

Configuración de la integración de pxGrid de ISE 2.4 y FMC 6.2.3

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configuración de ISE](#)

[Paso 1. Habilitar servicios pxGrid](#)

[Paso 2. Configuración de ISE para aprobar todas las cuentas basadas en certificados de pxGrid](#)

[Paso 3. Exportar certificado de administración MNT de ISE y certificados de CA pxGrid](#)

[Configurar FMC](#)

[Paso 4. Añadir un nuevo rango a FMC](#)

[Paso 5. Generar certificado de CA de FMC](#)

[Paso 6. Extraiga el certificado y la clave privada del certificado generado con OpenSSL](#)

[Paso 7. Instalar certificado en FMC](#)

[Paso 8. Importar el certificado de FMC a ISE](#)

[Paso 9. Configuración de la conexión pxGrid en FMC](#)

[Verificación](#)

[Verificación en ISE](#)

[Verificación en CSP](#)

[Troubleshoot](#)

Introducción

Este documento describe el proceso de configuración para la integración de ISE pxGrid versión 2.4 y FMC versión 6.2.3.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- ISE 2.4
- CSP 6.2.3
- Active Directory/Protocolo ligero de acceso a directorios (LDAP)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y

hardware.

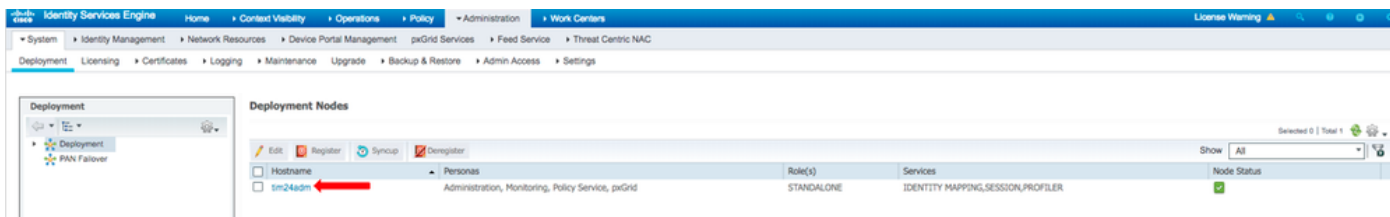
- ISE 2.4 independiente
- FMCv 6.2.3
- Active Directory 2012R2
- Identity Services Engine (ISE) pxGrid versión 2.4
- Firepower Management Center (FMC) versión 6.2.3

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configuración de ISE

Paso 1. Habilitar servicios pxGrid

1. Inicie sesión en la GUI de administración de ISE y navegue hasta **Administration > Deployment**.
2. Seleccione el nodo de ISE que se utilizará para pxGrid persona.



3. Habilite el servicio pxGrid y haga clic en **Guardar** como se muestra en la imagen.

Deployment Nodes List > tim24adm

Edit Node

General Settings | Profiling Configuration

Hostname
FQDN
IP Address
Node Type: Identity Services Engine (ISE)

Role: STANDALONE **Make Primary**

Administration

Monitoring

Role: PRIMARY

Other Monitoring Node

Policy Service

Enable Session Services (i)

Include Node in Node Group: None (i)

Enable Profiling Service (i)

Enable Threat Centric NAC Service (i)

Enable SXP Service (i)

Enable Device Admin Service (i)

Enable Passive Identity Service (i)

pxGrid (i)

Save Reset

4. Compruebe que los servicios pxGrid se ejecutan desde la CLI.

Nota: El proceso requiere hasta 5 minutos para que los servicios pxGrid se inicien por completo y determinen el estado de alta disponibilidad (HA) si hay más de un nodo pxGrid en uso.

