

Configuración de la autenticación VPN SSL a través de FTD, ISE, DUO y Active Directory

Contenido

[Introducción](#)

[Requirements](#)

[Componentes Utilizados](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configuraciones de FTD.](#)

[Integre un servidor RADIUS en Firepower Management Center \(FMC\)](#)

[Configure la VPN remota.](#)

[Configuraciones de ISE.](#)

[Integre DUO como servidor RADIUS externo.](#)

[Integre el FTD como un dispositivo de acceso a la red.](#)

[configuraciones DUO.](#)

[Instalación del proxy DUO.](#)

[Integre el proxy DUO con ISE y la nube DUO.](#)

[Integre DUO con Active Directory.](#)

[Exportar cuentas de usuario desde Active Directory \(AD\) a través de DUO Cloud.](#)

[Inscriba a los usuarios en la nube de Cisco DUO.](#)

[Procedimiento de validación de la configuración.](#)

[Problemas comunes.](#)

[Escenario de trabajo.](#)

[Error11353 No hay más servidores RADIUS externos; no se puede realizar la conmutación por error](#)

[Las sesiones RADIUS no aparecen en los registros en directo de ISE.](#)

[Resolución de otros problemas.](#)

Introducción

Este documento describe la integración de SSLVPN en Firepower Threat Defense mediante Cisco ISE y DUO Security para AAA.

Requirements

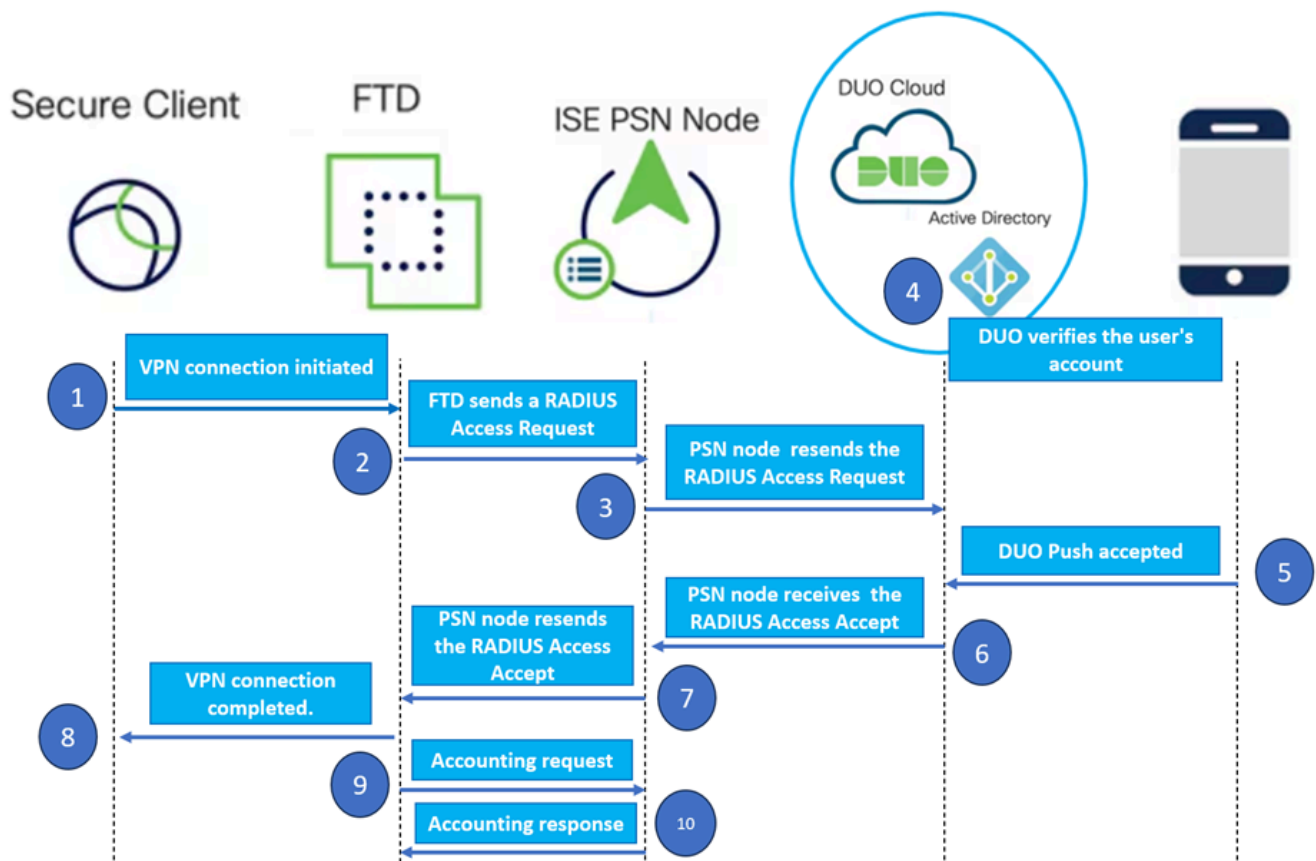
- ISE 3.0 o superior.
- FMC 7.0 o superior.
- FTD 7.0 o superior.
- Proxy de autenticación DUO.
- Licencias de ISE Essentials
- Licencia DUO Essentials.

Componentes Utilizados

- Parche 3 de ISE 3.2
- CSP 7.2.5
- FTD 7.2.5
- Proxy DUO 6.3.0
- Any Connect 4.10.08029

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.

Diagrama de la red



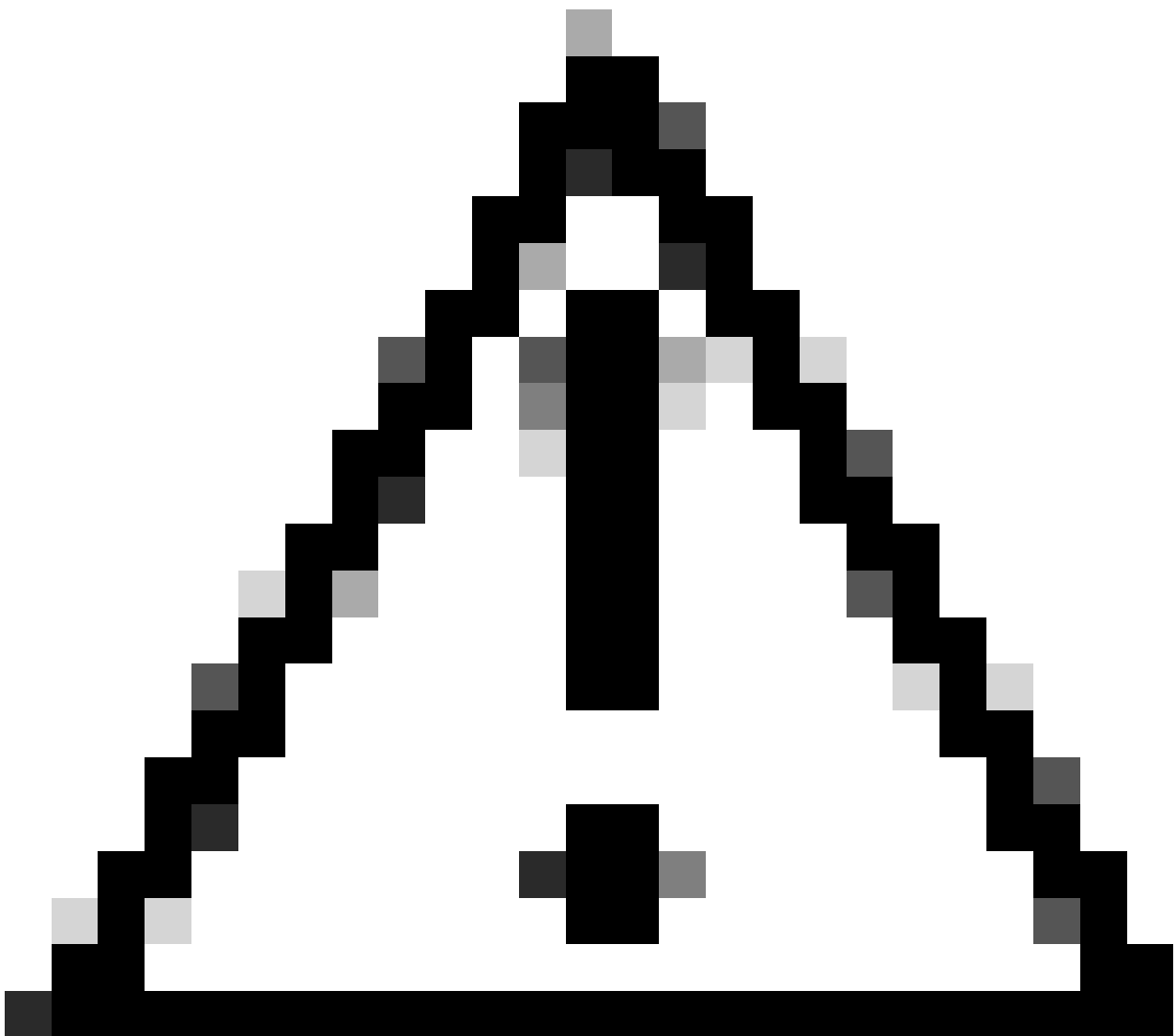
Topología.

En nuestra solución propuesta, Cisco ISE es un proxy de servidor RADIUS fundamental. En lugar de evaluar directamente las políticas de autenticación o autorización, ISE se configura para reenviar los paquetes RADIUS del FTD al proxy de autenticación DUO.

El proxy de autenticación DUO funciona como un intermediario dedicado dentro de este flujo de autenticación. Instalado en un servidor Windows, salva la brecha entre Cisco ISE y la nube DUO. La función principal del proxy es transmitir las solicitudes de autenticación (encapsuladas en paquetes RADIUS) a la nube DUO. En última instancia, la nube DUO permite o deniega el acceso

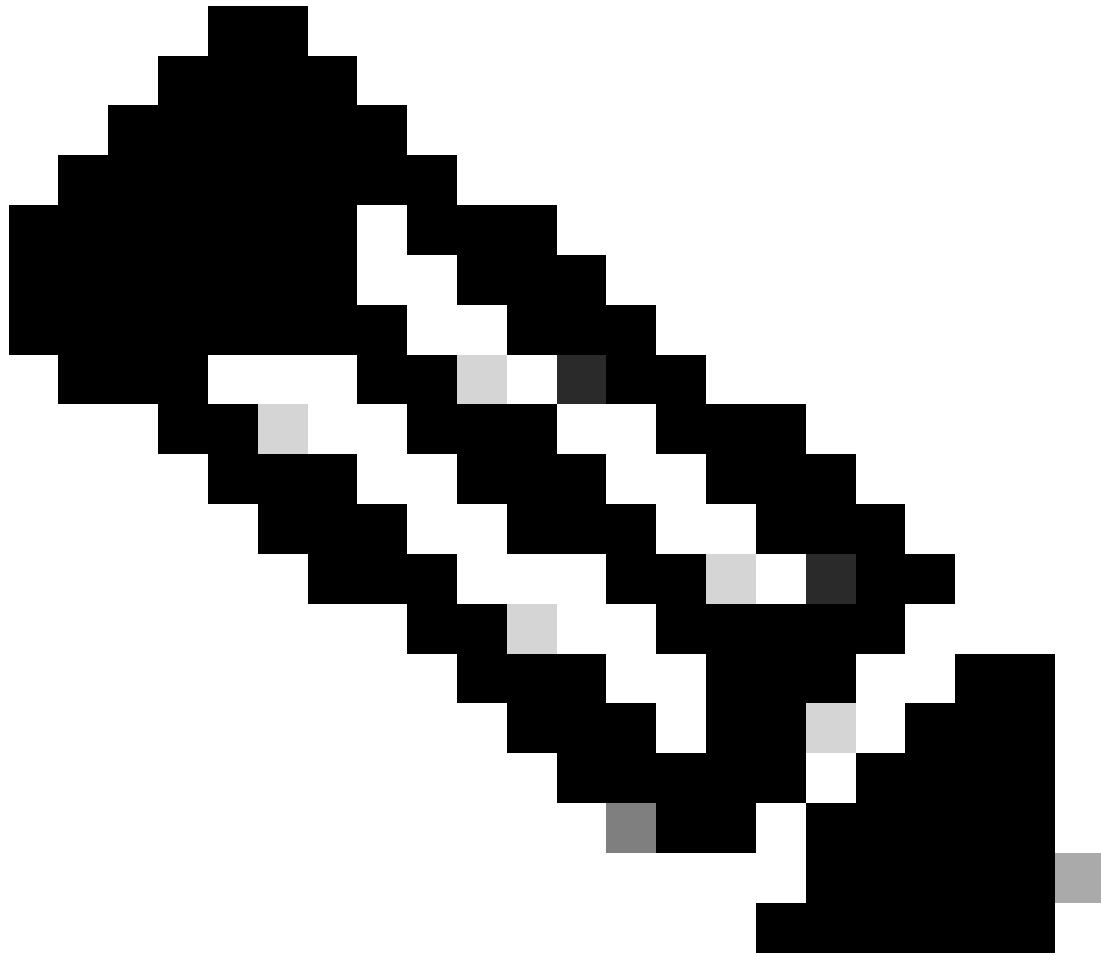
a la red en función de las configuraciones de autenticación de dos factores.

