# Configurar o ISE 2.4 e a integração do FMC 6.2.3 pxGrid

## Contents



## Introduction

Este documento descreve o processo de configuração para integração do ISE pxGrid versão 2.4 e do FMC versão 6.2.3.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- ISE 2.4
- CVP 6.2.3
- Ative Diretory/Lightweight Diretory Access Protocol (LDAP)

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

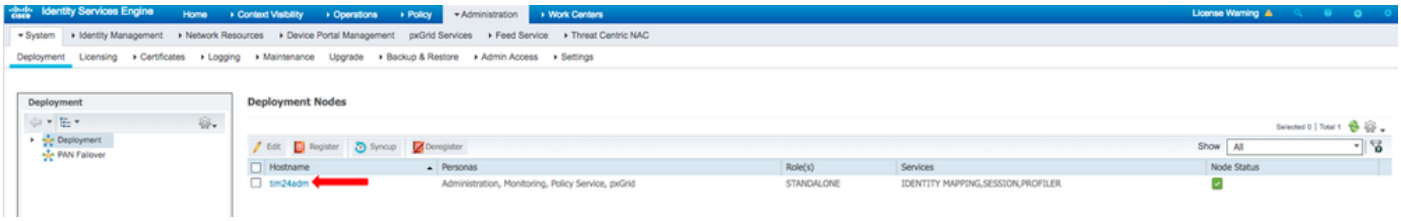
- ISE 2.4 independente
- FMCv 6.2.3
- Ative Diretory 2012R2
- Identity Services Engine (ISE) pxGrid versão 2.4
- Firepower Management Center (FMC) versão 6.2.3

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

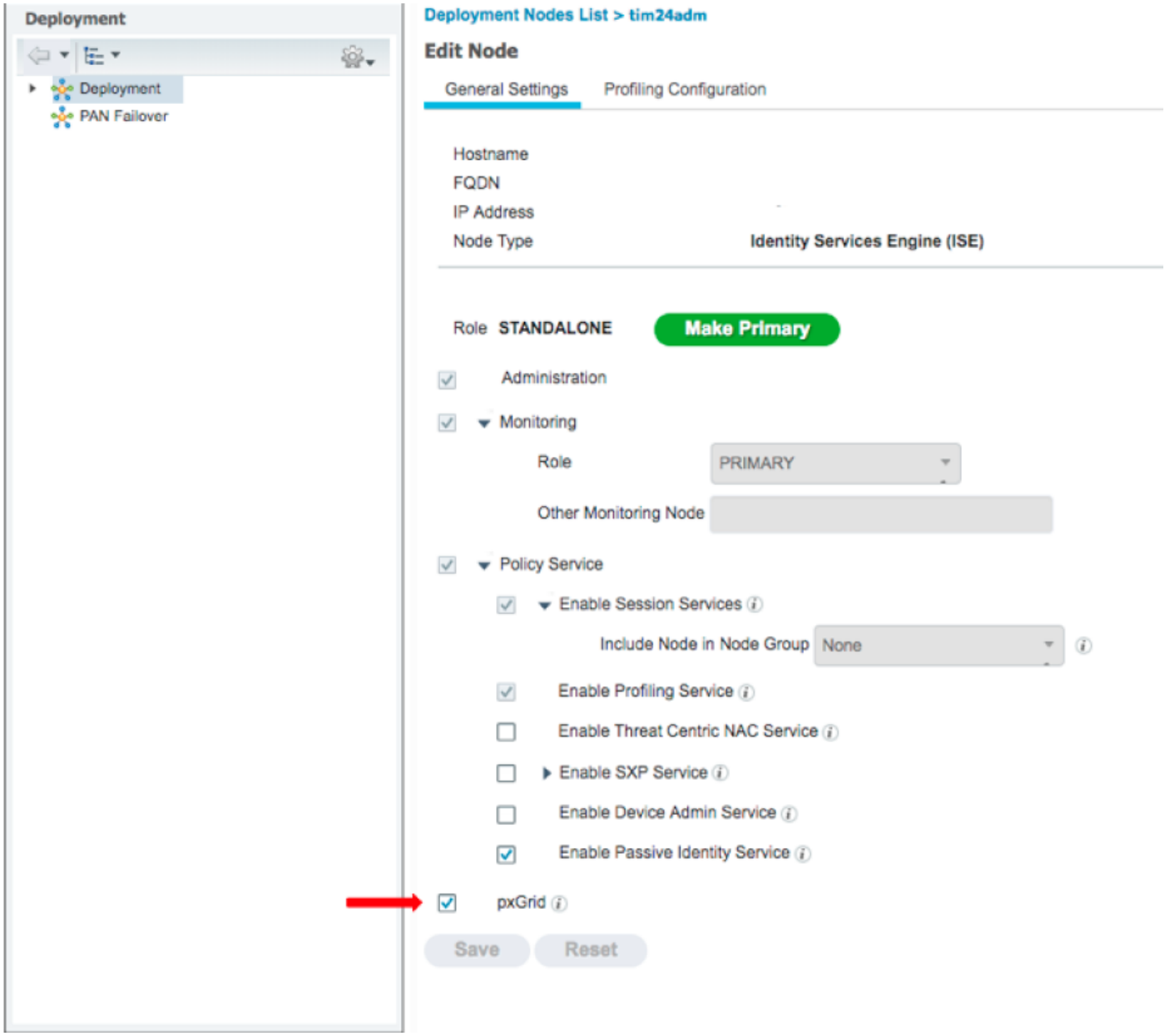
# Configurar o ISE

## Etapa 1. Habilitar serviços pxGrid

1. Faça login na GUI do ISE Admin e navegue até **Administração > Implantação.**
2. Selecione o nó ISE a ser usado para pxGrid persona.




3. Ative o serviço pxGrid e clique em **Salvar** como mostrado na imagem.




4. Verifique se os serviços do pxGrid são executados a partir da CLI.

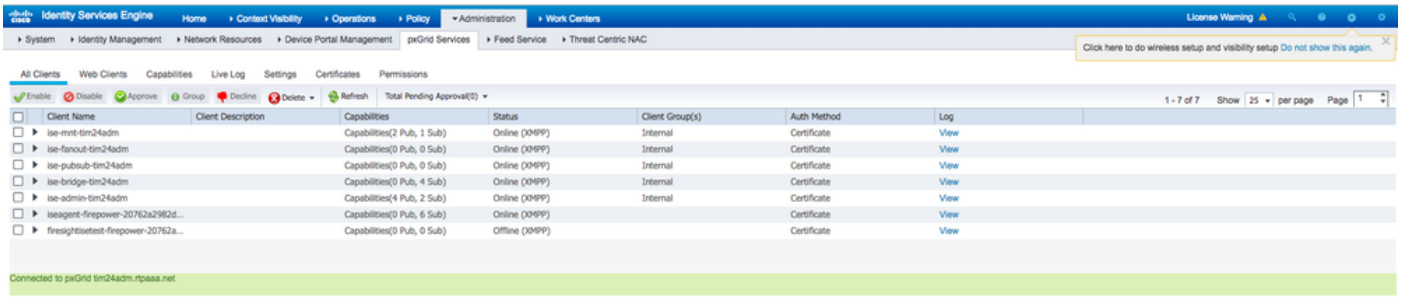
**Observação**: o processo requer até 5 minutos para que os serviços pxGrid sejam totalmente iniciados e determinem o estado de Alta Disponibilidade (HA) se mais de um nó pxGrid estiver em uso.

5. Use SSH para acessar a CLI do nó do pxGrid do ISE e verifique o status do aplicativo.

```
# 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. Acesse a GUI do administrador do ISE e verifique se os serviços estão on-line e funcionam. Navegue até **Administração > pxGrid Services**.