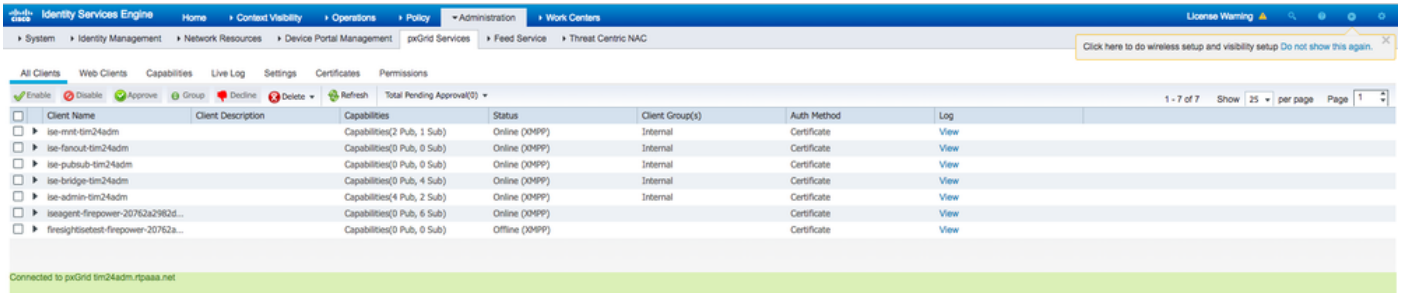
5. SSH en la CLI del nodo pxGrid de ISE y compruebe el estado de la aplicación.

```
# 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. Acceder a la GUI de administración de ISE y comprobar que los servicios están online y funcionan. Vaya a **Administration > pxGrid Services**.

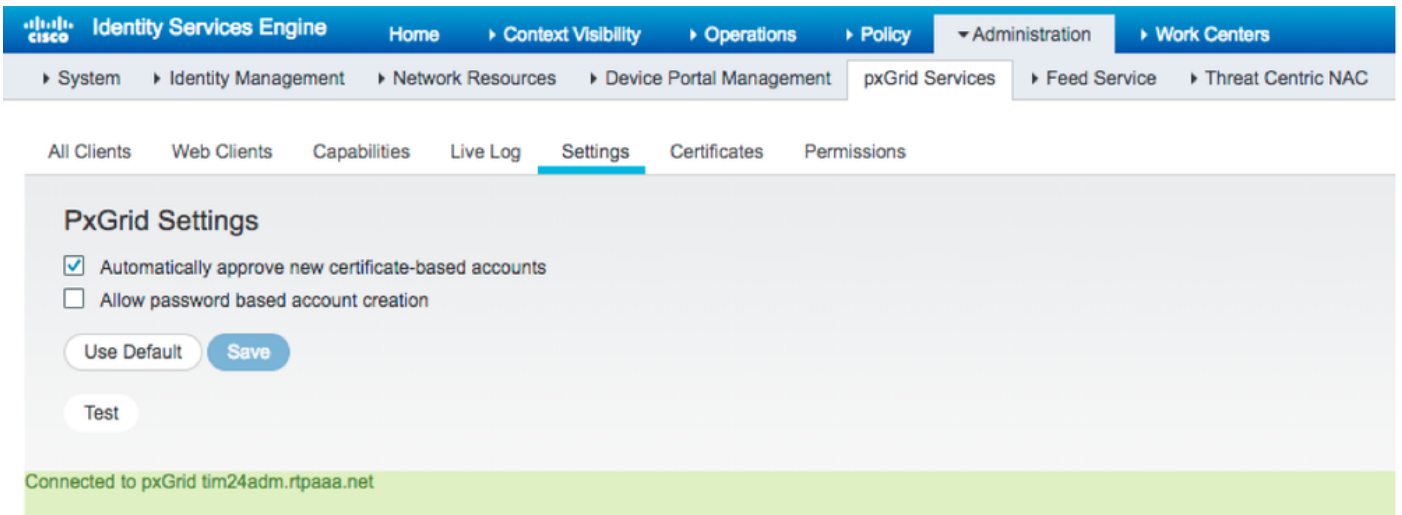
7. En la parte inferior de la página, ISE muestra **Conectado a pxGrid <FQDN de nodo de**

pxGrid>.



Paso 2. Configuración de ISE para aprobar todas las cuentas basadas en certificados de pxGrid

1. Vaya a **Administration > pxGrid Services > Settings**.
2. Marque la casilla: "Aprobar automáticamente nuevas cuentas basadas en certificados" y haga clic en **Guardar**.



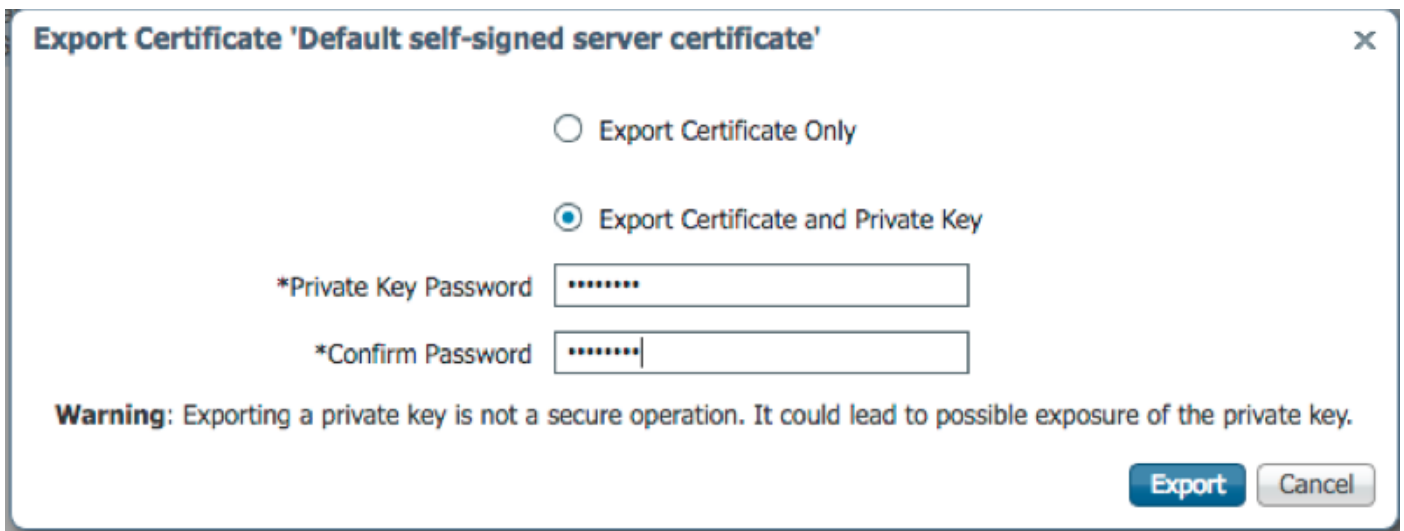
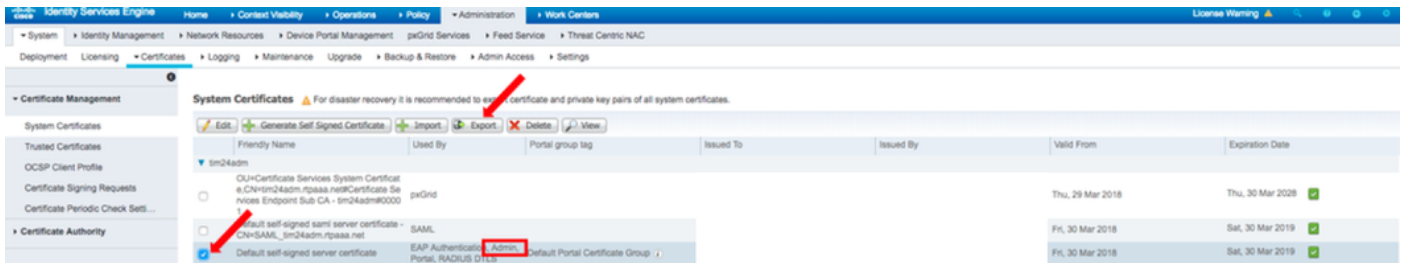
Nota: el administrador debe aprobar manualmente la conexión de FMC a ISE si esta opción no está activada.

Paso 3. Exportar certificado de administración MNT de ISE y certificados de CA pxGrid

1. Vaya a **Administration > Certificates > System Certificates**.
2. Expanda el nodo Supervisión principal (MNT) si no está activado en el nodo Administración principal.
3. Seleccione el certificado con el campo Utilizado por "Admin".

Nota: esta guía utiliza el certificado autofirmado de ISE predeterminado para uso del administrador. Si utiliza un certificado de administrador firmado por la autoridad certificadora (CA), exporte la CA raíz que firmó el certificado de administrador en el nodo MNT de ISE.

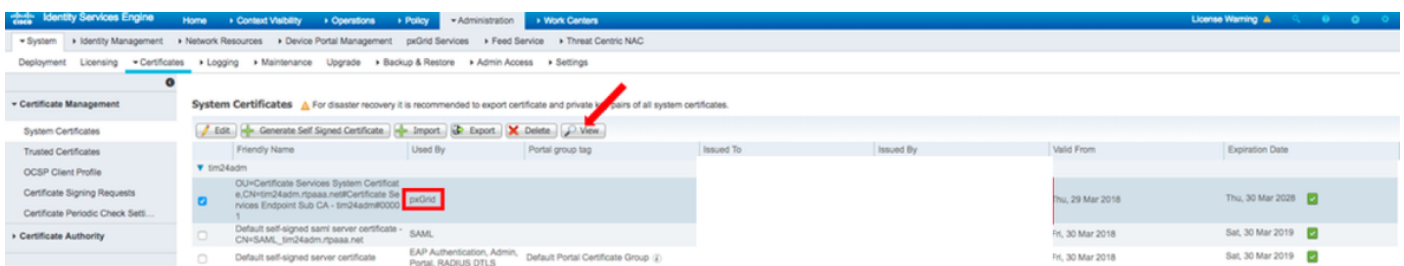
- Haga clic en **Exportar**.
- Seleccione la opción Exportar Certificado y Clave Privada.
- Establezca una clave de cifrado.
- Exportar y Guardar** el archivo como se muestra en la imagen.



- Vuelva a la pantalla ISE System Certificates.
- Determine el campo Emitido por en el certificado con el uso "pxGrid" en la columna Utilizado por.

Nota: en versiones anteriores de ISE, se trataba de un certificado autofirmado, pero a partir de la versión 2.2 este certificado lo emite la cadena interna de CA de ISE de forma predeterminada.

- Seleccione el certificado y haga clic en **Ver** como se muestra en la imagen.




