Configure and Troubleshoot ISE 3.2 with FMC 7.2.4 Integration

Contents

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
- Platform Exchange Grid
- Firewall Management Center
- 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 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.

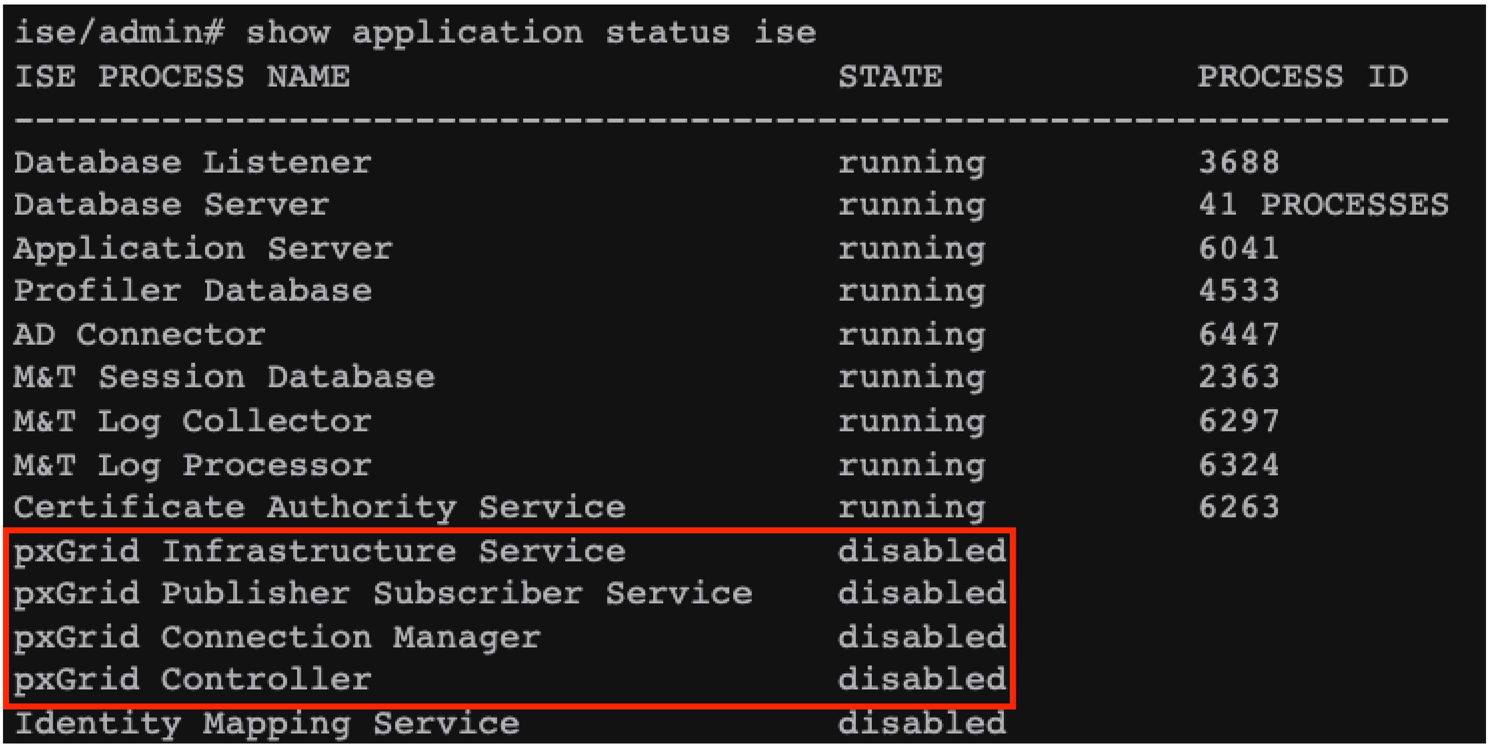
PxGrid framework has 2 versions. The one to use depends upon the ISE version and patch you need to review.

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 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 this version. This platform operates now by using REST operations on ISE and WebSocket protocols which brings enhancements, with 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 the mechanisms that you can check to

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.

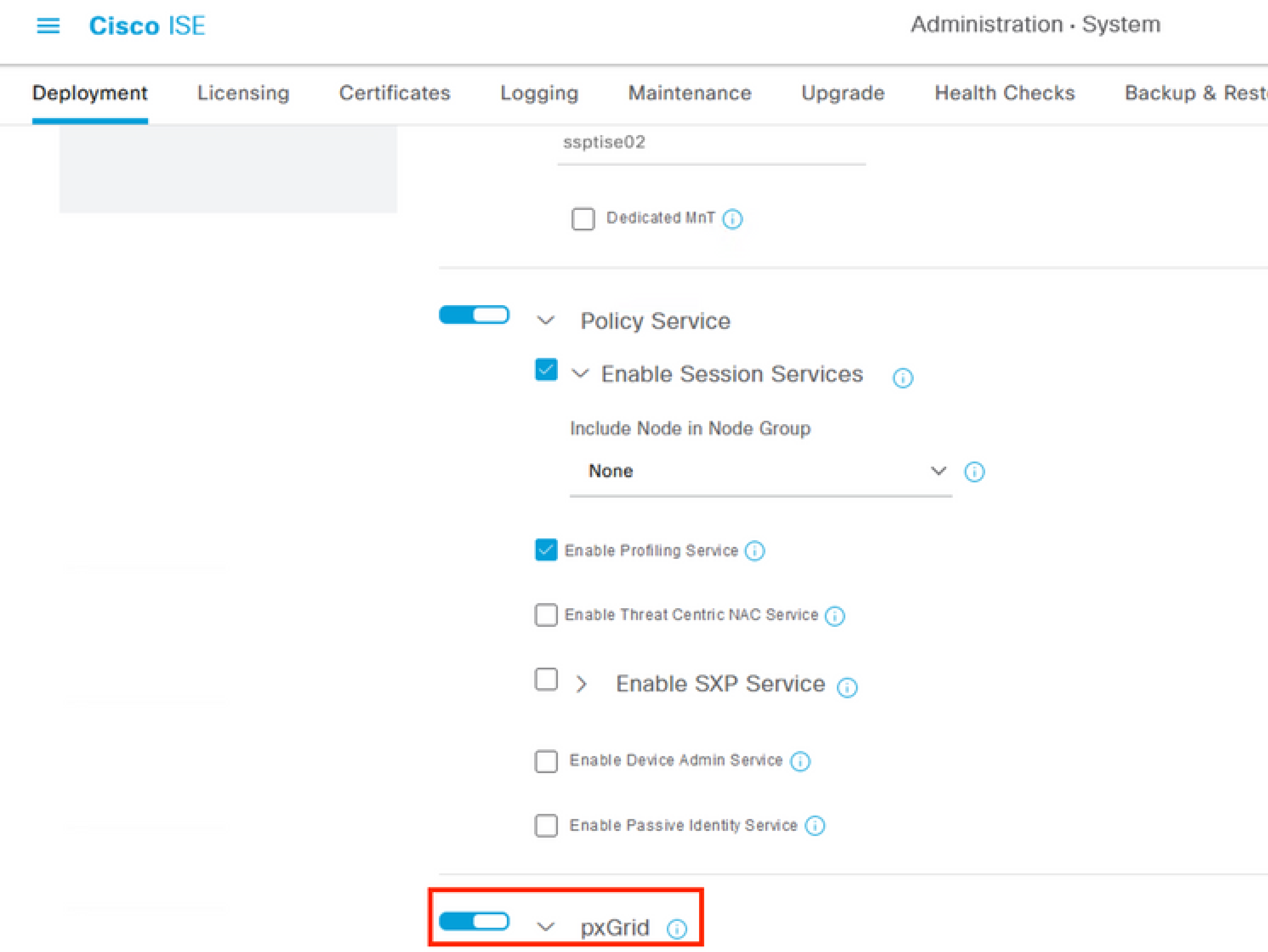
This integration allows you to create content policies on FMC based on the information that is shared by ISE and their published topics (related to the endpoint activity).