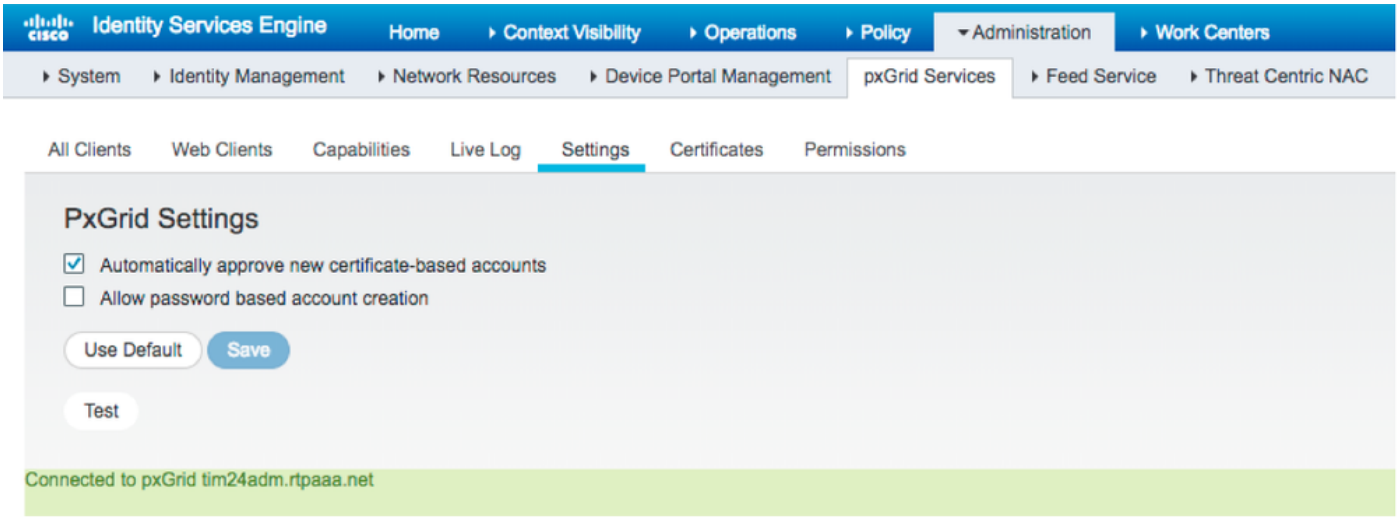
7. Na parte inferior da página, o ISE exibe **Connected to pxGrid <pxGrid node FQDN>**.



## Etapa 2. Configurar o ISE para aprovar todas as contas baseadas em certificado do pxGrid

1. Navegue até **Administration > pxGrid Services > Settings.**

2. Marque a caixa: "Aprovar automaticamente novas contas baseadas em certificado" e clique em **Salvar**.




> **Observação**: o administrador deve aprovar manualmente a conexão do FMC ao ISE se essa opção não estiver habilitada.

## Etapa 3. Exportar Certificado Admin MNT do ISE e Certificados CA pxGrid

1. Navegue até **Administração > Certificados > Certificados do Sistema**.

2. Expanda o nó Monitoramento Principal (MNT) se não estiver ativado no nó Administração Principal.

3. Selecione o certificado com o campo Used-By "Admin".

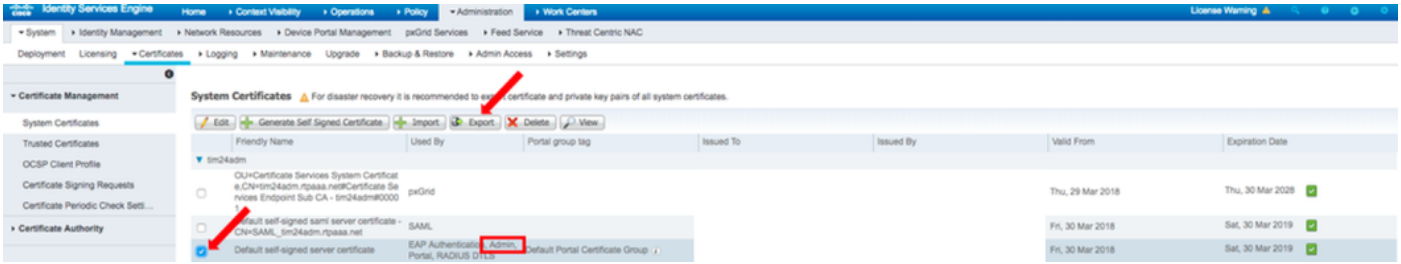
> **Observação**: este guia usa o certificado autoassinado padrão do ISE para uso do administrador. Se você usar um Certificado Admin assinado por uma Autoridade de Certificação (CA), exporte a CA raiz que assinou o certificado Admin no nó ISE MNT.

4. Clique em **Exportar**.

5. Escolha a opção para Exportar Certificado e Chave Privada.

6. Defina uma chave de criptografia.

7. **Exportar** e **Salvar** o arquivo como mostrado na imagem.

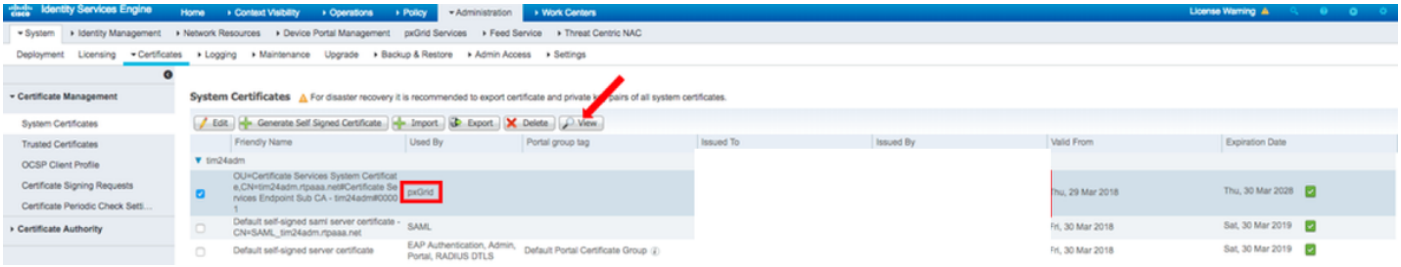



9. Retorne à tela Certificados do Sistema ISE.

10. Determine o campo Emitido por no certificado com o uso de "pxGrid" na coluna Usado por.

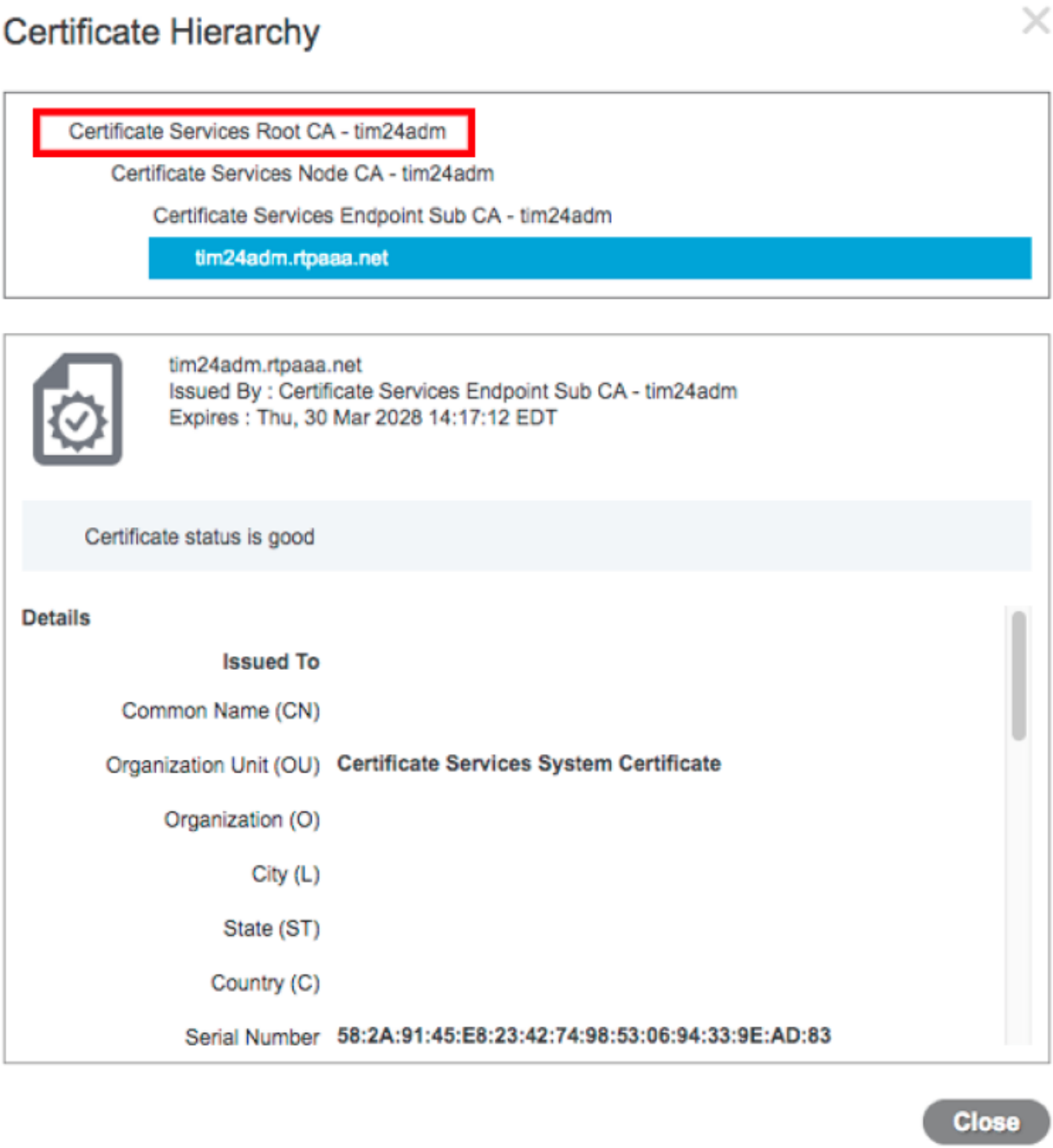
> **Observação**: em versões mais antigas do ISE, esse era um certificado autoassinado, mas a partir da versão 2.2 esse certificado é emitido pela Cadeia de CA interna do ISE por padrão.

