配置ISE 2.4和FMC 6.2.3 pxGrid集成

目录

简介

本文档介绍集成ISE pxGrid版本2.4和FMC版本6.2.3的配置流程。

先决条件

要求

Cisco 建议您了解以下主题：

- ISE 2.4
- FMC 6.2.3
- Active Directory/轻量目录访问协议(LDAP)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 独立ISE 2.4

- FMCv 6.2.3
- Active Directory 2012R2
- 身份服务引擎(ISE)pxGrid版本2.4
- Firepower管理中心(FMC)版本6.2.3

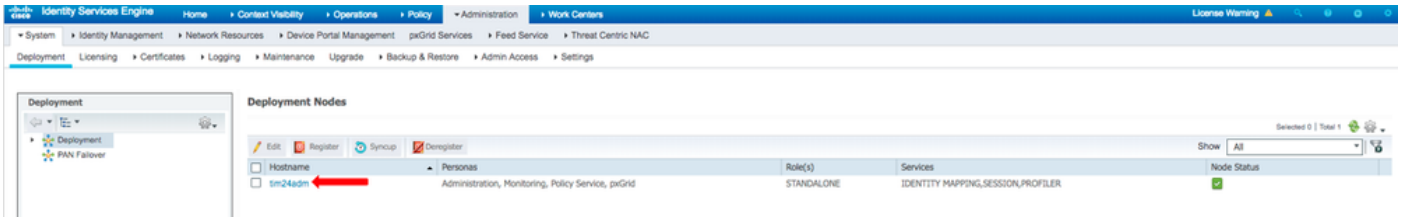
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置ISE

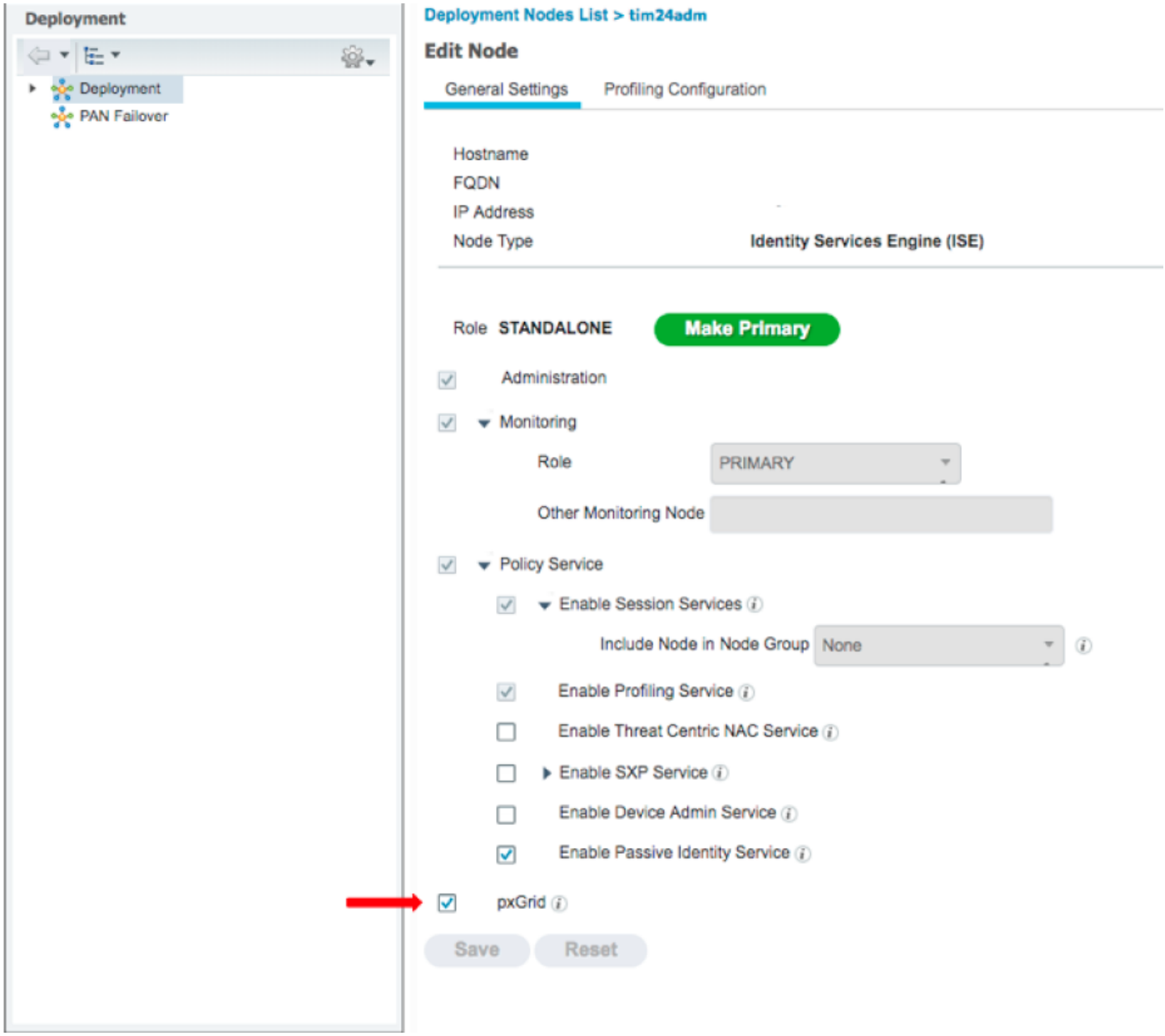
步骤1:启用pxGrid服务

1. 登录ISE管理员GUI，导航到**管理>部署**。

2.选择要用于pxGrid角色的ISE节点。



3.启用pxGrid服务，然后单击**保存**，如图所示。



4.验证pxGrid服务是否从CLI运行。

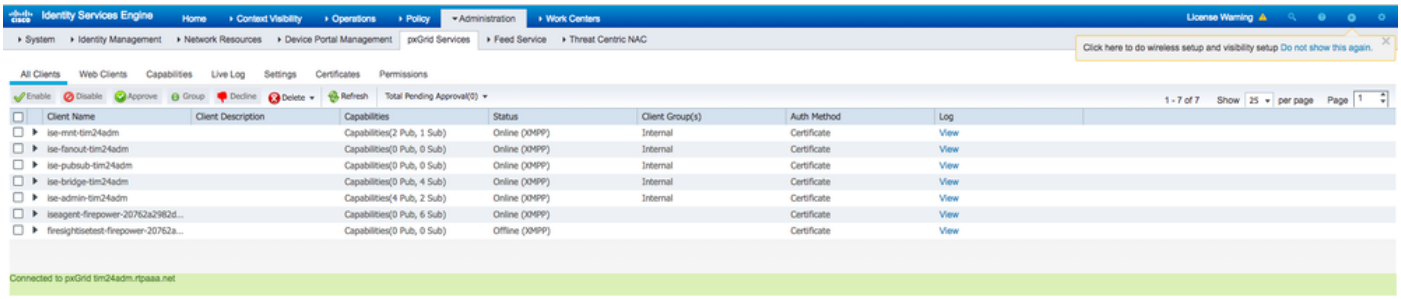
注意：如果使用了多个pxGrid节点，则此过程最多需要5分钟，pxGrid服务才能完全启动并确定高可用性(HA)状态。

