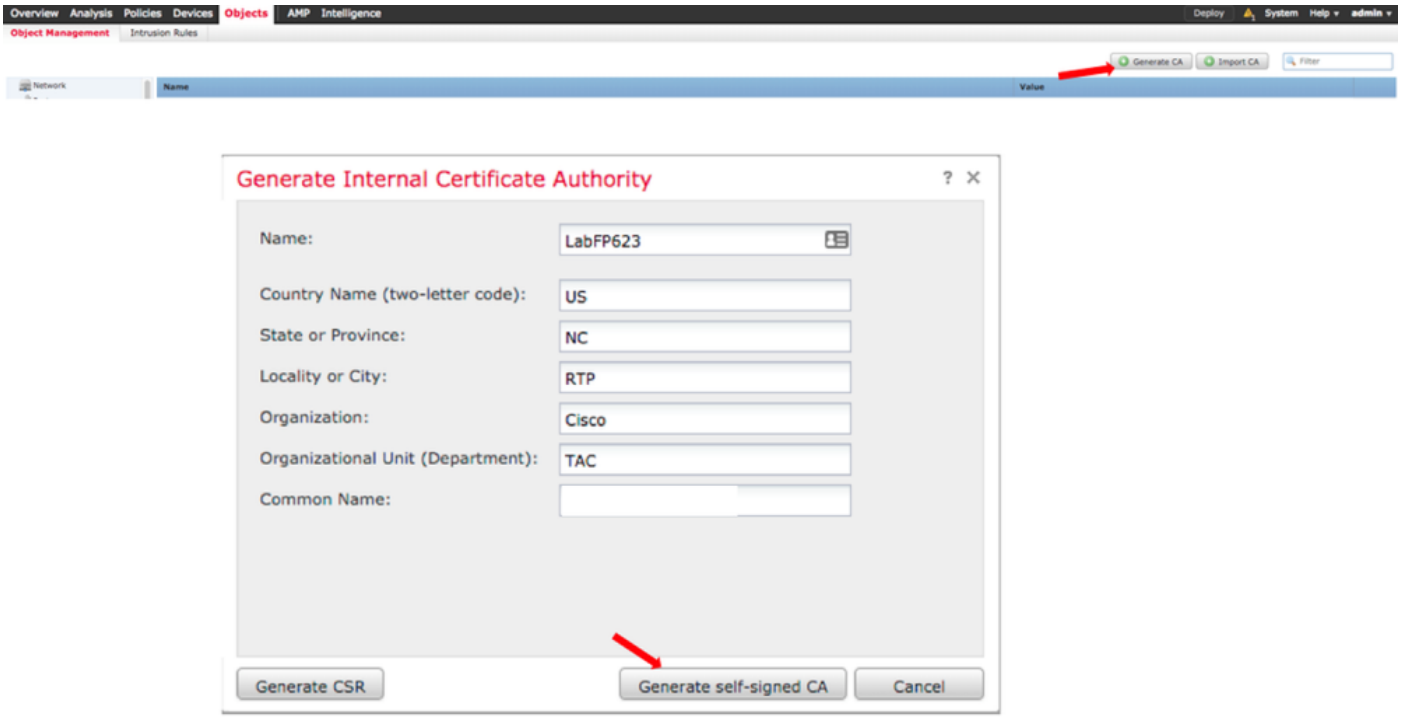
Schritt 5: FMC CA-Zertifikat generieren

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



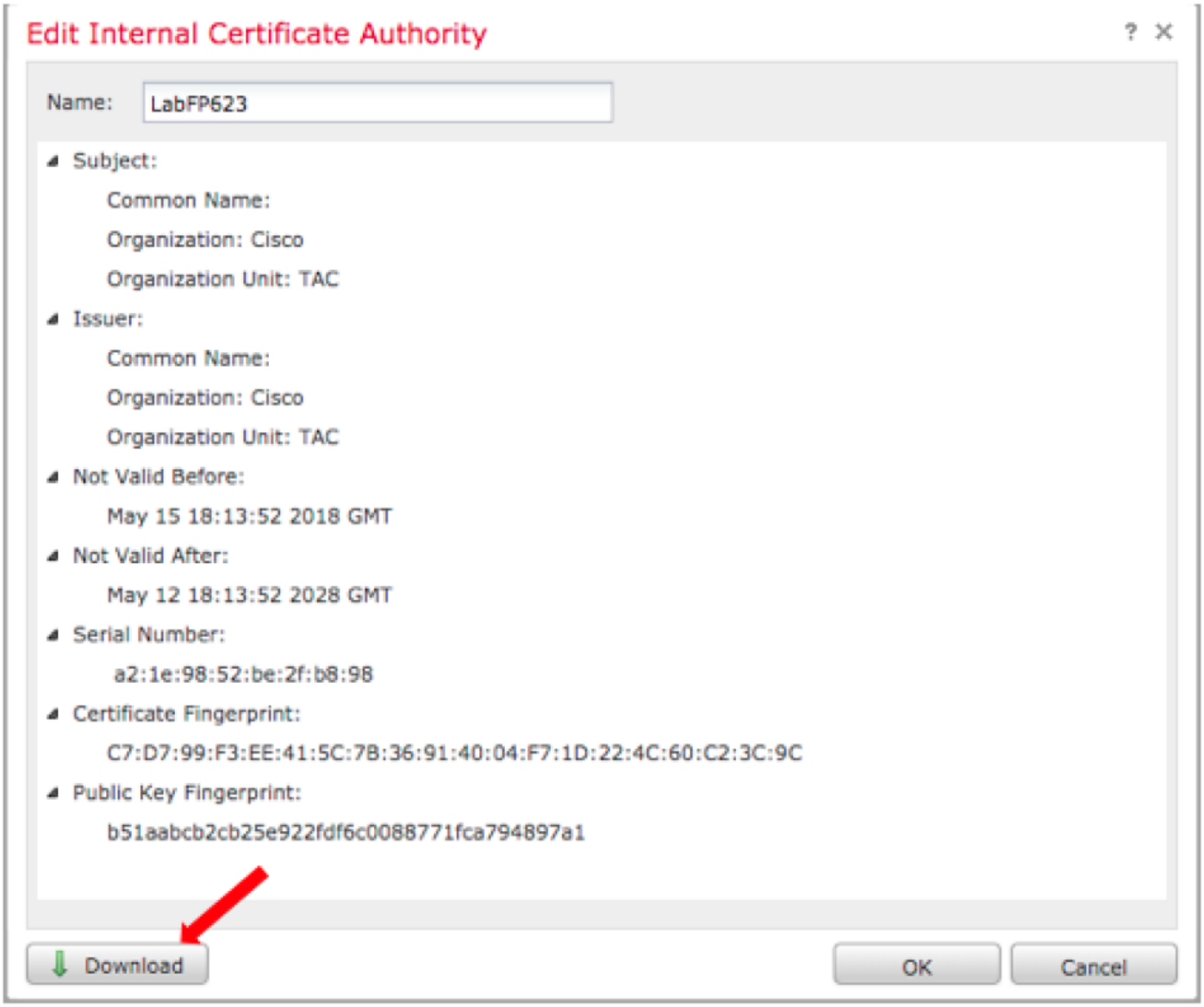
2. Klicken Sie auf **Zertifizierungsstelle erstellen**.

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



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.

