ISE 3.2 mit FMC 7.2.4-Integration konfigurieren und Fehlerbehebung dafür durchführen

Inhalt

Einleitung

Voraussetzungen

- Verwendete Komponenten

Hintergrundinformationen.

Konfigurieren

- Vorbereitung der ISE auf die Integration
- Bereiten Sie das FMC auf die Integration vor.
- Einrichten der pxGrid-Verbindung zwischen ISE und FMC

Überprüfung.

- Validierung auf FMC
- Validierung auf der ISE

Fehlerbehebung

- Fehlerbehebung auf FMC
- Fehlerbehebung auf der ISE.

Häufige Probleme.

- Der PxGrid-Subscriber-Client ist für die ISE nicht zugelassen.
- PxGrid ISE-Zertifikatkette unvollständig.

Referenz.

Einleitung

In diesem Dokument werden Verfahren zur Integration der Identity Services Engine in das Firewall Management Center unter Verwendung von Platform Exchange Grid-Verbindungen beschrieben.

Voraussetzungen

Cisco empfiehlt Fachwissen in folgenden Bereichen:

- Identity Services Engine (ISE)
- Plattform-Austausch-Grid
- Firewall Management Center (FMC)
- TLS/SSL-Zertifikate

Verwendete Komponenten

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

- Identity Services Engine (ISE) Version 3.2 Patch 3
- Firewall Management Center Version 7.2.4

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 kennen.

Hintergrundinformationen.

Diese Dokumentation bietet eine Lösung zur Integration von FMC und ISE mit pxGrid Version 2.

Das Cisco FirePOWER Management Center (FMC) ist eine zentralisierte Plattform für Firewalls der nächsten Generation und Intrusions Prevention Systems und bietet Richtlinienmanagement, Bedrohungserkennung und Reaktion auf Vorfälle.

Die Cisco Identity Services Engine ist eine umfassende Lösung, die einen sicheren Zugriff auf Endgeräte ermöglicht, indem sie Services für Authentifizierung, Autorisierung und Rechenschaftspflicht (AAA) sowie die Durchsetzung von Richtlinien bereitstellt.

Mit Platform Exchange Grid (pxGrid) können Sie Informationen zwischen anbieterübergreifenden, plattformübergreifenden Netzwerken austauschen.

Diese Integration ermöglicht eine sichere Überwachung und Erkennung von Bedrohungen sowie die Festlegung von Netzwerkrichtlinien auf Basis der gemeinsam genutzten Informationen.

PxGrid Framework hat 2 Versionen. Die zu verwendende hängt von der ISE-Version und dem Patch ab, die Sie überprüfen müssen.

Ab Version ISE 3.1 werden alle pxGGrid-Verbindungen von ISE basieren auf pxgrid-Version 2.

PxGrid Version 1.

TDie erste Version dieses Frameworks (pxGrid v1) zeichnet sich durch die Betriebsfähigkeit aus, die durch den Befehl show application status ise wie es in der folgenden Ausgabe angezeigt wird.

Wenn die Funktion pxGrid im Knoten aktiviert ist, wird das pxGrid angezeigt. Funktionen im Betriebszustand.

```
ise/admin# show application status ise
ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          3688
Database Server                        running          41 PROCESSES
Application Server                     running          6041
Profiler Database                      running          4533
AD Connector                           running          6447
M&T Session Database                   running          2363
M&T Log Collector                      running          6297
M&T Log Processor                      running          6324
Certificate Authority Service          running          6263
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
pxGrid Connection Manager              disabled
pxGrid Controller                      disabled
Identity Mapping Service               disabled
```

Benutzerfreundlichkeit von PxGrid Version 1.

In dieser Version dieser Plattform ist es bekannt, nur einen pxGrid-Knoten mit den pxGrid-Prozessen im laufenden Status zu haben, während sich die anderen pxGrid-Knoten im Standby-Status befinden.

Diese Knoten überwachen ständig den Status des pxGrid-Knotens mit zugehörigen Services, die mit der Ausführung zusammenhängen.

In diesem, der primäre pxGrid-Knoten gab es eine Promotion und die anderen pxGrid-Knoten aktiviert ihre pxGrid-Dienste.

Dies bedeutete jedoch eine Ausfallzeit, wenn dieses Failover auftrat.

Die erste Version von pxgrid basiert auf der Kommunikation im Extensible Messaging and Presence Protocol (XMPP), einer Reihe von Technologien, die in der Collaboration- und Sprachinfrastruktur verwendet werden.

Folgende Themen werden in einer pxGrid v1-Verbindung behandelt:

- Sitzungsverzeichnis
- Endpunktprofil-Metadaten
- TrustSec-Metadaten
- Funktion zum Schutz von Endgeräten
- Adaptive Netzwerkkontrolle
- MDM_Offline - Thema
- Identität
- SXP

PxGrid Version 2.

Dieses Dokument behandelt die Verwendung von PxGrid Version 2. Diese Plattform arbeitet mit REST-Operationen auf ISE und WebSocket-Protokolle, die Verbesserungen, verbesserte Skalierbarkeit, Leistung und Flexibilität in Datenmodellen bringt.

In dieser Version werden pxgrid-Features nicht wie in der vorherigen Version mit dem Befehl show application status ise ausgeführt.

Im Abschnitt zur Validierung der ISE in diesem Dokument erfahren Sie, welche Mechanismen Sie überprüfen müssen, um die pxGrid-Funktionalität zu überprüfen.

Mit dieser Version haben Sie alle pxGrid-Knoten, die Sie als aktive pxGrid-Knoten konfigurieren. Sie sind jederzeit bereit, sich am Informationsaustausch zu beteiligen.

In Version 1 wurde die Betriebsfähigkeit von pxGrid nur auf einem Knoten ausgeführt.

Folgende Themen werden in einer pxGrid v2-Verbindung behandelt:

- Sitzungsverzeichnis
- Radius-Fehler
- Profiler-Konfiguration
- Systemstatus
- MDM
- ANC-Status
- TrustSec
- TrustSec-Konfiguration
- TrustSec-SXP
- Endgerät-Ressource.

Komponenten von pxGrid als Plattform.

PxGrid-Controller (ISE): Muss allen Teilnehmern vertrauen, die pxGrid verwenden.

Kunde: Kann Abonnent und Herausgeber verschiedener Themen sein.

Herausgeber: Client, der Informationen mit dem Controller teilt.

Teilnehmer: Client, der die Informationen eines Themas verwendet.

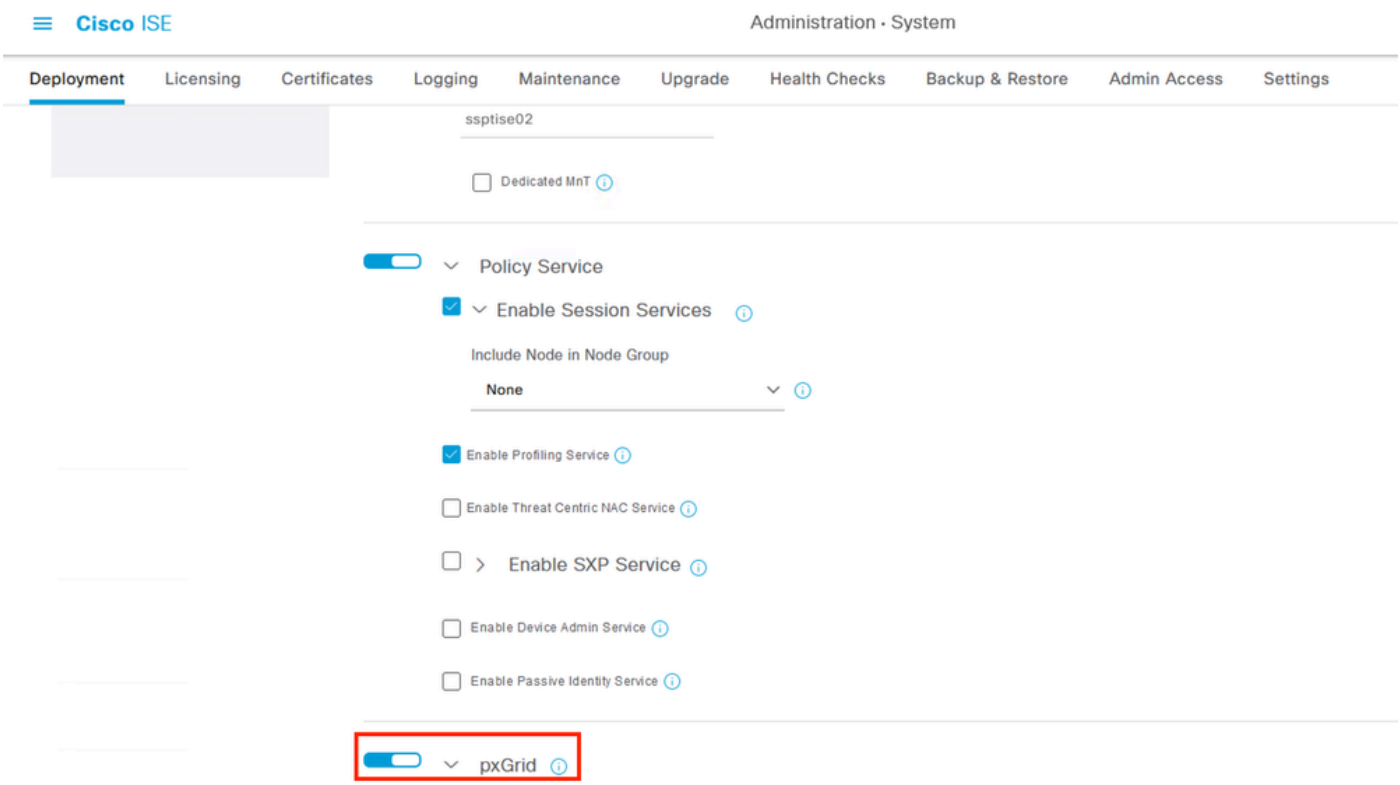
Durch diese Integration können Sie Content-Richtlinien auf FMC-Basis erstellen. Diese basieren auf den von der ISE freigegebenen Informationen und den veröffentlichten Themen (im Zusammenhang mit der Endgerätaktivität).

Konfigurieren

Vorbereitung der ISE auf die Integration

Schritt 1. Konfigurieren Sie den ISE-Knoten, um die pxGrid persona darauf im Menü Administration > System > Deployment auszuführen.

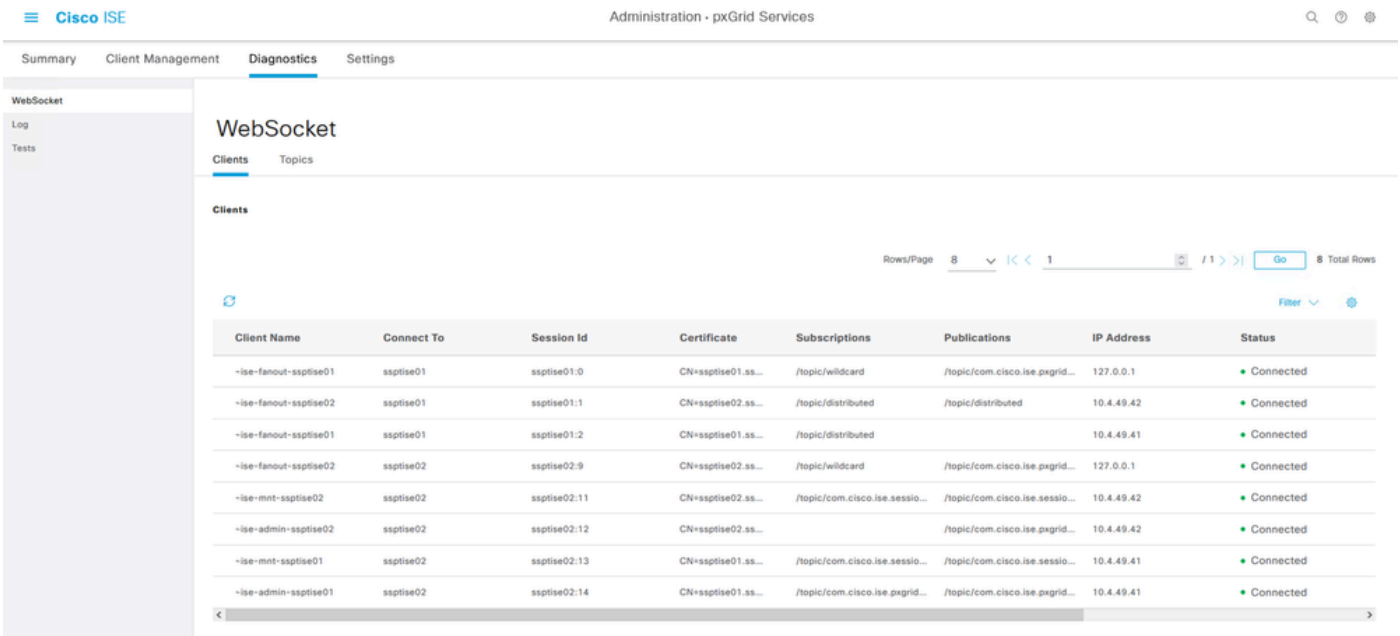
Wählen Sie die Knoten und aktivieren Sie die Funktion pxGrid.



Aktivieren von ISE-pxGrid-Services in einem Knoten

Schritt 2: Nachdem Sie die Knoten mit der Funktion pxGrid aktiviert haben, überprüfen Sie den Status der Websockets, die sich auf die verbundenen internen Clients beziehen.

Navigieren Sie zu Administration > pxGrid Services > Websocket. Beachten Sie, dass Clients direkt über die IP-Adresse 127.0.0.1 auf die ISE-Services verweisen.



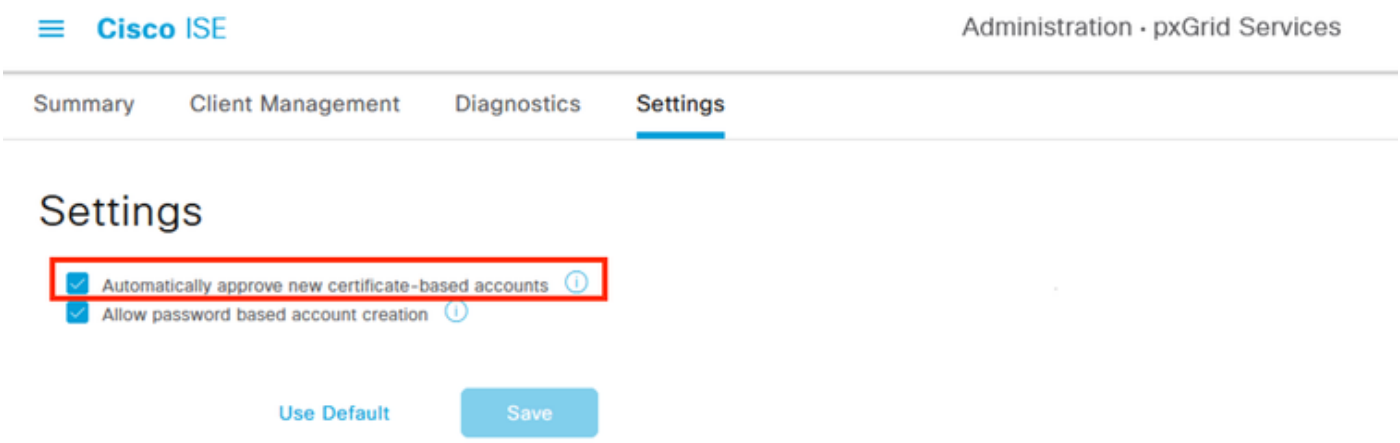
Interne WebSockets von der ISE.

Schritt 3: Navigieren Sie durch das Menü Administration > pxGrid Services > Settings

(Verwaltung > pxGrid-Dienste > Einstellungen), und wählen Sie die Option zum automatischen Genehmigen neuer Zertifikatbasiskonten aus.

Dieser Schritt ist zu diesem Zeitpunkt optional. Für die pxGrid-Verbindung wird jedoch empfohlen, dieses Kontrollkästchen zu aktivieren.

Sie können das FMC anschließend manuell als Teilnehmer akzeptieren.



Aktivieren der automatischen Genehmigung für pxGrid-Zertifikatkonten.

Schritt 4: Überprüfen Sie die Zertifikate für die pxGrid-Funktion Ihrer Umgebung unter Administration > System > System Certificates,

Es wird empfohlen, dass Sie homogene pxGrid-Zertifikate in allen Knoten Ihrer Bereitstellung haben, die von der gleichen Stammzertifizierungsstelle (Certificate Authority, CA) signiert werden

In diesem Szenario werden die generierten internen ISE-Zertifikate verwendet. Bei dieser Version der ISE, bei der in diesem Beispiel die Stammzertifizierungsstelle dem PAN-Knoten entspricht.