5.通过SSH连接到ISE pxGrid节点CLI并检查应用状态。

```
# 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.访问ISE管理员GUI并验证服务是否在线且正常运行。导航到**管理> pxGrid服务**。

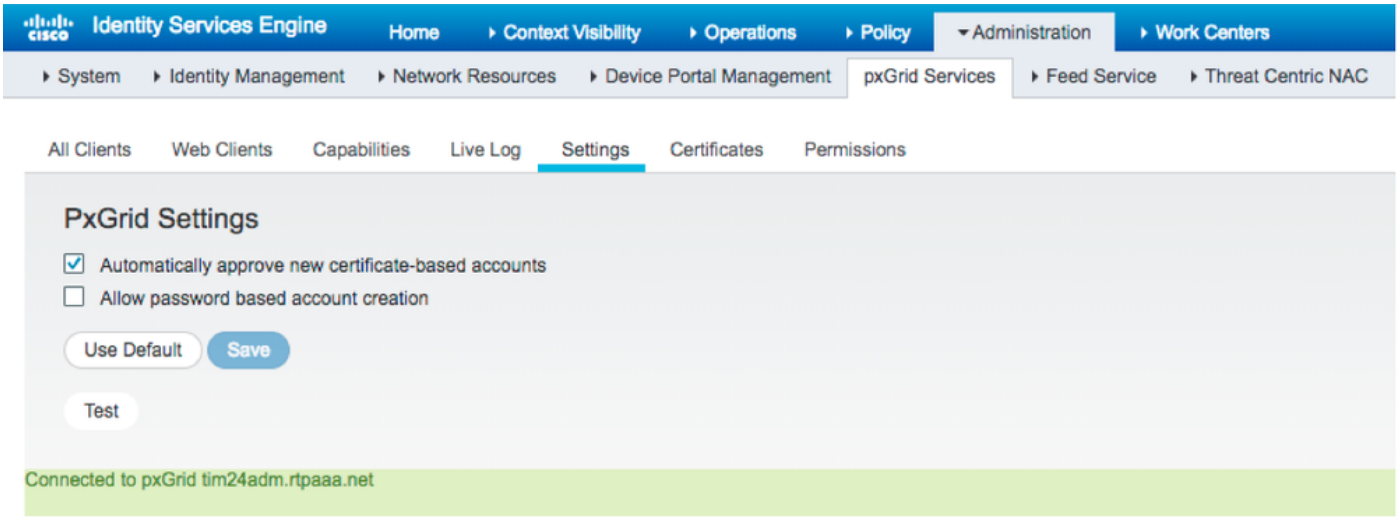
7.在页面底部，ISE显示**Connected to pxGrid <pxGrid node FQDN>**。



第二步：配置ISE以批准所有pxGrid基于证书的帐户

1.导航到**管理> pxGrid服务>设置。**

2.选中复选框：“自动批准基于证书的新帐户”，然后单击**保存**。



注意：如果未启用此选项，管理员必须手动批准与ISE的FMC连接。

第三步：导出ISE MNT管理员证书和pxGrid CA证书

1.导航到**管理>证书>系统证书。**

2.如果未在主要管理节点上启用，请展开主要监控(MNT)节点。

3.使用使用者“管理员”字段选择证书。

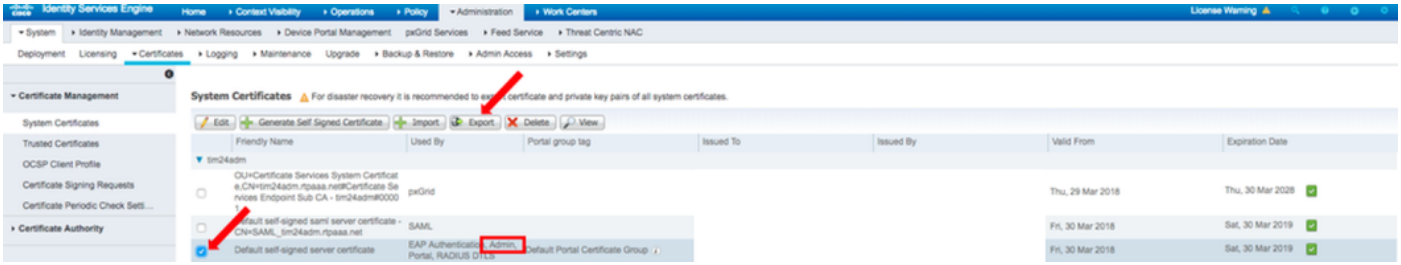
注意：本指南使用默认ISE自签名证书作为管理员使用。如果使用证书颁发机构(CA)签名的管理员证书，请导出在ISE MNT节点上签名的管理员证书的根CA。