- Determine el certificado de nivel superior (raíz). En este caso es **"Certificate Services Root CA - tim24adm"**.

13. Cierre la ventana de vista de certificado como se muestra en la imagen.

Certificate Hierarchy



Certificate Services Root CA - tim24adm
Certificate Services Node CA - tim24adm
Certificate Services Endpoint Sub CA - tim24adm
tim24adm.rtpaaa.net

 tim24adm.rtpaaa.net
Issued By : Certificate Services Endpoint Sub CA - tim24adm
Expires : Thu, 30 Mar 2028 14:17:12 EDT

Certificate status is good

Details

Issued To

Common Name (CN)

Organization Unit (OU) **Certificate Services System Certificate**

Organization (O)

City (L)

State (ST)

Country (C)

Serial Number **58:2A:91:45:E8:23:42:74:98:53:06:94:33:9E:AD:83**

Close

14. Expanda el menú ISE Certificate Authority.

15. Seleccione **Certificados de Autoridad Certificadora**.

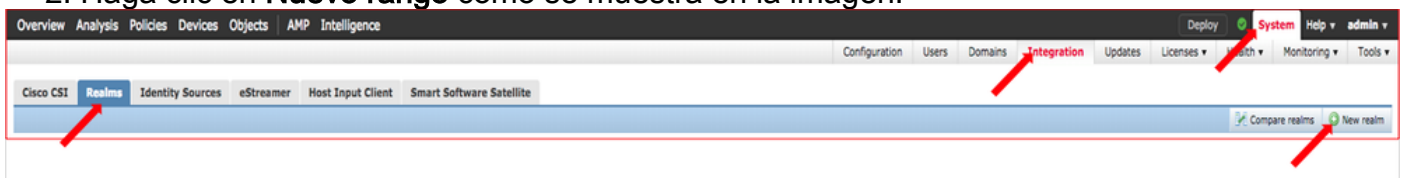
16. Seleccione el certificado raíz identificado y haga clic en **Exportar**. A continuación, guarde el certificado de CA raíz de pxGrid como se muestra en la imagen.

Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiration Status
Certificate Services Endpoint Sub CA - sm24adm#00003	Enabled	Infrastructure.Endpoints	32 D2 72 55 A9 7D 40 13 8F 2A EF CF 0D 1C 41 AB	Certificate Services Endpoint Sub CA - sm24adm	Certificate Services Node CA - sm24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2028	✓
Certificate Services Root CA - sm24adm#00001	Enabled	Infrastructure.Endpoints	36 67 74 15 A6 A8 4F EB B7 46 87 37 1A A8 56	Certificate Services Root CA - sm24adm	Certificate Services Root CA - sm24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2028	✓
Certificate Services Node CA - sm24adm#00002	Enabled	Infrastructure.Endpoints	30 1A 22 E7 AA E5 45 35 8C 65 7B EE 53 09 34 3E	sm24adm	sm24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2028	✓
Certificate Services OCSP Responder - sm24adm#00004	Enabled	Infrastructure.Endpoints	74 C2 35 B8 32 6A 40 0F AC C8 D9 B9 51 DC 07 7D	Certificate Services OCSP Responder - sm24adm	Certificate Services Node CA - sm24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2023	✓

Configurar FMC

Paso 4. Añadir un nuevo rango a FMC

1. Acceda a la GUI de FMC y navegue hasta **System > Integration > Realms**.