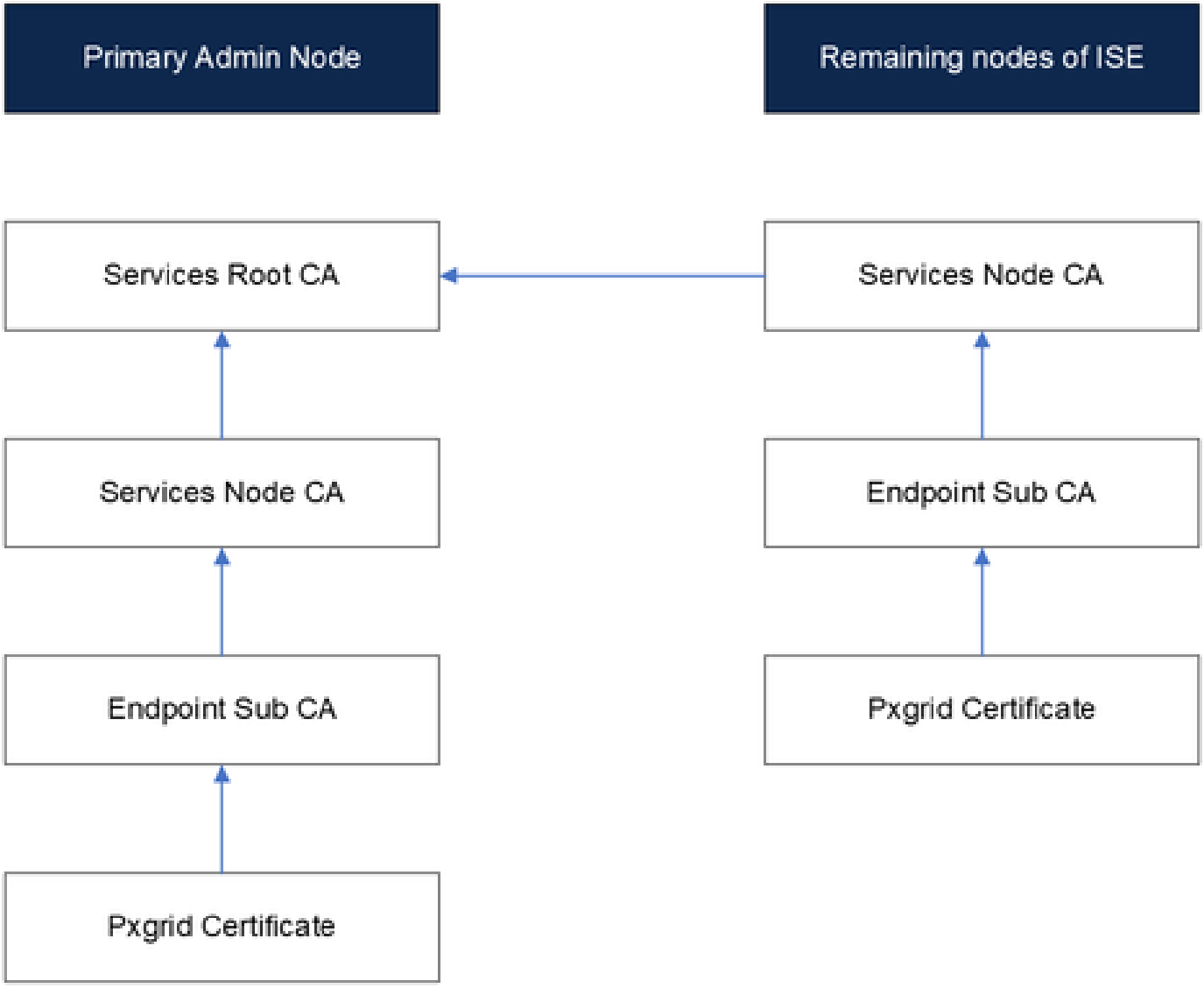
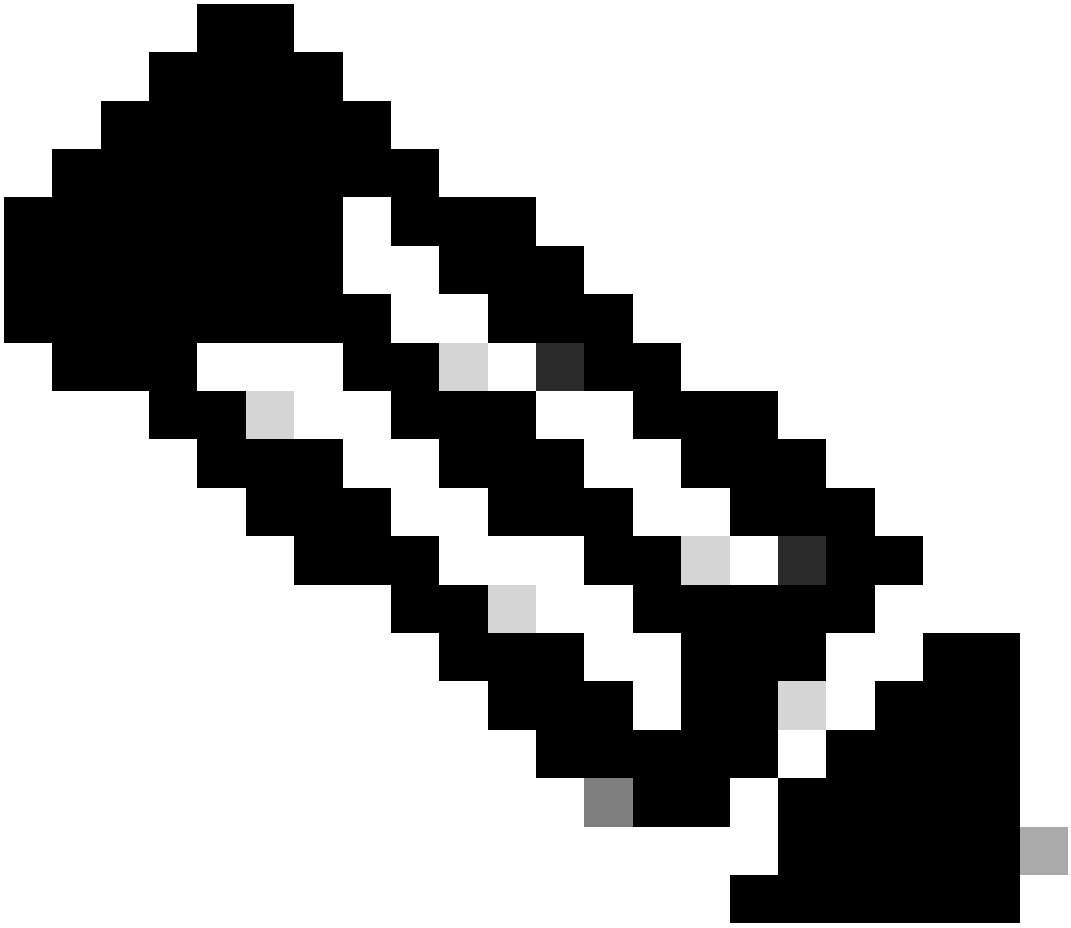
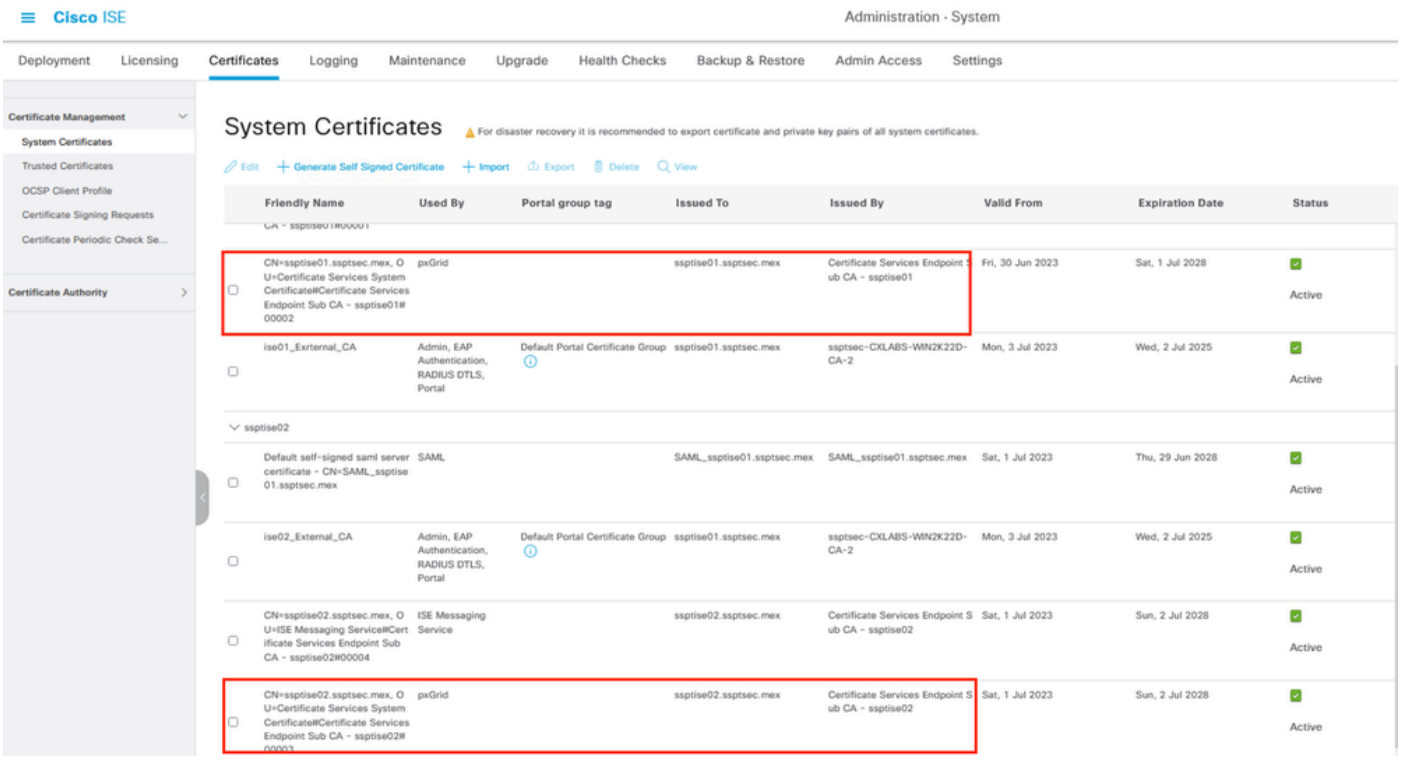


Diagramm der internen Zertifikate auf der ISE.



Anmerkung: Weitere Informationen zur internen Struktur der auf der ISE generierten Zertifikate finden Sie unter Verstehen der internen Services der ISE-Zertifizierungsstelle.

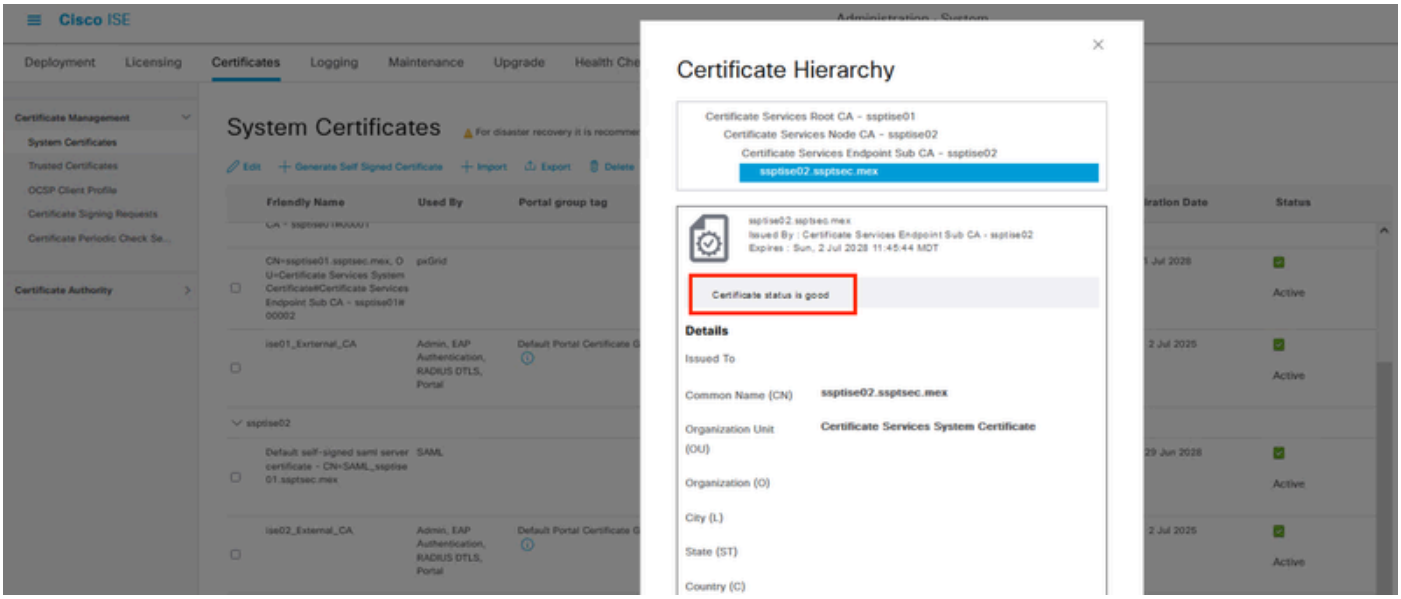


PxGrid-Zertifikate in einer verteilten Bereitstellung.

Schritt 5: Überprüfen des Status der pxGrid-Zertifikate

Wählen Sie aus dem vorherigen Menü ein Kontrollkästchen aus einem Knoten pxGrid-Zertifikat und anschließend die Option Ansicht.

Die Ausgabe ähnelt der Ausgabe, die hier in den pxGrid-Zertifikaten angezeigt wird.

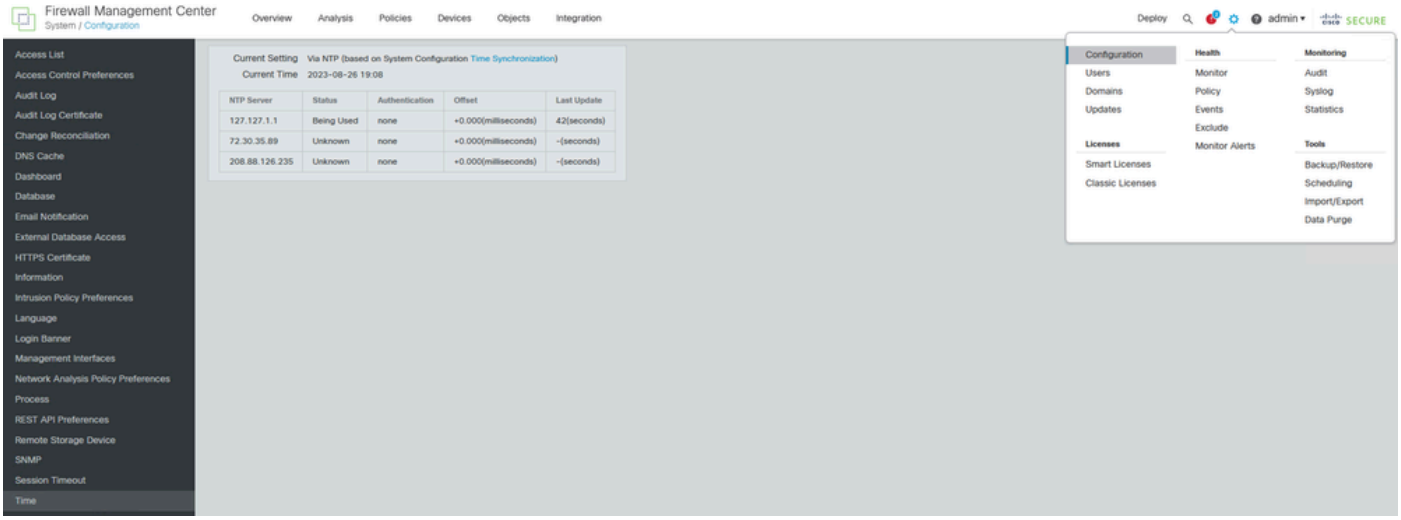


Verifizierung des pxGrid-Zertifikats.

Bereiten Sie das FMC auf die Integration vor.

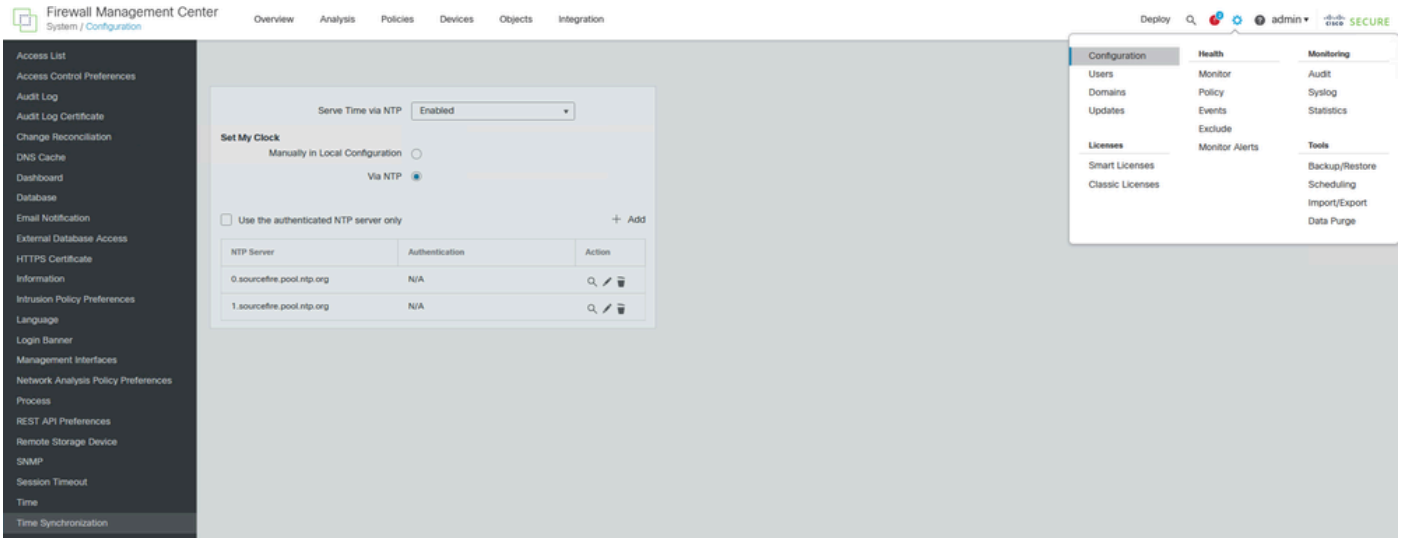
Schritt 1:Bestätigen, dass die interne FMC-Zeit aktuell.