1. El usuario inicia el proceso de autenticación VPN introduciendo su nombre de usuario y contraseña únicos.
2. Firewall Threat Defence (FTD) envía la solicitud de autenticación a Cisco Identity Services Engine (ISE).
3. El nodo de servicios de directivas (PSN) reenvía la solicitud de autenticación al servidor proxy de autenticación DUO. Posteriormente, el Servidor de autenticación DUO valida las credenciales a través del servicio de nube DUO.
4. La nube DUO valida el nombre de usuario y la contraseña contra su base de datos sincronizada.



Precaución: la sincronización entre la nube DUO y Active Directory de la organización debe estar activa para mantener una base de datos de usuarios actualizada en la nube DUO.

5. Una vez que la autenticación es exitosa, la nube DUO inicia un DUO Push para los usuarios del dispositivo móvil registrado a través de una notificación push cifrada y segura. El usuario debe aprobar la inserción DUO para confirmar su identidad y continuar.
6. Una vez que el usuario aprueba la transferencia DUO, el servidor proxy de autenticación DUO envía una confirmación al PSN para indicar que el usuario ha aceptado la solicitud de autenticación.
7. El nodo PSN envía la confirmación al FTD para informar de que el usuario se ha autenticado.
8. El FTD recibe la confirmación de autenticación y establece la conexión VPN con el terminal con las medidas de seguridad adecuadas.
9. El FTD registra los detalles de la conexión VPN correcta y transmite de forma segura los datos de contabilidad al nodo ISE para fines de mantenimiento de registros y auditoría.
10. El nodo de ISE registra la información contable en sus livelogs, lo que garantiza que todos los registros se almacenan de forma segura y son accesibles para futuras auditorías o comprobaciones de conformidad.



Nota:

La configuración de esta guía utiliza los siguientes parámetros de red:

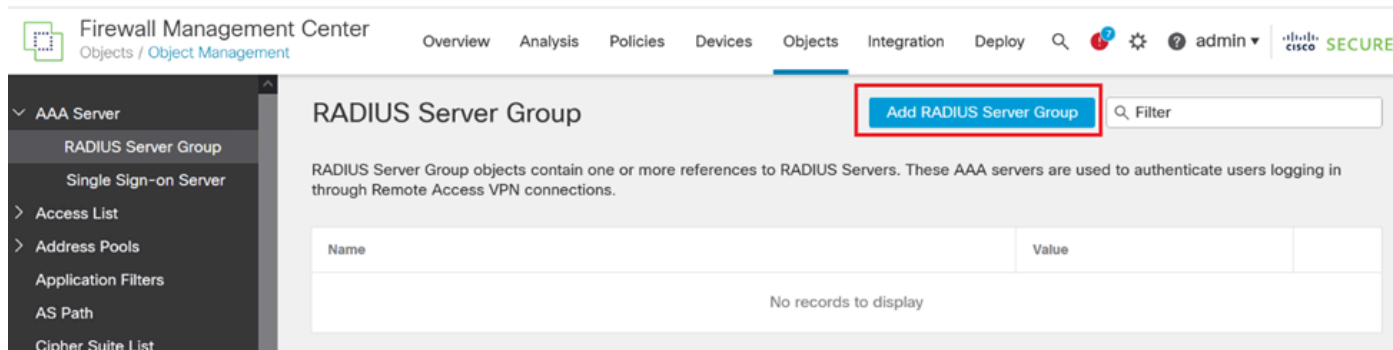
- IP de nodo del servidor de red principal (PNS): 10.4.23.21
- IP de Firepower Threat Defence (FTD) para VPN de mismo nivel: 10.4.23.53
- IP de proxy de autenticación DUO: 10.31.126.207
- Nombre de dominio: testlab.local

Configuraciones

Configuraciones de FTD.

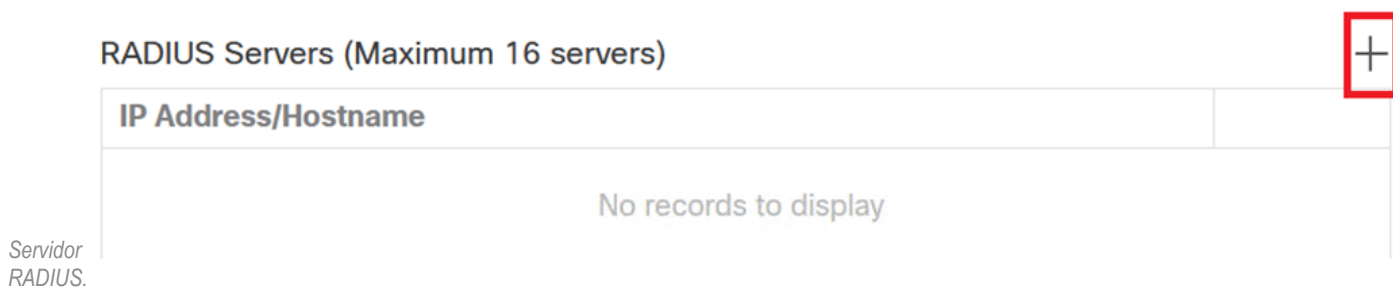
Integre un servidor RADIUS en Firepower Management Center (FMC)

1. Acceda al CSP iniciando el navegador web e introduciendo la dirección IP del CSP para abrir la interfaz gráfica de usuario (GUI).
2. Acceda al menú Objetos, seleccione Servidor AAA y continúe con la opción Grupo de Servidores RADIUS.
3. Haga clic en el botón Add RADIUS Server Group para crear un nuevo grupo para servidores RADIUS.



Grupo de servidores RADIUS.

4. Introduzca un nombre descriptivo para el nuevo grupo de servidores RADIUS AAA para garantizar una identificación clara en la infraestructura de red.
5. Proceda a agregar un nuevo servidor RADIUS seleccionando la opción apropiada dentro de la configuración de grupo.



6. Especifique la dirección IP de los servidores RADIUS e introduzca la clave secreta compartida.



Nota: Es fundamental asegurarse de que esta clave secreta se comparta de forma segura con el servidor ISE para establecer una conexión RADIUS correcta.

New RADIUS Server



IP Address/Hostname:*

10.4.23.21

Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port:* (1-65535)

1812

Key:*

●●●●●●●●

Confirm Key:*

●●●●●●●●

Accounting Port: (1-65535)

1813

Timeout: (1-300) Seconds

10

Connect using:

Routing Specific Interface



Cancel

Save

Nuevo servidor RADIUS.

7. Después de configurar los detalles del servidor RADIUS, haga clic en Guardar para conservar los valores para el grupo de servidores RADIUS.

Add RADIUS Server Group



Enable authorize only

Enable interim account update

Interval:* (1-120) hours

24

Enable dynamic authorization

Port:* (1024-65535)

1700

RADIUS Servers (Maximum 16 servers)



IP Address/Hostname

10.4.23.21



Cancel

Save

Detalles del grupo de servidores.

8. Para finalizar e implementar la configuración del servidor AAA en la red, acceda al menú Desplegar y seleccione Desplegar Todo para aplicar los parámetros.

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices Objects Integration **Deploy** admin **SECURE**

AAA Server

- RADIUS Server Group
- Single Sign-on Server
- Access List
- Address Pools
- Application Filters
- AS Path

RADIUS Server Group

RADIUS Server Group objects contain one or through Remote Access VPN connections.

Name	ISE
------	-----

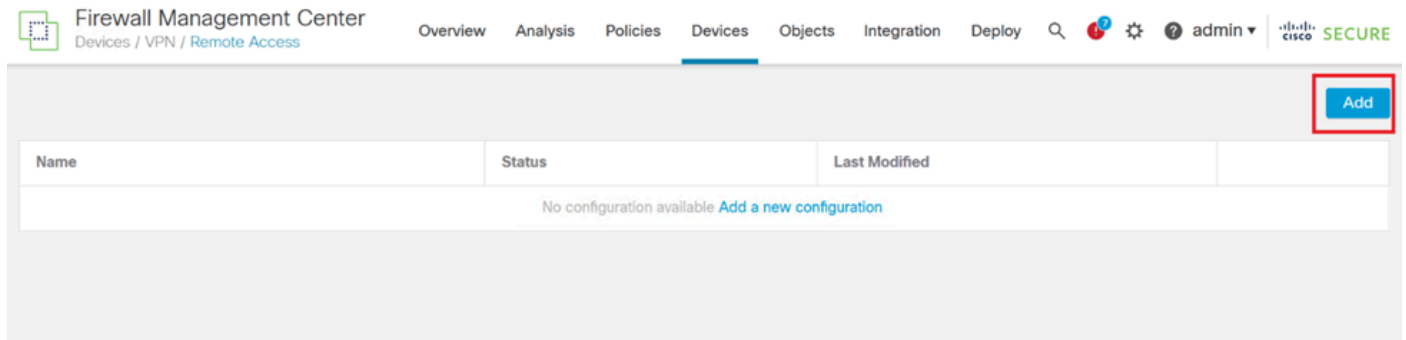
Search	Advanced Deploy	Deploy All
FTD_01	Ready for Deployment	

Implementación del Servidor AAA.

Configure la VPN remota.

1. Navegue hasta Devices > VPN > Remote Access en la GUI de FMC para comenzar el proceso de configuración de VPN.

2. Haga clic en el botón Add para crear un nuevo perfil de conexión VPN.

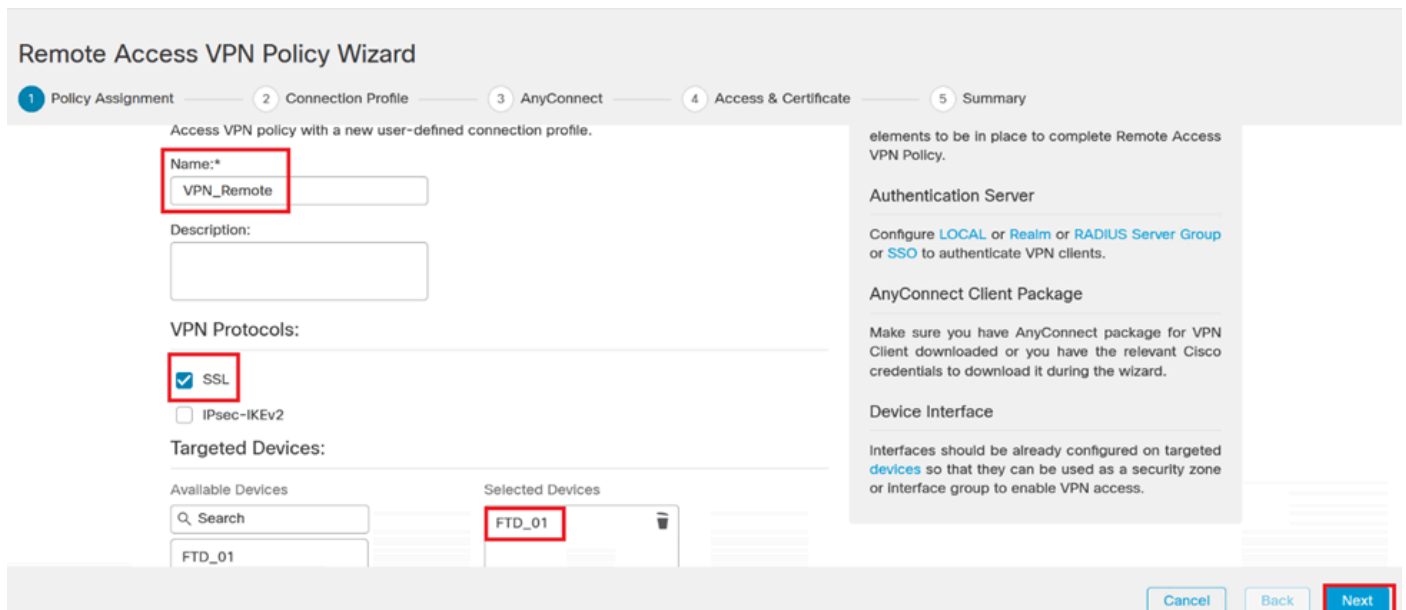


Perfil de conexión VPN.

