Configuración de la integración Duo con Active Directory e ISE para la autenticación de dos factores en clientes VPN de acceso remoto/Anyconnect

Contenido

Introducción

Este documento describe la integración de inserción Duo con AD e ISE como la autenticación de dos factores para los clientes de AnyConnect conectados a ASA.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de VPN de RA en ASA
- Configuración RADIUS en ASA
- ISE
- Directorio activo
- Aplicaciones Duo

Componentes Utilizados

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

- Microsoft 2016 Server
- ASA 9.14(3)18

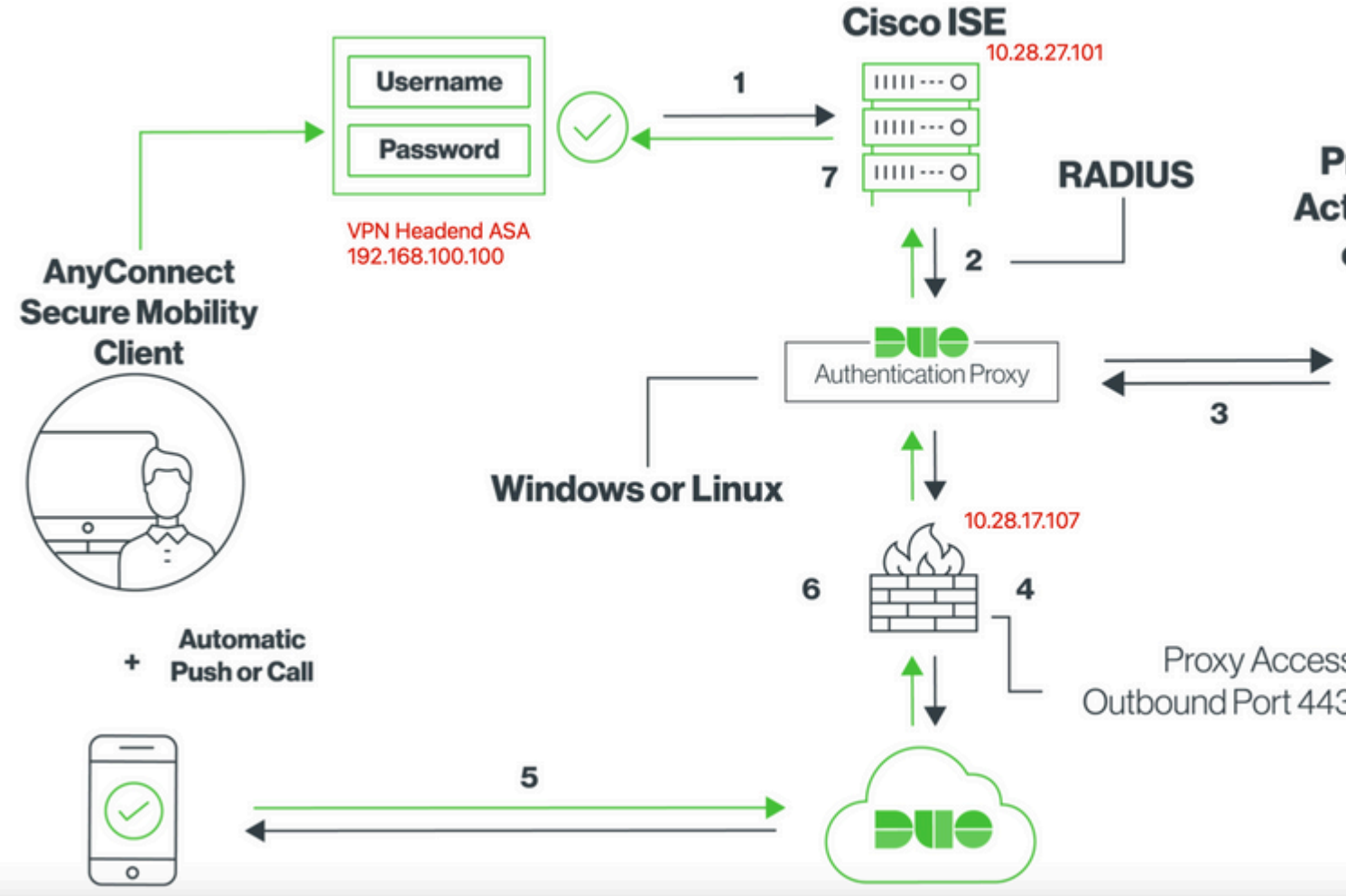
- Servidor ISE 3.0
- Servidor Duo
- Administrador de proxy de autenticación Duo

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.

Antecedentes

Este documento describe cómo configurar la integración de inserción Duo con Active Directory (AD) y Cisco Identity Service Engine (ISE) como autenticación de dos factores para los clientes de AnyConnect que se conectan a Cisco Adaptive Security Appliance (ASA).

Diagrama y escenario de la red



Proceso de comunicación

https://duo.com/docs/ciscoise-radius

1. Autenticación principal iniciada a Cisco ISE
2. Cisco ISE envía una solicitud de autenticación al proxy de autenticación dúo
3. La autenticación principal utiliza Active Directory o RADIUS
4. Conexión del proxy de autenticación dúo establecida para seguridad dúo a través del puerto TCP 443

5. Autenticación secundaria a través del servicio Duo Security
6. El proxy de autenticación dúo recibe respuesta de autenticación
7. Acceso a Cisco ISE concedido

Cuentas de usuario:

- Administrador de Active Directory: se utiliza como cuenta de directorio para permitir que el proxy de autenticación Duo se enlace al servidor de Active Directory para la autenticación principal.
- usuario de prueba de Active Directory
- Usuario de prueba Duo para autenticación secundaria

Configuraciones de Active Directory

El servidor de Windows está preconfigurado con los servicios de dominio de Active Directory.

> **Nota**: Si RADIUS Duo Auth Proxy Manager se ejecuta en el mismo equipo host de Active Directory, los roles del servidor de directivas de redes (NPS) deben desinstalarse/eliminarse; si se ejecutan ambos servicios RADIUS, pueden entrar en conflicto y afectar al rendimiento.

Para lograr la configuración de AD para la autenticación y la identidad de usuario en usuarios de VPN de acceso remoto, se requieren algunos valores.

Todos estos detalles deben crearse o recopilarse en Microsoft Server antes de poder realizar la configuración en el servidor proxy ASA y Duo Auth.

Los valores principales son:

- Nombre de dominio. Este es el nombre de dominio del servidor. En esta guía de configuración, agarciam.cisco es el nombre de dominio.

- Dirección IP/FQDN del servidor. La dirección IP o FQDN utilizado para alcanzar el servidor de Microsoft. Si se utiliza un FQDN, se debe configurar un servidor DNS dentro de ASA y el proxy de Duo Auth para resolver el FQDN.

En esta guía de configuración, este valor es agarciam.cisco (que se resuelve en 10.28.17.107).

- Puerto del servidor. El puerto utilizado por el servicio LDAP. De forma predeterminada, LDAP y STARTTLS utilizan el puerto TCP 389 para LDAP, y LDAP sobre SSL (LDAP) utiliza el puerto TCP 636.

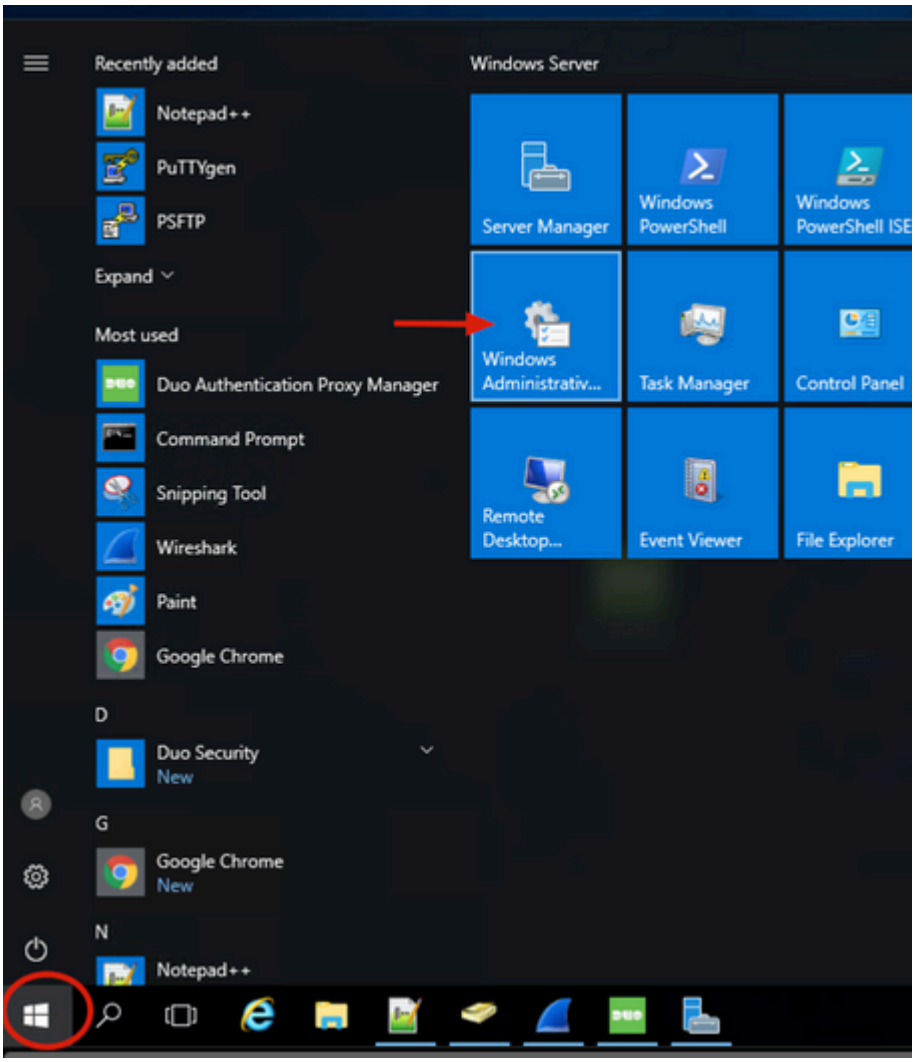
- CA raíz. Si se utiliza LDAPS o STARTTLS, se requiere la CA raíz utilizada para firmar el certificado SSL utilizado por LDAPS.

- Nombre de usuario y contraseña del directorio. Esta es la cuenta utilizada por el servidor proxy Duo Auth para enlazar al servidor LDAP y autenticar usuarios y buscar usuarios y grupos.

- Nombre distinguido (DN) de base y grupo. El DN base es el punto de partida para el proxy de Duo Auth e indica al directorio activo que comience la búsqueda y autentique a los usuarios.

En esta guía de configuración, el dominio raíz agarciam.cisco se utiliza como DN base y el DN de grupo es Duo-USERS.

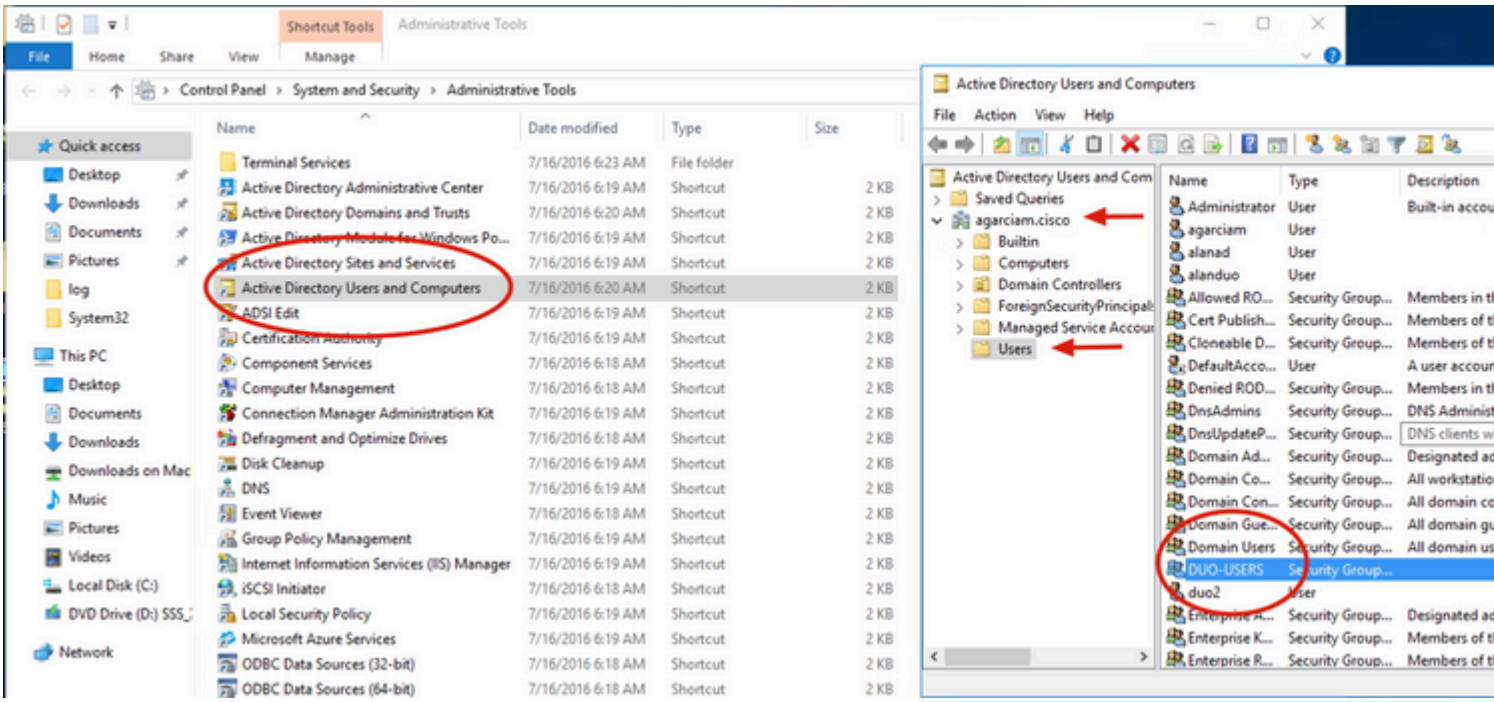
1. Para agregar un nuevo usuario Duo, en Windows Server, navegue hasta el icono **Windows** en la parte inferior izquierda y haga clic en **Windows Administrative tools**, como se muestra en la imagen.



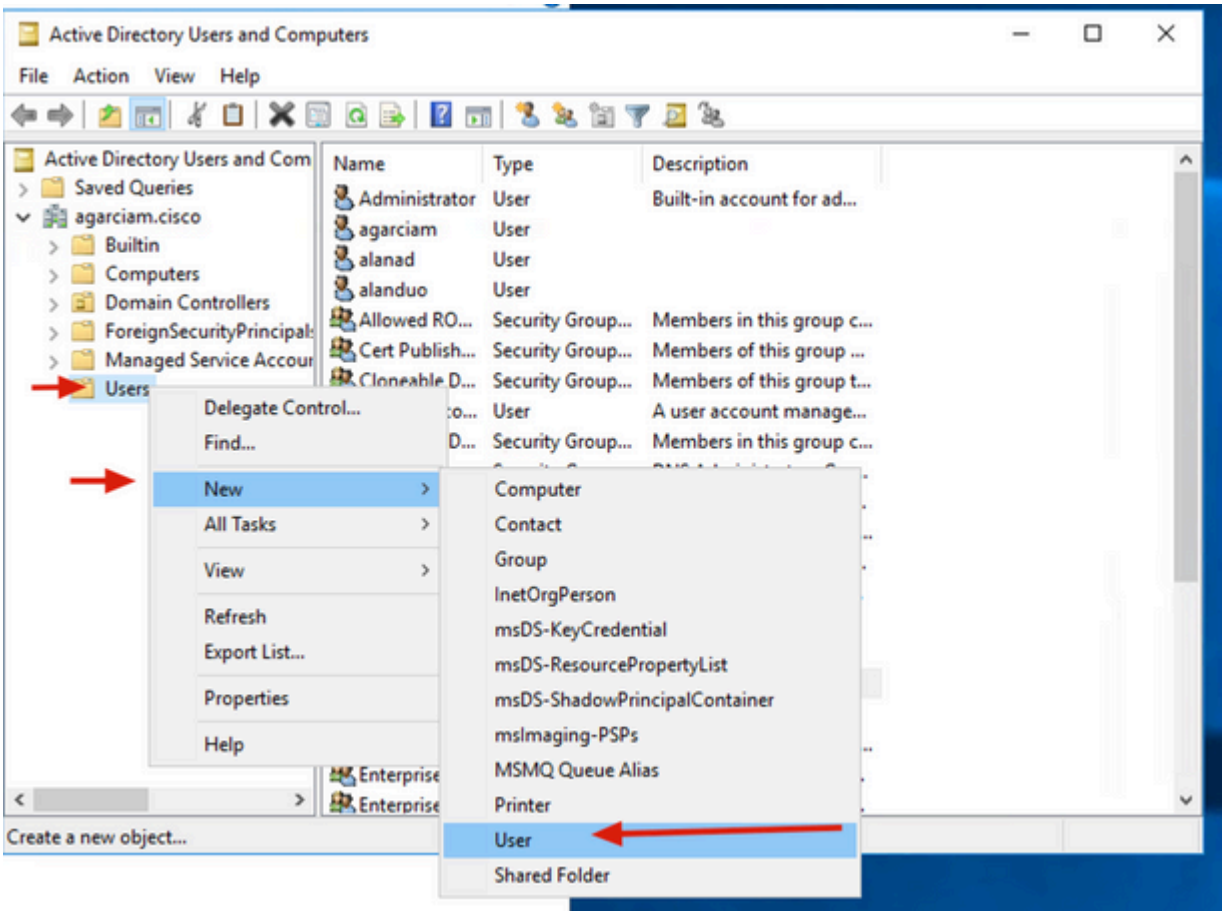
2. En la ventana Herramientas administrativas de Windows, navegue hasta **Usuarios y equipos de Active Directory**.