2. Haga clic en **Nuevo rango** como se muestra en la imagen.



3. Rellene el formulario y haga clic en el botón Probar unión a Active Directory (AD).

Nota: el nombre de usuario de la unión a AD debe estar en formato de nombre principal de usuario (UPN); de lo contrario, la prueba fallará.

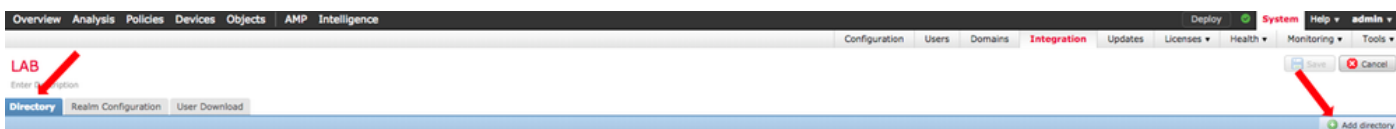
4. Si la unión de prueba de AD es satisfactoria, haga clic en **Aceptar**.

Add New Realm

Name *	ISEpxGrid	
Description	Realm for use with pxGrid	
Type *	AD	
AD Primary Domain *		ex: domain.com
AD Join Username		ex: user@domain
AD Join Password	<input type="button" value="Test AD Join"/>
Directory Username *	admin	ex: user@domain
Directory Password *	
Base DN *	CN=Users,DN=rtpaaa,DN=net	ex: ou=user,dc=cisco,dc=com
Group DN *	DN=rtpaaa,DN=net	ex: ou=group,dc=cisco,dc=com
Group Attribute	Member	

* Required Field

5. Haga clic en la pestaña **Directorio** y luego haga clic en **Agregar directorio** como se muestra en la imagen.



6. Configure el nombre de host/IP y pruebe la conexión.

Nota: Si la prueba falla, verifique las credenciales en la ficha Configuración de rango.

7. Haga clic en **Aceptar**.

Edit directory

Hostname / IP Address	
Port	389
Encryption	<input type="radio"/> STARTTLS <input type="radio"/> LDAPS <input checked="" type="radio"/> None
SSL Certificate	<input type="text"/> <input type="button" value="+"/>



8. Haga clic en la ficha **Descarga de usuario**.



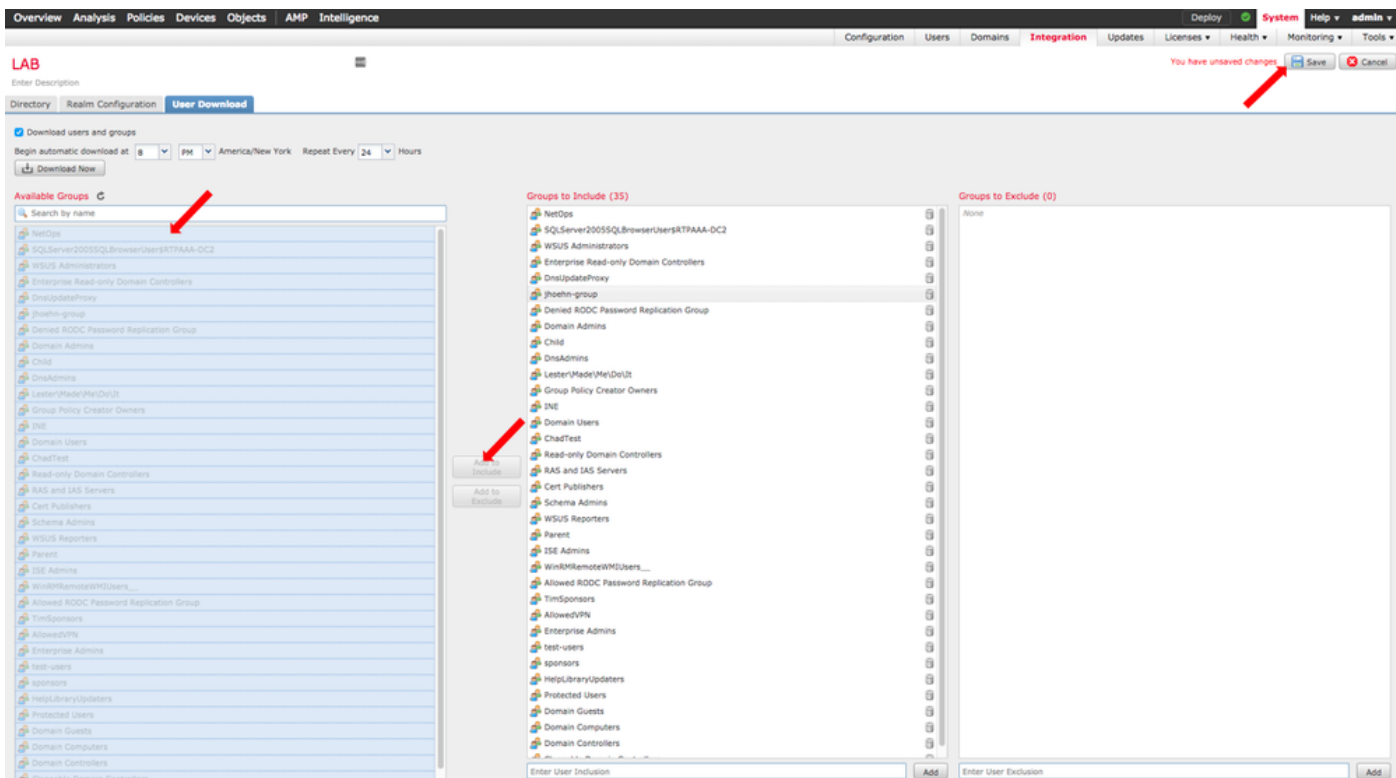
9. Si aún no está seleccionado, active la descarga de usuarios y grupos

10. Haga clic en Descargar ahora



11. Una vez cumplimentada la lista, agregue los grupos deseados y seleccione **Agregar a Incluir**.

12. Guarde la **configuración de rango**.

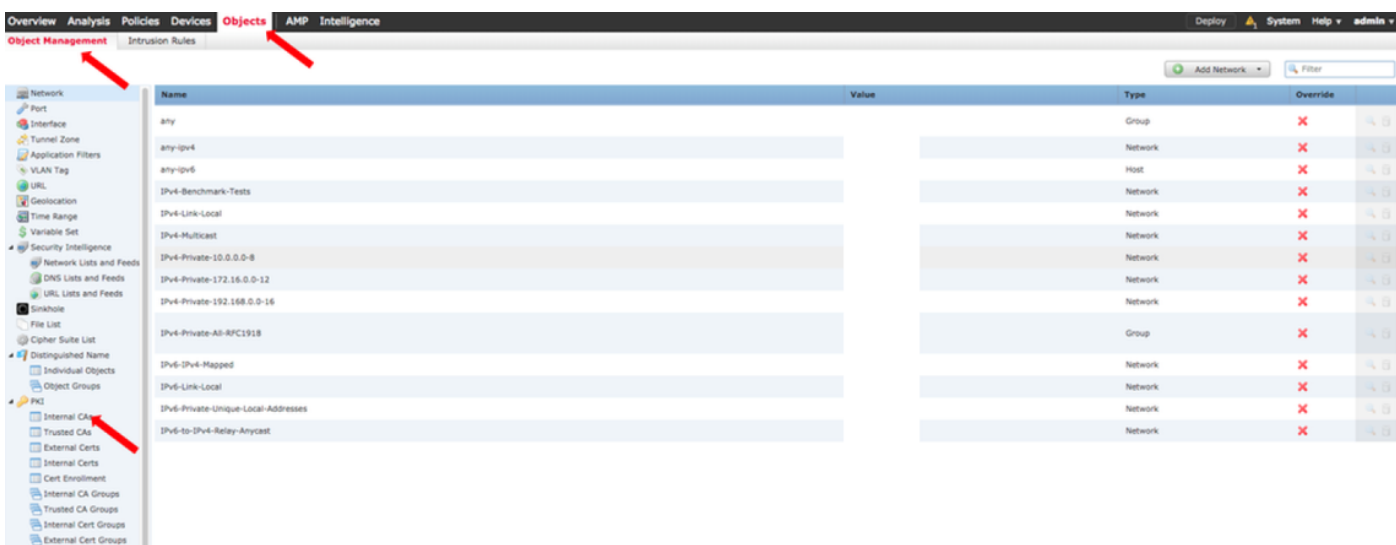


13. Active el estado de rango.



Paso 5. Generar certificado de CA de FMC

1. Navegue hasta **Objetos > Administración de objetos > CA internas** como se muestra en la imagen.



2. Haga clic en **Generar CA**.

3. Rellene el formulario y haga clic en **Generar CA autofirmada**.



Generate Internal Certificate Authority

Name:

Country Name (two-letter code):

State or Province:

Locality or City:

Organization:

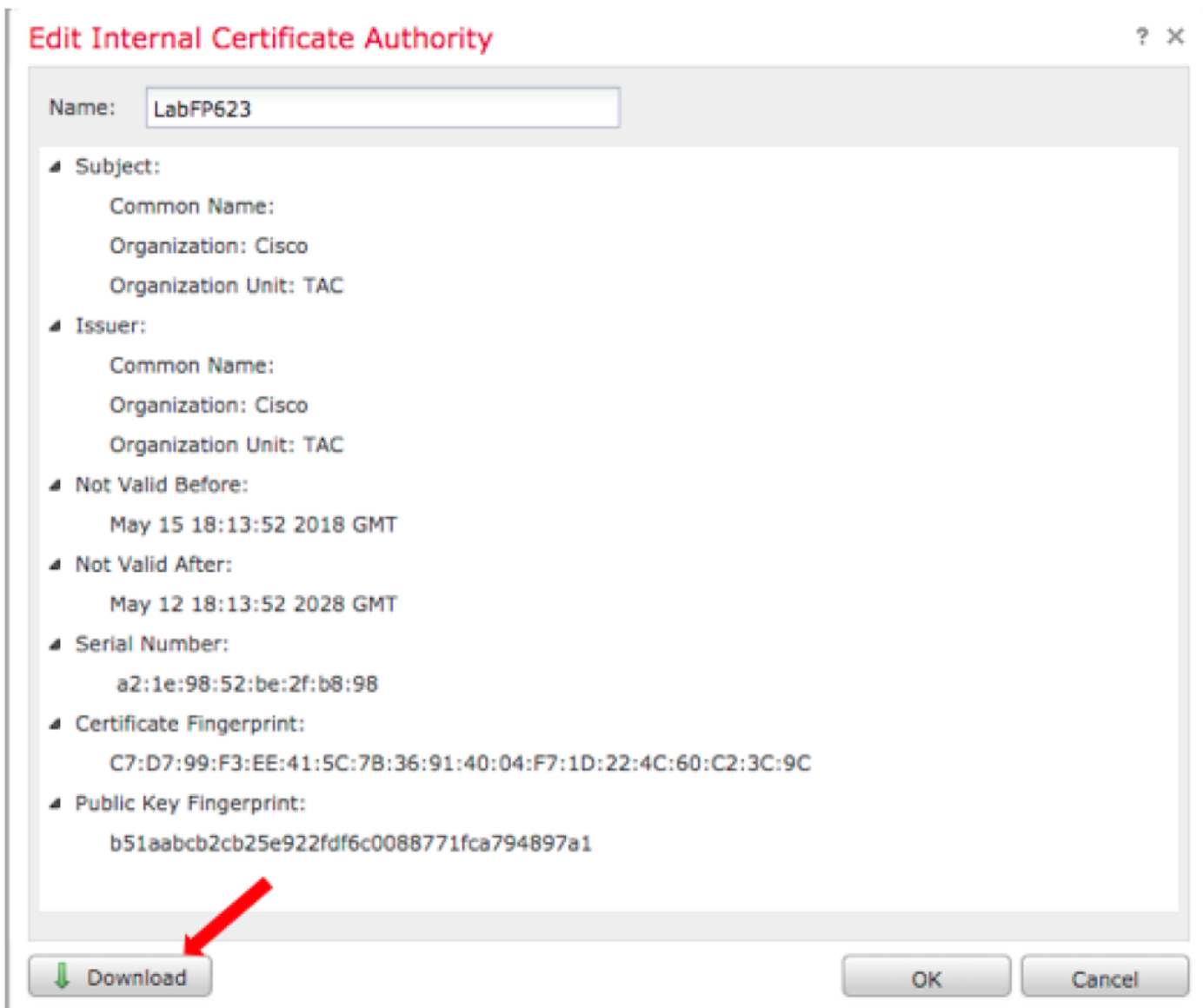