Navigieren Sie zu System > Konfiguration > Zeit und stellen Sie sicher, dass die auf dem FMC konfigurierte Zeit aktuell.



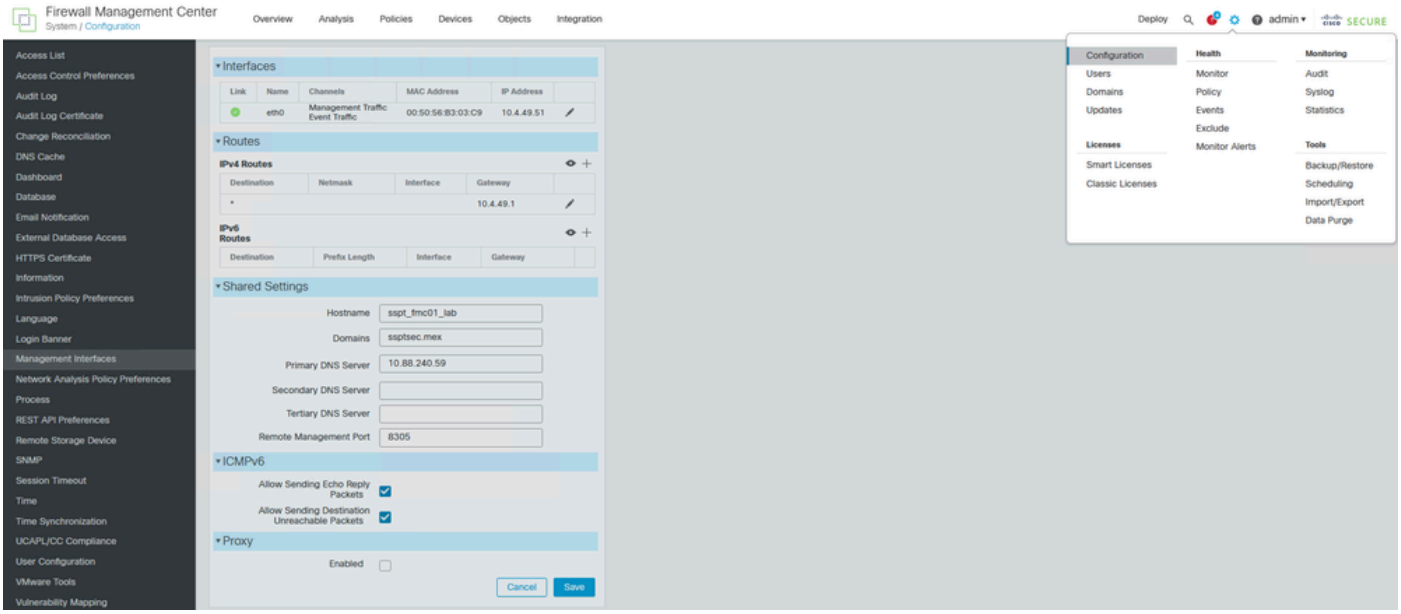
Überprüfen der Aktualität des FMC

Wenn die FMC-Zeit nicht aktualisiert wird, stellen Sie sicher, dass das NTP richtig konfiguriert ist. und in Synchronisierung. NTP kann konfiguriert werden unter System > Konfiguration > Zeit > + Hinzufügen.



Zeitsynchronisierung auf FMC

Schritt 2: Navigieren Sie zu System > Konfiguration > Management-Schnittstelle > Gemeinsame Einstellungen und überprüfen, ob mindestens Primärer DNS-Server feld enthält eine gültige DNS-Server-IP.



DNS-Konfiguration auf FMC

Schritt 3: Bestätigen Sie die Konfiguration des FMC-Hostnamens.

Navigieren Sie zu System > Konfiguration > Verwaltungsschnittstelle > Gemeinsam genutzte Einstellungen und überprüfen Sie, Hostname enthält den FMC-Hostnamen.

Sie können diesen Schritt überprüfen, während Sie den vorherigen Schritt in diesem Abschnitt lesen.

Einrichten der pxGrid-Verbindung zwischen ISE und FMC

Schritt 1. Navigieren Sie zum Menü Administration > pxGrid Services > Client Management > Certificates (Verwaltung > pxGrid-Dienste > Client-Verwaltung > Zertifikate).

Wählen Sie in der ersten Option I want to Generate a single certificate (without a certificate signing request) aus.

Geben Sie im Abschnitt Common Name (CN) den FQDN des FMC ein, das die ISE ausstellen soll.

Geben Sie eine Beschreibung an.

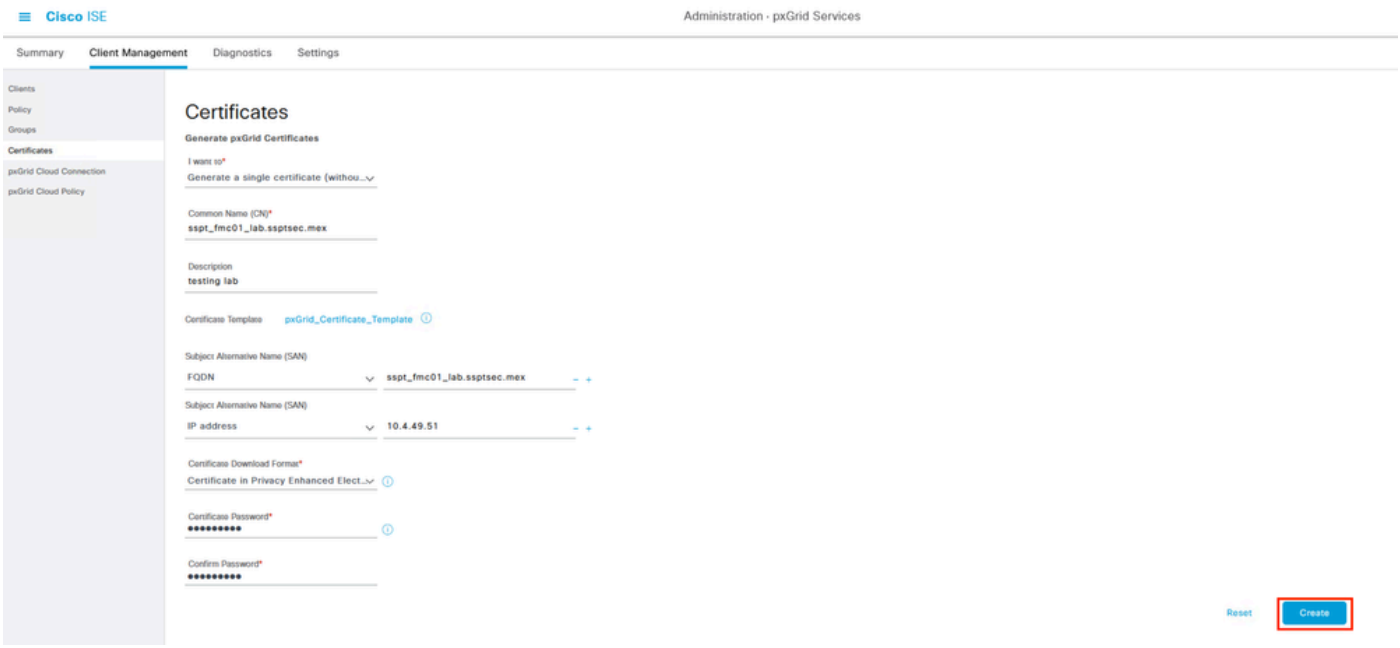
Geben Sie im Abschnitt Subject Alternative Name (SAN) den FQDN und die IP-Adresse des anzuschließenden FMC ein.

Wählen Sie unten im Certificate Download Format aus dem Dropdown-Menü die Option Certificate in Privacy Enhanced Electronic Mail (PEM) format.

PKCSS-PEM-Format eingeben (einschließlich Zertifikatkette).

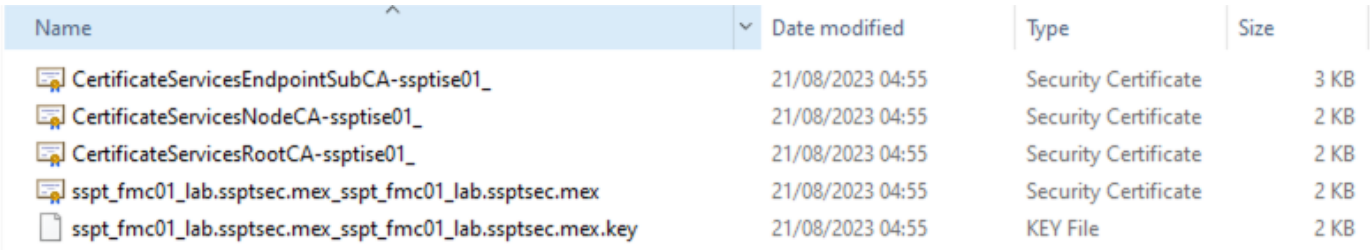
Geben Sie ein Kennwort in das Zertifikatkennwort ein, und speichern Sie es so, wie Sie es später im FMC verwenden.

Bestätigen Sie das Kennwort, und wählen Sie dann Erstellen aus.



Beispiel für pxGrid-Zertifikatgenerierung.

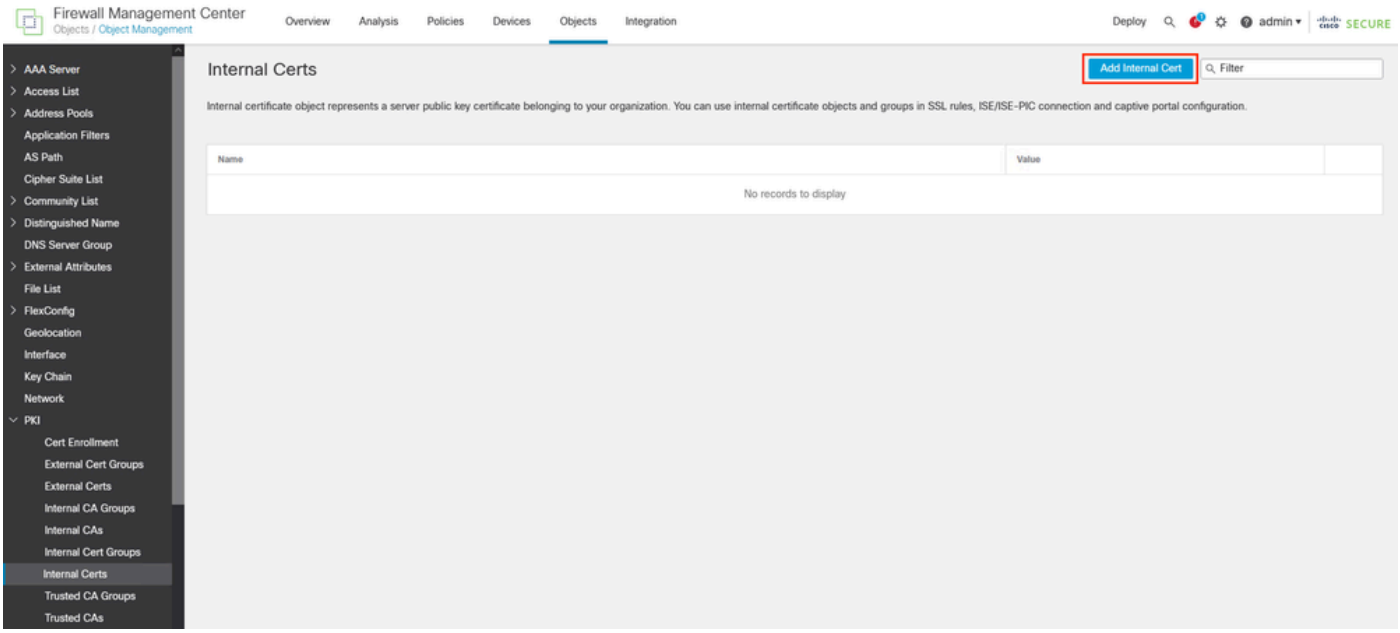
Schritt 2. Eine ZIP-Datei wird auf Ihren Computer heruntergeladen. Dekomprimieren Sie die Datei, und vergewissern Sie sich, dass Sie die folgenden Dateien in Ihrer Umgebung installiert haben:



Von ISE generierte PxGrid-Zertifikate.

Schritt 3: Navigieren Sie im FMC zum Menü Objekte > Objektverwaltung > PKI > Interne Zertifikate.

Wählen Sie die Option Internes Zertifikat hinzufügen aus.



FMC-Zertifikat als internes Zertifikat hinzugefügt.

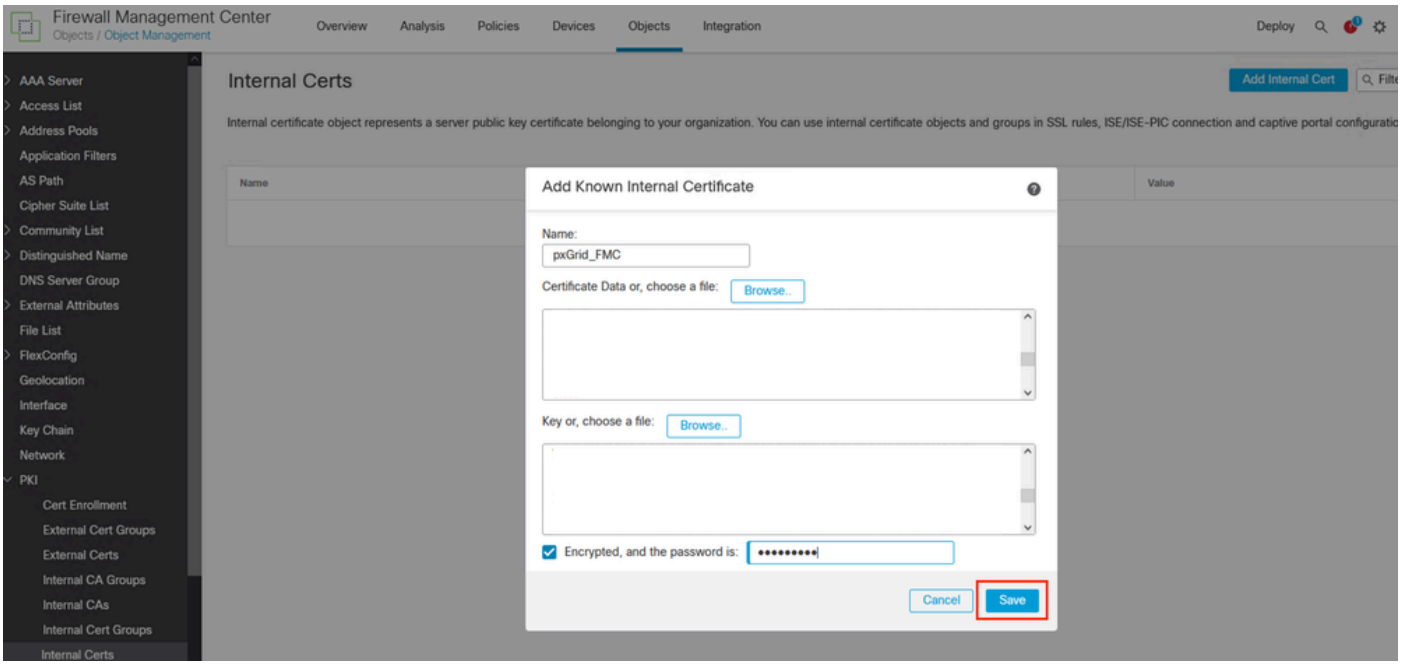
Schritt 4: Nennen Sie das Zertifikat, das auf dem FMC zugewiesen ist.

Durchsuchen Sie das von Ihnen für das FMC von der ISE erstellte Zertifikat im Abschnitt Zertifikatsdaten.

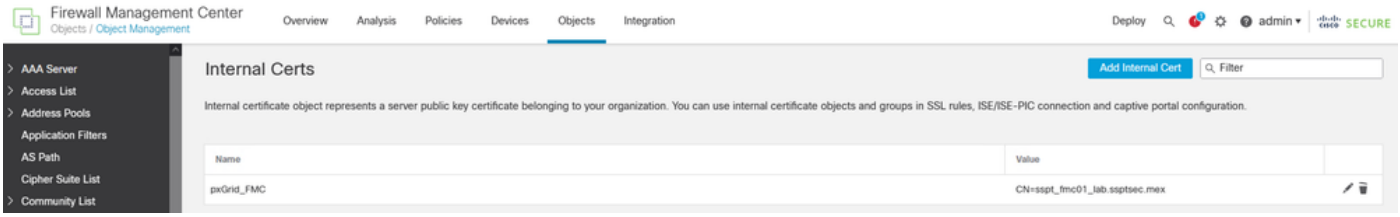
Durchsuchen Sie die Datei mit der Erweiterung .key, um das nächste Feld auszufüllen.

Wählen Sie die Option Verschlüsselt aus, und geben Sie das Kennwort ein, das Sie beim Erstellen des Zertifikats auf der ISE verwendet haben.

Speichern Sie die Konfiguration.



