Configuración y administración de cuentas de usuario en un router serie RV34x

Objetivo

El objetivo de este artículo es mostrarle cómo configurar y administrar las cuentas de usuario locales y remotas en un RV34x Series Router. Esto incluye, cómo configurar la complejidad de la contraseña de los usuarios locales, configurar/editar/importar usuarios locales, configurar el servicio de autenticación remota usando RADIUS, Active Directory y LDAP.

Dispositivos aplicables | Versión del firmware

- Serie RV34x | 1.0.01.16 (Descarga más reciente)

Introducción

El router serie RV34x proporciona cuentas de usuario para ver y administrar los parámetros. Los usuarios pueden pertenecer a diferentes grupos o a grupos lógicos de redes privadas virtuales (VPN) de capa de conexión segura (SSL) que comparten el dominio de autenticación, la red de área local (LAN) y las reglas de acceso a servicios, así como la configuración de tiempo de espera inactivo. La administración de usuarios define qué tipo de usuarios pueden utilizar un determinado tipo de recurso y cómo se puede hacer.

La prioridad de la base de datos externa siempre es Servicio de usuario de acceso telefónico de autenticación remota (RADIUS)/Protocolo ligero de acceso a directorios (LDAP)/Directorio activo (AD)/Local. Si agrega el servidor RADIUS en el router, el servicio de inicio de sesión web y otros servicios utilizarán la base de datos externa RADIUS para autenticar al usuario.

No hay ninguna opción para habilitar una base de datos externa para el servicio de inicio de sesión web solo y configurar otra base de datos para otro servicio. Una vez que se crea RADIUS y se habilita en el router, el router utilizará el servicio RADIUS como base de datos externa para el inicio de sesión web, VPN de sitio a sitio, VPN EzVPN/de terceros, VPN SSL, VPN de protocolo de transporte punto a punto (PPTP)/VPN de protocolo de transporte de capa 2 (L2TP) y 802.1x.

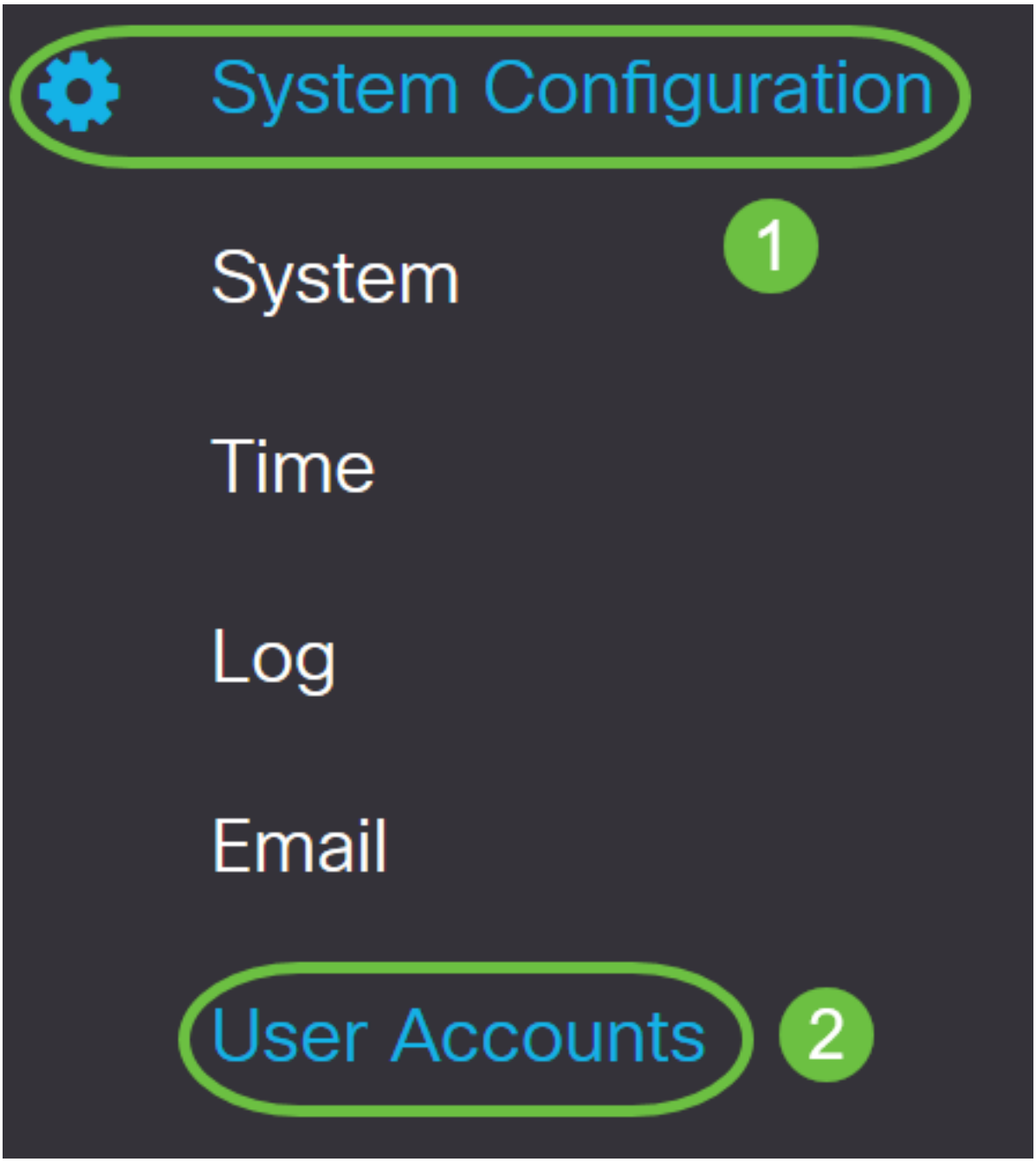
Table Of Contents

- Configurar una cuenta de usuario local
- Complejidad de la contraseña de los usuarios locales
- Configurar usuarios locales
- Editar usuarios locales
- Importar usuarios locales
- Configuración del servicio de autenticación remota
- RADIUS
- Configuración de Active Directory
- Integración de Active Directory
- Configuración de integración de Active Directory
- LDAP

Configurar una cuenta de usuario local

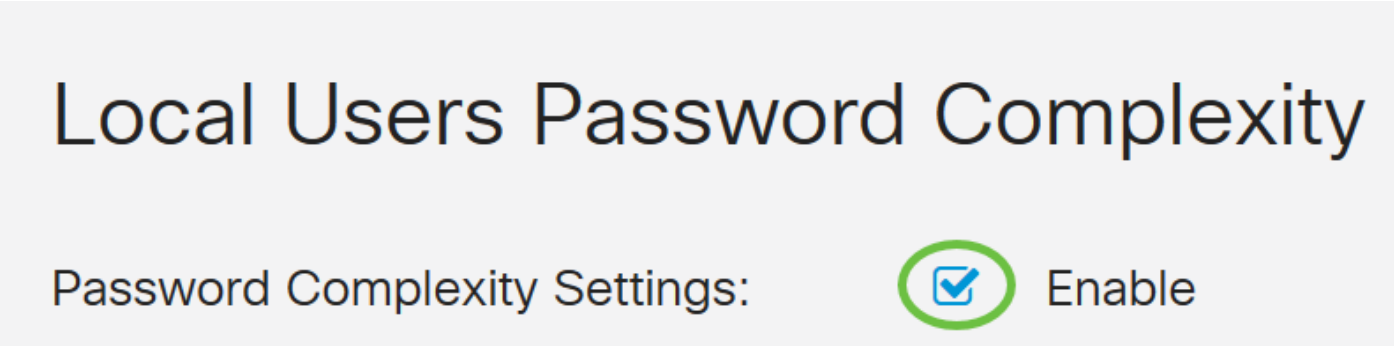
Complejidad de la contraseña de los usuarios locales

Paso 1. Inicie sesión en la utilidad basada en web del router y elija **Configuración del sistema > Cuentas de usuario**.