En el panel Usuarios y equipos de Active Directory, expanda la opción de dominio y desplácese a la carpeta **Usuarios**.

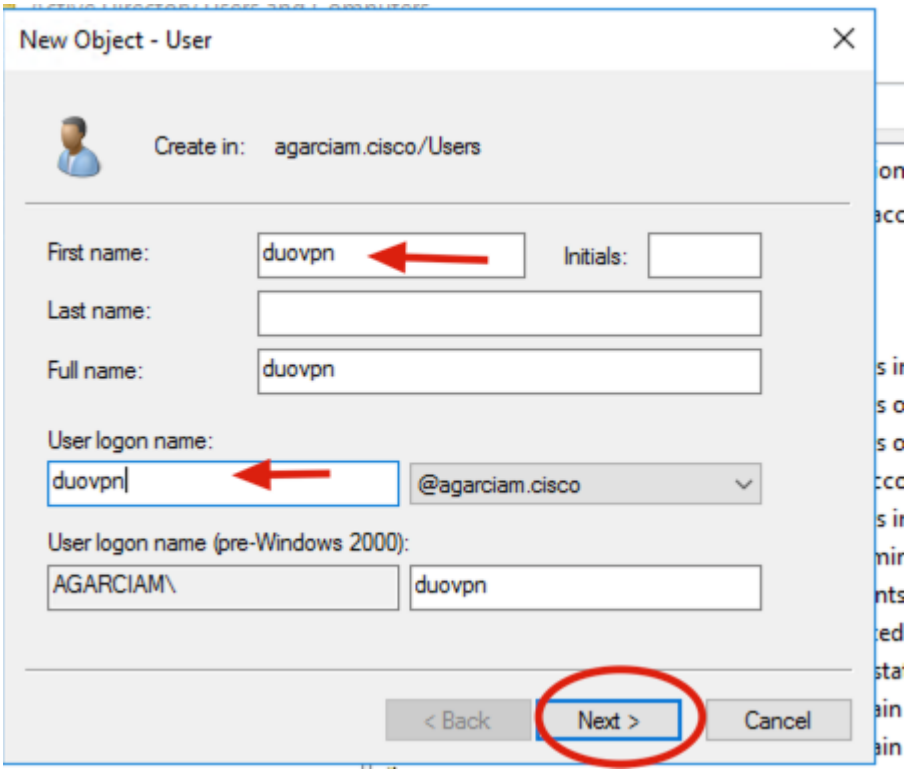
En este ejemplo de configuración, Duo-USERS se utiliza como el grupo de destino para la autenticación secundaria.



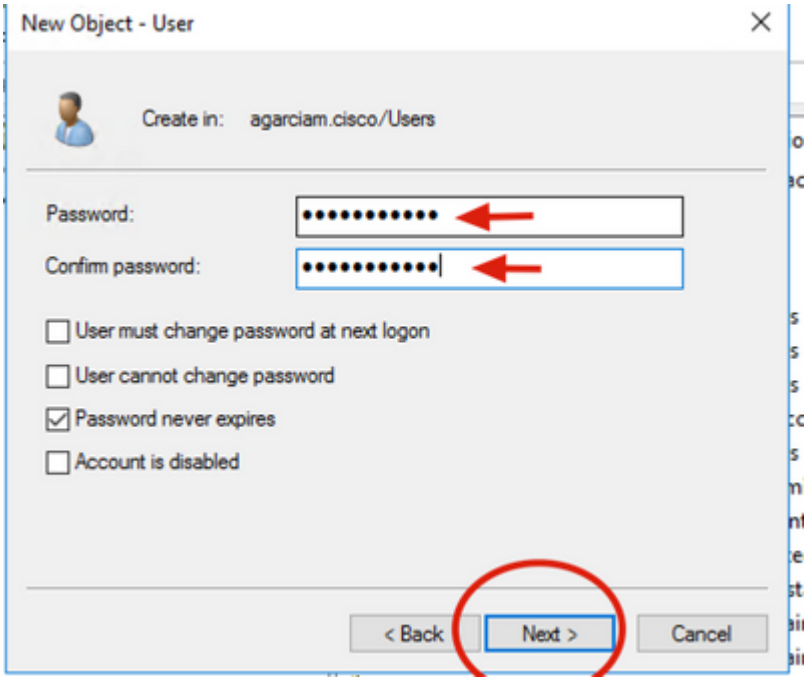
3. Haga clic con el botón derecho del ratón en la carpeta **Users** y seleccione **New** > **User**, como se muestra en la imagen.



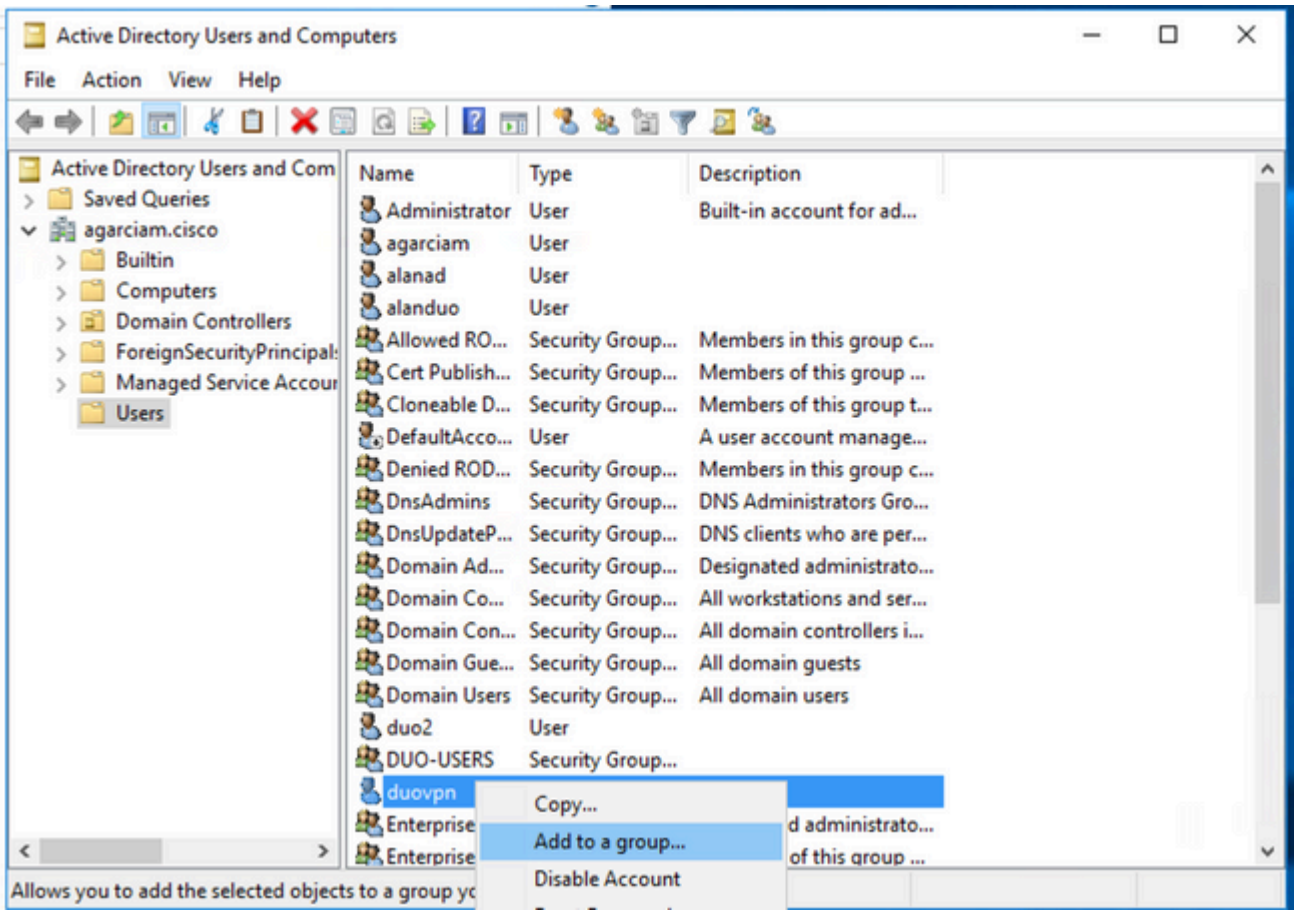
4. En la ventana Nuevo Usuario de Objeto, especifique los atributos de identidad para este nuevo usuario y haga clic en **Siguiente**, como se muestra en la imagen.



5. Confirme la contraseña y haga clic en **Next**, luego en **Finish** cuando se verifique la información del usuario.

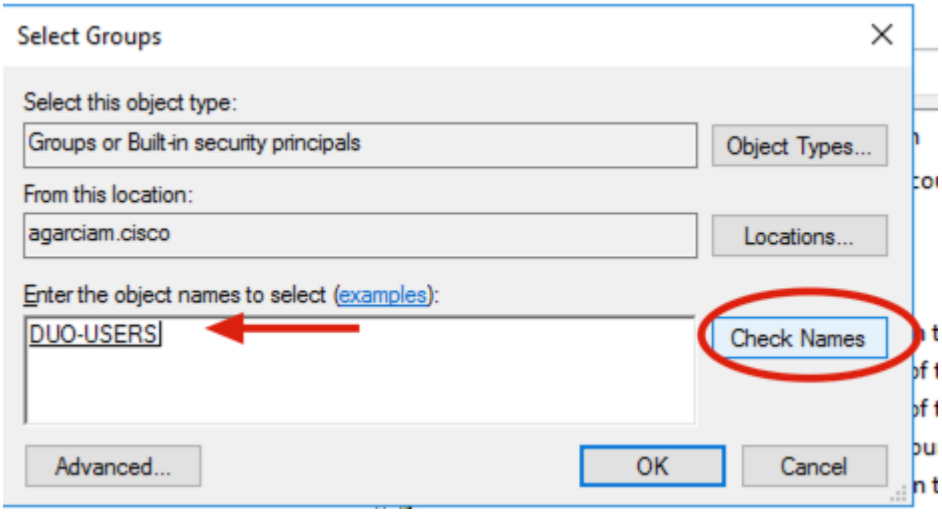


6. Asigne el nuevo usuario a un grupo específico, haga clic con el botón derecho en él y seleccione **Agregar a un grupo**, como se muestra en la imagen.



7. En el panel Seleccionar grupos, escriba el nombre del grupo deseado y haga clic en **Comprobar nombres**.

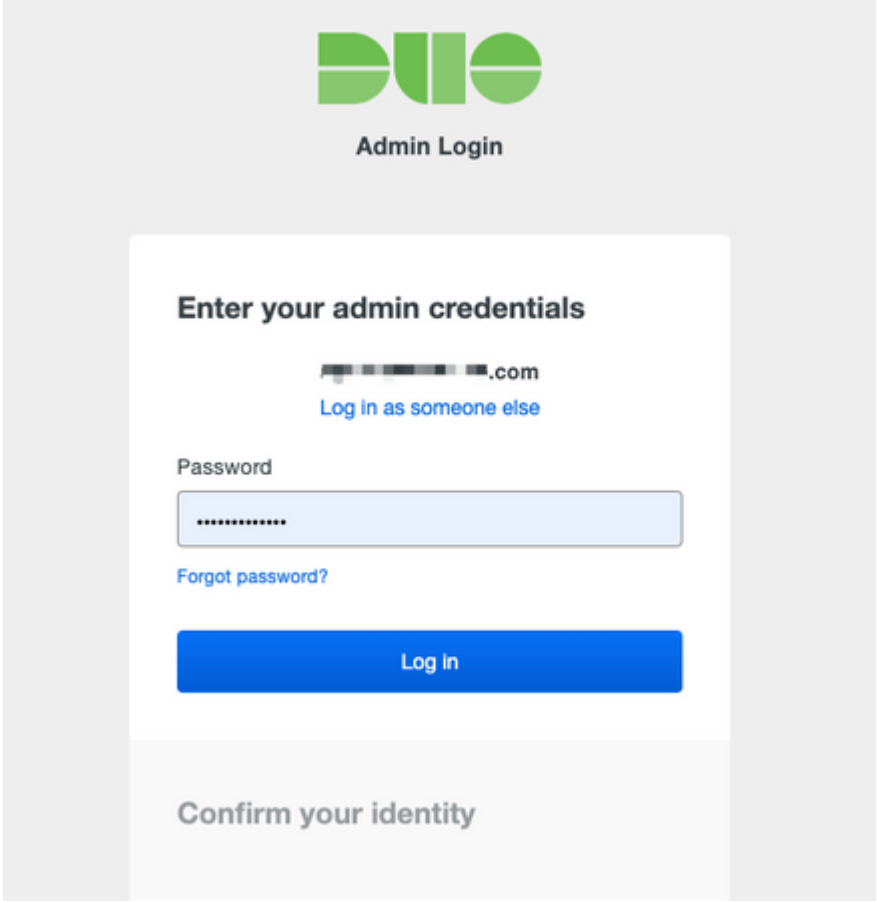
A continuación, seleccione el nombre que coincida con los criterios y haga clic en **Aceptar**.



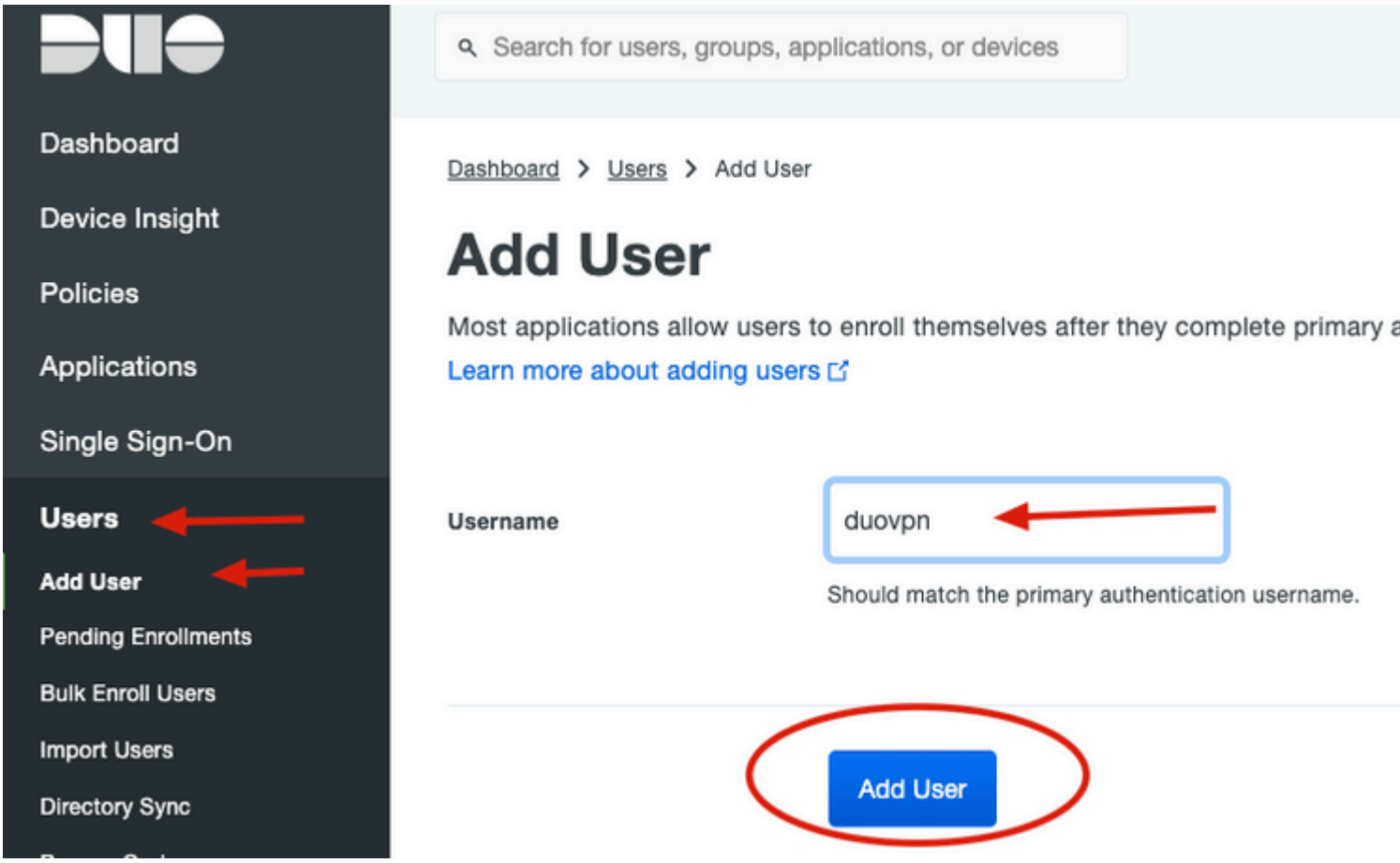
8. Este es el usuario que se utiliza en este documento como ejemplo.

Configuraciones Duo

1. Inicie sesión en el portal de administración de Dudo.



2.En el panel lateral izquierdo, navegue hasta **Usuarios**, haga clic en **Agregar usuario** y escriba el nombre del usuario que coincida con su nombre de usuario de dominio activo, luego haga clic en **Agregar usuario**.



3. En el nuevo panel de usuario, rellene el espacio en blanco con toda la información necesaria.

duovpn

This user has not enrolled yet. See our enrollment documentation to learn

Username duovpn

Username aliases + Add a username alias

Users can have up to 8 aliases.