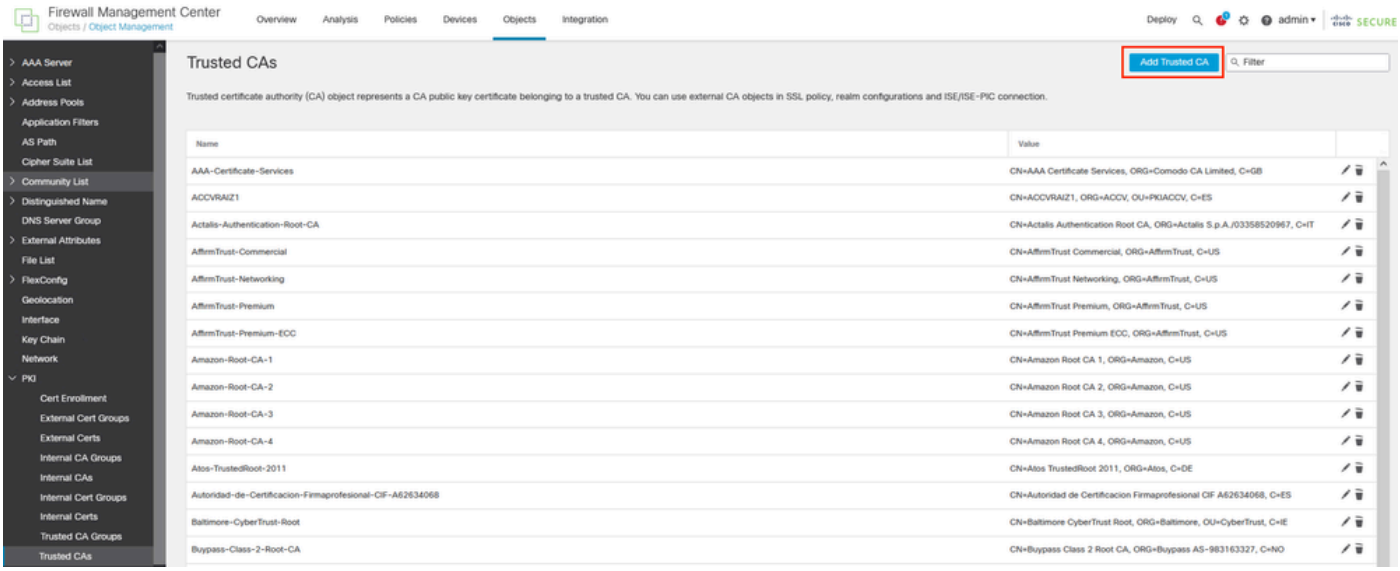
Exportieren des von der ISE generierten FMC-Zertifikats.



FMC-Zertifikat.

Schritt 5: Navigieren Sie zum Menü Objekte > Objektverwaltung > PKI > Vertrauenswürdige Zertifizierungsstellen,

Wählen Sie Vertrauenswürdige Zertifizierungsstellen hinzufügen aus.

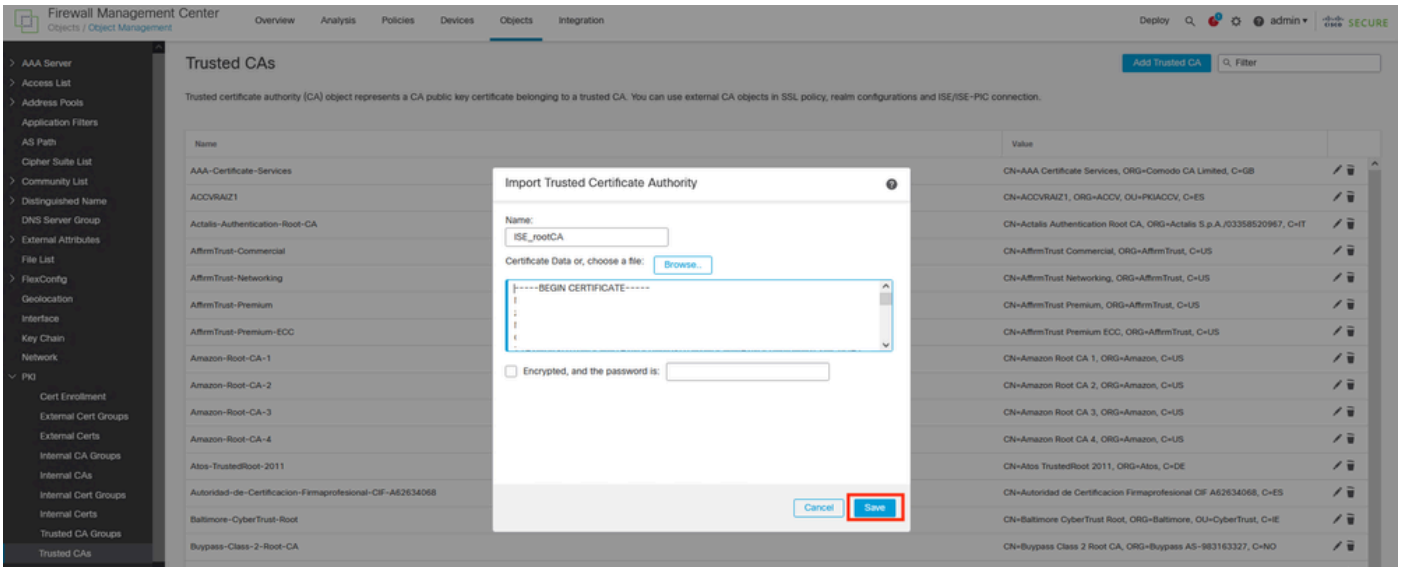


Hinzufügen der ISE-Stammzertifizierungsstelle als vertrauenswürdiges Zertifikat.

Schritt 6: Benennen Sie die Zertifizierungsstelle.

Durchsuchen Sie die ISE-Stammzertifizierungsstelle, die von der ISE-Datei heruntergeladen wurde, und wählen Sie sie aus.

Speichern Sie Ihre Konfiguration.



Exportieren der ISE-Stammzertifizierungsstelle.

Schritt 7: Navigieren Sie zum Menü Integration > Weitere Integrationen > Identitätsquellen.

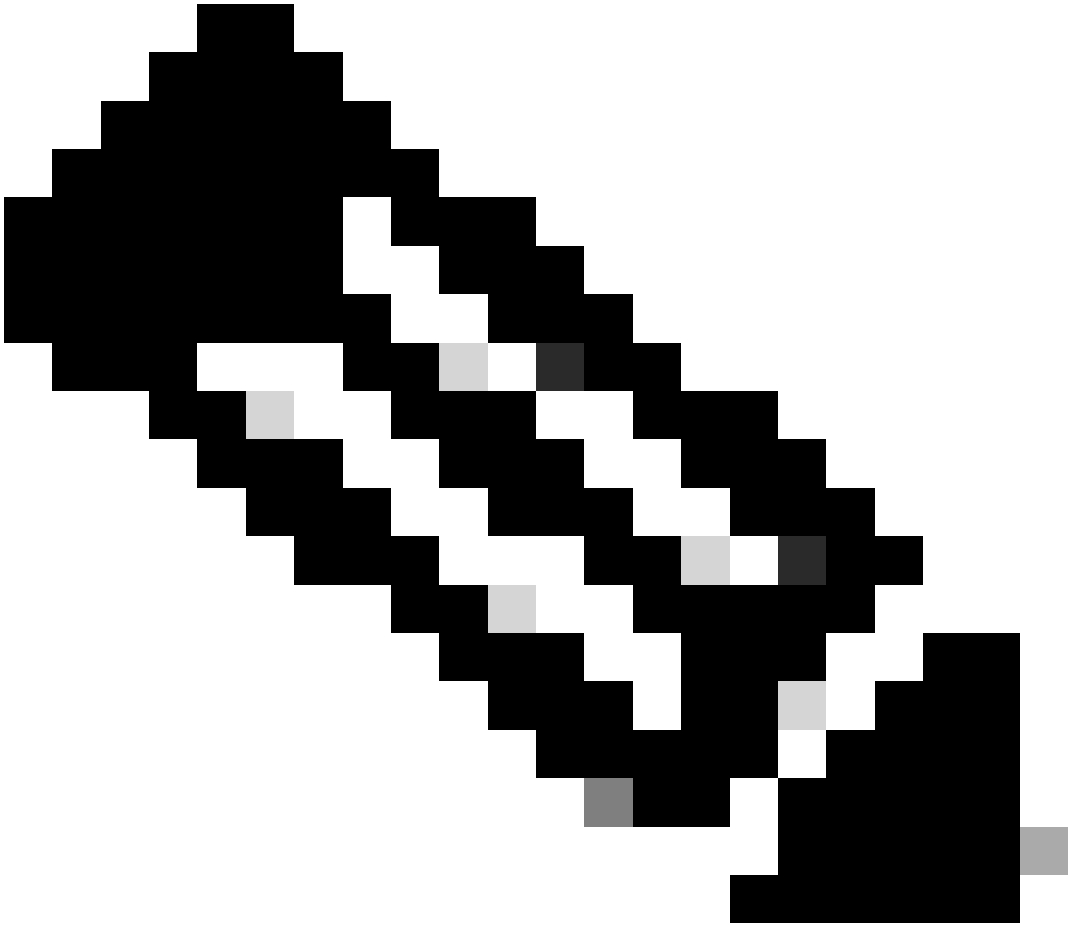
Wählen Sie unter Servicetyp: Identity Services Engine,

Geben Sie die IP-Adresse oder den FQDN des pxGrid-Knotens ein, der zum primären Knoten wird.

Wiederholen Sie den Vorgang für den sekundären pxGrid-Knoten.

Wählen Sie aus dem Dropdown-Menü das von ISE generierte pxGrid-Zertifikat für den Abschnitt pxGrid-Client-Zertifikat aus.

Wählen Sie im Abschnitt MNT Server CA und pxGrid Server CA die ISE-Stammzertifizierungsstelle aus, die Sie im letzten Schritt exportiert haben.

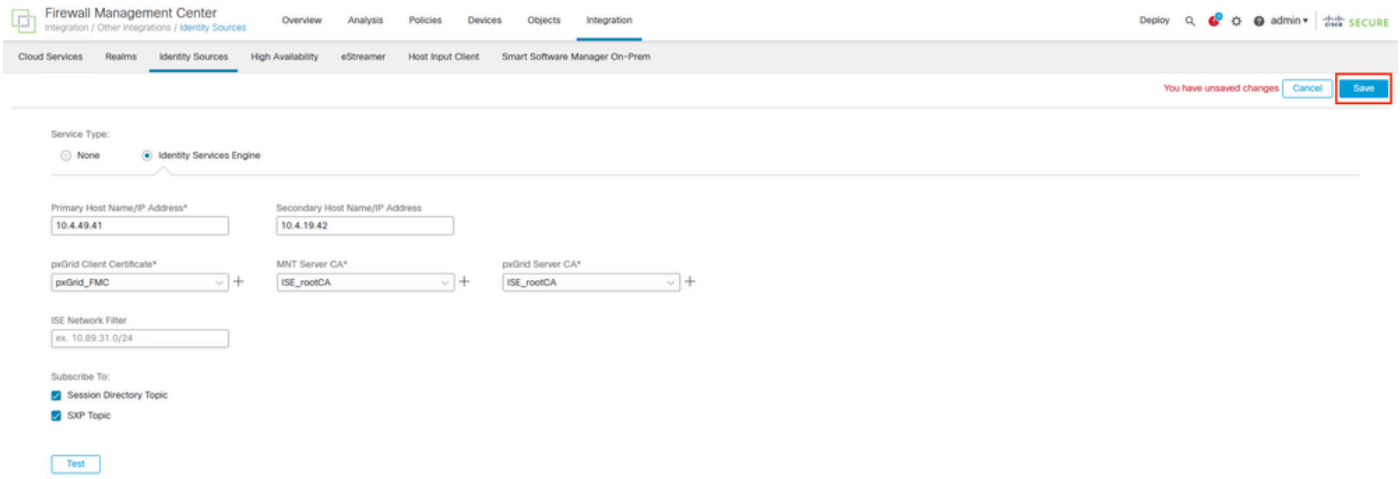


Anmerkung: Die pxGrid Server-CA entspricht der Stammzertifizierungsstelle des Zertifikats, das von pxGrid auf den pxGrid-Knoten verwendet wird.

Die MNT Server CA entspricht der Certificate Authority des Zertifikats, das von pxGrid auf den MNT-Knoten verwendet wird.

(Optional) Sie können das Sitzungsverzeichnis und das SXP-Thema von der ISE abonnieren.

Speichern Sie die Konfiguration.

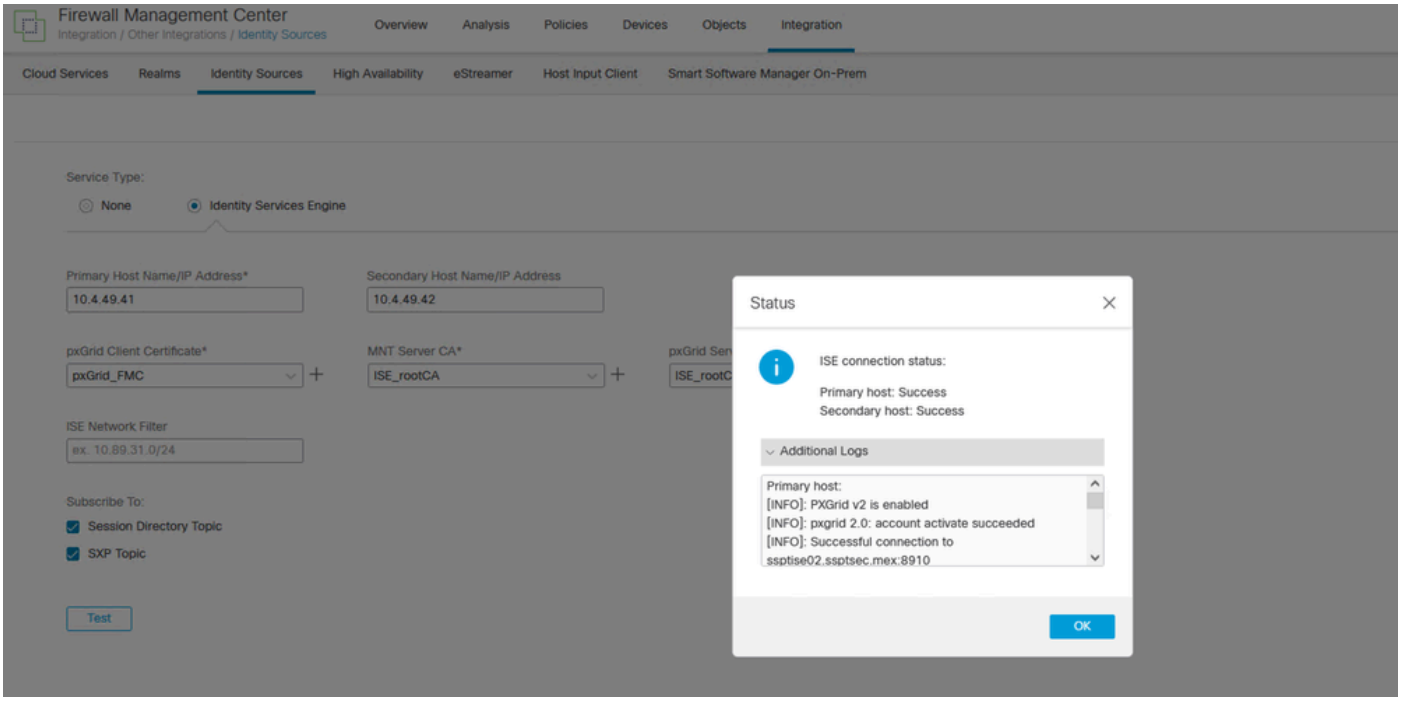


Einrichten der ISE als Identitätsquelle in FMC

Überprüfung.

Validierung auf FMC

Navigieren Sie im Menü zu Integration > Other Integrations > Identity Sources > Identity Services Engine, bevor Sie Ihre Konfiguration speichern. Sie können die Einstellungen für den pxGrid-Link testen.