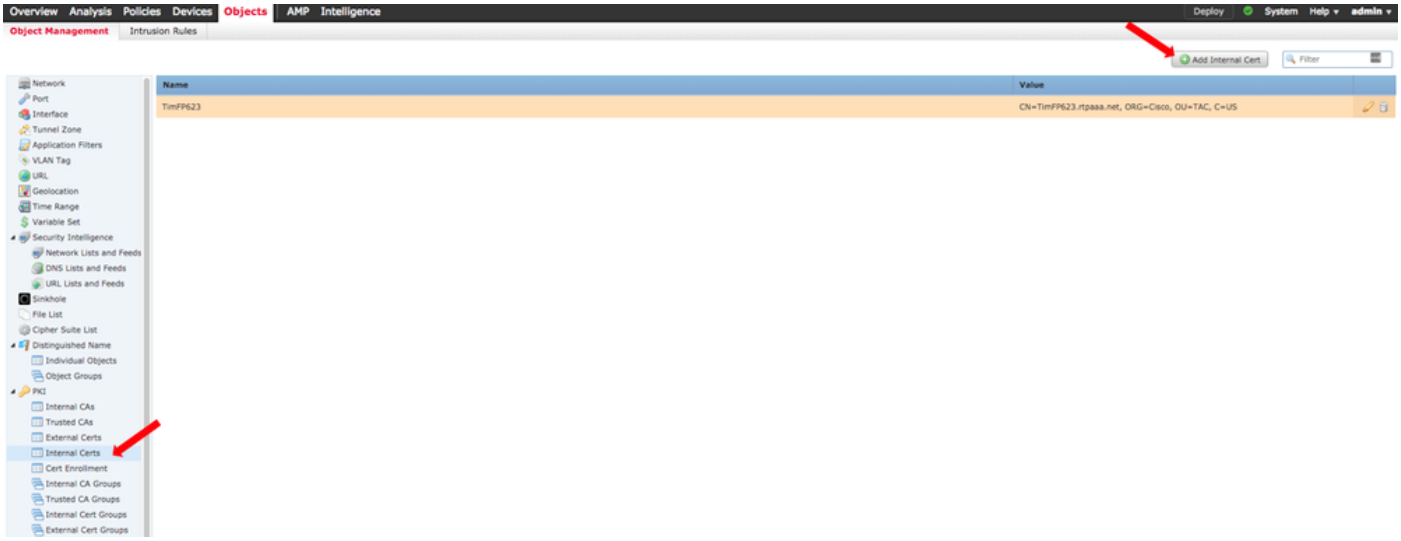
```
~$ openssl pkcs12 -nocerts -in <filename.p12> -out <filename.pvk>
Password:   Last login: Tue May 15 18:46:41 UTC 2018   Enter Import Password:   MAC verified OK
```

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.