3. Introduzca un nombre único y descriptivo para la VPN que le ayudará a identificarla en la configuración de red.

4. Seleccione la opción SSL para garantizar una conexión segura mediante el protocolo SSL VPN.

5. En la lista de dispositivos, seleccione el dispositivo FTD específico.



Configuración de VPN.

6. Configure el método AAA para utilizar el nodo PSN en los parámetros de autenticación.

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method: **AAA Only** ▼

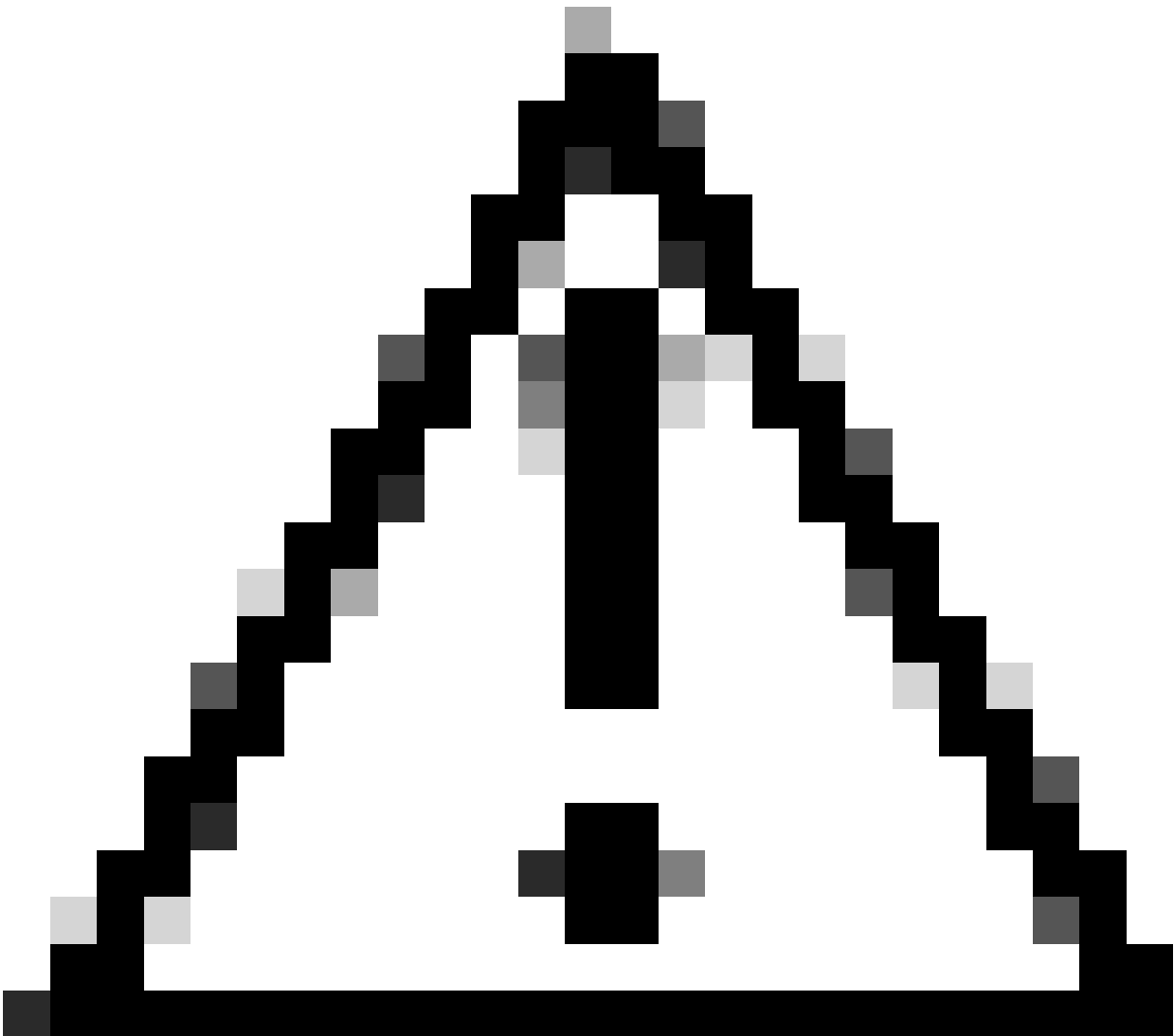
Authentication Server:* **ISE** ▼ +
(LOCAL or Realm or RADIUS)
 Fallback to LOCAL Authentication

Authorization Server: **Use same authentication server** ▼ +
(realm or RADIUS)

Accounting Server: **ISE** ▼ +
(RADIUS)

Perfil de conexión.

7. Configure la asignación de direcciones IP dinámicas para VPN.



Precaución: por ejemplo, se seleccionó el grupo de VPN DHCP.

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (Realm or RADIUS only) ⓘ

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools: 

IPv6 Address Pools: 

Grupo de direcciones IP.

8. Proceda a crear una nueva directiva de grupo.

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:* 

[Edit Group Policy](#)

Directiva de grupo.

9. En la configuración de Directiva de grupo, asegúrese de que el protocolo SSL está seleccionado.

Add Group Policy



Name:*

VPN_Remote_Policy

Description:

General

AnyConnect

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

VPN Tunnel Protocol:

Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

SSL

IPsec-IKEv2

Cancel

Save

Protocolos VPN.

10. Cree un nuevo grupo VPN o seleccione uno existente para definir el rango de direcciones IP disponibles para los clientes VPN.

Add Group Policy



Name:*

VPN_Remote_Policy

Description:

General

AnyConnect

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

IP Address Pools:



Name

IP Address Range

Cancel

Save

VPN de grupo.

11. Especifique los detalles del servidor DNS para la conexión VPN.

Add Group Policy



Name:*

VPN_Remote_Policy

Description:

General

AnyConnect

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

Primary DNS Server:

+

Secondary DNS Server:

+

Primary WINS Server:

+

Secondary WINS Server:

+

DHCP Network Scope:

+

Only network object with ipv4 address is allowed (Ex: 10.72.3.5)

Default Domain:

Cancel

Save

Configuración de DNS.



Advertencia: Tenga en cuenta que las funciones adicionales como el banner, la tunelización dividida, AnyConnect y las opciones avanzadas se consideran opcionales para esta configuración.

12. Después de configurar los detalles necesarios, haga clic en Next para continuar con la siguiente fase de la configuración.

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

Use AAA Server (Realm or RADIUS only) ●

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools:

IPv6 Address Pools:

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:*

[Edit Group Policy](#)

Cancel

Back

Next

Directiva de grupo.

13. Seleccione el paquete de AnyConnect adecuado para los usuarios de VPN. Si el paquete requerido no aparece en la lista, tiene la opción de agregar el paquete necesario en esta etapa.

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from [Cisco Software Download Center](#).

Select at least one AnyConnect Client image

[Show Re-order buttons](#)

<input type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input type="checkbox"/>	anyconnect-win-4.10.08029-we...	anyconnect-win-4.10.08029-webdeploy-k9...	Windows

Cancel

Back

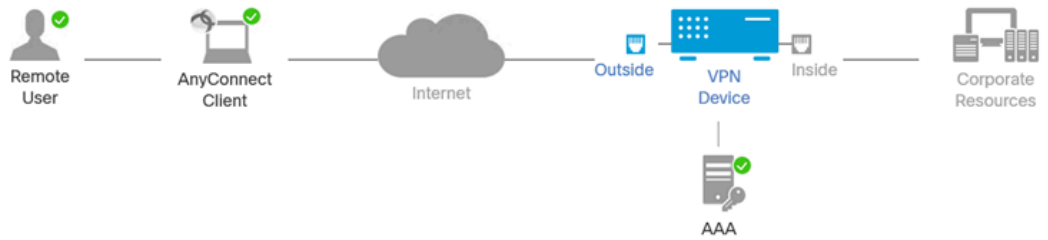
Next

Instalación del paquete.

14. Seleccione la interfaz de red en el dispositivo FTD en el que desea activar la función de remoto VPN.

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary



Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

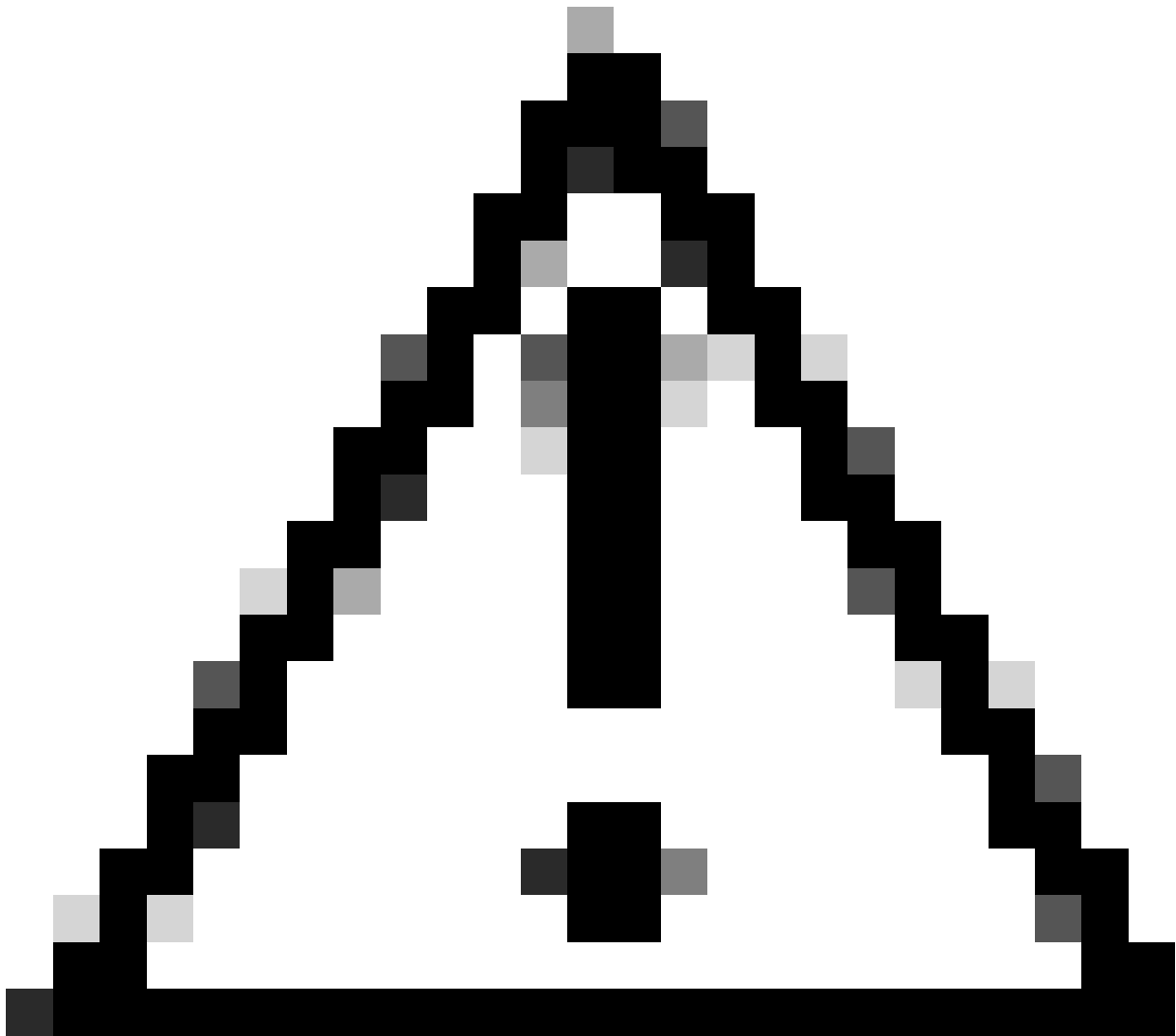
Interface group/Security Zone:* +

Enable DTLS on member interfaces

▲ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

Interfaz VPN

15. Establezca un proceso de inscripción de certificados seleccionando uno de los métodos disponibles para crear e instalar el certificado en el firewall, que es crucial para conexiones VPN seguras.



