Configure ISE 2.4 and FMC 6.2.3 pxGrid Integration

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Configure ISE](#)
[Step 1. Enable pxGrid Services](#)
[Step 2. Configure ISE to Approve all pxGrid Certificate-Based Accounts](#)
[Step 3. Export ISE MNT Admin Certificate and pxGrid CA Certificates](#)
[Configure FMC](#)
[Step 4. Add a new realm to FMC](#)
[Step 5. Generate FMC CA Certificate](#)
[Step 6. Extract the Certificate and Private Key from the Generated Certificate with the Use of OpenSSL](#)
[Step 7. Install certificate into FMC](#)
[Step 8. Import the FMC Certificate into ISE](#)
[Step 9. Configure pxGrid Connection on FMC](#)
[Verify](#)
[Verification in ISE](#)
[Verification in FMC](#)
[Troubleshoot](#)

Introduction

This document describes the configuration process for integration of the ISE pxGrid version 2.4 and FMC version 6.2.3.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

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

Components Used

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

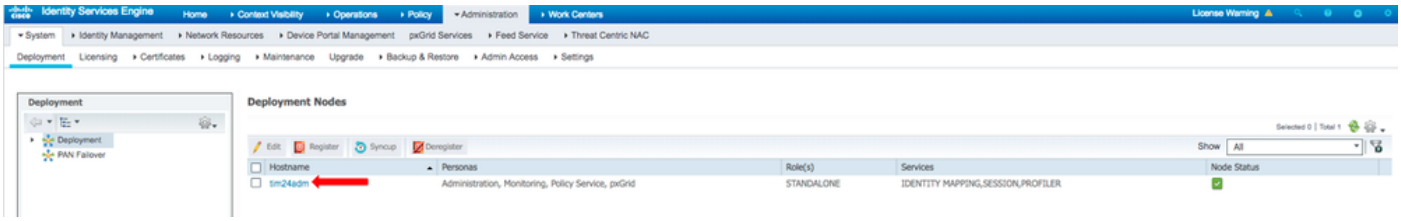
- Standalone ISE 2.4
- FMCv 6.2.3
- Active Directory 2012R2
- Identity Services Engine (ISE) pxGrid version 2.4
- Firepower Management Center (FMC) version 6.2.3

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.

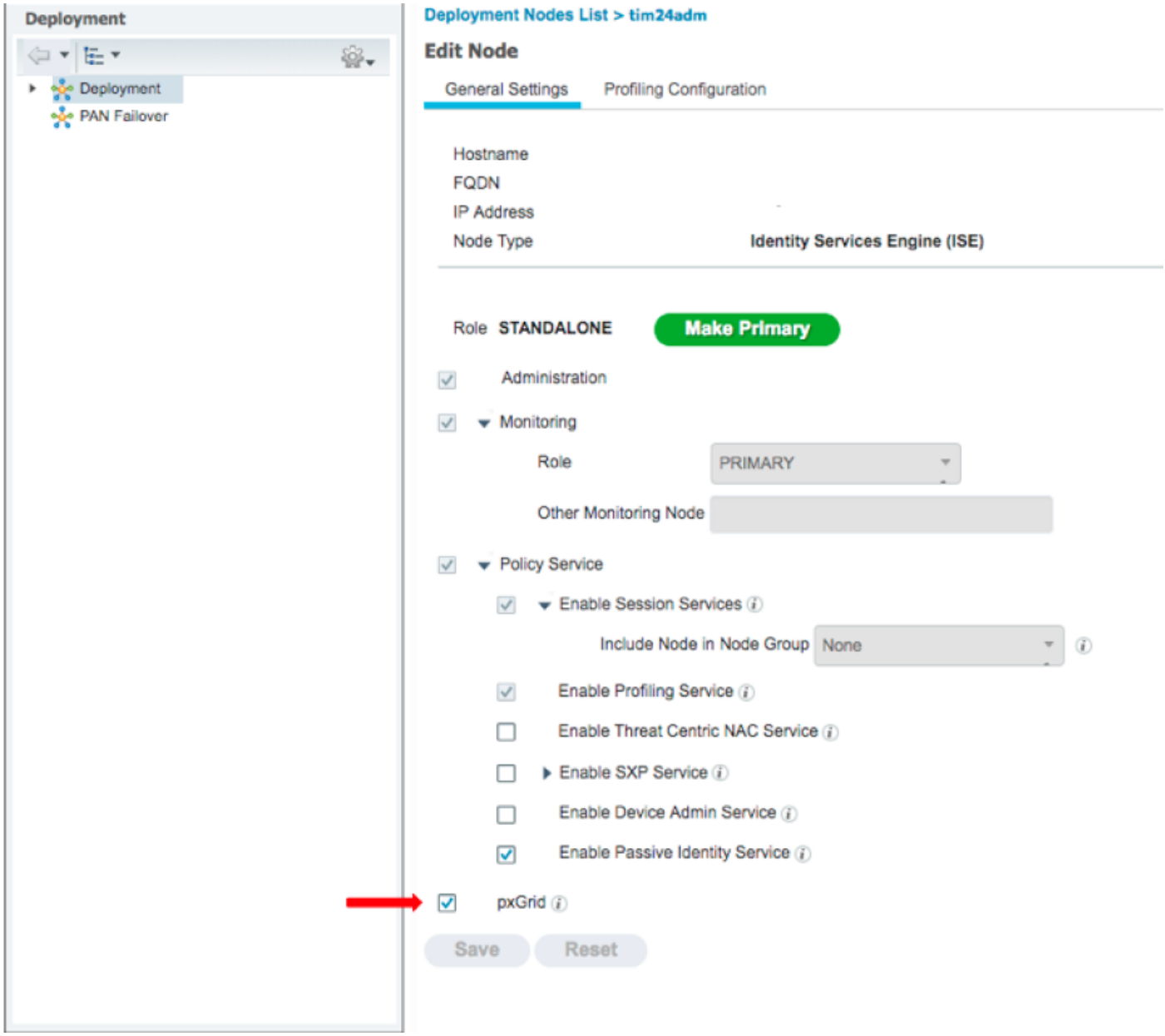
Configure ISE

Step 1. Enable pxGrid Services

1. Log into the ISE Admin GUI, navigate to **Administration > Deployment.**
2. Select the ISE node to be used for pxGrid persona.



3. Enable pxGrid service and click **Save** as shown in the image.



4. Verify that the pxGrid services run from the CLI.

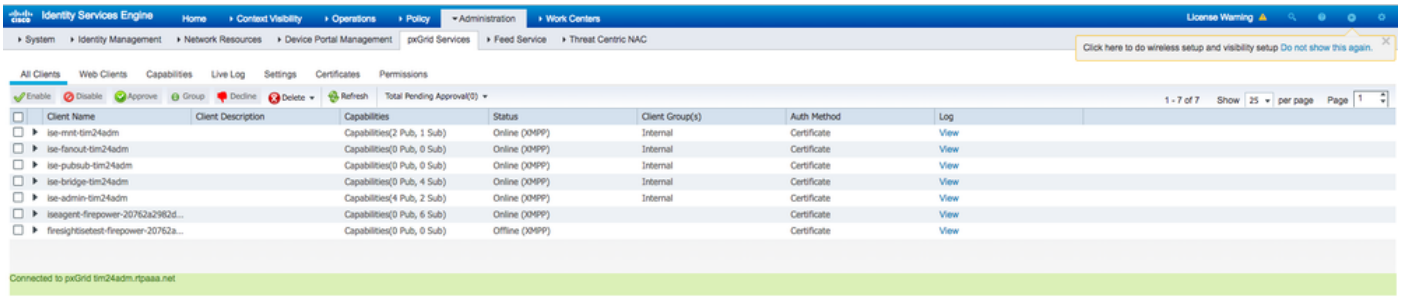
> **Note**: The process requires up to 5 minutes for the pxGrid services to fully start and determine High Availability (HA) state if more than one pxGrid node is in use.

5. SSH into the ISE pxGrid node CLI and check the application status.

```
# show application status ise | in pxGrid
pxGrid Infrastructure Service running 24062
pxGrid Publisher Subscriber Service running 24366
pxGrid Connection Manager running 24323
pxGrid Controller running 24404
#
```

6. Access the ISE Admin GUI and verify that the services are online and function. Navigate to **Administration > pxGrid Services**.