Optionally, you may choose to reserve using an alias number f

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

Full name test vpn user

Email [redacted].com

Status

- **Active** — Require multi-factor authentication (default).
- Bypass — Allow users to skip two-factor authentication and log in w
- Disabled — Automatically deny access

This controls the user's two-factor authentication process.

Groups You don't have any editable groups. Add one.

Groups can be used for management, reporting, and policy. Le

Notes

Policies
Applications
Single Sign-On
Users
Add User
Pending Enrollments
Bulk Enroll Users
Import Users
Directory Sync
Bypass Codes
Groups
Endpoints
2FA Devices
Trusted Endpoints
Trust Monitor
Reports
Settings

Versioning
Core Authentication Service:
D235.6
Admin Panel:
D235.6
Read Release Notes

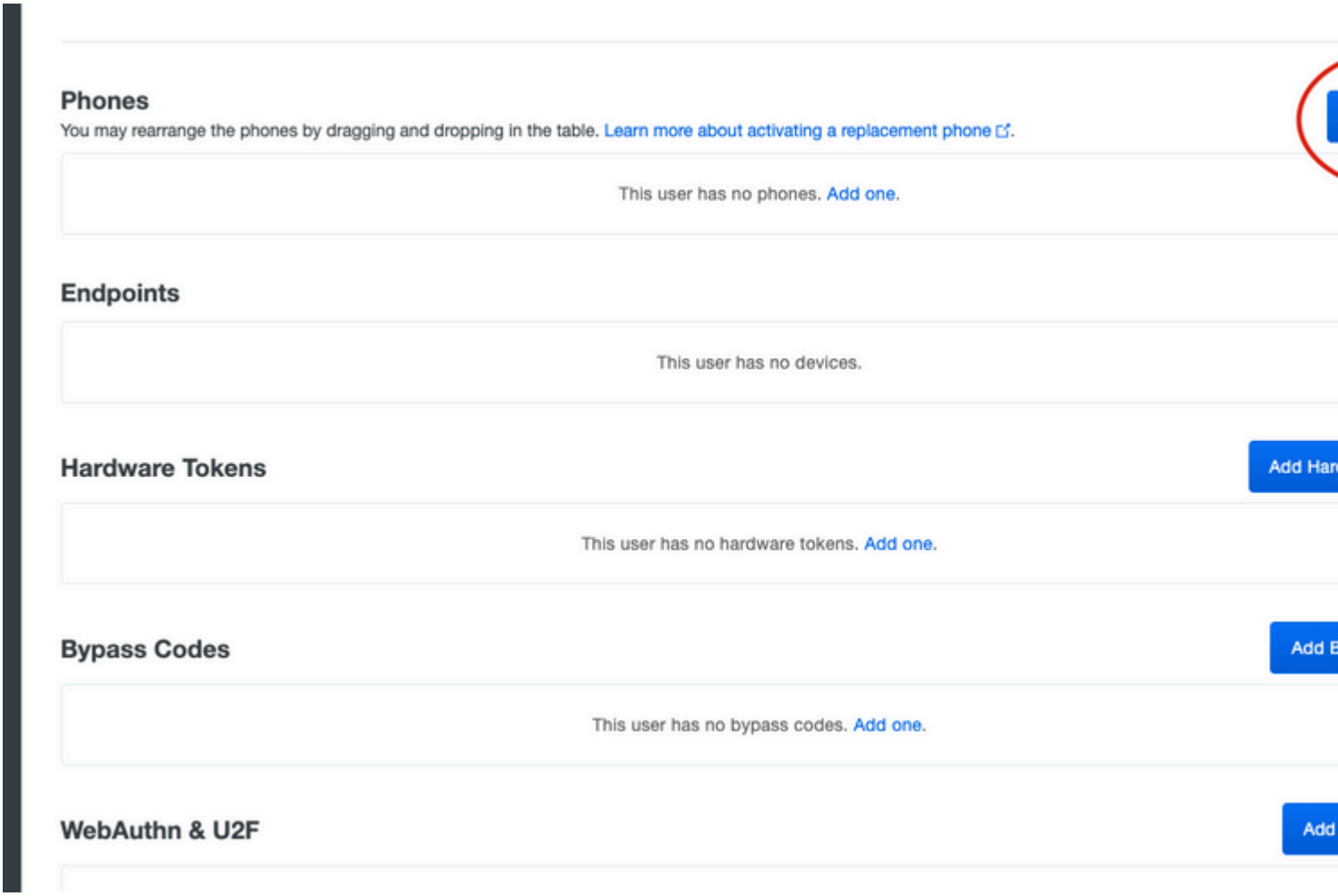
Account ID
2910-6030-53

Deployment ID
DUO63

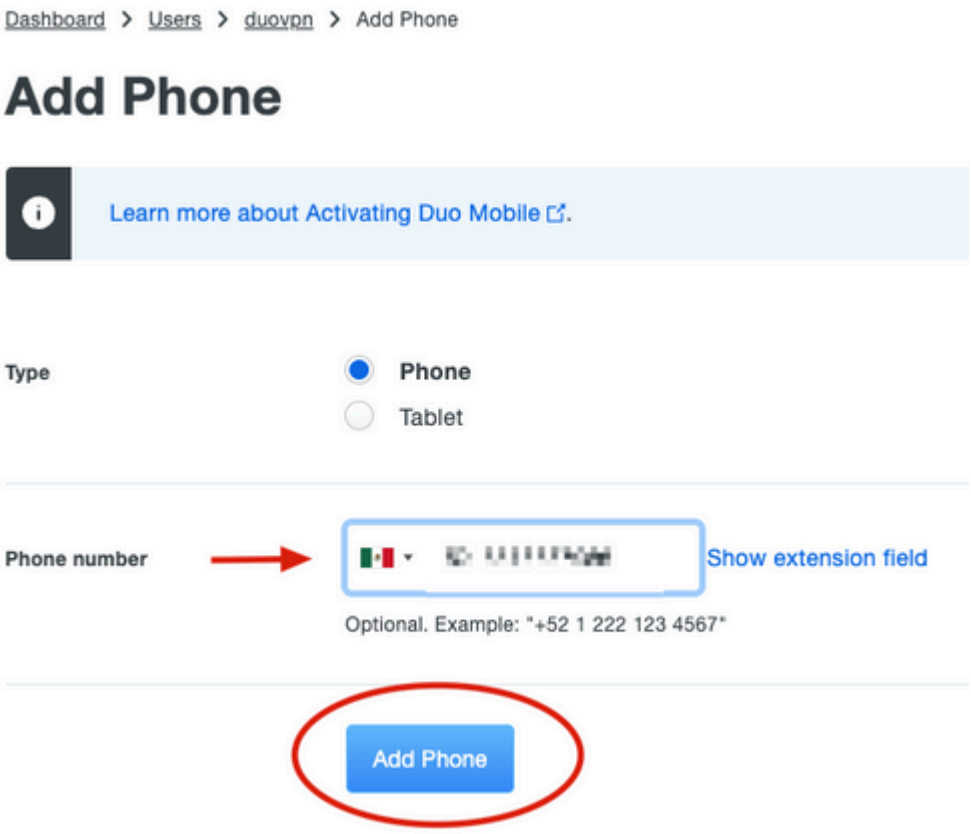
Helpful Links
Documentation
User Guide

: En este documento se utiliza el método Duo push para dispositivos móviles, por lo que es necesario agregar un dispositivo telefónico.

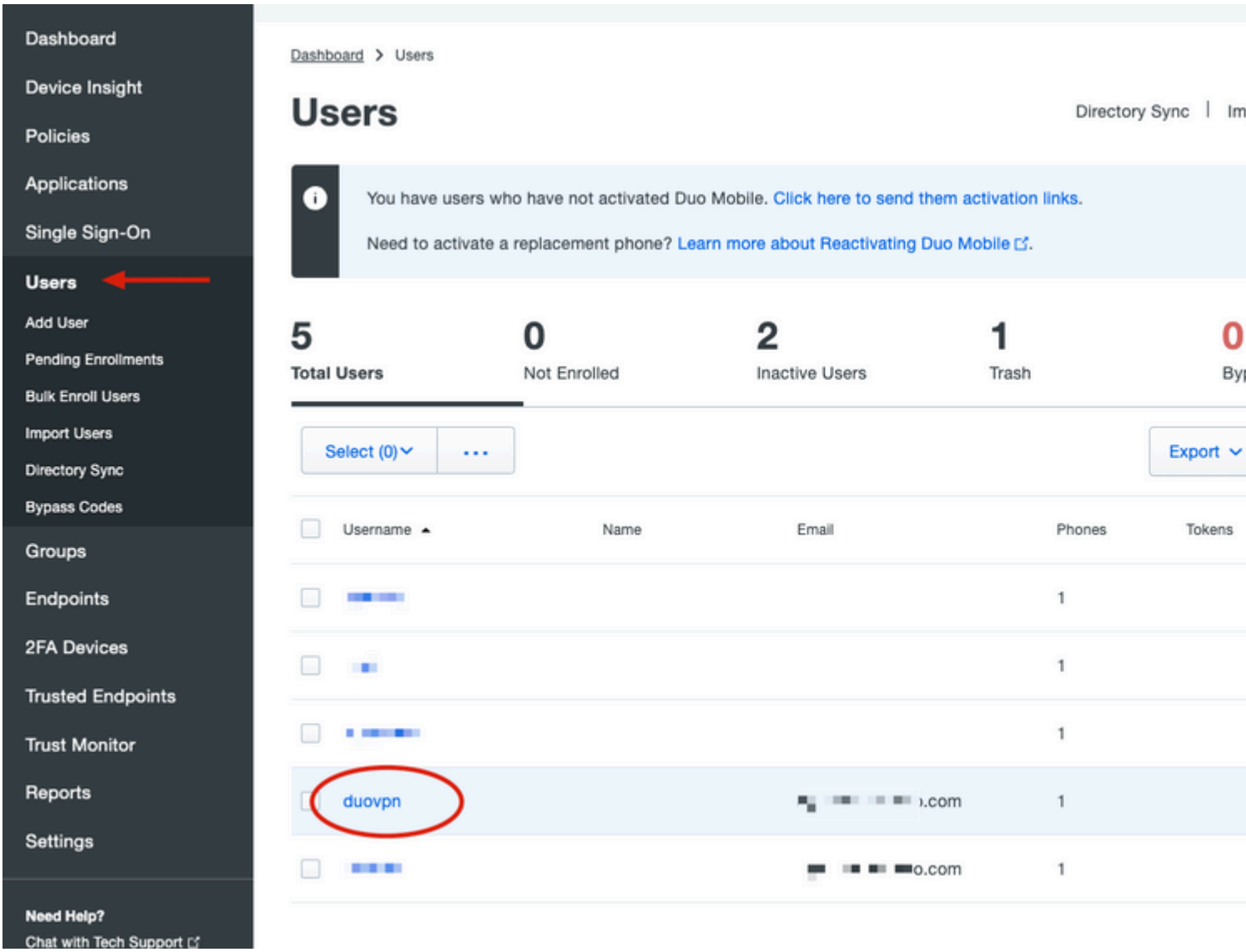
Haga clic en **Agregar teléfono**.



5. Escriba el número de teléfono del usuario y haga clic en **Agregar teléfono**.

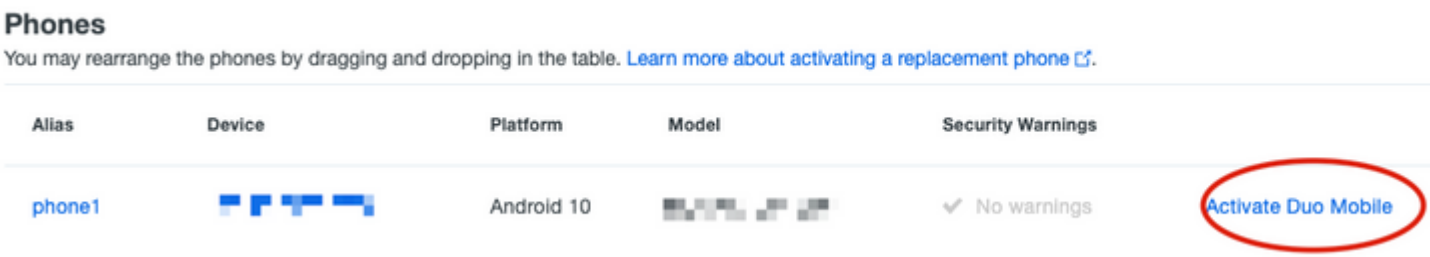


6. En el panel izquierdo Duo Admin, navegue hasta **Users** y haga clic en el nuevo usuario.

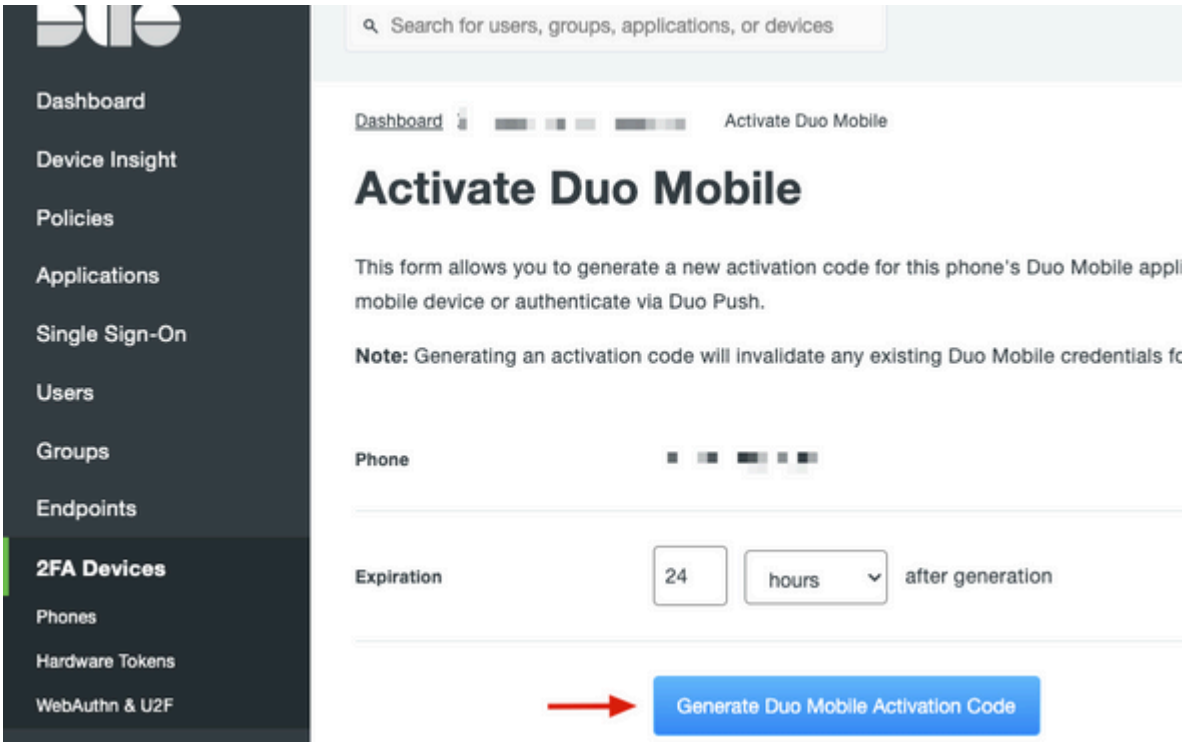


Nota: En caso de que no tenga acceso a su teléfono en este momento, puede seleccionar la opción de correo electrónico.

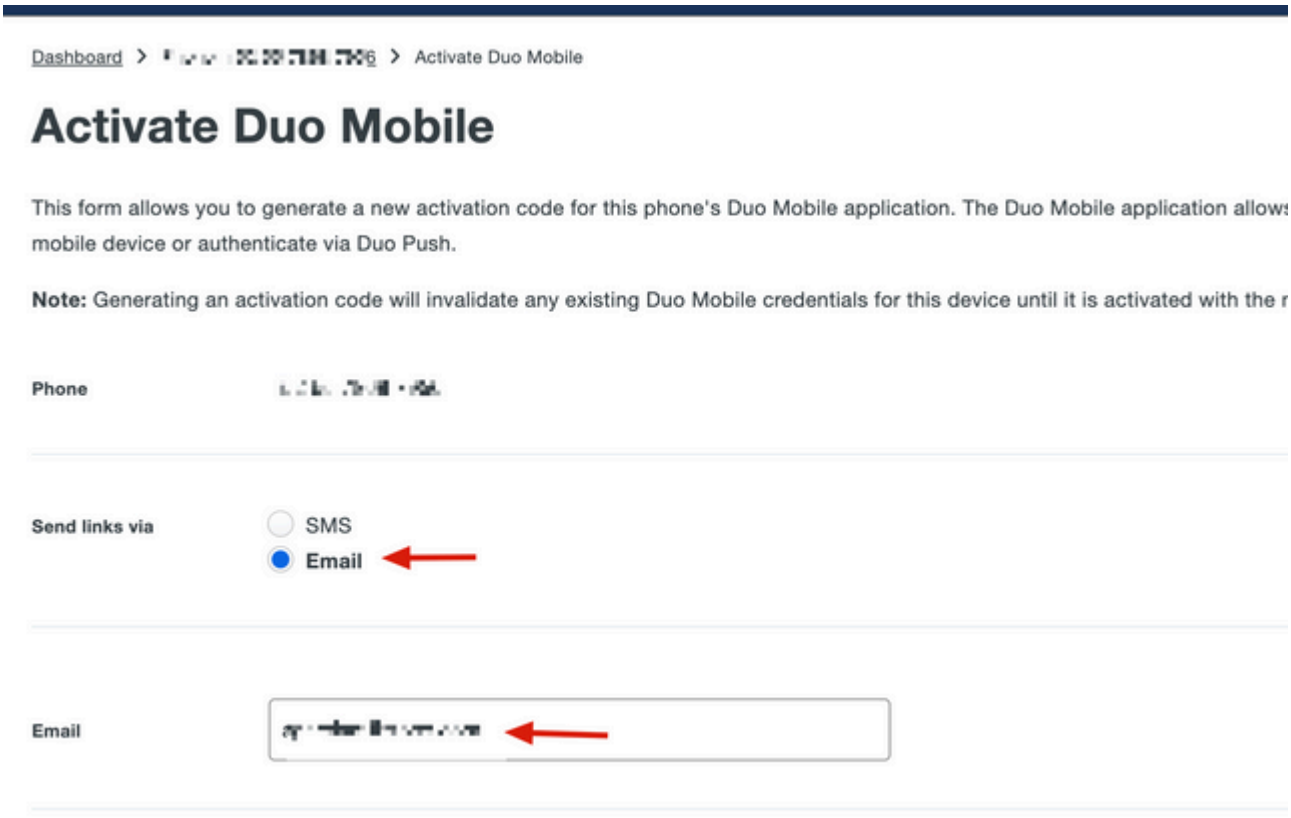
7.Navegue hasta la sección **Teléfonos** y haga clic en **Activar Duo Mobile**.