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.



ssptise02

□ Dedicated MnT

Policy Service

☑ Enable Session Services

Include Node in Node Group

None

☑ Enable Profiling Service

□ Enable Threat Centric NAC Service

□ Enable SXP Service

□ Enable Device Admin Service

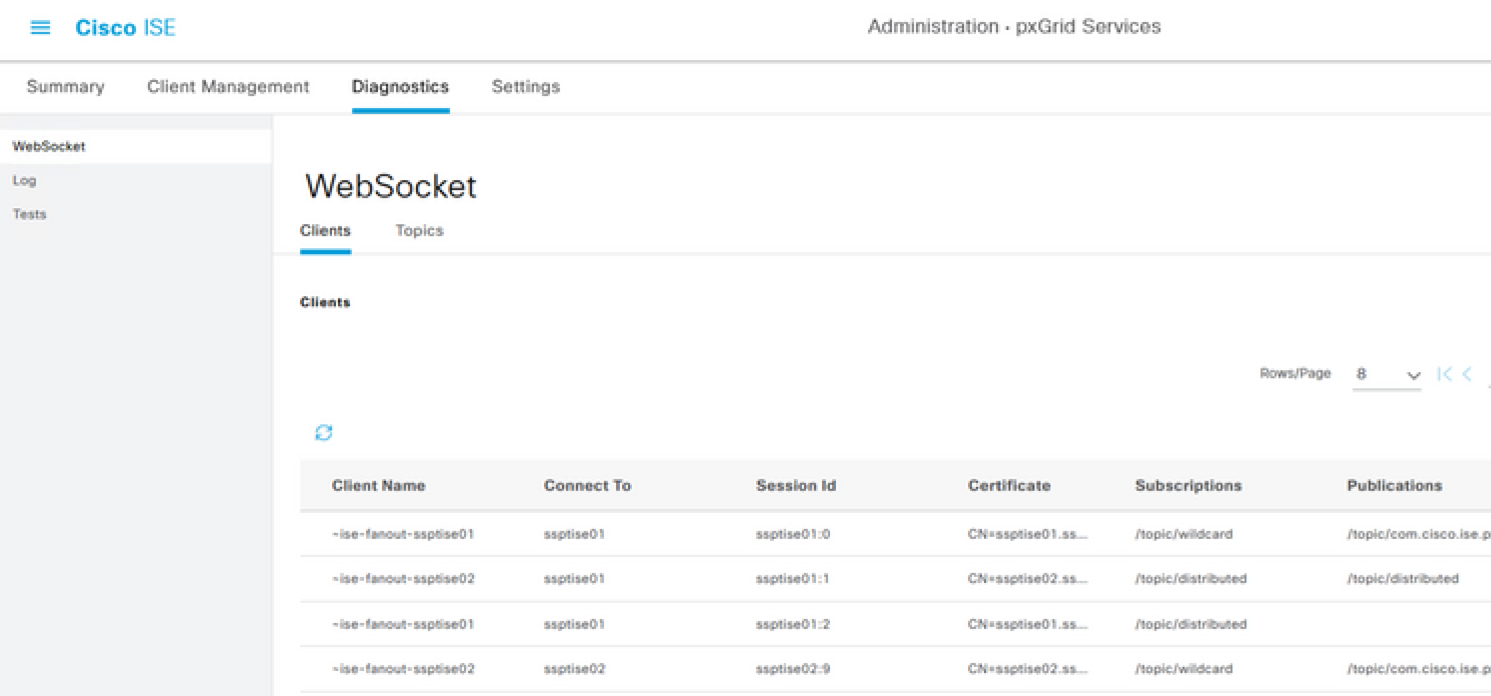
□ Enable Passive Identity Service

pxGrid

Enabling ISE pxGrid services in a node.

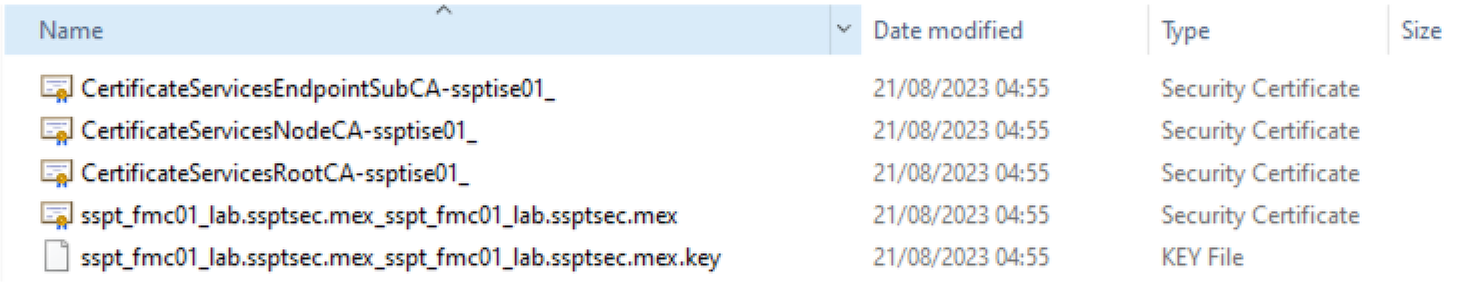
Step 2. After enabling the nodes with the pxGrid feature, review the status of the Websockets related to the internal clients are connected.