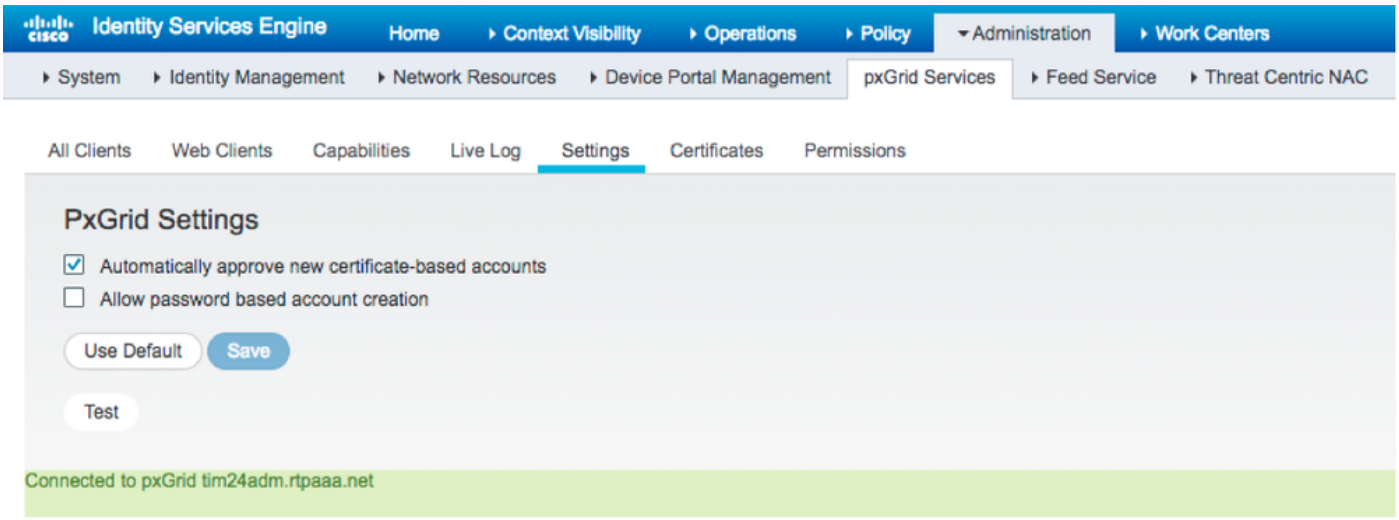
7. At the bottom of the page, ISE displays **Connected to pxGrid <pxGrid node FQDN>**.



Step 2. Configure ISE to Approve all pxGrid Certificate-Based Accounts

1. Navigate to **Administration > pxGrid Services > Settings.**

2. Check the box: "Automatically approve new certificate-based accounts" and click **Save**.



> **Note**: The administrator must manually approve the FMC connection to ISE if this option is not enabled.

Step 3. Export ISE MNT Admin Certificate and pxGrid CA Certificates

1. Navigate to **Administration > Certificates > System Certificates**.

2. Expand the Primary Monitoring (MNT) node if not enabled on the Primary Administration node.

3. Select the certificate with the Used-By "Admin" field.

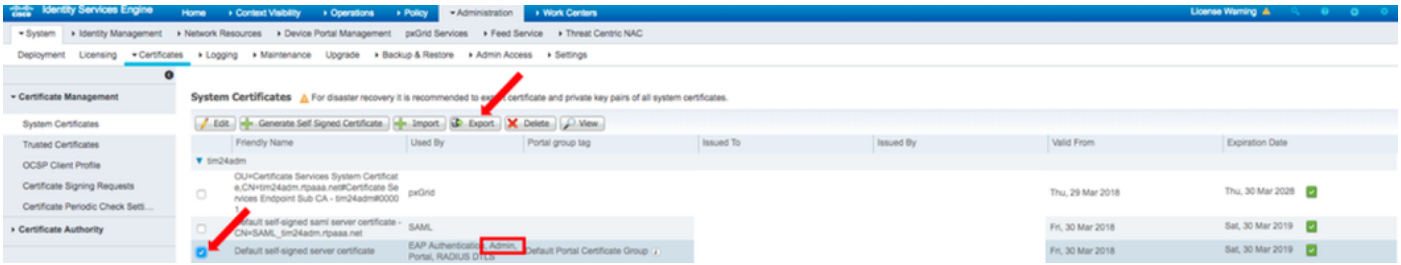
> **Note**: This guide uses the default ISE Self-Signed Certificate for Admin usage. If you use a Certificate Authority (CA) signed Admin Certificate, export the Root CA that signed the Admin certificate on the ISE MNT node.

4. Click **Export**.

5. Choose the option to Export Certificate and Private Key.

6. Set an encryption key.

7. **Export** and **Save** the file as shown in the image.



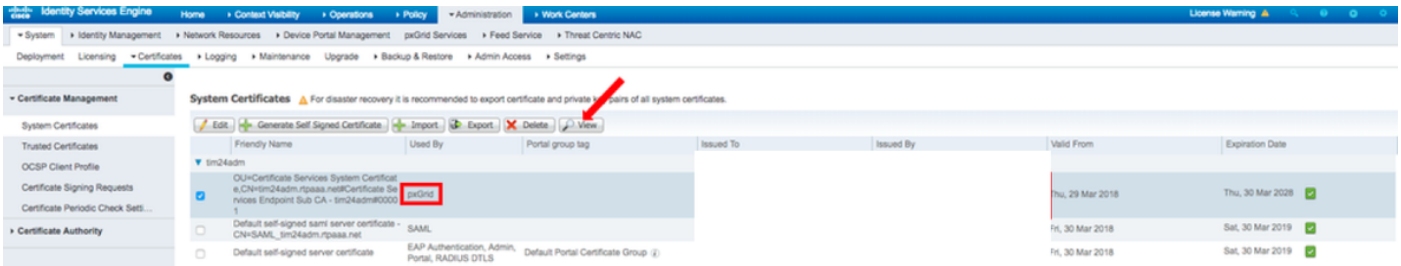


9. Return to the ISE System Certificates screen.

10. Determine the Issued By field on the certificate with the "pxGrid" usage in the Used By column.

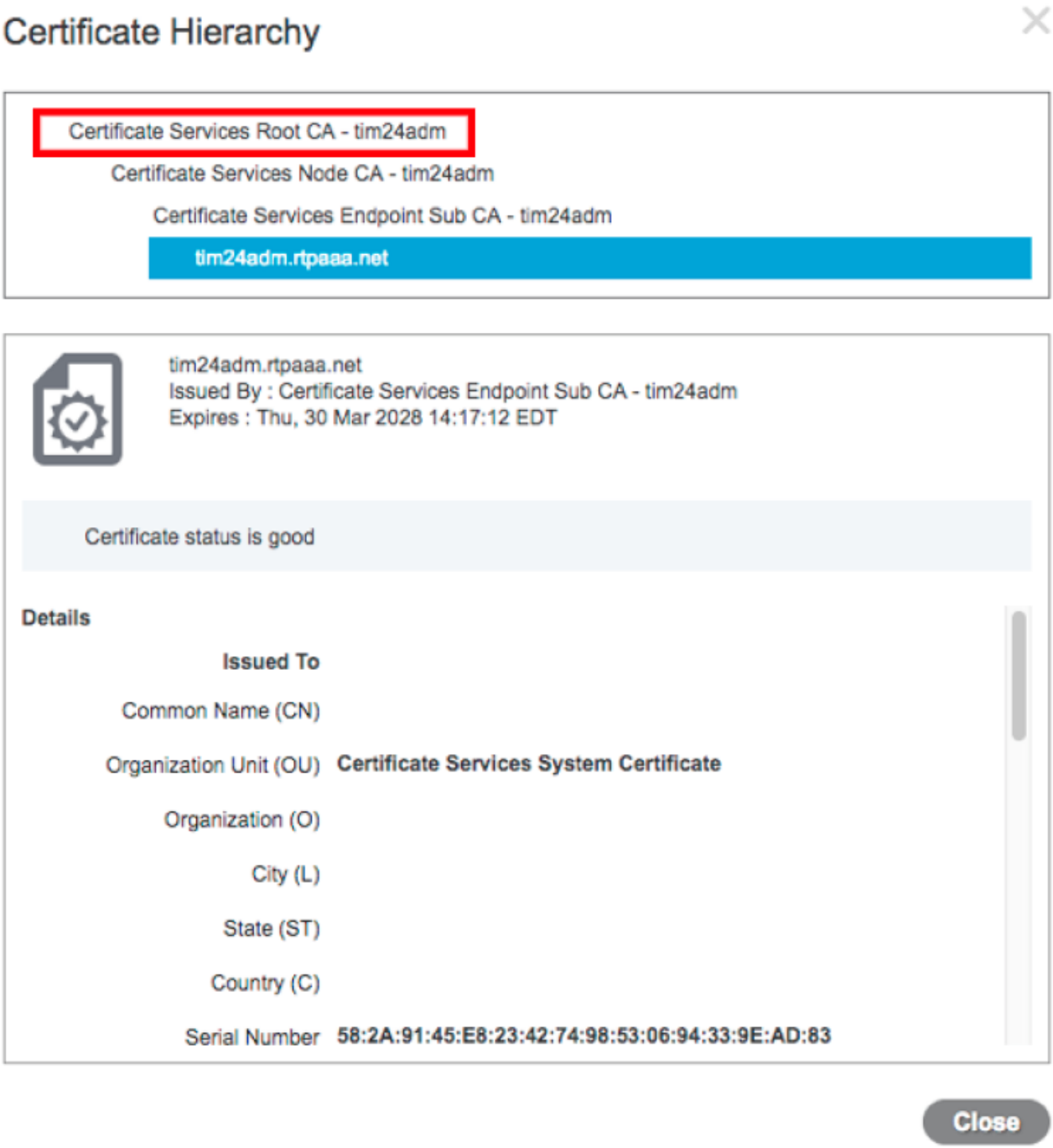
> **Note**: In older versions of ISE, this was a self-signed certificate, but from 2.2 onwards this certificate is issued by the Internal ISE CA Chain by default.