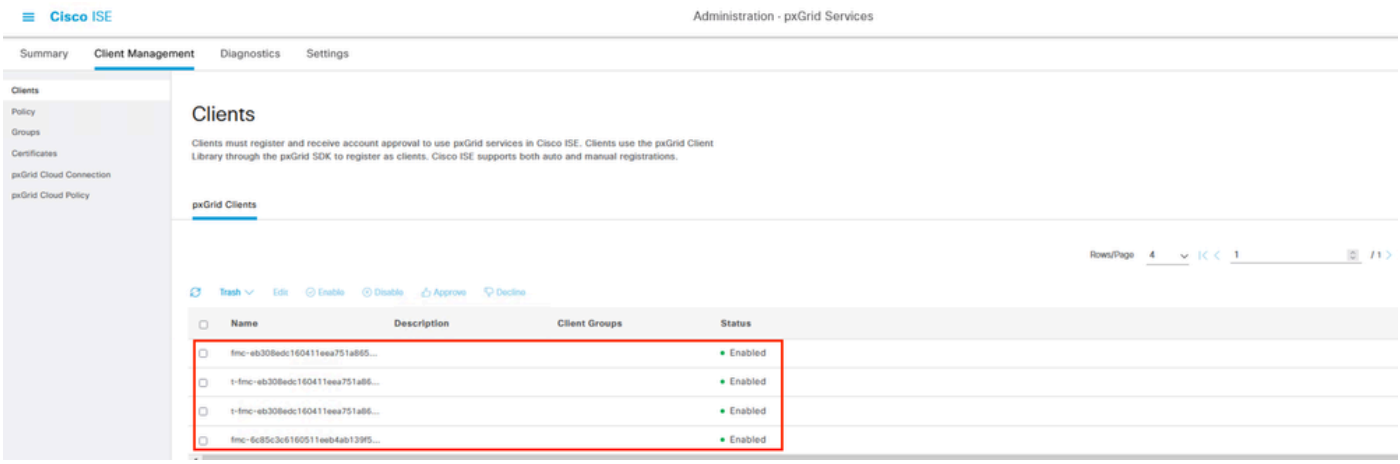
PxGrid-Kommunikation erfolgreich.

```
Primary host:

[INFO]: PXGrid v2 is enabled
[INFO]: pxgrid 2.0: account activate succeeded
[INFO]: Successful connection to ssptise02.ssptsec.mex:8910
[INFO]: Successful connection to ssptise01.ssptsec.mex:8910
```

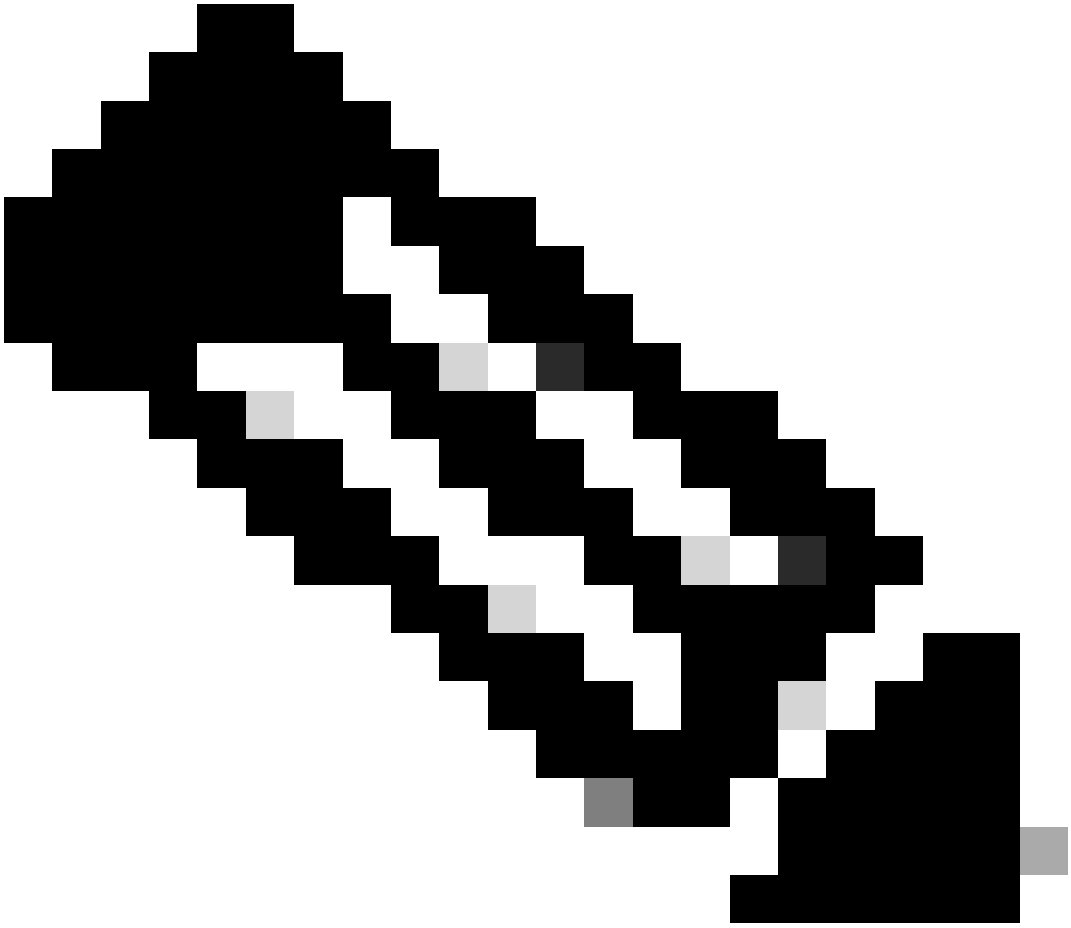
```
[INFO]: These ISE Services are up: SessionDirectory, SXP, EndpointProfile, SecurityGroups, AdaptiveNetw
[INFO]: All requested ISE Services are online.

Secondary host:

[INFO]: PXGrid v2 is enabled
[INFO]: pxgrid 2.0: account activate succeeded
[INFO]: Successful connection to ssptise02.ssptsec.mex:8910
[INFO]: Successful connection to ssptise01.ssptsec.mex:8910
[INFO]: These ISE Services are up: SessionDirectory, SXP, EndpointProfile, SecurityGroups, AdaptiveNetw
[INFO]: All requested ISE Services are online.
```

Validierung auf der ISE

Wenn der FMC pxGrid-Client erfolgreich in die ISE integriert wurde, Sie siehe dann (im Administration > pxGrid Services > Client-Verwaltung > Clients-Menü) Clients mit dem Namen fmc sind enthalten und aktiviert.



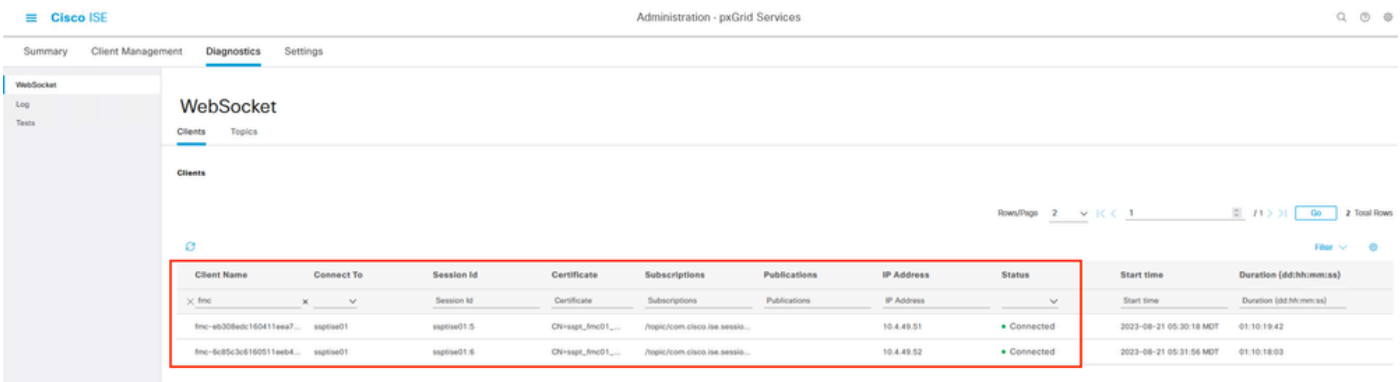
PxGrid-Clients verfügbar und aktiviert.



Anmerkung: Die pxGrid-Clients, deren Präfix mit "t-fmc" beginnt, werden über die Testtaste vom FMC verwendet.

Darüber hinaus Wenn Sie zum Menü Administration > pxGrid Services > Diagnostics > WebSocket navigieren, sehen Sie dann die Verbindungs in Richtung FMC

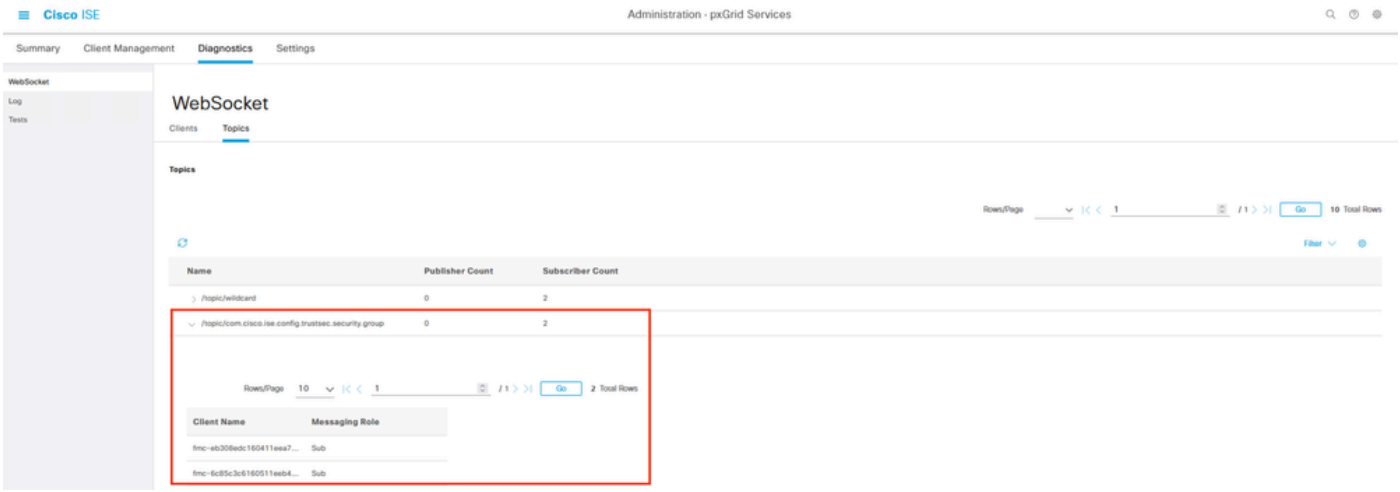
Im Szenario, in dem das FMC hohe Verfügbarkeit, sehen Sie dann die primäre und sekundäre Einheit, wie sie in diesem Beispiel angezeigt wird:



WebSockets sind auf der ISE verfügbar.

Auf der nächsten Registerkarte aus diesem Menü genannt TThemen, können Sie überprüfen Sie, ob die FMC-Abonnenten zu den von der ISE veröffentlichten pxGrid-Themen hinzugefügt wurden.

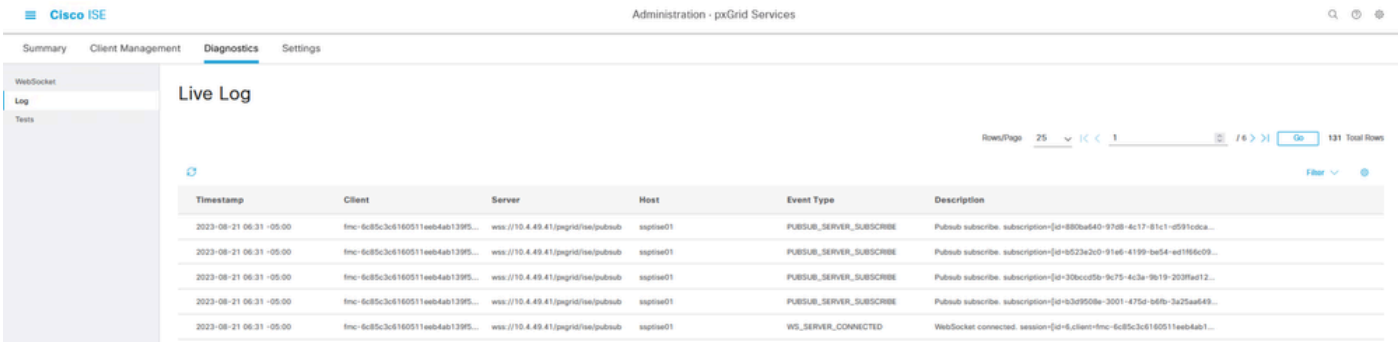
Zum Beispiel gibt es das Thema zur Sicherheitsgruppe von Dabei gilt Sie kann erkennen, dass beide FMC abonniert werden und Informationen erhalten, zu SGT veröffentlicht von ISE.



Themen pro pxGrid-Abonnent.

IIm Menü Administration > pxGrid Services > Diagnostics > Log, wichtige Ereignisse in pxGrid-Kommunikation (für die Knoten mit aktivierter Funktion) werden angezeigt.

Diese stellen die Informationen zur Integration dar.



PxGrid-Live-Protokolle.

Fehlerbehebung

Fehlerbehebung auf FMC

Bestätigen Sie, dass FMC in der Lage ist, seinen eigenen Hostnamen und ISE-Knoten nach Hostnamen aufzulösen.

Beispiele:

<#root>

```
> expert
admin@sspt_fmc01_lab:~$ ping sspt_fmc01_lab

PING sspt_fmc01_lab (10.4.49.51) 56(84) bytes of data.
64 bytes from sspt_fmc01_lab (10.4.49.51): icmp_seq=1 ttl=64 time=0.029 ms
64 bytes from sspt_fmc01_lab (10.4.49.51): icmp_seq=2 ttl=64 time=0.071 ms
64 bytes from sspt_fmc01_lab (10.4.49.51): icmp_seq=3 ttl=64 time=0.055 ms
^C
--- sspt_fmc01_lab ping statistics ---
```

3 packets transmitted, 3 received,

```
 0% packet loss, time 27ms

admin@sspt_fmc01_lab:~$ ping ssptise01
PING ssptise01.ssptsec.mex (10.4.49.41) 56(84) bytes of data.
64 bytes from ssptise01.ssptsec.mex (10.4.49.41): icmp_seq=1 ttl=64 time=0.586 ms
64 bytes from ssptise01.ssptsec.mex (10.4.49.41): icmp_seq=2 ttl=64 time=0.646 ms
64 bytes from ssptise01.ssptsec.mex (10.4.49.41): icmp_seq=3 ttl=64 time=0.743 ms
^C
--- ssptise01.ssptsec.mex ping statistics ---
```

3 packets transmitted, 3 received,

```
 0% packet loss, time 82ms
rtt min/avg/max/mdev = 0.586/0.658/0.743/0.068 ms
admin@sspt_fmc01_lab:~$
admin@sspt_fmc01_lab:~$ ping ssptise02

PING ssptise02.ssptsec.mex (10.4.49.42) 56(84) bytes of data.
64 bytes from ssptise02.ssptsec.mex (10.4.49.42): icmp_seq=1 ttl=64 time=0.588 ms
64 bytes from ssptise02.ssptsec.mex (10.4.49.42): icmp_seq=2 ttl=64 time=0.609 ms
64 bytes from ssptise02.ssptsec.mex (10.4.49.42): icmp_seq=3 ttl=64 time=0.628 ms
^C
--- ssptise02.ssptsec.mex ping statistics ---
```

3 packets transmitted, 3 received

```
, 0% packet loss, time 45ms
rtt min/avg/max/mdev = 0.588/0.608/0.628/0.025 ms
```

Stellen Sie Folgendes sicher Der ADI-Prozess ist aktiv:

<#root>

```
>
```

expert

```
sudo suadmin@sspt_fmc01_lab:~$
```

sudo su

```
root@sspt_fmc01_lab:/Volume/home/admin#
```

pmtool status | grep adi

adi (normal) - Running 7911

OKommunikation von FMC zu ISE sicherstellen am SchlechtDie Verwendung von TCPP 8910 ist zulässig. Von FMC CLI können wir konfigurieren a TCPpudump Paketerfassung zur Bestätigung der bidirektionalen Kommunikation.

<#root>

>

expert

sudo suadmin@sspt_fmc01_lab:~$

sudo su

root@sspt_fmc01_lab:/Volume/home/admin#

tcpdump -i any tcp and port 8910

22:34:08.415370 IP

sspt_fmc01_lab.46248 > ssptise01.ssptsec.mex.8910

: Flags [S], seq 3033526171, win 29200, options [mss 1460,sackOK,TS val 2701166399 ecr 0,nop,wscale 7],
22:34:08.415840 IP

ssptise01.ssptsec.mex.8910 > sspt_fmc01_lab.46248

: Flags [S.], seq 3024877968, ack 3033526172, win 28960, options [mss 1460,sackOK,TS val 2268665064 ecr
22:34:08.415894 IP

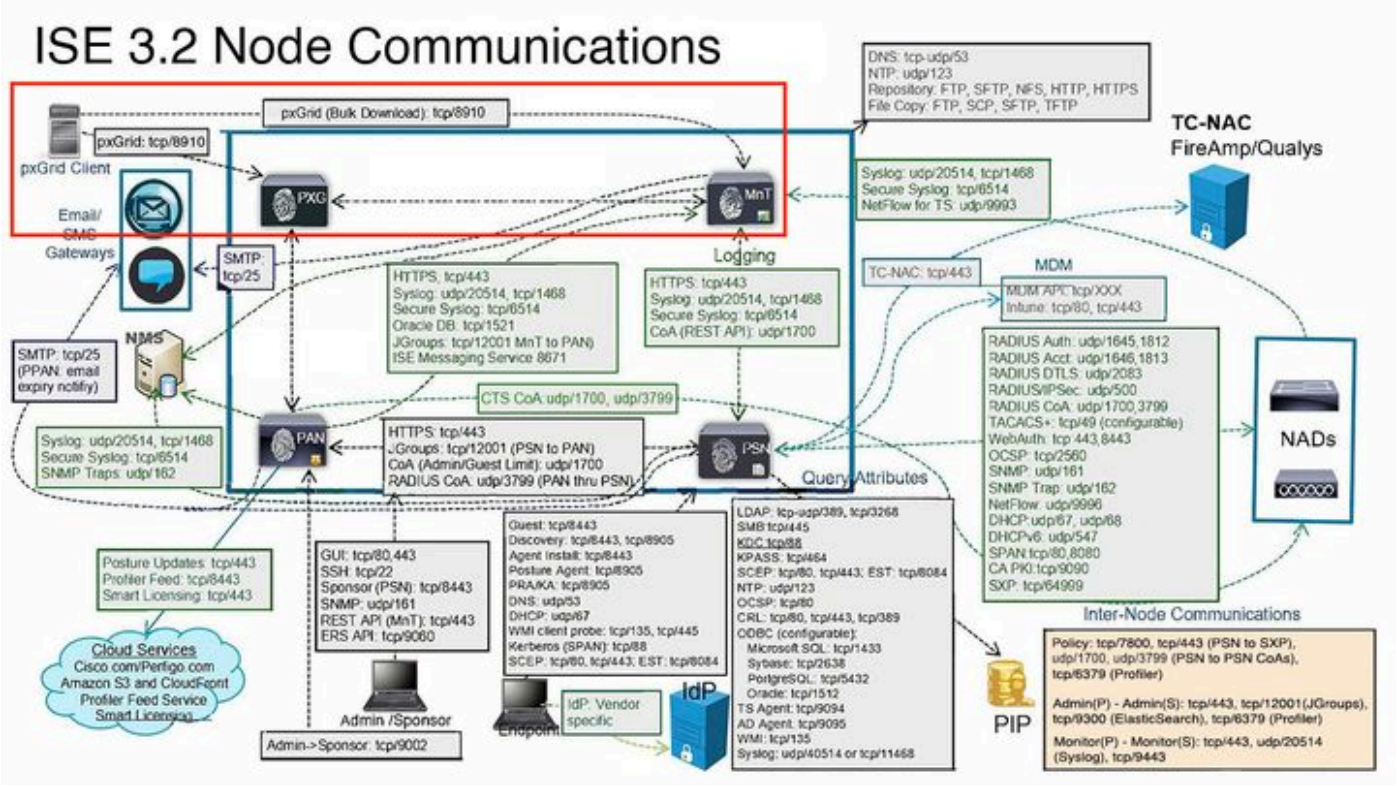
sspt_fmc01_lab.46248 > ssptise01.ssptsec.mex.8910

: Flags [.], ack 1, win 229, options [nop,nop,TS val 2701166400 ecr 2268665064], length 0
[...]