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



Client Name	Connect To	Session Id	Certificate	Subscriptions	Publications
~ise-fanout-ssptise01	ssptise01	ssptise01:0	CN=ssptise01.ss...	/topic/wildcard	/topic/com.cisco.ise.p
~ise-fanout-ssptise02	ssptise01	ssptise01:1	CN=ssptise02.ss...	/topic/distributed	/topic/distributed
~ise-fanout-ssptise01	ssptise01	ssptise01:2	CN=ssptise01.ss...	/topic/distributed	
~ise-fanout-ssptise02	ssptise02	ssptise02:9	CN=ssptise02.ss...	/topic/wildcard	/topic/com.cisco.ise.p

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

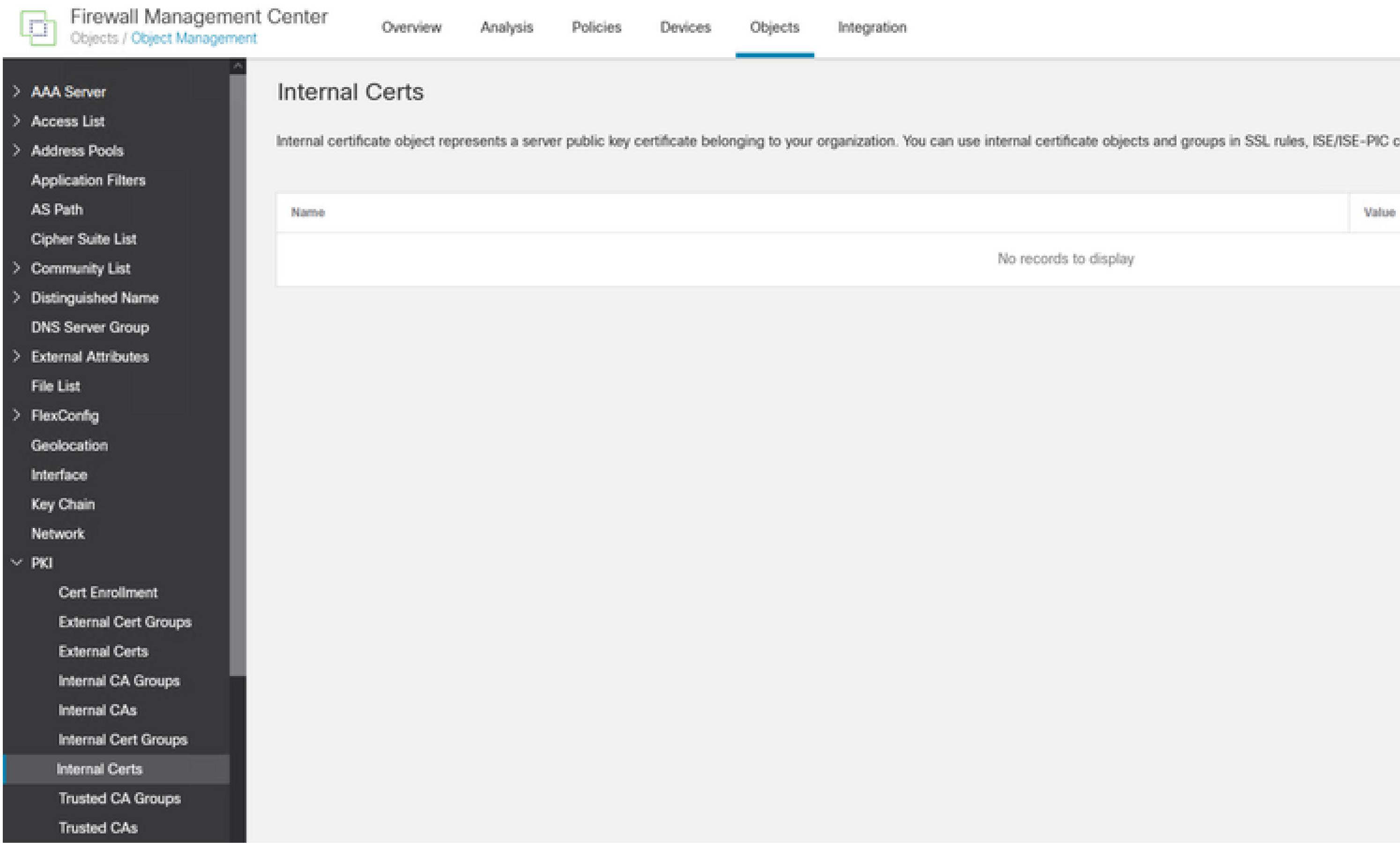


Name	Date modified	Type	Size
CertificateServicesEndpointSubCA-ssptise01_	21/08/2023 04:55	Security Certificate	
CertificateServicesNodeCA-ssptise01_	21/08/2023 04:55	Security Certificate	
CertificateServicesRootCA-ssptise01_	21/08/2023 04:55	Security Certificate	
sspt_fmc01_lab.ssptsec.mex_sspt_fmc01_lab.ssptsec.mex	21/08/2023 04:55	Security Certificate	
sspt_fmc01_lab.ssptsec.mex_sspt_fmc01_lab.ssptsec.mex.key	21/08/2023 04:55	KEY File	

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**.



Internal Certs

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 c

Name	Value
No records to display	

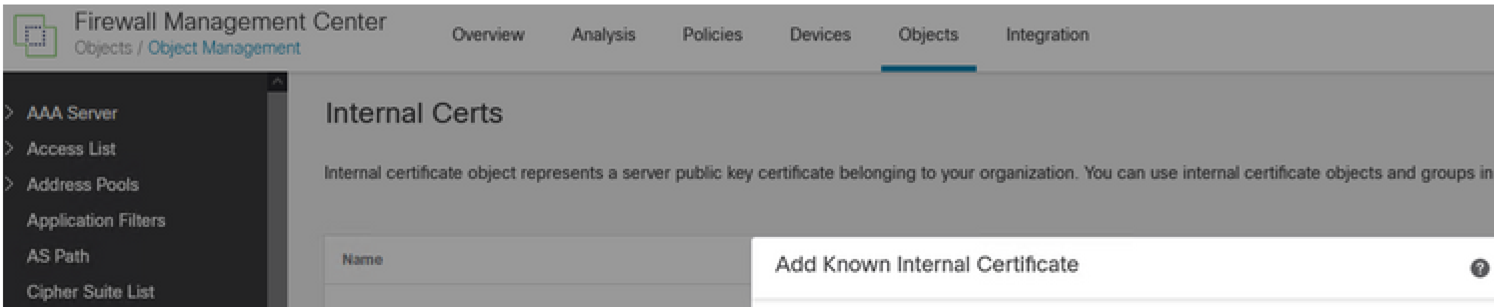
Adding the FMC certificate as internal certificate.