8. Haga clic en **Generar Duo Mobile Activation Code**.



9. Seleccione **Correo electrónico** para recibir las instrucciones por correo electrónico, escriba su dirección de correo electrónico y haga clic en **Enviar instrucciones por correo electrónico**.



10. Recibe un correo electrónico con las instrucciones, como se muestra en la imagen.

This is an automated email from Duo Security.

Your organization invites you to set up Duo Mobile on your phone. You will find instructions from your Duo administrator below. If you have questions, please reach out to your organization's IT or help desk team.

This email will help you add your Cisco account to Duo Mobile on this device:

Just tap this link from + ır copy and paste it into Duo Mobile manually:

If you're not reading this from + n Duo Mobile on your phone and scan this barcode:

Don't have Duo Mobile yet? Install it first:

iPhone: https://itunes.apple.com/us/app/duo-mobile/id422663827

Android: https://play.google.com/store/apps/details?id=com.duosecurity.duomobile

11. Abra la aplicación Duo Mobile desde su dispositivo móvil y haga clic en **Agregar**, luego seleccione **Usar código QR** y escanee el código desde el correo electrónico de instrucciones.

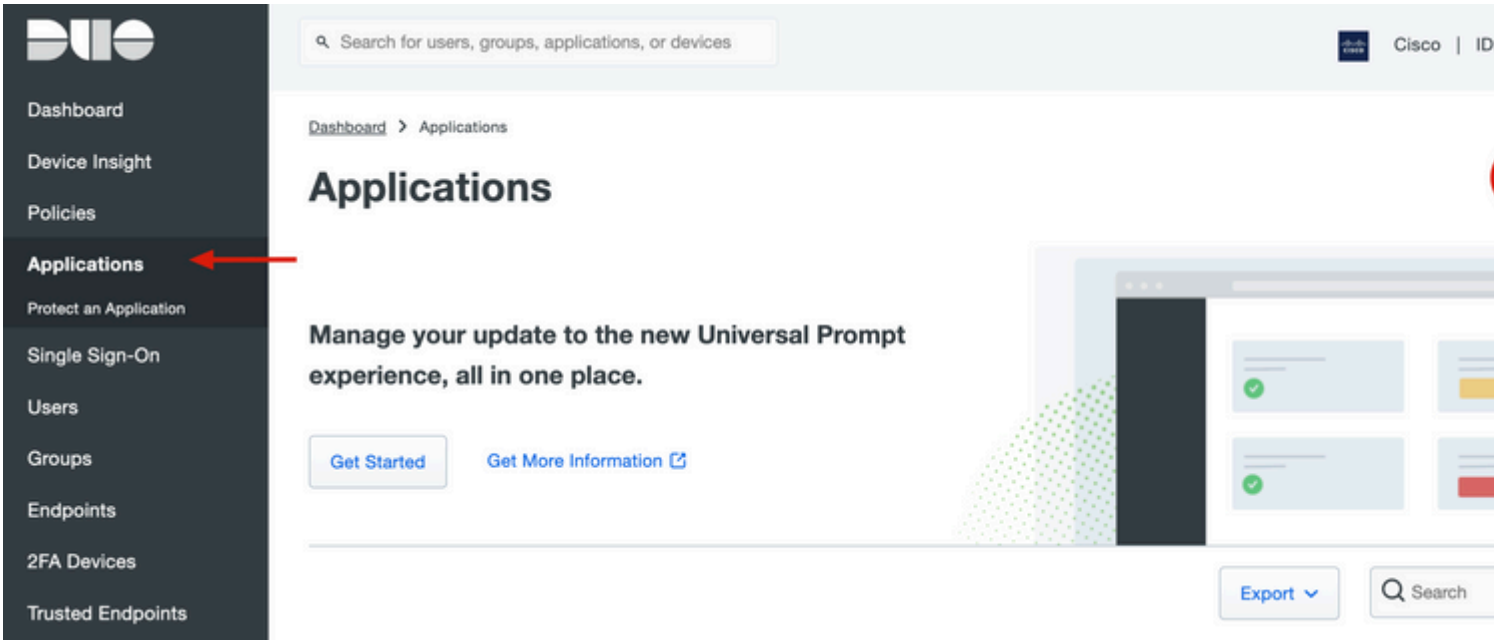
12. Se agrega un nuevo usuario a la aplicación Duo Mobile.

Configuración de proxy de autenticación Duo

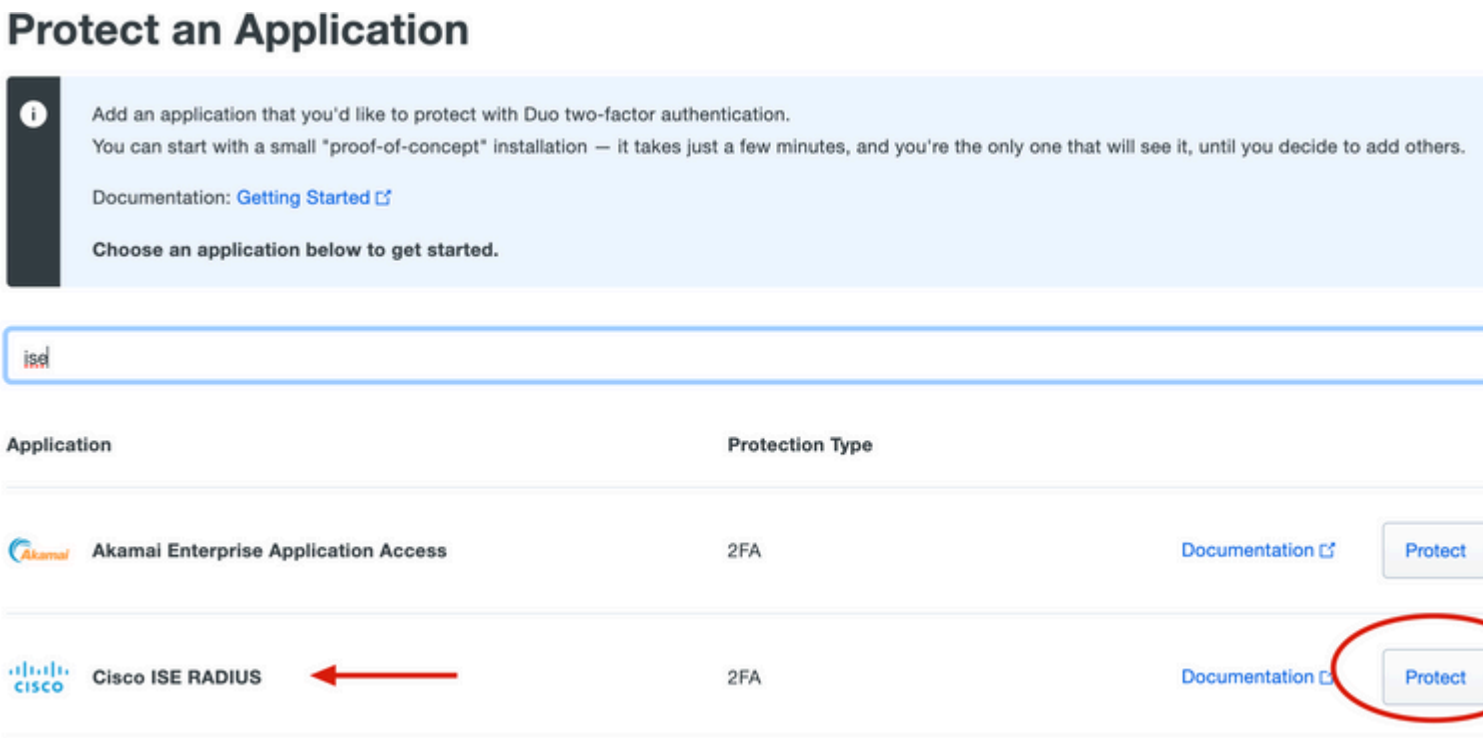
1.Descargue e instale Duo Auth Proxy Manager desde https://duo.com/docs/authproxy-reference.

> **Nota**: En este documento, Duo Auth Proxy Manager está instalado en el mismo servidor de Windows que aloja los servicios de Active Directory.

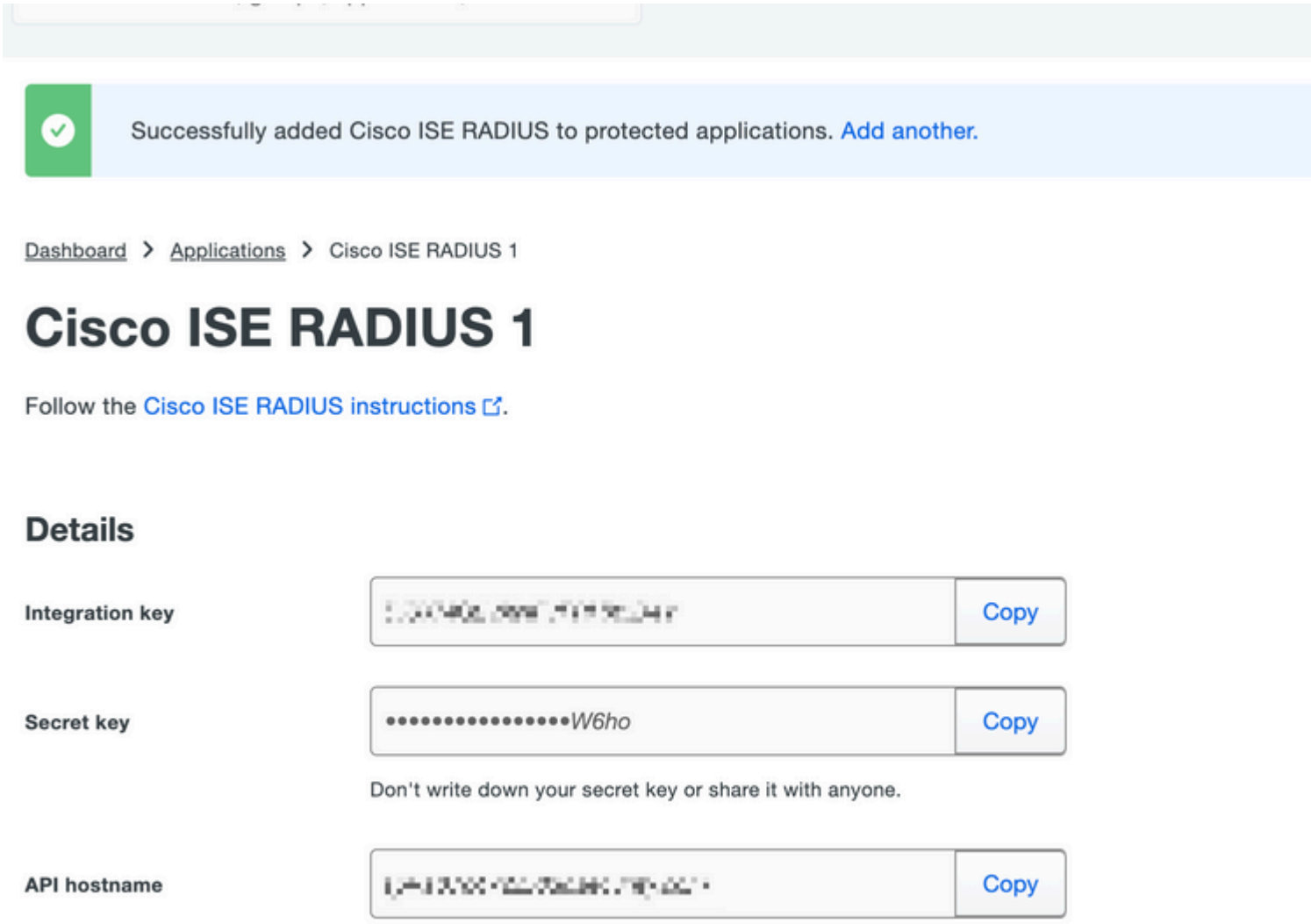
2.En el panel Duo Admin, navegue hasta **Applications** y haga clic en **Protect an Application**.



3. En la barra de búsqueda, busque Cisco ISE Radius.

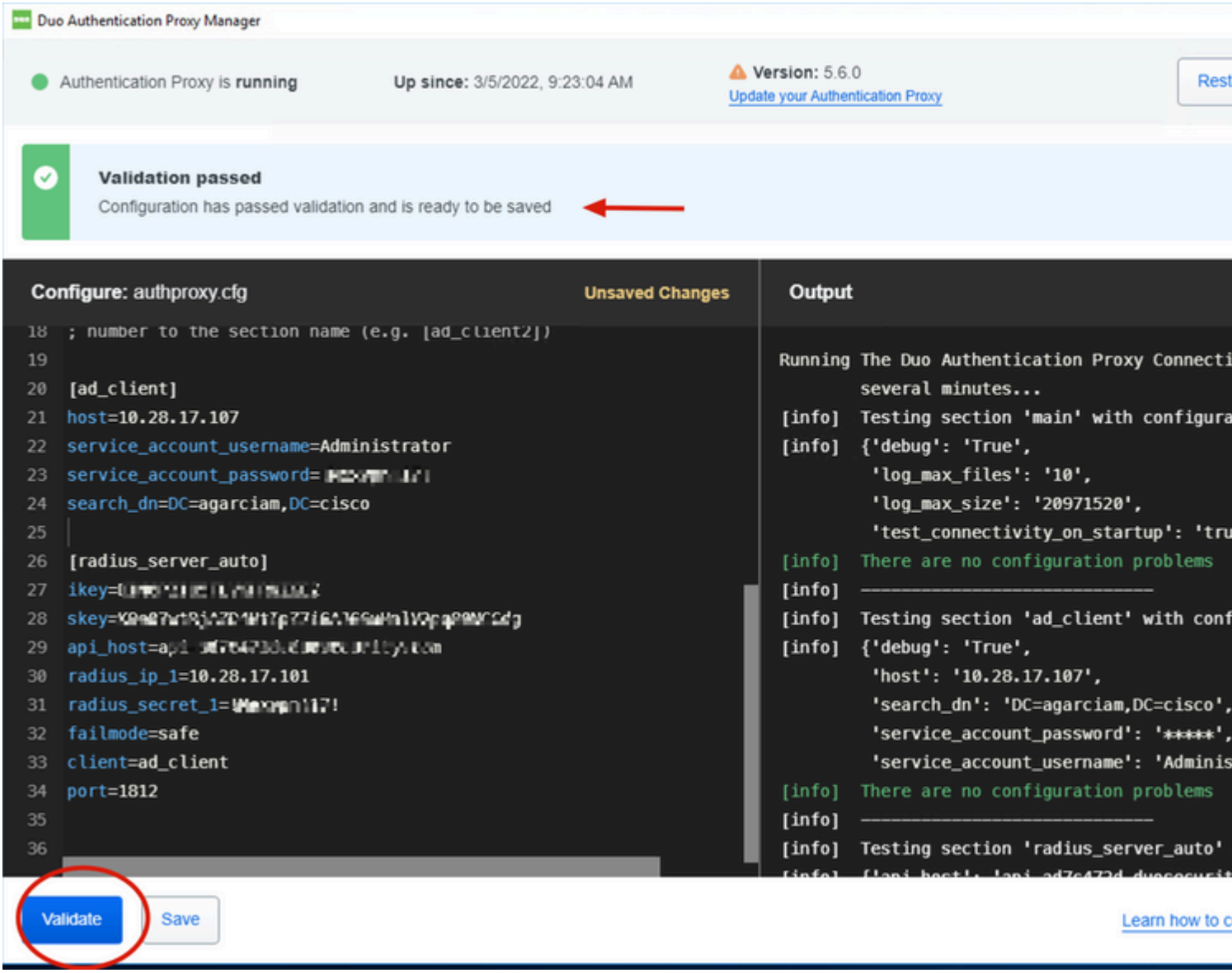


4. Copie la clave de integración, la clave secreta y el nombre de host de la API. Necesita esta información para la configuración de Duo Authentication Proxy.



5. Ejecute la aplicación Duo Authentication Proxy Manager y complete la configuración para el cliente de Active Directory y el servidor ISE Radius y haga clic en **Validar**.