Precaución: por ejemplo, se ha seleccionado un certificado autofirmado en esta guía.

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:*

Certificado del dispositivo.

Add Cert Enrollment



Name*

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: SCEP

Enrollment URL:* Self Signed Certificate

Challenge Password: EST

Confirm Password: SCEP

Retry Period: Manual

Retry Count: 10 (Range 0-100)

Fingerprint:

PKCS12 File

Cancel Save

Inscripción de certificados.

16. Haga clic en Next una vez configurada la inscripción de certificados.

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

will access for VPN connections.

Interface group/Security Zone:* +

Enable DTLS on member interfaces

▲ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* +

Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

Resumen de acceso y servicios

17. Revise el resumen de todas las configuraciones para asegurarse de que son precisas y reflejan la configuración prevista.

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

Firepower Management Center will configure an RA VPN Policy with the following settings

Name:	VPN_Remote
Device Targets:	FTD_01
Connection Profile:	VPN_Remote
Connection Alias:	VPN_Remote
AAA:	
Authentication Method:	AAA Only
Authentication Server:	ISE (RADIUS)
Authorization Server:	ISE (RADIUS)
Accounting Server:	ISE
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	Pool_VPN
Address Pools (IPv6):	-
Group Policy:	VPN_Remote_Policy
AnyConnect Images:	anyconnect-win-4.10.08029-webdeploy-k9.pkg
Interface Objects:	Outside
Device Certificates:	Cert_Enrollment

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- Access Control Policy Update

An [Access Control](#) rule must be defined to allow VPN traffic on all targeted devices.
- NAT Exemption

If NAT is enabled on the targeted devices, you must define a [NAT Policy](#) to exempt VPN traffic.
- DNS Configuration

To resolve hostname specified in AAA Servers or CA Servers, configure DNS using [FlexConfig Policy](#) on the targeted devices.
- Port Configuration

SSL will be enabled on port 443. Please ensure that these ports are not used in [NAT Policy](#) or other services before deploying the configuration.
- ▲ Network Interface Configuration

Make sure to add interface from targeted

Resumen de la configuración VPN.

18. Para aplicar y activar la configuración de acceso remoto VPN, navegue hasta Deploy > Deploy All y ejecute la implementación en el dispositivo FTD seleccionado.

Implementando la configuración VPN.

Configuraciones de ISE.

Integre DUO como servidor RADIUS externo.

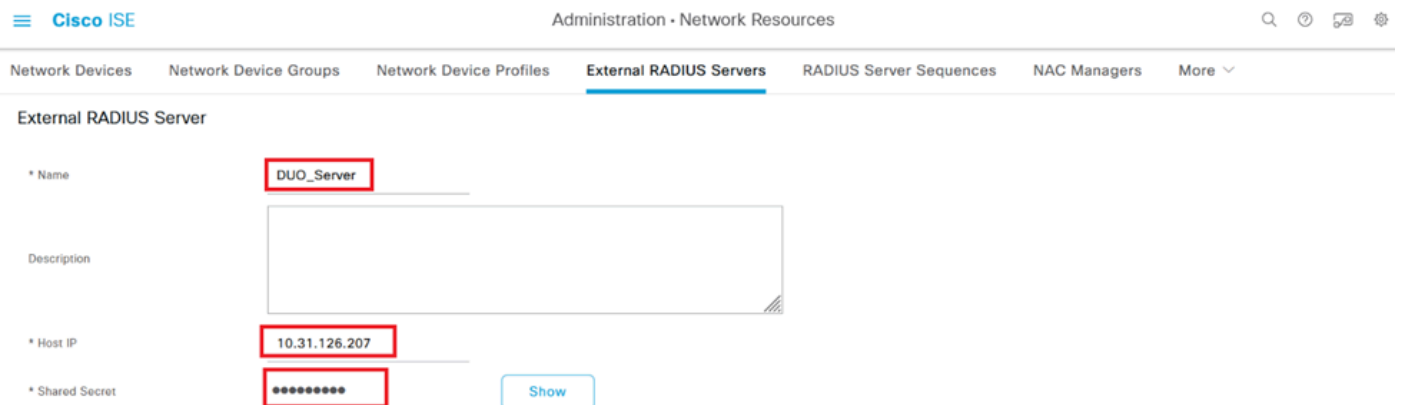
1. Vaya a Administration > Network Resources > External RADIUS Servers en la interfaz administrativa de Cisco ISE.
2. Haga clic en el botón Add para configurar un nuevo servidor RADIUS externo.

Servidores Radius externos

3. Introduzca un nombre para el servidor Proxy DUO.
4. Introduzca la dirección IP correcta para el servidor Proxy DUO para garantizar una comunicación adecuada entre ISE y el servidor DUO.
5. Establezca la clave secreta compartida.

Nota: Esta clave secreta compartida debe configurarse en el servidor Proxy DUO para establecer correctamente una conexión RADIUS.

6. Una vez introducidos correctamente todos los detalles, haga clic en **Enviar** para guardar la nueva configuración del servidor Proxy DUO.



The screenshot shows the Cisco ISE Administration interface for configuring an External RADIUS Server. The breadcrumb navigation is "Administration > Network Resources". The main menu includes "Network Devices", "Network Device Groups", "Network Device Profiles", "External RADIUS Servers" (which is selected), "RADIUS Server Sequences", "NAC Managers", and "More".

The "External RADIUS Server" configuration form contains the following fields:

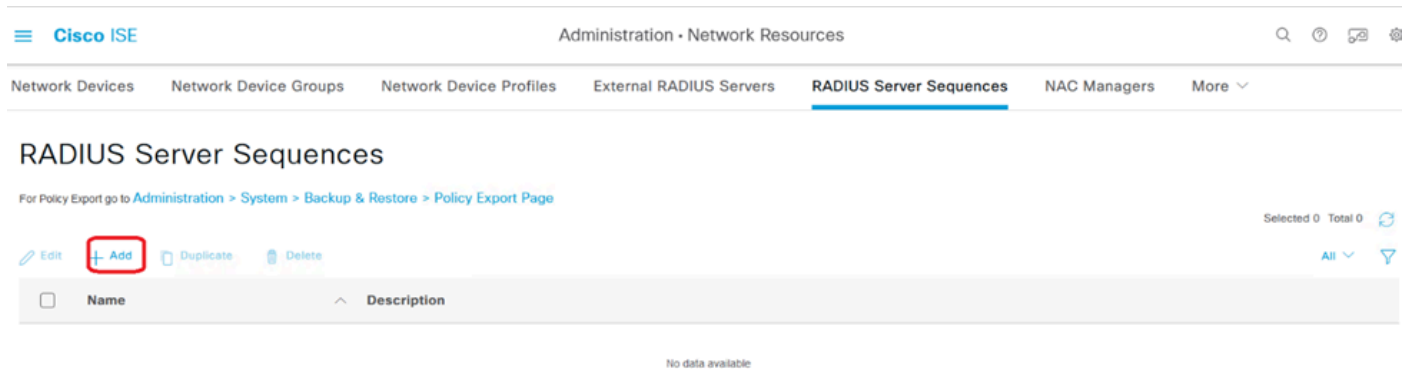
- Name:** DUO_Server
- Description:** (Empty text area)
- Host IP:** 10.31.126.207
- Shared Secret:** (Masked with asterisks)

A "Show" button is located next to the Shared Secret field.

Servidores RADIUS externos

7. Vaya a Administration > RADIUS Server Sequences.

8. Haga clic en Agregar para crear una nueva secuencia de servidor RADIUS.

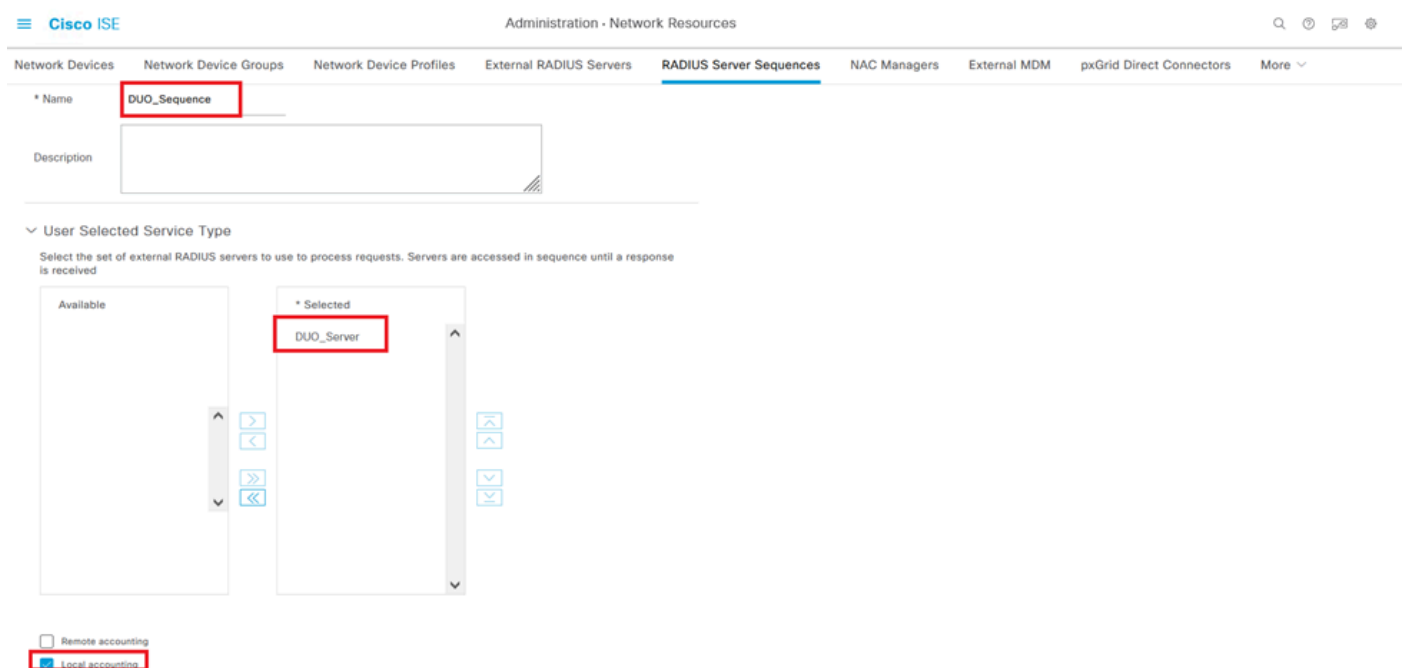


Secuencias de servidor RADIUS

9. Proporcione un nombre distinto para la secuencia del servidor RADIUS para facilitar la identificación.

10. Localice el servidor RADIUS DUO configurado anteriormente, denominado DUO_Server en esta guía, y muévelo a la lista seleccionada de la derecha para incluirlo en la secuencia.