11. Select the Certificate and click **View** as shown in the image.



12. Determine the top level (Root) certificate. In this case it is **"Certificate Services Root CA - tim24adm".**

13. Close the certificate view window as shown in the image.

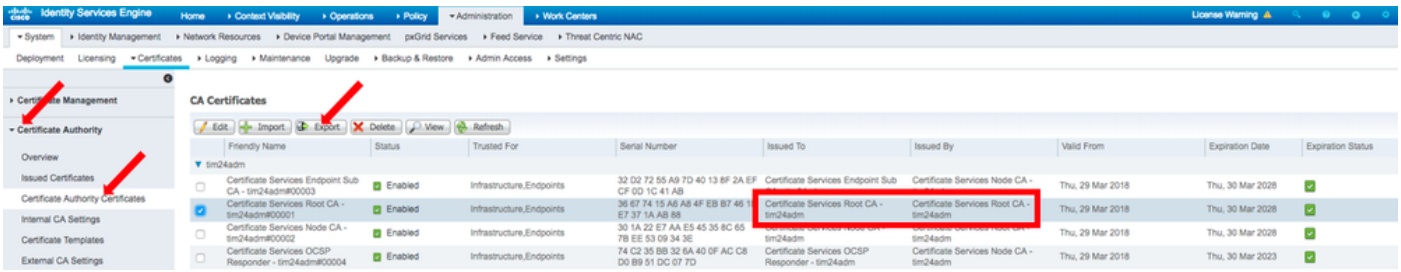


---

14. Expand the ISE Certificate Authority Menu.

15. Select **Certificate Authority Certificates**.

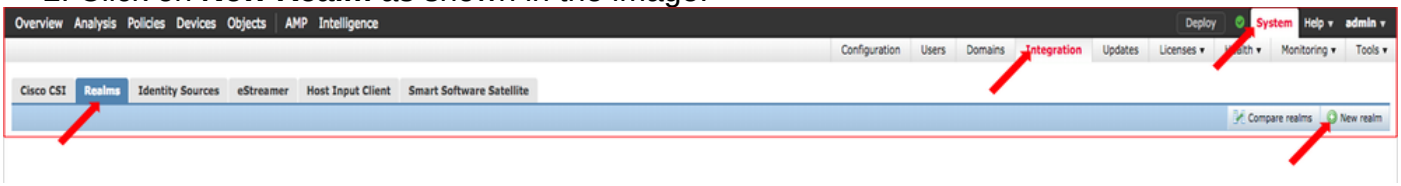
16. Select the Root Certificate that was identified and click **Export.** Then save the pxGrid Root CA certificate as shown in the image.



Configure FMC

Step 4. Add a new realm to FMC

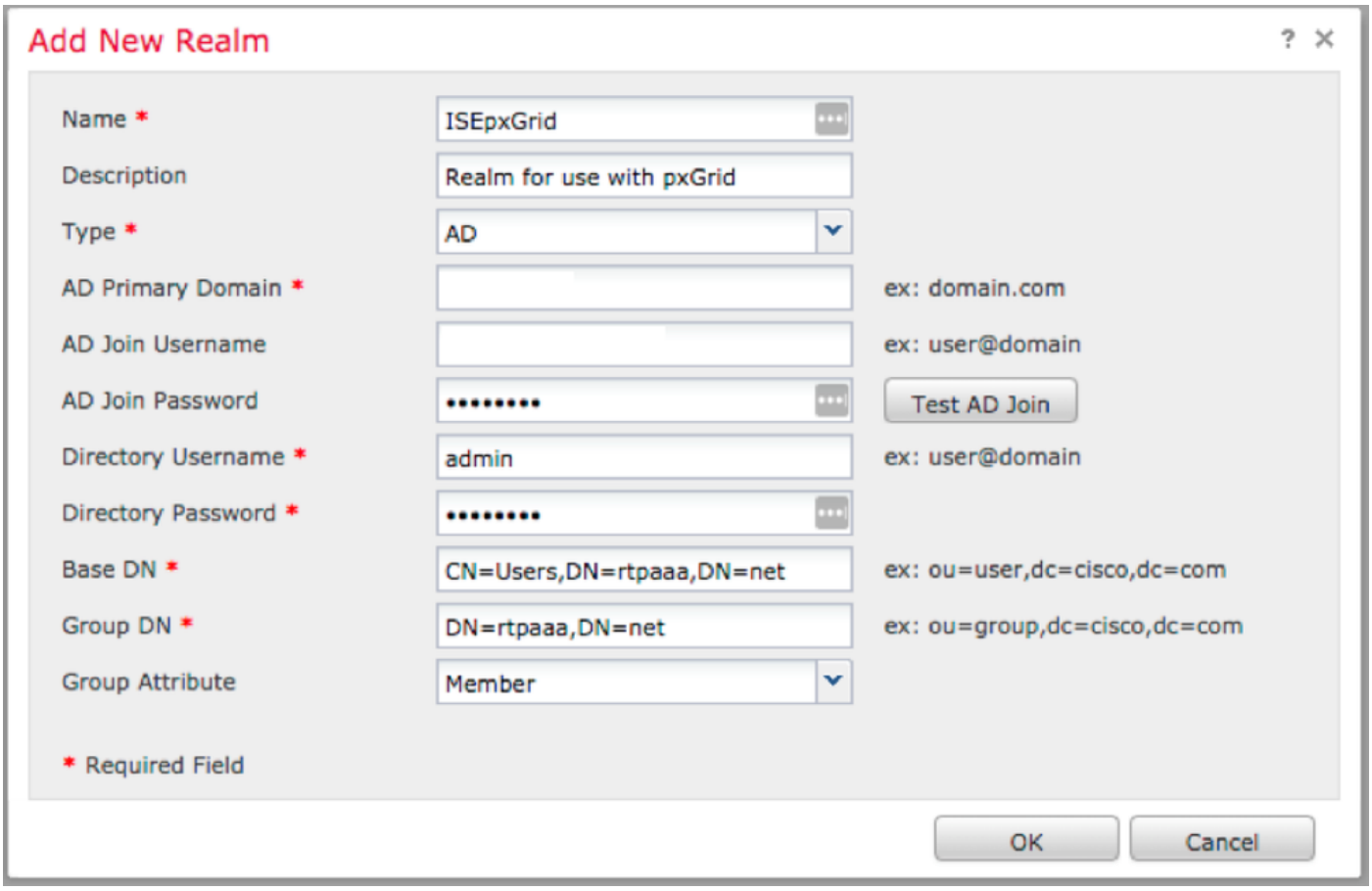
1. Access the FMC GUI and navigate to **System > Integration > Realms**.
2. Click on **New Realm** as shown in the image.