11. Selecione o Certificado e clique em **Exibir** conforme mostrado na imagem.



12. Determine o certificado de nível superior (Raiz). Nesse caso, é **"Certificate Services Root CA - tim24adm".**

13. Feche a janela de visualização do certificado como mostrado na imagem.

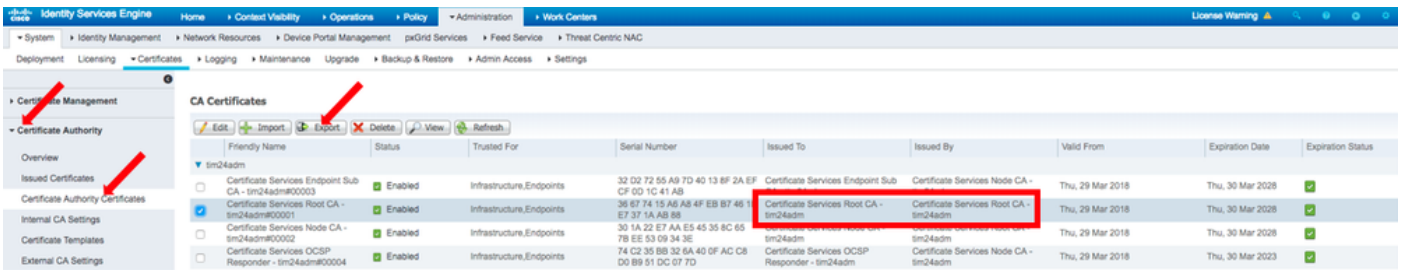



---

14. Expanda o menu ISE Certificate Authority.

15. Selecione **Certificados da Autoridade de Certificação**.

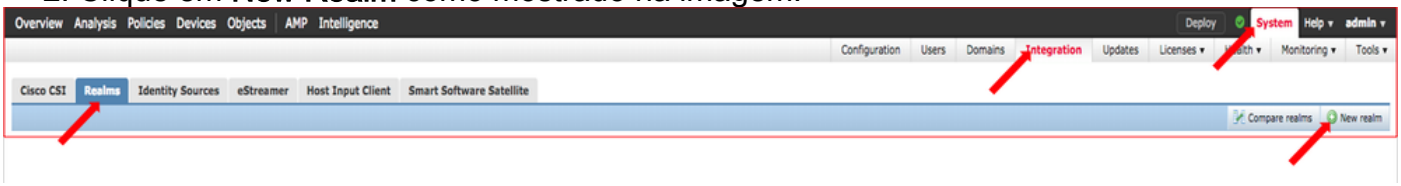
16. Selecione o Certificado Raiz identificado e clique em **Exportar.** Em seguida, salve o certificado CA raiz do pxGrid como mostrado na imagem.



# Configurar o FMC

## Etapa 4. Adicionar um novo território ao FMC

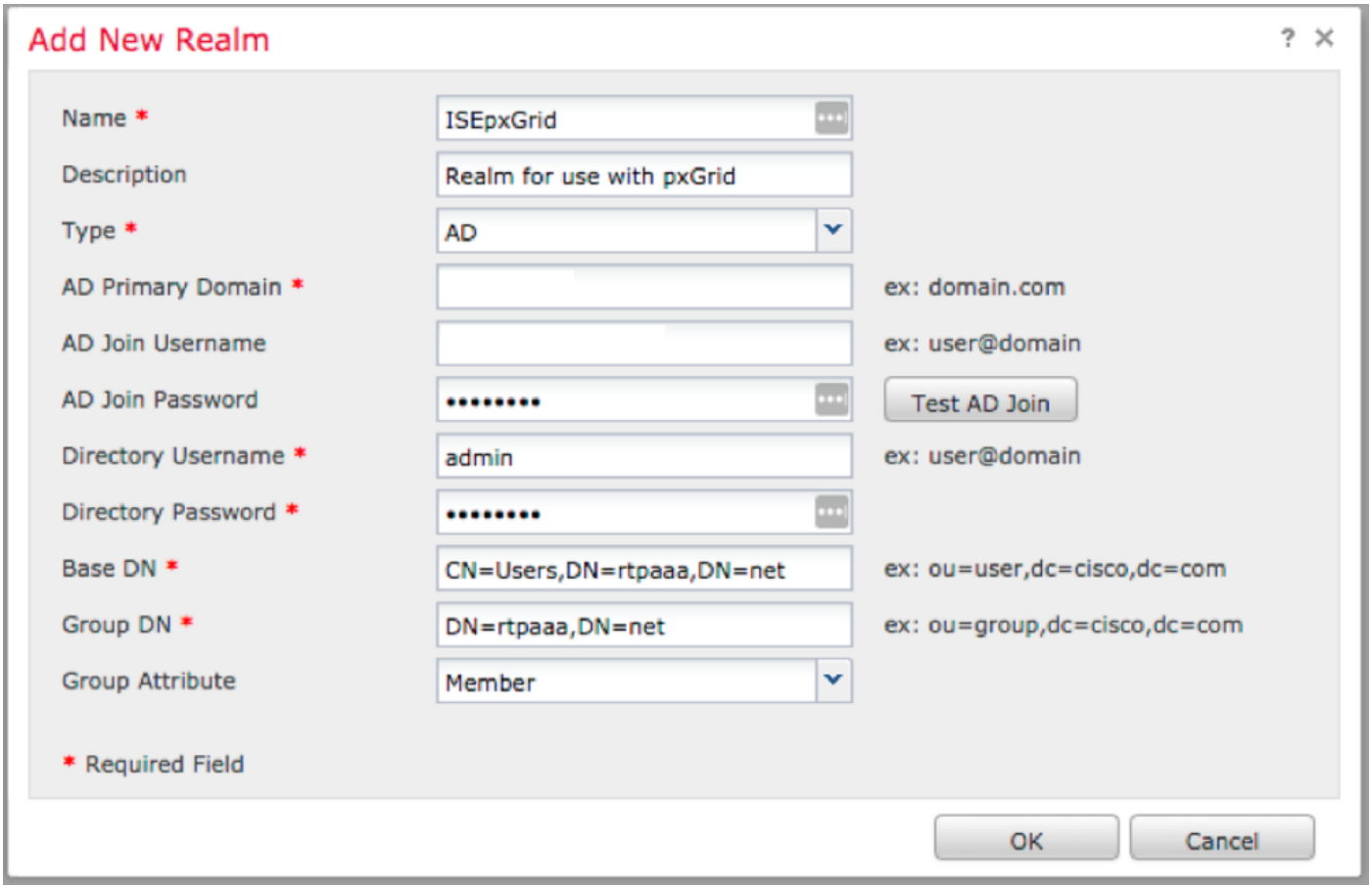
1. Acesse a GUI do FMC e navegue para **System > Integration > Realms**.
2. Clique em **New Realm** como mostrado na imagem.



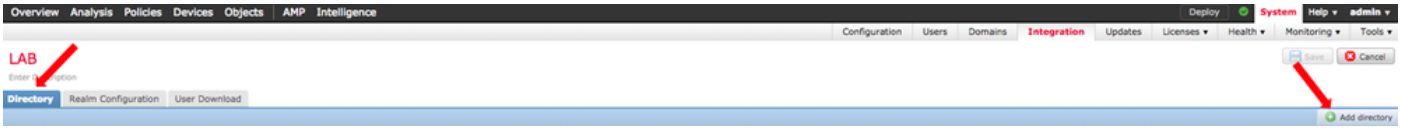

3. Preencha o formulário e clique no botão Testar associação do Ative Diretory (AD).

> **Observação**: o nome de usuário de associação ao AD deve estar no formato UPN ou o teste falhará.