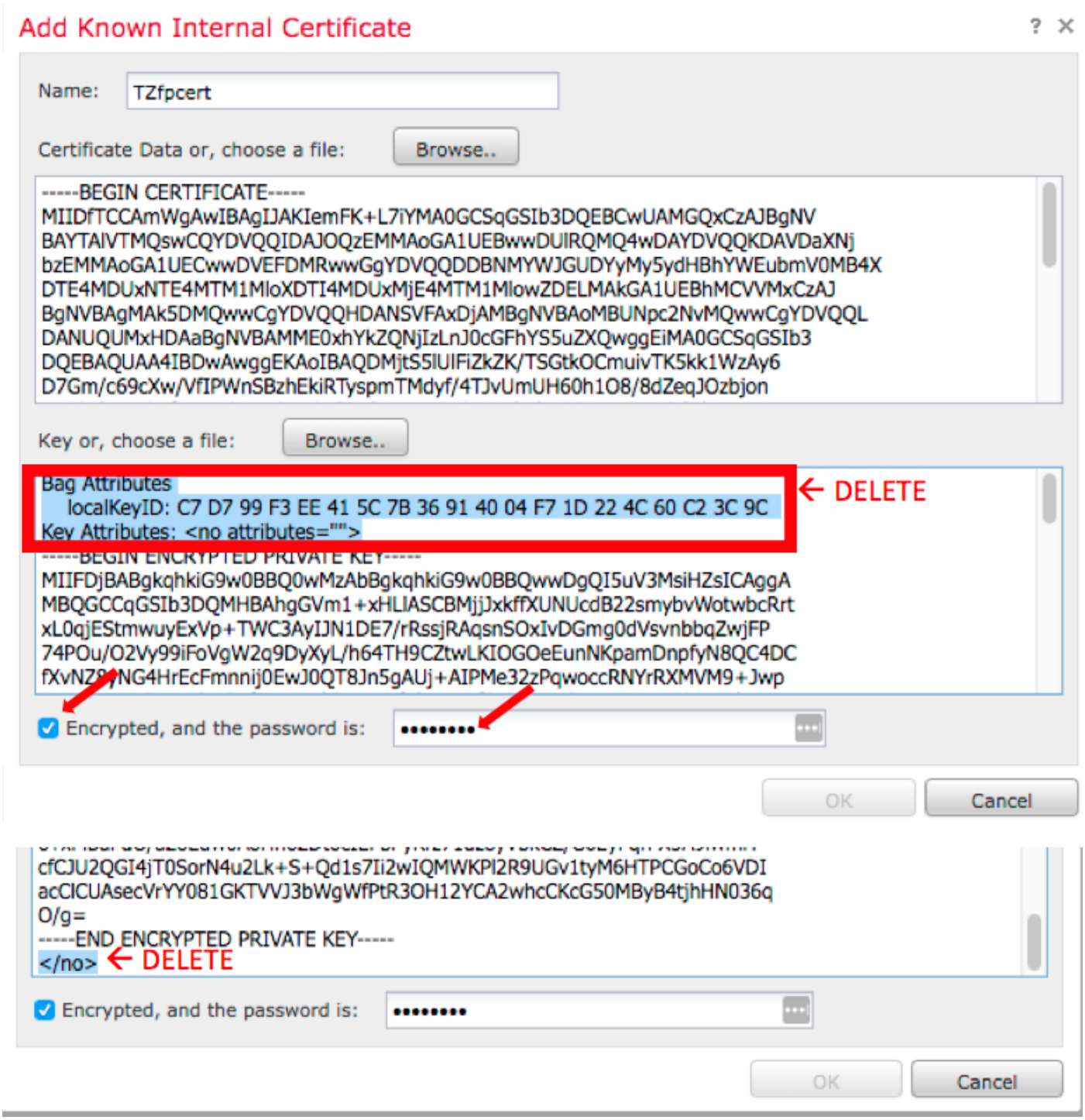
5. Durchsuchen Sie **Option** und wählen Sie die PVK-Datei.

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 voran- 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.

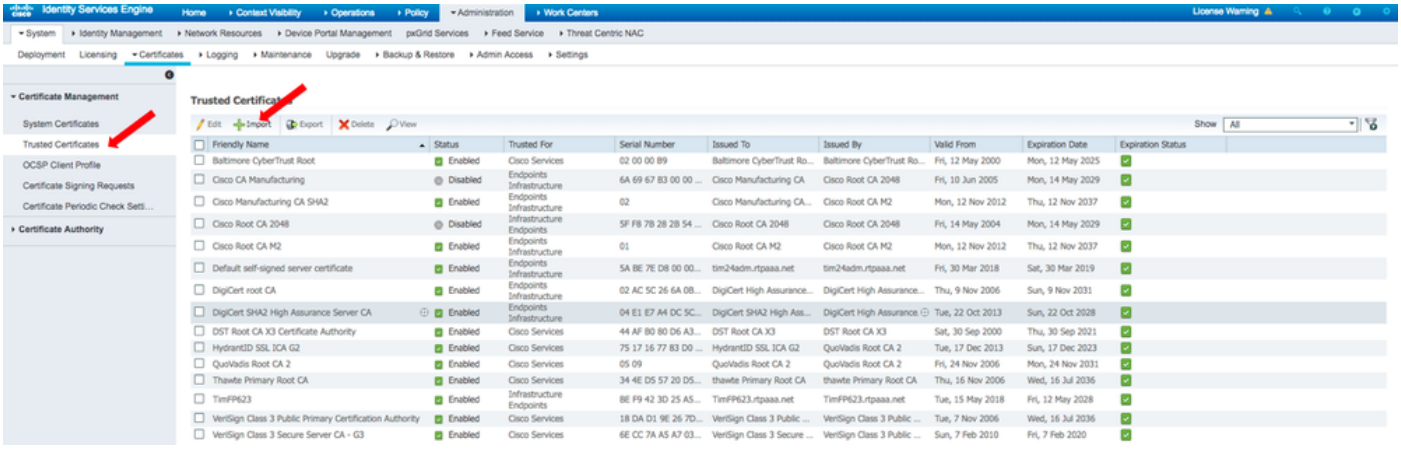
8. Klicken Sie auf **OK**.