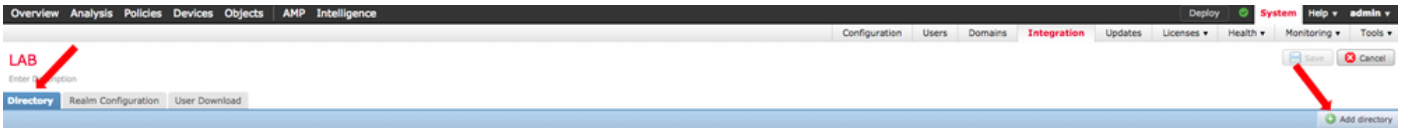
3. Fill out the form and click the Test Active Directory (AD) Join button.

   Note: The AD Join Username must be in User Principal Name (UPN) format or the test fails.

4. If the Test AD Join is successful, click **OK**.



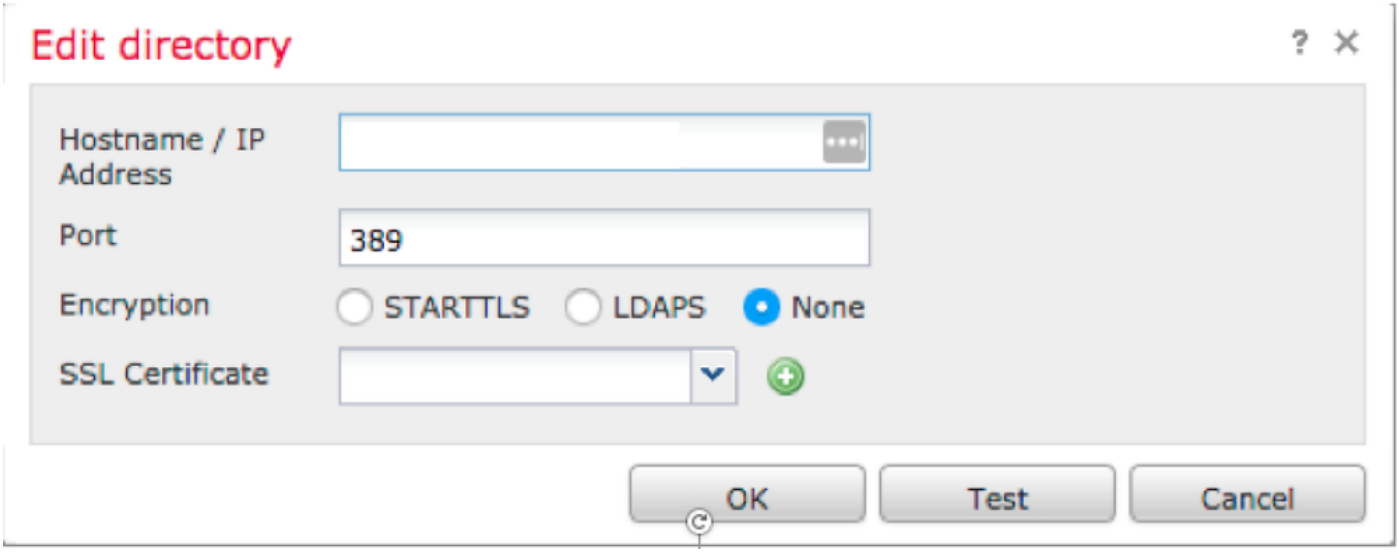
5. Click the **Directory** tab and then click **Add directory** as shown in the image.

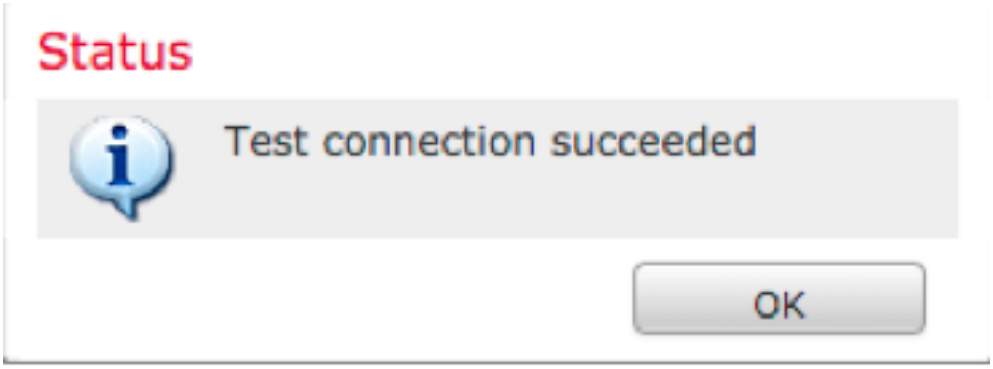


6. Configure IP/Hostname and Test Connection.

Note: If the Test fails, verify the credentials on the Realm Configuration tab.

7. Click **OK**.





8. Click the **User Download** tab.



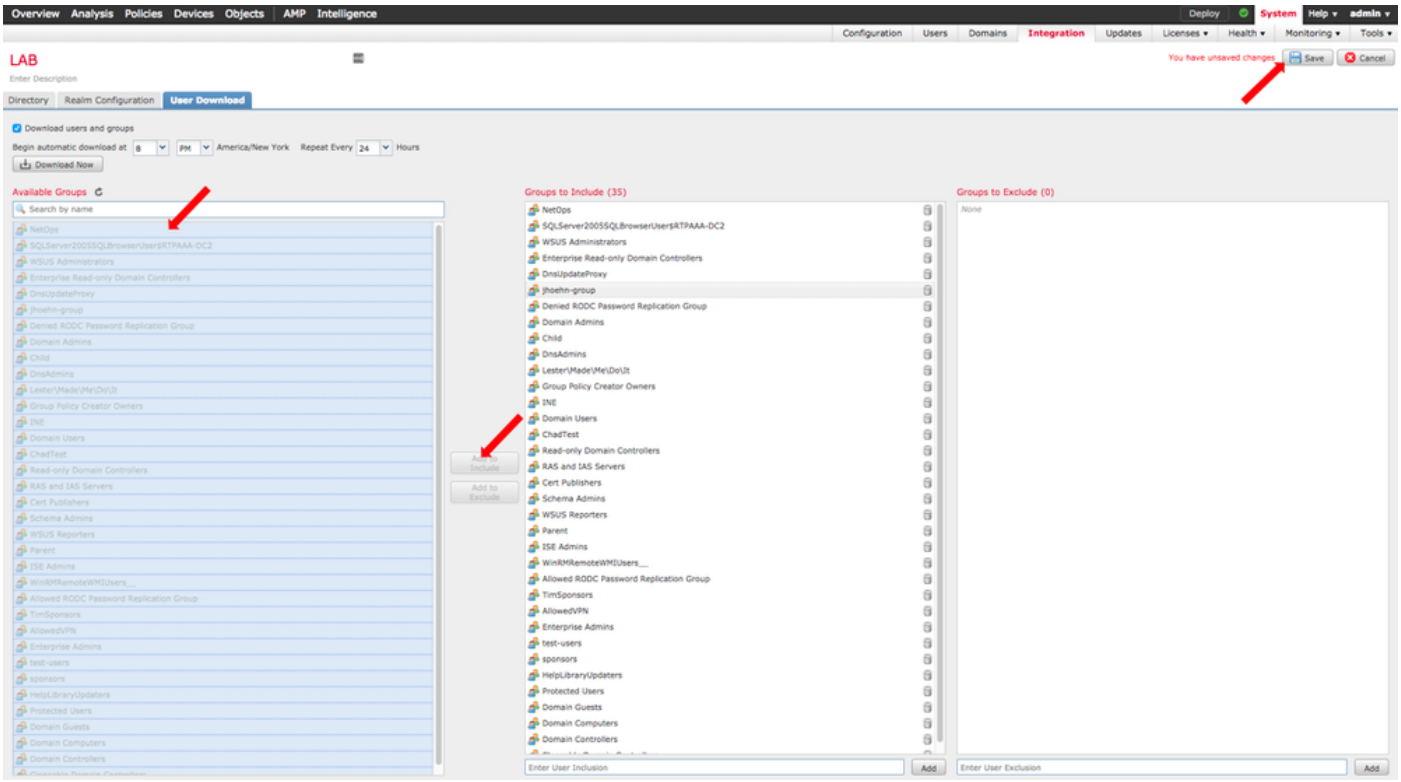
9. If not already selected, enable user and group download