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** as well 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.



Internal Certs

Internal certificate object represents a server public key certificate belonging to your organization. You can use internal certificate objects and groups in

Name

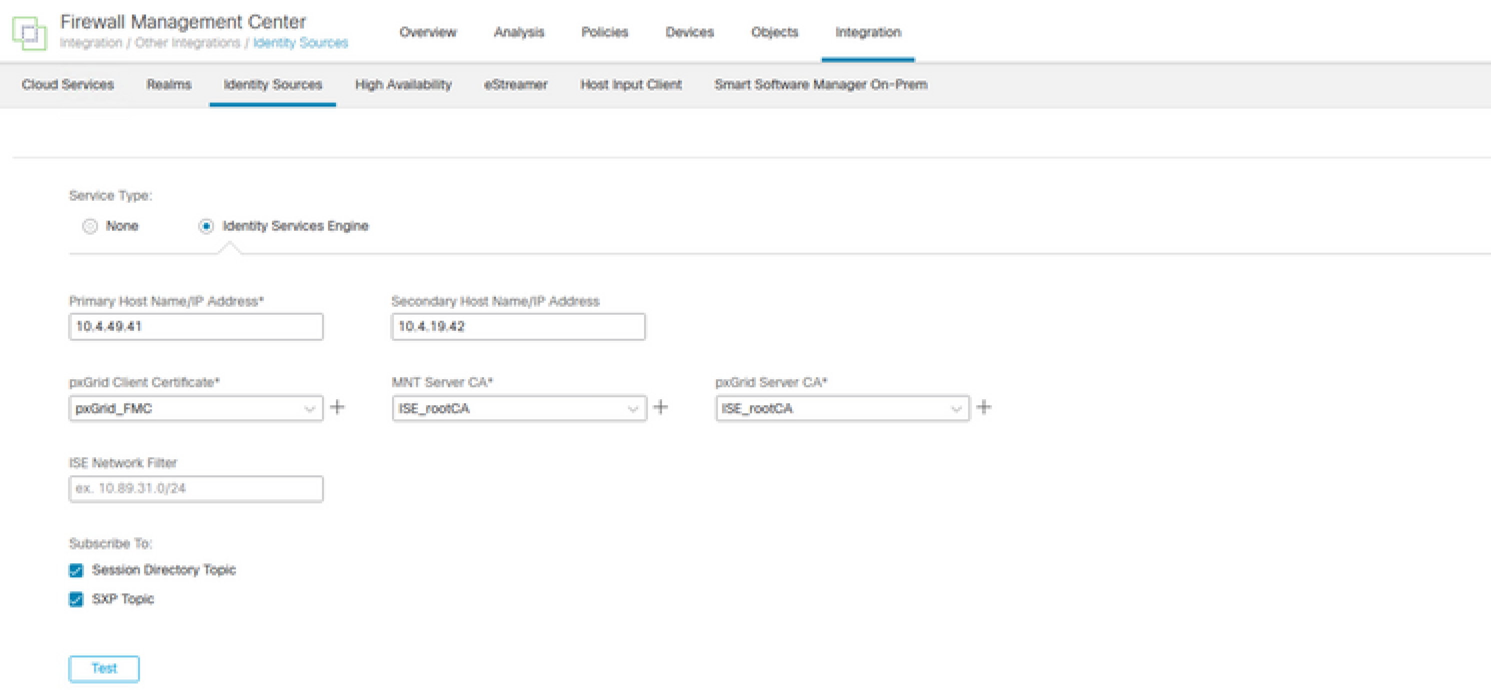
Add Known Internal Certificate

: The pxGrid Server CA correspond 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.



Service Type:
○ None ● Identity Services Engine

Primary Host Name/IP Address*: 10.4.49.41
Secondary Host Name/IP Address: 10.4.19.42
pxGrid Client Certificate*: pxGrid_FMC
MNT Server CA*: ISE_rootCA
pxGrid Server CA*: ISE_rootCA
ISE Network Filter: ex. 10.89.31.0/24