4.单击**导出。**

5.选择“导出证书和私钥”选项。

6.设置加密密钥。

7. **导出**和**保存**文件（如图所示）。

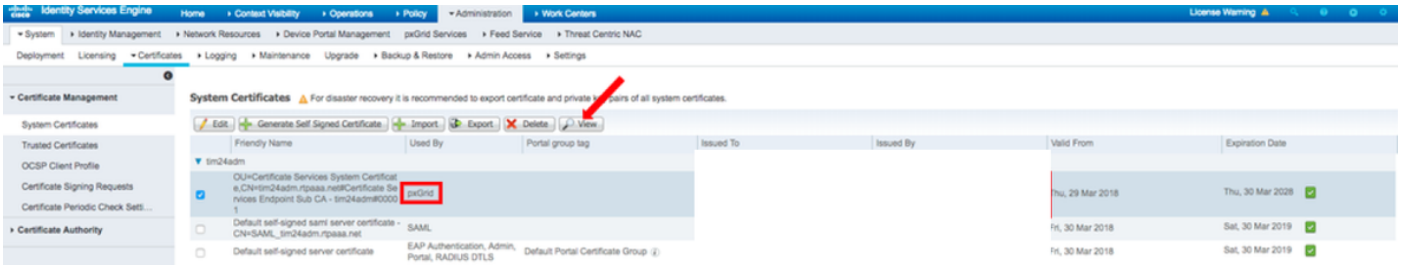


9.返回ISE系统证书屏幕。

10.确定证书上的“颁发者”字段，并在“使用者”列中使用“pxGrid”。

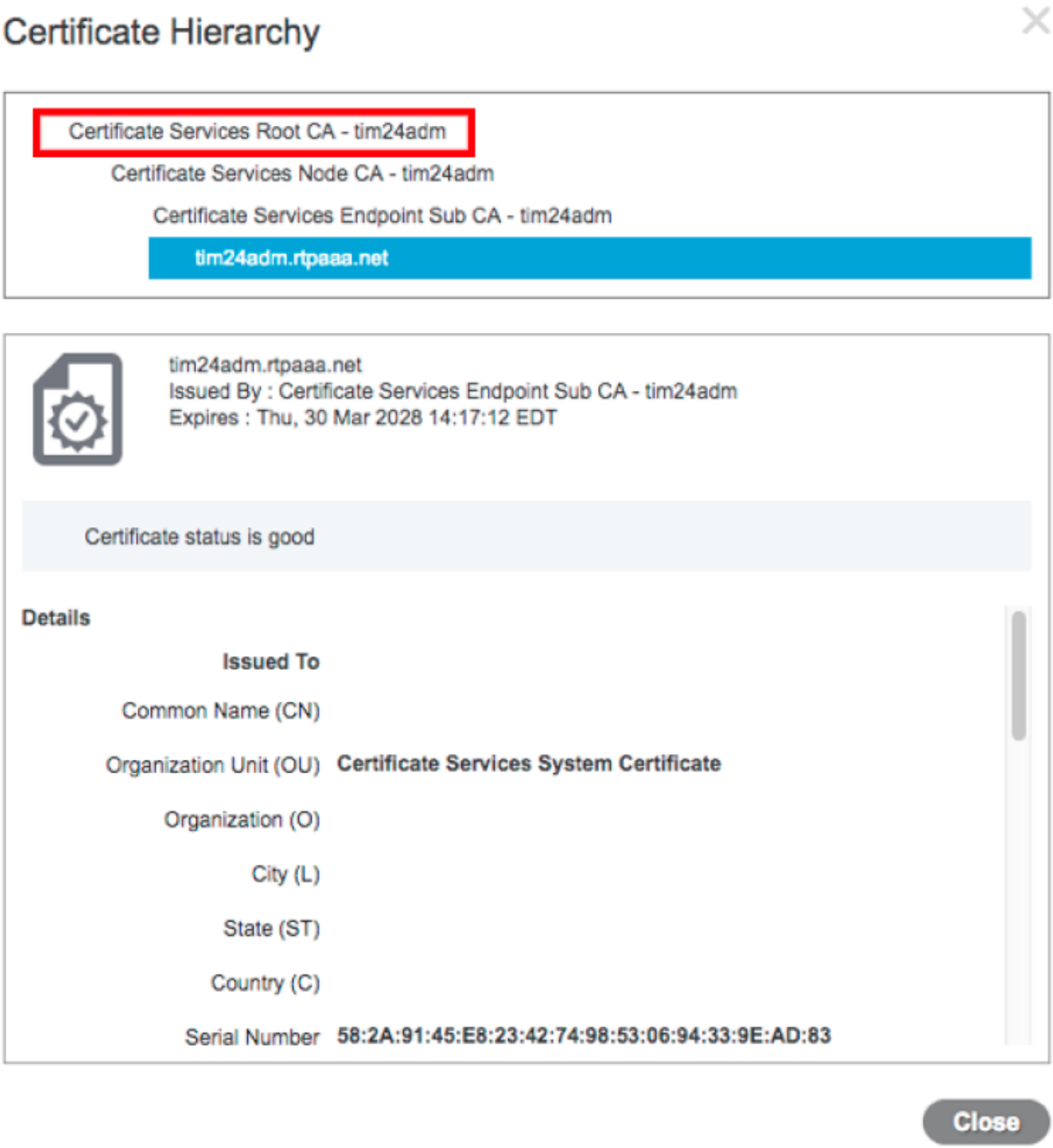
> **注**：在较早版本的ISE中，这是一个自签名证书，但自2.2起，此证书默认由内部ISE CA链颁发。

11.选择“证书”，然后单击**查看**，如图所示。



12.确定顶级（根）证书。在本例中，它是**“Certificate Services Root CA - tim24adm”。**

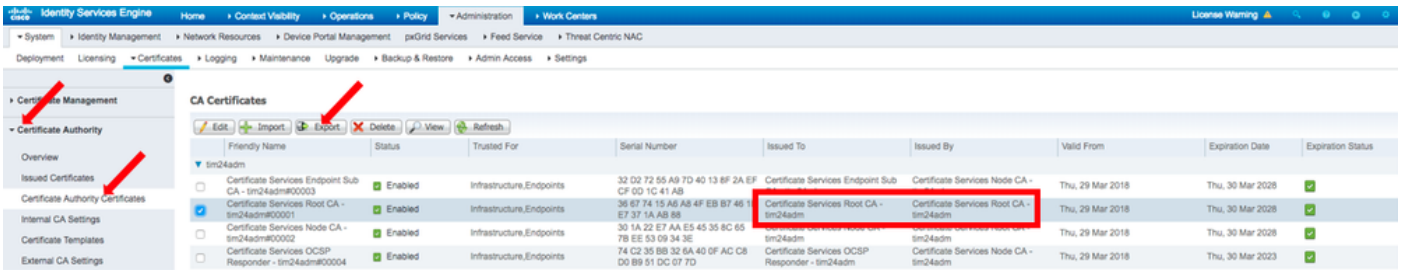
13.如图所示关闭证书视图窗口。



14.展开ISE证书颁发机构菜单。

15.选择**证书颁发机构证书**。

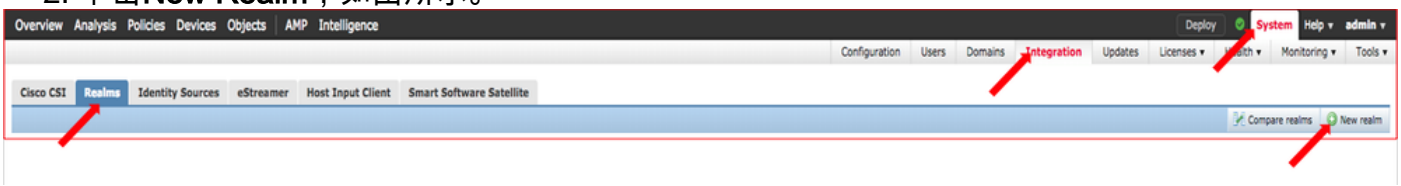
16.选择已标识的根证书，然后单击**导出。** 然后保存pxGrid根CA证书，如图所示。



