

Configure and Troubleshoot ISE 3.2 with FMC

7.2.4 Integration

Contents

[Introduction](#)

[Prerequisites](#)

[Components Used](#)

[Background Information.](#)

[Configure](#)

[Prepare the ISE for the integration.](#)

[Prepare the FMC for the integration.](#)

[Setting up the pxGrid connection between ISE and FMC.](#)

[Verify.](#)

[Validation on FMC.](#)

[Validation on ISE.](#)

[Troubleshoot](#)

[Troubleshooting on FMC.](#)

[Troubleshooting on ISE.](#)

[Common problems.](#)

[PxGrid subscriber client is not approved on ISE.](#)

[PxGrid ISE certificate chain incomplete.](#)

[Reference.](#)

Introduction

This document describes procedures to integrate Identity Services Engine with Firewall Management Center using Platform Exchange Grid connections.

Prerequisites

Cisco recommends knowledge in these topics:

- Identity Services Engine (ISE)
- Platform Exchange Grid
- Firewall Management Center (FMC)
- TLS/SSL Certificates.

Components Used

The information in this document is based on these software and hardware versions:

- Identity Services Engine (ISE) version 3.2 patch 3
- Firewall Management Center version 7.2.4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information.

This documentation provides a solution to integrate FMC and ISE using pxGrid version 2.

Cisco Firepower Management Center (FMC) is a centralized platform for Next generation Firewall and Intrusions Prevention System, offering policy management, threat detection, and incident response.

Cisco Identity Services Engine is a comprehensive solution that provides secure access to endpoints by providing services of authentication, authorization, and accountability (AAA) and policy enforcement.

Platform Exchange Grid (pxGrid) enables you to interchange information among multivendor, cross-platform network.

This integration enables you to get secure monitoring, detection of threats, and the set network policies based on the information shared.

PxGrid framework has 2 versions. The one to use depends upon the ISE version and patch you need to review.

Starting with version ISE 3.1, all the pxGrid connections from ISE are based on pxgrid version 2.

PxGrid version 1.

The first version of this framework (pxGrid v1) is characterized due to the serviceability that was seen through the command **show application status ise** as it is displayed in the ensuing output.

When pxGrid feature is enabled in the node you see the pxGrid features in a running status.

```
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
```

PxGrid version 1 serviceability.

In this version of this platform, it is known to have only one pxGrid node with the pxGrid processes in

running status while the other pxGrid nodes are in a standby status.

These nodes are constantly monitoring the status of the pxGrid node with related services related running.

In that, the primary pxGrid node there was a promotion and the other pxGrid node enabled their pxGrid services.

However, that represented a downtime when this failover occurred.

The first version of **pxgrid** was based on communication in **Extensible Messaging and Presence Protocol (XMPP)** which is a set of technologies used in collaboration and voice infrastructures.

The topics shared in a pxGrid v1 connection are:

- Session Directory
- Endpoint Profile MetaData
- Trustsec MetaData
- Endpoint Protection Capability
- Adaptive Network Control
- MDM_Offline Topic
- Identity
- SXP

PxGrid version 2.

This document covers the use of PxGrid version 2. This platform operates using REST operations on ISE and WebSocket protocols which brings enhancements, improved scalability, performance, and flexibility in data models.

In this version, you do not see **pxgrid** features running as in previous version with the **command show application status ise**.

Please refer to the validation section for ISE in this document to know which mechanisms to check to review pxGrid functionality.

With this version, you have all the **pxGrid** nodes that you configure as active pxGrid nodes. These are ready to participate in the exchange of information at any time.

In version 1, only one node held the serviceability of pxGrid as running.

The topics shared in a pxGrid v2 connection are:

- Session Directory
- Radius Failure
- Profiler Configuration
- System Health
- MDM
- ANC Status
- TrustSec
- TrustSec Configuration
- TrustSec SXP
- Endpoint Asset.

Components of pxGrid as platform.

PxGrid controller (ISE) : Must trust each of the participants that use pxGrid.

Client: Can be subscriber and publisher of different topics.

Publisher: Client that shares information with the controller.

Subscriber: Client that consumes the information of a topic.

This integration allows you to create content policies on FMC based on the information that is shared by ISE and their published topics (related to the endpoint activity).

Configure

Prepare the ISE for the integration.

Step 1. Configure the ISE node to run the pxGrid persona on it in the menu **Administration > System > Deployment**.

Select the nodes and enable the feature pxGrid.

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE' and 'Administration - System'. Below this is a menu with 'Deployment' selected. The main content area shows the configuration for a node named 'ssptise02'. Under the 'Policy Service' section, the 'Enable Session Services' checkbox is checked. Below this, the 'Include Node in Node Group' dropdown is set to 'None'. Other services listed include 'Enable Profiling Service' (checked), 'Enable Threat Centric NAC Service', 'Enable SXP Service', 'Enable Device Admin Service', and 'Enable Passive Identity Service'. At the bottom, the 'pxGrid' feature is enabled, indicated by a blue toggle switch and a red box around the 'pxGrid' label.

Enabling ISE pxGrid services in a node.

Step 2. After enabling the nodes with the pxGrid feature, review the status of the Websockets related to the connected internal clients.

Navigate to **Administration > pxGrid Services > Websocket**. Notice clients pointing to the ISE services directly through the IP address 127.0.0.1.

Cisco ISE Administration - pxGrid Services

Summary Client Management **Diagnostics** Settings

WebSocket

Log Tests

WebSocket Clients Topics

Clients

Rows/Page 8 1 1 8 Total Rows

Client Name	Connect To	Session Id	Certificate	Subscriptions	Publications	IP Address	Status
-ise-fanout-ssptise01	ssptise01	ssptise01:0	CN=ssptise01.ss...	/topic/wildcard	/topic/com.cisco.ise.pxgrid...	127.0.0.1	Connected
-ise-fanout-ssptise02	ssptise01	ssptise01:1	CN=ssptise02.ss...	/topic/distributed	/topic/distributed	10.4.49.42	Connected
-ise-fanout-ssptise01	ssptise01	ssptise01:2	CN=ssptise01.ss...	/topic/distributed		10.4.49.41	Connected
-ise-fanout-ssptise02	ssptise02	ssptise02:9	CN=ssptise02.ss...	/topic/wildcard	/topic/com.cisco.ise.pxgrid...	127.0.0.1	Connected
-ise-mnt-ssptise02	ssptise02	ssptise02:11	CN=ssptise02.ss...	/topic/com.cisco.ise.sessio...	/topic/com.cisco.ise.sessio...	10.4.49.42	Connected
-ise-admin-ssptise02	ssptise02	ssptise02:12	CN=ssptise02.ss...		/topic/com.cisco.ise.pxgrid...	10.4.49.42	Connected
-ise-mnt-ssptise01	ssptise02	ssptise02:13	CN=ssptise01.ss...	/topic/com.cisco.ise.sessio...	/topic/com.cisco.ise.sessio...	10.4.49.41	Connected
-ise-admin-ssptise01	ssptise02	ssptise02:14	CN=ssptise01.ss...	/topic/com.cisco.ise.pxgrid...	/topic/com.cisco.ise.pxgrid...	10.4.49.41	Connected

Internal WebSockets from ISE.

Step 3. Navigate through the menu **Administration > pxGrid Services > Settings** and select the option to **Automatically approve new certificate-based accounts**,

This step is optional at this point, however, for the pxGrid connection, it is suggested to enable this checkbox.

You can accept the FMC as subscriber manually afterwards.

Cisco ISE Administration - pxGrid Services

Summary Client Management Diagnostics **Settings**

Settings

Automatically approve new certificate-based accounts ⓘ

Allow password based account creation ⓘ

Use Default Save

Enabling Automatic approval for pxGrid certificate based accounts.

Step 4. Review the certificates related to the pxGrid functionality of your environment in **Administration > System > System Certificates**,

It is recommended that you have homogenous pxGrid certificates in all the nodes of your deployment signed by the same root Certificate Authority (CA)

In this scenario, we are using the internal ISE certificates generated. For this version of ISE where in this example, the root CA corresponds to the PAN node.

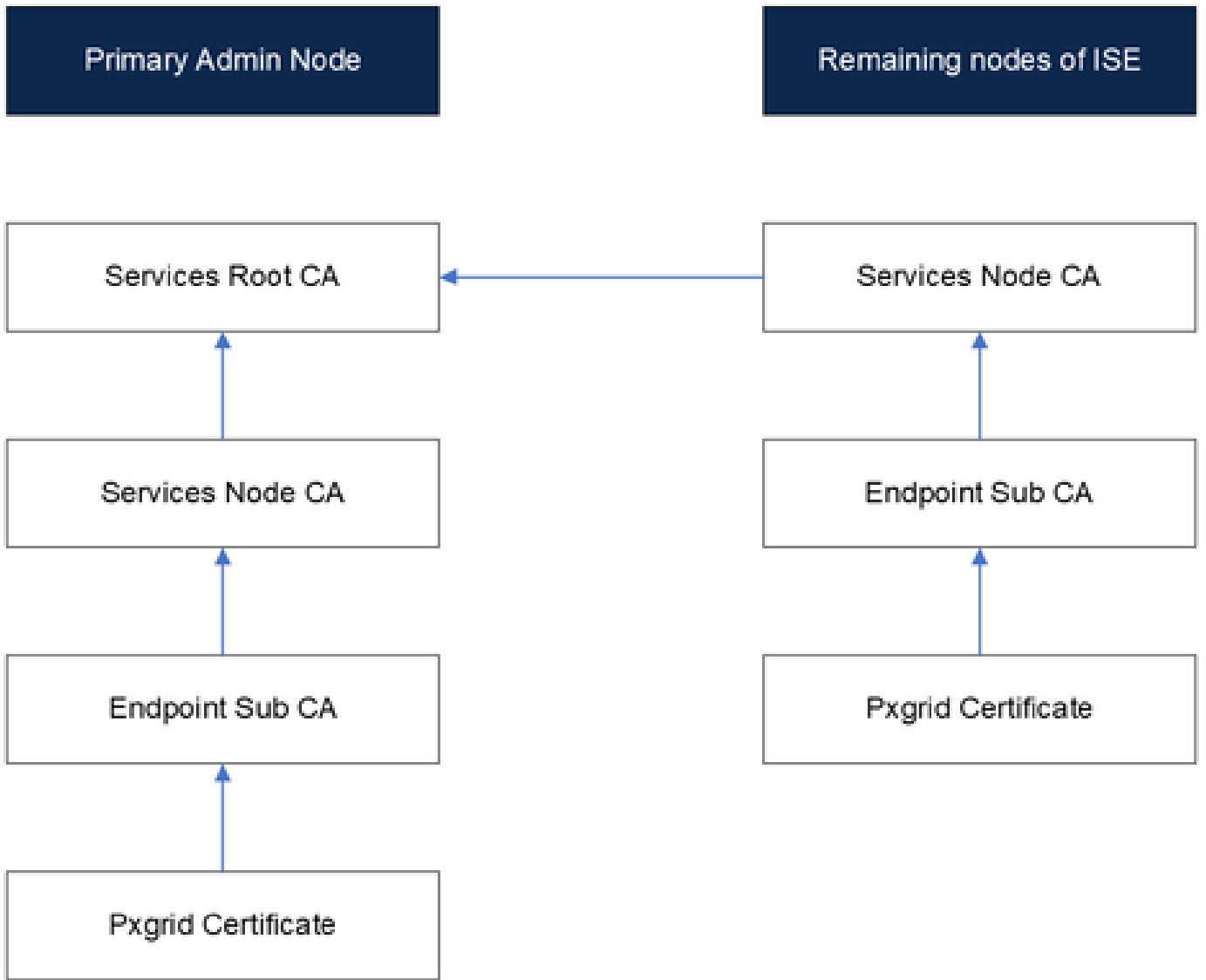
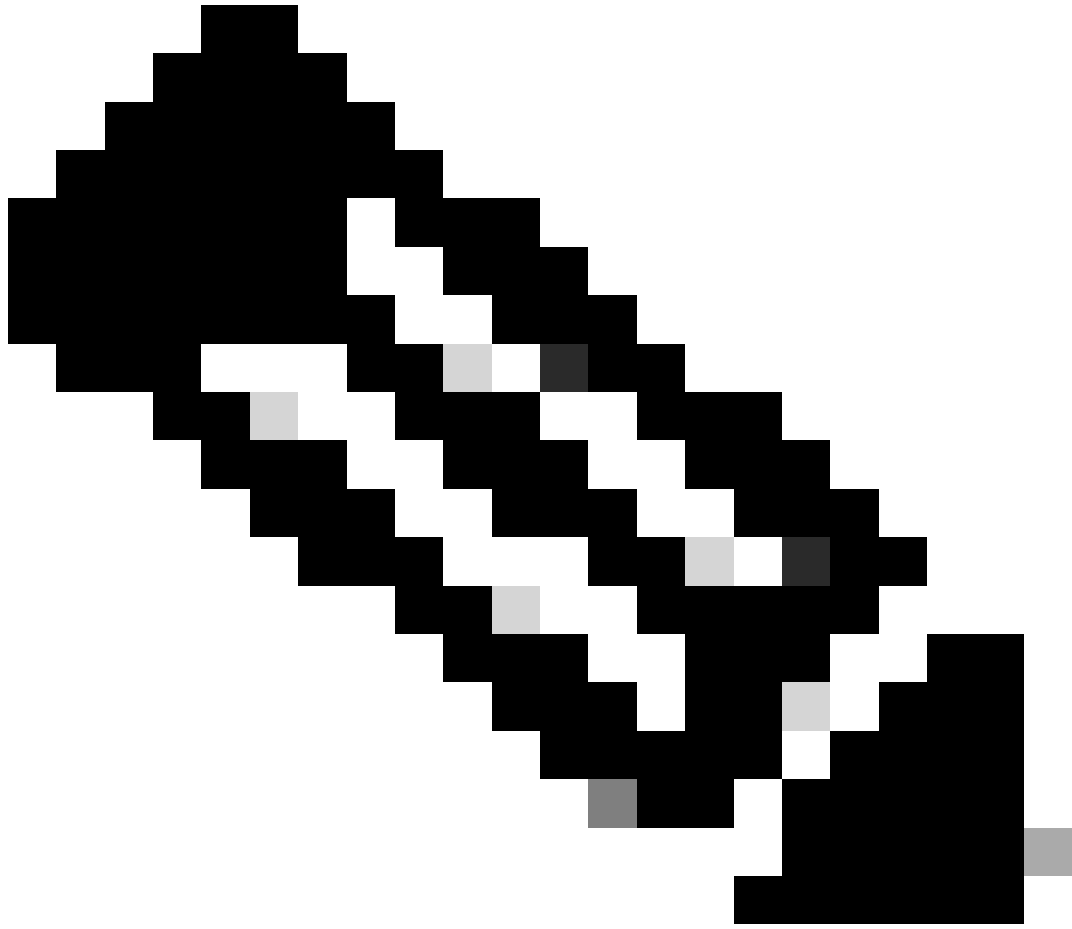