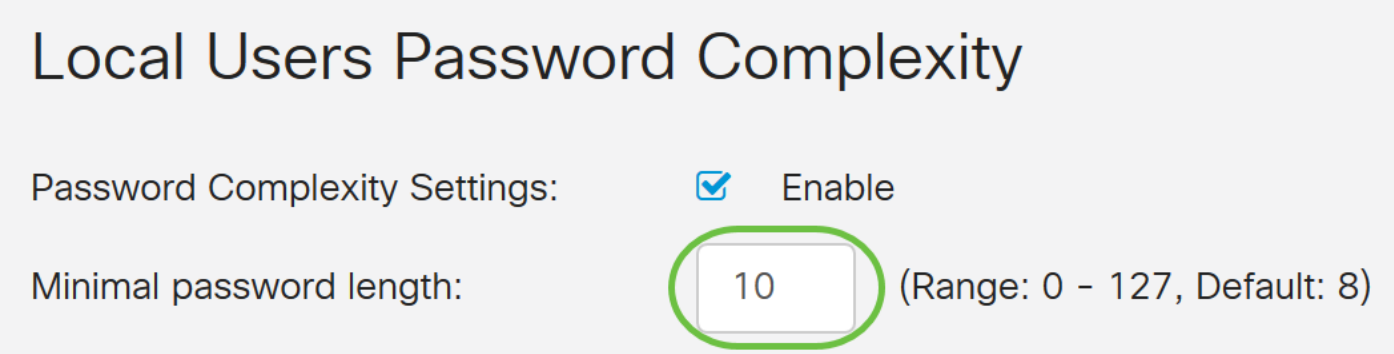
Paso 2. Marque la casilla de verificación **Enable Password Complexity Settings** para habilitar los parámetros de complejidad de la contraseña.

Si no se marca, vaya directamente a Configurar usuarios locales.



Paso 3. En el campo *Longitud mínima de la contraseña*, introduzca un número entre 0 y 127 para establecer el número mínimo de caracteres que debe contener una contraseña. El valor predeterminado es 8.

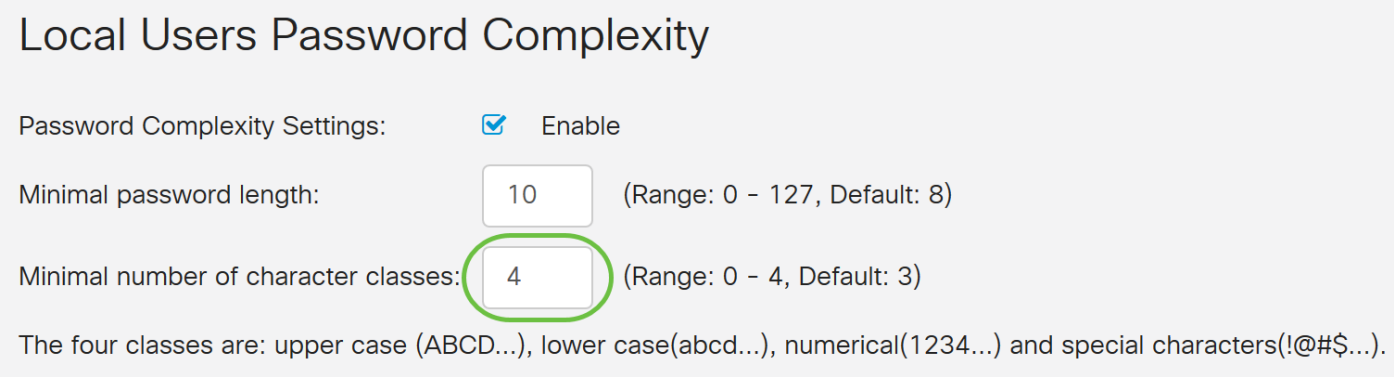
Para este ejemplo, el número mínimo de caracteres se establece en **10**.



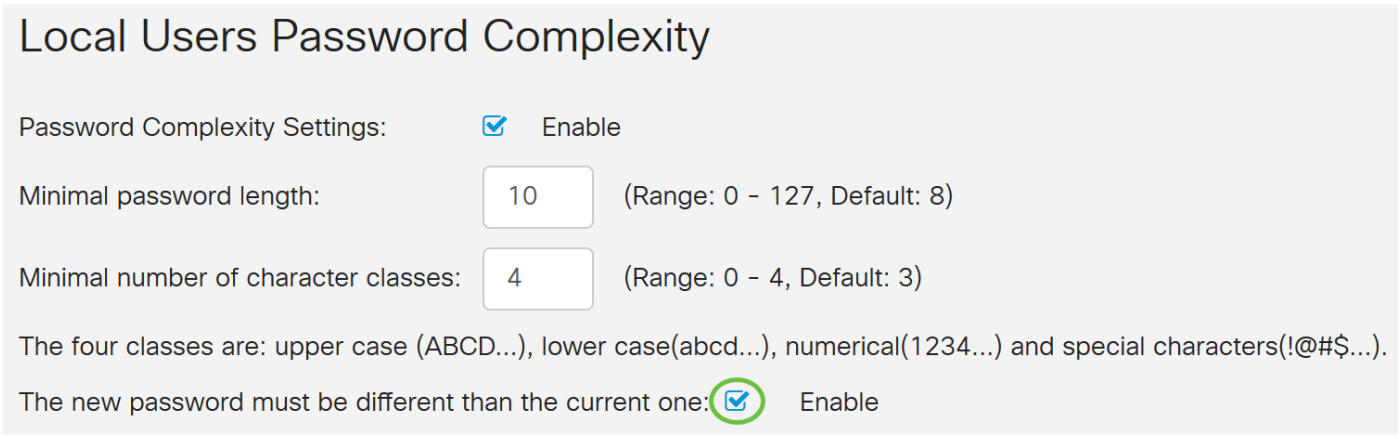
Paso 4. En el campo *Número mínimo de clases de caracteres*, introduzca un número entre 0 y 4 para establecer la clase. El número introducido representa el número de caracteres mínimo o máximo de las diferentes clases:

- La contraseña consta de caracteres en mayúsculas (ABCD).
- La contraseña consta de caracteres en minúsculas (abcd).
- La contraseña consta de caracteres numéricos (1234).
- La contraseña consta de caracteres especiales (!@#$).

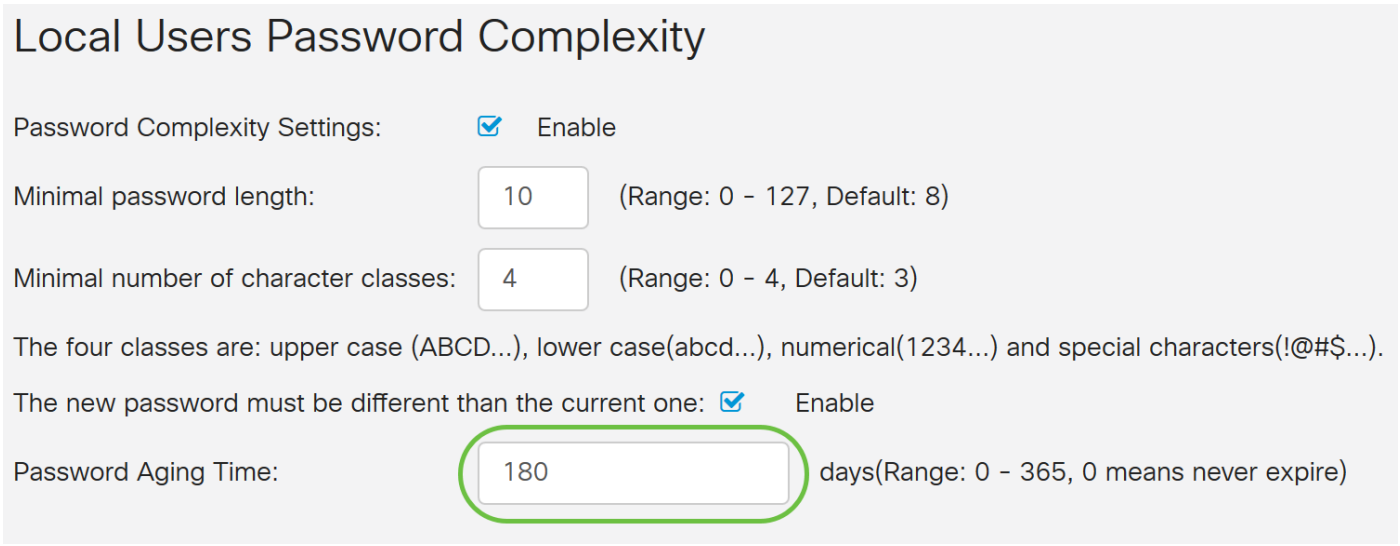
En este ejemplo, se utiliza **4**.