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**.



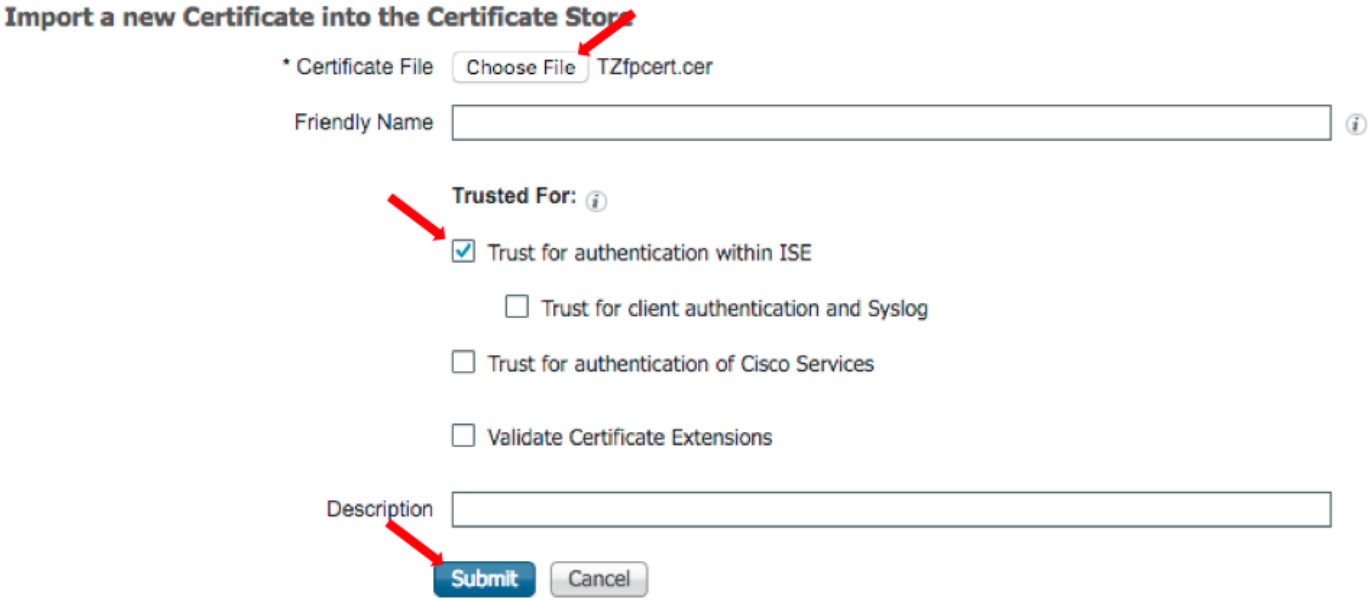
3. Klicken Sie auf **Choose File (Datei auswählen)**, und wählen Sie die FMC CER-Datei von Ihrem lokalen System aus.

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.



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.