Diagram Internal Certificates on ISE.



Note: For further about the internal structure of certificates generated on ISE please refer to [Understand ISE Internal Certificate Authority Services.](#)

System Certificates								
Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status	
CA - ssp1se01 (1000001)								
<input type="checkbox"/> CN=ssp1se01.ssp1sec.mex, O=U=Certificate Services System Certificate/Certificate Services Endpoint Sub CA - ssp1se01#00002	pxGrid		ssp1se01.ssp1sec.mex	Certificate Services Endpoint Sub CA - ssp1se01	Fri, 30 Jun 2023	Sat, 1 Jul 2028	Active	<input checked="" type="checkbox"/>
<input type="checkbox"/> ise01_External_CA	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group	ssp1se01.ssp1sec.mex	ssp1sec-CXLABS-WIN2K22D-CA-2	Mon, 3 Jul 2023	Wed, 2 Jul 2025	Active	<input checked="" type="checkbox"/>
ssps1se02								
<input type="checkbox"/> Default self-signed saml server certificate - CN=SAML_ssp1se01.ssp1sec.mex	SAML		SAML_ssp1se01.ssp1sec.mex	SAML_ssp1se01.ssp1sec.mex	Sat, 1 Jul 2023	Thu, 29 Jun 2028	Active	<input checked="" type="checkbox"/>
<input type="checkbox"/> ise02_External_CA	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group	ssp1se01.ssp1sec.mex	ssp1sec-CXLABS-WIN2K22D-CA-2	Mon, 3 Jul 2023	Wed, 2 Jul 2025	Active	<input checked="" type="checkbox"/>
<input type="checkbox"/> CN=ssp1se02.ssp1sec.mex, O=U=ISE Messaging Services/Certificate Services Endpoint Sub CA - ssp1se02#00004	ISE Messaging Service		ssp1se02.ssp1sec.mex	Certificate Services Endpoint Sub CA - ssp1se02	Sat, 1 Jul 2023	Sun, 2 Jul 2028	Active	<input checked="" type="checkbox"/>
<input type="checkbox"/> CN=ssp1se02.ssp1sec.mex, O=U=Certificate Services System Certificate/Certificate Services Endpoint Sub CA - ssp1se02#00003	pxGrid		ssp1se02.ssp1sec.mex	Certificate Services Endpoint Sub CA - ssp1se02	Sat, 1 Jul 2023	Sun, 2 Jul 2028	Active	<input checked="" type="checkbox"/>

PxGrid certificates in a distributed deployment.

Step 5. Verify the status of the pxGrid certificates.

From the previous menu, select a checkbox from a node pxGrid certificate then select the option **View**.

The output looks like the one displayed here in the pxGrid certificates.

The screenshot shows a 'Certificate Hierarchy' dialog box with the following structure:

- Certificate Services Root CA - ssp1se01
 - Certificate Services Node CA - ssp1se02
 - Certificate Services Endpoint Sub CA - ssp1se02
 - ssp1se02.ssp1sec.mex** (highlighted)

Below the hierarchy, the details for the selected certificate are shown:

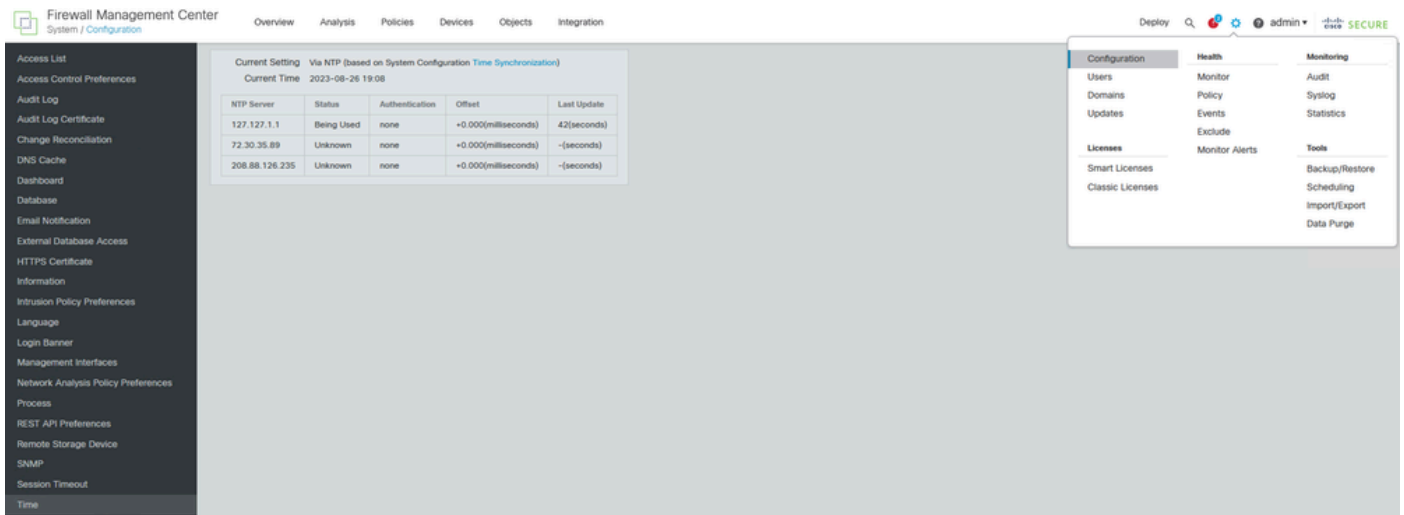
- Certificate status is good
- Details**
 - Issued To: ssp1se02.ssp1sec.mex
 - Common Name (CN): ssp1se02.ssp1sec.mex
 - Organization Unit (OU): Certificate Services System Certificate
 - Organization (O):
 - City (L):
 - State (ST):
 - Country (C):

Verification of pxGrid certificate.

Prepare the FMC for the integration.

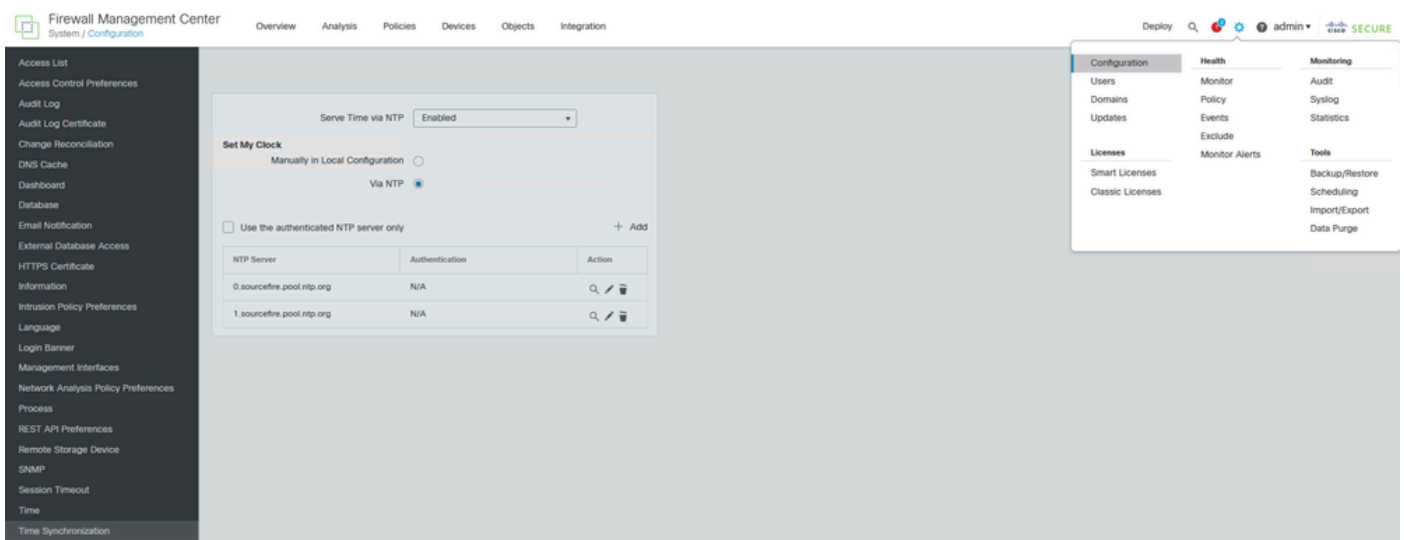
Step 1. Confirm that FMC internal time is up to date.

Navigate to **System > Configuration > Time** and ensure the time configured on the FMC is up-to-date.



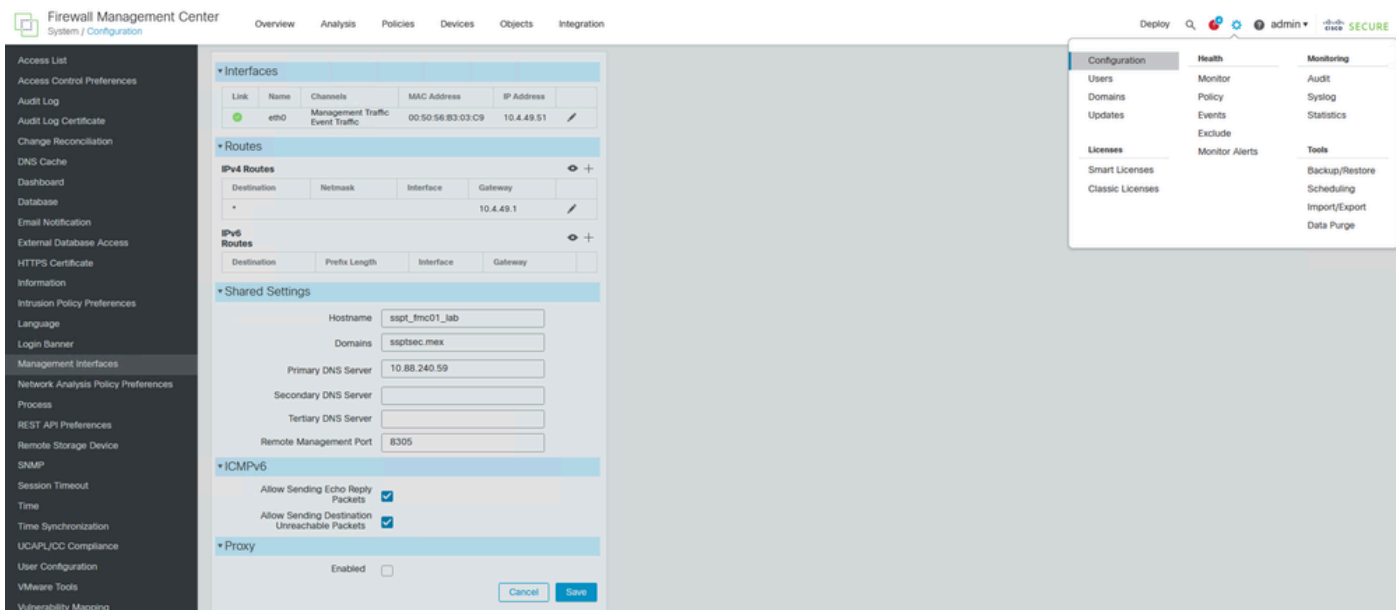
Verifying that the FMC is up to date.