Paso 5. Marque la casilla de verificación **Enable** para que la nueva contraseña sea diferente a la actual.



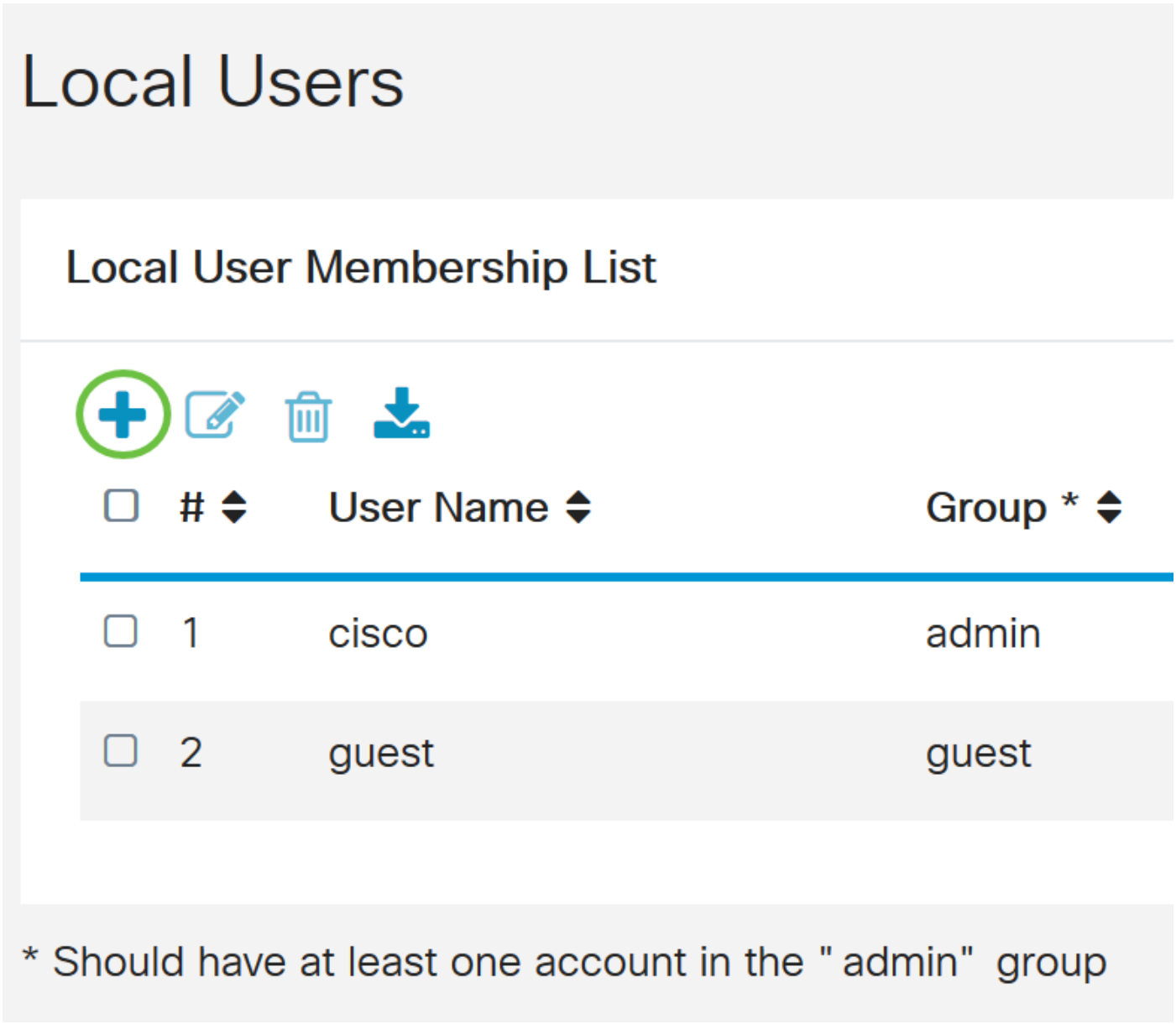
Paso 6. En el campo *Password Ageing Time (Tiempo de caducidad de la contraseña)*, introduzca el número de días (0 - 365) para la caducidad de la contraseña. En este ejemplo, se han introducido **180** días.



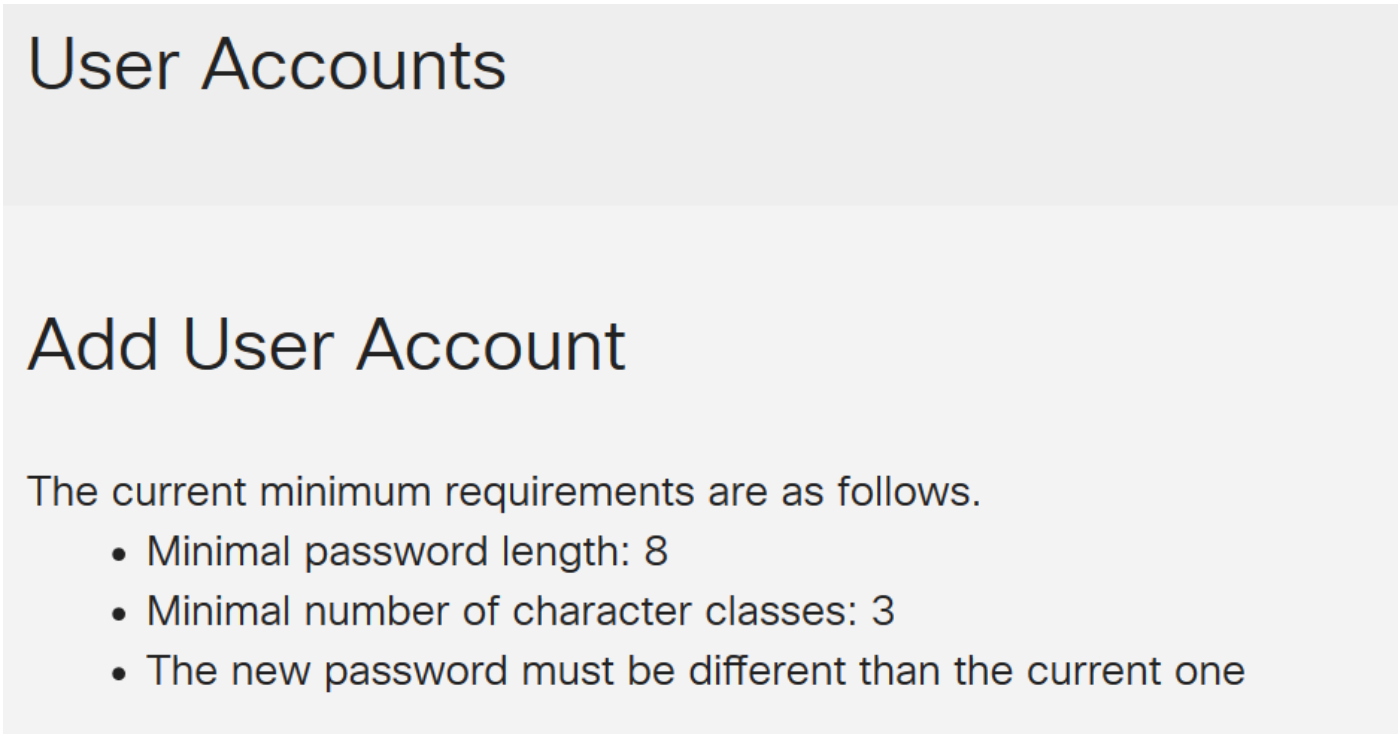
Ahora ha configurado correctamente los parámetros de complejidad de contraseña de usuario local en el router.