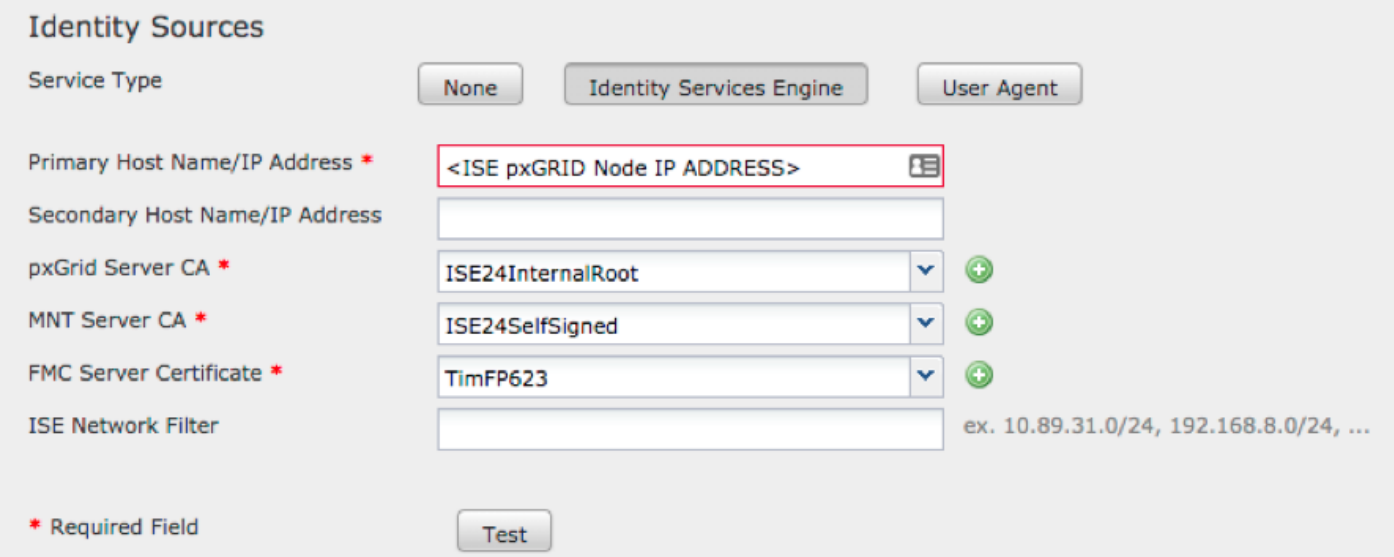
4. Wählen Sie das + rechts neben pxGrid Server CA.

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.

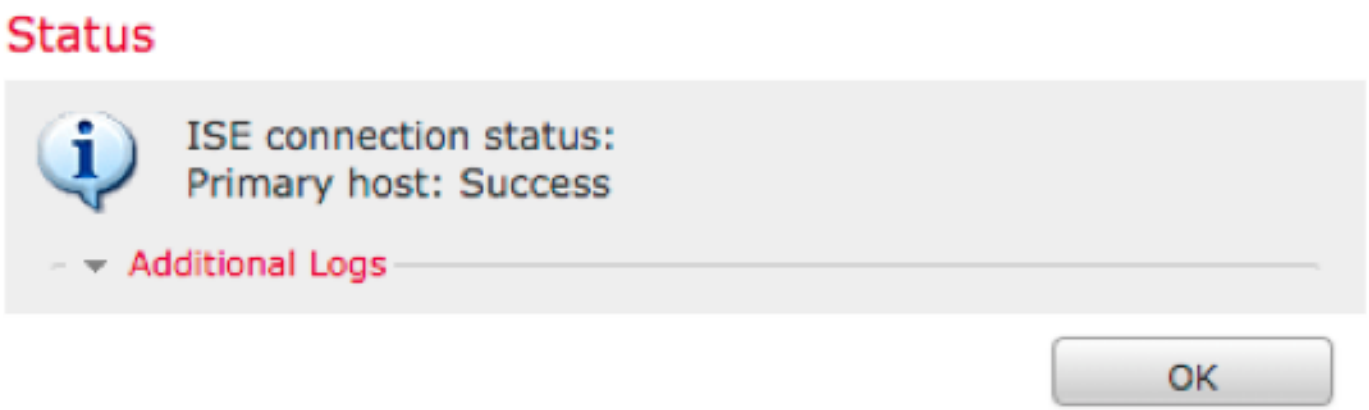
7. Benennen Sie die Server-CA-Datei, und navigieren Sie zu dem in Schritt 3 erfassten Admin-Zertifikat, und klicken Sie auf **Speichern**.