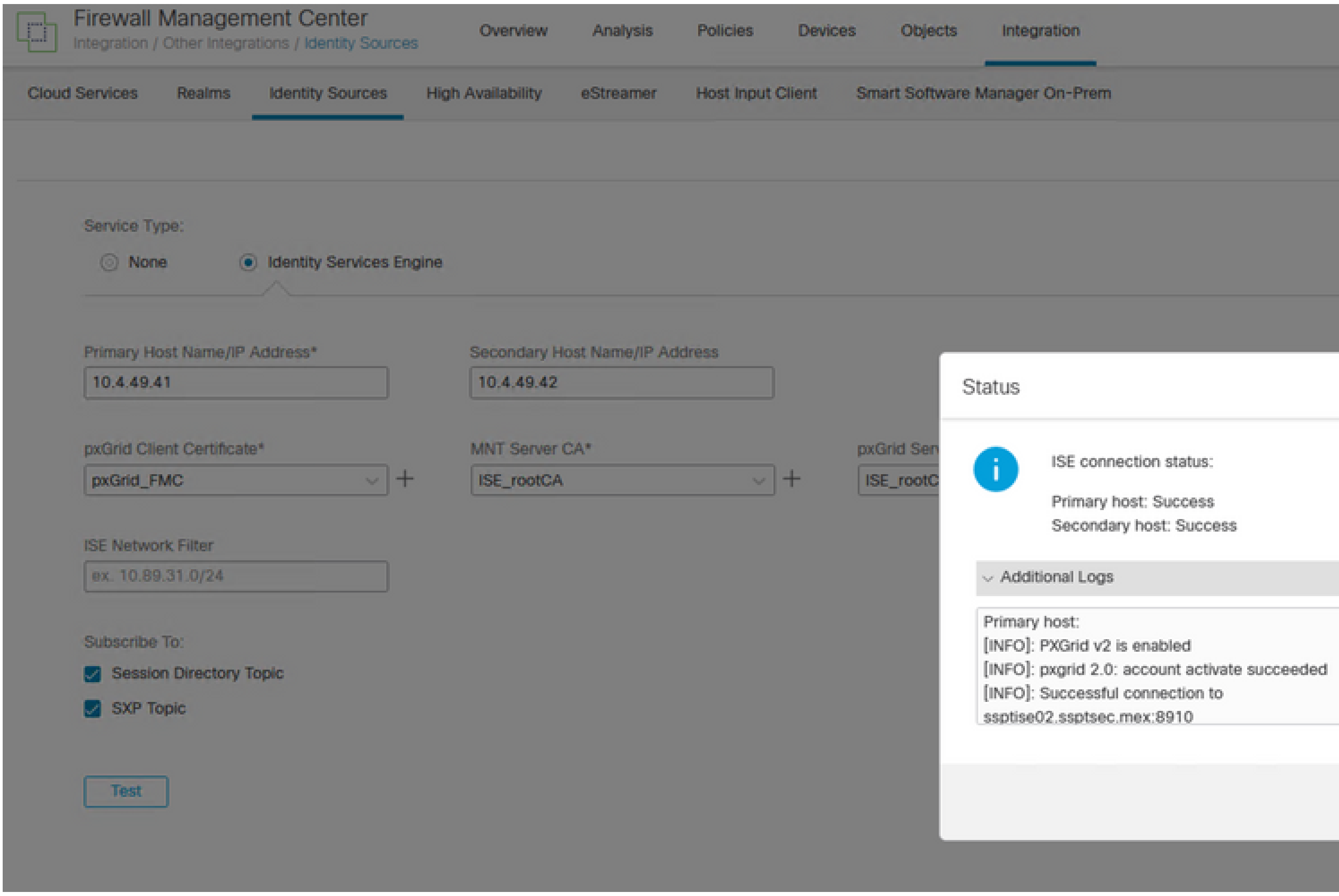
Subscribe To:
☑ Session Directory Topic
☑ SXP Topic

Setting up ISE as Identity Source in FMC.

Verify.

Validation on FMC.

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



Service Type:
○ None ● Identity Services Engine

Primary Host Name/IP Address*: 10.4.49.41
Secondary Host Name/IP Address: 10.4.49.42
pxGrid Client Certificate*: pxGrid_FMC
MNT Server CA*: ISE_rootCA
pxGrid Ser: ISE_rootC
ISE Network Filter: ex. 10.89.31.0/24

Subscribe To:
☑ Session Directory Topic
☑ SXP Topic

ISE connection status:

Primary host: Success
Secondary host: Success

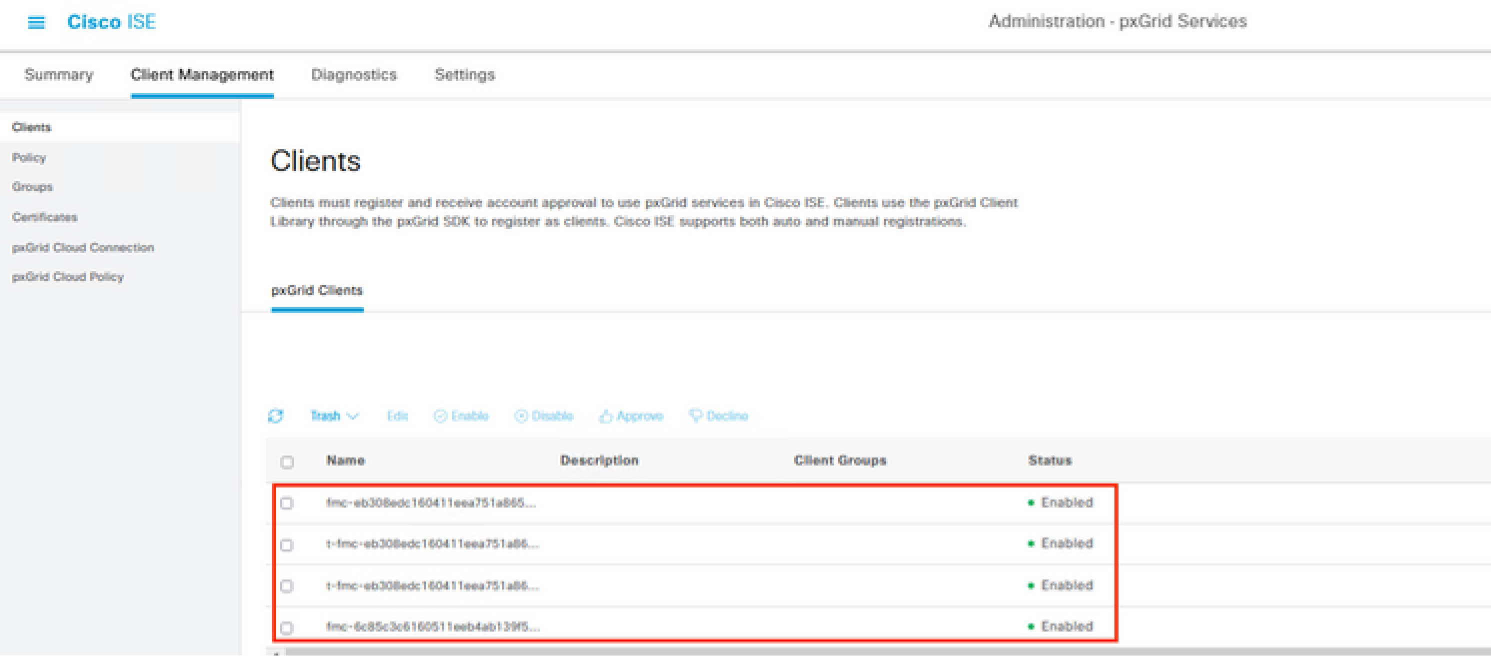
```
Primary host:
[INFO]: PXGrid v2 is enabled
[INFO]: pxgrid 2.0: account activate succeeded
[INFO]: Successful connection to
ssptise02.ssptsec.mex:8910
```