Configurar usuarios locales

Paso 1. En la tabla Lista de miembros de usuario local, haga clic en **Agregar** para crear una nueva cuenta de usuario. Accederá a la página Agregar cuenta de usuario.

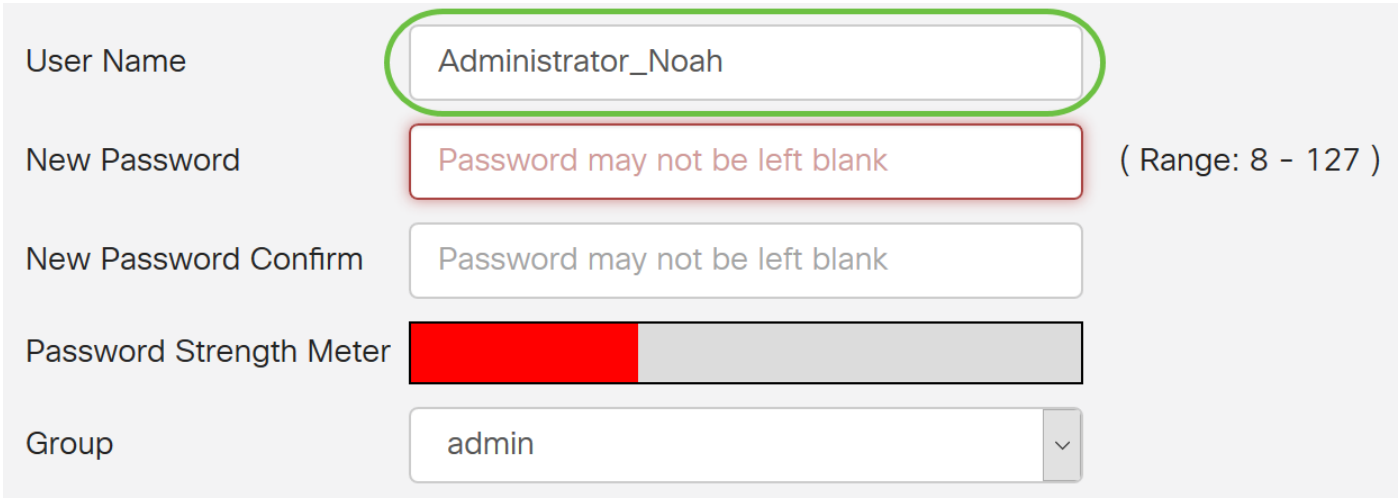


En el encabezado *Add User Account*, se muestran los parámetros definidos en los pasos Local Password Complexity (Complejidad de la contraseña local).

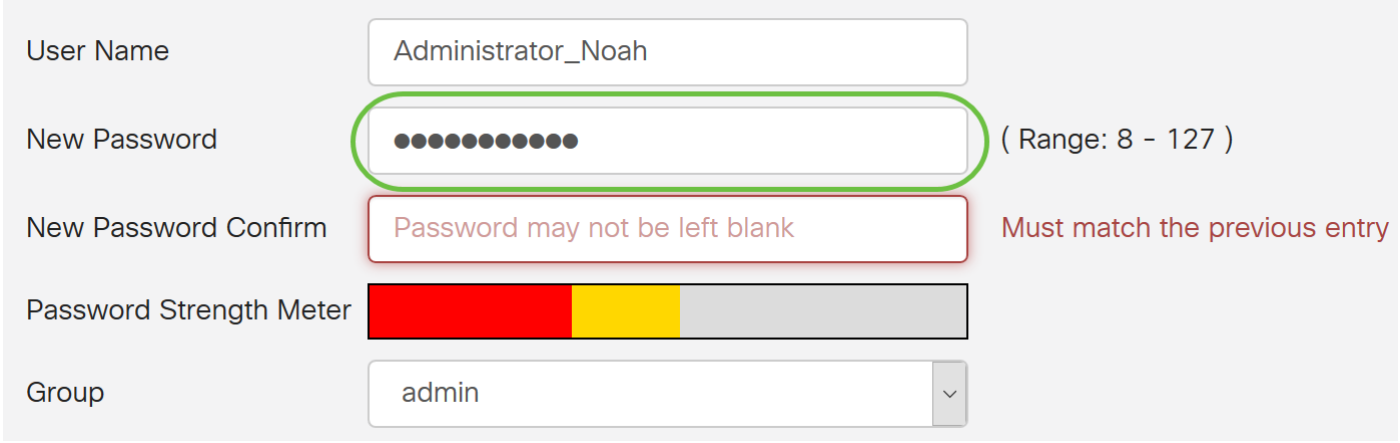


Paso 2. En el campo *User Name*, ingrese un nombre de usuario para la cuenta.

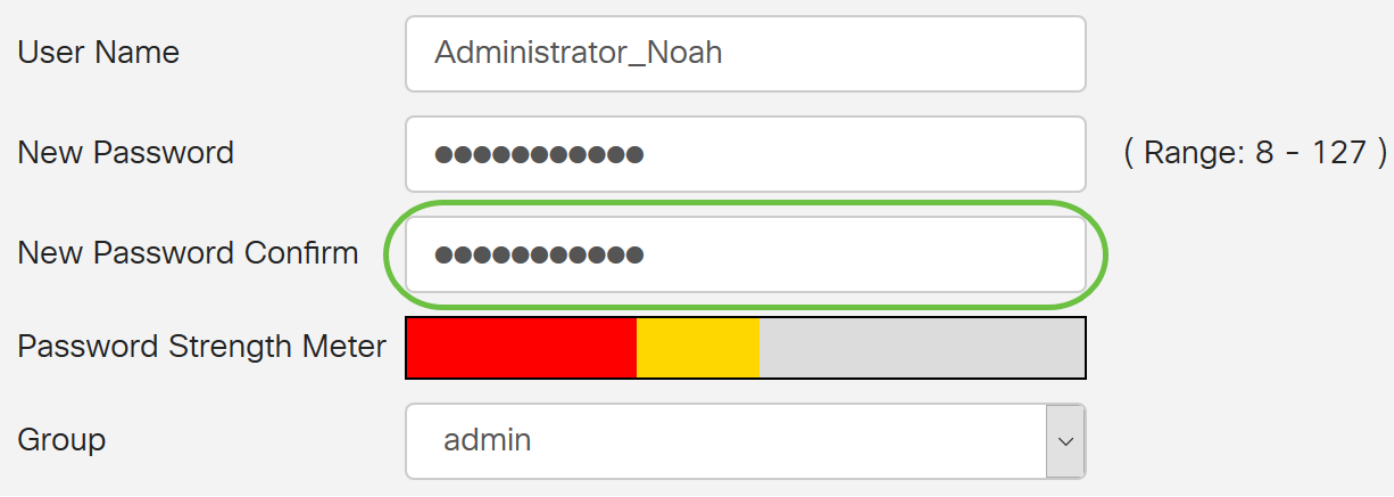
En este ejemplo, se utiliza **Administrator_Noah**.



Paso 3. En el campo *New Password*, ingrese una contraseña con los parámetros definidos. En este ejemplo, la longitud mínima de la contraseña debe constar de 10 caracteres con una combinación de mayúsculas, minúsculas, números y caracteres especiales.