配置FMC

第四步：向FMC添加新领域

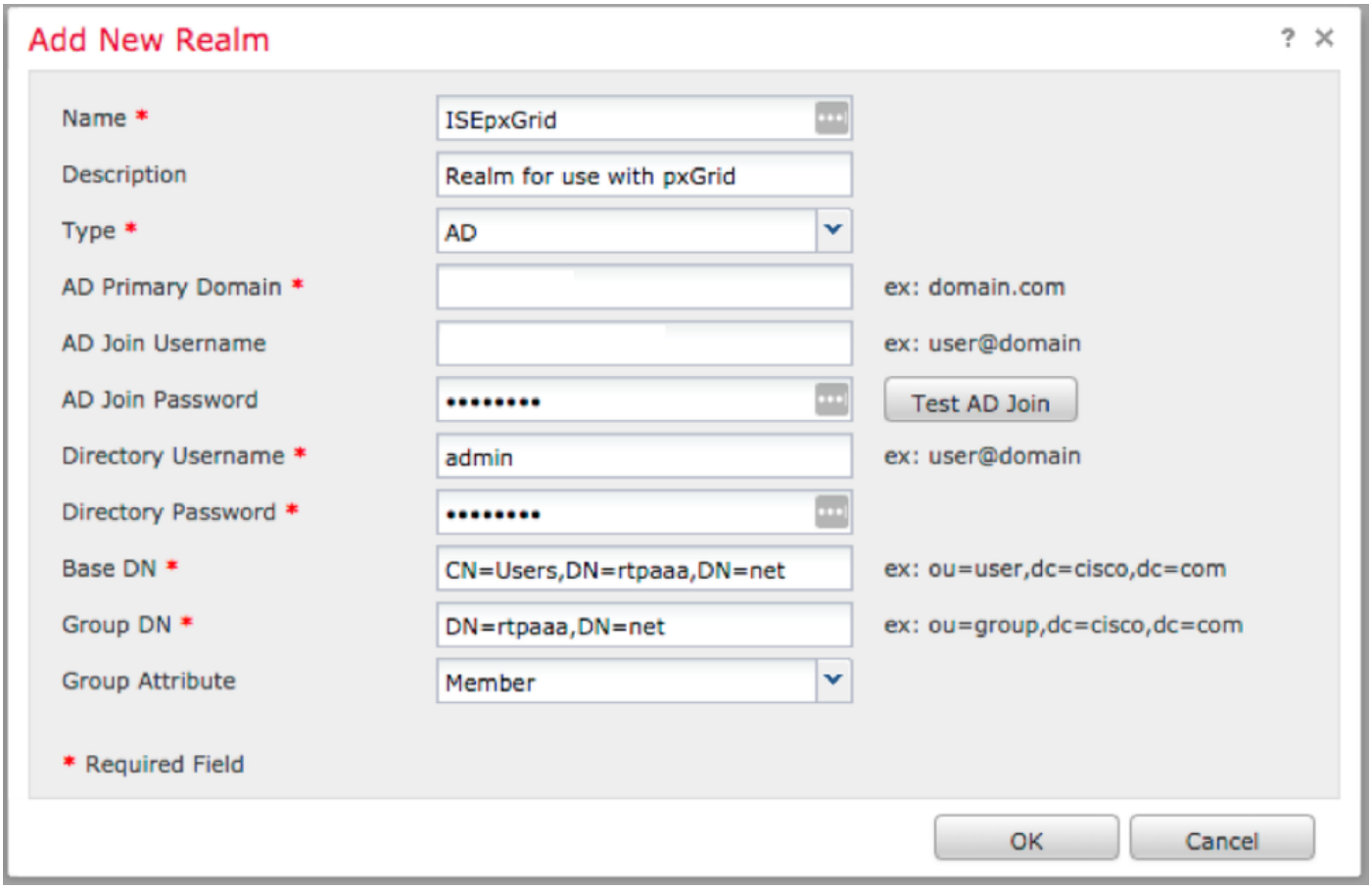
1. 访问FMC GUI并导航到**System > Integration > Realms**。
2. 单击**New Realm**，如图所示。



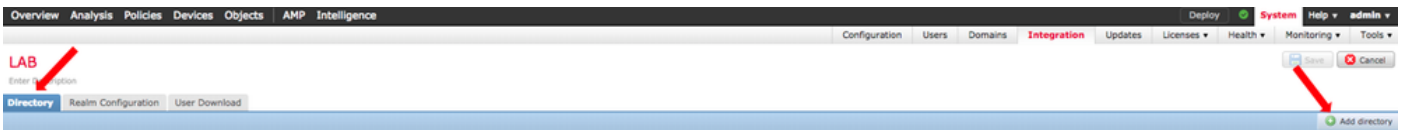
3.填写表格并点击“测试Active Directory(AD)加入”按钮。

注意:AD加入用户名必须采用用户主体名称(UPN)格式，否则测试失败。

4.如果“测试AD加入”成功，请单击**确定**。



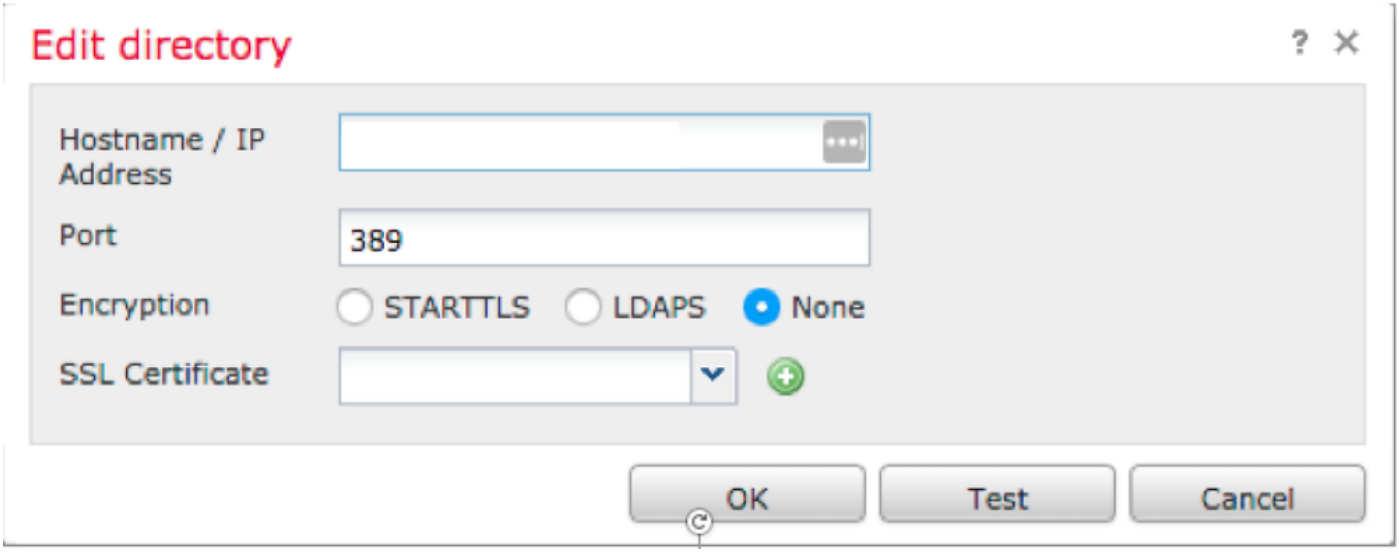
5.单击**Directory**选项卡，然后单击**Add directory**，如图所示。

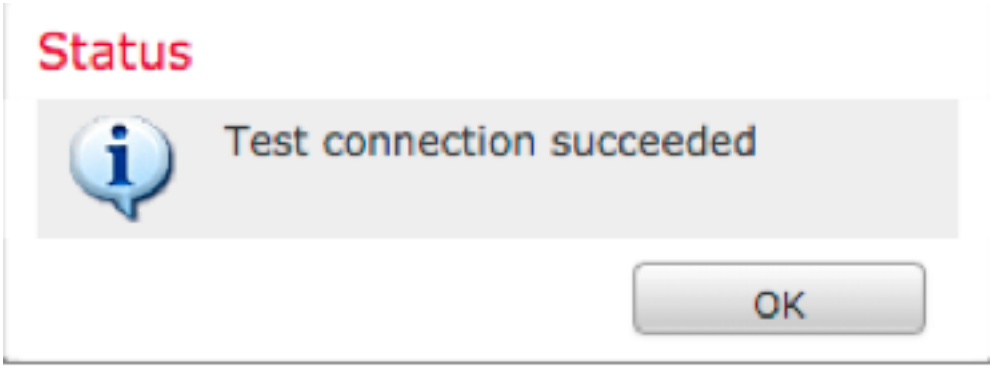


6.配置IP/主机名并测试连接。

注意：如果测试失败，请在“领域配置”选项卡上验证凭证。

7.单击**确定**。





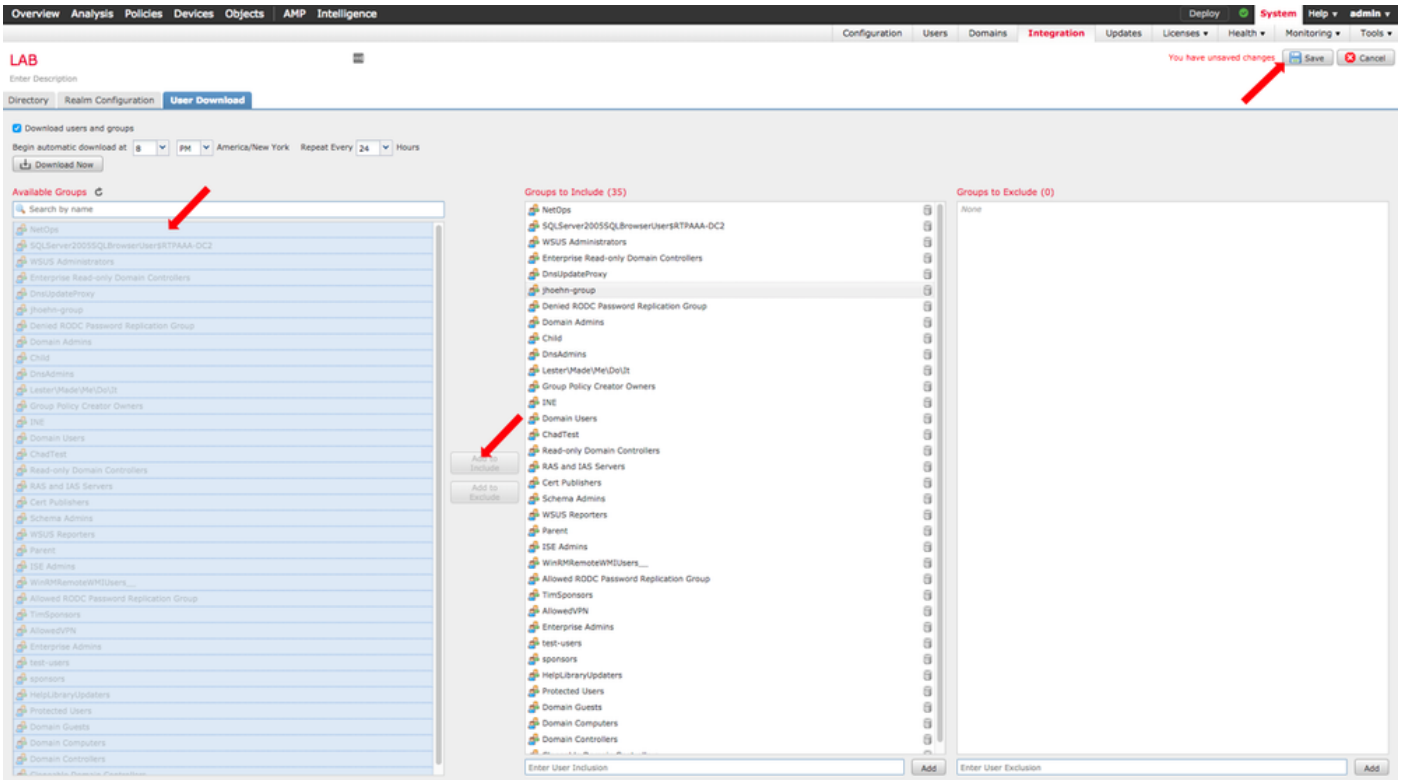
8.单击**User Download**选项卡。

9.如果尚未选择，请启用用户和组下载