If FMC time is not updated, ensure that NTP is properly configured and in Sync. NTP can be configured under **System > Configuration > Time > + Add**.



Time Synchronization on FMC.

Step 2. Navigate to **System > Configuration > Management Interface > Shared Settings** and verify that at least **Primary DNS Server** field contains a valid DNS server IP.



DNS configuration on FMC.

Step 3. Confirm that FMC hostname is configured.

Navigate to **System > Configuration > Management Interface > Shared Settings** and verify that **Hostname** field contains the FMC hostname.

You can verify this step while reviewing the previous step in this section .

Setting up the pxGrid connection between ISE and FMC.

Step 1. Navigate to the menu **Administration > pxGrid Services > Client Management > Certificates.**

In the first option, select **I want to Generate a single certificate (without a certificate signing request).**

In the **Common Name (CN)** section, input the FQDN of the FMC that the ISE is to issue a certificate.

Provide a **Description.**

In the section of **Subject Alternative Name (SAN)**, input the FQDN and IP address of the FMC to connect.

At the bottom in the **Certificate Download Format**, select from the drop-down menu the option **Certificate in Privacy Enhanced Electronic Mail (PEM)** format.

Input **PKCSS PEM format** (including certificate chain).

Input and store a password in **Certificate Password** as you use this password later in the FMC.

Confirm the password and then select **Create.**

Cisco ISE Administration - pxGrid Services

Summary Client Management Diagnostics Settings

Clients
Policy
Groups
Certificates

pxGrid Cloud Connection
pxGrid Cloud Policy

Certificates

Generate pxGrid Certificates

I want to*
Generate a single certificate (withou...v

Common Name (CN)*
sspt_fm01_lab.ssptsec.mex

Description
testing lab

Certificate Template pxGrid_Certificate_Template ⓘ

Subject Alternative Name (SAN)
FQDN sspt_fm01_lab.ssptsec.mex -- +

Subject Alternative Name (SAN)
IP address 10.4.49.51 -- +

Certificate Download Format*
Certificate in Privacy Enhanced Elect...v ⓘ

Certificate Password*
***** ⓘ

Confirm Password*

Reset **Create**

Example of pxGrid certificate generation.

Step 2. A zip file is downloaded to your computer. Decompress the file, and confirm that you have these files from your environment:

Name	Date modified	Type	Size
CertificateServicesEndpointSubCA-ssptise01_	21/08/2023 04:55	Security Certificate	3 KB
CertificateServicesNodeCA-ssptise01_	21/08/2023 04:55	Security Certificate	2 KB
CertificateServicesRootCA-ssptise01_	21/08/2023 04:55	Security Certificate	2 KB
sspt_fm01_lab.ssptsec.mex_sspt_fm01_lab.ssptsec.mex	21/08/2023 04:55	Security Certificate	2 KB
sspt_fm01_lab.ssptsec.mex_sspt_fm01_lab.ssptsec.mex.key	21/08/2023 04:55	KEY File	2 KB

PxGrid certificates generated by ISE.

Step 3. In the FMC, Navigate to the menu **Objects > Objects Management > PKI > Internal Certs**.
Select the option **Add Internal Cert**.

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** Integration

Deploy 🔍 ⚙️ 👤 admin | 🔒 SECURE

Add Internal Cert 🔍 Filter

Internal certificate object represents a server public key certificate belonging to your organization. You can use internal certificate objects and groups in SSL rules, ISE/ISE-PIC connection and captive portal configuration.

Name	Value
No records to display	

- AAA Server
- Access List
- Address Pools
- Application Filters
- AS Path
- Cipher Suite List
- Community List
- Distinguished Name
- DNS Server Group
- External Attributes
- File List
- FlexConfig
- Geolocation
- Interface
- Key Chain
- Network
- PKI
 - Cert Enrollment
 - External Cert Groups
 - External Certs
 - Internal CA Groups
 - Internal CAs
 - Internal Cert Groups
 - Internal Certs**
 - Trusted CA Groups
 - Trusted CAs

Adding the FMC certificate as internal certificate.

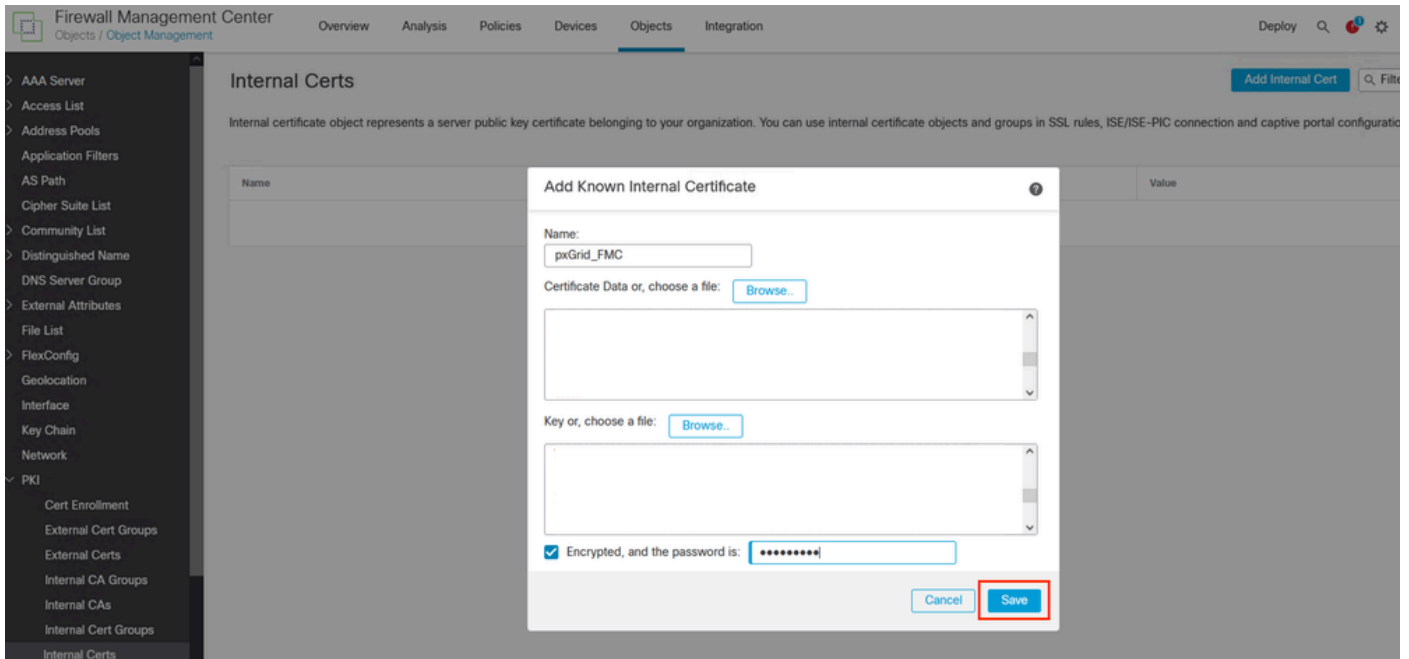
Step 4. Name the certificate that is allocated on FMC.

Browse the certificate you created for the FMC from ISE in the section **Certificate Data**.

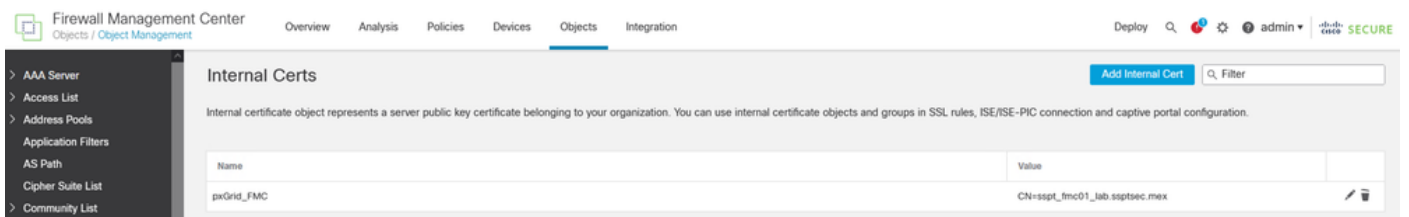
Browse the file with the extension **.key** to fill the next field.

Select the option **Encrypted**, and input the password that you used when you created the certificate on ISE.

Save the configuration.



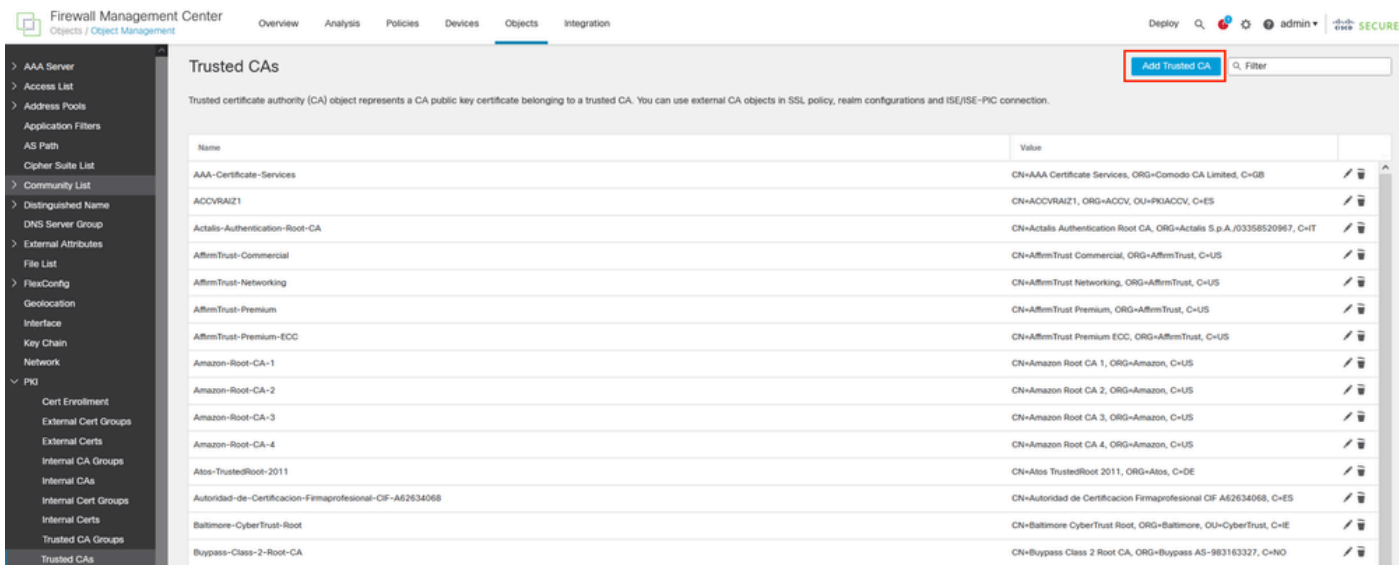
Exporting the FMC certificate that was generated by ISE.



FMC certificate.

Step 5. Navigate to the menu **Objects > Objects Management > PKI > Trusted CAs**,

Select **Add Trusted CAs**.