Paso 4. En el campo *Confirmar contraseña nueva*, vuelva a introducir la contraseña para confirmarla. Si las contraseñas no coinciden, aparecerá un texto junto al campo.

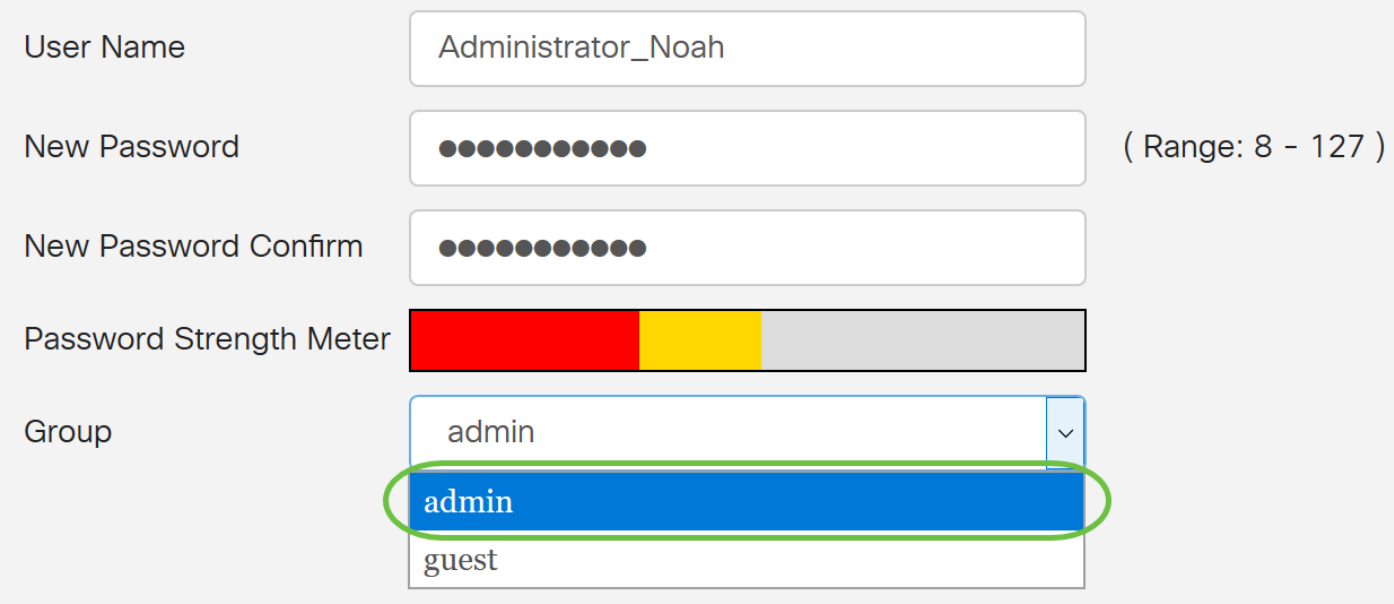


El medidor de fuerza de contraseña cambia en función de la fuerza de la contraseña.

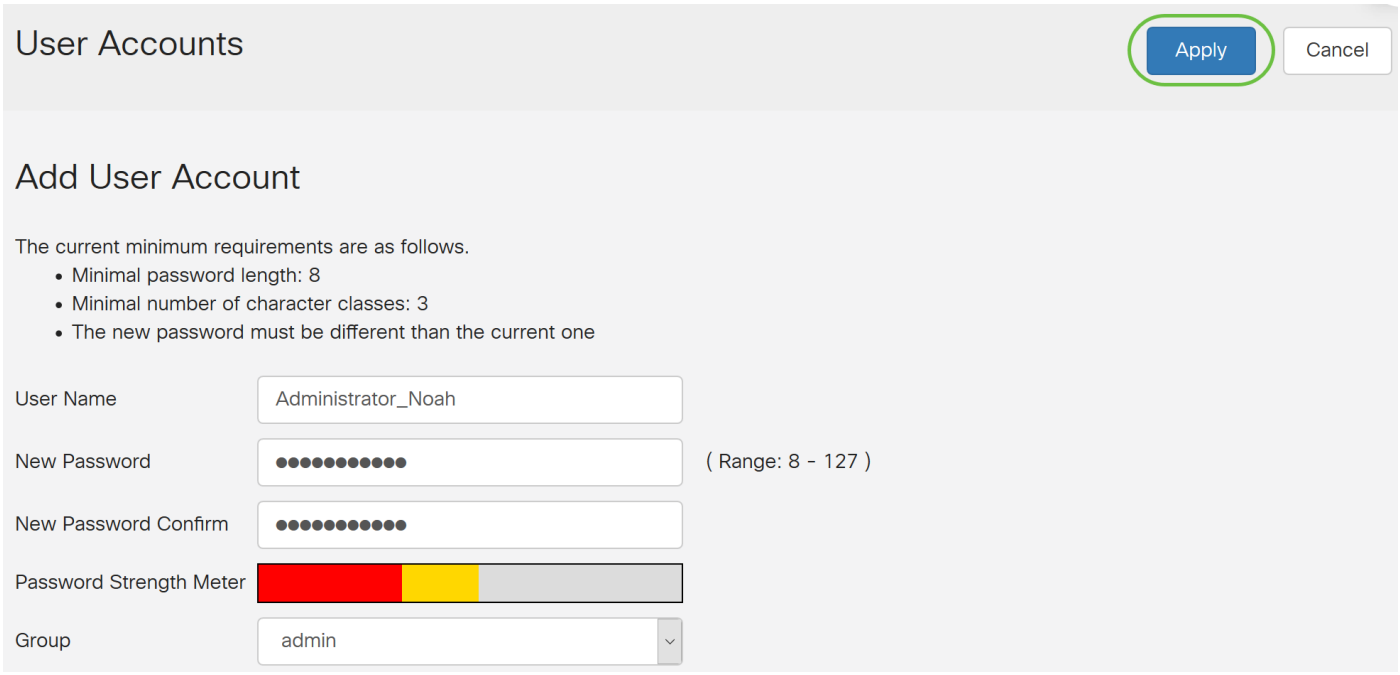
Paso 5. En la lista desplegable *Grupo*, elija un grupo para asignar un privilegio a una cuenta de usuario. Las opciones son:

- admin - Privilegios de lectura y escritura.
- guest (invitado): privilegios de sólo lectura.

Para este ejemplo, se elige **admin**.



Paso 6. Haga clic en Apply (Aplicar).