PxGrid successful communication.

```
[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, AdaptiveNetwo
[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, AdaptiveNetwo
[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 menu **Administration** > **pxGrid Services** > **Client Management** > **Clients**) clients with the name **fmc** are included and enabled.



Clients

Clients must register and receive account approval to use pxGrid services in Cisco ISE. Clients use the pxGrid Client Library through the pxGrid SDK to register as clients. Cisco ISE supports both auto and manual registrations.

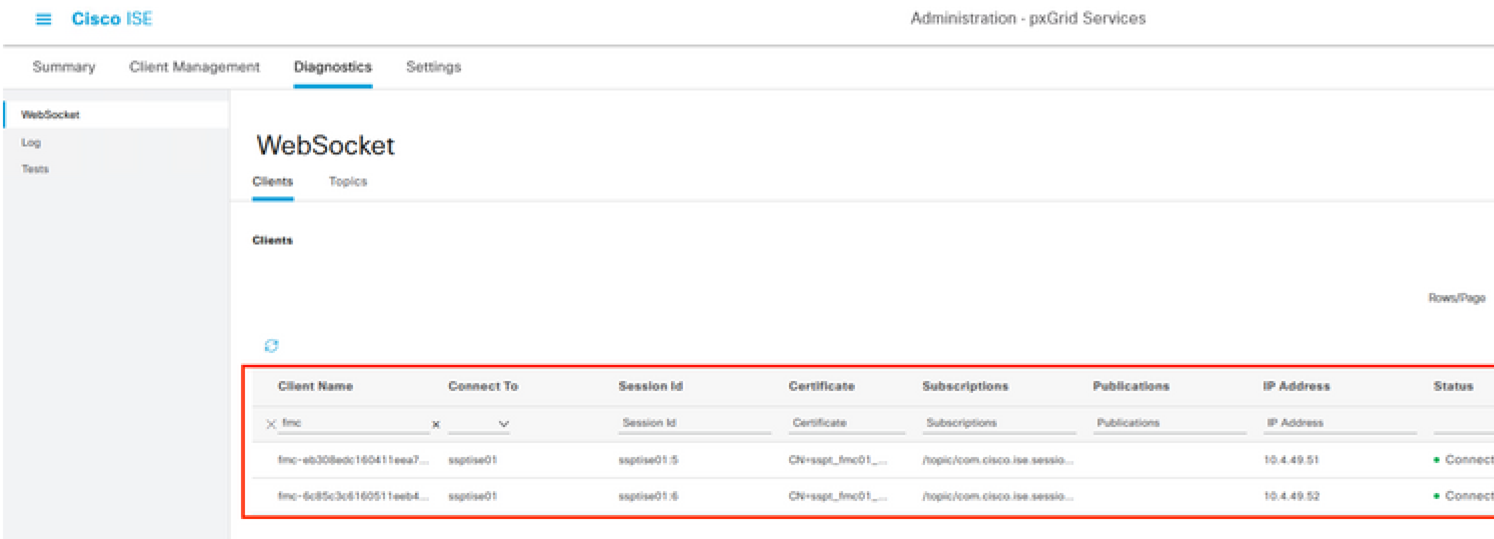
□	Name	Description	Client Groups	Status
□	fmc-eb308edc160411eea751a865...			● Enabled
□	t-fmc-eb308edc160411eea751a86...			● Enabled
□	t-fmc-eb308edc160411eea751a86...			● Enabled
□	fmc-6c85c3c6160511eeb4ab139f5...			● Enabled

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:



Client Name	Connect To	Session Id	Certificate	Subscriptions	Publications	IP Address	Status
fmc		Session Id	Certificate	Subscriptions	Publications	IP Address	
fmc-eb308edc160411eea7...	ssptise01	ssptise01:5	CN=sspt_fmc01_...	/topic/com.cisco.ise.sessio...		10.4.49.51	● Connect
fmc-6c85c3c6160511eeb4...	ssptise01	ssptise01:6	CN=sspt_fmc01_...	/topic/com.cisco.ise.sessio...		10.4.49.52	● Connect

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.

WebSocket

```
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 tcpudump packet capture to confirm bidirectional communication.

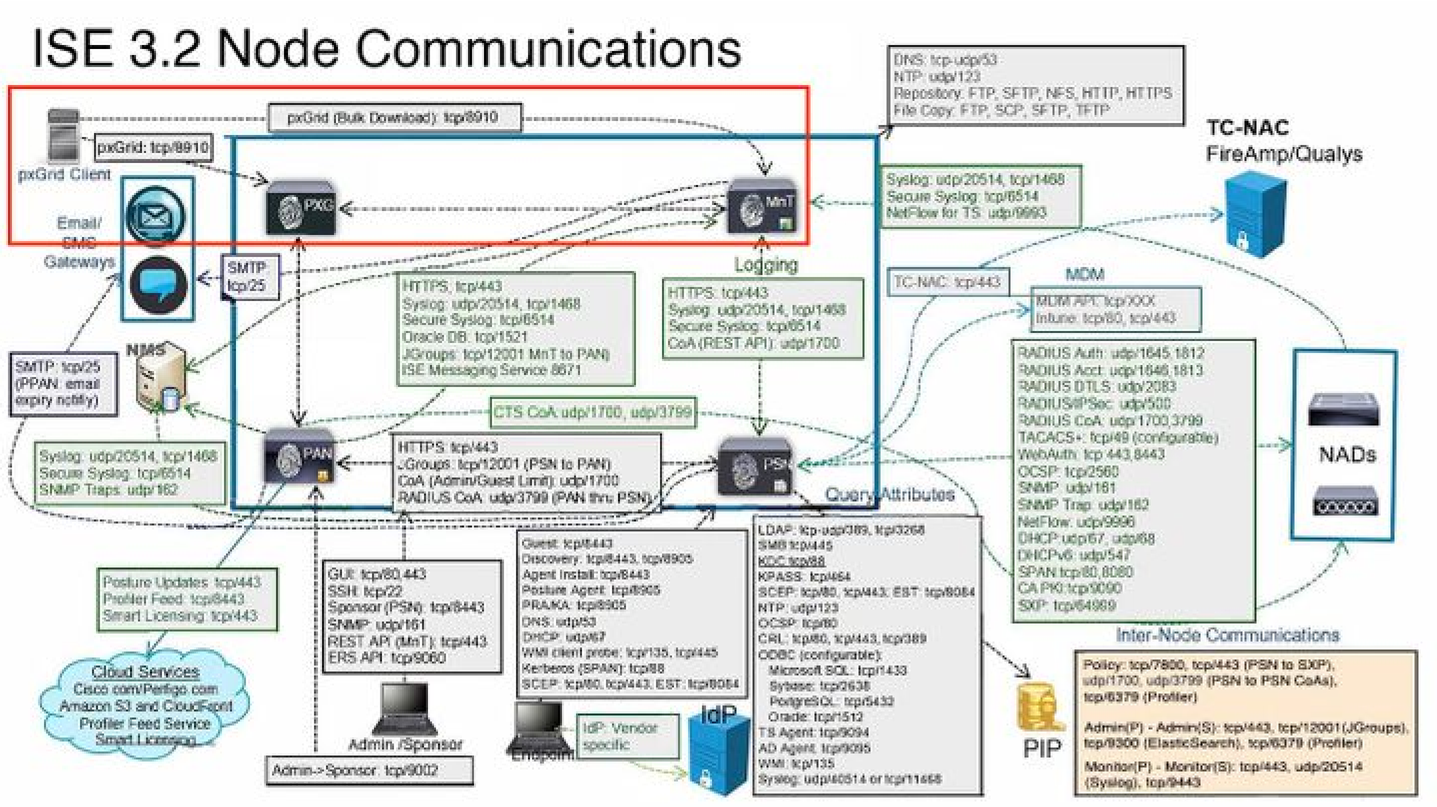
<#root>

```
>

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



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,
```