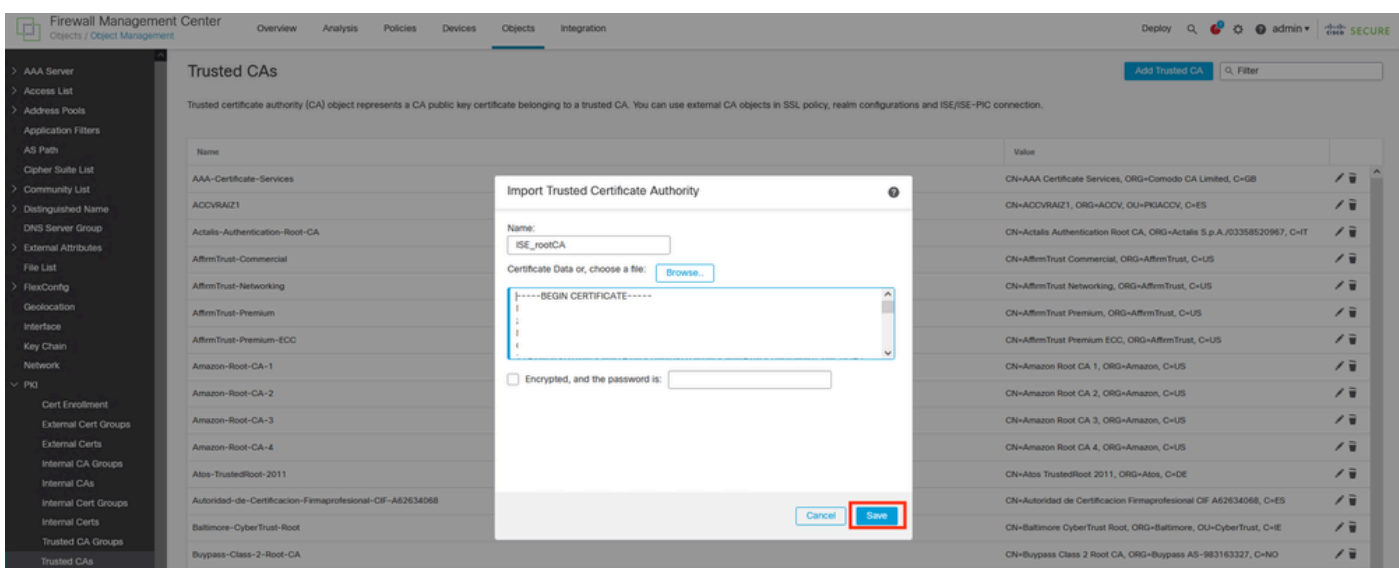


Adding the ISE rootCA as trusted certificate.

Step 6. Name the Certificate Authority.

Browse and select the ISE rootCA that was downloaded from the ISE file.

Save your configuration.



Exporting the ISE rootCA.

Step 7. Navigate to the menu **Integration > Other Integrations > Identity Sources**.

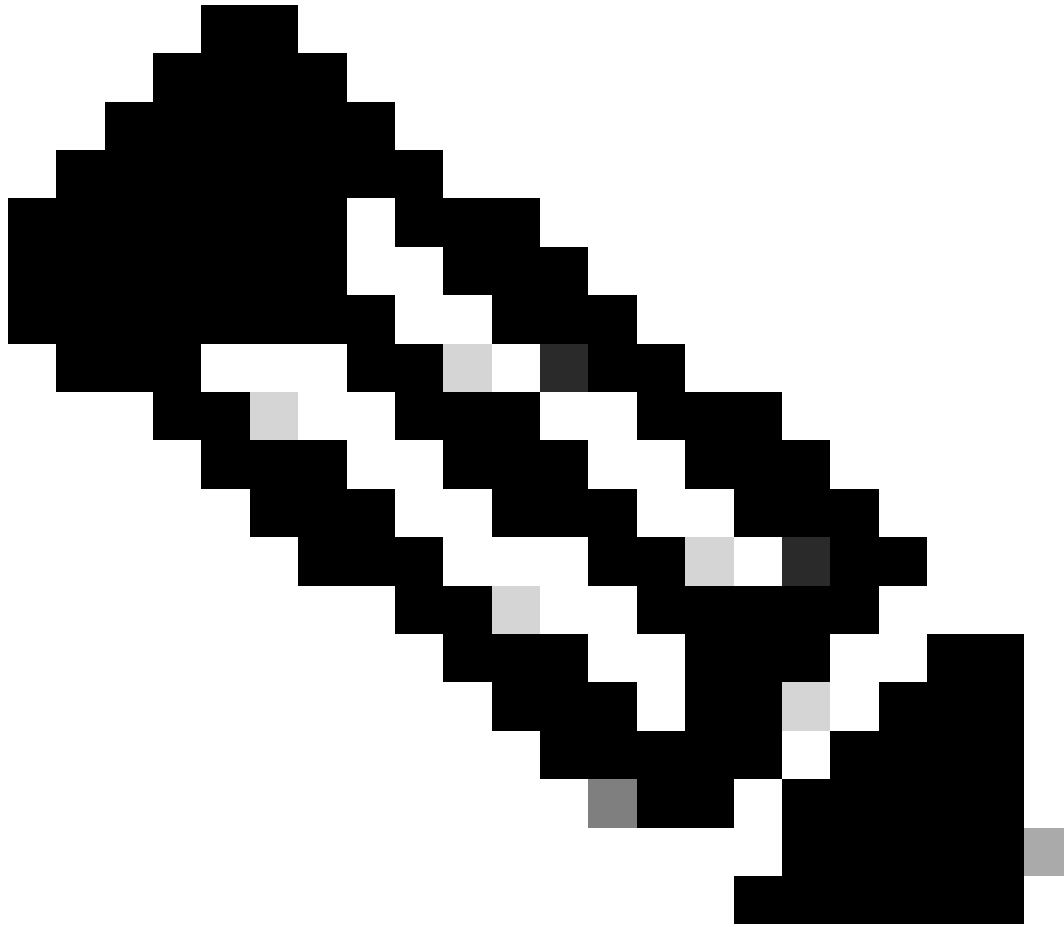
Select in **Service Type: Identity Services Engine**,

Input the IP address or the FQDN of the pxGrid node that becomes the Primary node.

Repeat the procedure for the Secondary pxGrid node.

Select from the drop-down menu the pxGrid certificate generated by ISE for the section **pxGrid Client Certificate**,

In the section MNT Server CA and pxGrid Server CA, select the ISE rootCA that you exported in the last step.

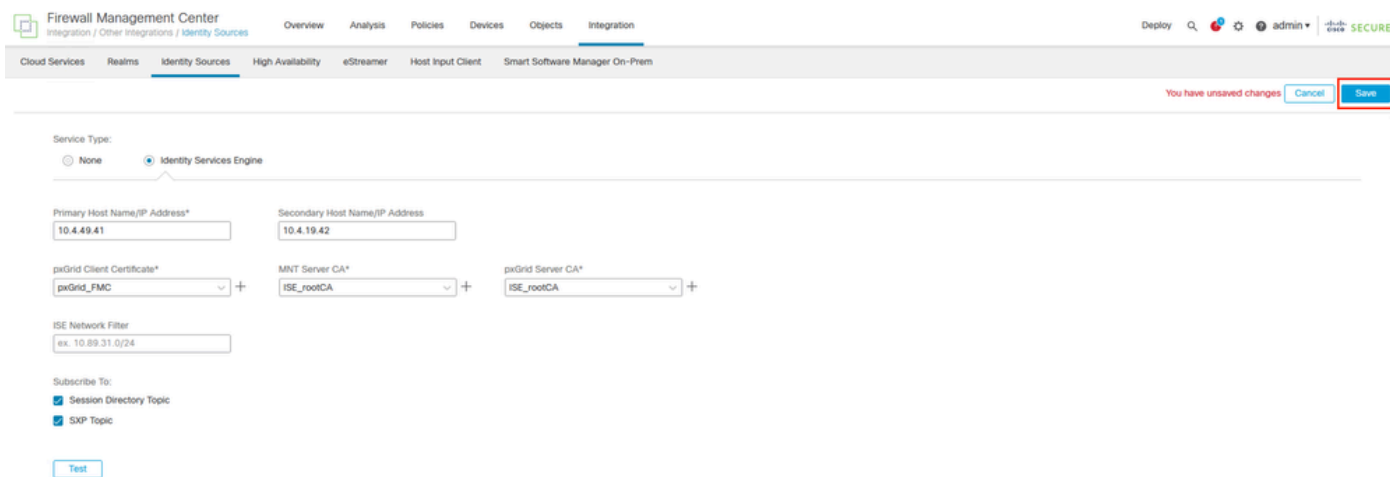


Note: The pxGrid Server CA corresponds the root Certificate Authority of the certificate that is being used by pxGrid on the pxGrid nodes.

The MNT Server CA corresponds to the Certificate Authority of the certificate that is being used by pxGrid on the MNT nodes.

(Optional) You can subscribe to the Session Directory and SXP topic from ISE.

Save the configuration.

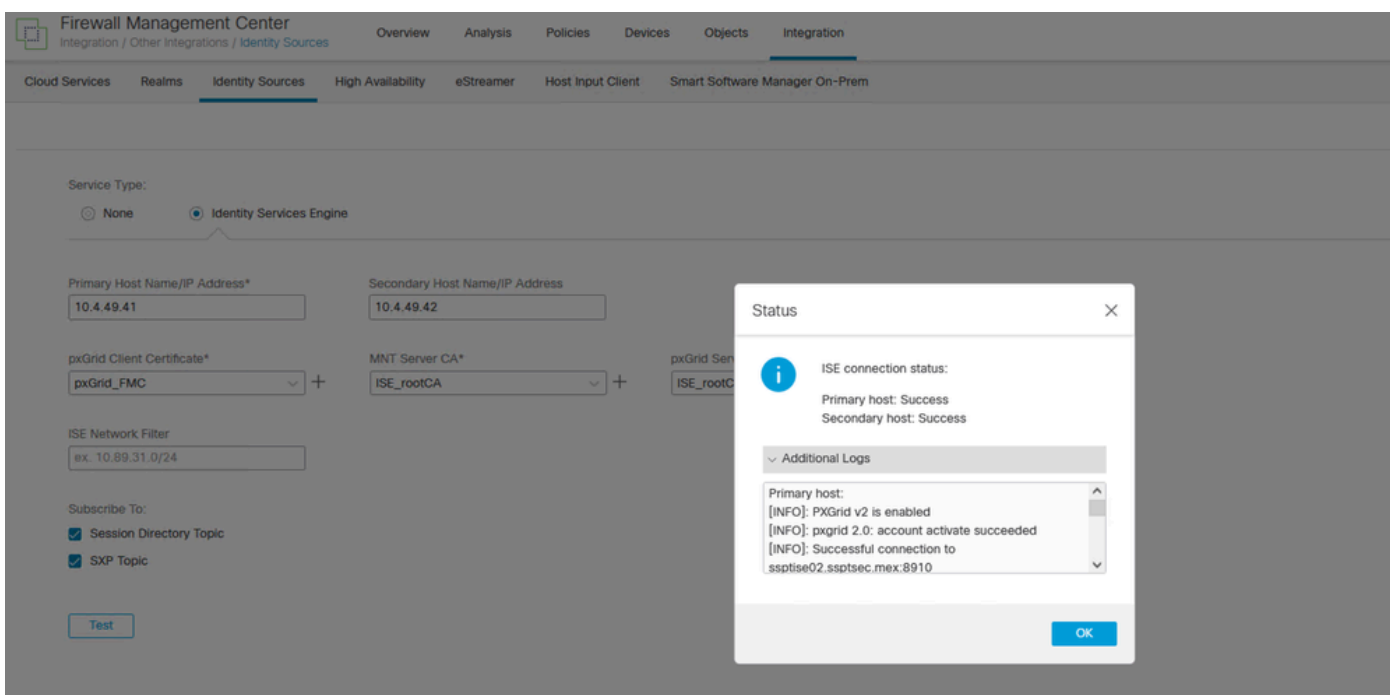


Setting up ISE as Identity Source in FMC.

Verify.

Validation on FMC.

In the menu, navigate to **Integration > Other Integrations > Identity Sources > Identity Services Engine**, before saving your configuration. You can test the settings for the pxGrid link.



PxGrid successful communication.