10. Click Download Now



11. Once the list populates, add desired groups and select **Add to Include**.

12. Save the **Realm Configuration**.

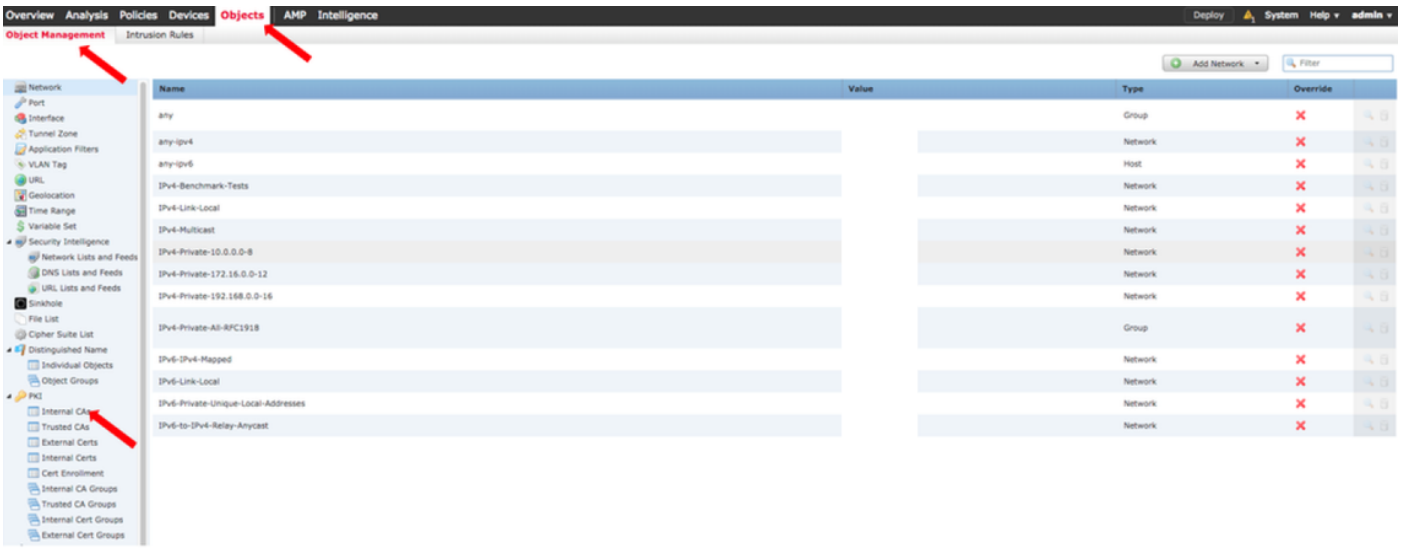


13. Enable the Realm State.



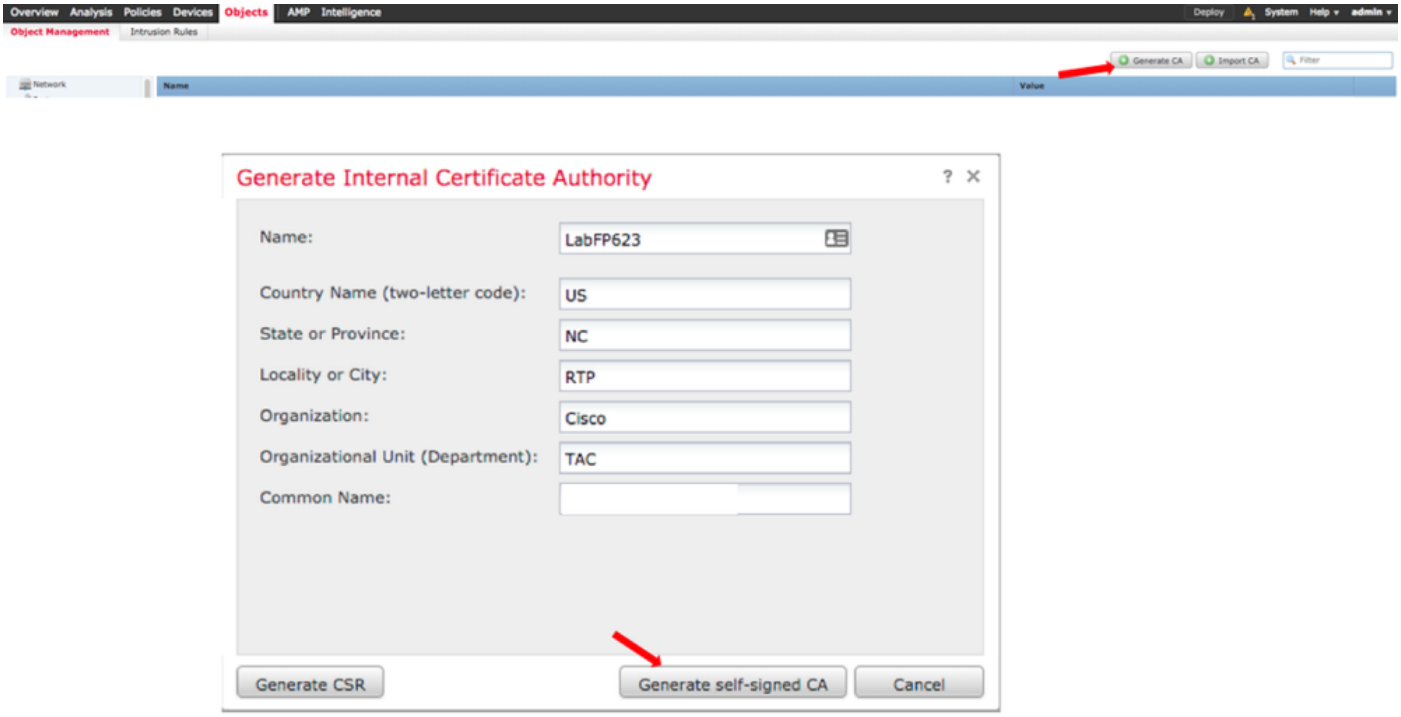
Step 5. Generate FMC CA Certificate

1. Navigate to **Objects > Object Management > Internal CAs** as shown in the image.



2. Click **Generate CA**.

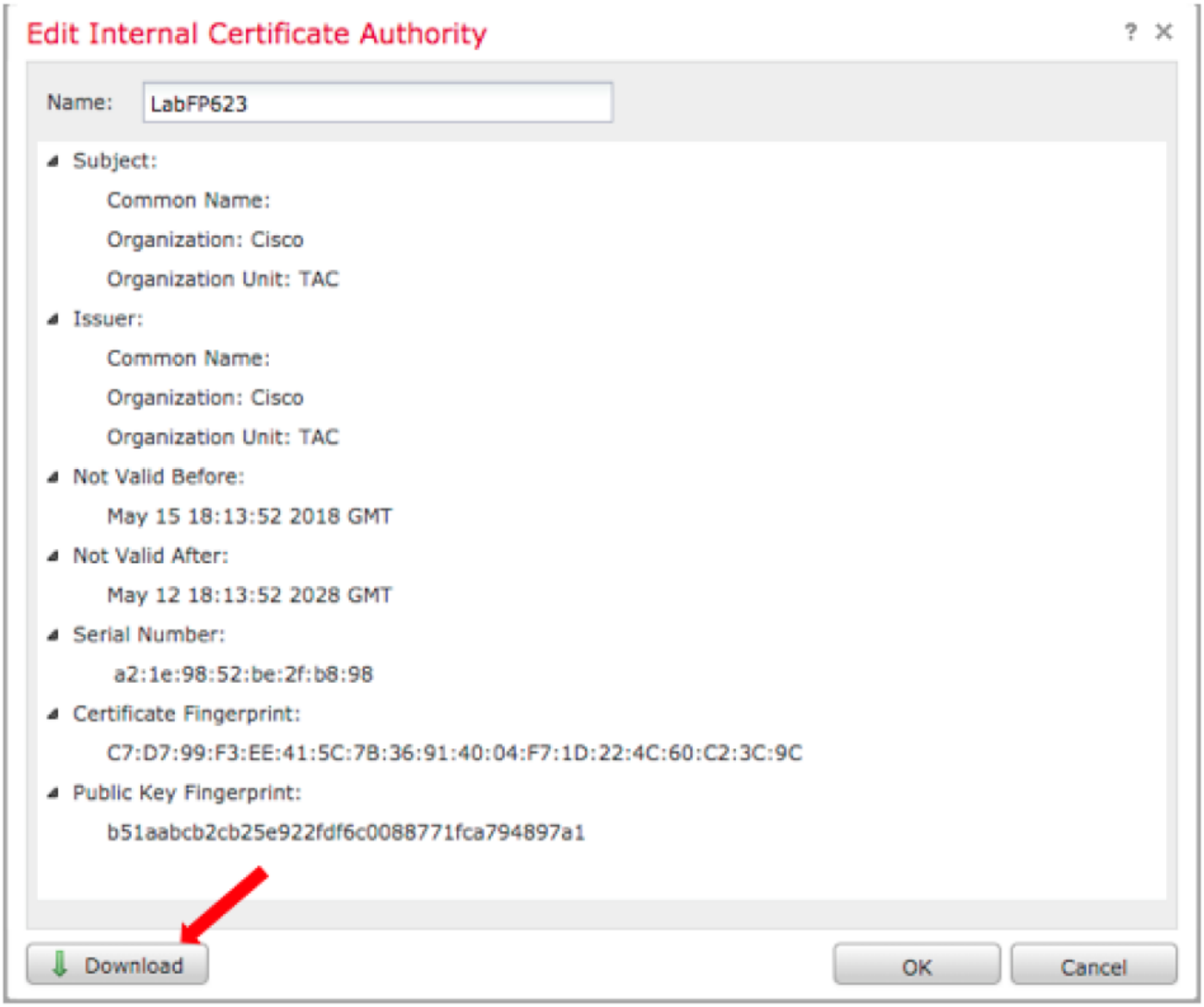
3. Fill out the form and click **Generate self-signed CA**.