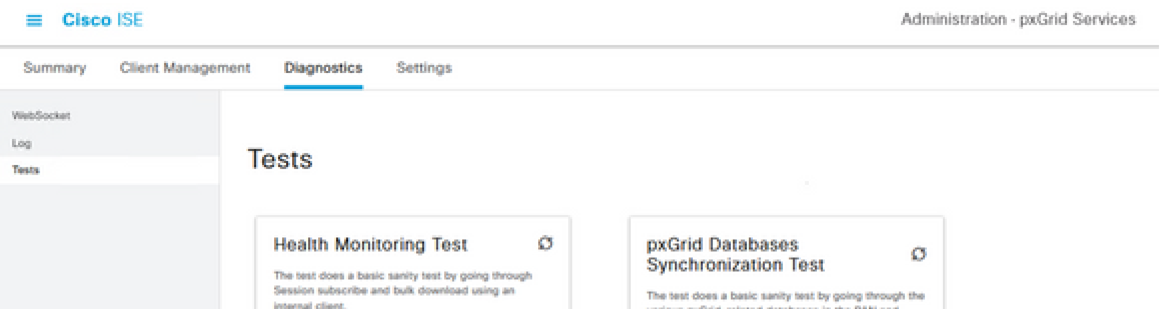
There are 2 test available on ISE that diagnose the overall status of the pxGrid implementations.

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.



The test does a basic sanity test by going through Session subscribe and bulk download using an internal client.

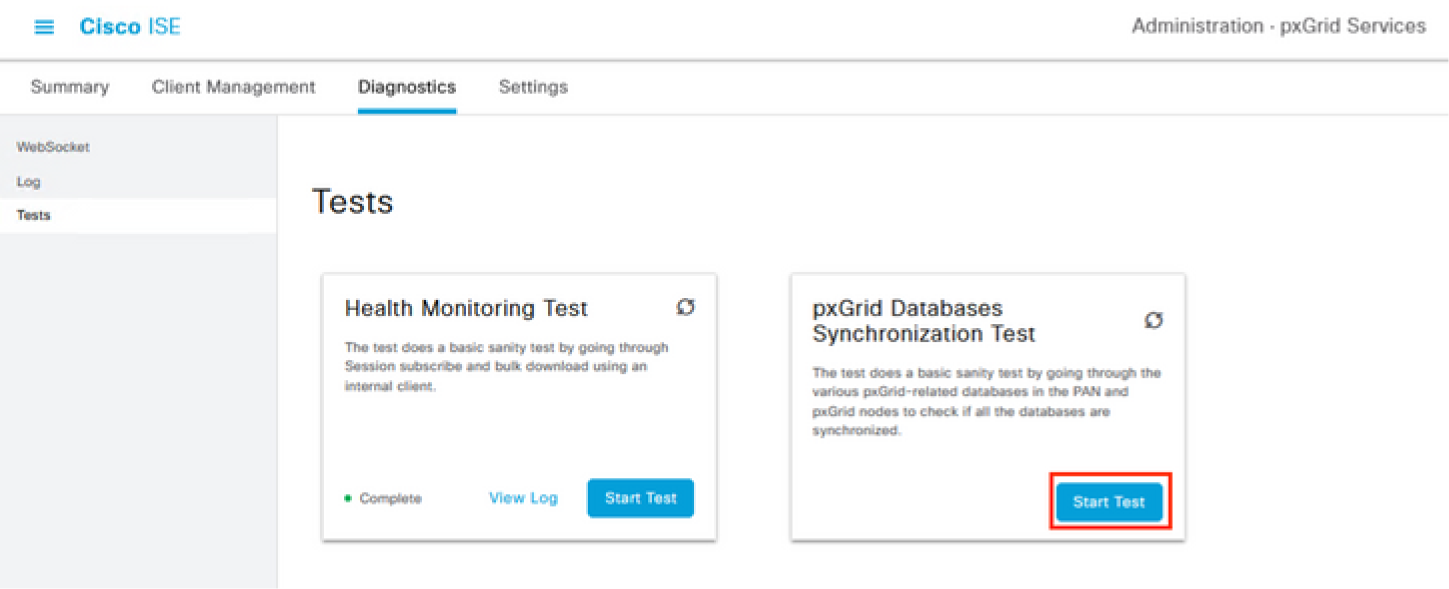
The test does a basic sanity test by going through the

```
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.



The test does a basic sanity test by going through Session subscribe and bulk download using an internal client.

The test does a basic sanity test by going through the various pxGrid-related databases in the PAN and pxGrid nodes to check if all the databases are synchronized.

PxGrid Databases Synchronization Test.

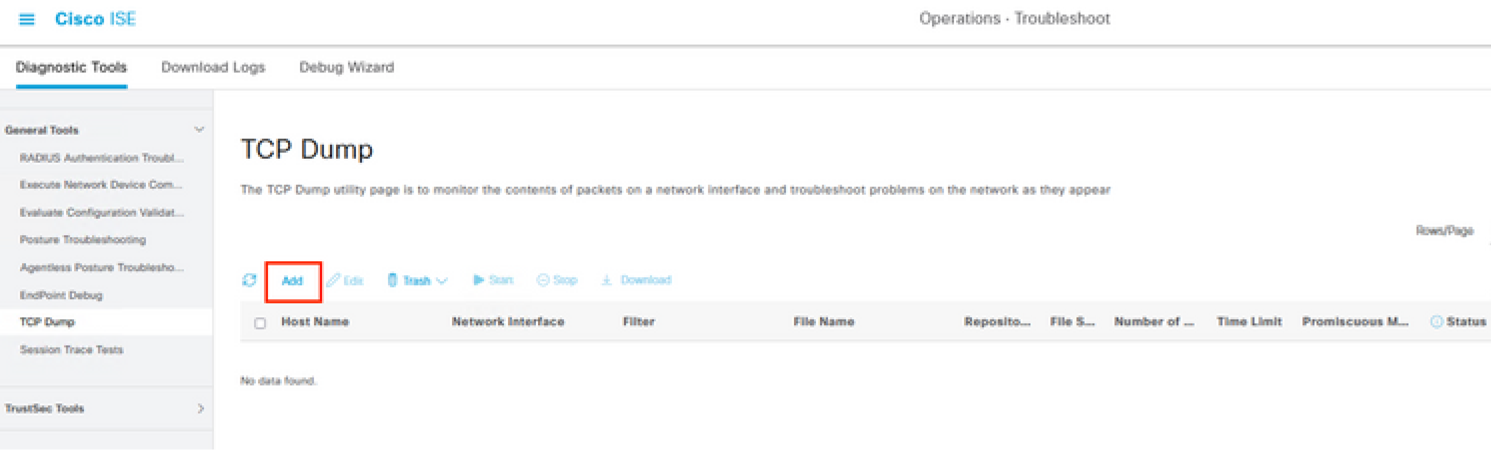
From the logs generated, this output was obtained.