4. Se Testar Ingresso do AD for bem-sucedido, clique em **OK**.



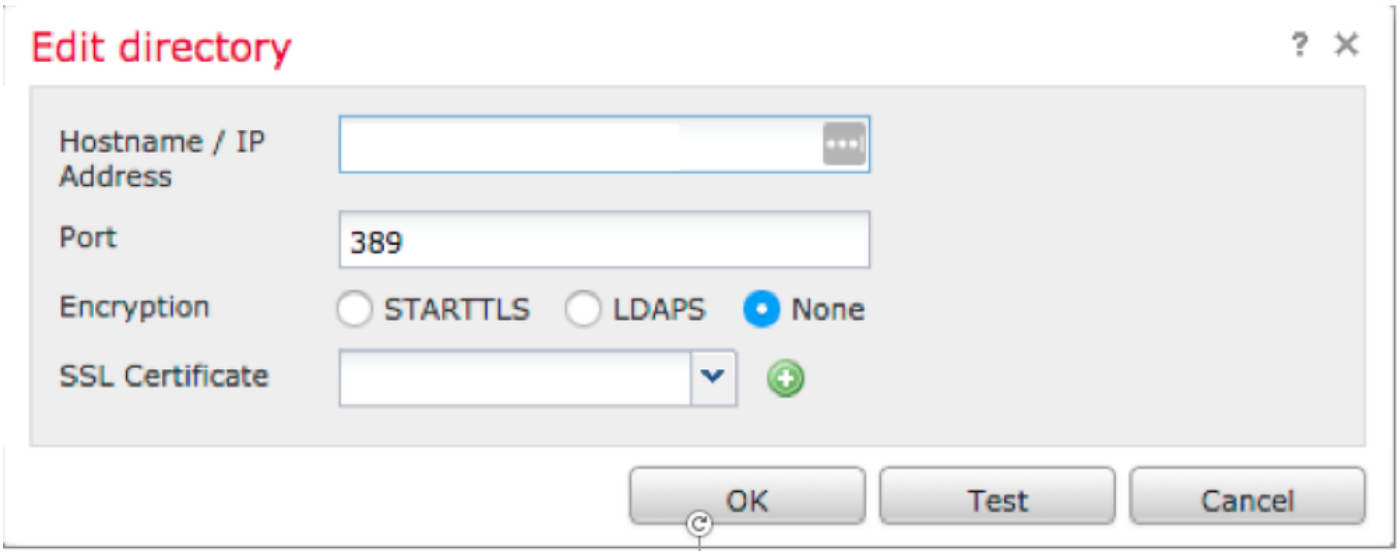

5. Clique na guia **Diretório** e, em seguida, clique em **Adicionar diretório** conforme mostrado na imagem.

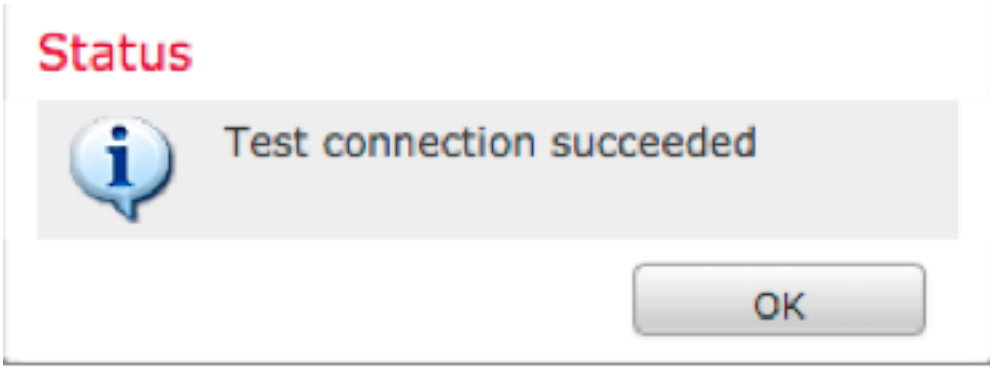



6. Configurar IP/Nome do Host e Testar Conexão.

**Observação**: Se o Teste falhar, verifique as credenciais na guia Configuração do Realm.

7. Clique em **OK**.



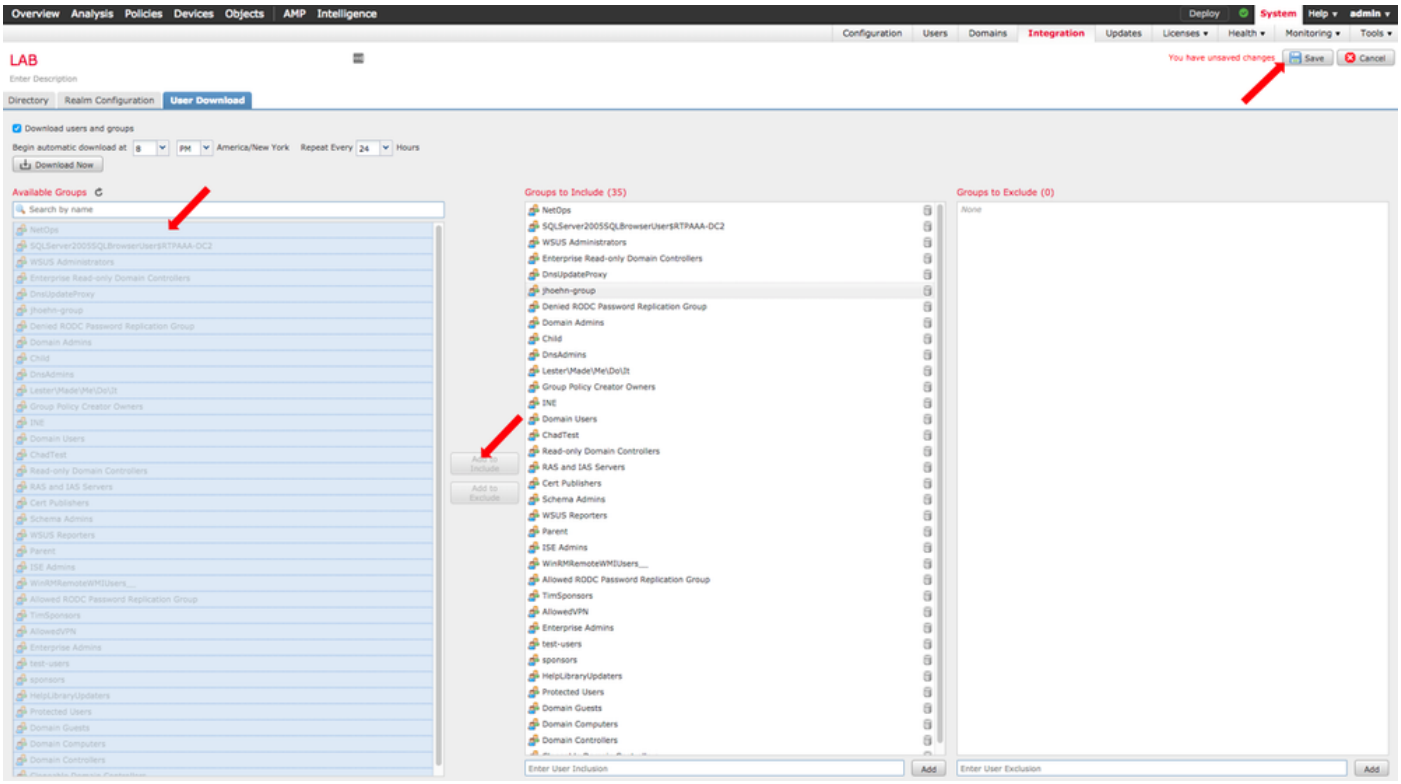

8. Clique na guia **Download do Usuário**.


9. Se ainda não estiver selecionado, habilite o download de usuários e grupos

10. Clique em Baixar Agora