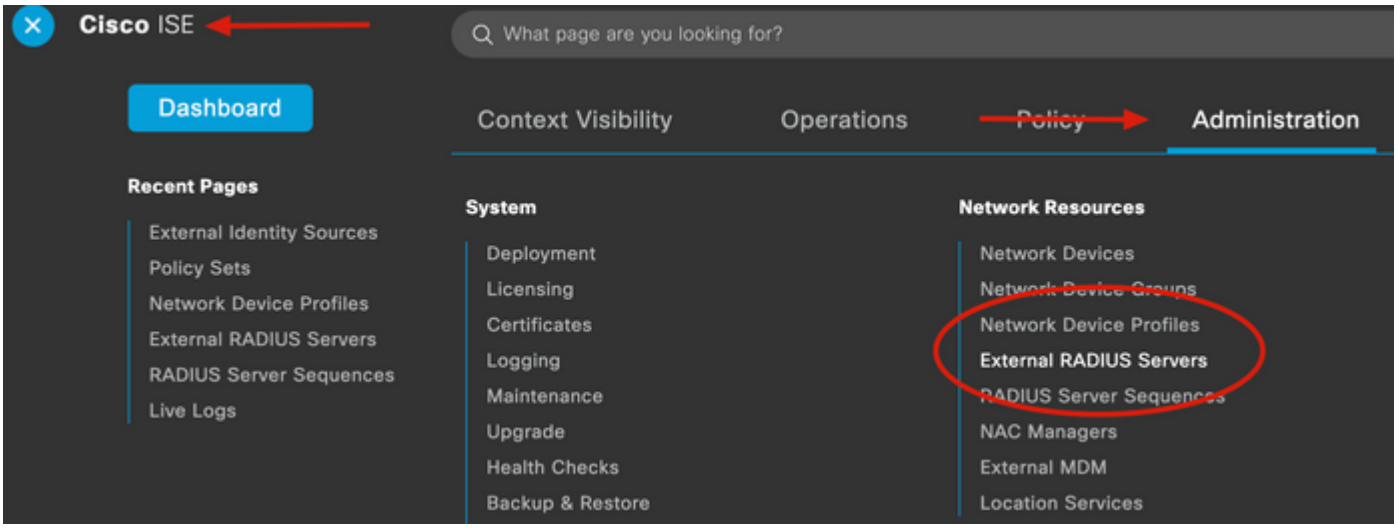
> **Nota**: Si la validación no se realiza correctamente, consulte la ficha debug para obtener detalles y corrija en consecuencia.



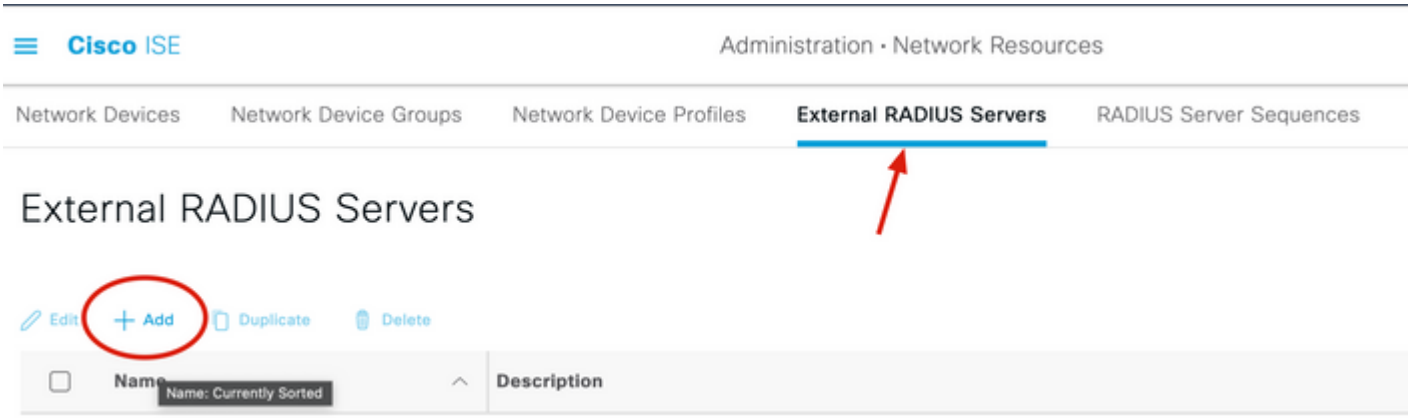
Configuraciones de Cisco ISE

1. Inicie sesión en el portal ISE Admin.

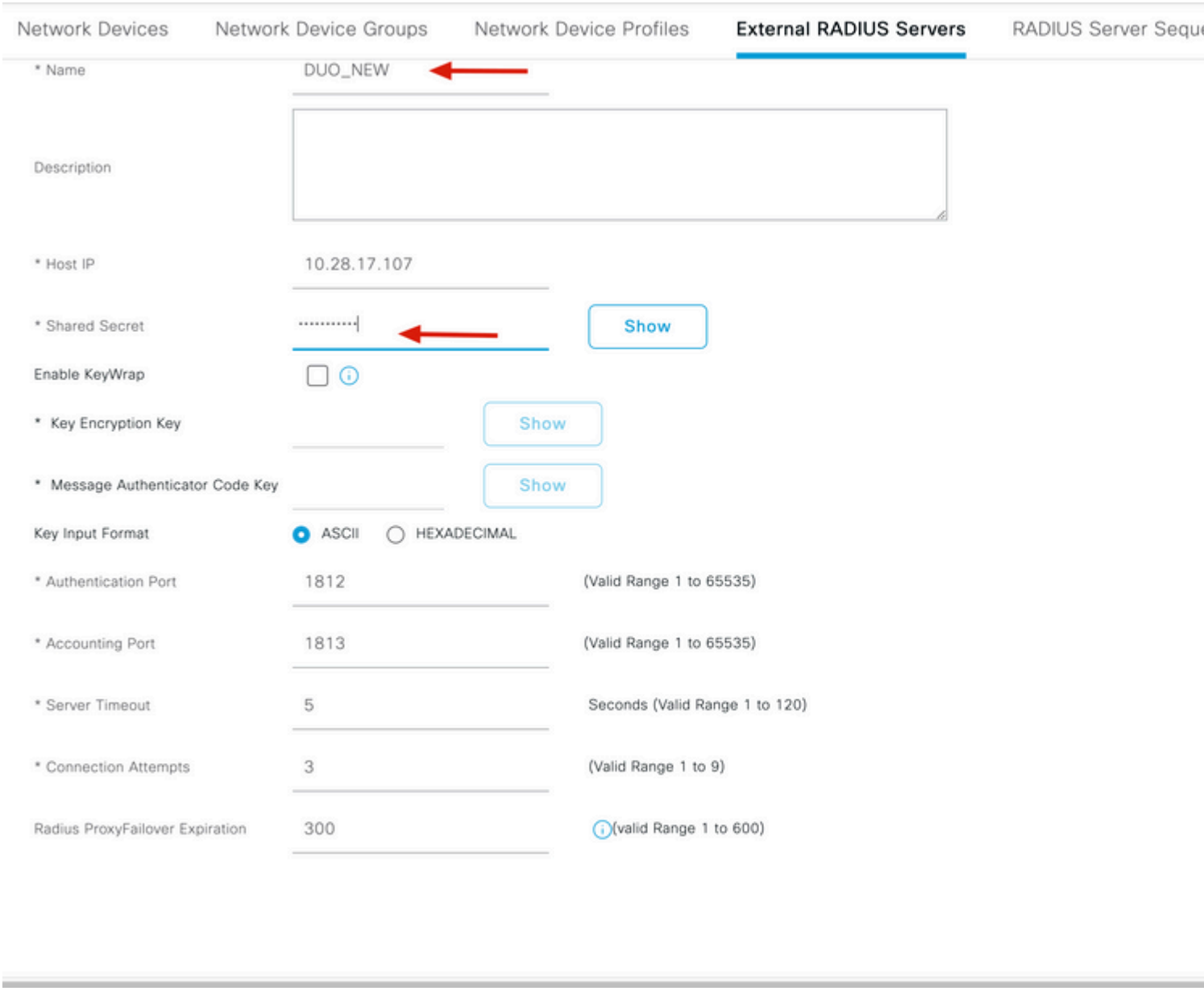
2.Expanda la pestaña Cisco ISE y navegue hasta **Administration**, luego haga clic en **Network Resources** y haga clic en **External RADIUS Servers**.



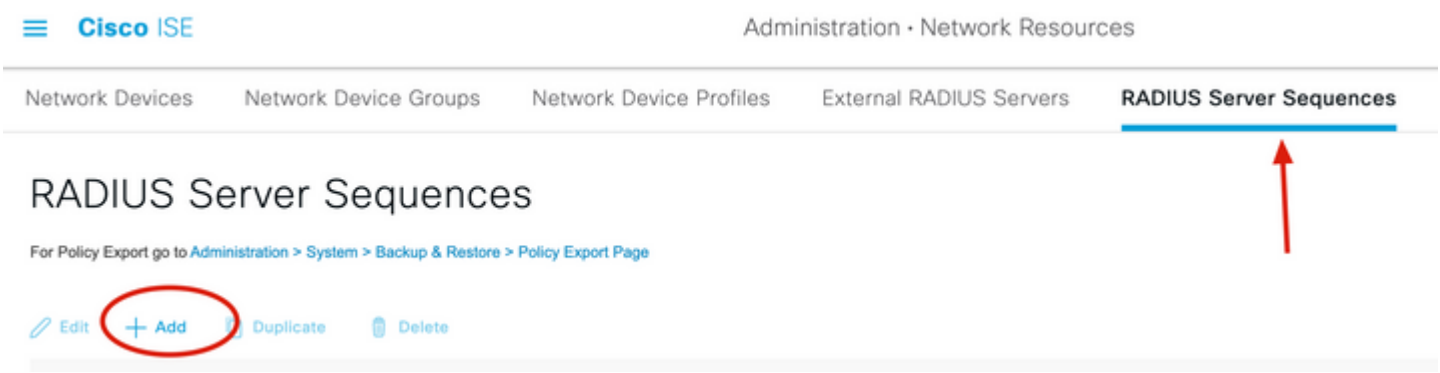
3. En la pestaña **External Radius Servers**, haga clic en **Add**.



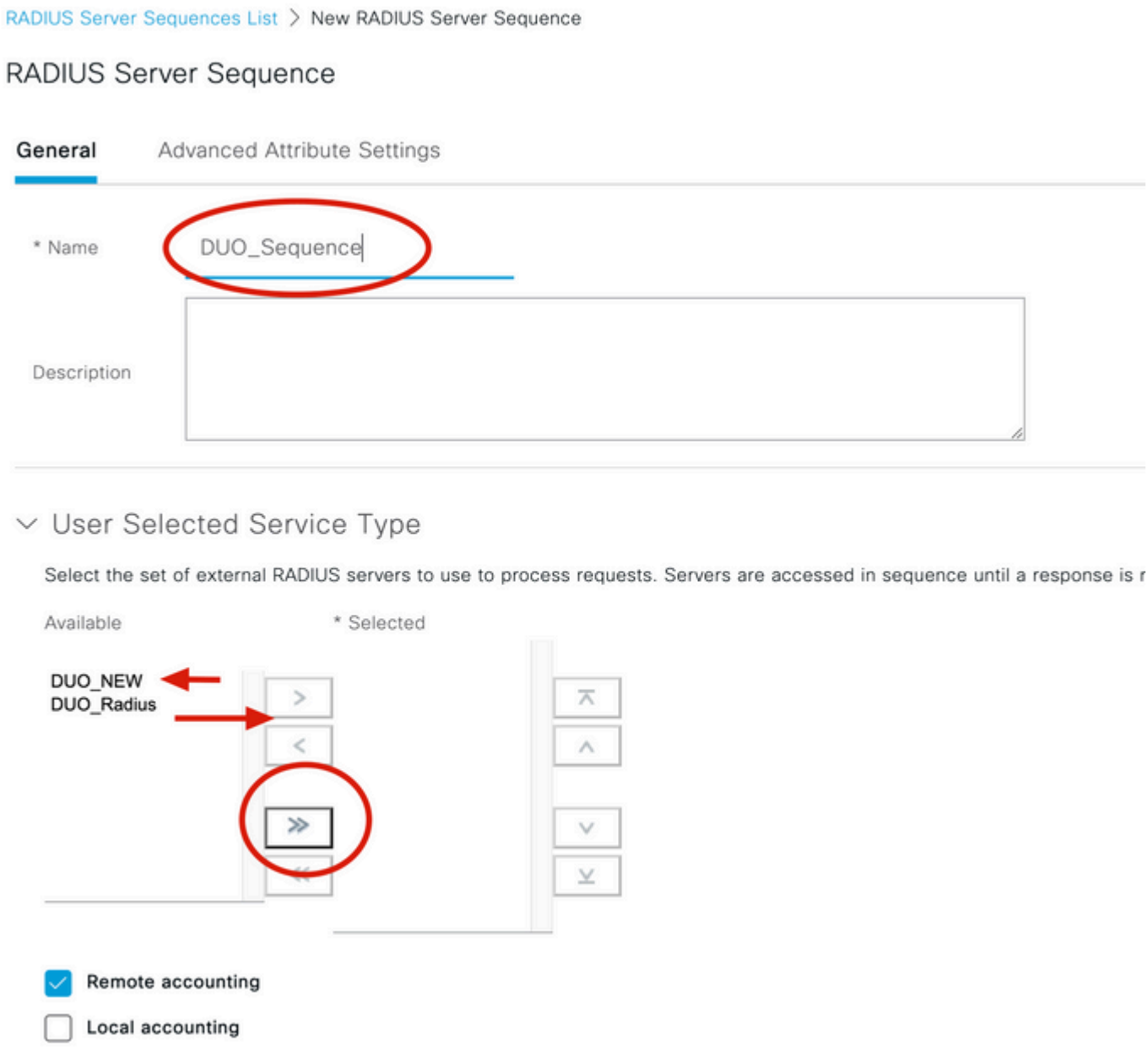
4. Rellene el espacio en blanco con la configuración RADIUS utilizada en el Administrador de Proxy de Autenticación Duo y haga clic en **Enviar**.



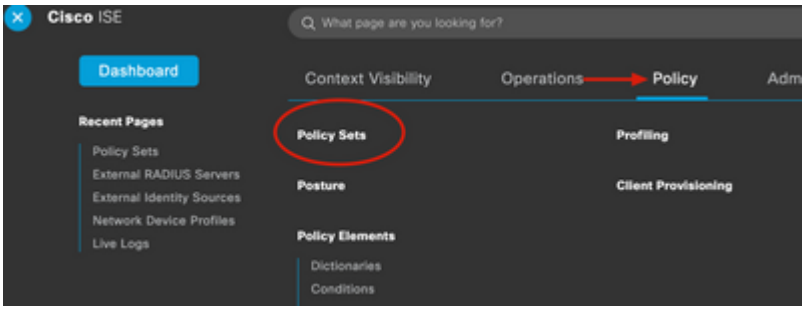
5. Acceda a la pestaña **Secuencias de Servidor RADIUS** y haga clic en **Agregar**.