```
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.



The TCP Dump utility page is to monitor the contents of packets on a network interface and troubleshoot problems on the network as they appear

□	Host Name	Network Interface	Filter	File Name	Reposito...	File S...	Number of ...	Time Limit	Promiscuous M...	Status

No data found.

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**.

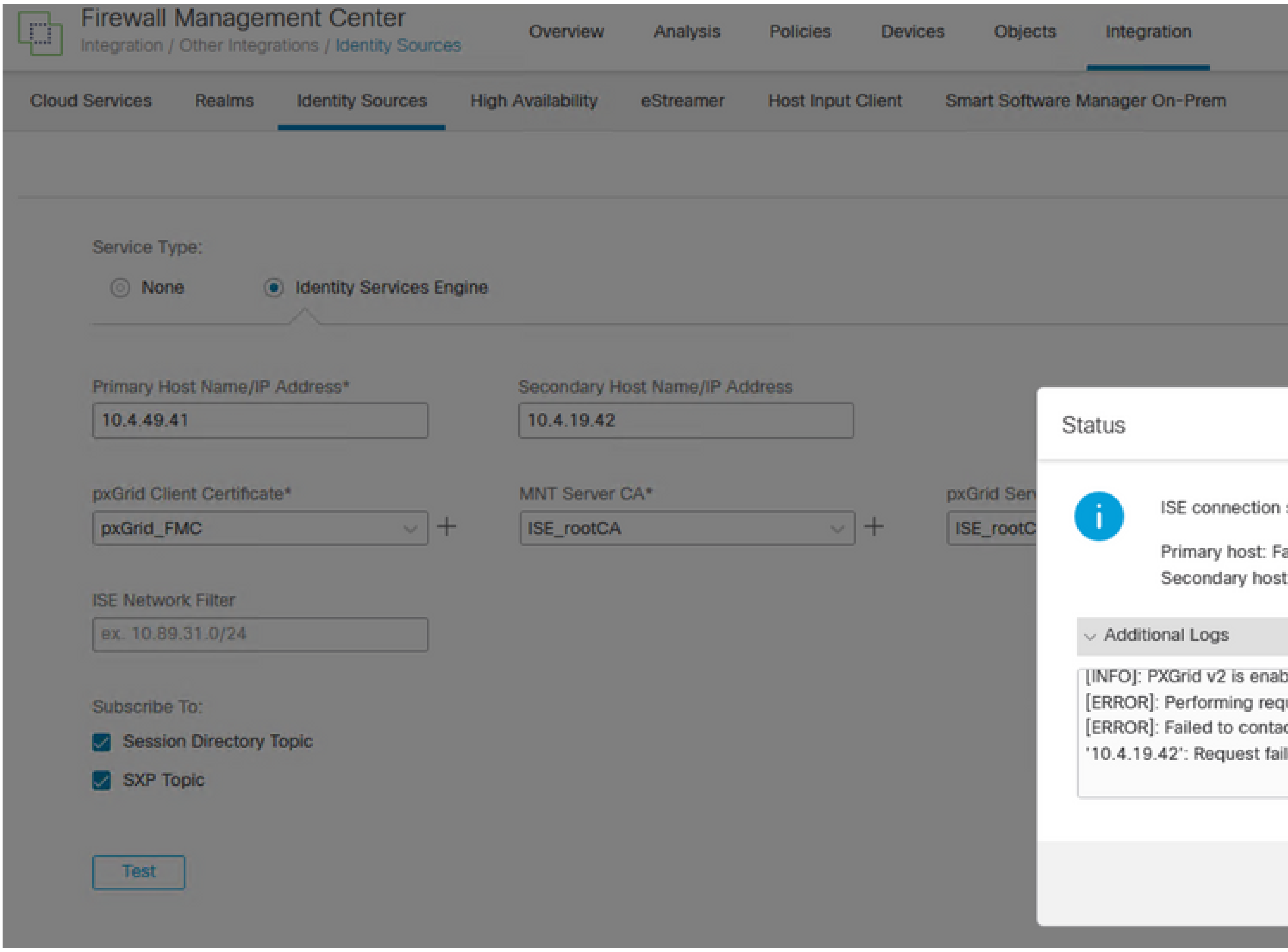
```
ise-pxgriddirect.log
pxgrid/pxgrid-server.log
pxgrid/pxgrid-test.log
pxgrid/pxgrid_dbsync_summary.log
pxgrid/pxgrid_internal_dbsync_summary.log
pxgriddirect.log
```

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:



Service Type:

○ None ● Identity Services Engine

Primary Host Name/IP Address*: 10.4.49.41

Secondary Host Name/IP Address: 10.4.19.42

pxGrid Client Certificate*: pxGrid_FMC

MNT Server CA*: ISE_rootCA

pxGrid Ser: ISE_rootC

ISE Network Filter: ex. 10.89.31.0/24

Subscribe To:

☑ Session Directory Topic

☑ SXP Topic

Status

ISE connection

Primary host: Fa
Secondary host

Additional Logs

```
[INFO]: PXGrid v2 is enab
[ERROR]: Performing requ
[ERROR]: Failed to contac
'10.4.19.42': Request fail
```

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.