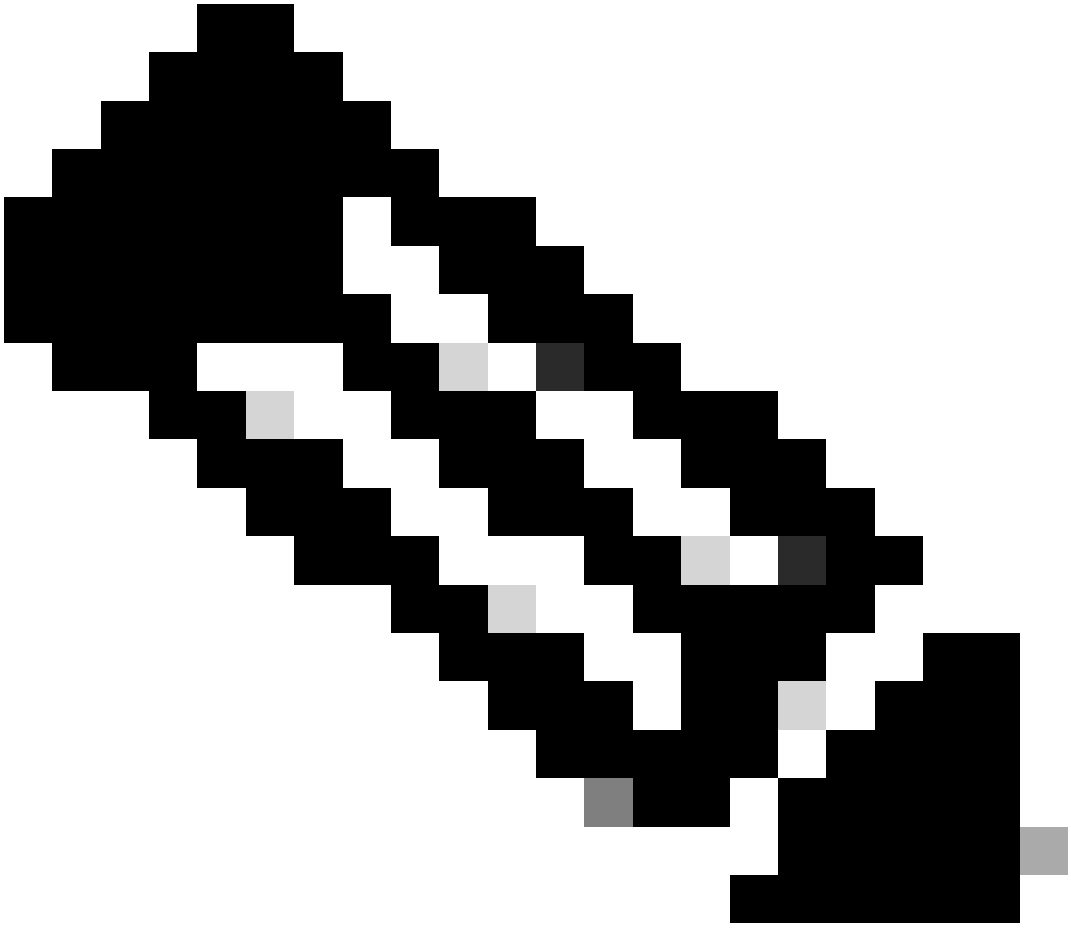
Fehlerbehebung auf der ISE.

Prüfen Sie, ob die Kommunikation an Port 8910 ist betriebsbereit.

Dies ist der Port, der vom pxGrid-Client verwendet wirds zu kommunizieren mit pxGrid-Knoten und MnT-Knoten für den Massen-Download von Informationen.



Interaktion von PxGrid in der ISE-Umgebung.



Anmerkung: Der pxGrid-Client, in diesem Fall kommuniziert das FMC mit den pxGrid-Knoten und dem sekundären MNT (SMNT)-Knoten, um die (Bulk Download) der Informationen zu erhalten, im Falle eines Fehlers in der SMNT sucht es nach den Informationen über die primäre MNT.

IAuf den ISE-Knoten, auf denen die Kommunikation mit dem pxGrid-Client stattfindet, können Sie Wenn die Port ist offen oder wenn Steckdosen angeschlossen sind an diesen Port.

```
#show ports | include 8910
tcp: (output omitted), :::8910,
```

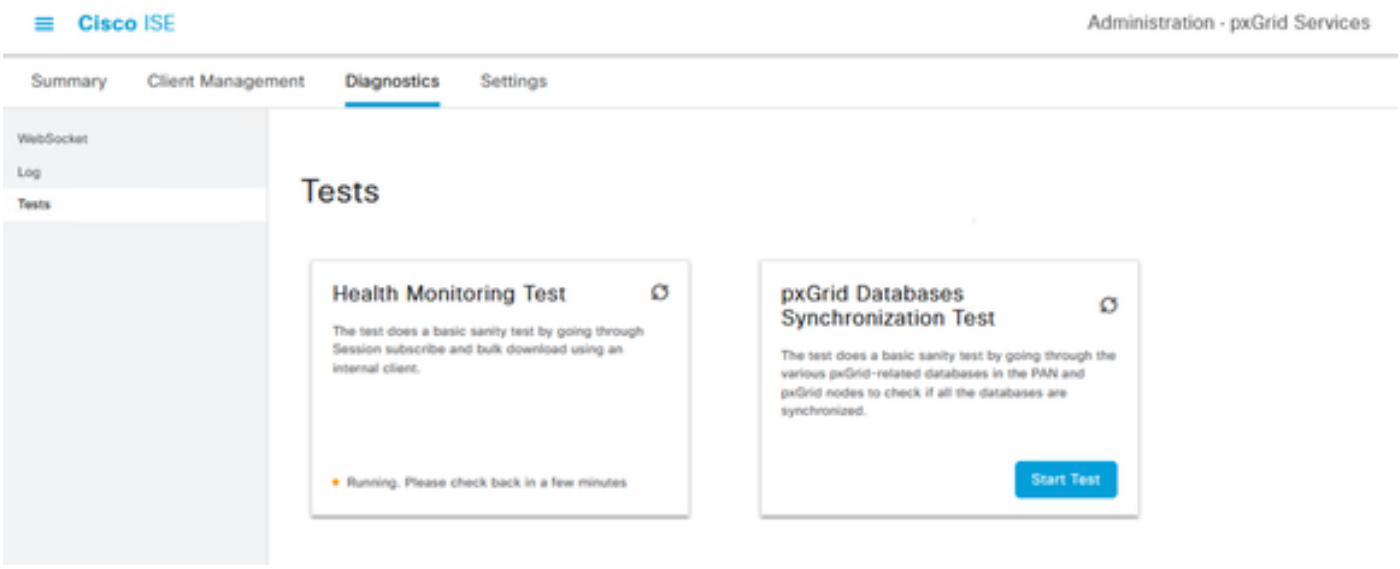
Es stehen 2 Tests auf der ISE zur Verfügung, die den Gesamtstatus der pxGrid-Implementierungen diagnostizieren.

Diese finden Sie im Menü Administration > pxGrid Services > Diagnostics > Test.

Die in diesem Abschnitt angezeigten Tests werden intern auf der ISE durchgeführt.

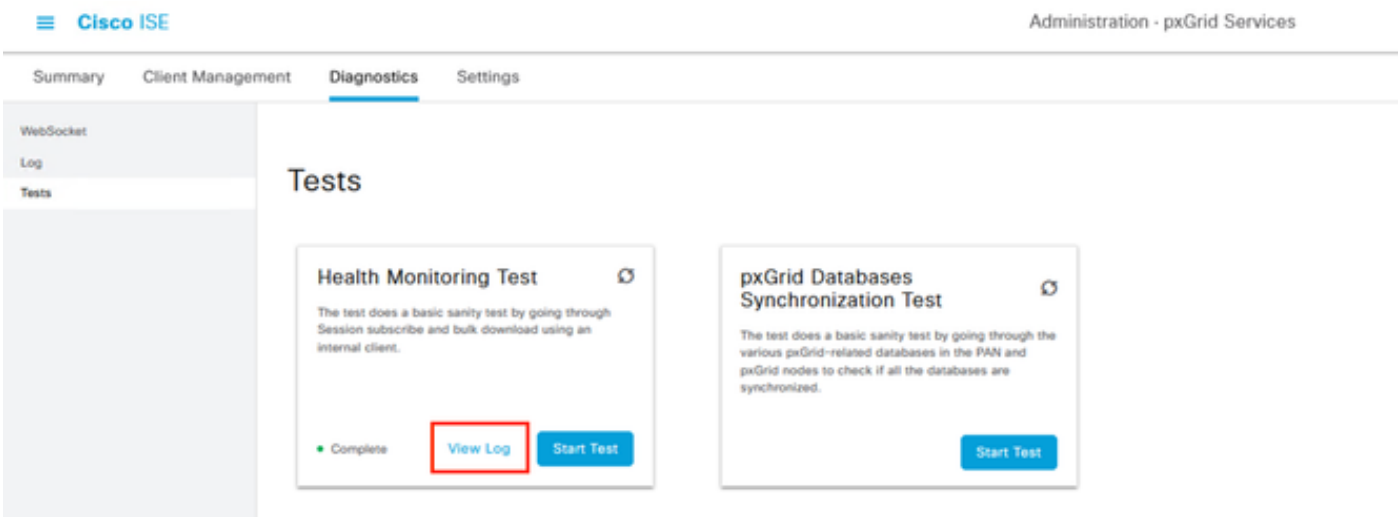
Health Monitoring-Test überprüft das pxGrid-Service-Aussehennach oben, die auswertet, ob ein Client auf das Sitzungsverzeichnis, den Dienst und die vom pxGrid-Controller veröffentlichten Themen zugreifen kann.

Wählen Sie Option Start Test und warten, bis die Protokolle erfasst werden.



PxGrid-Systemüberwachungstest.

Wenn der Test abgeschlossen ist, wählen Sie Option Protokoll anzeigen. In diesem Beispiel wird der Inhalt des Protokolls ist:



Überprüfung des Integritätsüberwachungstests

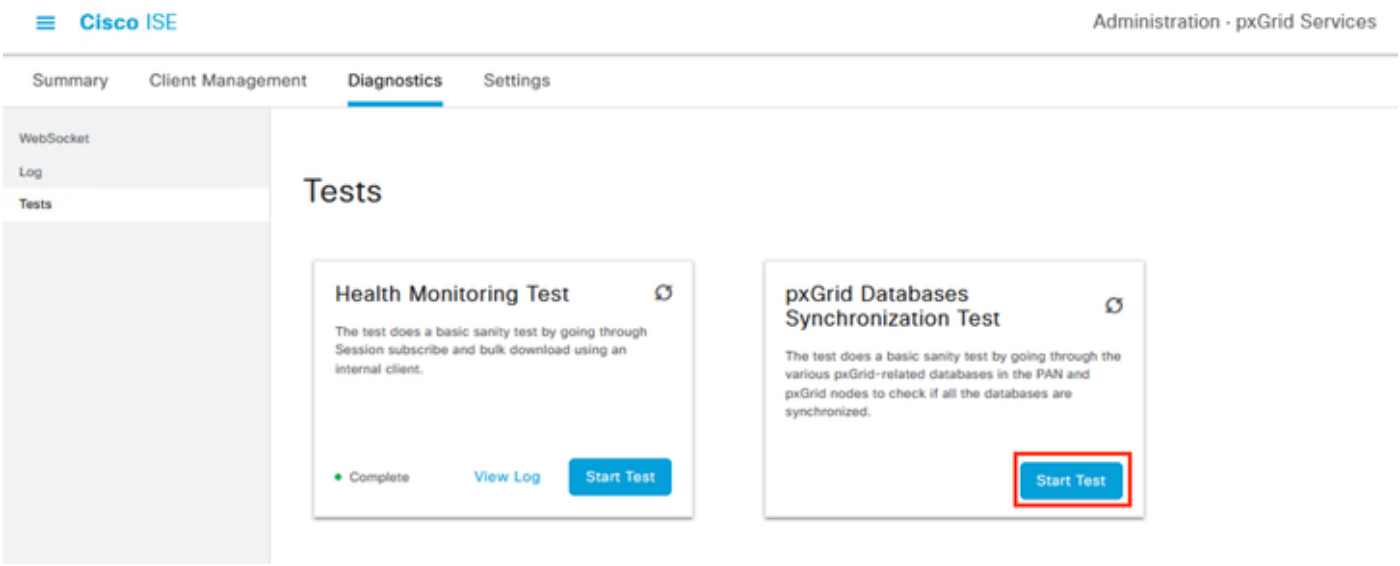
```
22-Aug-2023 17:03:13 [INFO] ************** pxGrid Session Directory Test ***************
22-Aug-2023 17:03:13 [INFO] ----------------- Starting Connection Test -----------------
22-Aug-2023 17:03:14 [INFO] pxGrid Node: ssptise01.ssptsec.mex
22-Aug-2023 17:03:14 [INFO] wsPubsubServiceName=com.cisco.ise.pubsub
22-Aug-2023 17:03:14 [INFO] sessionTopic=/topic/com.cisco.ise.session
22-Aug-2023 17:03:14 [INFO] sessionRestBaseUrl=https://ssptise01.ssptsec.mex:8910/pxgrid/mnt/sd
22-Aug-2023 17:03:14 [INFO] wsUrl=wss://ssptise02.ssptsec.mex:8910/pxgrid/ise/pubsub
```

```
22-Aug-2023 17:03:15 [INFO] ---------------- Connection Test Completed ----------------
22-Aug-2023 17:03:15 [INFO] ------------------ Starting Download Test ------------------
22-Aug-2023 17:03:15 [INFO] Downloading sessions since 2023-08-21T17:03:15.273-06:00
22-Aug-2023 17:03:15 [INFO] Response status=200
22-Aug-2023 17:03:15 [INFO] Number of sessions read: 0
22-Aug-2023 17:03:15 [INFO] ------------------ Download Test Completed ------------------
22-Aug-2023 17:03:15 [INFO] ------------------ Starting Subscribe Test ------------------
22-Aug-2023 17:03:16 [INFO] STOMP CONNECT host=ssptise02.ssptsec.mex
22-Aug-2023 17:03:16 [INFO] STOMP SUBSCRIBE topic=/topic/com.cisco.ise.session
22-Aug-2023 17:03:16 [INFO] STOMP CONNECTED version=1.2
22-Aug-2023 17:07:16 [INFO] A total of 0 notifications were received.
22-Aug-2023 17:07:16 [INFO] STOMP RECEIPT id=77
22-Aug-2023 17:07:19 [INFO] ------------------ Subscribe Test Completed ------------------
22-Aug-2023 17:07:19 [INFO] ********** pxGrid Session Directory Test Complete **********
```

Der PxGrid-Datenbanksynchronisierungstest überprüft, ob die Informationen innerhalb der Datenbanken ist zwischen den PAN-und pxGrid-Knoten korrekt und synchronisiert.

Daher werden die an die pxGrid-Abonnenten gesendeten Informationen genau.

Wählen Sie Option Test starten und warten, bis die Ergebnisse bewertet werden.



Synchronisierungstest für PxGrid-Datenbanken.

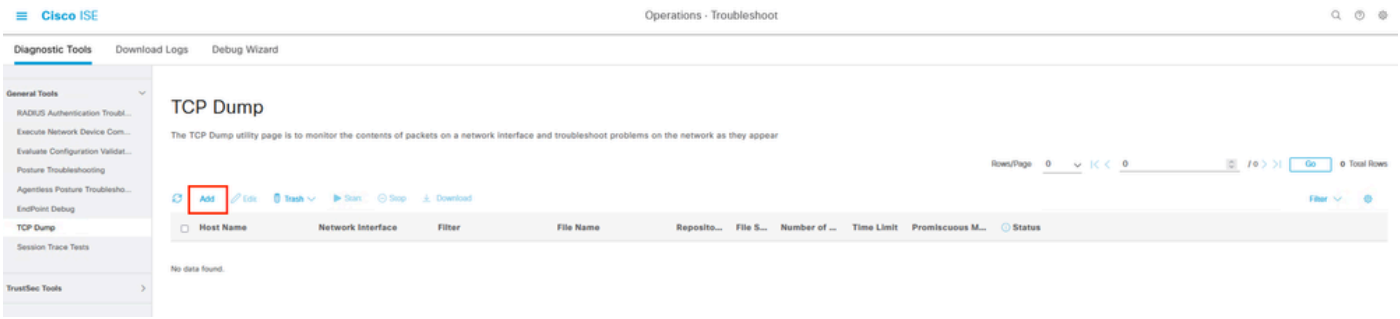
Aus den generierten Protokollen wurde diese Ausgabe abgerufen.

```
ssptise01.ssptsec.mex : In Sync
ssptise02.ssptsec.mex : In Sync

Primary PAN : ssptise01.ssptsec.mex
pxGrid Nodes : ssptise01.ssptsec.mex ssptise02.ssptsec.mex
```

Erfassung erfassen am von den pxGrid-Knoten, die auf den primären FMC-Knoten zeigen.