11. Haga clic en Submit para finalizar y guardar la configuración de la secuencia del servidor RADIUS.



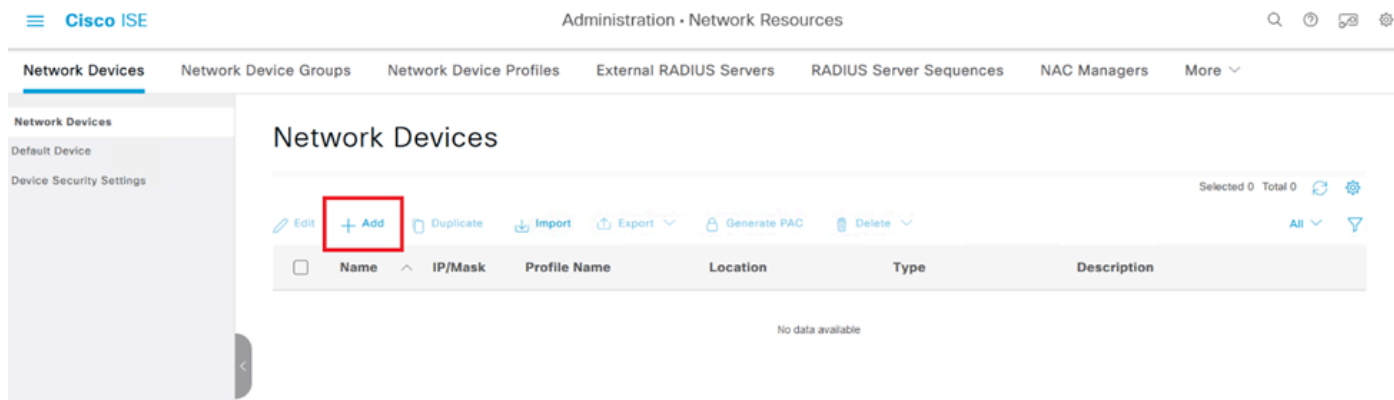
Configuración de las secuencias del servidor Radius.

Integre el FTD como un dispositivo de acceso a la red.

1. Vaya a la sección Administración de la interfaz del sistema y, desde allí, seleccione Recursos de red para acceder al área de configuración de los dispositivos de red.

2. Una vez en la sección Recursos de red, localice y haga clic en el botón Agregar para iniciar el

proceso de agregar un nuevo dispositivo de acceso a la red.



Dispositivos de acceso a la red.

3. En los campos proporcionados, introduzca el nombre del dispositivo de acceso a la red para identificar el dispositivo dentro de la red.
4. Especifique la dirección IP del dispositivo FTD (Firepower Threat Defence).
5. Introduzca la clave que se estableció anteriormente durante la configuración de FMC (FirePOWER Management Center). Esta clave es esencial para una comunicación segura entre dispositivos.
6. Complete el proceso haciendo clic en el botón Ejecutar.

[Network Devices List](#) > **FTD**

Network Devices

Name

FTD

Description

IP Address

* IP :

10.4.23.53

/

32



Adición de FTD como NAD.

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret

••••••••

Show

Use Second Shared Secret ⓘ

Second Shared Secret

Show

CoA Port **1700**

Set To Default

Parámetros de RADIUS

configuraciones DUO.

Instalación del proxy DUO.

Para acceder a la guía de descarga e instalación de proxy DUO, haga clic en el siguiente enlace:

<https://duo.com/docs/authproxy-reference>

Integre el proxy DUO con ISE y la nube DUO.

1. Inicie sesión en el sitio web de DUO Security en <https://duo.com/> con sus credenciales.
2. Navegue hasta la sección Aplicaciones y seleccione Proteger una aplicación para continuar.

Dashboard > Applications

Applications

Protect an Application

Manage your update to the new Universal Prompt experience, all in one place.

See My Progress Get More Information ⓘ

0 All Applications 0 End of Support

Export Search

3. Busque la opción "Cisco ISE RADIUS" en la lista y haga clic en Proteger para agregarla a sus aplicaciones.

Add an application that you'd like to protect with Duo two-factor authentication. You can start with a small "proof-of-concept" installation — it takes just a few minutes, and you're the only one that will see it, until you decide to add others. Documentation: [Getting Started](#) Choose an application below to get started.

Cisco ISE RADIUS

Application	Protection Type		
Cisco ISE Administrative Web Login	2FA with SSO hosted by Duo (Single Sign-On)	Documentation	Configure
Cisco ISE RADIUS	2FA	Documentation	Protect
Cisco RADIUS VPN	2FA	Documentation	Protect

opción RADIUS de ISE

4. Tras la adición exitosa, usted va a ver los detalles de la aplicación DUO. Desplácese hacia abajo y haga clic en Guardar.

5. Copie la clave de integración, la clave secreta y el nombre de host de la API proporcionados; estos son cruciales para los próximos pasos.

Application modified successfully.

Dashboard > Applications > Cisco ISE RADIUS

Cisco ISE RADIUS

[Authentication Log](#) | [Remove Application](#)

Follow the [Cisco ISE RADIUS instructions](#).

Details

[Reset Secret Key](#)

Integration key [Copy](#)

Secret key [Copy](#)

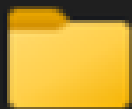
Don't write down your secret key or share it with anyone.

API hostname [Copy](#)

Detalles del servidor ISE

6. Inicie DUO Proxy Manager en el sistema para continuar con la configuración.

D



Duo Security

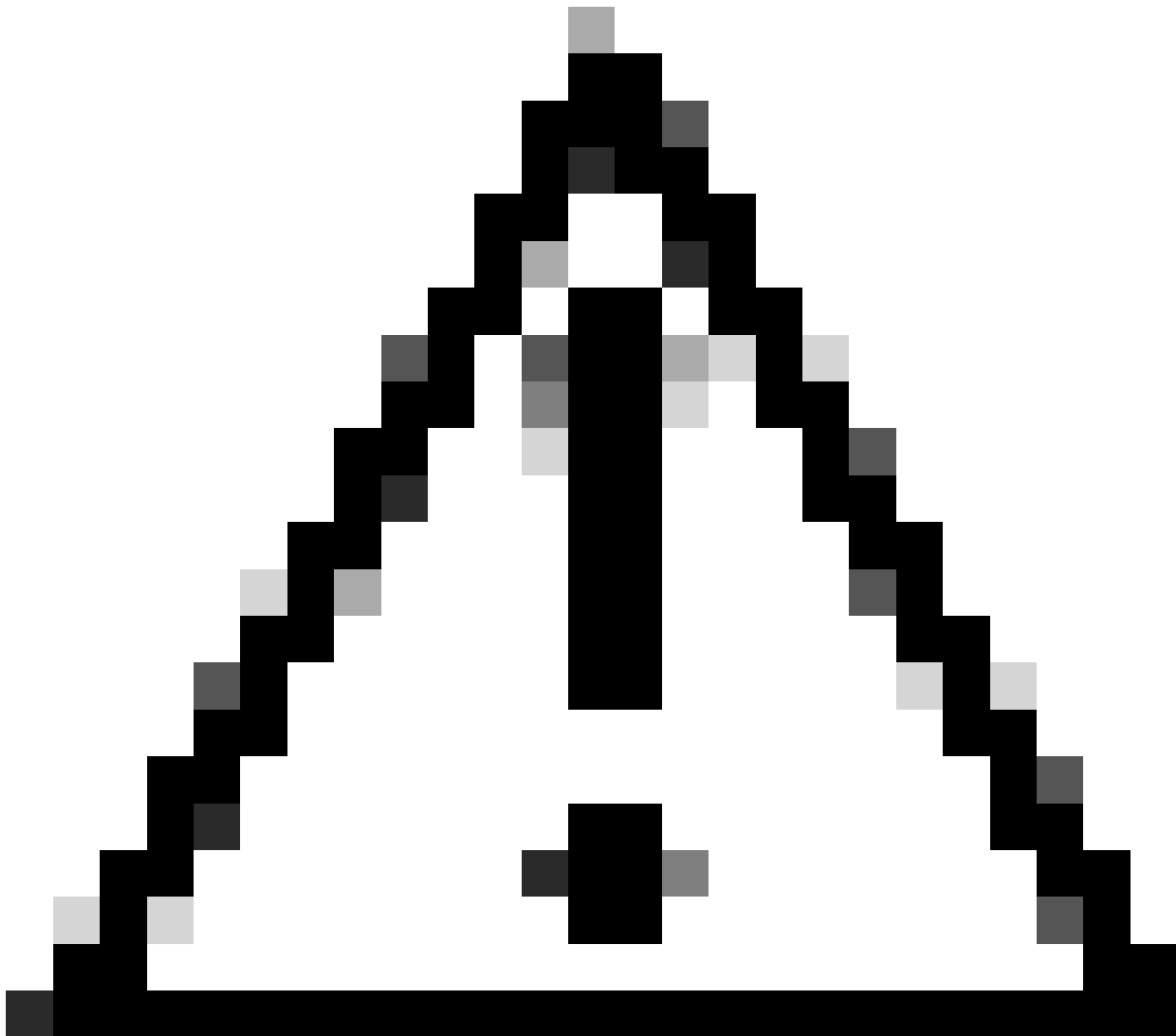


Duo Authentication Proxy Manager

Administrador de proxy DUO

7. (Opcional) Si el servidor proxy DUO requiere una configuración de proxy para conectarse a la nube DUO, introduzca los siguientes parámetros:

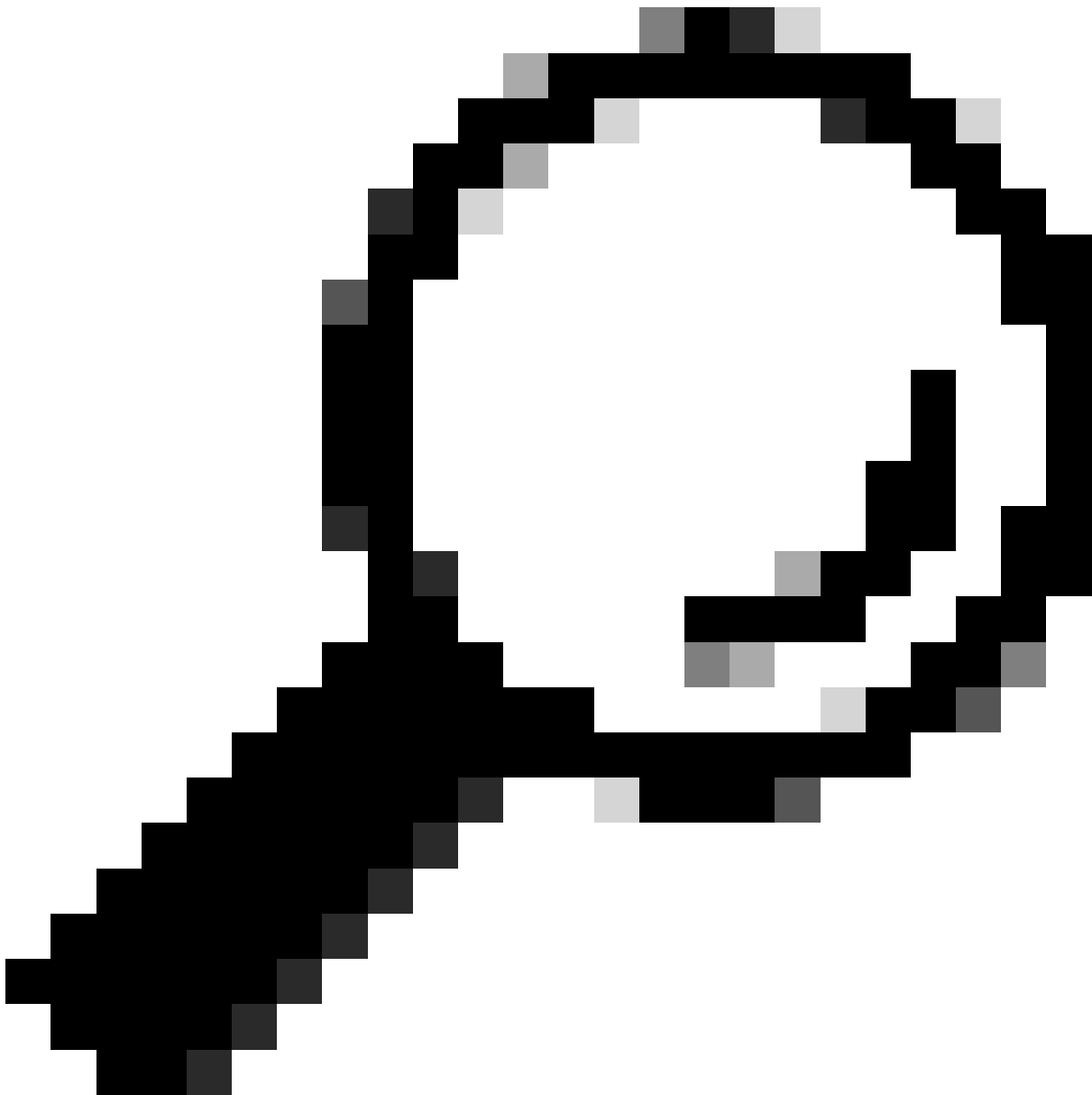
```
[main]
http_proxy_host=<Proxy IP Address or FQDN >
http_proxy_port=<port>
```



Precaución: asegúrese de reemplazar y con los detalles reales de su proxy.