4. Once generation completes, click on the pencil to the right of the generated CA Certificate as shown in the image.



5. Click **Download**.



6. Configure and confirm the encryption password and click **OK**.

7. Save the Public-Key Cryptography Standards (PKCS) p12 file to your local file system.

Step 6. Extract the Certificate and Private Key from the Generated Certificate with the Use of OpenSSL

This is done either on root of the FMC, or on any client capable of OpenSSL commands. This example uses a standard Linux shell.

1. Use **openssl** in order to extract the certficate (CER) and private key (PVK) from the p12 file.

2. Extract the CER file then configure the certificate export key from the cert generation on FMC.

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

3. Extract the PVK file, configure the certificate export key, then set a new PEM pass phrase and confirm.

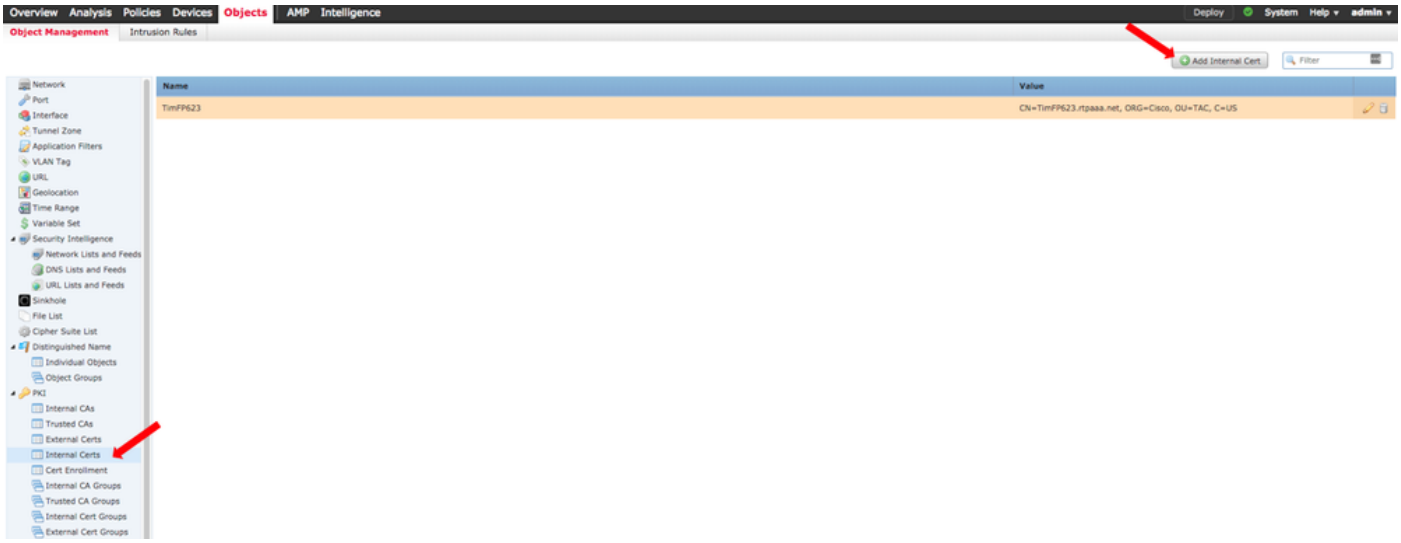
```
~$ openssl pkcs12 -nocerts -in <filename.p12> -out <filename.pvk>
Password:   Last login: Tue May 15 18:46:41 UTC 2018   Enter Import Password:   MAC verified OK
```

4. This PEM phrase is needed in the next step.

Step 7. Install certificate into FMC

1. Navigate to **Objects > Object Management > PKI > Internal Certs**.

2. Click **Add Internal Cert** as shown in the image.



3. Configure a name for the Internal Certificate.

4. Browse to the location of the CER file and select it. Once the Certificate Data populates, select the second.

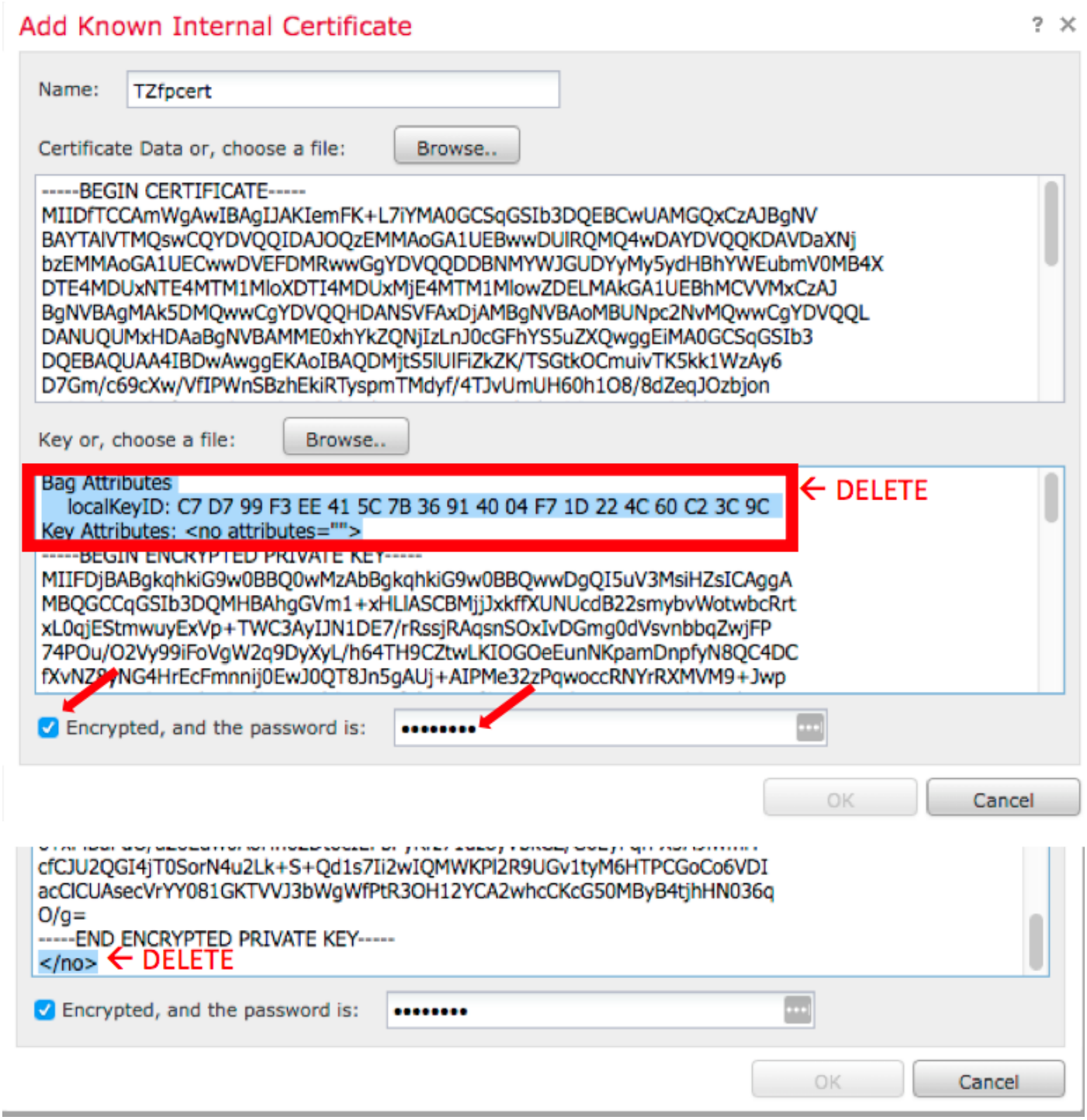
5. Browse **Option** and select the PVK file.