10.单击“立即下载”

11.填写列表后，添加所需的组并选择**Add to Include**。

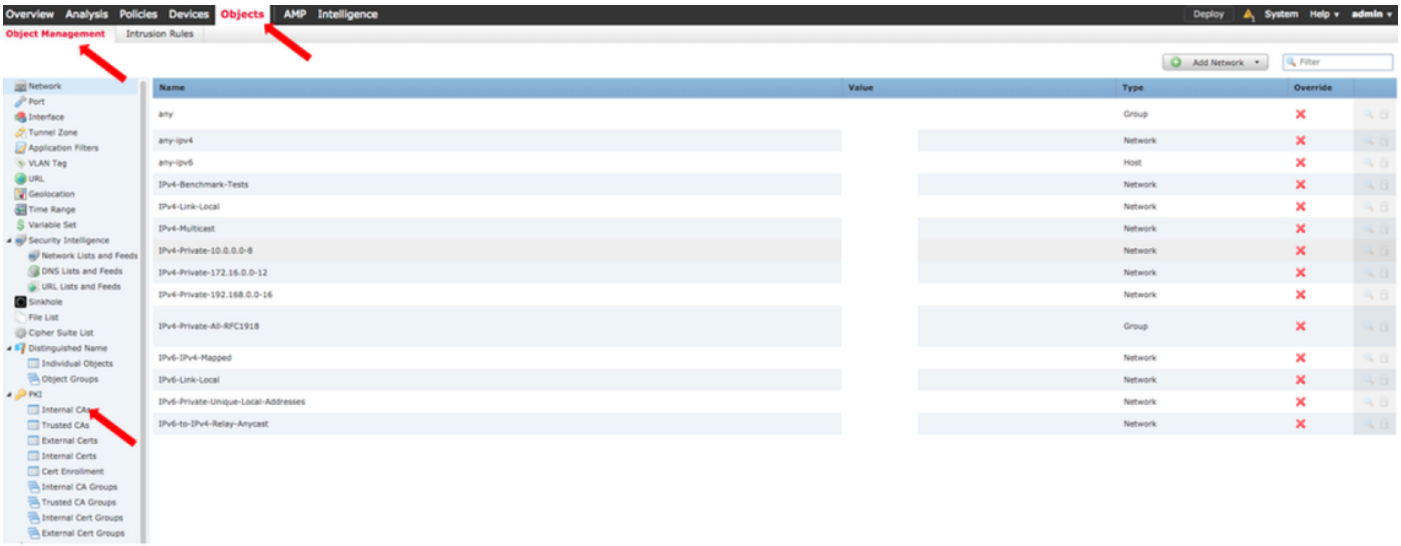
12.保存领**域配置**。



13.启用领域状态。

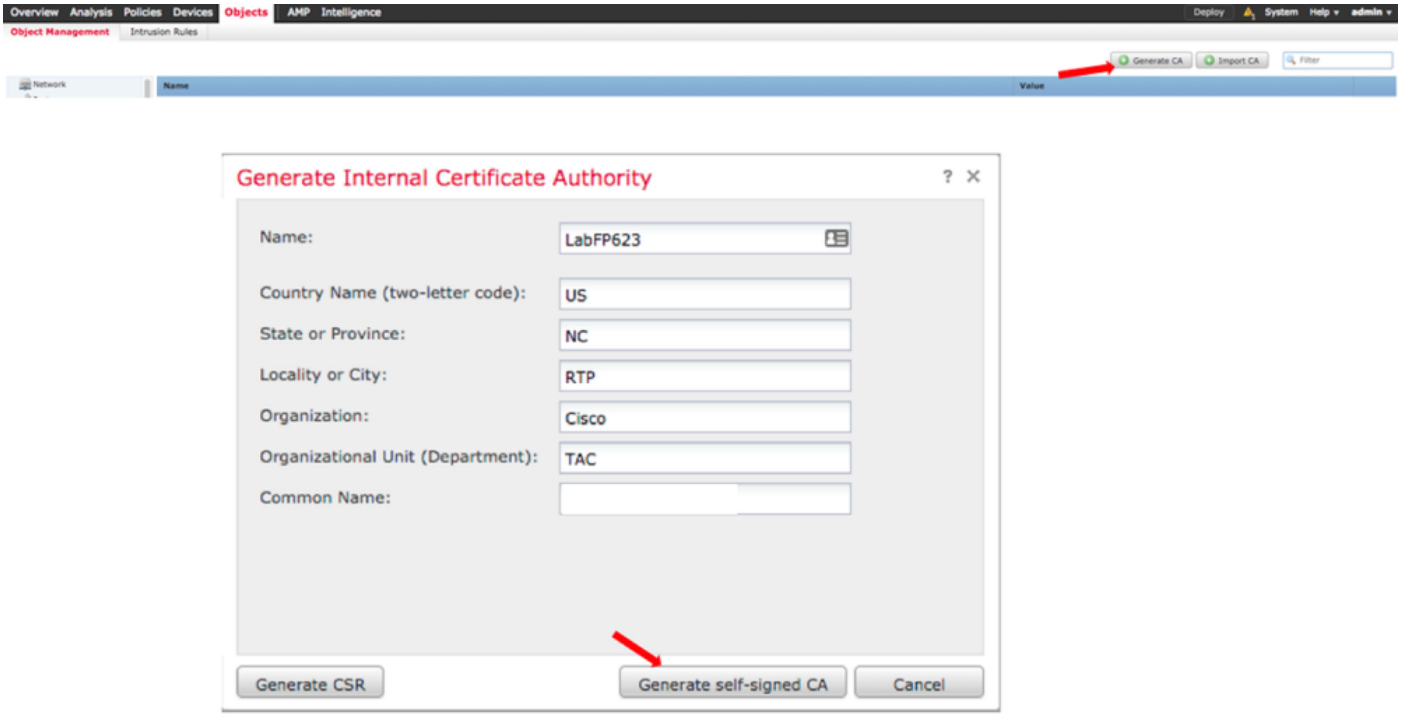
第五步：生成FMC CA证书

1.定位至**对象>对象管理>内部CA**，如图所示。



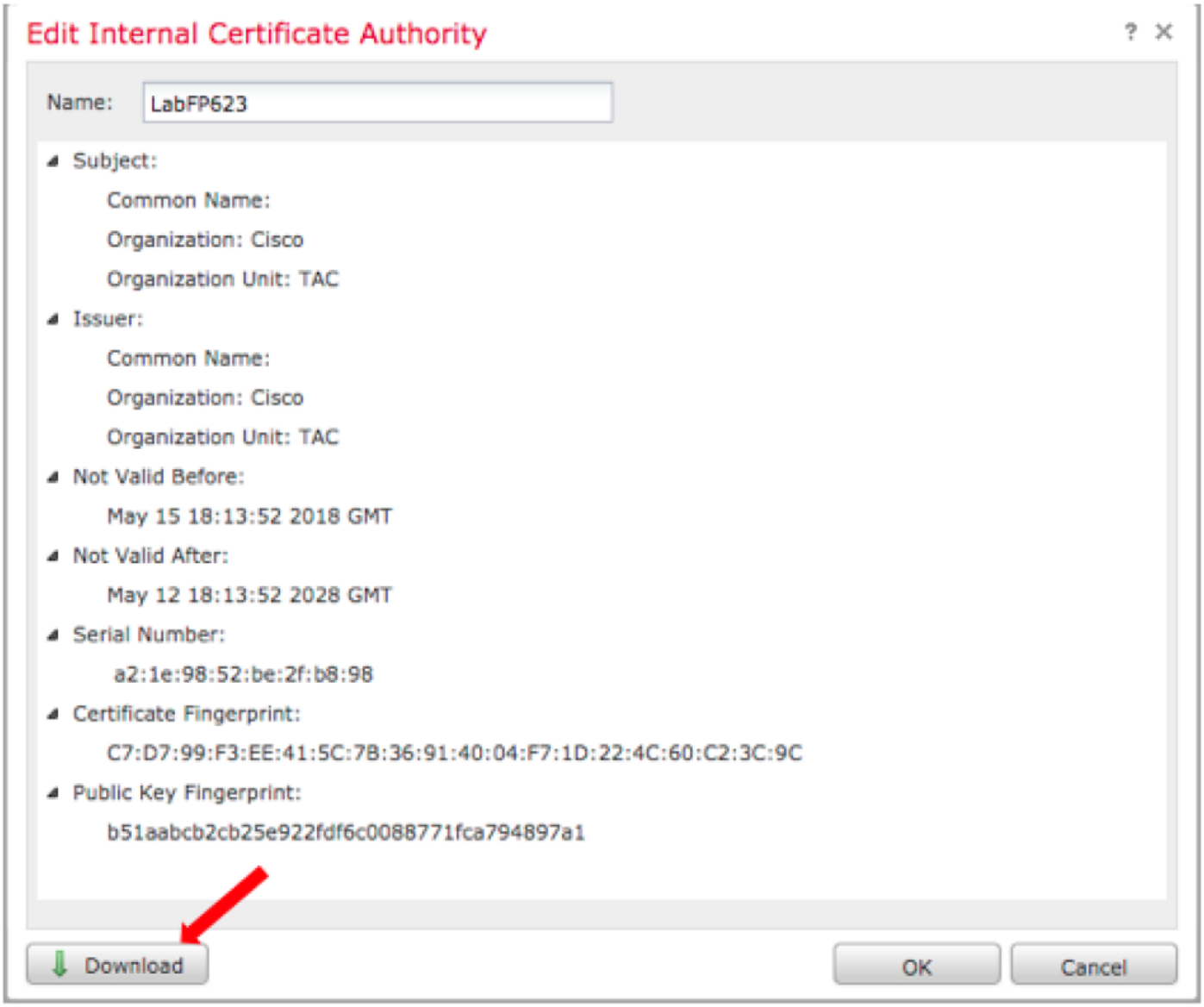
2.单击**生成CA**。

3.填写表格并点击**生成自签名CA**。



4.生成完成后，单击生成的CA证书右侧的铅笔，如图所示。

5.单击**下载**。



6.配置并确认加密密码，然后单击**OK**。

7.将Public-Key Cryptography Standards(PKCS)p12文件保存到本地文件系统。

第六步：使用OpenSSL从生成的证书中提取证书和私钥

此操作在FMC的根上或在任何支持OpenSSL命令的客户端上完成。此示例使用标准Linux外壳。

1.使用**openssl**从p12文件中提取证书(CER)和私钥(PVK)。

2.提取CER文件，然后从FMC上的证书生成配置证书导出密钥。