8. Ahora, utilice la información que copió anteriormente para completar la configuración de integración.

```
[radius_server_auto]
ikey=<integration key>
skey=<secret key>
api_host=<API hostname>
radius_ip_1=<ISE IP address>
radius_secret_1=<secret key configured in the external RADIUS server section>
failmode=safe
port=1812
client=ad_client
```



Sugerencia: La línea `client=ad_client` es una indicación de que el proxy DUO se autentica mediante una cuenta de Active Directory. Asegúrese de que esta información es correcta para completar la sincronización con Active Directory.

Integre DUO con Active Directory.

1. Integre el proxy de autenticación DUO con su Active Directory.

```
[ad_client]
host=<AD IP Address>
service_account_username=<service_account_username>
service_account_password=<service_account_password>
search_dn=DC=<domain>,DC=<TLD>
```

2. Únase a su Active Directory con los servicios en la nube DUO. Inicie sesión en <https://duo.com/>.

3. Navegue hasta "Usuarios" y seleccione "Sincronización de directorios" para administrar la configuración de sincronización.

Dashboard > Users

Users

Directory Sync | Import Users | Bulk Enroll Users | Add User

Need to activate a replacement phone? [Learn more about Reactivating Duo Mobile](#).

0 Total Users | 0 Not Enrolled | 0 Inactive Users | 0 Trash | 0 Bypass Users | 0 Locked Out

Select (0) | ... | Export | Search

No users shown based on your search.

Sincronización de directorios

4. Haga clic en "Add New Sync" y elija "Active Directory" entre las opciones proporcionadas.

Dashboard > Users > Directory Sync

Directory Sync

Add New Sync

Directory Syncs | Connections

You don't have any directories yet.

Agregar nueva sincronización

5. Seleccione Agregar nueva conexión y haga clic en Continuar.

Agregando nuevo Active Directory

6. Copie la clave de integración generada, la clave secreta y el nombre de host de la API.

Detalles del proxy de autenticación

7. Vuelva a la configuración del proxy de autenticación DUO y configure la sección [cloud] con los nuevos parámetros que ha obtenido, así como las credenciales de la cuenta de servicio para un administrador de Active Directory:

```
[cloud]
ikey=<integration key>
skey=<secret key>
api_host=<API hostname>
service_account_username=<your domain>\<service_account_username>
service_account_password=<service_account_password>
```


8. Valide la configuración seleccionando la opción "validate" para asegurarse de que todos los parámetros son correctos.

```
1 [main]
2 http_proxy_host=cx[redacted]
3 http_proxy_port=3128
4
5 [radius_server_auto]
6 ikey=DIX[redacted]
7 skey=[redacted]uXWYwLM
8 api_host=a[redacted].duosecurity.com
9 radius_ip_1=10.4.23.21
10 radius_secret_1=po[redacted]
11 failmode=safe
12 port=1812
13 client=ad_client
14
15 [ad_client]
16 host=10.4.23.42
17 service_account_username=administrator
18 service_account_password=[redacted]
```

Configuración de Proxy DUO.

9. Después de la validación, guarde la configuración y reinicie el servicio de proxy de autenticación DUO para aplicar los cambios.

```
Running The Duo Authentication Proxy Connectivity Tool. This may take
several minutes...
[info] Testing section 'main' with configuration:
[info] {'http_proxy_host': 'cx[redacted]',
'http_proxy_port': '3128'}
[info] There are no configuration problems
[info]
[info] Testing section 'radius_server_auto' with configuration:
[info] {'api_host': '[redacted].duosecurity.com',
'client': 'ad_client',
'failmode': 'safe',
'http_proxy_host': '[redacted]',
'http_proxy_port': '3128',
'key': 'DIX[redacted]'}
```

Opción Reiniciar servicio.

10. Vuelva al panel de administración de DUO e introduzca la dirección IP del servidor de Active Directory junto con el DN base para la sincronización de usuarios.

Directory Configuration

Domain controller(s)

Hostname or IP address (1) *

10.4.23.42

Port (1) *

389

[+ Add Domain controller](#)

The port is typically 389 for cleartext LDAP or STARTTLS, and 636 for LDAPS.

Base DN *

DC=testlab,DC=local

Enter the full distinguished name (DN) of the directory location to search for users and groups. We recommend setting this to the directory root (example: DC=domain,DC=local). If specifying the DN of an OU or container, ensure it is **above both the users and groups to sync**.

Configuración del directorio.

11. Seleccione la opción Plain para configurar el sistema para la autenticación no NTLMv2.

Authentication type



Integrated

Performs Windows authentication from a domain-joined system.



NTLMv2

Performs Windows NTLMv2 authentication.



Plain

Performs username-password authentication.

Tipo de autenticación.

12. Guarde los nuevos parámetros para asegurarse de que se actualicen.

 Delete Connection

Save

Status

Not connected

Add Authentication Proxy



Configure Directory

Connected Directory Syncs

User Syncs

[AD Sync](#)

Guardar, opción

13. Utilice la función "probar conexión" para verificar que el servicio DUO Cloud pueda

comunicarse con su Active Directory.

Authentication Proxy

1. To set up this directory, you need to install the Duo Authentication Proxy software on a machine that Duo can connect to and that can connect to your LDAP server. [View instructions](#)
2. Configure your Authentication Proxy. Update the `ikey`, `skey`, and `api_host` entries in the `[cloud]` section of your configuration, or [download a pre-configured file](#).

Integration key [Copy](#)

Secret key [Copy](#)

Don't write down your secret key or share it with anyone.

[Reset Secret Key](#)

API hostname [Copy](#)

3. If you are using NTLM or plain authentication, update the `[cloud]` section of your configuration with the username and password for the LDAP account that has read access for your LDAP directory.

```
service_account_username=myusername
```

```
service_account_password=mypassword
```

4. Restart your Authentication Proxy.

5. [Test Connection](#).

Opción de conexión de prueba.

14. Confirme que el estado de Active Directory se muestre como "Conectado", lo que indica que la integración se ha realizado correctamente.

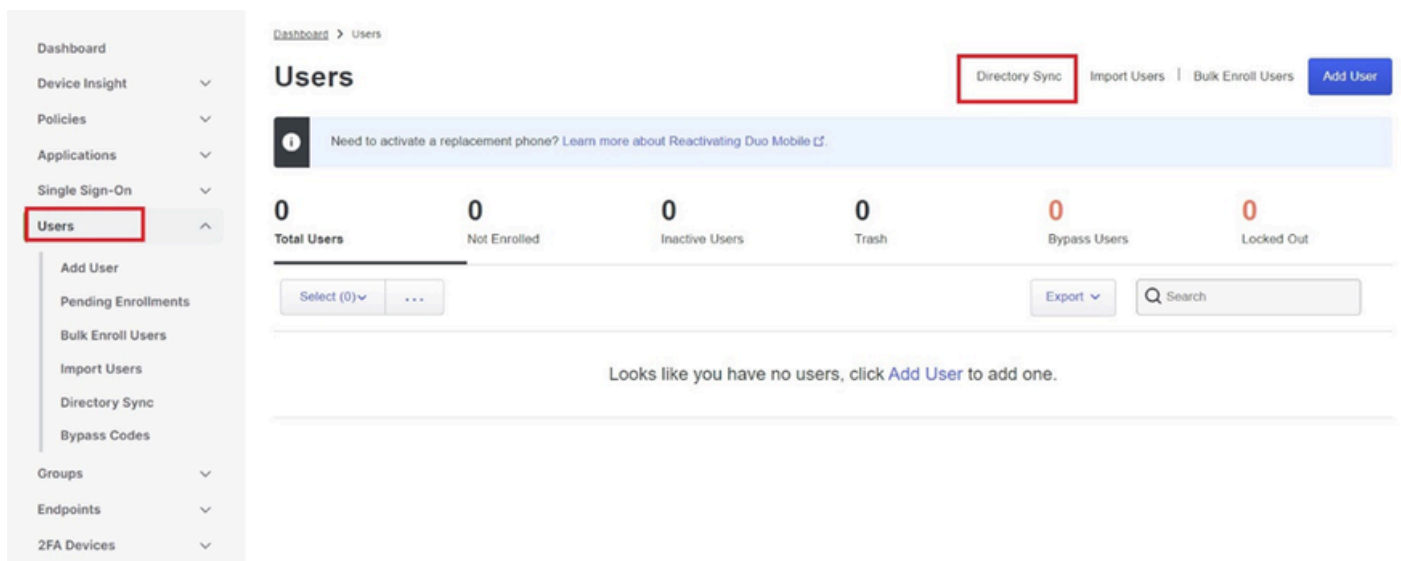
Status

Connected

Estado correcto.

Exportar cuentas de usuario desde Active Directory (AD) a través de DUO Cloud.

1. Navegue hasta Users > Directory Sync dentro del Duo Admin Panel para localizar la configuración relacionada con la sincronización de directorios con Active Directory.

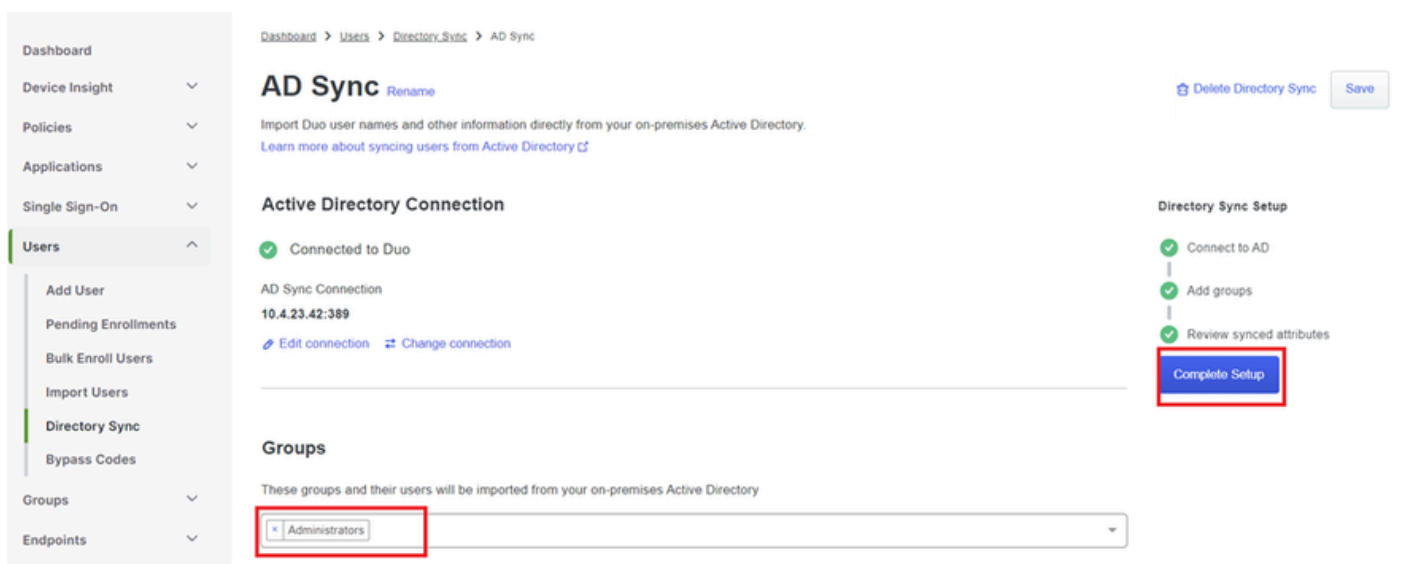


Lista de usuarios.