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, AdaptiveNetwork
[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, AdaptiveNetwork
[INFO]: All requested ISE Services are online.
```

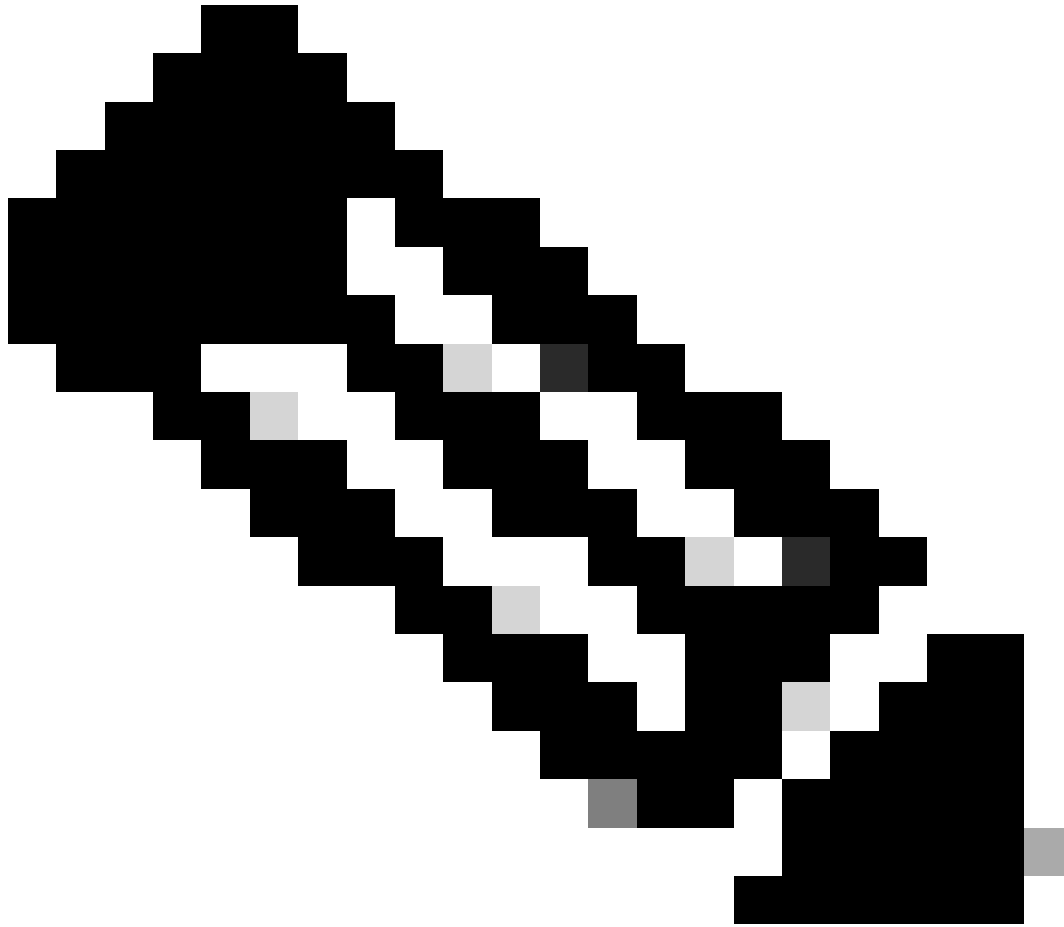
Validation on ISE.

When the FMC pxGrid client has been successfully integrated on ISE, you then see (in the **Administration > pxGrid Services > Client Management > Clients** menu) clients with the name **fmc** are included and enabled.

The screenshot shows the Cisco ISE Administration interface for pxGrid Services. The navigation menu includes Summary, Client Management, Diagnostics, and Settings. The main content area is titled 'Clients' and contains a table of pxGrid Clients. The table has columns for Name, Description, Client Groups, and Status. Four clients are listed, all with a status of 'Enabled'. A red box highlights the first four rows of the table.

Name	Description	Client Groups	Status
fmc-eb308edc160411ea751a865...			Enabled
t-fmc-eb308edc160411ea751a86...			Enabled
t-fmc-eb308edc160411ea751a86...			Enabled
fmc-6c85c3c6160511eb4ab139f5...			Enabled

PxGrid Clients available and enable.



Note: The pxGrid clients which prefix starts with "t-fmc" are the ones that is used through the testing button from the FMC.

Also, if you navigate to the menu **Administration > pxGrid Services > Diagnostics > WebSocket**, you then see the connections towards the FMC.

In the scenario in which you have the FMC in high availability, you then see the primary and secondary units as it is displayed in this example:

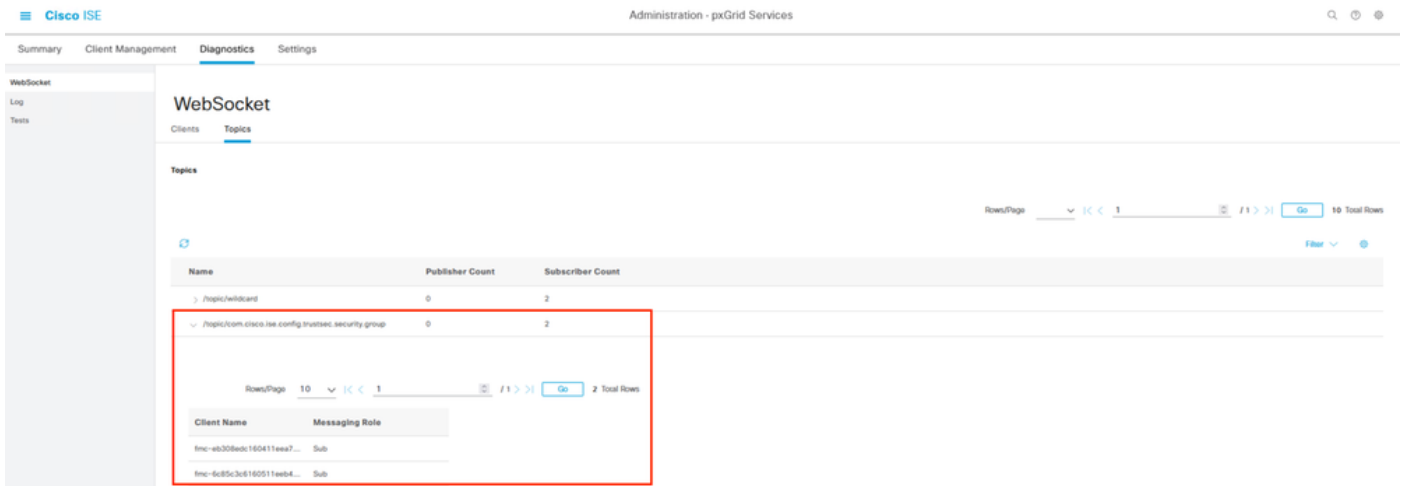
The screenshot shows the Cisco ISE Administration interface for pxGrid Services. The 'Diagnostics' tab is selected, and the 'WebSocket' section is active. A table lists active connections. Two rows are highlighted with a red box, representing connections to FMC units in a high availability configuration.

Client Name	Connect To	Session Id	Certificate	Subscriptions	Publications	IP Address	Status	Start time	Duration (dd:hh:mm:ss)
fmc-4b308bd0160411ea7...	sapria01	sapria01.5	CN=rspt_fmc01...	/topic/com.cisco.ise.sessio...		10.4.49.51	Connected	2023-08-21 05:30:18 MDT	01:10:19.42
fmc-6d85c3c6160511ea4...	sapria01	sapria01.6	CN=rspt_fmc01...	/topic/com.cisco.ise.sessio...		10.4.49.52	Connected	2023-08-21 05:31:54 MDT	01:10:18.03

WebSockets available on ISE.

In the next tab from this menu named **Topics**, you can verify that the FMC subscribers have been added to the pxGrid topics published by ISE.

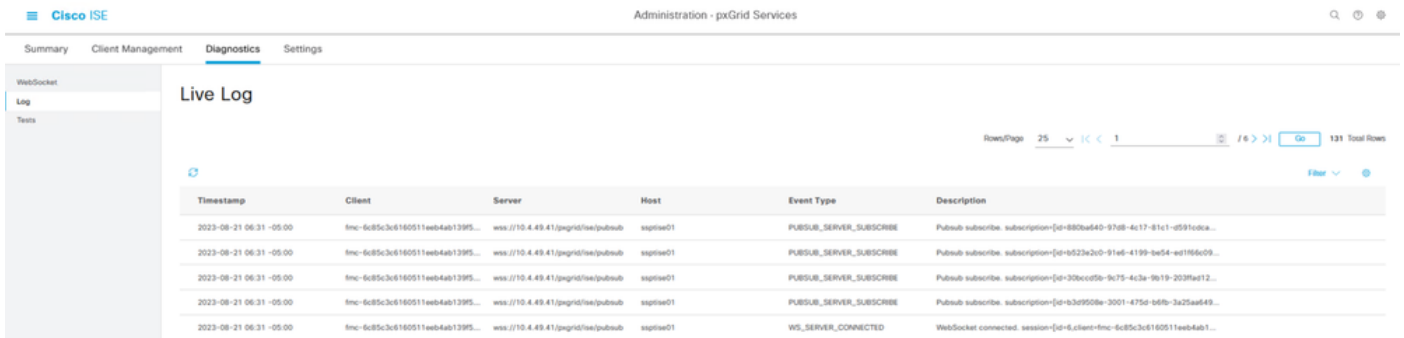
For example, there is the topic related to security group from where you can see that both FMC are subscribed and receiving information related to SGT posted by ISE.



Topics per pxGrid subscriber.

In the menu **Administration > pxGrid Services > Diagnostics > Log**, important events related to in pxGrid communication (for the nodes with the enabled feature enabled) are displayed.

These portray the information related to the integration.



PxGrid live logs.

Troubleshoot

Troubleshooting on FMC.

Confirm that FMC is able to resolve its own hostname and ISE nodes by hostnames.

For example:

```
</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
```

Ensure that ADI process is up and running:

```
<#root>
```

```
>
```

```
expert
```

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

```
sudo su
```

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

```
pmtool status | grep adi
```

```
adi (normal) - Running 7911
```

Ensure that communication from FMC to ISE on port TCPP 8910 is allowed. From FMC CLI we can configure a tcpdump packet capture to confirm bidirectional communication.