Zum Menü navigieren Vorgänge > Fehlerbehebung > Diagnosetools > TCP-Dump,

Wählen Sie Option zu Hinzufügen eine neue Erfassung.



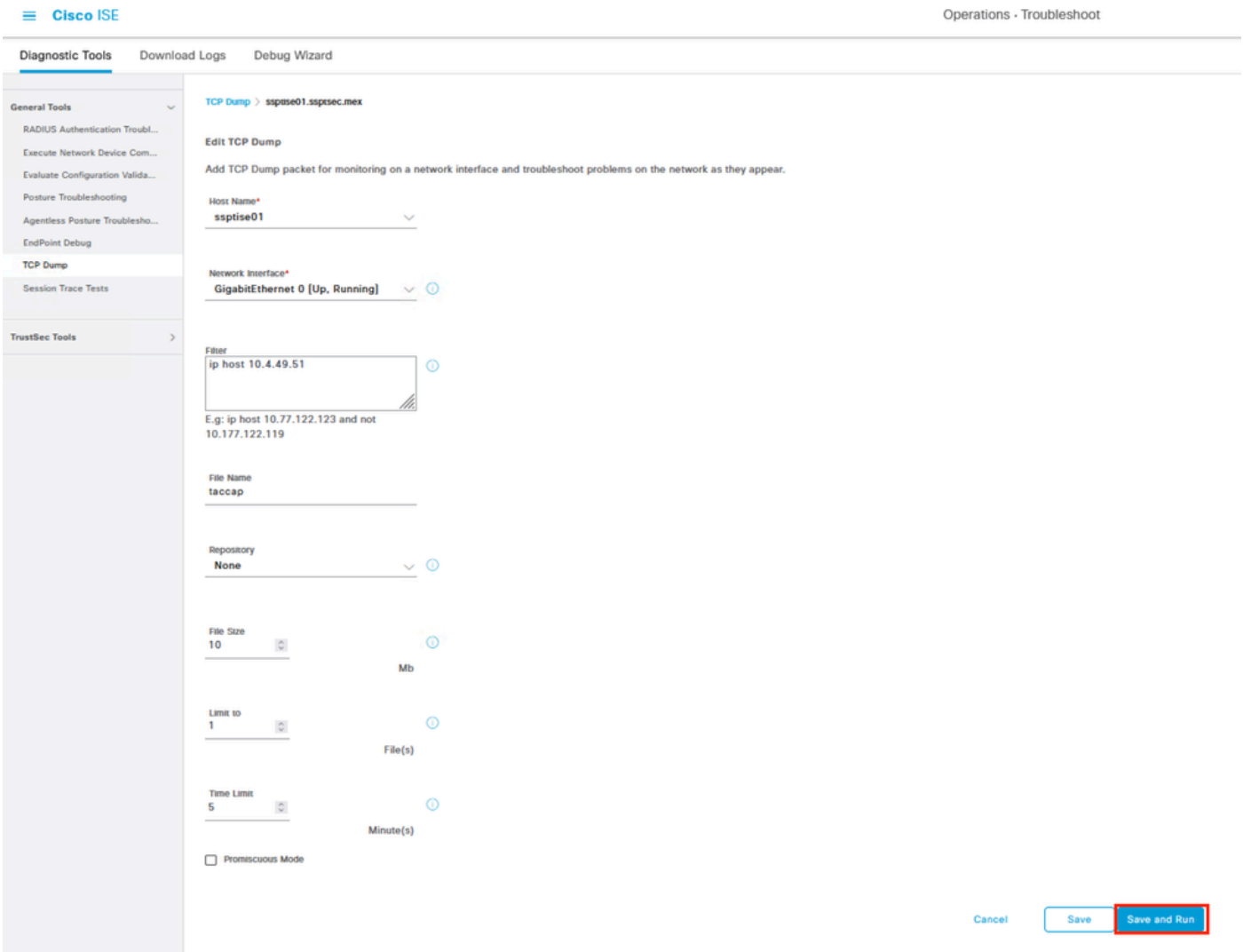
Generieren einer Paketerfassung auf der ISE.

Konfigurieren der Parameter für die Erfassung.

In Host-Name, Wählen Sie den im FMC ausgewählten primären pxGrid-Knoten aus.

Filter den Datenverkehr mit diesem Syntax ip host <FMC IP>

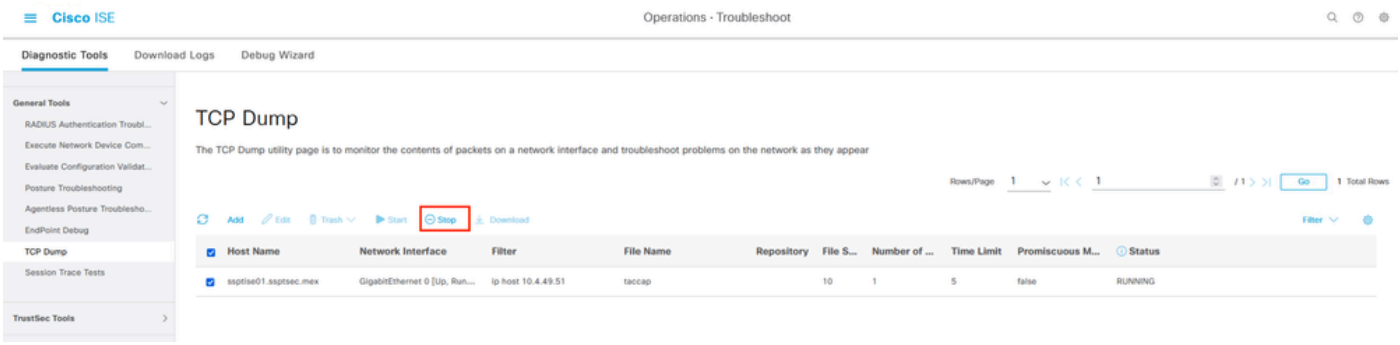
Erfassung benennen und dann fortfahren zu Speichern und ausführen.



Beispiel einer Konfiguration für die Paketerfassung.

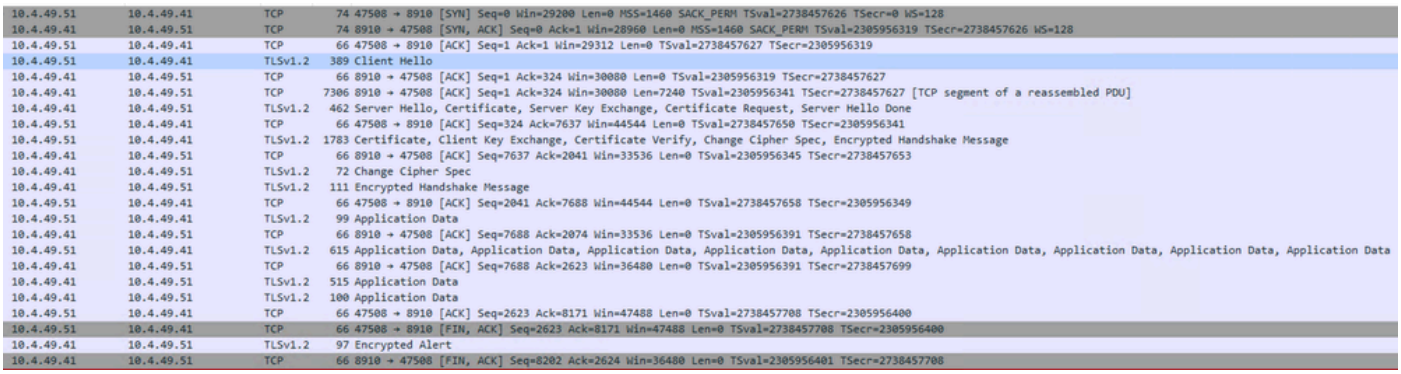
In einem anderen Fenster, im FMC-Menü Integration > Weitere Integrationen > Identität Quellen, Testen Sie die Verbindung mit der ISE über den pxGrid-Kanal.

WWenn das Testergebnis angezeigt wird, fortfahren zu Soberste die Erfassung auf der ISE.



Anhalten einer Paketerfassung auf der ISE.

Herunterladen die Erfassung und den Start der Analyse. In diesem Szenario wird eine Erfassung einer funktionierenden Verbindung angezeigt, die als Referenz dienen kann.

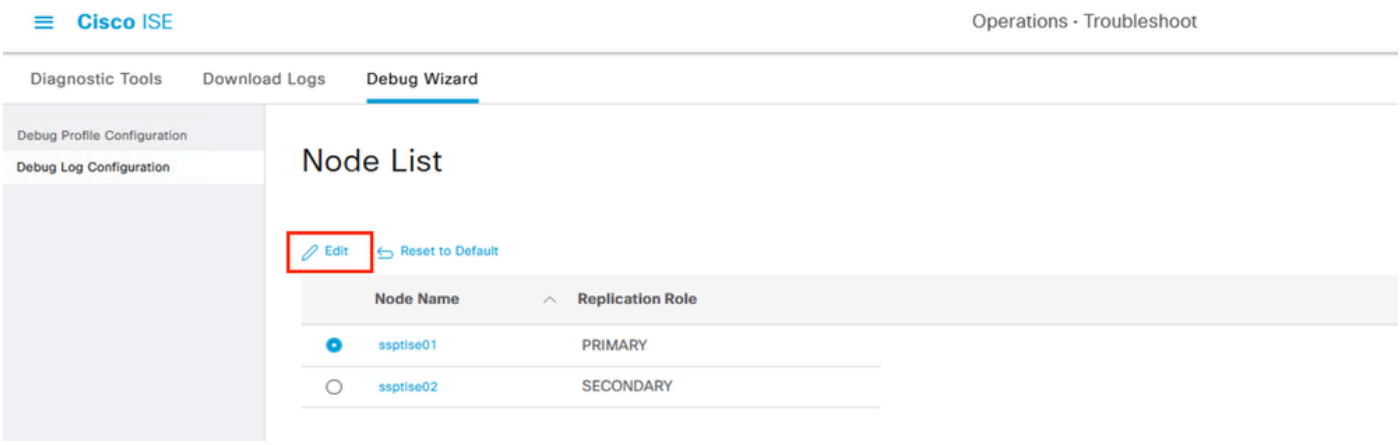


PxGrid-Kommunikation zwischen ISE und FMC

Darüber hinaus können Sie auf der ISE Debug-Meldungen für px sammeln.Grid-Verarbeitung.

Durch das Menü navigieren Vorgänge > Fehlerbehebung > Debug-Assistent > Debuggen Protokollkonfiguration,

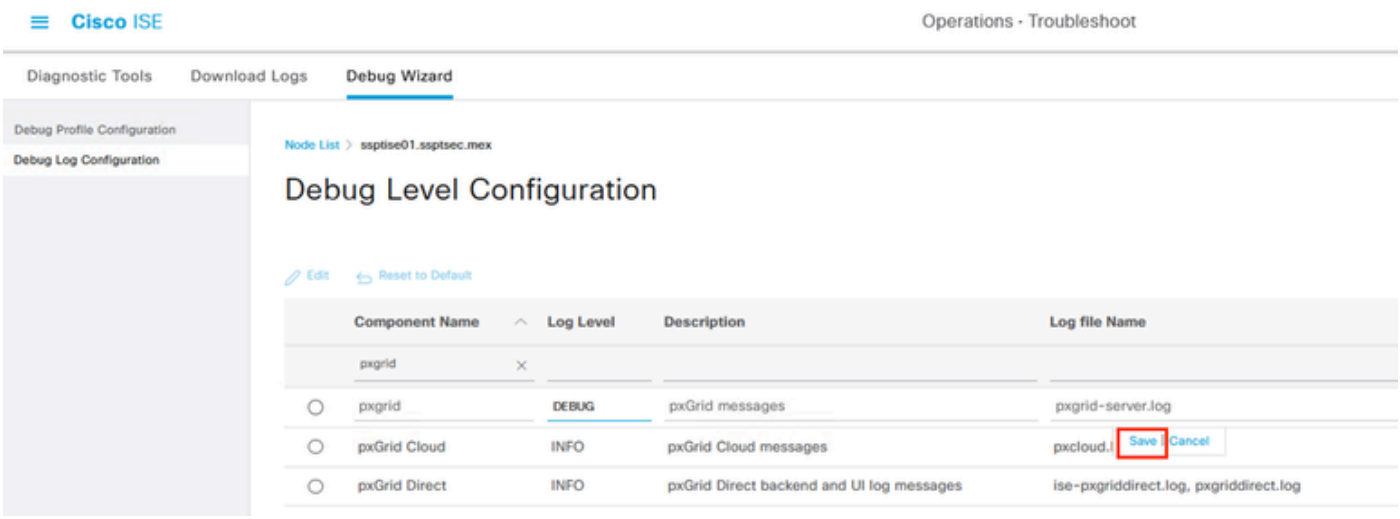
Wählen Sie den entsprechenden ISE-Knoten für die Analyse aus, und Bearbeiten.



Auswählen eines Knotens zum Debuggen auf der ISE.

Die angezeigten Komponenten filtern und die Protokollstufe bis DEBUG des pxgrid Komponente zu fortfahren mit einer Analyse.

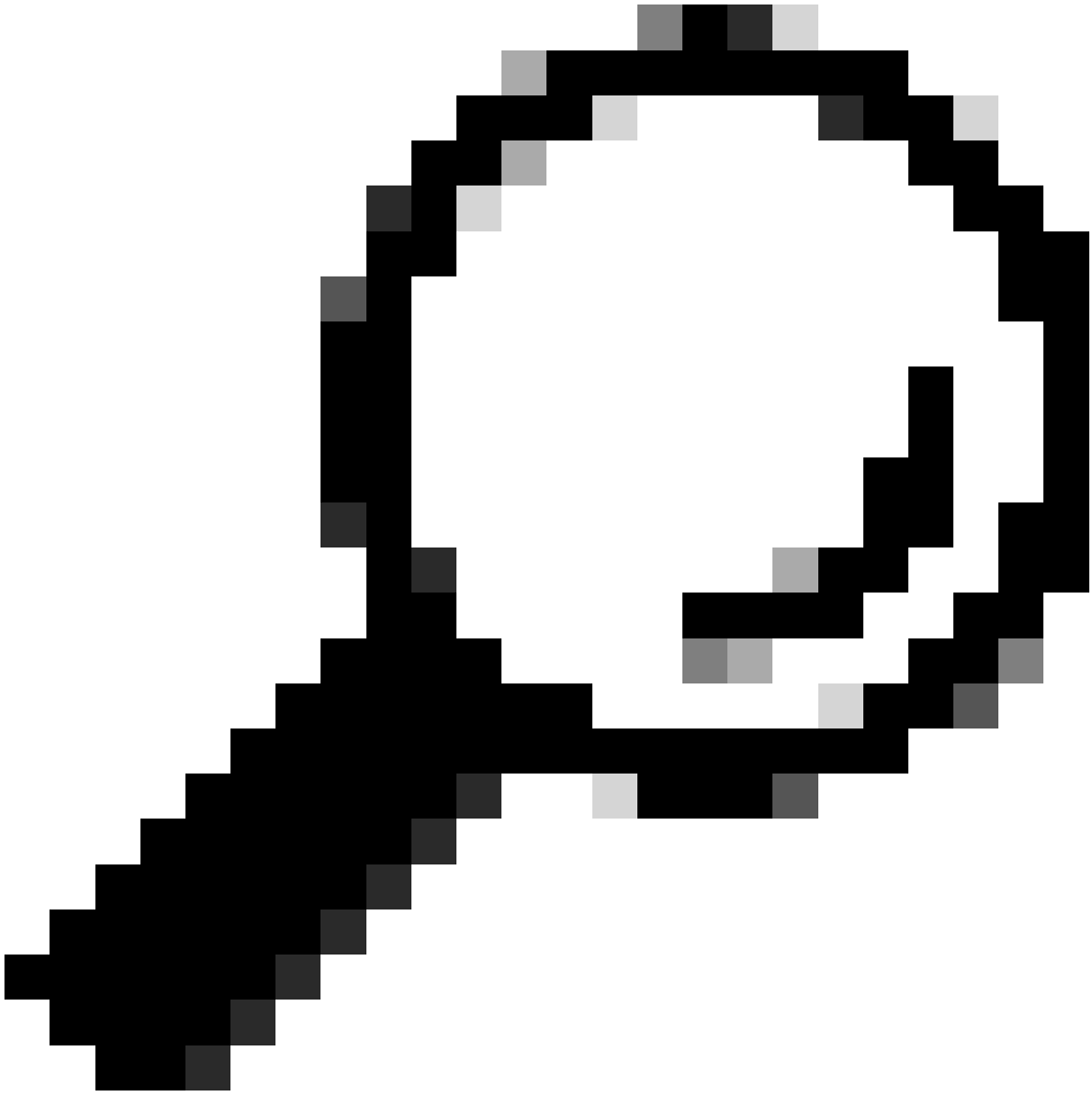
Speichern die Konfiguration.



Ändern der pxGrid-Komponente in die Debugebene.