2. Seleccione la configuración de Active Directory que desea gestionar.

3. Dentro de los ajustes de configuración, identifique y elija los grupos específicos dentro de Active Directory que desea sincronizar con Duo Cloud. Considere la posibilidad de utilizar las opciones de filtrado para la selección.

4. Haga clic en Complete Setup.



Sincronización de AD.

5. Para iniciar la sincronización inmediatamente, haga clic en Sincronizar ahora. Esto exporta las cuentas de usuario de los grupos especificados en Active Directory a la nube Duo, lo que permite gestionarlas dentro del entorno de seguridad Duo.

AD Sync Rename

Delete Directory Sync No Changes

Import Duo user names and other information directly from your on-premises Active Directory. [Learn more about syncing users from Active Directory](#)

Sync Controls

Sync status

Scheduled to automatically synchronize every 12 hours, next around 2:00 AM UTC [Pause automatic syncs](#)

Sync Now

Troubleshooting

Active Directory Connection

Connected to Duo

AD Sync Connection

10.4.23.42:389

Edit connection

Change connection

Iniciando sincronización

Inscriba a los usuarios en la nube de Cisco DUO.

La inscripción de usuarios permite la verificación de la identidad a través de varios métodos, como el acceso al código, la inserción DUO, los códigos SMS y los tokens.

1. Navegue hasta la sección Usuarios en el panel de Cisco Cloud.
2. Localice y seleccione la cuenta del usuario que desea inscribir.

Dashboard > Users

Users

Directory Sync | Import Users | Bulk Enroll Users | Add User

Need to activate a replacement phone? [Learn more about Reactivating Duo Mobile](#)

1 Total Users | 1 Not Enrolled | 1 Inactive Users | 0 Trash | 0 Bypass Users | 0 Locked Out

Select (0) | ... | Export | Search

<input type="checkbox"/>	Username	Name	Email	Phones	Tokens	Status	Last Login
<input checked="" type="checkbox"/>	administrator		oteg [redacted]			Active	Never authenticated

1 total

Lista de cuentas de usuario.

3. Haga clic en el botón Send Enrollment Email para iniciar el proceso de inscripción.

administrator

Logs

Send Enrollment Email

Sync This User



This user has not enrolled yet. See our [enrollment documentation](#) to learn more about enrolling users.



This user was synced from the directory **AD Sync**. Some fields are read-only.

Username

administrator

Username aliases

[+ Add a username alias](#)

Users can have up to 8 aliases.

Optionally, you may choose to reserve using an alias number for a specific alias

(e.g., Username alias 1 should only be used for Employee ID).

Inscripción por correo electrónico.

4. Marque la bandeja de entrada de correo electrónico y abra la invitación de inscripción para completar el proceso de autenticación.

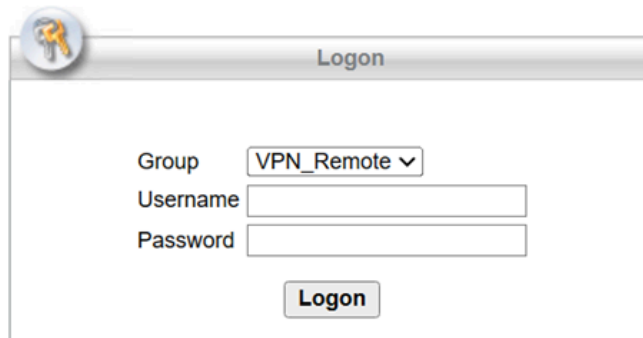
Para obtener más información sobre el proceso de inscripción, consulte estos recursos:

- Guía de inscripción universal: <https://guide.duo.com/universal-enrollment>
- Guía de inscripción tradicional: <https://guide.duo.com/traditional-enrollment>

Procedimiento de validación de la configuración.

Para asegurarse de que sus configuraciones son precisas y operativas, valide los siguientes pasos:

1. Inicie un navegador web e introduzca la dirección IP del dispositivo Firepower Threat Defence (FTD) para acceder a la interfaz VPN.



The screenshot shows a web browser window with a title bar that says "Logon". Inside the window, there is a form with the following elements:

- A "Group" label followed by a dropdown menu showing "VPN_Remote".
- A "Username" label followed by a text input field.
- A "Password" label followed by a text input field.
- A "Logon" button located below the input fields.

Inicio de sesión en VPN.

2. Introduzca su nombre de usuario y contraseña cuando se le solicite.



Nota: las credenciales forman parte de las cuentas de Active Directory.

3. Cuando reciba una notificación DUO Push, apruébela mediante el software DUO Mobile para continuar con el proceso de validación.

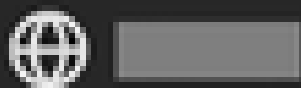


(1) Login request waiting.

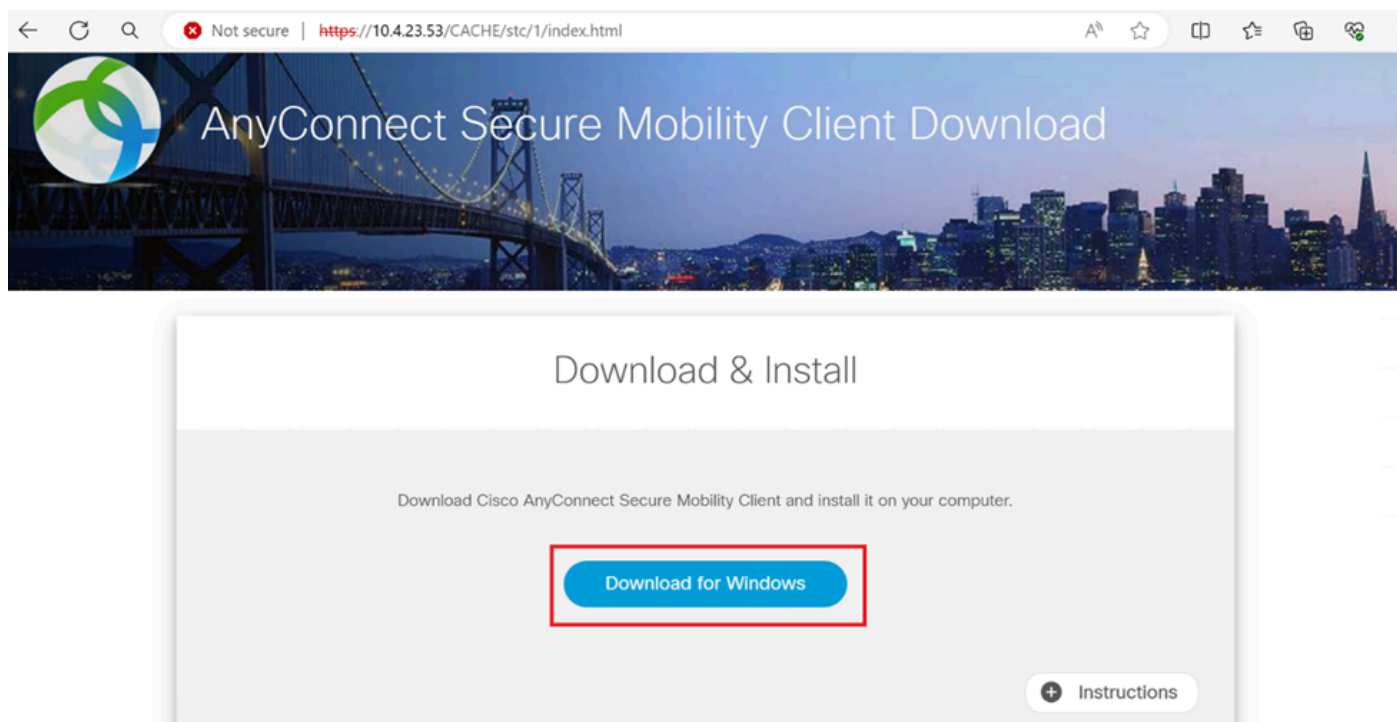
[Respond](#)



Are you logging in to Cisco ISE
RADIUS?

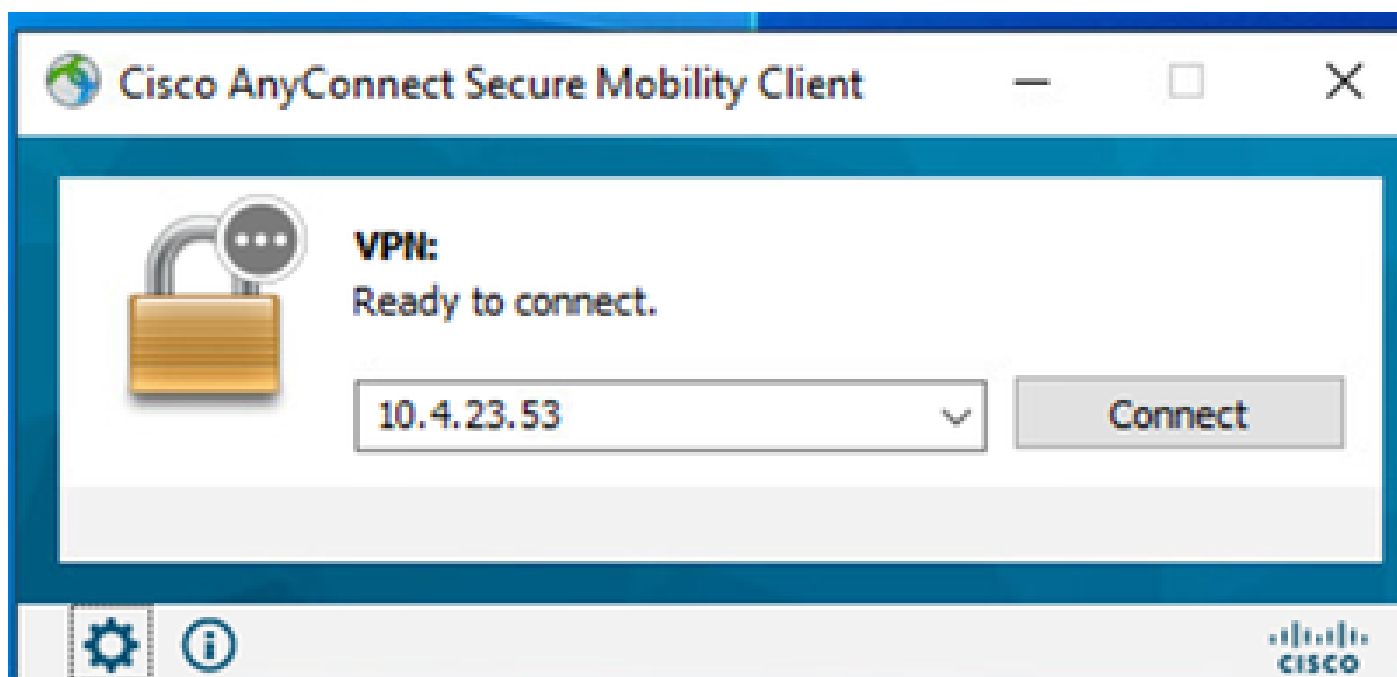


Localice y descargue el paquete Cisco AnyConnect VPN Client adecuado para los sistemas Windows.



Descargar e instalar.

5. Ejecute el archivo de instalación de AnyConnect descargado y continúe para completar las instrucciones proporcionadas por el instalador en su dispositivo Windows.
6. Abra el software Cisco AnyConnect Secure Mobility Client. Conéctese a la VPN introduciendo la dirección IP del dispositivo FTD.



Cualquier software de conexión.

7. Cuando se le solicite, introduzca sus credenciales de acceso a VPN y vuelva a autorizar la

notificación DUO Push para autenticar la conexión.



(1) Login request waiting.