```
<#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
```

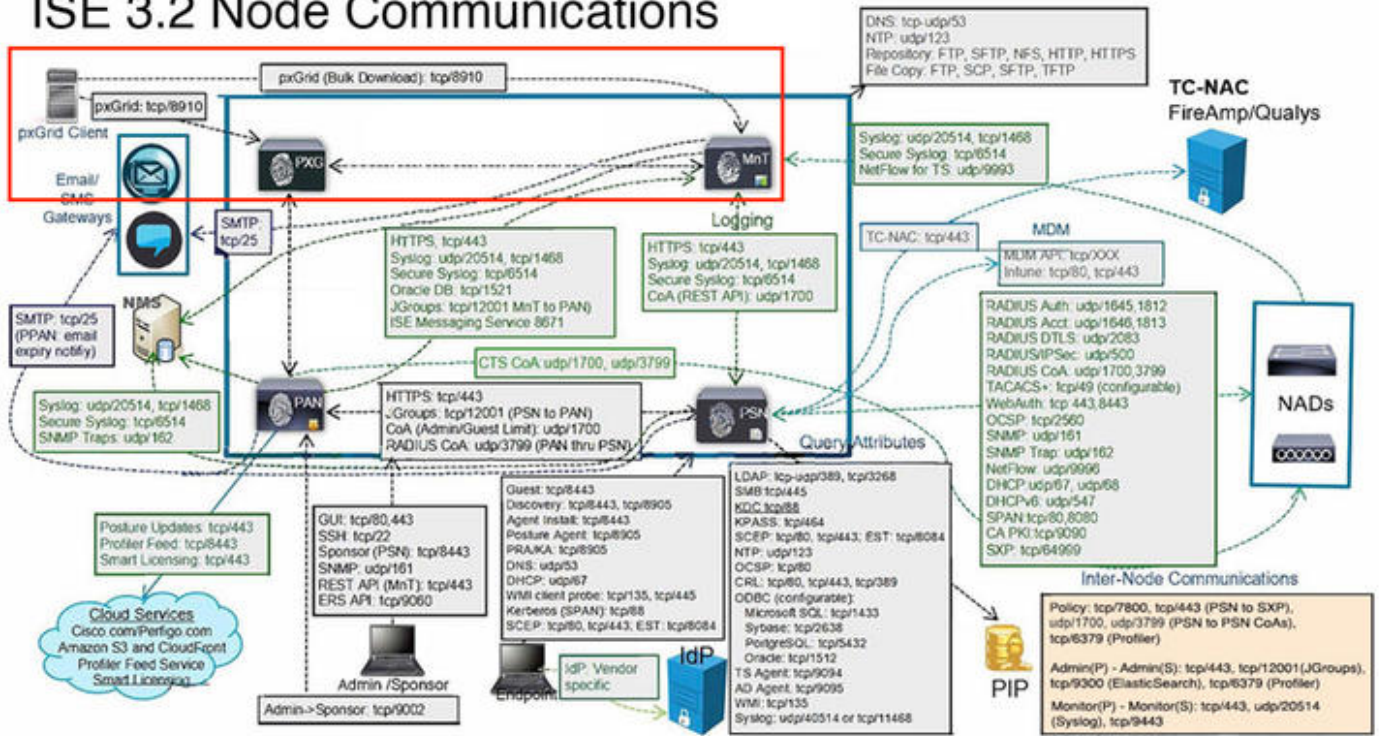
```
: Flags [.] , ack 1, win 229, options [nop,nop,TS val 2701166400 ecr 2268665064], length 0  
[...]
```

Troubleshooting on ISE.

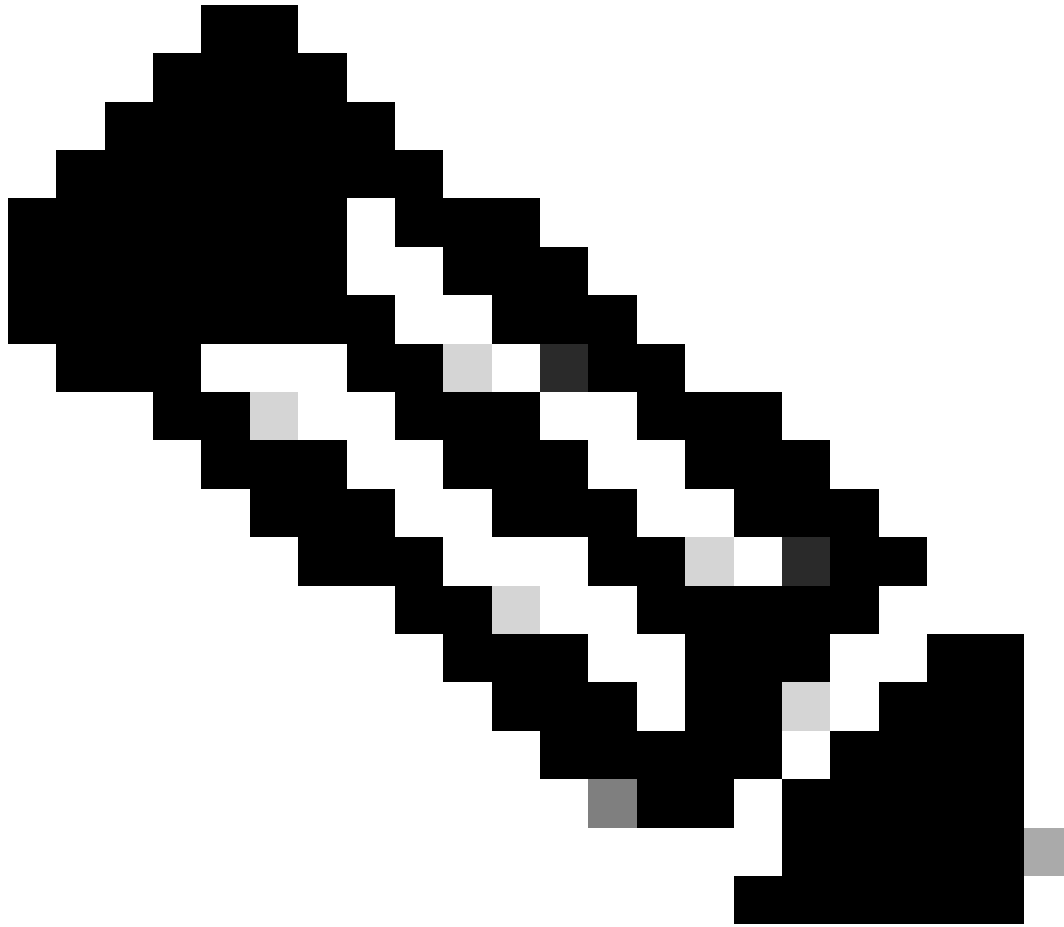
Verify that the communications on port 8910 is operational.

This is the port used by the pxGrid clients to communicate with pxGrid nodes and MnT nodes for the bulk download of information.

ISE 3.2 Node Communications



PxGrid interaction in ISE environment.



Note: The pxGrid client, in this case the FMC communicates to the pxGrid nodes and the Secondary MNT (SMNT) node to get the (Bulk Download) of the information, in case of failure in the SMNT it looks for the information through the Primary MNT.

In the ISE nodes where the communication with the pxGrid client is held, you can review if the port is open or if there are sockets connected to that port.

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

There are 2 test available on ISE that diagnose the overall status of the pxGrid implementations.

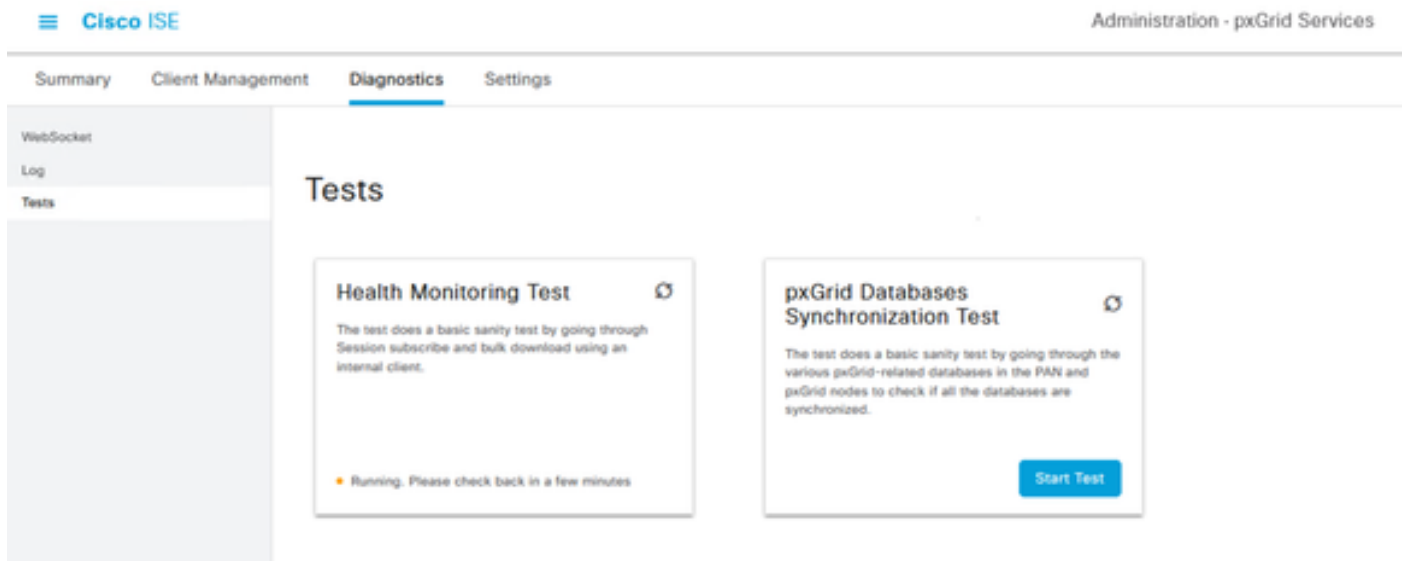
Those can be found in the menu **Administration > pxGrid Services > Diagnostics > Test.**

The tests displayed in this section are performed internally on ISE.

Health Monitoring Test reviews the pxGrid service lookup, which evaluates if a client can access the

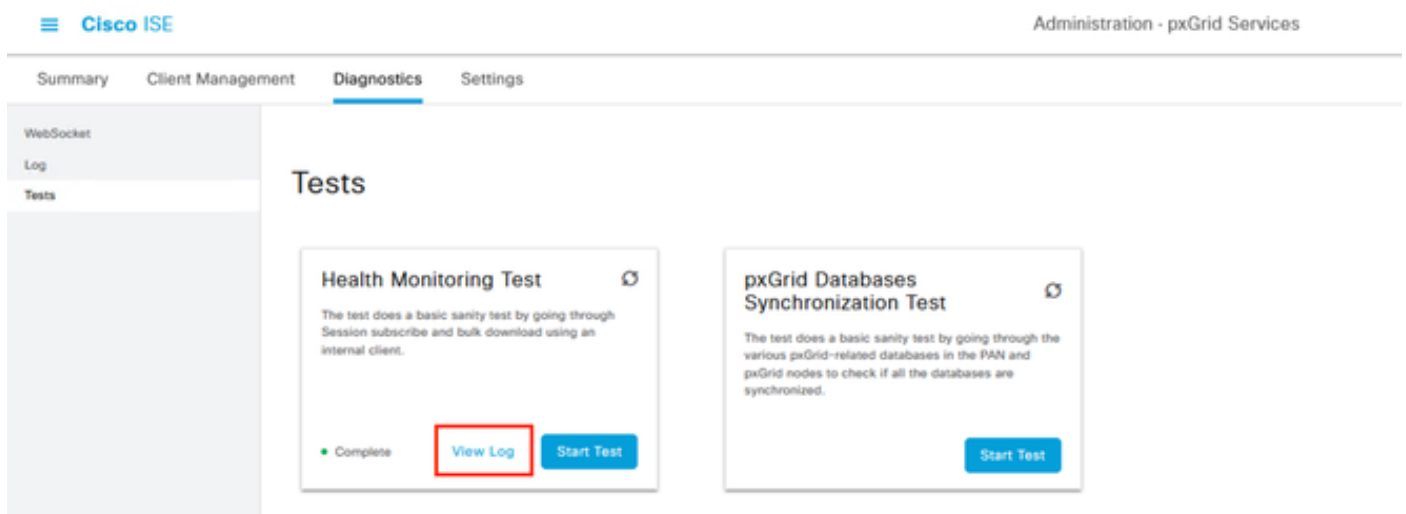
Session Directory, service, and topics published by the pxGrid controller.

Select the option **Start Test** and wait for the logs to be gathered.



PxGrid Health Monitoring Test.

Once the test has completed, select the option **View Log**. For this example, the content of the log is:



Review of Health Monitoring Test.

```
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 -----
```

```

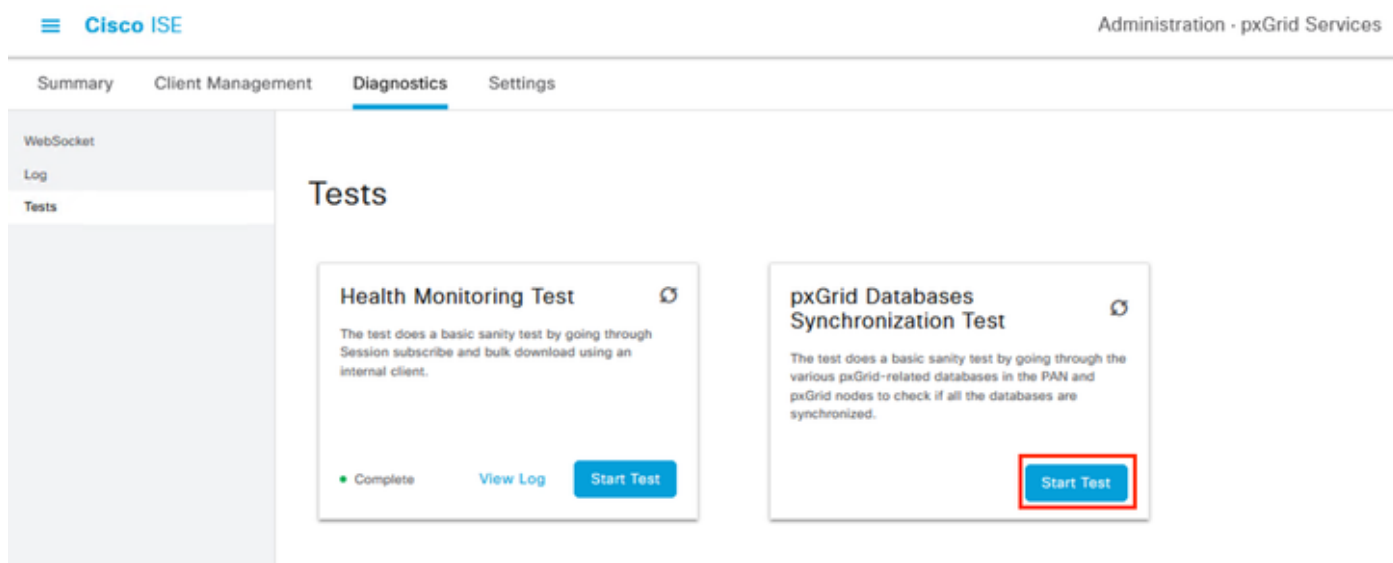
22-Aug-2023 17:03:16 [INFO] STOMP CONNECT host=ssptise02.ssptsec.mex
22-Aug-2023 17:03:16 [INFO] STOMP SUBSCRIBE topic=/topic/com.cisco.ise.session
22-Aug-2023 17:03:16 [INFO] STOMP CONNECTED version=1.2
22-Aug-2023 17:07:16 [INFO] A total of 0 notifications were received.
22-Aug-2023 17:07:16 [INFO] 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 *****

```

PxGrid Database Synchronization Test checks if the information within the databases is correct between the PAN and pxGrid nodes and synchronized.

Therefore, the information sent to the pxGrid subscribers is accurate.

Select the option **Start Test** and wait for the results to come to be evaluated.



PxGrid Databases Synchronization Test.

From the logs generated, this output was obtained.