```
~$ 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.提取PVK文件，配置证书导出密钥，然后设置新的PEM密码短语并确认。

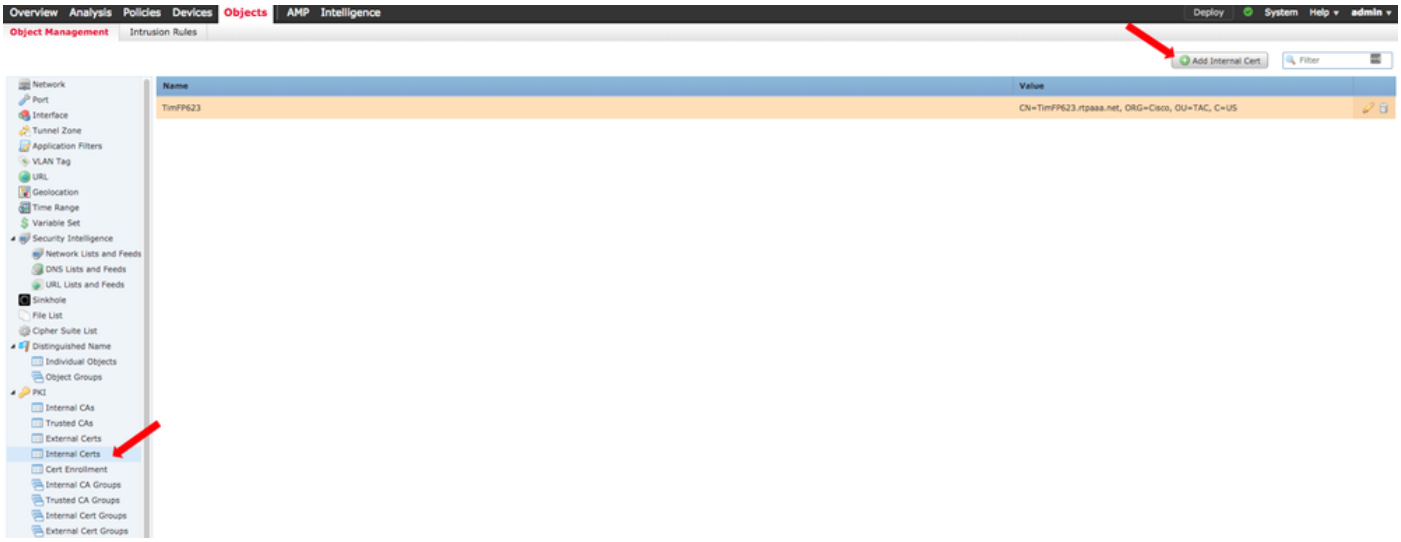
```
~$ openssl pkcs12 -nocerts -in <filename.p12> -out <filename.pvk>
```

```
Password:   Last login: Tue May 15 18:46:41 UTC 2018   Enter Import Password:   MAC verified OK
```
4.下一步需要此PEM短语。