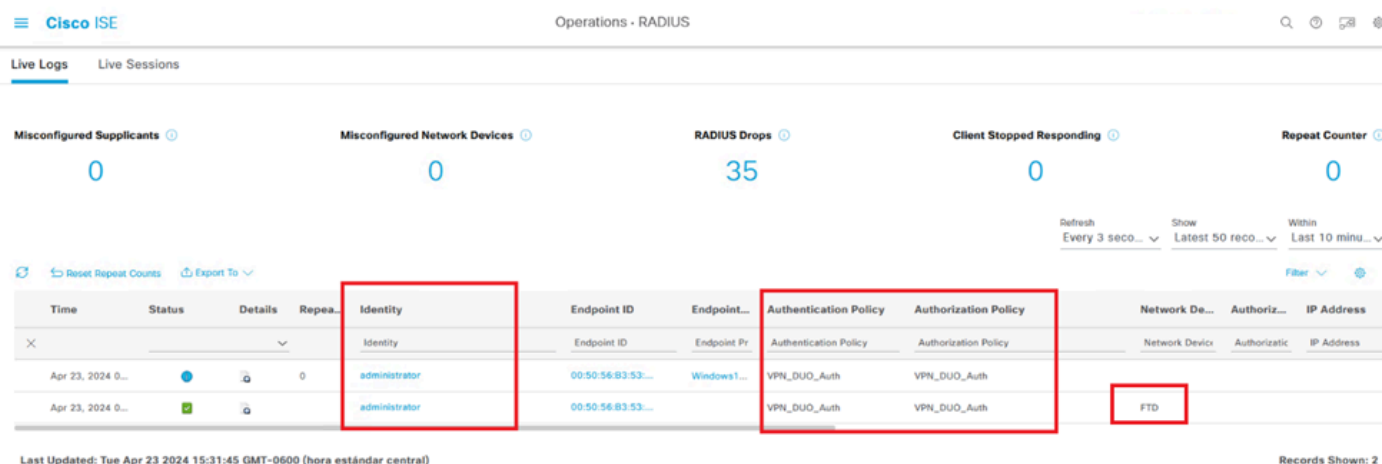
[Respond](#)



Are you logging in to Cisco ISE
RADIUS?

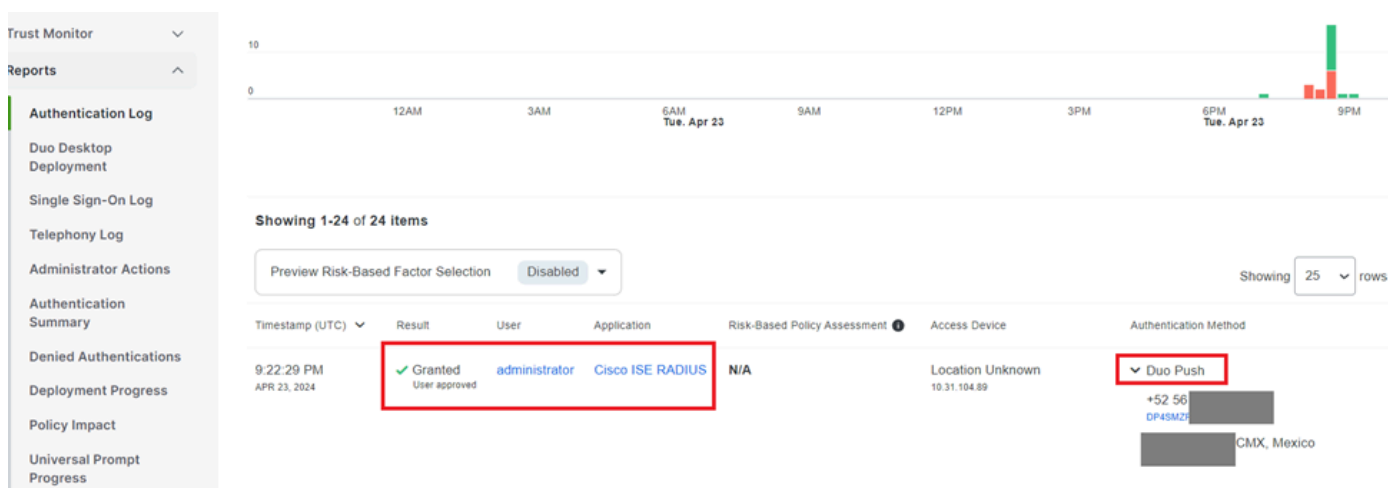


para supervisar la actividad en tiempo real y verificar que la conectividad es correcta; acceda a los registros en directo de Cisco Identity Services Engine (ISE).



Livelogs de ISE.

9. Vaya a Reports > Authentication logs para revisar los logs de autenticación en el panel de administración de DUO para confirmar verificaciones exitosas.



Registros de autenticación.

Problemas comunes.

Escenario de trabajo.

Antes de explorar errores específicos relacionados con esta integración, es crucial entender el escenario de trabajo general.

En los livelogs de ISE podemos confirmar que ISE reenvió los paquetes RADIUS al proxy DUO y, una vez que el usuario aceptó la transferencia DUO, se recibió la aceptación de acceso RADIUS del servidor proxy DUO.

Overview

Event	5200 Authentication succeeded
Username	administrator
Endpoint Id	00:50:56:B3:53:D6
Endpoint Profile	
Authentication Policy	VPN_DUO_Auth
Authorization Policy	VPN_DUO_Auth
Authorization Result	

Authentication Details

Source Timestamp	2024-04-24 20:03:33.142
Received Timestamp	2024-04-24 20:03:33.142
Policy Server	asc-ise32p3-1300
Event	5200 Authentication succeeded
Username	administrator
Endpoint Id	00:50:56:B3:53:D6
Calling Station Id	10.31.104.89
Audit Session Id	000000000002e000662965a9
Network Device	FTD

Steps

- 11001 Received RADIUS Access-Request
- 11017 RADIUS created a new session
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15048 Queried PIP - Network Access.NetworkDeviceName
- 11358 Received request for RADIUS server sequence.
- 11361 Valid incoming authentication request
- 11355 Start forwarding request to remote RADIUS server
- 11365 Modify attributes before sending request to external radius server
- 11100 RADIUS-Client about to send request - (port = 1812)
- 11101 RADIUS-Client received response (Step latency=5299 ms)
- 11357 Successfully forwarded request to current remote RADIUS server
- 11002 Returned RADIUS Access-Accept

Autenticación correcta.

CiscoAVPair

```
mdm-tlv=device-platform=win,  
mdm-tlv=device-mac=00-50-56-b3-53-d6,  
mdm-tlv=device-type=VMware, Inc. VMware7,1,  
mdm-tlv=device-platform-version=10.0.19045 ,  
mdm-tlv=device-public-mac=00-50-56-b3-53-d6,  
mdm-tlv=ac-user-agent=AnyConnect Windows 4.10.08029,  
mdm-tlv=device-uid-  
global=4CEBE2C21A8B81F490AC91086452CF3592593437,  
mdm-tlv=device-  
uid=3C5C68FF5FD3B6FA9D364DDB90E2B0BFA7E44B0EAAA  
CA383D5A8CE0964A799DD,  
audit-session-id=000000000002e000662965a9,  
ip:source-ip=10.31.104.89  
coa-push=true,  
proxy-flow=[10.4.23.53,10.4.23.21]
```

Result

Reply-Message Success. Logging you in...

Resultado correcto.

Una captura de paquetes del lado de ISE muestra la siguiente información:

Source	Destination	Protocol	Length	Info	
10.4.23.53	10.4.23.21	RADIUS	741	Access-Request id=138	→ The FTD sends the RADIUS request to ISE
10.4.23.21	10.31.126.207	RADIUS	883	Access-Request id=41	→ ISE resends the same RADIUS requests to the DUO Proxy
10.31.126.207	10.4.23.21	RADIUS	190	Access-Accept id=41	→ DUO Proxy sends the RADIUS accept (DUO push approved)
10.4.23.21	10.4.23.53	RADIUS	90	Access-Accept id=138	→ ISE resend the RADIUS accept to the FTD
10.4.23.53	10.4.23.21	RADIUS	739	Accounting-Request id=139	→ FTD sends the accounting for the current VPN connection
10.4.23.21	10.4.23.53	RADIUS	62	Accounting-Response id=139	→ ISE registered the accounting on its dashboard

Captura de paquetes ISE.

Error11368 Revise los registros en el servidor RADIUS externo para determinar el motivo exacto de la falla.

Event	5400 Authentication failed
Failure Reason	11368 Please review logs on the External RADIUS Server to determine the precise failure reason.
Resolution	Please review logs on the External RADIUS Server to determine the precise failure reason.
Root cause	Please review logs on the External RADIUS Server to determine the precise failure reason.

Error: 11368.

Resolución de problemas:

- Verifique que la clave secreta compartida RADIUS en ISE sea la misma que la clave configurada en el FMC.

1. Abra la GUI de ISE.
2. Administración > Recursos de red > Dispositivos de red.
3. Seleccione el servidor proxy DUO.
4. Junto al secreto compartido, haga clic en "Mostrar" para ver la clave en formato de texto sin formato.
5. Abra la GUI del FMC.
6. Objetos > Gestión de Objetos > Servidor AAA > Grupo de Servidores RADIUS.
7. Seleccione el servidor ISE.
8. Vuelva a introducir la clave secreta.

- Verifique la integración de Active Directory en DUO.

1. Abra el Administrador de proxy de autenticación DUO.

2. Confirme el usuario y la contraseña en la sección [ad_client].
3. Haga clic en Validar para confirmar que las credenciales actuales son correctas.

Error 1353 No hay más servidores RADIUS externos; no se puede realizar la conmutación por error

Event	5405 RADIUS Request dropped
Failure Reason	11353 No more external RADIUS servers; can't perform failover
Resolution	Verify the following: At least one of the remote RADIUS servers in the ISE proxy service is up and configured properly ; Shared secret specified in the ISE proxy service for every remote RADIUS server is same as the shared secret specified for the ISE server ; Port of every remote RADIUS server is properly specified in the ISE proxy service.
Root cause	Failover is not possible because no more external RADIUS servers are configured. Dropping the request.

Error: 11353.

Resolución de problemas:

- Compruebe que la clave secreta compartida RADIUS en ISE es la misma que la clave configurada en el servidor proxy DUO.

1. Abra la GUI de ISE.
2. Administración > Recursos de red > Dispositivos de red.
3. Seleccione el servidor proxy DUO.
4. Junto al secreto compartido, haga clic en "Mostrar" para ver la clave en formato de texto sin formato.
5. Abra el Administrador de proxy de autenticación DUO.
6. Verifique la sección [radius_server_auto] y compare la clave secreta compartida.

Las sesiones RADIUS no aparecen en los registros en directo de ISE.

Resolución de problemas:

- Verifique la configuración DUO.

1. Abra el Administrador de proxy de autenticación DUO.
2. Verifique la dirección IP de ISE en la sección [radius_server_auto]

- Verifique la configuración de FMC.

1. Abra la GUI del FMC.

2. Vaya a Objetos > Administración de Objetos > Servidor AAA > Grupo de Servidores RADIUS.

3. Seleccione el servidor ISE.

4. Compruebe la dirección IP de ISE.

- Realice una captura de paquetes en ISE para confirmar la recepción de los paquetes RADIUS.

1. Vaya a Operaciones > Troubleshooting > Herramientas de diagnóstico > TCP Dump

Resolución de otros problemas.

- Habilite los siguientes componentes en el PSN como debug:

Policy-engine

Port-JNI

Runtime-AAA

Para obtener más información sobre la resolución de problemas en el Administrador de proxy de autenticación DUO, consulte el siguiente enlace:

https://help.duo.com/s/article/1126?language=en_US

Plantilla DUO.

Puede utilizar la siguiente plantilla para completar la configuración en el servidor proxy DUO.

```
[main] <--- OPTIONAL
http_proxy_host=<Proxy IP address or FQDN>
http_proxy_port=<Proxy port>
[radius_server_auto]
ikey=xxxxxxxxxxxxxxxx
skey=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=xxxxxxxxxxxxxxxxxxxxxxxx
radius_ip_1=<PSN IP Address>
radius_secret_1=xxxxxxxx
failmode=safe
port=1812
client=ad_client
```

```
[ad_client]
host=<AD IP Address>
service_account_username=xxxxxxx
service_account_password=xxxxxxx
```

search_dn=DC=xxxxxx,DC=xxxx

[cloud]

ikey=xxxxxxxxxxxxxxxxxxxx

skey=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

api_host=xxxxxxxxxxxxxxxxxxxx

service_account_username=<your domain\username>

service_account_password=xxxxxxxxxxxx

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).