```

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

```

```

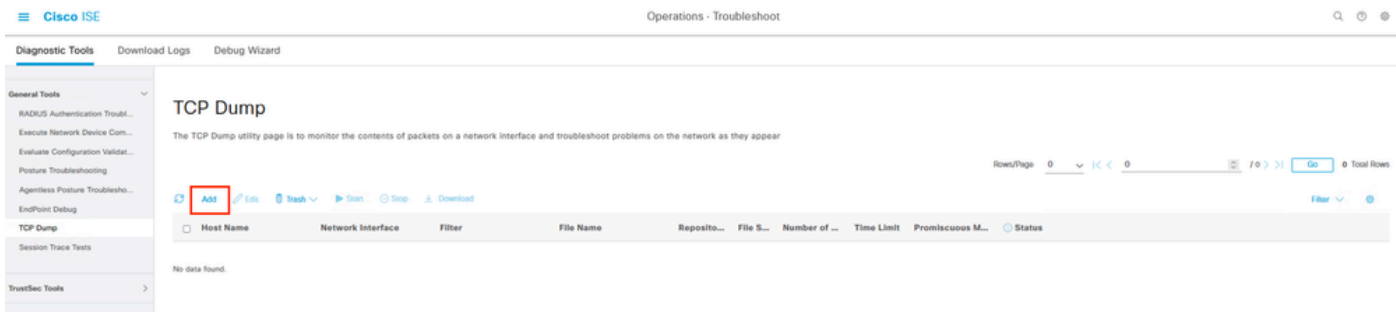
Primary PAN : ssptise01.ssptsec.mex
pxGrid Nodes : ssptise01.ssptsec.mex ssptise02.ssptsec.mex

```

Collect a capture on from the pxGrid nodes pointing towards the primary FMC node.

Navigate to the menu **Operations > Troubleshoot > Diagnostic Tools > TCP Dump**,

Select the option to **Add** a new capture.



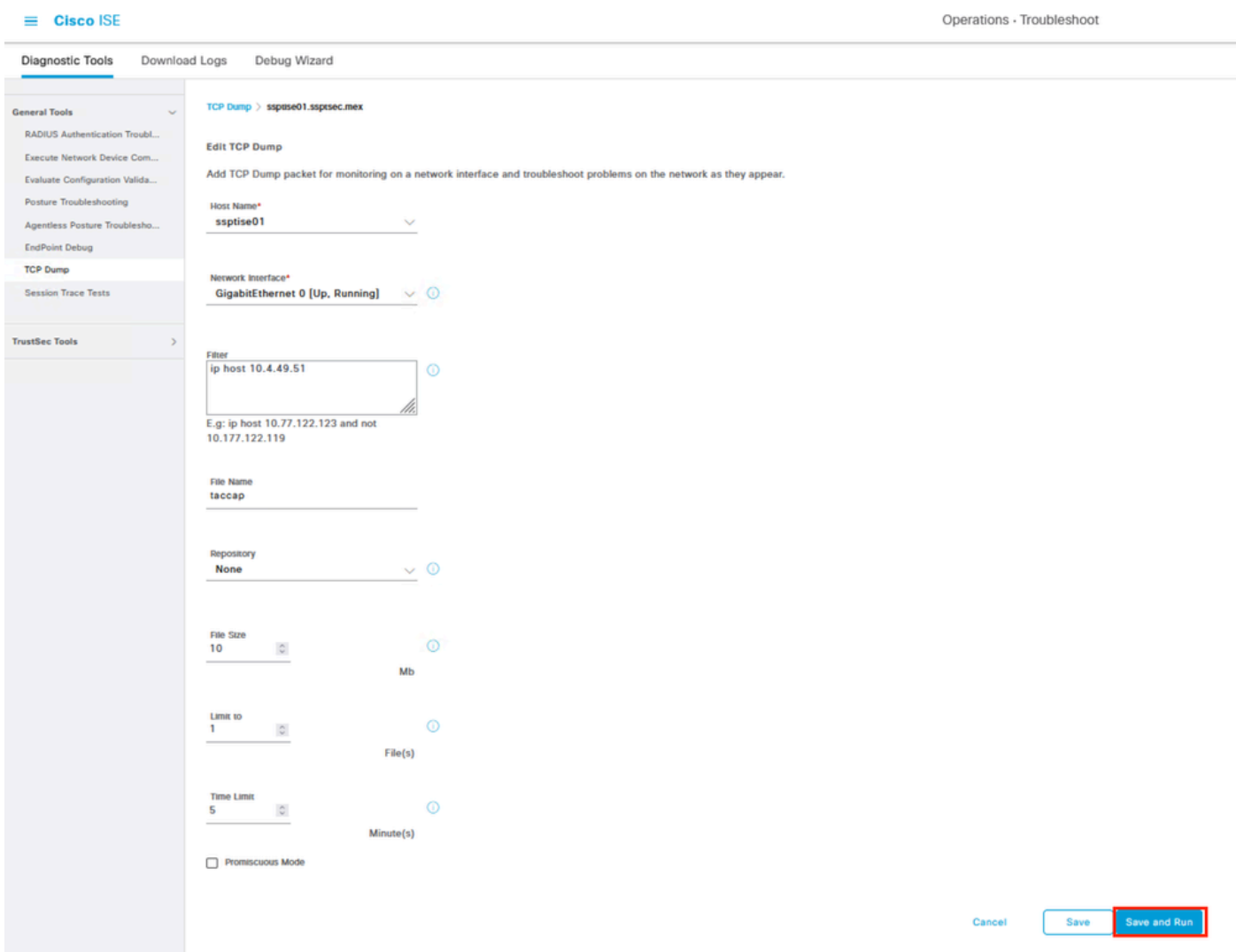
Generating a packet capture on ISE.

Configure the parameters for the capture.

In **Host Name**, select the primary pxGrid node selected in the FMC.

Filter the traffic with this syntax **ip host <FMC IP>**

Name the capture and then proceed to **Save and Run**.



Example of packet capture configuration.

In another window, in the FMC menu **Integration > Other Integrations > Identity Sources**, **Test** the connection with the ISE through the pxGrid channel.

When you get the outcome of the test, proceed to **Stop** the capture on ISE.

Diagnostic Tools Download Logs **Debug Wizard**

Debug Profile Configuration
Debug Log Configuration

Node List > ssptise01.sspitsec.mex

Debug Level Configuration

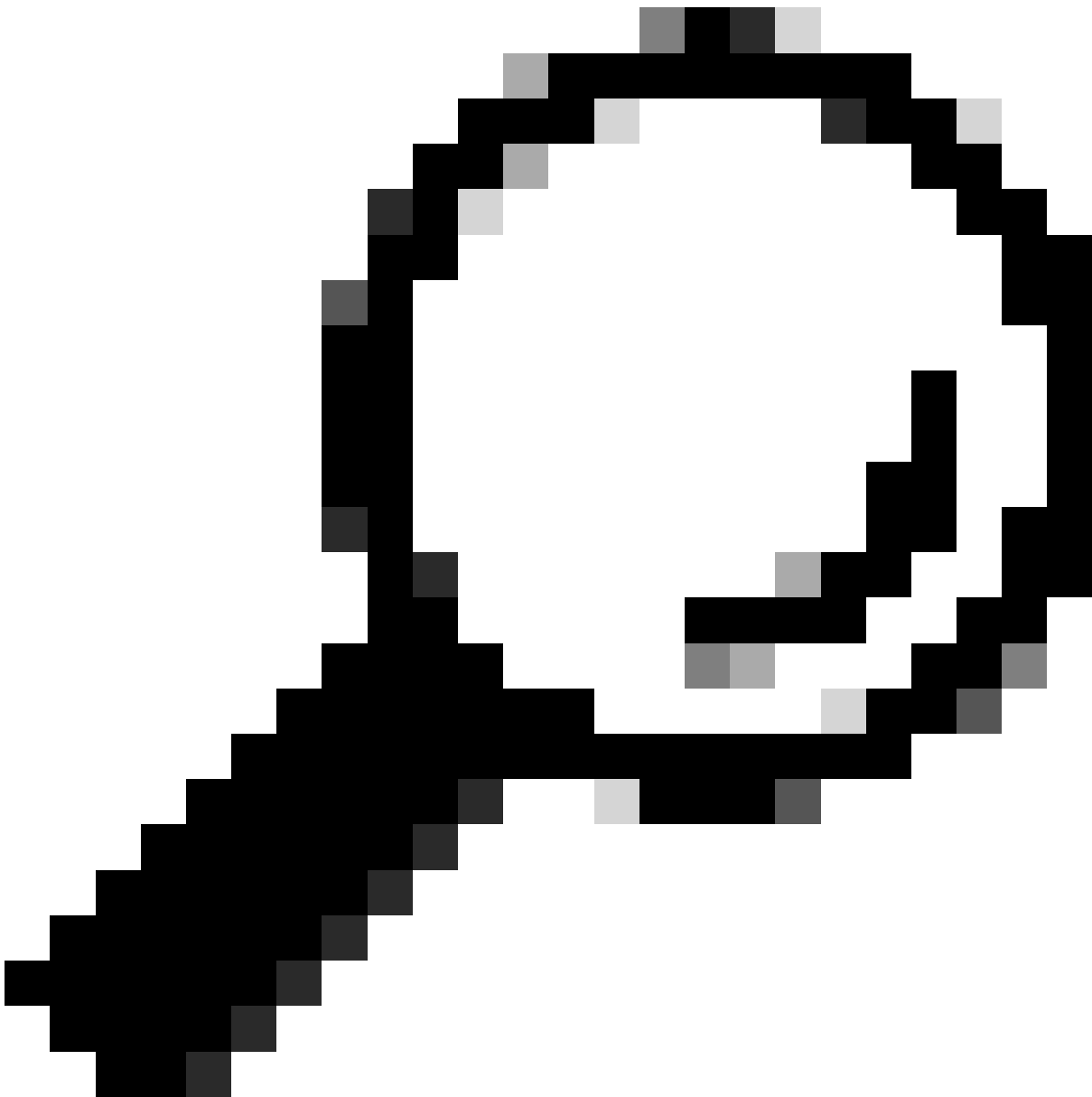
[Edit](#) [Reset to Default](#)

Component Name	Log Level	Description	Log file Name
pxgrid			
<input type="radio"/> pxgrid	DEBUG	pxGrid messages	pxgrid-server.log
<input type="radio"/> pxGrid Cloud	INFO	pxGrid Cloud messages	pxcloud.log Save Cancel
<input type="radio"/> pxGrid Direct	INFO	pxGrid Direct backend and UI log messages	ise-pxgriddirect.log, pxgriddirect.log

Changing the pxGrid component to debug level.

Reproduce the behavior to analyze, then proceed to analyze the logs collected on pxgrid-server.log file. Other logs that you can review on ISE node to troubleshoot are:

```
#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
```

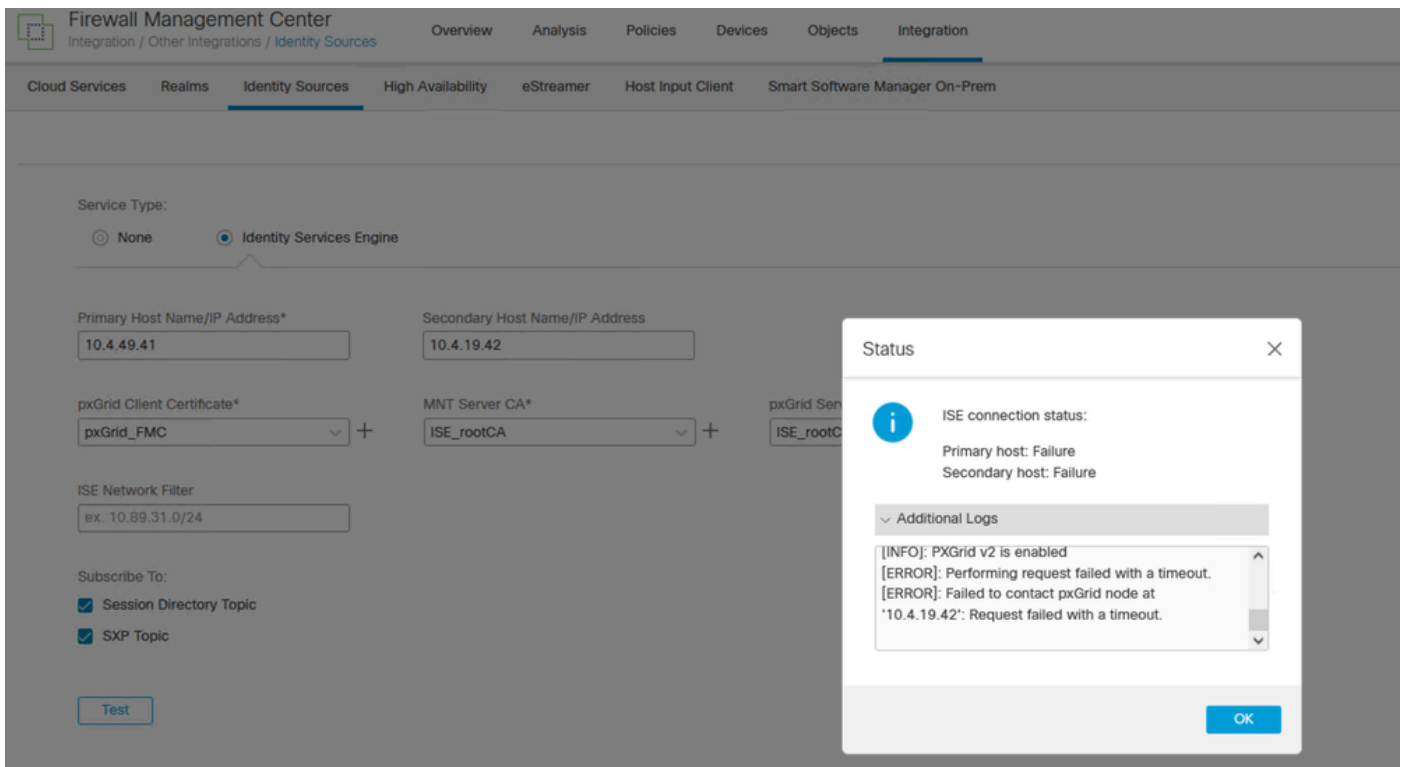


Tip: For further log collection recommendations please review the video [How to Enable Debugs on ISE 3.x Versions.](#)

Common problems.

PxGrid subscriber client is not approved on ISE.

For this use case, the output related from the FMC test pxGrid button shows this behavior:



FMC pxGrid connection failed.

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
```