步骤 7.将证书安装到FMC

1.导航到**对象>对象管理> PKI >内部证书**。

2.单击Add Internal Cert，如图所示。



3.配置内部证书的名称。

4.浏览到CER文件的位置并将其选中。填写“证书数据”后，选择第二个。

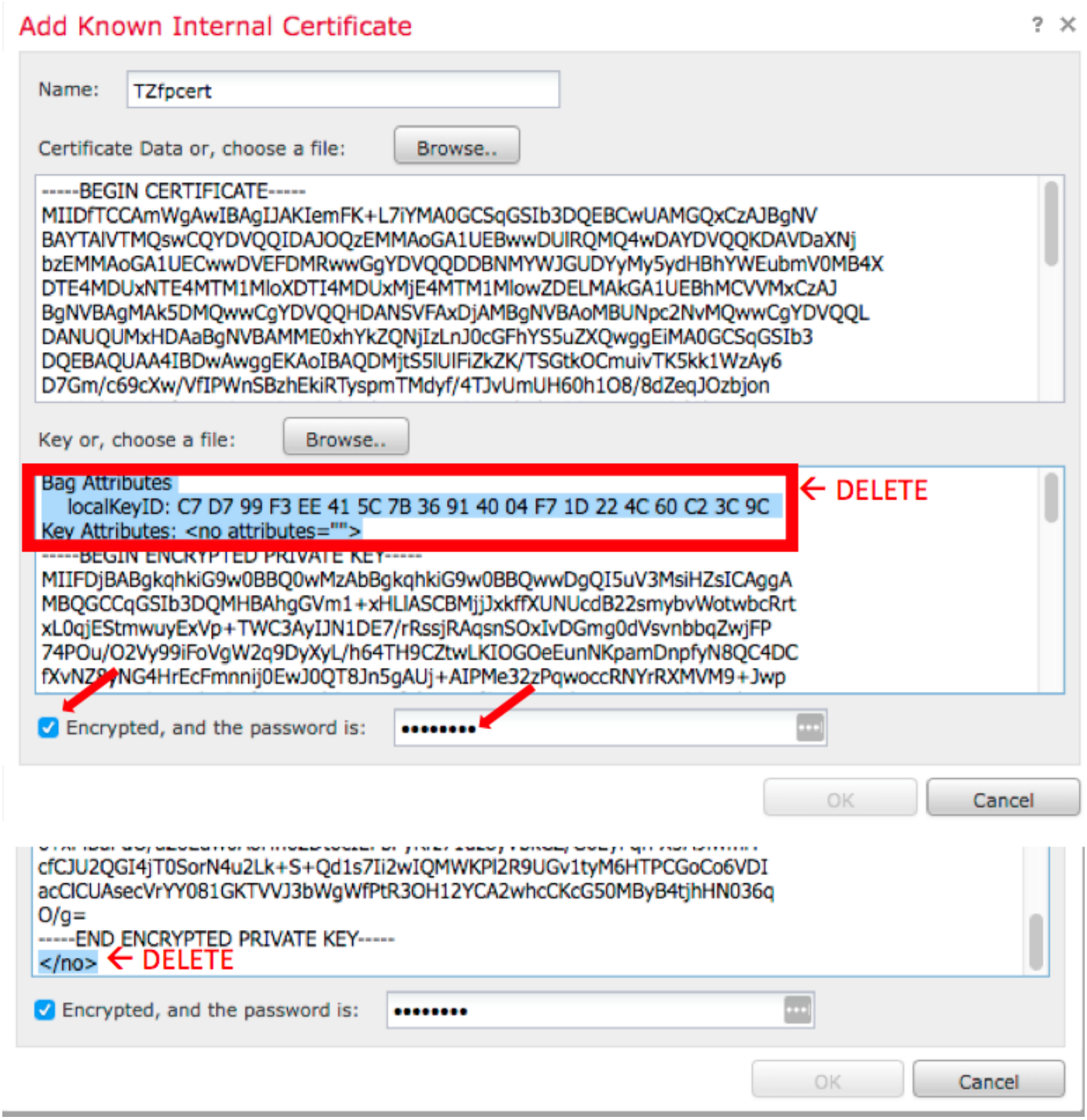
5.浏览**选项**并选择PVK文件。

6.删除PVK部分中的任何前导“Bag attributes”和所有尾随值。PVK以**-----BEGIN ENCRYPTED PRIVATE KEY**开头，以**-----END ENCRYPTED PRIVATE KEY**结尾。

注：如果PVK文本的前导和尾随连字符之外有任何字符，则无法单击**OK**。

7.选中Encrypted框并配置在步骤6中导出PVK时创建的密码。

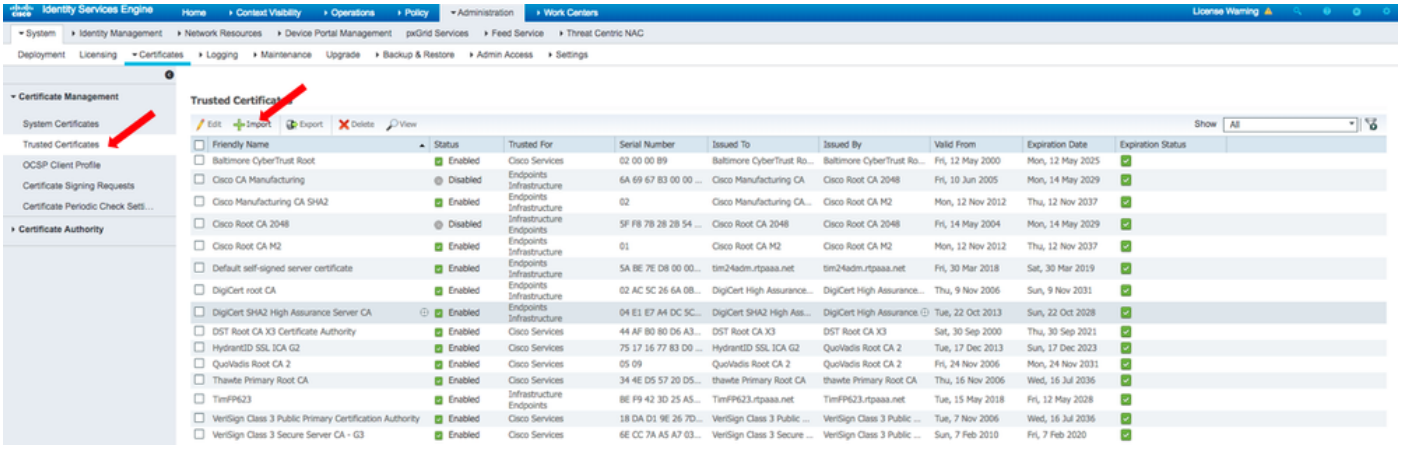
8.单击**确定**。



步骤 8将FMC证书导入ISE

1.访问ISE GUI并导航到**管理>系统>证书>受信任证书。**

2.单击**导入。**



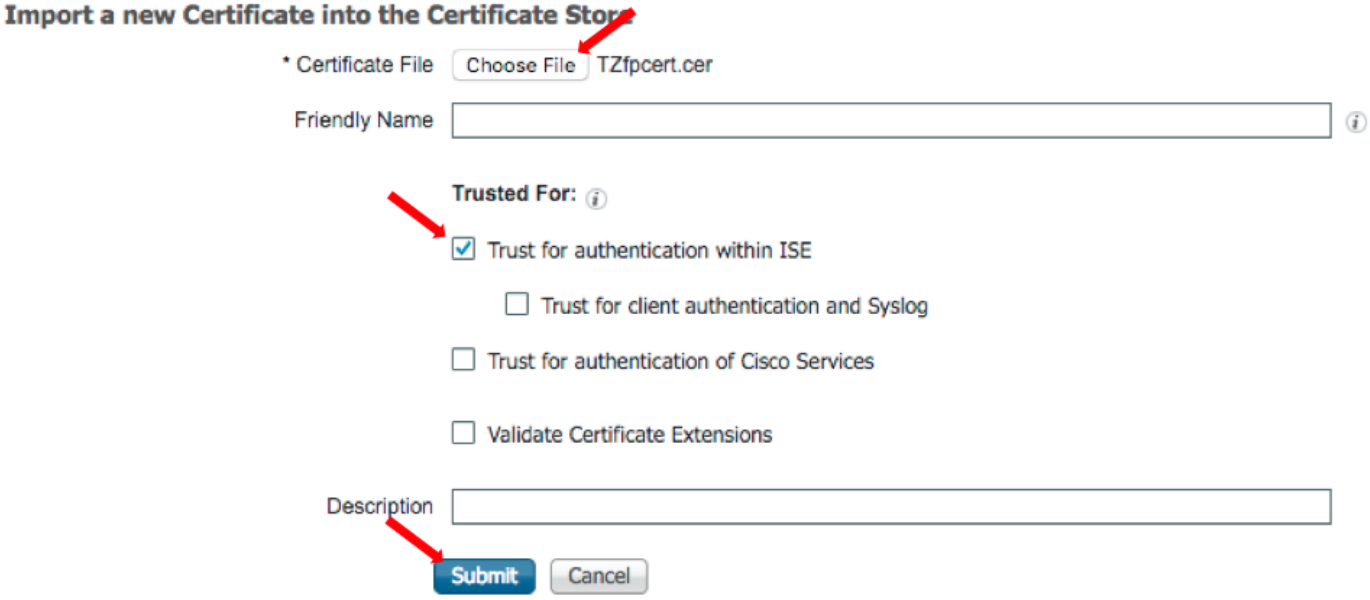
3.单击**Choose File**，然后从本地系统中选择FMC CER文件。