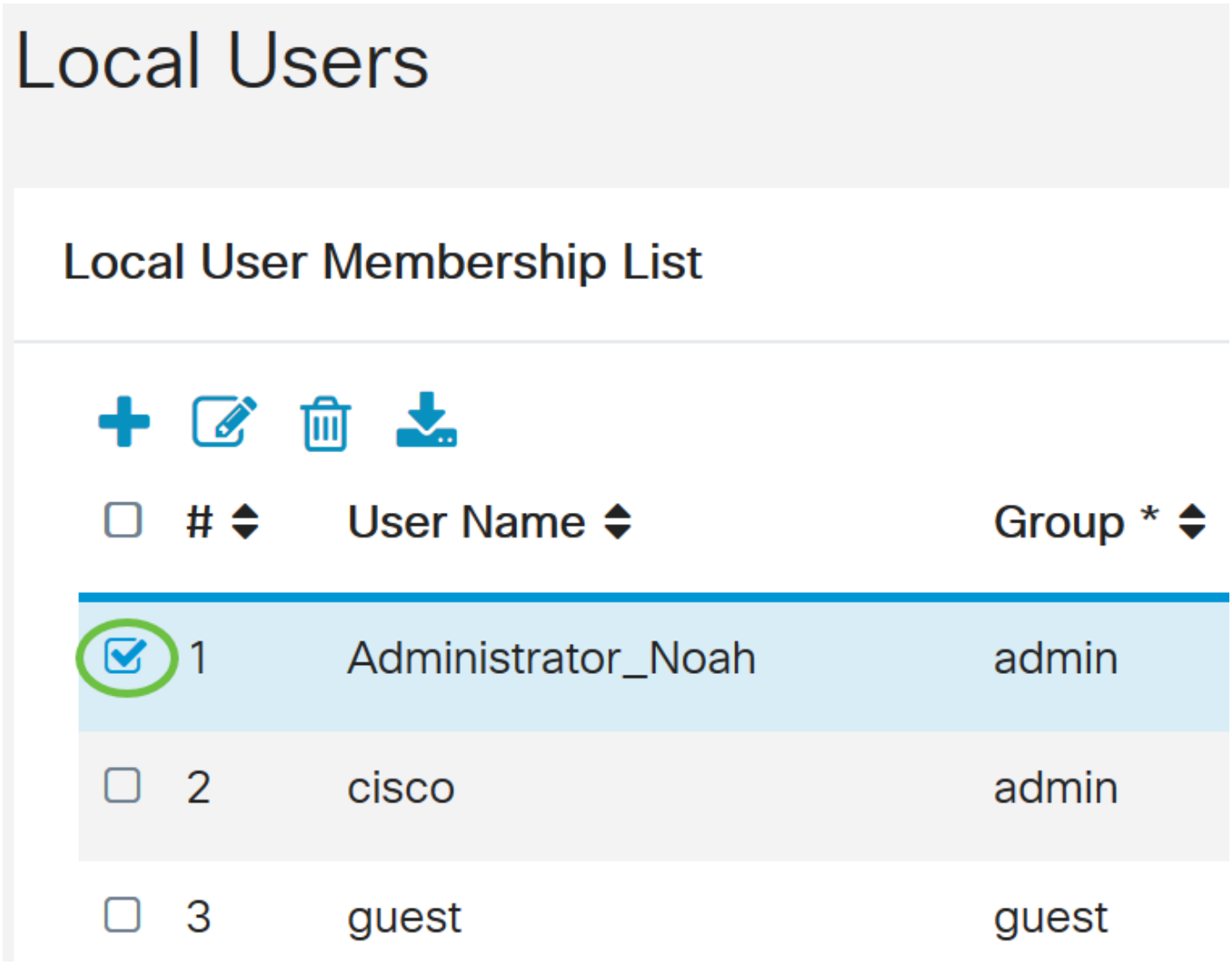


Ahora ha configurado correctamente la pertenencia del usuario local en un router serie RV34x.

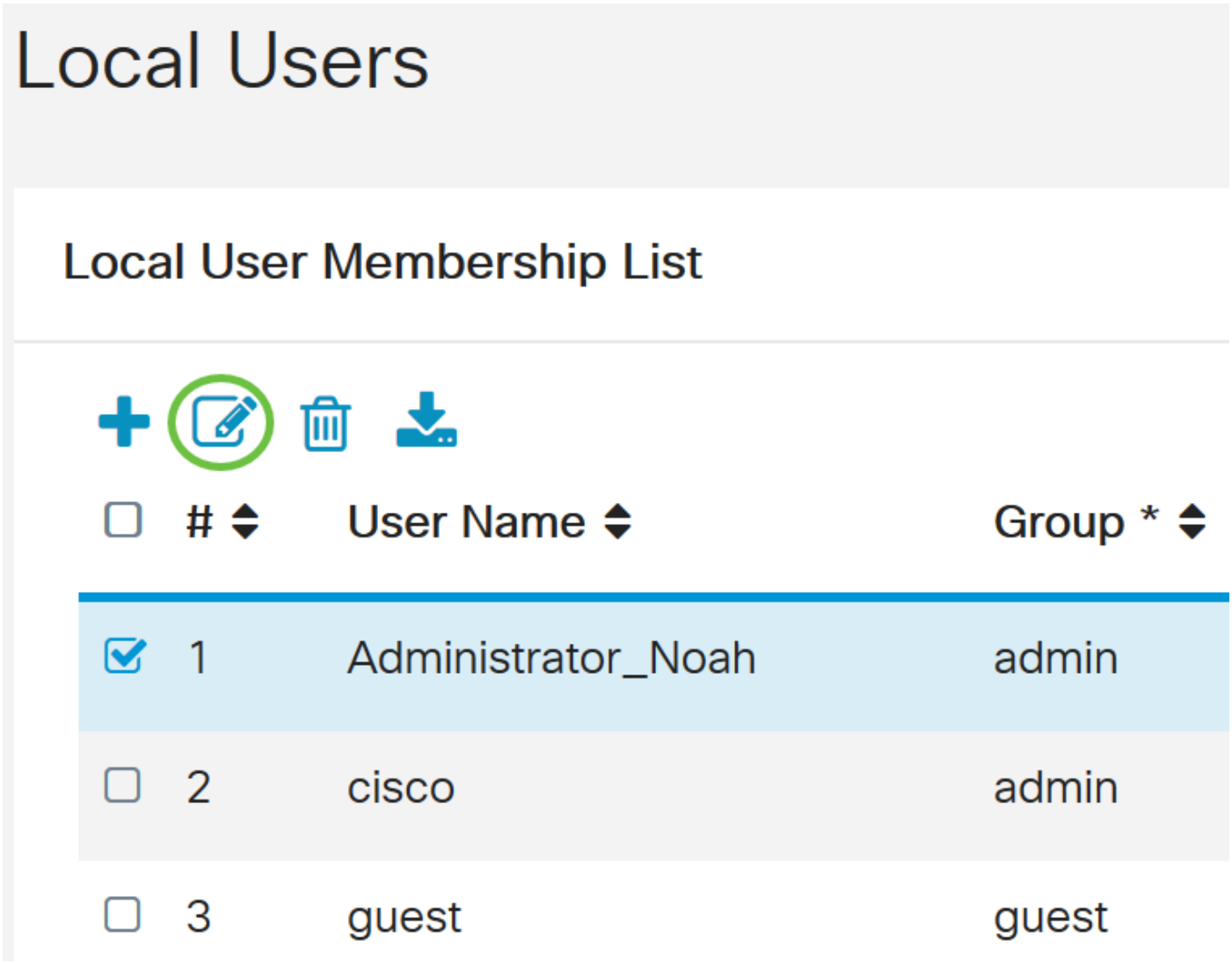
Editar usuarios locales

Paso 1. Active la casilla de verificación junto al nombre de usuario del usuario local en la tabla Lista de suscripciones de usuario local.

Para este ejemplo, se elige **Administrator_Noah**.

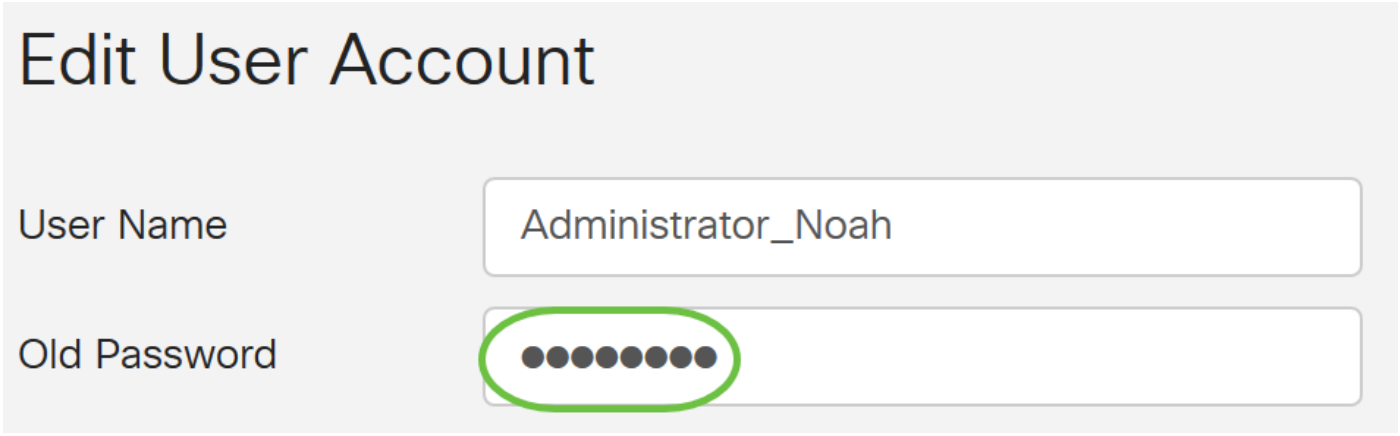


Paso 2. Haga clic en **Editar**.