Organizational Unit (Department):

Common Name:

4. Una vez finalizada la generación, haga clic en el lápiz situado a la derecha del certificado de CA generado, como se muestra en la imagen.



5. Haga clic en **Descargar**.



6. Configure y confirme la contraseña de cifrado y haga clic en **Aceptar**.

7. Guarde el archivo Public-Key Cryptography Standards (PKCS) p12 en su sistema de archivos local.

Paso 6. Extraiga el certificado y la clave privada del certificado generado con OpenSSL

Esto se hace en la raíz del FMC, o en cualquier cliente capaz de comandos OpenSSL. Este ejemplo utiliza un shell estándar de Linux.

1. Utilice **openssl** para extraer el certificado (CER) y la clave privada (PVK) del archivo p12.
2. Extraiga el archivo CER y, a continuación, configure la clave de exportación del certificado de la generación de certificados en 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. Extraiga el archivo PVK, configure la clave de exportación del certificado, luego establezca una nueva frase de contraseña PEM y confirme.

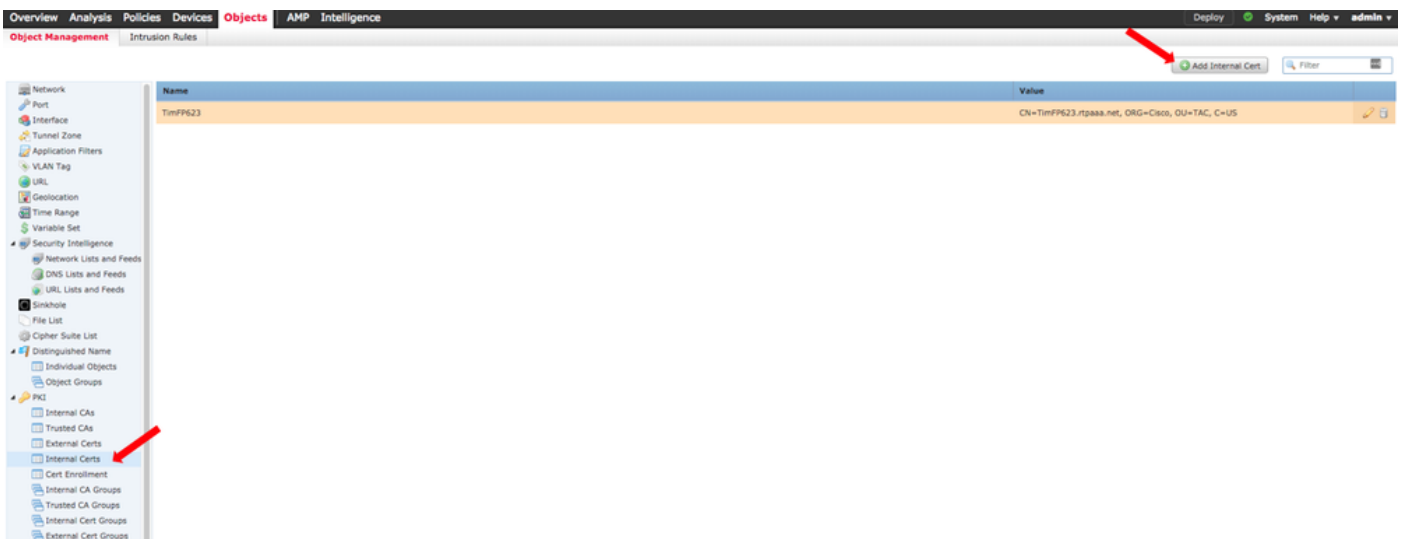
```
~$ openssl pkcs12 -nocerts -in <filename.p12> -out <filename.pvk>
```

Password: Last login: Tue May 15 18:46:41 UTC 2018 Enter Import Password: MAC verified OK

4. Esta frase PEM es necesaria en el siguiente paso.

Paso 7. Instalar certificado en FMC

1. Acceda a **Objetos > Gestión de Objetos > PKI > Certificados Internos**.
2. Haga clic en **Add Internal Cert** como se muestra en la imagen.



3. Configure un nombre para el certificado interno.

4. Busque la ubicación del archivo CER y selecciónelo. Una vez cumplimentados los datos del certificado, seleccione el segundo.

5. Busque **Opción** y seleccione el archivo PVK.

6. Elimine los "atributos Bag" iniciales y los valores finales de la sección PVK. La PVK comienza con -----BEGIN ENCRYPTED PRIVATE KEY y termina con -----END ENCRYPTED PRIVATE KEY.

Nota: No puede hacer clic en **Aceptar** si el texto PVK tiene caracteres fuera de los guiones inicial y final.

7. Marque la casilla Encrypted (Cifrado) y configure la contraseña creada al exportar el PVK en el paso 6.

8. Haga clic en **Aceptar**.

Add Known Internal Certificate



Name:

Certificate Data or, choose a file:

```
-----BEGIN CERTIFICATE-----
MIIDFTCCAmWgAwIBAgIJAKIemFK+L7iYMA0GCSqGSIb3DQEBCwUAMGQxCzAJBgNV
BAYTAIVTMQswCQYDVQQIDAJOQzEMMAoGA1UEBwwDUIRQM4wDAYDVQQKDAVDAxNj
bzEMMAoGA1UECwwDVEFDMRwwGgYDVQQDDDBNMYWJGUDYyMy5ydHBhYWEubmV0MB4X
DTE4MDUxNTE4MTM1MlloXDTI4MDUxMjE4MTM1MlowZDELMAkGA1UEBhMCVVMx
BgNVBAGMAK5DMQwwCgYDVQQHDANSVFAXDjAMBgNVBAoMBUNpc2NmMQwwCgYDVQQL
DANUQUxHDAaBgNVBAMME0xhYkZQNjIzLnJ0cGFhYS5uZXQwgwEIMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQMjtS5IUIFIZkZK/TSGtkOCmuivTK5kk1WzAy6
D7Gm/c69cXw/VfIPWnSBzhEkiRTyspmTMdyf/4TJvUmUH60h1O8/8dZeqJOzbjon
-----
```

Key or, choose a file:

Bag Attributes
localKeyID: C7 D7 99 F3 EE 41 5C 7B 36 91 40 04 F7 1D 22 4C 60 C2 3C 9C ← DELETE
Key Attributes: <no attributes="">

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQI5uV3MsiHZsICAggA
MBQGCCqGSIb3DQMHBABGVM1+xHLIASCBMjjJxkffXUNUcdB22smybvWotwbcRrt
xL0qjEStmwuyExVp+TWC3AyIJN1DE7/rRssjRAqsnSOxIvDGmg0dVsvnbqZwjFP
74POu/O2Vy99iFoVgW2q9DyXyL/h64TH9CZtwLKIOGOeEunNKpamDnpfyN8QC4DC
fXvNZ8jNG4HrEcFmnnij0EwJ0QT8Jn5gAUj+AIPMe32zPqwocCRNYrRXMVM9+Jwp
-----
```