可选：配置友好名称。

4.检查ISE中的**Trust**身份验证。

可选：配置说明。

5.单击**提交**，如图所示。



步骤 9在FMC上配置pxGrid连接

1.定位至**系统>集成>身份源**，如图所示。

2.单击**ISE**。

3.配置ISE pxGrid节点的IP地址或主机名。

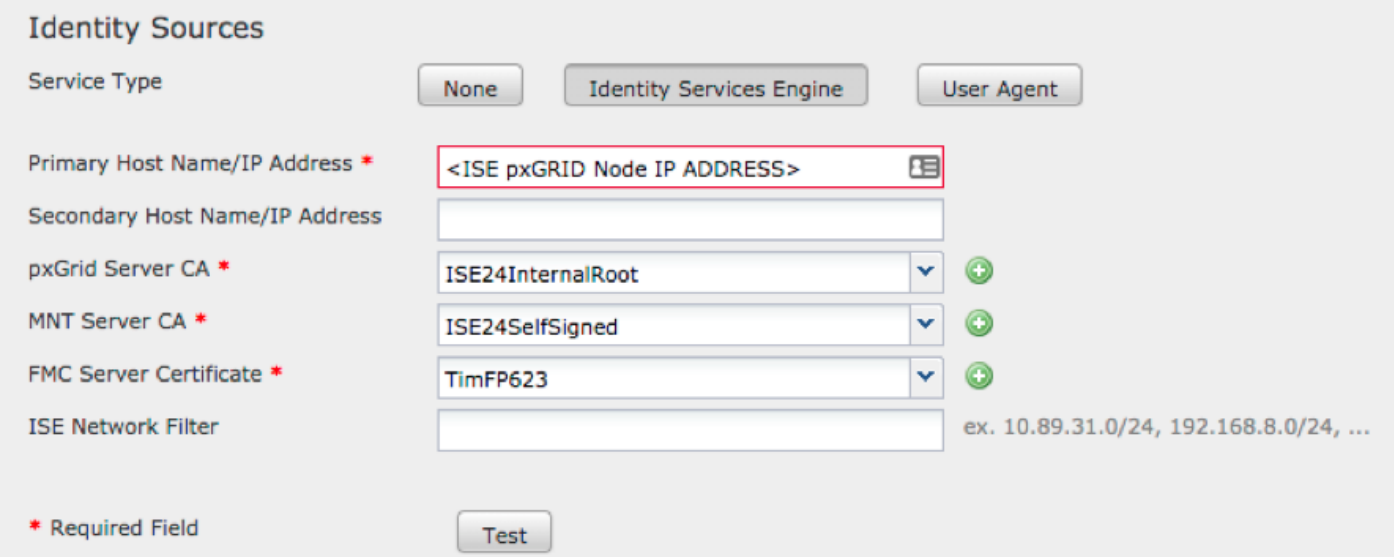
4.选择pxGrid服务器CA右侧的+。

5.命名服务器CA文件，然后浏览到步骤3中收集的pxGrid根签名CA，然后单击**Save**。

6.选择MNT Server CA右侧的**+**。

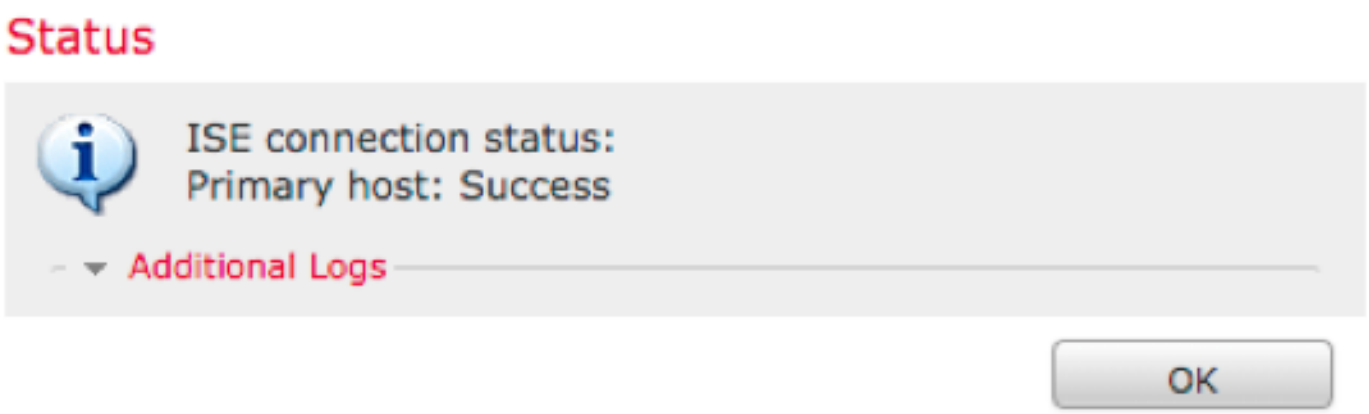
7.命名服务器CA文件，然后浏览到步骤3中收集的管理证书，然后单击**Save**。

8.从下拉**列表中**选择**FMC** CER文件。



9.单击**测试**。

10.如果测试成功，请点击**确定**，然后点击屏幕右上方的**保存**。



注意：运行两个ISE pxGrid节点时，一个主机显示成功(Success)和一个主机显示失败(Failure)是正常的，因为pxGrid一次只在一个ISE节点上主动运行。具体取决于配置，哪个主主机可能会显示Failure，哪个辅助主机可能会显示Success。这完全取决于ISE中的哪个节点是活动的pxGrid节点。

验证

在ISE中验证

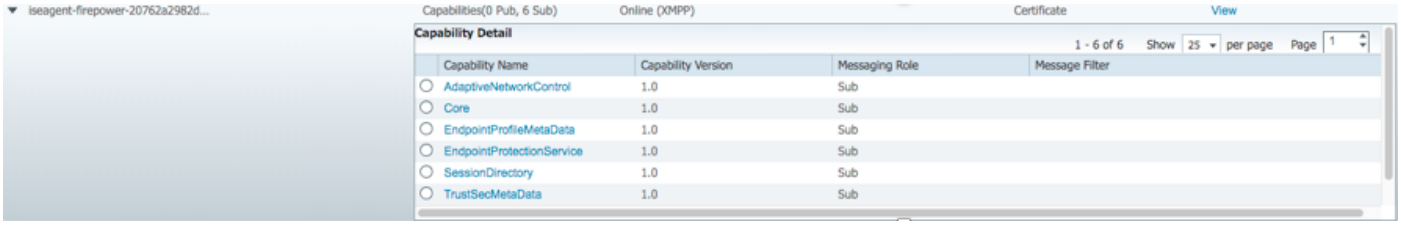
1.打开**ISE GUI**并导航到**管理> pxGrid服务**。

如果成功，客户端列表中将列出两个firepower连接。一个用于实际FMC(iseagent-hostname-33bytes)，一个用于测试设备(firesightistest-hostname-33bytes)。

iseagent-firepower连接显示六(6)个子并在线显示。

firesightiestest-firepower连接显示零(0)个订用程序，并且显示为脱机。

iseagent-firepower客户端的展开视图显示六个订用。

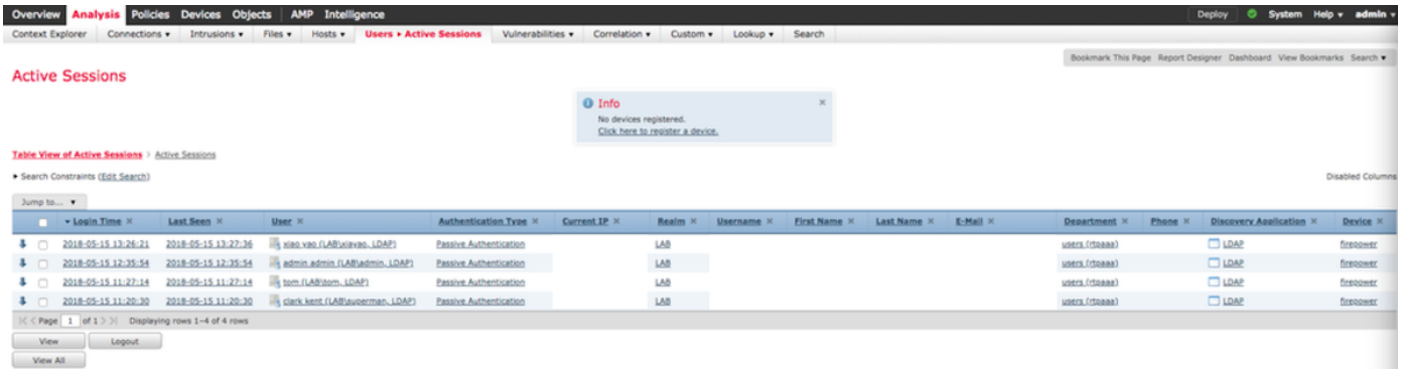


> **注**：由于Cisco bug IDCSCvo75376 存在主机名限制，批量下载失败。FMC上的测试按钮显示连接故障。这会影响2.3p6、2.4p6和2.6。当前建议运行2.3补丁5或2.4补丁5，直到发布正式补丁。

在FMC中验证

1.打开FMC GUI并导航到**分析>用户>活动会话**。

通过ISE中的会话目录功能发布的任何Active Sessions都显示在FMC的Active Sessions表中。



在FMC CLI sudo模式下，“**adi_cli session**”显示从ISE发送到FMC的用户会话信息。

```
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.
```

故障排除

目前没有针对此配置的故障排除信息。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。