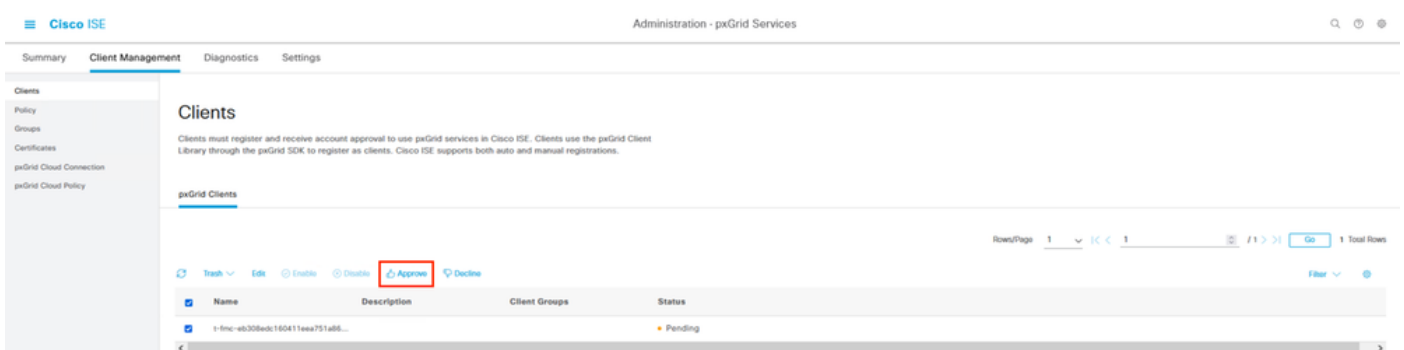
Secondary host:

```
[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.
```

On ISE, notice the behavior in the menu **Administration > PxGrid Services > Client Management > Clients** indicating that the pxGrid client (FMC) is pending for approval.

Select the button **Approve**, confirm the selection in the next window and attempt the integration again.

This time the integration is successful.



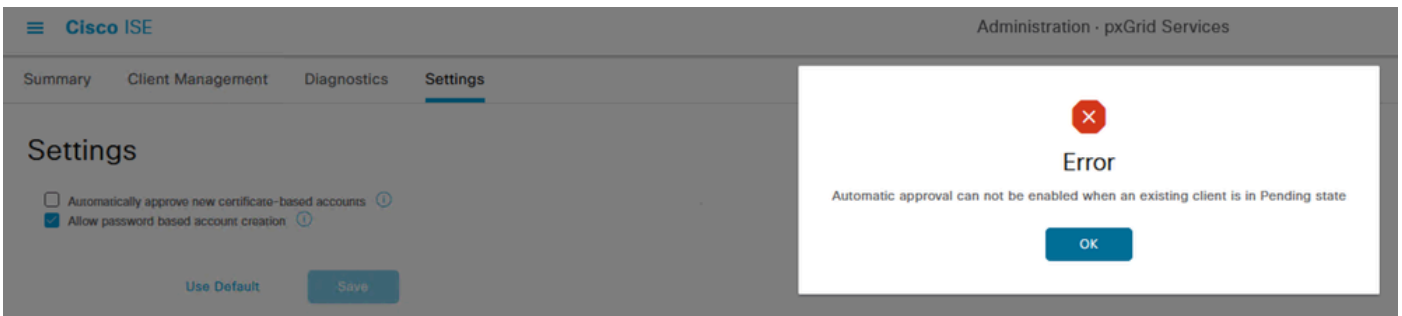
FMC client in pending status.



Confirmation of the approval of the pxGrid client.

Notice if you want to enable the Automatic approval of certificate based pxGrid clients.

Approve/Decline the clients from the previous page as this alarm can appear.



Error related to the approval of pxGrid clients.

PxGrid ISE certificate chain incomplete.

In this scenario, if you navigate to the menu **Administration > System > Certificate**, select the pxgrid certificate and select the option **View**,

In case you have a problem with the certificate, these related errors are possible.

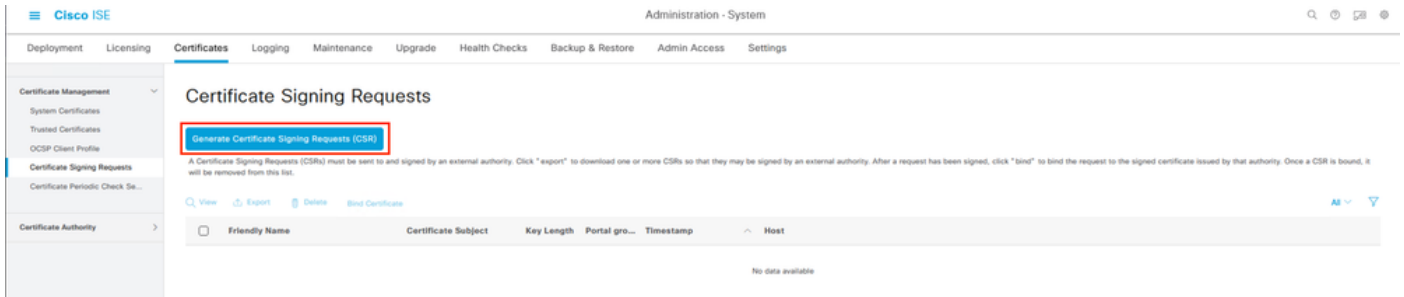


Error related to certificate chain incomplete.

The first step to check is if you have the ISE root CA is completed in the View option.

In case of a certificate missing in the hierarchy, you can issue the whole ISE deployment root CA.

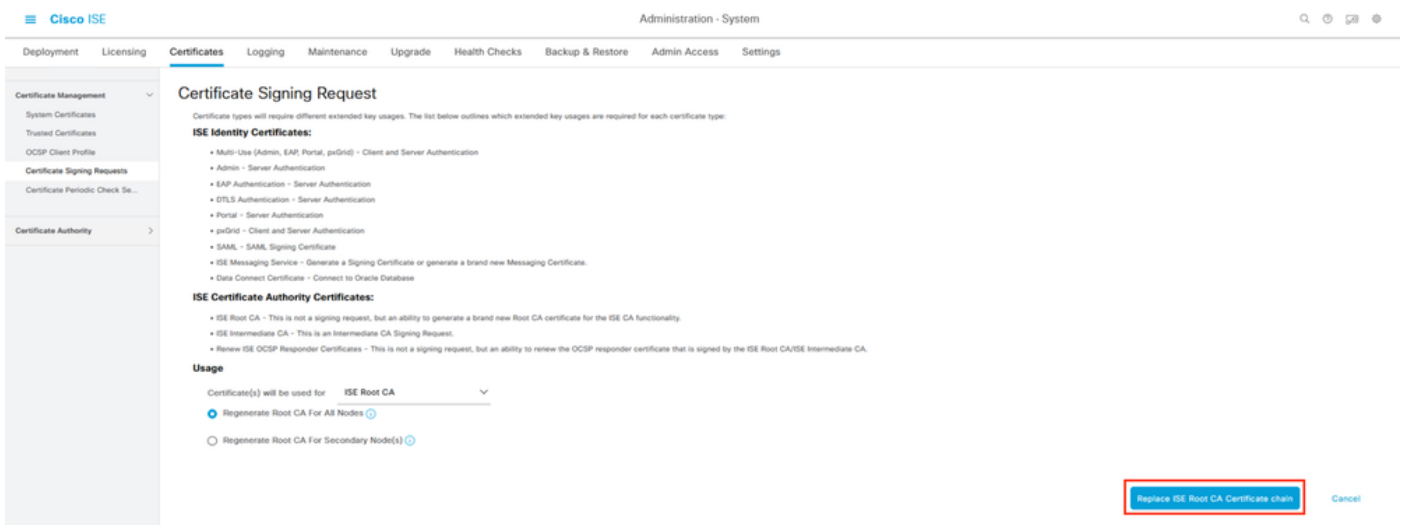
Browse to the menu **Administration > System > Certificates > Certificate Management > Certificate Signing Request (CSR)** and select that button.



Generating a CSR on ISE.

In this menu select in **Usage ISE Root CA** and Regenerate ISE Root CA for all Nodes.

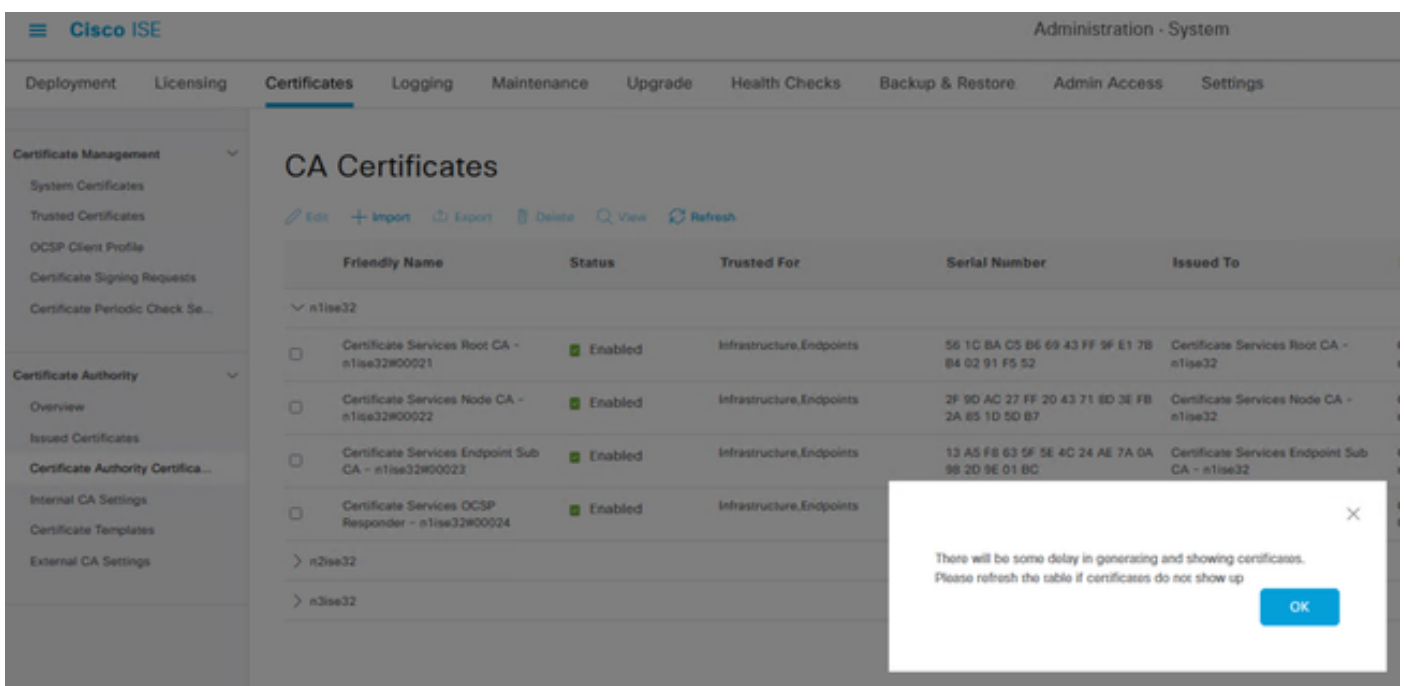
Proceed with the button **Replace ISE Root CA Certificate chain**.



Configuring the Certificate Signing Request.

Wait for the certificates to be generated in all the nodes of the implementation.

Upon completion, the ISE displays the next notification.



Confirmation of generation of certificates.

Confirm if the pxGrid certificate trust chain is completed by selecting the option View in System Certificates.

Reference.

[PxGrid Cisco Developer page.](#)

[Cisco Identity Services Engine Administrator Guide, Release 3.2 , Chapter: Cisco pxGrid.](#)

[Cisco Identity Services Engine Installation Guide, Release 3.2, Chapter: Cisco ISE Ports Reference](#)

[Cisco Identity Services Engine CLI Reference Guide, Release 2.4](#)