6. Delete any leading "Bag attributes" and any trailing values in the PVK section. The PVK begins with **-----BEGIN ENCRYPTED PRIVATE KEY-----** and end with **-----END ENCRYPTED PRIVATE KEY-----**.

> **Note**: You are not able to click **OK** if the PVK text has any characters outside of the leading and trailing hyphens.

7. Check the Encrypted box and configure the password created when the PVK was exported in Step 6.

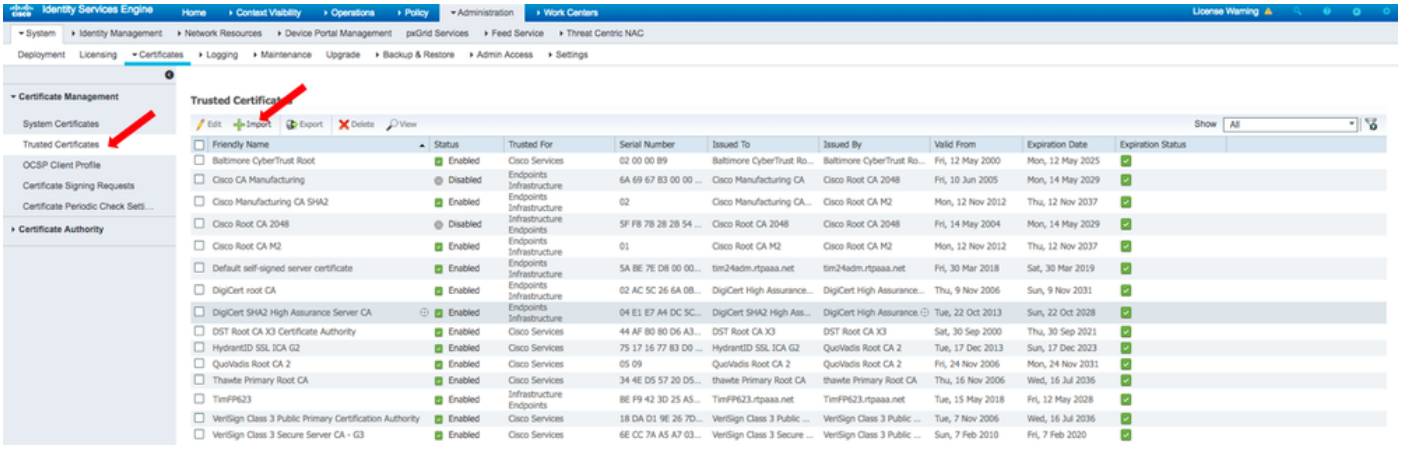
8. Click **OK**.



Step 8. Import the FMC Certificate into ISE

1. Access the **ISE GUI** and navigate to **Administration > System > Certificates > Trusted Certificates**.

2. Click **Import**.



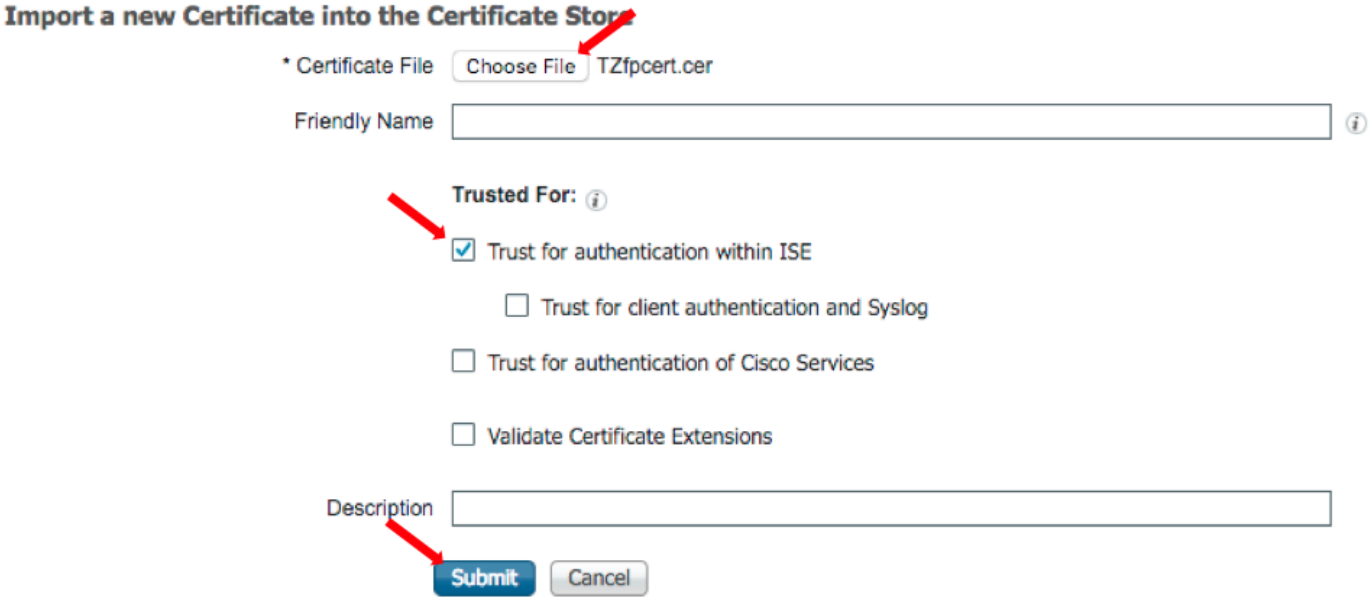
3. Click **Choose File** and select the FMC CER file from your local system.

   Optional: Configure a Friendly Name.

4. Check **Trust** for authentication within ISE.

   Optional: Configure a Description.

5. Click **Submit** as shown in the image.



Step 9. Configure pxGrid Connection on FMC

1. Navigate to **System > Integration > Identity Sources** as shown in the image.



2. Click **ISE**.

3. Configure the IP address or hostname of the ISE pxGrid node.

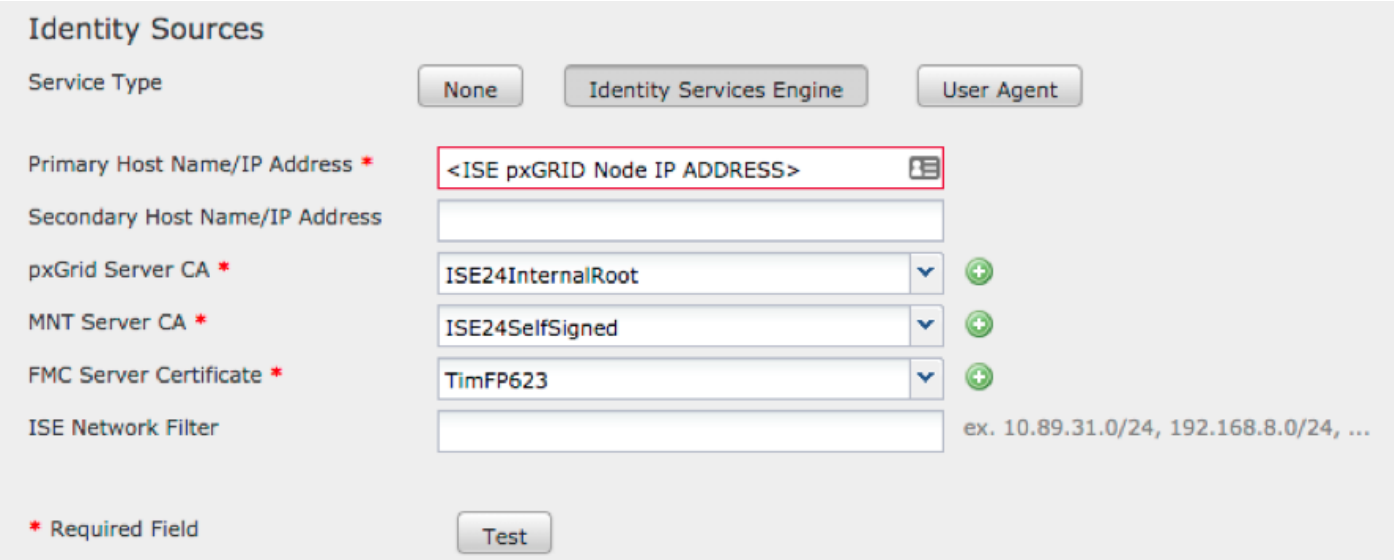
4. Select the + to the right of pxGrid Server CA.