11. Quando a lista for preenchida, adicione os grupos desejados e selecione **Adicionar à Inclusão**.

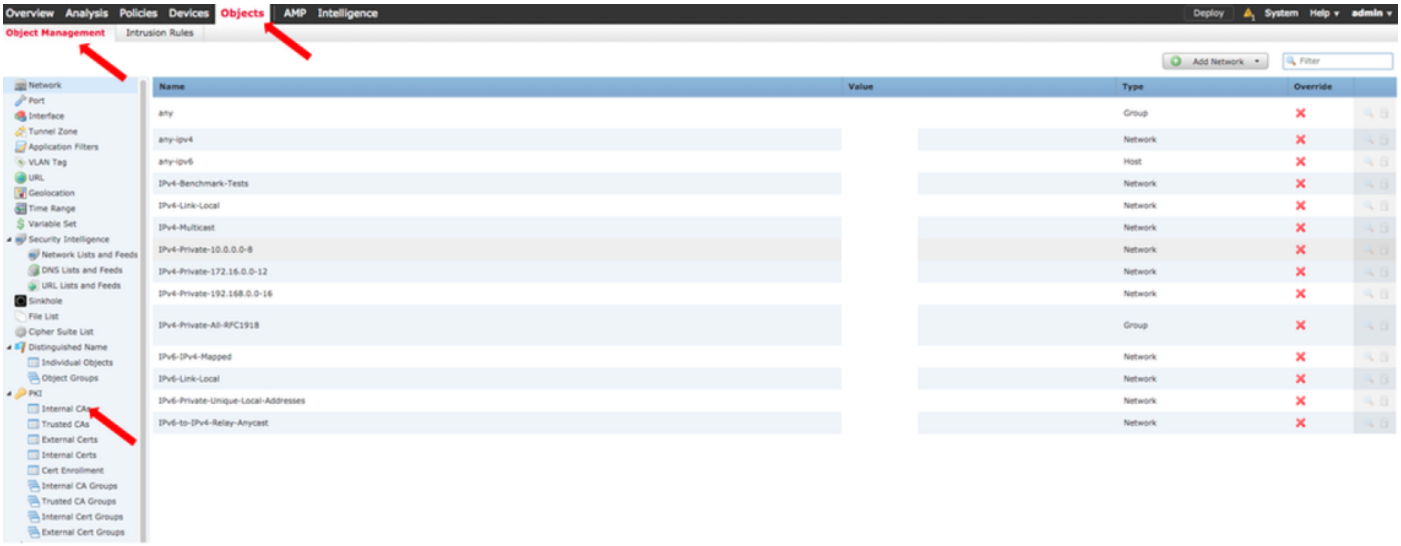
12. Salve a **Configuração do Realm**.



13. Ative o Estado do Realm.

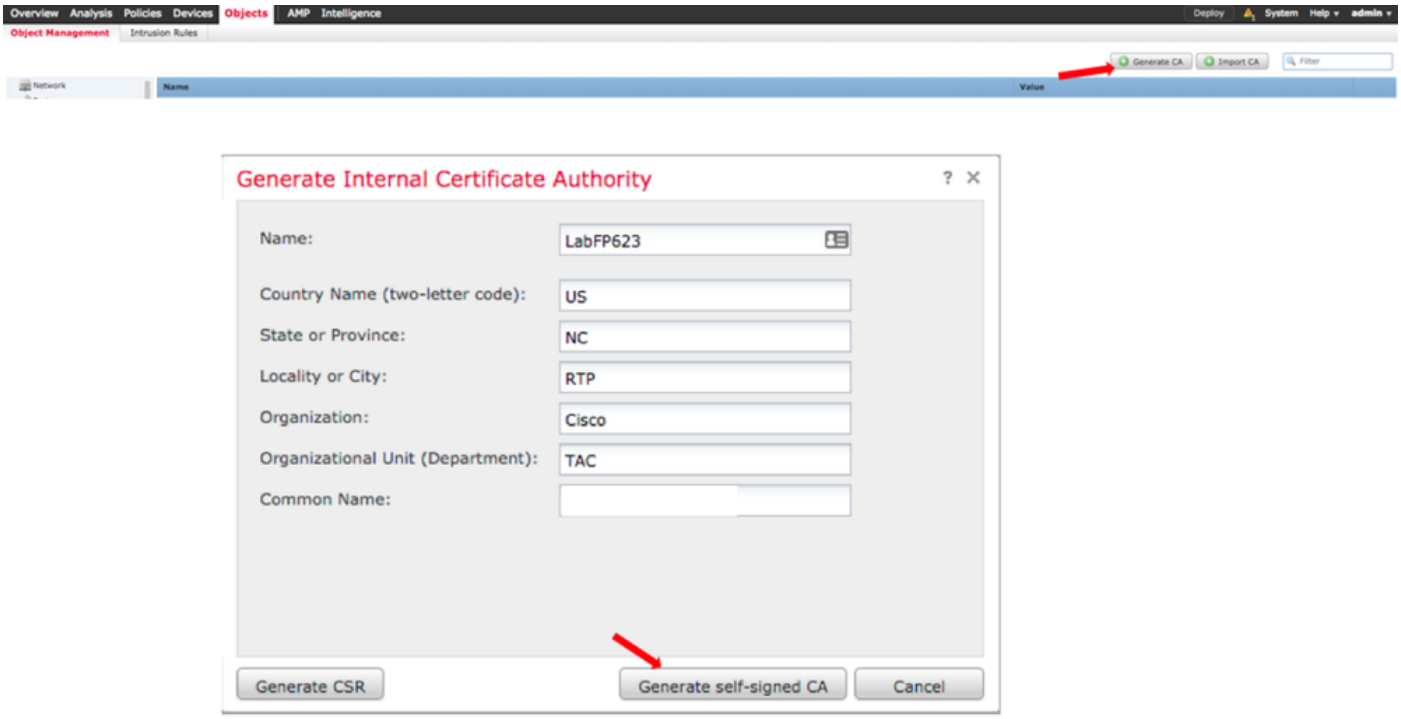
## Etapa 5. Gerar Certificado de CA do FMC

1. Navegue até **Objetos > Gerenciamento de Objetos > CAs Internas** conforme mostrado na imagem.



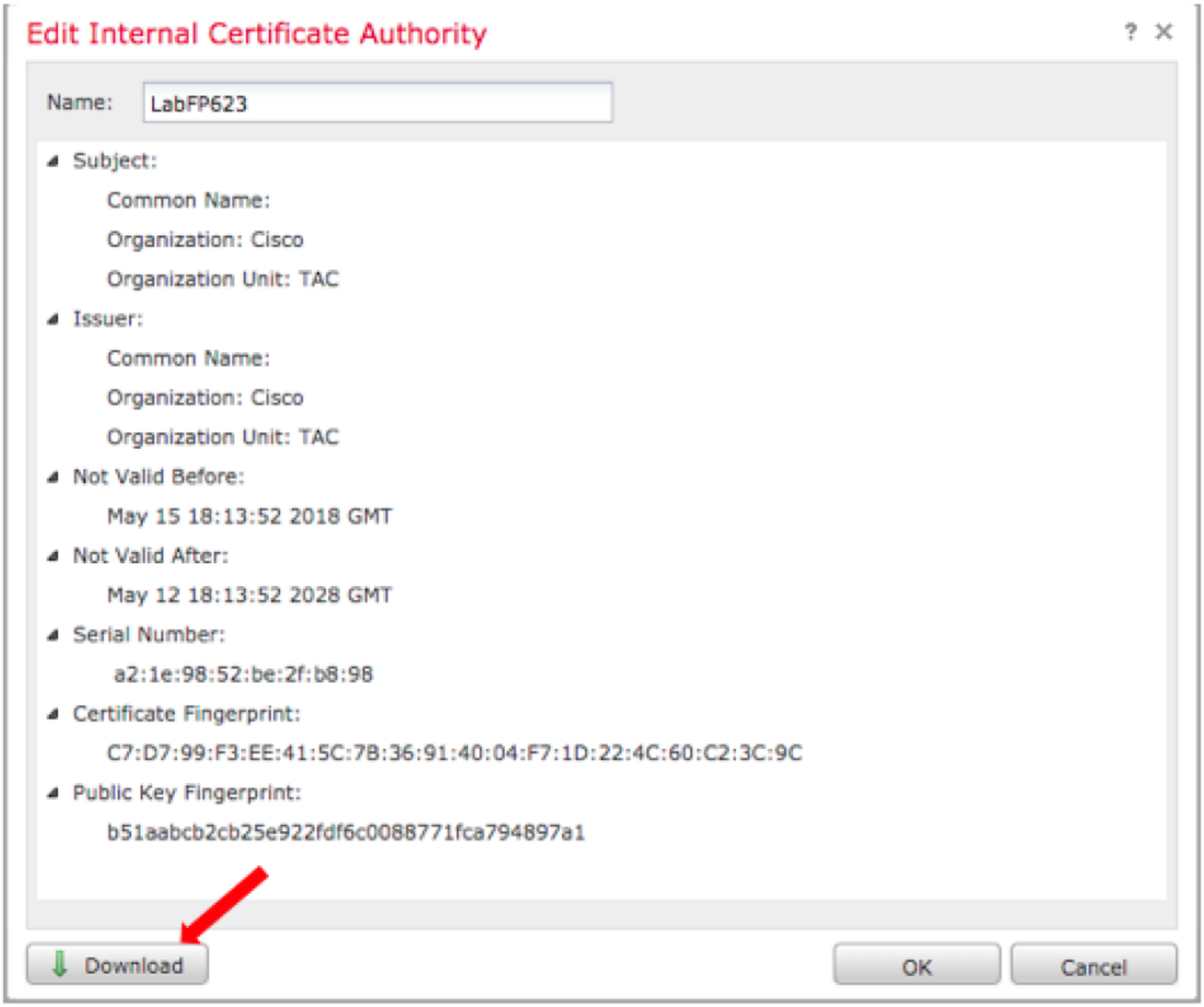