6. Especifique el nombre de la secuencia y asigne el nuevo servidor externo RADIUS. Haga clic en **Enviar**.

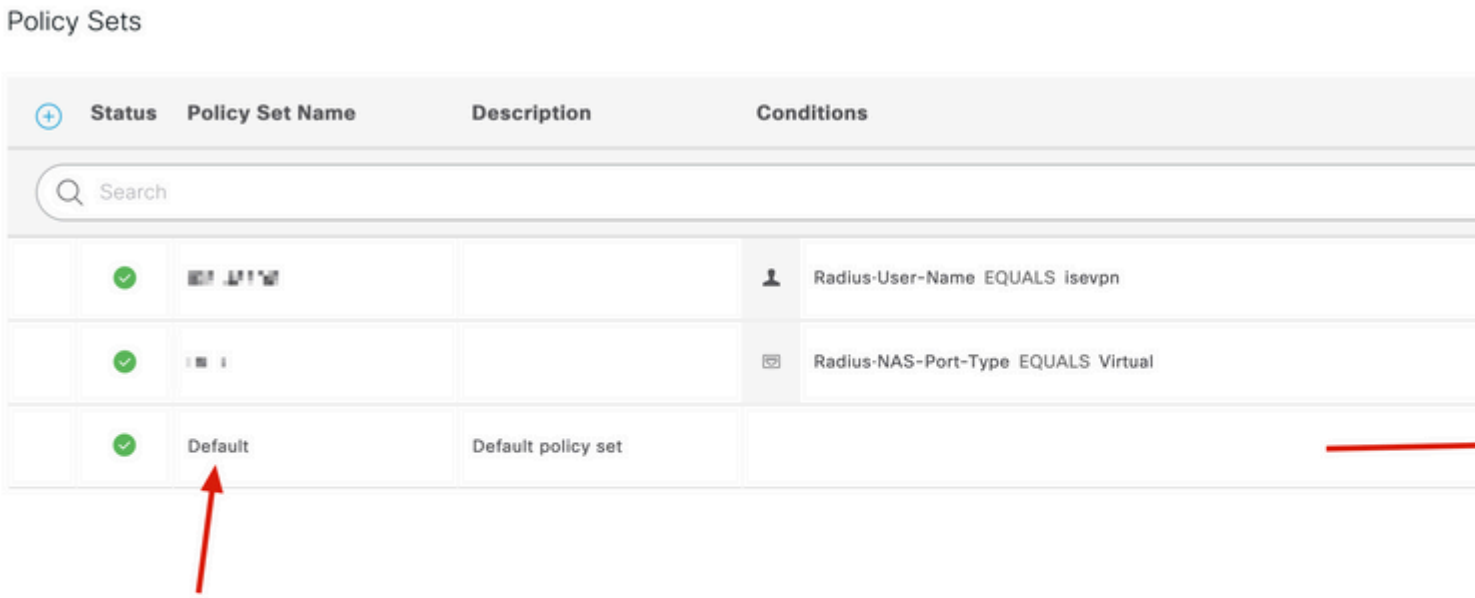


7. En el menú Panel, acceda a **Política** y haga clic en **Juegos de Políticas**.



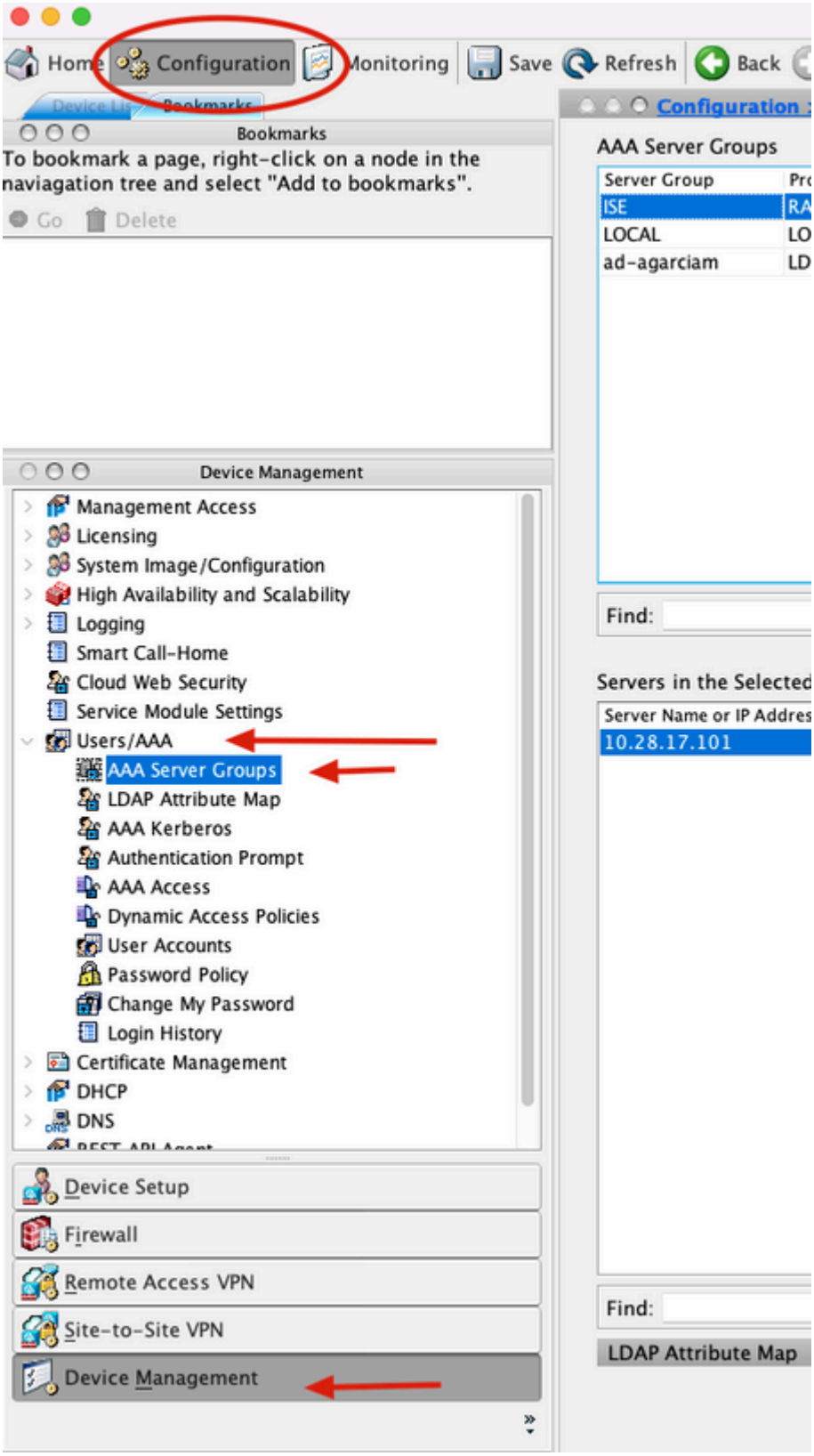
8. Asigne la secuencia RADIUS a la política por defecto.

Nota: En este documento, se aplica la secuencia Duo a todas las conexiones, por lo que se utiliza la política predeterminada. La asignación de políticas puede variar según los requisitos.

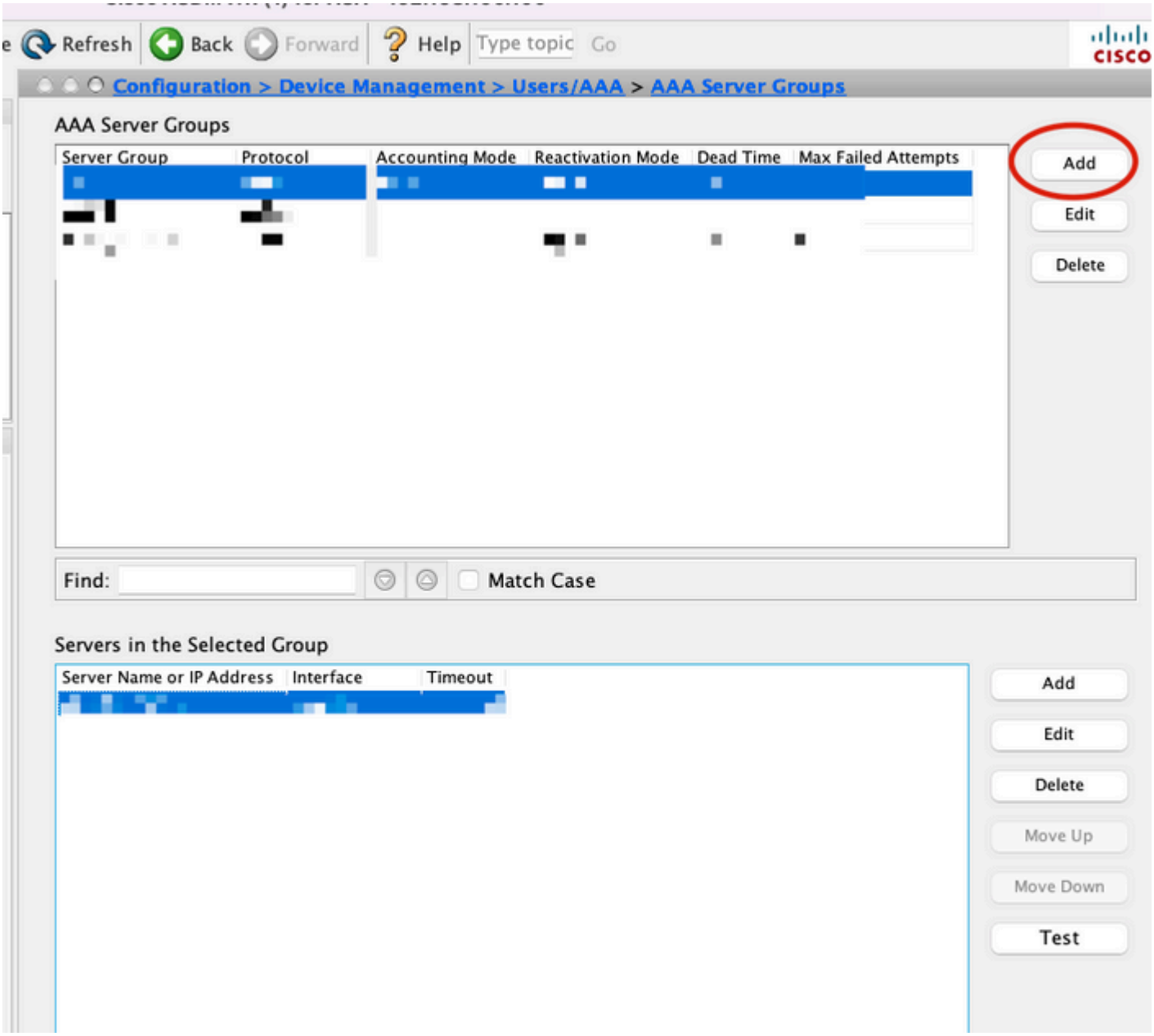


Configuración RADIUS/ISE de Cisco ASA

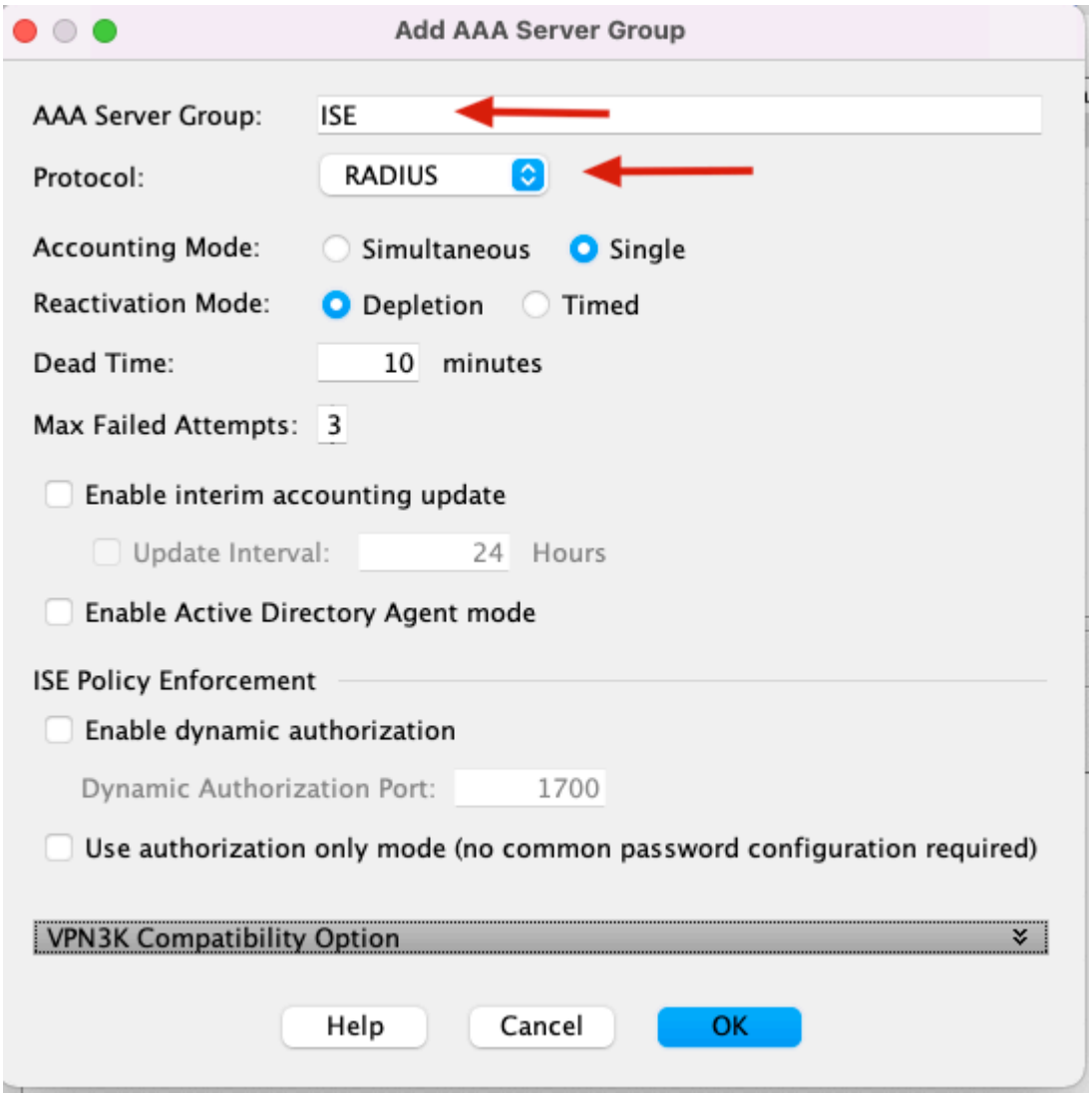
1. Configure el servidor RADIUS de ISE en Grupos de servidores AAA, navegue hasta **Configuración**, haga clic en **Administración de dispositivos** y expanda la sección **Usuarios/AAA**, seleccione **Grupos de servidores AAA**.



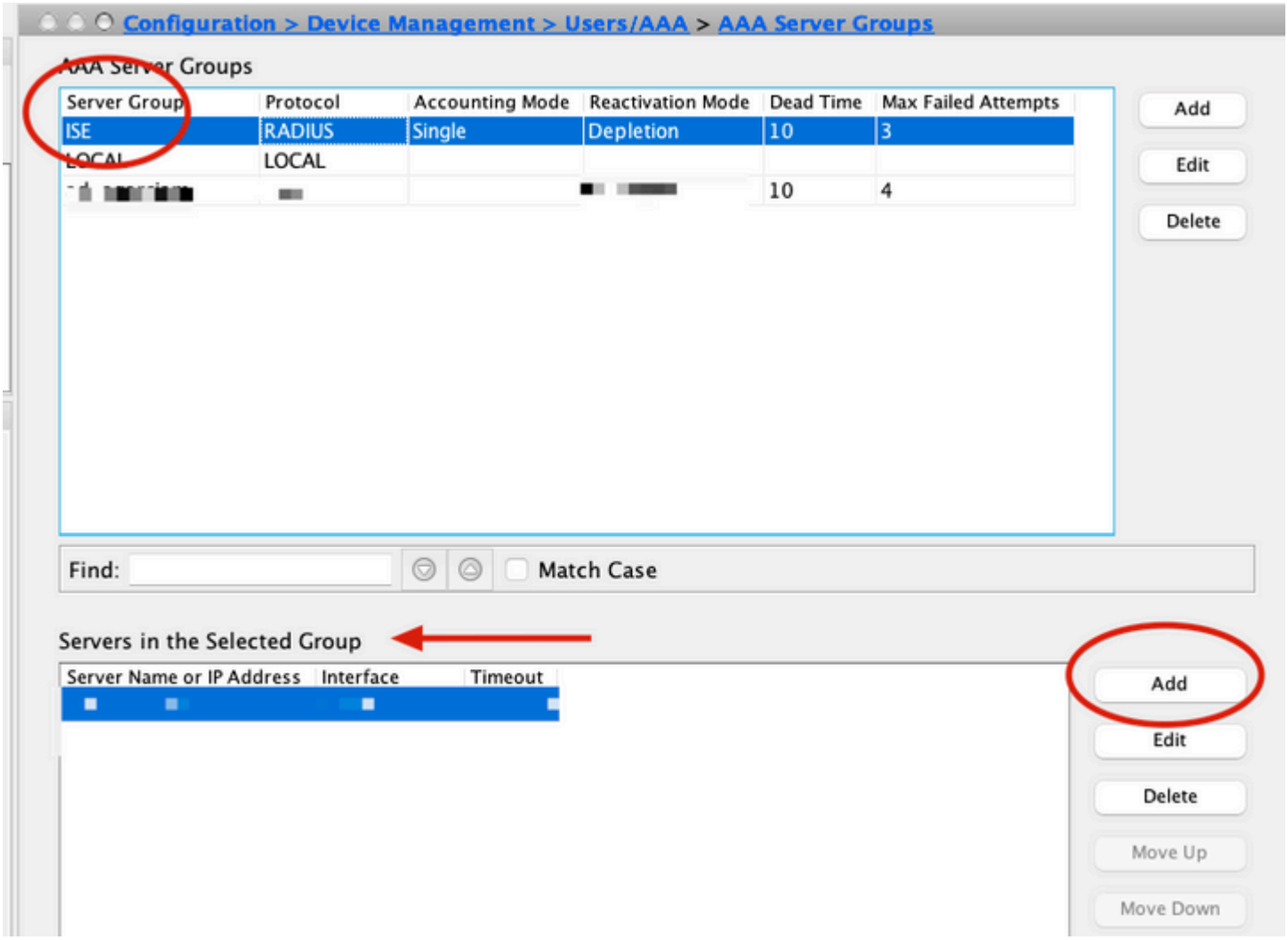
2. En el panel **AAA Server Groups**, haga clic en **Add**.



3. Seleccione el nombre del grupo de servidores y especifique **RADIUS** como el protocolo que desea utilizar y, a continuación, haga clic en **Aceptar**.