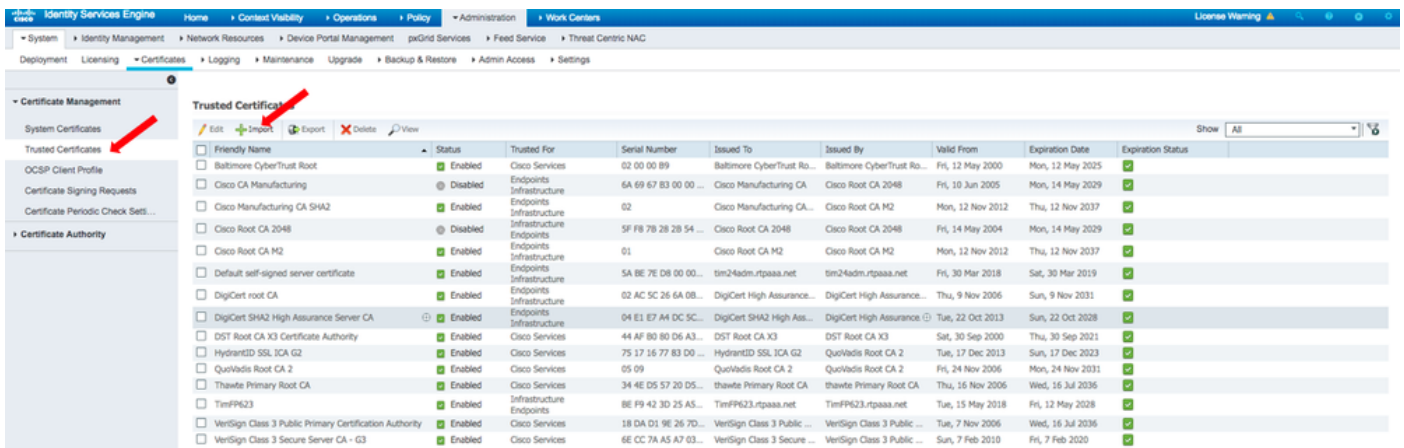
Encrypted, and the password is:

```
cfCJU2QGI4jT0SorN4u2Lk+S+Qd1s7Ii2wIQMWKPI2R9UGv1tyM6HTPCGoCo6VDI
acCICUAsecVrYY081GKTVVJ3bWgWfPtR3OH12YCA2whcCKcG50MByB4tjhHN036q
O/g=
-----END ENCRYPTED PRIVATE KEY-----
</no> ← DELETE
```