Wiedergabe des zu analysierenden Verhaltens und anschließende fortfahren , um die in der Datei pxgrid-server.log gesammelten Protokolle zu analysieren. Andere Protokolle die Sie auf dem ISE-Knoten überprüfen können, um Fehler zu beheben, sind:

```
#show logging application | include pxgrid
ise-pxgriddirect.log
pxgrid/pxgrid-server.log
pxgrid/pxgrid-test.log
pxgrid/pxgrid_dbsync_summary.log
pxgrid/pxgrid_internal_dbsync_summary.log
pxgriddirect.log
```

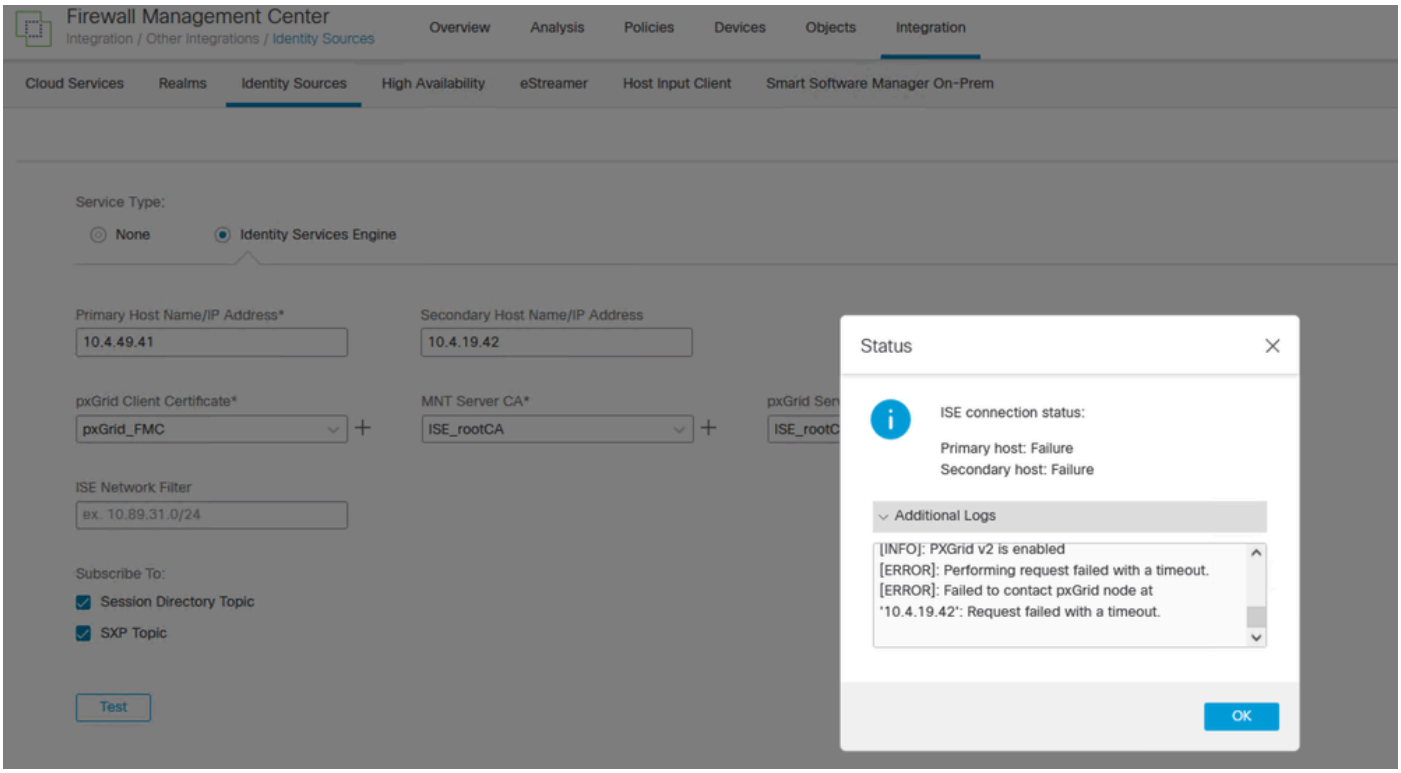


Tipp: Weitere Empfehlungen zur Protokollsammlung finden Sie im Video How to Enable Debugs on ISE 3.x Versions (So aktivieren Sie Debugs auf ISE 3.x-Versionen).

Häufige Probleme.

Der PxGrid-Subscriber-Client ist für die ISE nicht zugelassen.

Für diesen Anwendungsfall zeigt die Ausgabe, die von der FMC-Test-Schaltfläche pxGrid stammt, folgendes Verhalten:



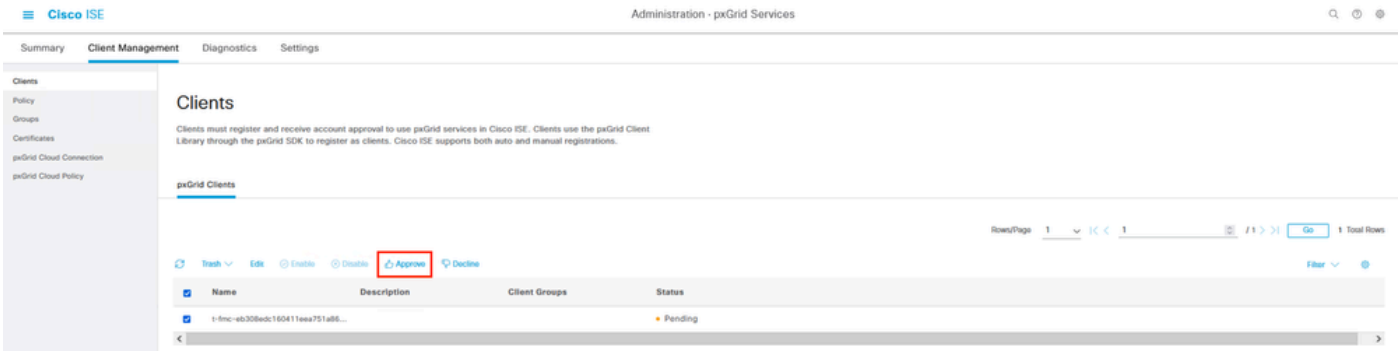
FMC pxGrid-Verbindung fehlgeschlagen.

```
Primary host:

[INFO]: PXGrid v2 is enabled
[ERROR]: pxgrid 2.0: failed account activation. accountState=PENDING
[ERROR]: Failed to contact pxGrid node at '10.4.49.41': pxgrid2.0: Could not activate account

Secondary host:

[INFO]: PXGrid v2 is enabled
[ERROR]: Performing request failed with a timeout.
[ERROR]: Failed to contact pxGrid node at '10.4.19.42': Request failed with a timeout.
```

Beachten Sie auf der ISE das Verhalten im Menü Administration > PxGrid Services > Client Management > Clients, das anzeigt, dass der pxGrid-Client (FMC) zur Genehmigung ansteht.

Klicken Sie auf die Schaltfläche Genehmigen, bestätigen Sie die Auswahl im nächsten Fenster, und wiederholen Sie den Integrationsvorgang.

Dieses Mal ist die Integration erfolgreich.

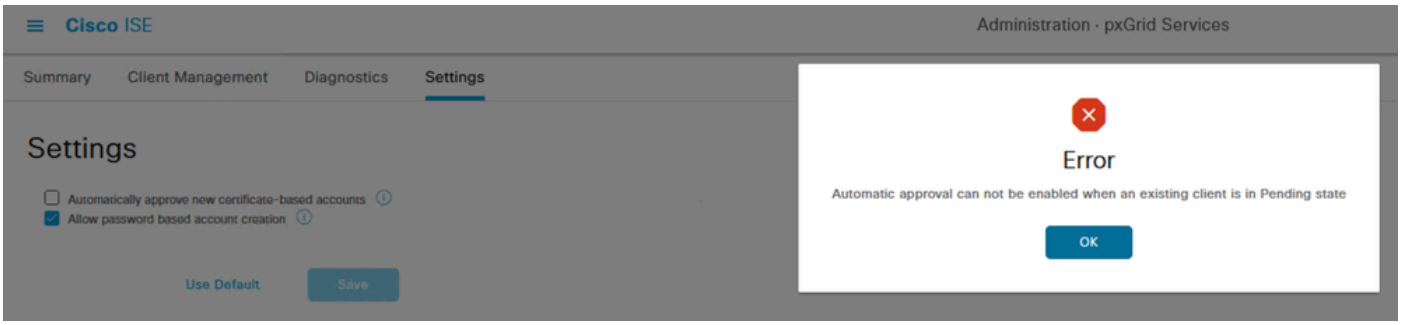


FMC-Client im Status "Ausstehend".

Bestätigung der Genehmigung des pxGrid-Clients.

Beachten Sie, wenn Sie die automatische Genehmigung zertifikatbasierter pxGrid-Clients aktivieren möchten.

Die Clients der vorherigen Seite genehmigen/ablehnen, da dieser Alarm angezeigt werden kann.



Fehler bei der Genehmigung von pxGrid-Clients.

PxGrid ISE-Zertifikat Kette unvollständig.

Wenn Sie in diesem Szenario zum Menü Administration > System > Certificate navigieren, wählen Sie das pxgrid-Zertifikat aus, und wählen Sie die Option View,

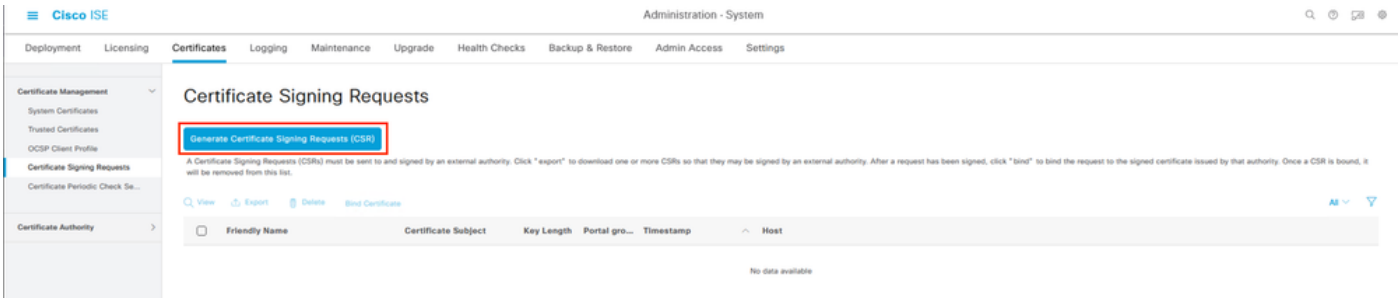
Falls Sie ein Problem mit dem Zertifikat haben, sind diese damit zusammenhängenden Fehler möglich.

Fehler in Bezug auf Zertifikatskette unvollständig.

TDer erste Schritt besteht darin, zu überprüfen, ob die ISE-Stammzertifizierungsstelle abgeschlossen ist.in der Option "Ansicht" beendet.

Wenn ein Zertifikat in der Hierarchie fehlt, können Sie die gesamte ISE-Bereitstellungsroot-Zertifizierungsstelle ausstellen.

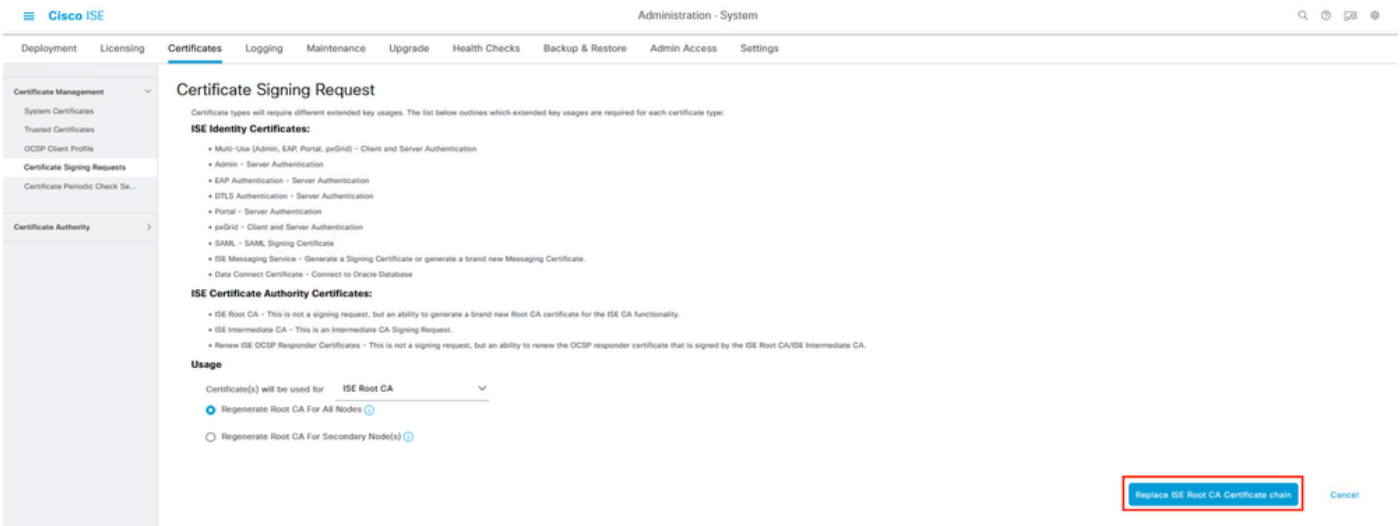
BWechseln Sie zum Menü Administration > System > Certificates > Certificate Management > Certificate Signing Request (CSR) und diese Schaltfläche auswählen.



Erstellen einer CSR-Anfrage auf der ISE.

Wählen Sie in diesem Menü ISE-Stammzertifizierungsstelle verwenden und ISE-Stammzertifizierungsstelle für alle Knoten neu generieren.

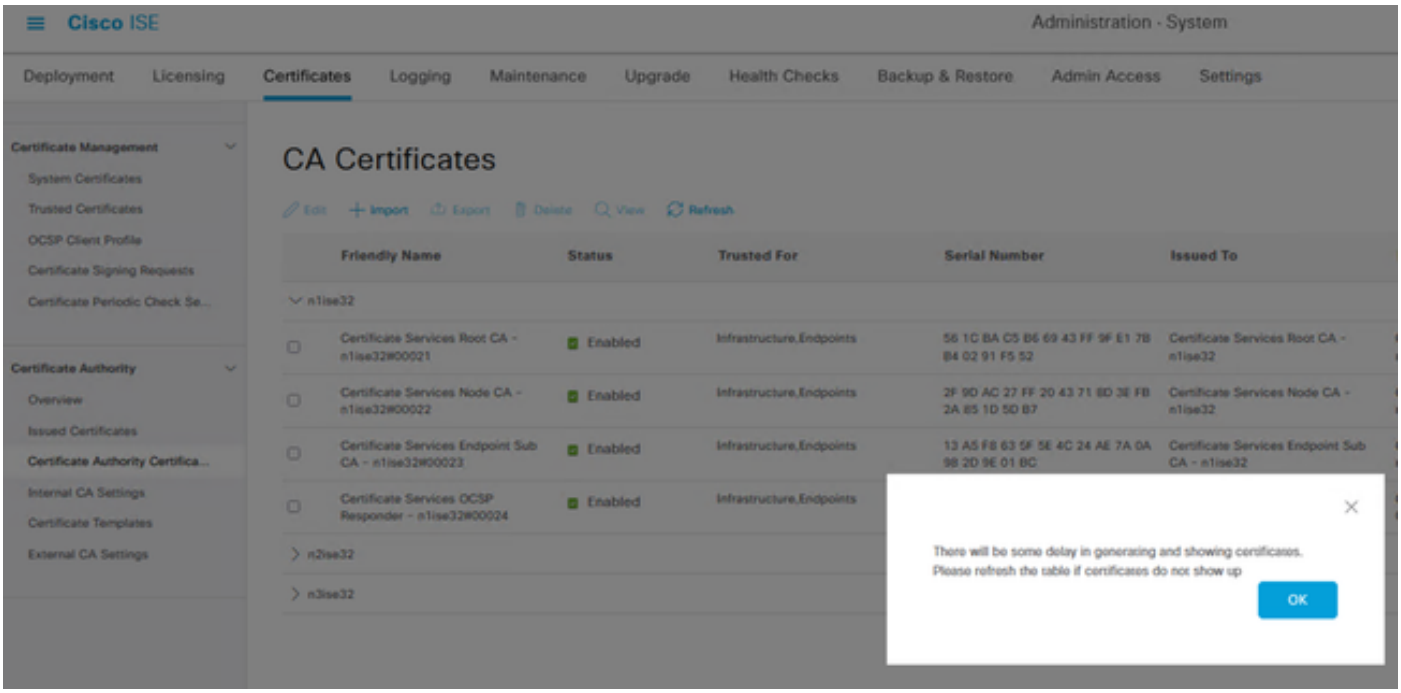
Mit der Schaltfläche fortfahren ISE-Stammzertifizierungsstelle ersetzen.



Konfigurieren der Zertifikatsignierungsanforderung.

Warten Sie, bis die Zertifikate in allen Knoten des Imp generiert werden.Implementierung.

Nach Fertigstellung zeigt die ISE die nächste Benachrichtigung an..



Bestätigung der Erstellung von Zertifikaten.

Bestätigen Sie, ob der pxGDie Zertifikatvertrauenskette des Rid-Zertifikats wurde abgeschlossen. durch Auswahl der Option Ansicht in Systemzertifikaten.

Referenz.

Cisco Developer-Seite zu PxGrid.

Cisco Identity Services Engine - Administratorhandbuch, Version 3.2, Kapitel: Cisco pxGrid

Cisco Identity Services Engine-Installationshandbuch, Version 3.2, Kapitel: Referenz der Cisco ISE-Ports

CLI-Referenzhandbuch zur Cisco Identity Services Engine, Version 2.4

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.