5. Name the Server CA file and then browse to the pxGrid Root Signing CA collected in Step 3. and click **Save**.

6. Select the **+** to the right of MNT Server CA.

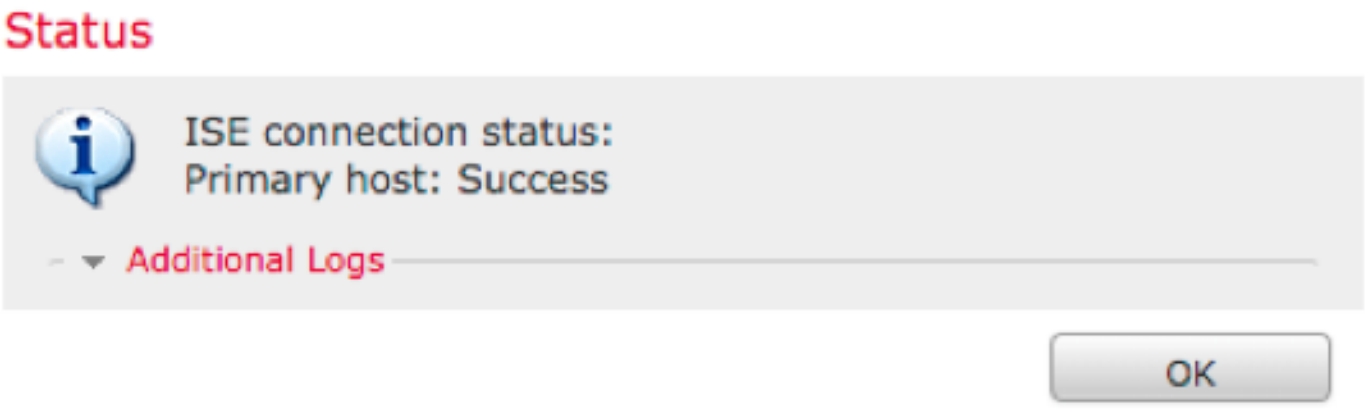
7. Name the Server CA file and then browse to the Admin certificate collected in Step 3. and click **Save**.

8. Select the **FMC CER** file from the dropdown list.



9. Click **Test**.

10. If the test is successful, click on **OK**, then **Save** at the top right of the screen.



> **Note**: When you run two ISE pxGrid nodes, it is normal for one host to show Success and one to show Failure since pxGrid only runs actively on one ISE node at a time. It depends on the configuration whether which Primary host might display Failure and Secondary host might display Success. This is all dependent on which node in ISE is the active pxGrid node.

Verify

Verification in ISE

1. Open the **ISE GUI** and navigate to **Administration > pxGrid Services**.

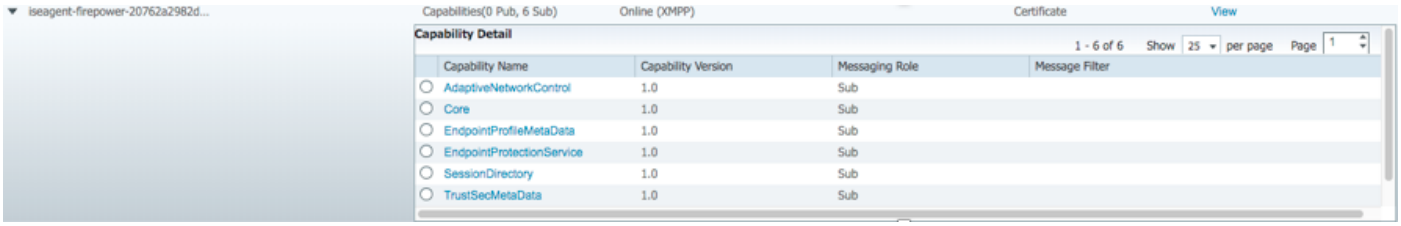
If successful, two firepower connections are listed in the client list. One for the actual FMC (iseagent-hostname-33bytes), and one for the test device (firesightisetest-hostname-33bytes).



The iseagent-firepower connection display six (6) subs and appears online.

The firesightisetest-firepower connection displays zero (0) subs and appears offline.

Expanded view of the iseagent-firepower client displays the six subscriptions..

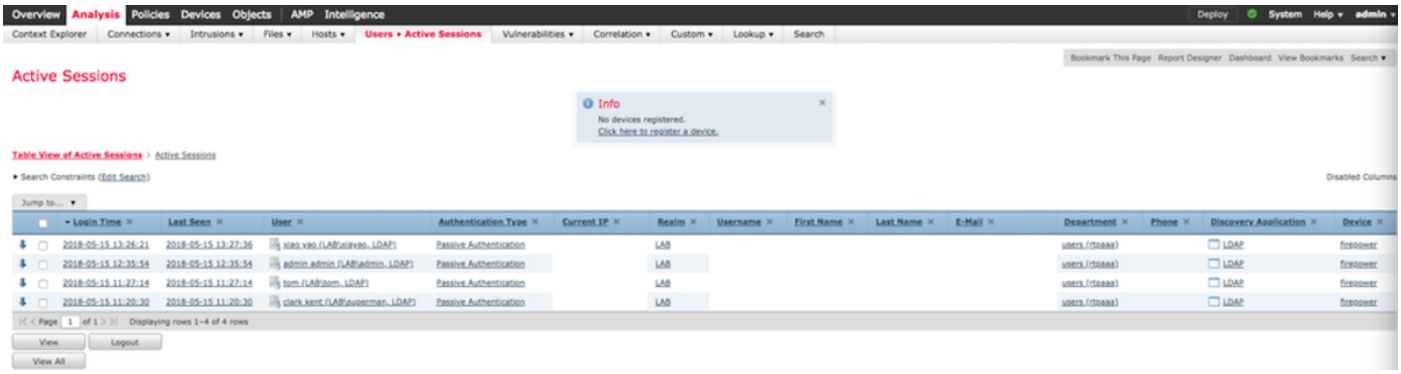


> **Note**: Due to Cisco bug IDCSCvo75376 there is a hostname limitation and Bulk Download fails. The test button on the FMC displays a connectivity failure. This affects 2.3p6, 2.4p6, and 2.6. The current recommendation is to run 2.3 patch 5 or 2.4 patch 5 until an official patch is released.

Verification in FMC

1. Open the FMC GUI and navigate to **Analysis > Users > Active Sessions**.

Any Active Sessions published via the Session Directory capability in ISE are displayed in the Active Sessions table on FMC.



From the FMC CLI sudo mode, the '**adi_cli session**' displays the user session information sent from ISE to FMC.

```
ssh admin@<FMC IP ADDRESS>
Password:
Last login: Tue May 15 19:03:01 UTC 2018 from dhcp-172-18-250-115.cisco.com on ssh
Last login: Wed May 16 16:28:50 2018 from dhcp-172-18-250-115.cisco.com

Copyright 2004-2018, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.2.3 (build 13)
Cisco Firepower Management Center for VMWare v6.2.3 (build 83)

admin@firepower:~$ sudo -i
Password:
Last login: Wed May 16 16:01:01 UTC 2018 on cron
root@firepower:~# adi_cli session

received user session: username tom, ip ::ffff:172.18.250.148, location_ip ::ffff:10.36.150.11,
realm_id 2, domain rtpaaa.net, type Add, identity Passive.
received user session: username xiayao, ip ::ffff:10.36.148.98, location_ip ::, realm_id 2,
domain rtpaaa.net, type Add, identity Passive.
received user session: username admin, ip ::ffff:10.36.150.24, location_ip ::, realm_id 2,
domain rtpaaa.net, type Add, identity Passive.
received user session: username administrator, ip ::ffff:172.18.124.200, location_ip ::,
realm_id 2, domain rtpaaa.net, type Add, identity Passive.
```

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.