2. Clique em **Gerar CA**.

3. Preencha o formulário e clique em **Gerar CA autoassinada**.




4. Quando a geração terminar, clique no lápis à direita do Certificado CA gerado, conforme mostrado na imagem.


5. Clique em **Download**.




6. Configure e confirme a senha de criptografia e clique em **OK**.

7. Salve o arquivo Public-Key Cryptography Standards (PKCS) p12 no sistema de arquivos local.

## Etapa 6. Extraia o certificado e a chave privada do certificado gerado com o uso do OpenSSL

Isso é feito na raiz do FMC ou em qualquer cliente capaz de comandos OpenSSL. Este exemplo usa um shell padrão do Linux.

1. Use **openssl** para extrair o certificado (CER) e a chave privada (PVK) do arquivo p12.

2. Extraia o arquivo CER e configure a chave de exportação do certificado a partir da geração do certificado no 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. Extraia o arquivo PVK, configure a chave de exportação do certificado, defina uma nova senha

PEM e confirme.

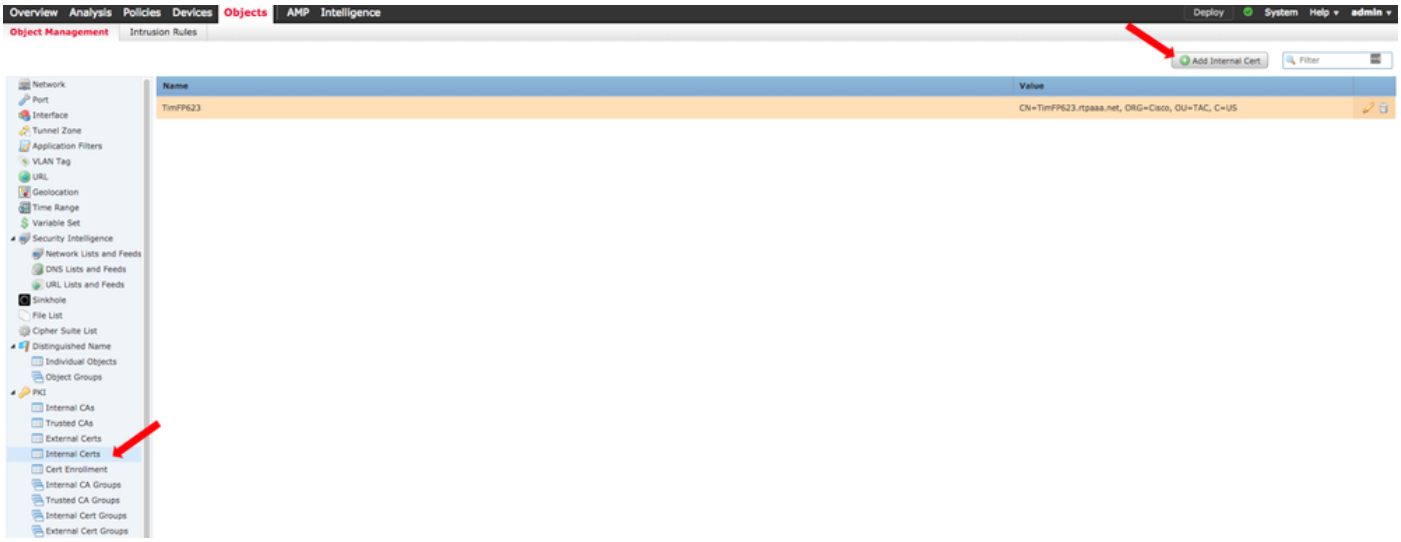
```
~$ openssl pkcs12 -nocerts -in <filename.p12> -out <filename.pvk>
Password:   Last login: Tue May 15 18:46:41 UTC 2018   Enter Import Password:   MAC verified OK
```

4. Esta frase PEM é necessária na próxima etapa.

## Passo 7. Instalar certificado no FMC

1. Navegue até **Objetos > Gerenciamento de Objetos > PKI > Certificados Internos**.

2. Clique em **Add Internal Cert** conforme mostrado na imagem.




3. Configure um nome para o Certificado Interno.

4. Navegue até o local do arquivo CER e selecione-o. Quando os Dados do certificado forem preenchidos, selecione o segundo.