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



9. Klicken Sie auf **Test**.

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



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

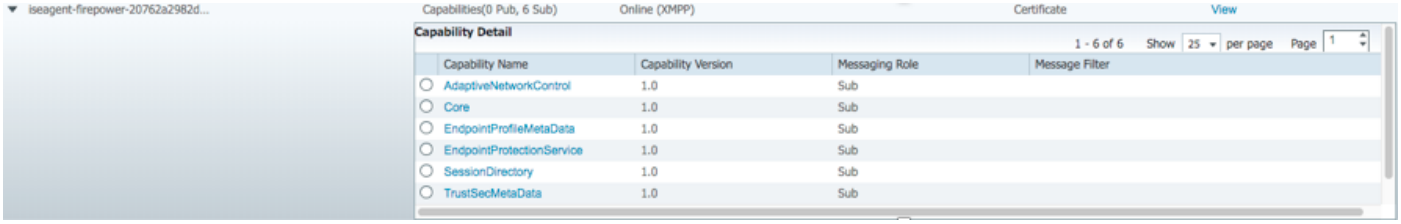
1. Öffnen Sie die **ISE-GUI**, und navigieren Sie zu **Administration > pxGrid Services**.

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).

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.

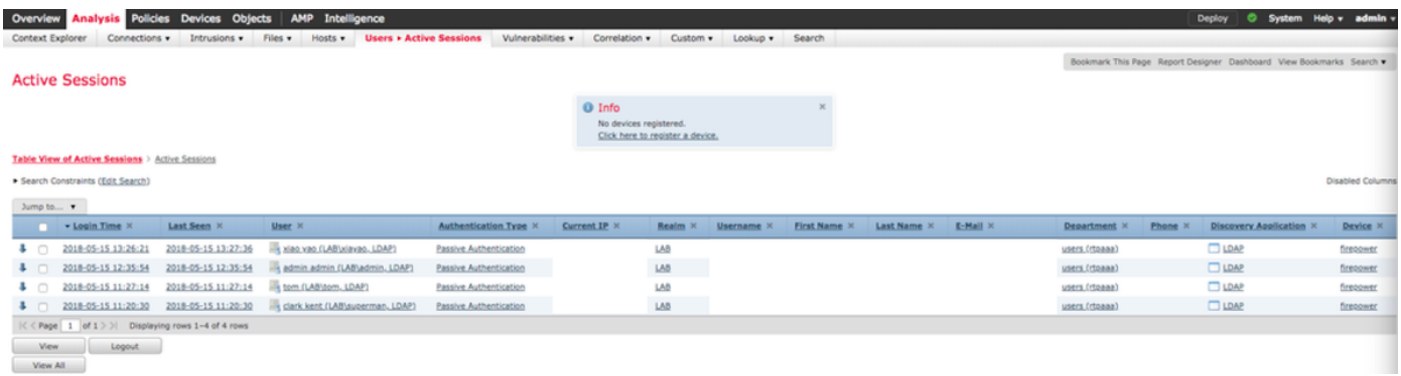


> **Hinweis**: Aufgrund des Cisco-Fehlers IDCSCvo75376 gibt es eine Hostnamensbeschränkung, und der Bulk-Download schlägt fehl. Die Testtaste am FMC zeigt einen Verbindungsfehler an. Dies betrifft 2.3p6, 2.4p6 und 2.6. Es wird empfohlen, 2.3 Patch 5 oder 2.4 Patch 5 so lange auszuführen, bis ein offizieller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



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.