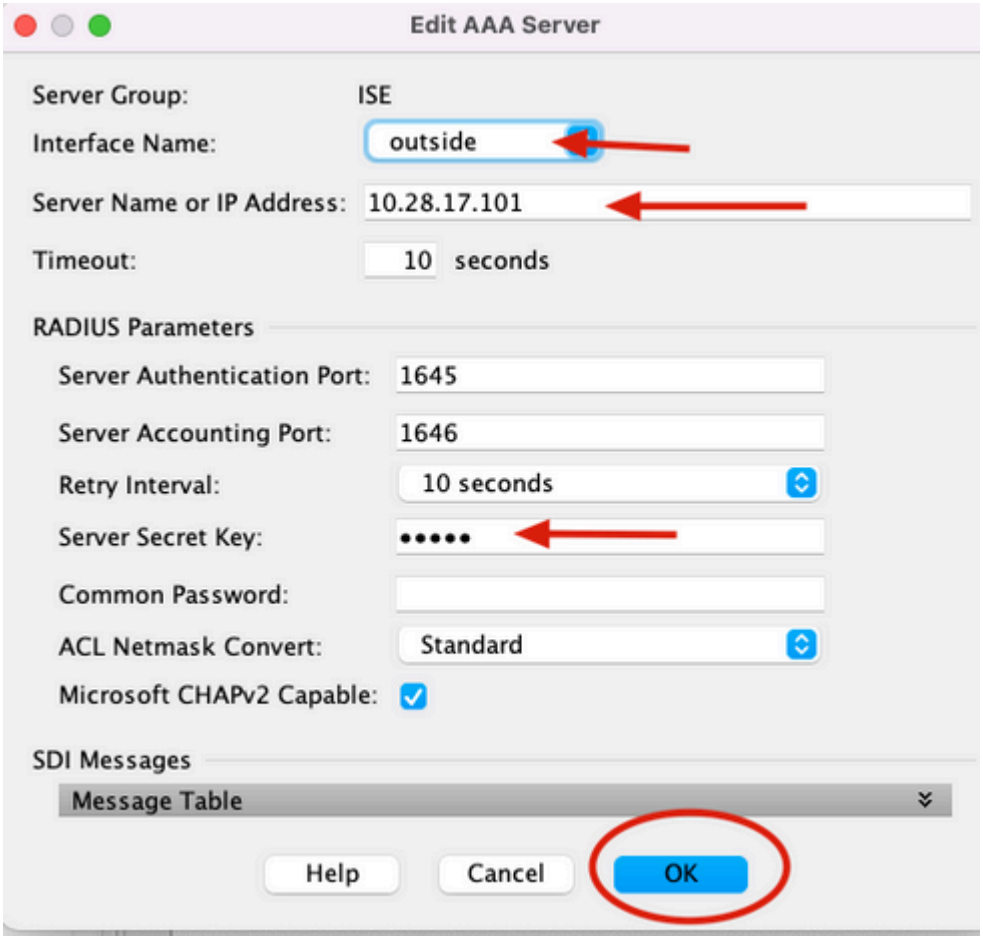


5. Seleccione el nuevo grupo de servidores y haga clic en **Agregar** en **Servidores en el** panel **Grupo Seleccionado**, como se muestra en la imagen.



6. En la ventana **Edit AAA Server**, seleccione el nombre de la interfaz, especifique la dirección IP del servidor ISE, escriba la clave secreta RADIUS y haga clic en **Ok**.

Nota: Toda esta información debe coincidir con la especificada en Duo Authentication Proxy Manager.



Configuración de CLI.

```
aaa-server ISE protocol radius
 dynamic-authorization
aaa-server ISE (outside) host 10.28.17.101
 key *****
```

Configuración de VPN de acceso remoto de Cisco ASA

```
ip local pool agarciam-pool 192.168.17.1-192.168.17.100 mask 255.255.255.0

group-policy DUO internal
group-policy DUO attributes
 banner value This connection is for DUO authorized users only!
 vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value split-agarciam
 address-pools value agarciam-pool

tunnel-group ISE-users type remote-access
tunnel-group ISE-users general-attributes
 address-pool agarciam-pool
 authentication-server-group ISE
```

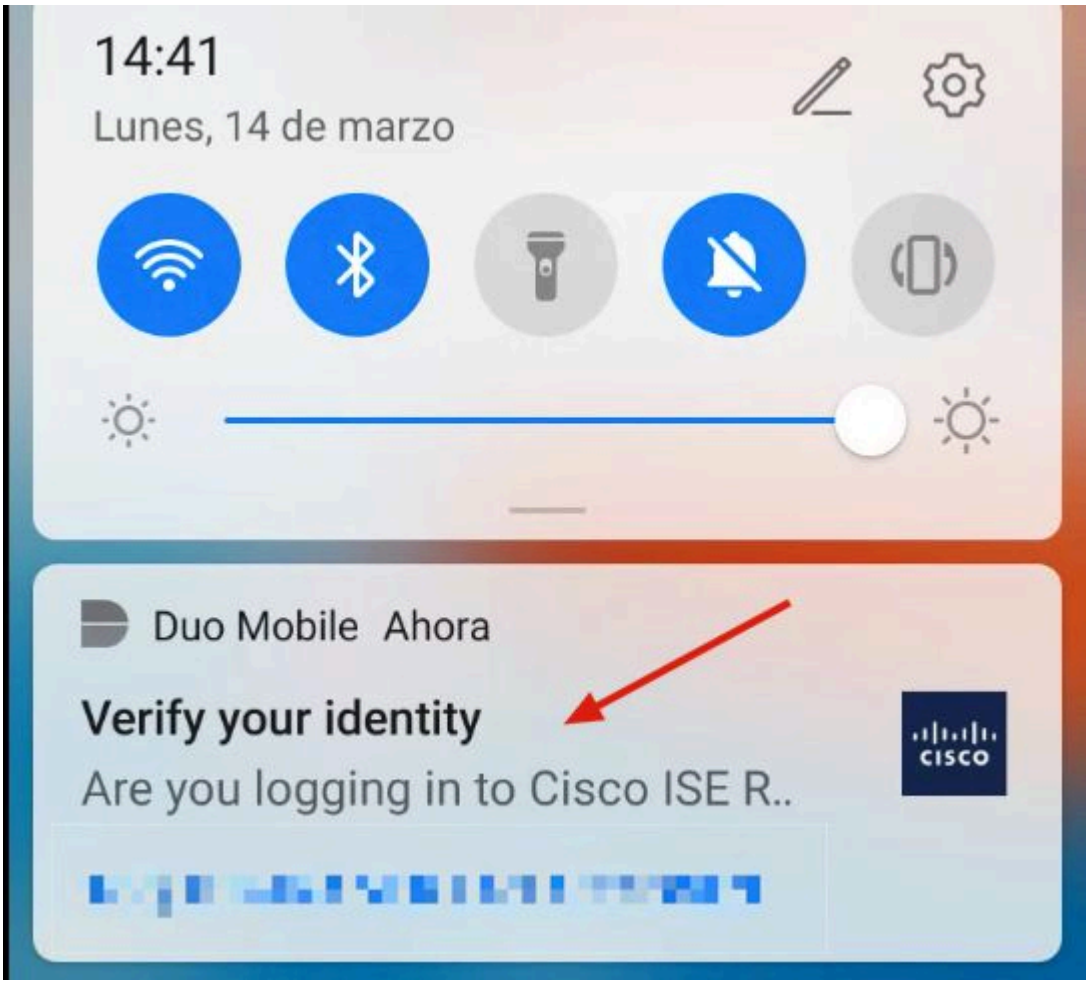
```
 default-group-policy DUO
tunnel-group ISE-users webvpn-attributes
 group-alias ISE enable
 dns-group DNS-CISCO
```

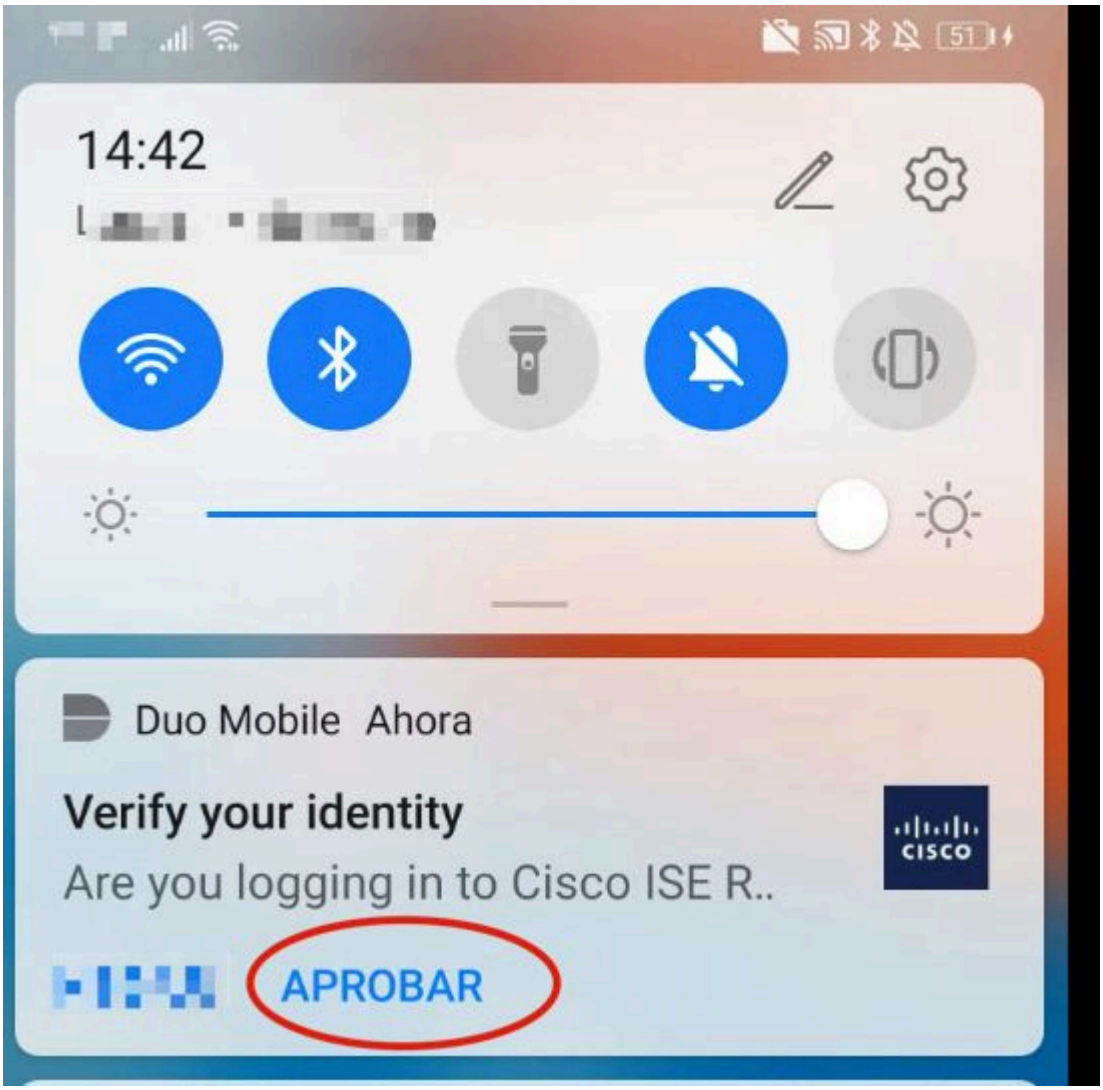
Prueba

1. Abra la aplicación **Anyconnect** en su dispositivo PC. Especifique el nombre de host de la cabecera VPN ASA e inicie sesión con el usuario creado para la autenticación secundaria Duo y haga clic en **Aceptar**.

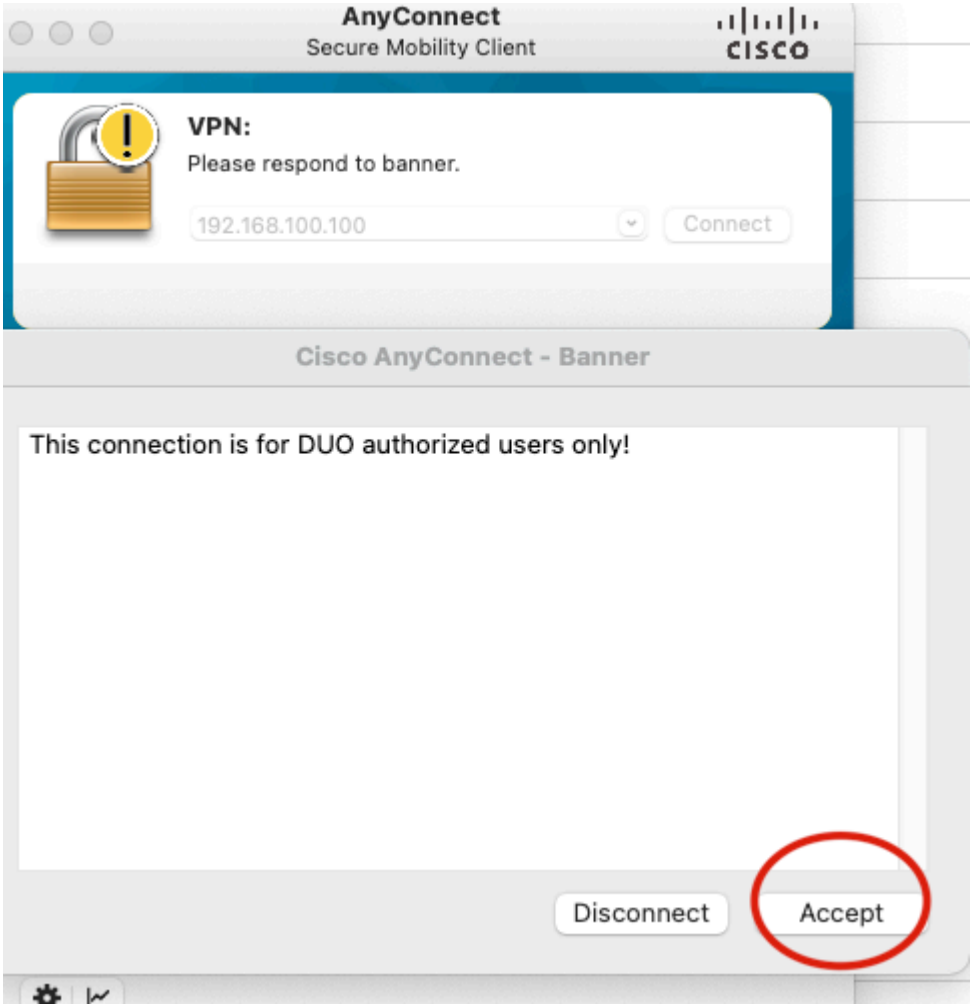
2. Recibió una notificación de inserción Duo en el dispositivo Duo Mobile del usuario especificado.

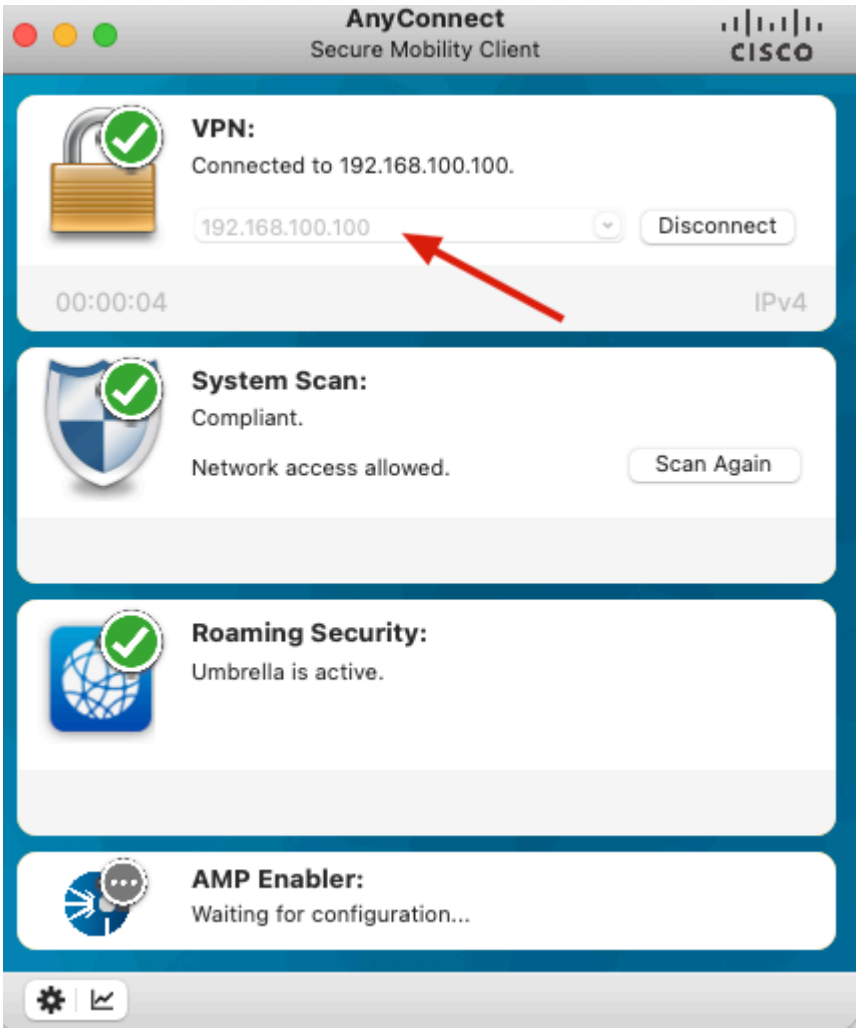
3. Abra la notificación de Duo Mobile App y haga clic en **Aprobar**.


14:41
Lunes, 14 de marzo
Duo Mobile Ahora
Verify your identity
Are you logging in to Cisco ISE R..
cisco



4. Acepte el banner y se establecerá la conexión.


AnyConnect
Secure Mobility Client
CISCO
VPN:
Please respond to banner.
192.168.100.100
Connect
Cisco AnyConnect - Banner
This connection is for DUO authorized users only!
Disconnect
Accept



Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Duo Authentication Proxy incluye una herramienta de depuración que muestra los motivos de error y fallo.

Depuraciones de trabajo

> **Nota**: La siguiente información se almacena en C:\Program Files\Duo Security Authentication Proxy\log\connectivity_tool.log.