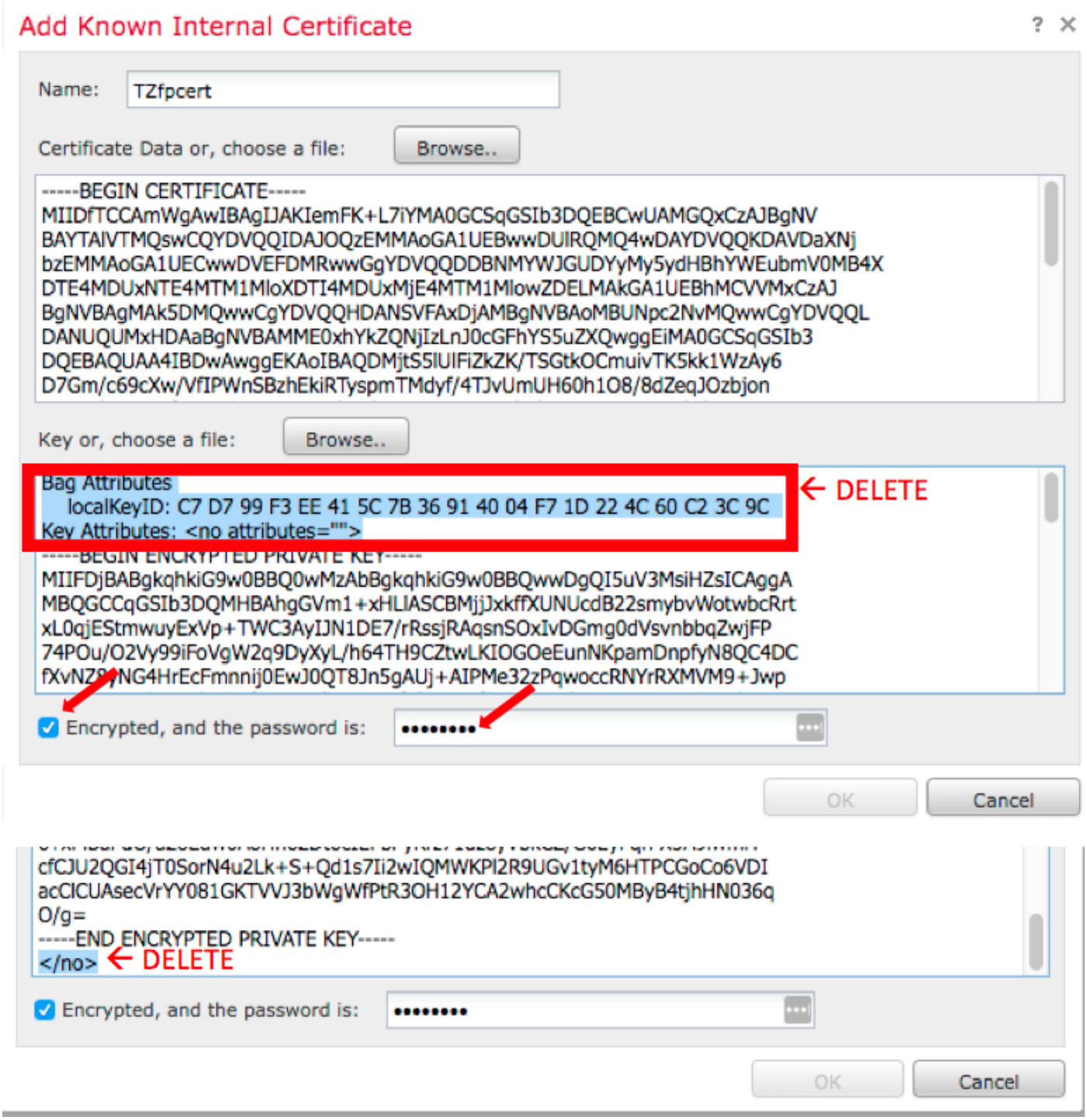
5. Navegue até **Opção** e selecione o arquivo PVK.

6. Exclua todos os "atributos de saco" à esquerda e todos os valores à direita na seção PVK. O PVK começa com **-----BEGIN ENCRYPTED PRIVATE KEY—** e termina com **-----END ENCRYPTED PRIVATE KEY—**.

> **Observação**: você não poderá clicar em **OK** se o texto PVK tiver caracteres fora dos hífens à esquerda e à direita.

7. Marque a caixa Encrypted e configure a senha criada quando o PVK foi exportado na Etapa 6.

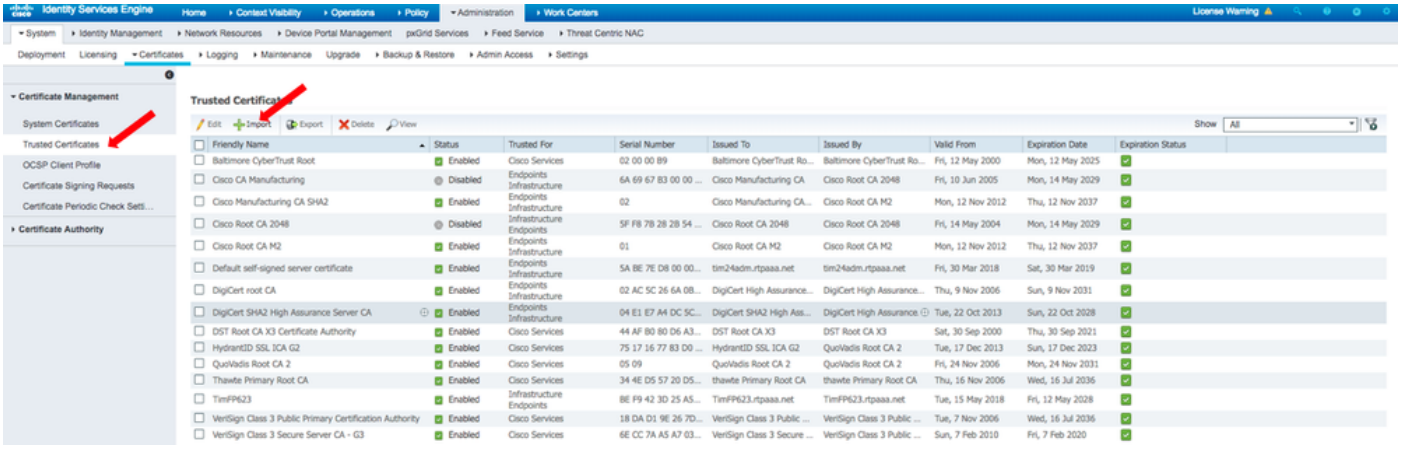
8. Clique em **OK**.




## Etapa 8. Importar o certificado FMC para o ISE

1. Acesse a **GUI do ISE** e navegue para **Administração > Sistema > Certificados > Certificados de Confiabilidade**.

2. Clique em **Importar**.



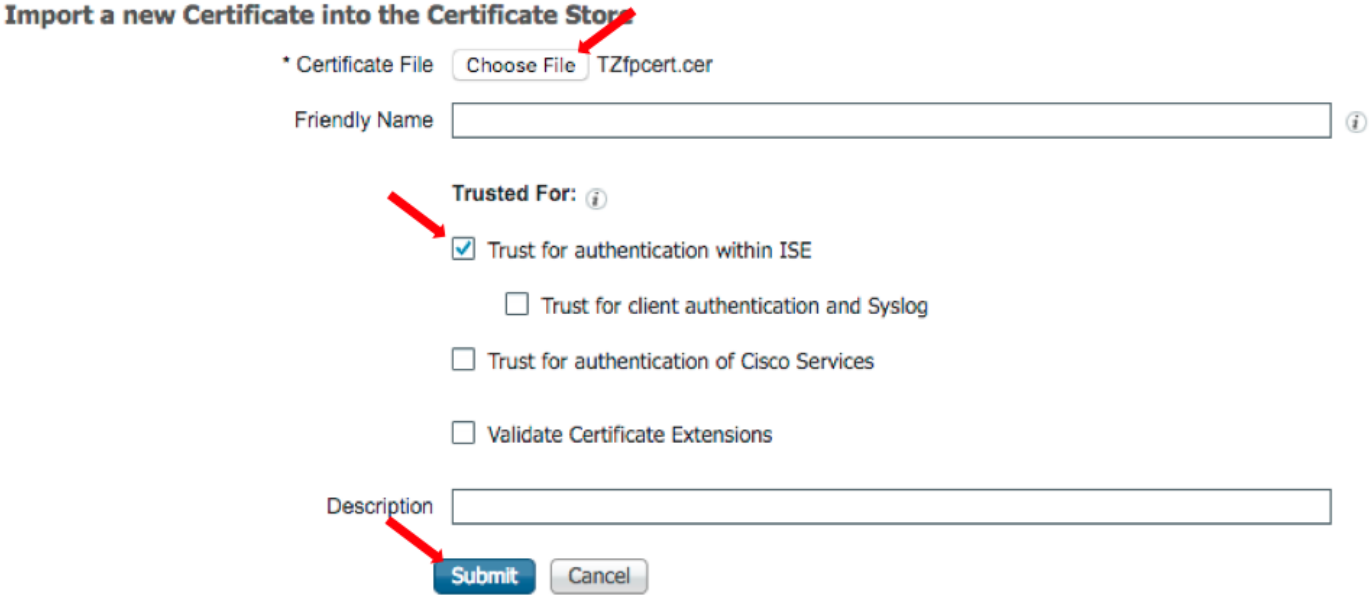
3. Clique em **Escolher arquivo** e selecione o arquivo CER do FMC do seu sistema local.

   Opcional: Configure um Nome Amigável.

4. Verifique a **Confiança** para a autenticação no ISE.

   Opcional: Configure uma Descrição.

5. Clique em **Enviar** conforme mostrado na imagem.




## Etapa 9. Configurar a conexão do pxGrid no FMC

1. Navegue até **System > Integration > Identity Sources** conforme mostrado na imagem.


2. Clique em **ISE**.