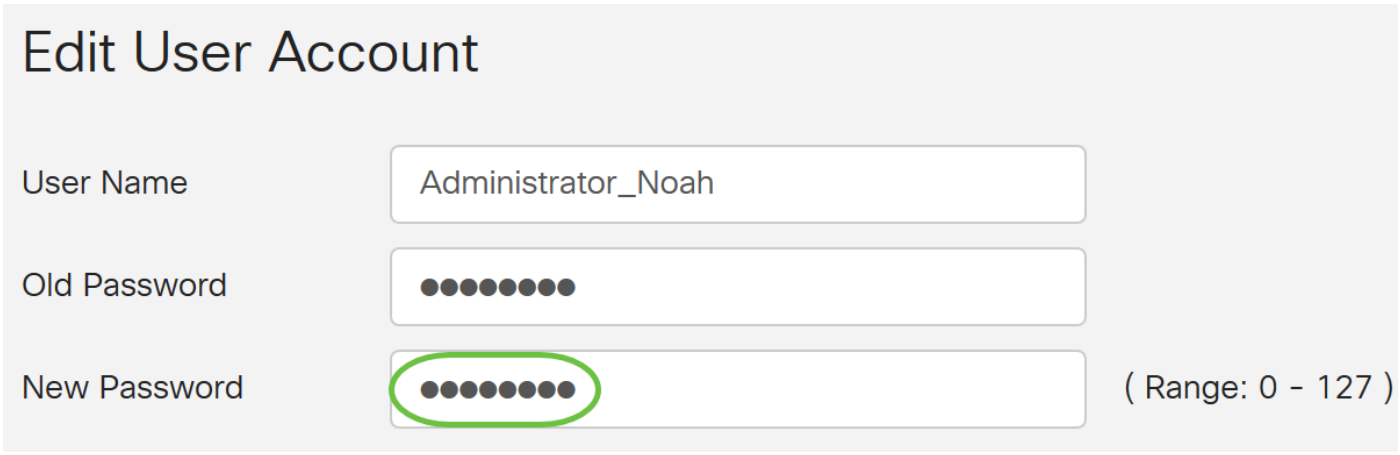


No se puede editar el nombre de usuario.

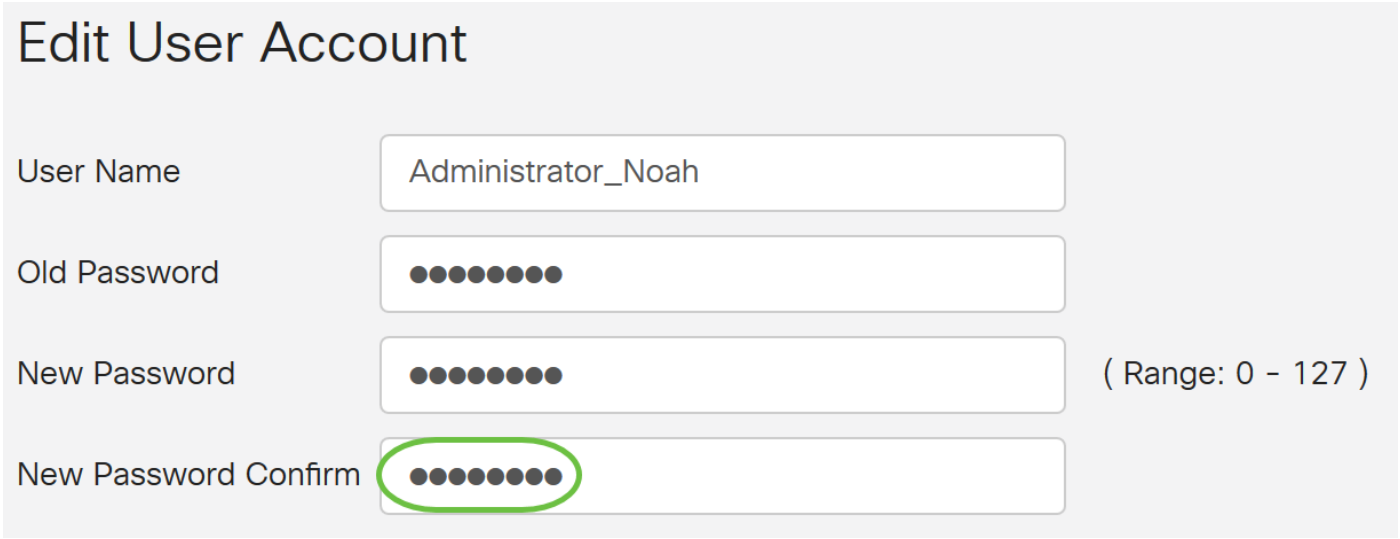
Paso 3. En el campo *Contraseña antigua*, ingrese la contraseña que se configuró previamente para la cuenta de usuario local.



Paso 4. En el campo *New Password*, ingrese una nueva contraseña. La nueva contraseña debe cumplir los requisitos mínimos.