Output

```
Running The Duo Authentication Proxy Connectivity Tool. This may take
        several minutes...
[info]  Testing section 'main' with configuration:
[info]  {'debug': 'True',
         'log_max_files': '10',
         'log_max_size': '20971520',
         'test_connectivity_on_startup': 'true'}
[info]  There are no configuration problems
[info]  ------------------------------
[info]  Testing section 'ad_client' with configuration:
[info]  {'debug': 'True',
         'host': '10.28.17.107',
         'search_dn': 'DC=agarciam,DC=cisco',
         'service_account_password': '*****',
         'service_account_username': 'Administrator'}
[info]  There are no configuration problems
```

```
[info]  ------------------------------
[info]  Testing section 'radius_server_auto' with configuration:
[info]  {'api_host': '[redacted]',
         'client': 'ad_client',
         'debug': 'True',
         'failmode': 'safe',
         'ikey': '[redacted]',
         'port': '1812',
         'radius_ip_1': '10.28.17.101',
         'radius_secret_1': '*****',
         'skey': '*****[40]'}
[info]  There are no configuration problems
```

```
[info]  Testing section 'main' with configuration:
[info]  {'debug': 'True',
         'log_max_files': '10',
         'log_max_size': '20971520',
         'test_connectivity_on_startup': 'true'}
[info]  There are no connectivity problems with the section.
```

```
[info]  There are no connectivity problems with the section.
[info]  ------------------------------
[info]  Testing section 'ad_client' with configuration:
[info]  {'debug': 'True',
         'host': '10.28.17.107',
         'search_dn': 'DC=agarciam,DC=cisco',
         'service_account_password': '*****',
         'service_account_username': 'Administrator'}
[info]  The LDAP Client section has no connectivity issues.
[info]  ------------------------------
[info]  Testing section 'radius_server_auto' with configuration:
[info]  {'api_host': '[redacted]',
         'client': 'ad_client',
         'debug': 'True',
         'failmode': 'safe',
         'ikey': '[redacted]',
         'port': '1812',
         'radius_ip_1': '10.28.17.101',
         'radius_secret_1': '*****',
         'skey': '*****[40]'}
[info]  The RADIUS Server has no connectivity problems.
[info]  ------------------------------
[info]  SUMMARY
[info]  No issues detected
```

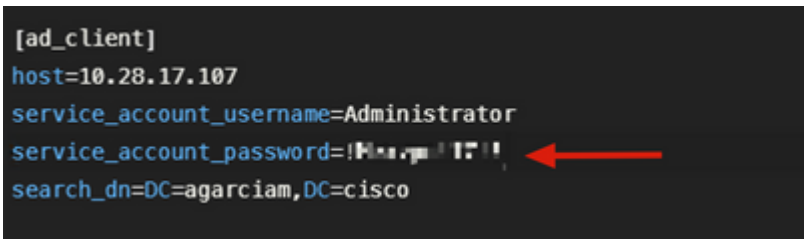
1. Problemas de conectividad, IP incorrecta, FQDN/nombre de host no resuelto en la configuración de Active Directory.

```
[ad_client]
host=10.28.17.106
service_account_username=Administrator
service_account_password=[redacted]
search_dn=DC=agarciam,DC=cisco
```

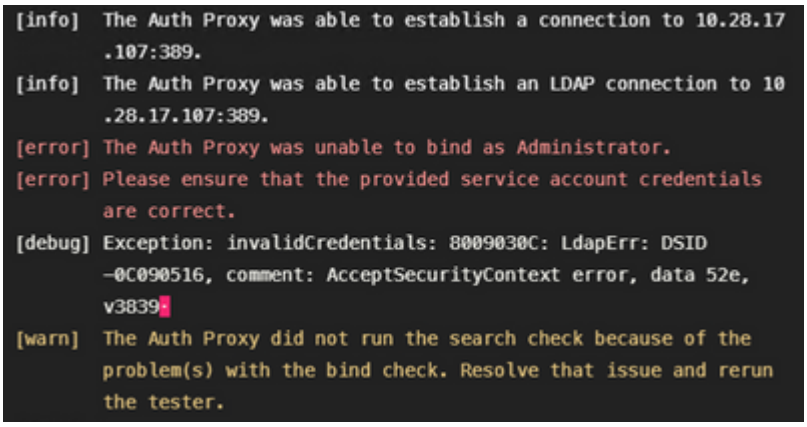
Output

```
        'host': '10.28.17.106',
        'search_dn': 'DC=agarciam,DC=cisco',
        'service_account_password': '*****',
        'service_account_username': 'Administrator'}
[warn]  The LDAP Client section has connectivity problems.
[warn]  The LDAP host clear connection to 10.28.17.106:389 has
        connectivity problems.
[error] The Auth Proxy was not able to establish a connection to 10
        .28.17.106:389.
```

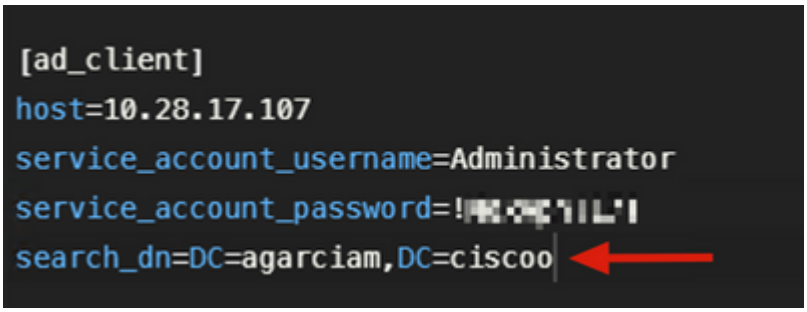
2. Contraseña incorrecta para el usuario Administrador en Active Directory.



Depuraciones.



3. Dominio base incorrecto.



Depuraciones.

```
[info]  The Auth Proxy was able to bind as A
[error] The Auth Proxy got an error searchin
        ,DC=ciscoo.
[debug] Exception: referral: 0000202B: RefEr
        1 access points
                ref 1: 'agarciam.ciscoo'
```

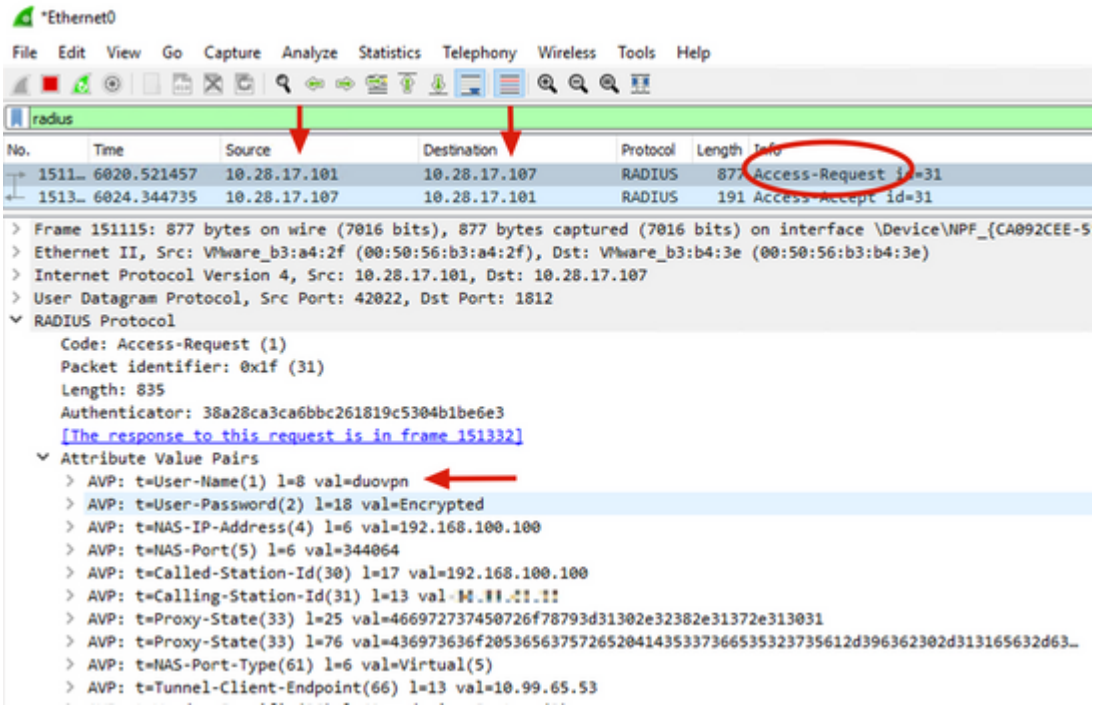
4. Valor de RADIUS de clave incorrecta.

```
[radius_server_auto]
ikey=[redacted]XHRNZ6EZ1
skey=[redacted]
api_host=[redacted]ity.com
radius_ip_1=10.28.17.101
radius_secret_1=!Mexvpn!17!
failmode=safe
client=ad_client
port=1812
```

Depuraciones

```
[error] The ikey value provided is invalid.
[info]  ----------------------------------
[info]  SUMMARY
[warn]  Checks for external connectivity were not run. Please fix the
        configuration and try again.
```

5. Compruebe que el servidor ISE envía paquetes de solicitud de acceso.

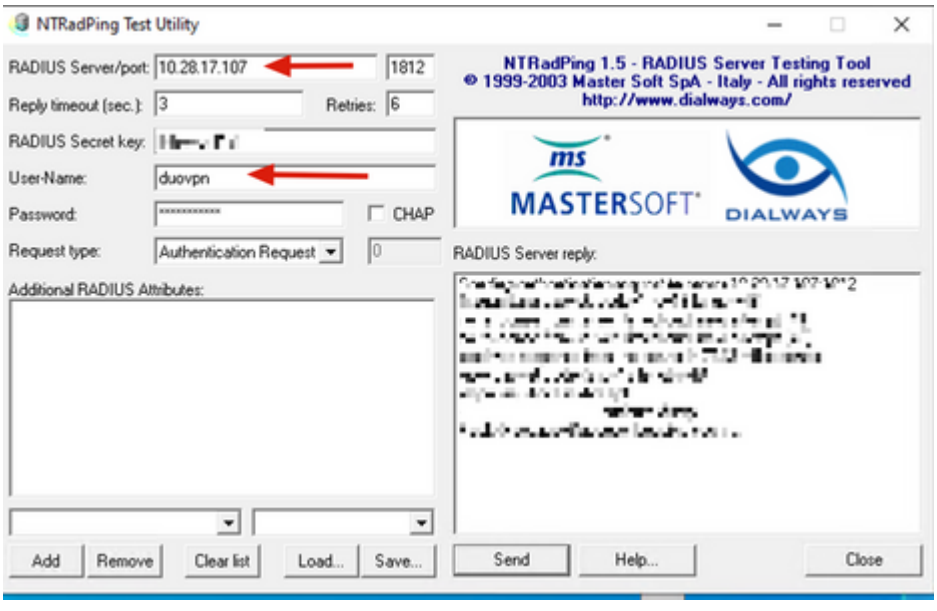


6. Para confirmar que el servidor proxy de autenticación Duo funciona, Duo proporciona la herramienta NTRadPing para simular paquetes de solicitud de acceso y respuesta con Duo.

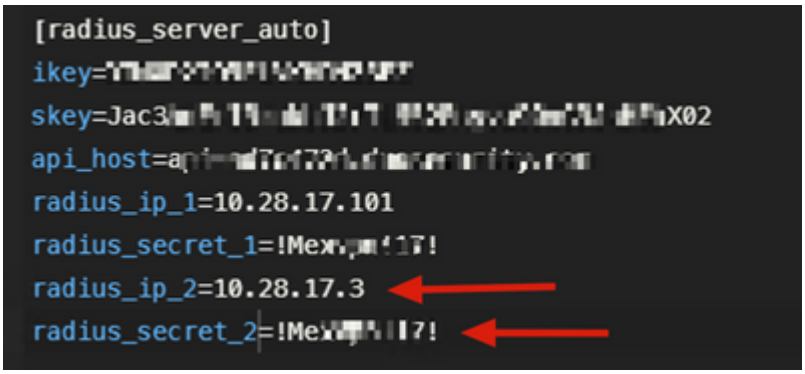
6.1 Instale NTRadPing en un equipo diferente y genere tráfico.

Nota: En este ejemplo se utiliza la máquina Windows 10.28.17.3.

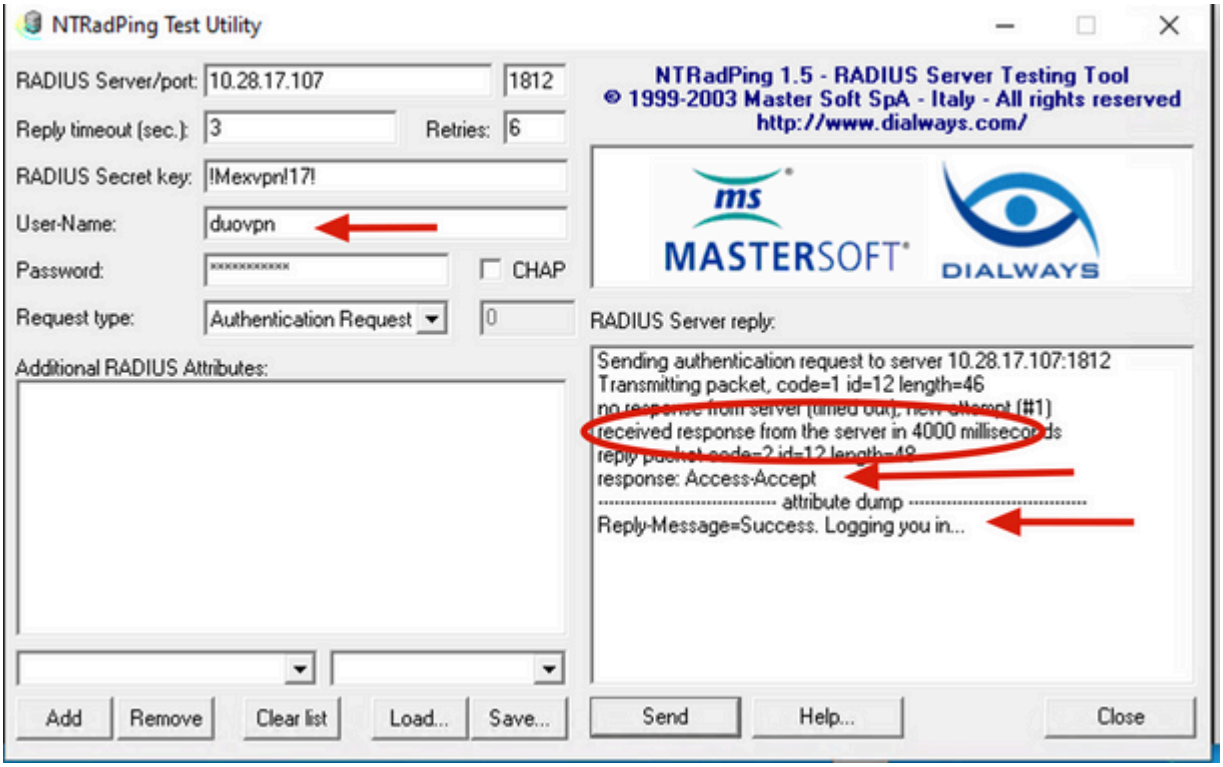
6.2 Configure con los atributos utilizados en la configuración de ISE Radius.

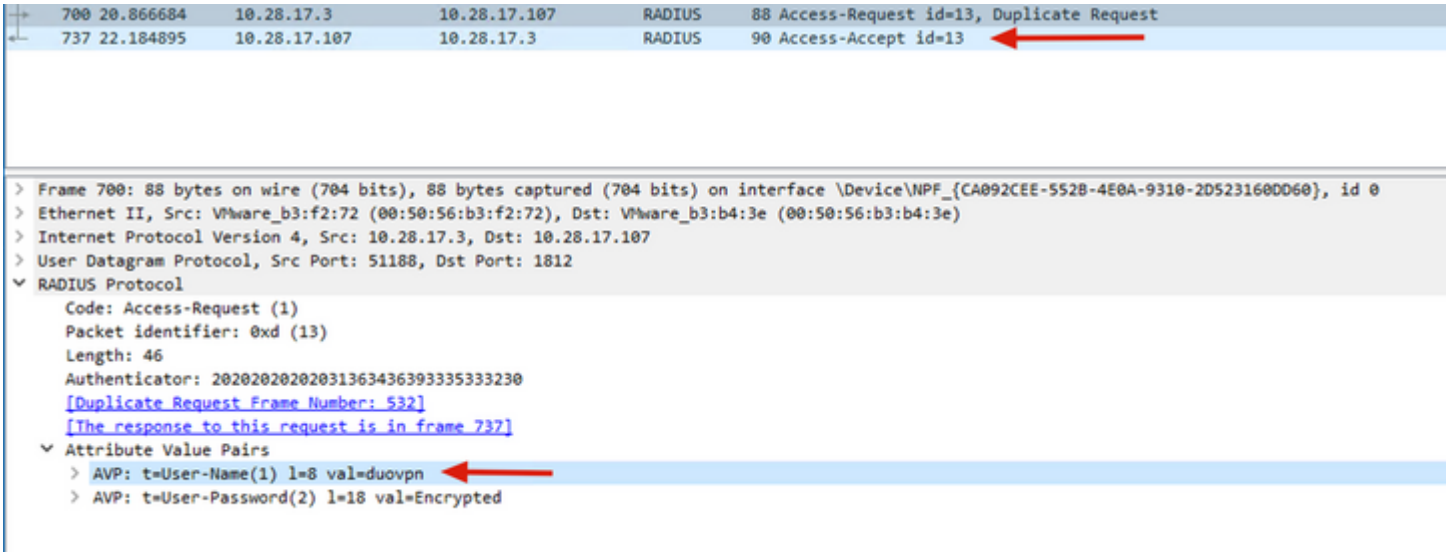


6.3 Configure Duo Authentication Proxy Manager de la siguiente manera.



6.4. Desplácese hasta la herramienta NTRadPing y haga clic en **Enviar**. Recibirá una notificación de inserción Duo en el dispositivo móvil asignado.





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).