Encrypted, and the password is:

Paso 8. Importar el certificado de FMC a ISE

1. Acceda a la GUI de ISE y navegue hasta Administration > System > Certificates > Trusted Certificates.
2. Haga clic en Importar.



3. Haga clic en **Choose File** y seleccione el archivo FMC CER de su sistema local.

Opcional: Configure un nombre descriptivo.

4. Verifique **Trust** para la autenticación dentro de ISE.

Opcional: configure una descripción.

5. Haga clic en **Enviar** como se muestra en la imagen.

Import a new Certificate into the Certificate Store

* Certificate File TZfpcert.cer

Friendly Name

Trusted For: Trust for authentication within ISE

Trust for client authentication and Syslog

Trust for authentication of Cisco Services

Validate Certificate Extensions

Description

Paso 9. Configuración de la conexión pxGrid en FMC

1. Vaya a **System > Integration > Identity Sources** como se muestra en la imagen.



2. Haga clic en **ISE**.

3. Configure la dirección IP o el nombre de host del nodo pxGrid de ISE.

4. Seleccione el signo + situado a la derecha de pxGrid Server CA.

5. Asigne un nombre al archivo de CA del servidor y, a continuación, busque la CA de firma raíz de pxGrid recopilada en el paso 3 y haga clic en **Guardar**.

6. Seleccione el + a la derecha de MNT Server CA.

7. Asigne un nombre al archivo de la CA del servidor y, a continuación, busque el certificado de administrador recopilado en el paso 3 y haga clic en **Guardar**.

8. Seleccione el archivo **FMC CER** en la lista desplegable.

Identity Sources

Service Type: None Identity Services Engine User Agent

Primary Host Name/IP Address *

Secondary Host Name/IP Address

pxGrid Server CA *

MNT Server CA *

FMC Server Certificate *


ISE Network Filter ex. 10.89.31.0/24, 192.168.8.0/24, ...

* Required Field

9. Haga clic en **Test**.

10. Si la prueba se realiza correctamente, haga clic en **Aceptar**, luego **Guardar** en la parte superior derecha de la pantalla.

Status

 ISE connection status:
Primary host: Success

Additional Logs

Nota: Cuando se ejecutan dos nodos pxGrid de ISE, es normal que un host muestre Success y otro que muestre Failure, ya que pxGrid sólo se ejecuta activamente en un nodo de ISE a la vez. Depende de la configuración si el host primario puede mostrar Falla y el host secundario puede mostrar Éxito. Todo esto depende de qué nodo de ISE sea el nodo pxGrid activo.

Verificación

Verificación en ISE

1. Abra la GUI de ISE y navegue hasta **Administration > pxGrid Services**.

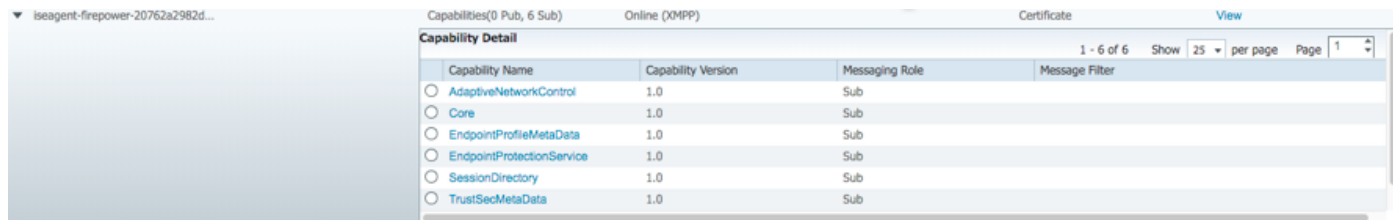
Si se realiza correctamente, se enumeran dos conexiones de firepower en la lista de clientes. Uno para el FMC real (iseagent-hostname-33bytes) y otro para el dispositivo de prueba (firesightisetest-hostname-33bytes).



La conexión iseagent-firepower muestra seis (6) suscripciones y aparece en línea.

La conexión firesightisetest-firepower muestra cero (0) subs y aparece sin conexión.

La vista expandida de iseagent-firepower client muestra las seis suscripciones.

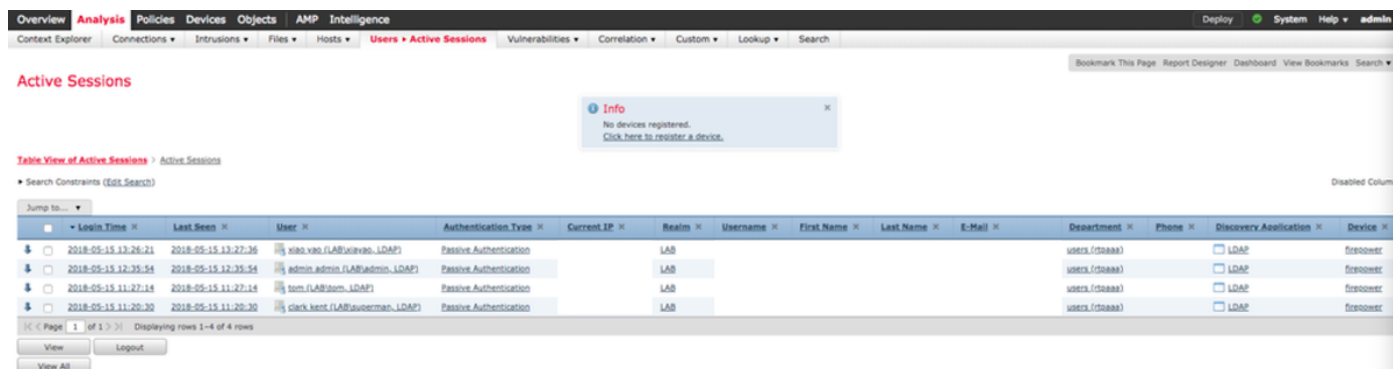


Nota: debido al error de Cisco [IDCSCvo75376](#) existe una limitación de nombre de host y falla la descarga masiva. El botón de prueba del FMC muestra un fallo de conectividad. Esto afecta a 2.3p6, 2.4p6 y 2.6. La recomendación actual es ejecutar el parche 2.3 5 o el parche 2.4 5 hasta que se libere un parche oficial.

Verificación en CSP

1. Abra la GUI de FMC y navegue hasta **Análisis > Usuarios > Sesiones activas**.

Todas las sesiones activas publicadas mediante la función Directorio de sesiones de ISE se muestran en la tabla Sesiones activas de FMC.



En el modo sudo de la CLI de FMC, la '**adi_cli session**' muestra la información de sesión de usuario enviada desde ISE a 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

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).