3. Configure o endereço IP ou o nome de host do nó pxGrid do ISE.

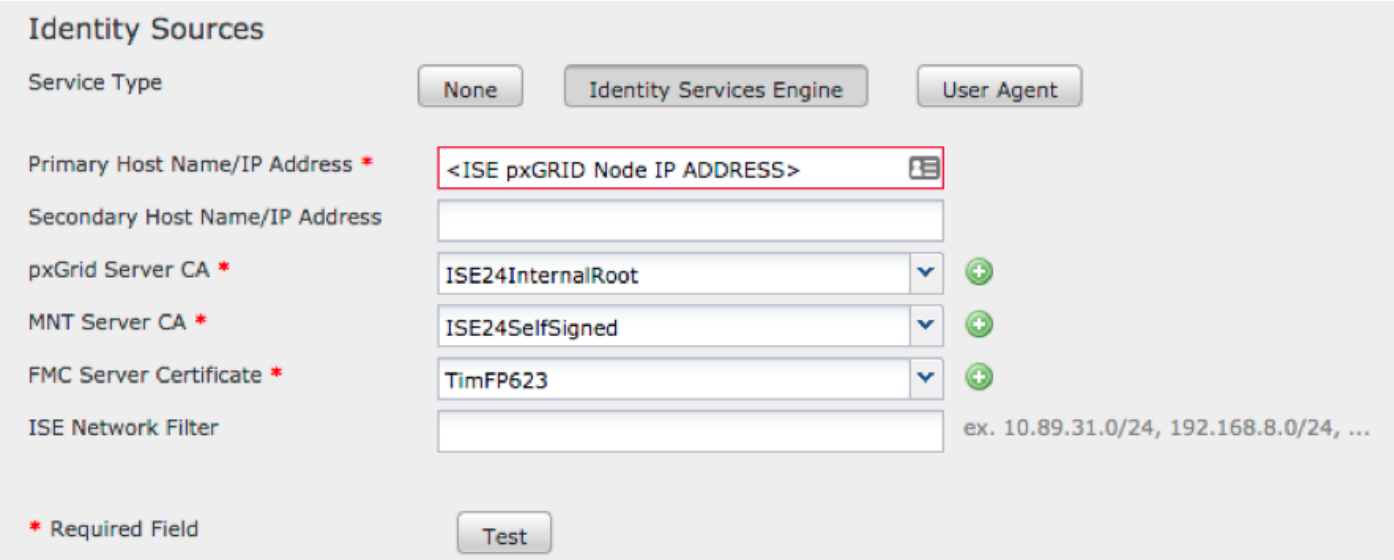
4. Selecione o + à direita de CA do pxGrid Server.

5. Nomeie o arquivo da CA do servidor e navegue até a CA de assinatura raiz do pxGrid coletada na Etapa 3. e clique em **Salvar**.

6. Selecione **+** à direita de MNT Server CA.

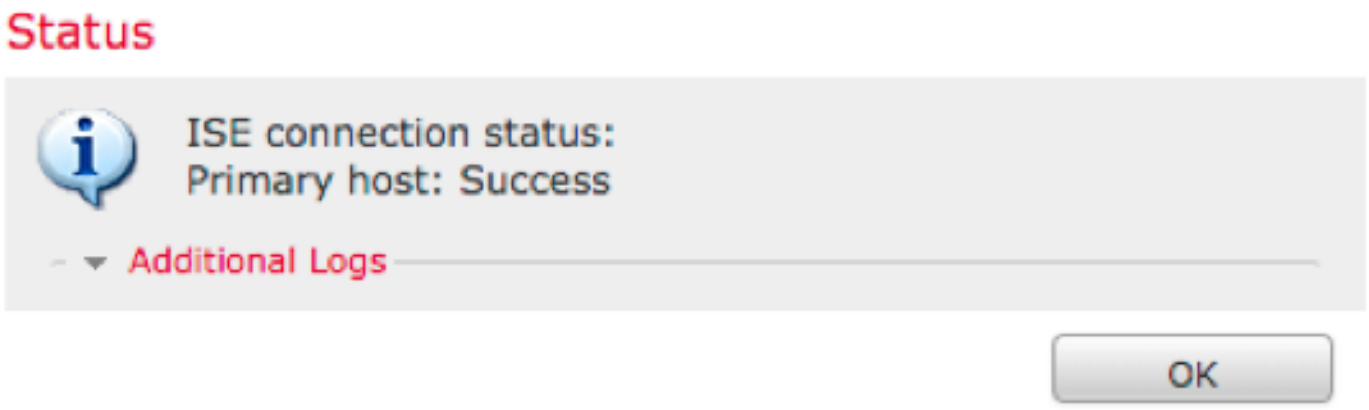
7. Nomeie o arquivo Server CA e navegue até o certificado Admin coletado na Etapa 3. e clique em **Salvar**.

8. Selecione o arquivo **FMC CER** na lista suspensa.




9. Clique em **Testar**.

10. Se o teste for bem-sucedido, clique em **OK**, depois em **Salvar** no canto superior direito da tela.




**Observação**: quando você executa dois nós do ISE pxGrid, é normal que um host mostre Êxito e outro mostre Falha, já que o pxGrid é executado ativamente apenas em um nó do ISE por vez. Depende da configuração se o host principal deve exibir Falha e o host secundário deve exibir Êxito. Tudo isso depende de qual nó no ISE é o nó pxGrid ativo.

# Verificar

## Verificação no ISE

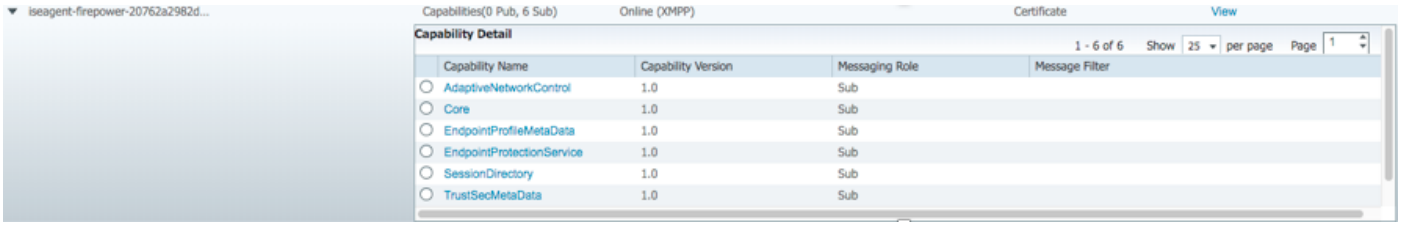
1. Abra a **GUI do ISE** e navegue para **Administração > serviços do pxGrid**.

Se obtiver êxito, duas conexões firepower serão listadas na lista de clientes. Um para o FMC real (iseagent-hostname-33bytes) e um para o dispositivo de teste (firesightisetest-hostname-33bytes).


A conexão iseagent-firepower exibe seis (6) subs e é exibida on-line.

A conexão firesightisetest-firepower exibe zero (0) subs e aparece offline.

A visualização expandida do cliente iseagent-firepower exibe as seis assinaturas.

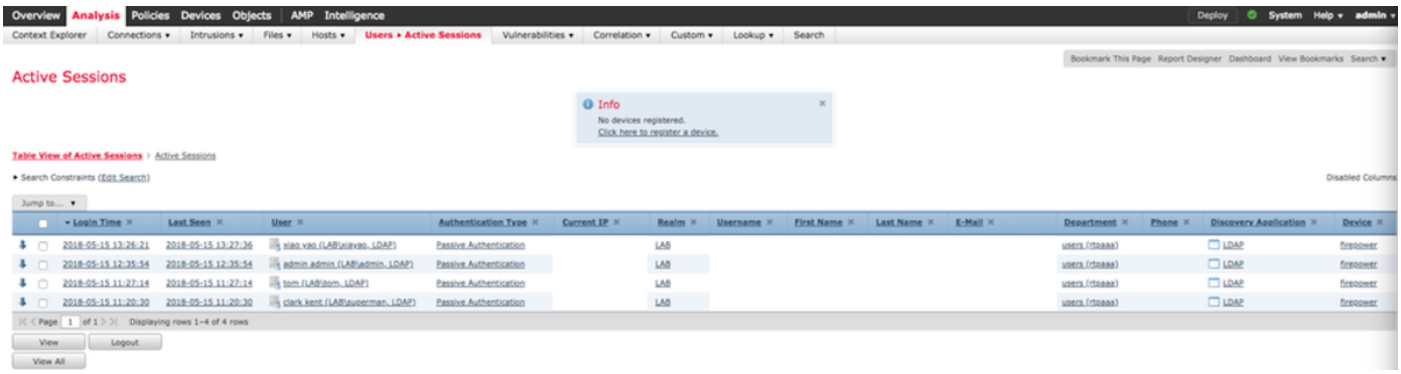



> **Observação**: devido ao bug da Cisco IDCSCvo75376 há uma limitação de nome de host e o download em massa falha. O botão de teste no FMC exibe uma falha de conectividade. Isso afeta 2.3p6, 2.4p6 e 2.6. A recomendação atual é executar o 2.3 patch 5 ou o 2.4 patch 5 até que um patch oficial seja liberado.

## Verificação no CVP

1. Abra a GUI do FMC e navegue para **Analysis > Users > Ative Sessions**.

Qualquer sessão ativa publicada através do recurso de diretório de sessão no ISE é exibida na tabela Sessões ativas no FMC.




No modo sudo da CLI do FMC, '**adi_cli session**' exibe as informações de sessão do usuário enviadas do ISE para o 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

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.