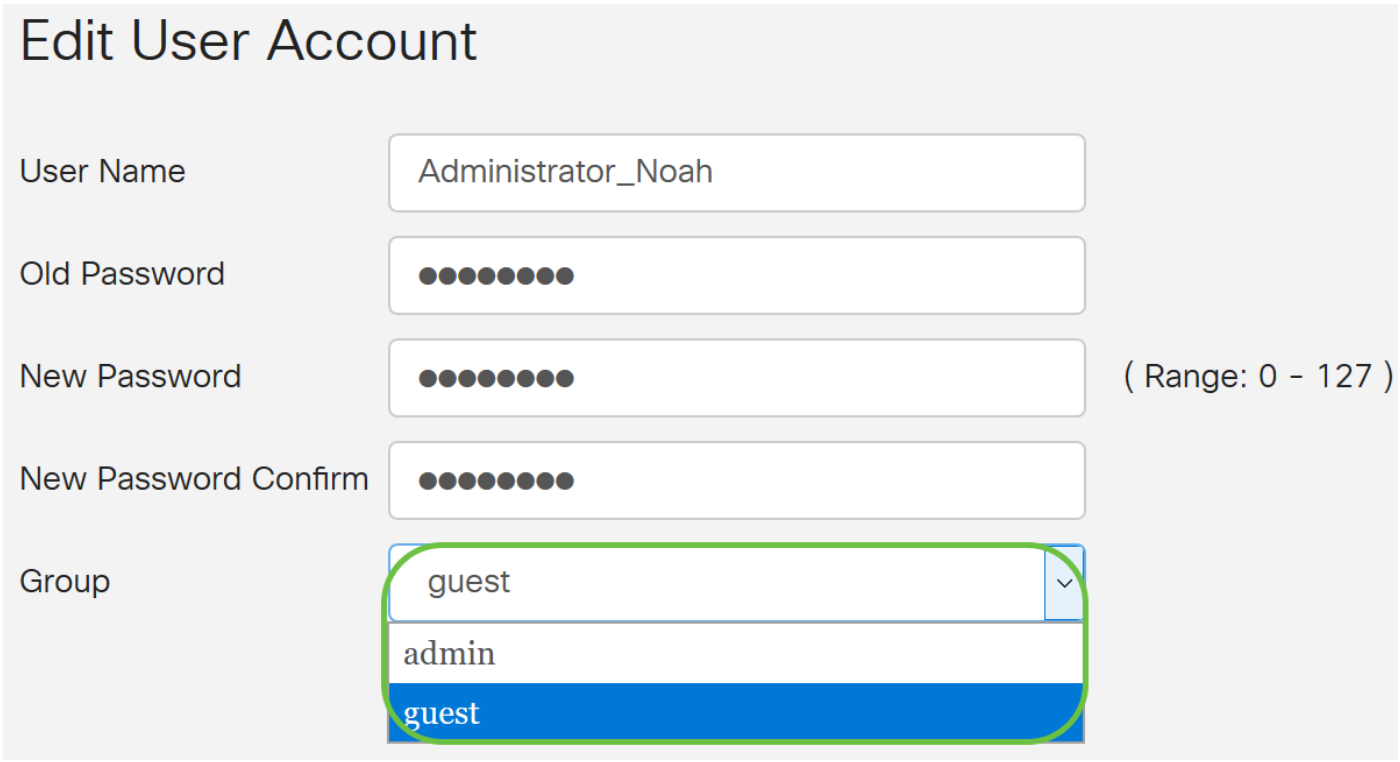


Paso 5. Ingrese la nueva contraseña una vez más en el campo *Confirmar contraseña nueva* para confirmarla. Estas contraseñas deben coincidir.

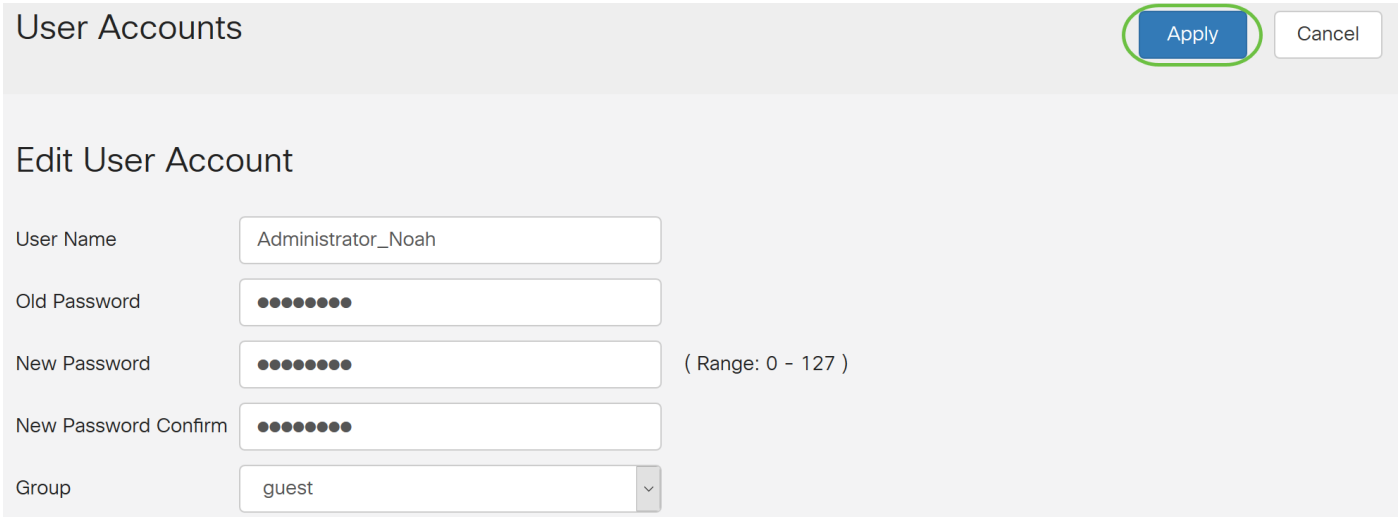


Paso 6. (Opcional) En la lista desplegable Grupo, elija un grupo para asignar un privilegio a una cuenta de usuario.

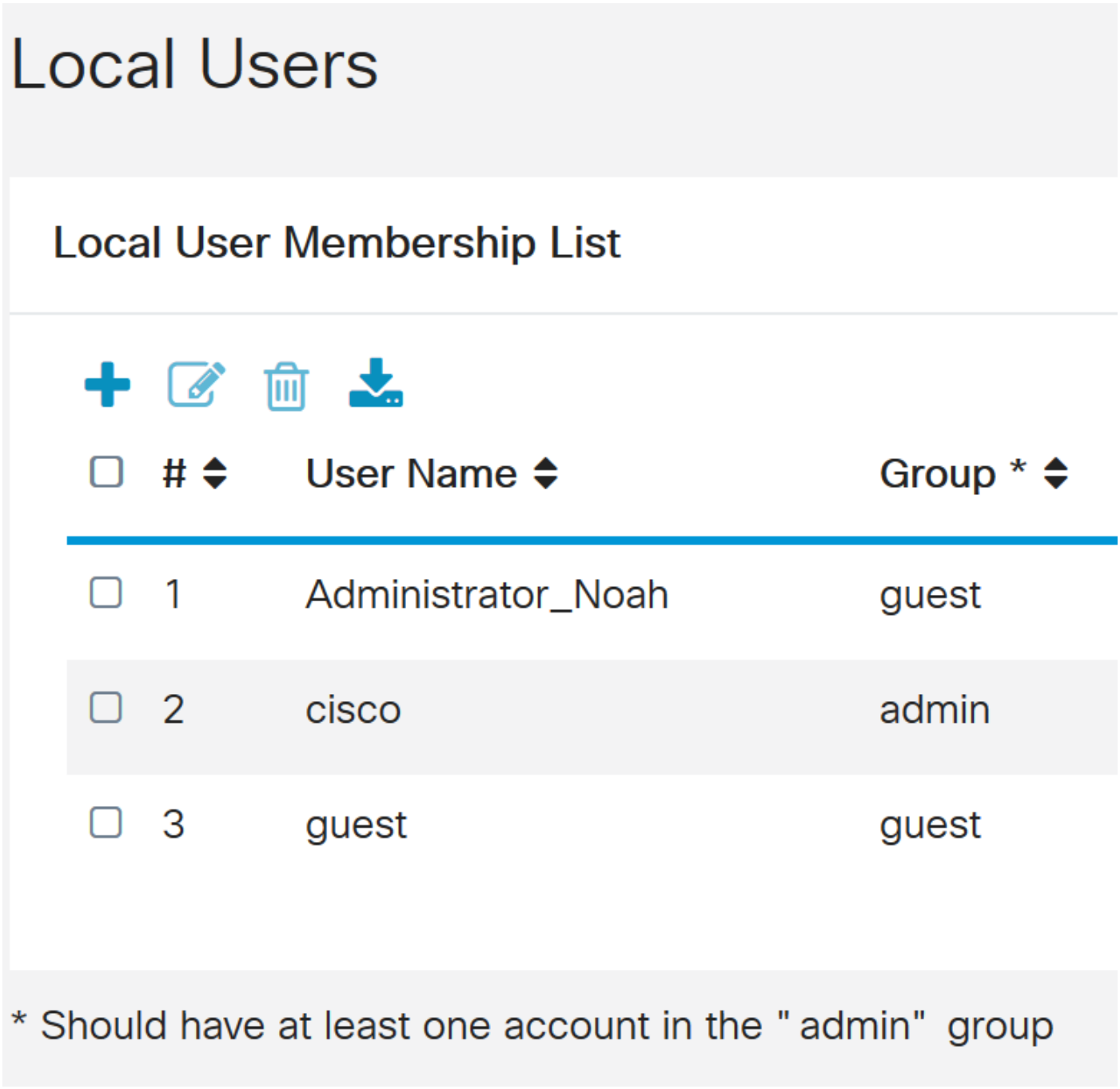
En este ejemplo, se elige **invitado**.



Paso 7. Haga clic en Apply (Aplicar).



Ahora debería haber editado correctamente una cuenta de usuario local.

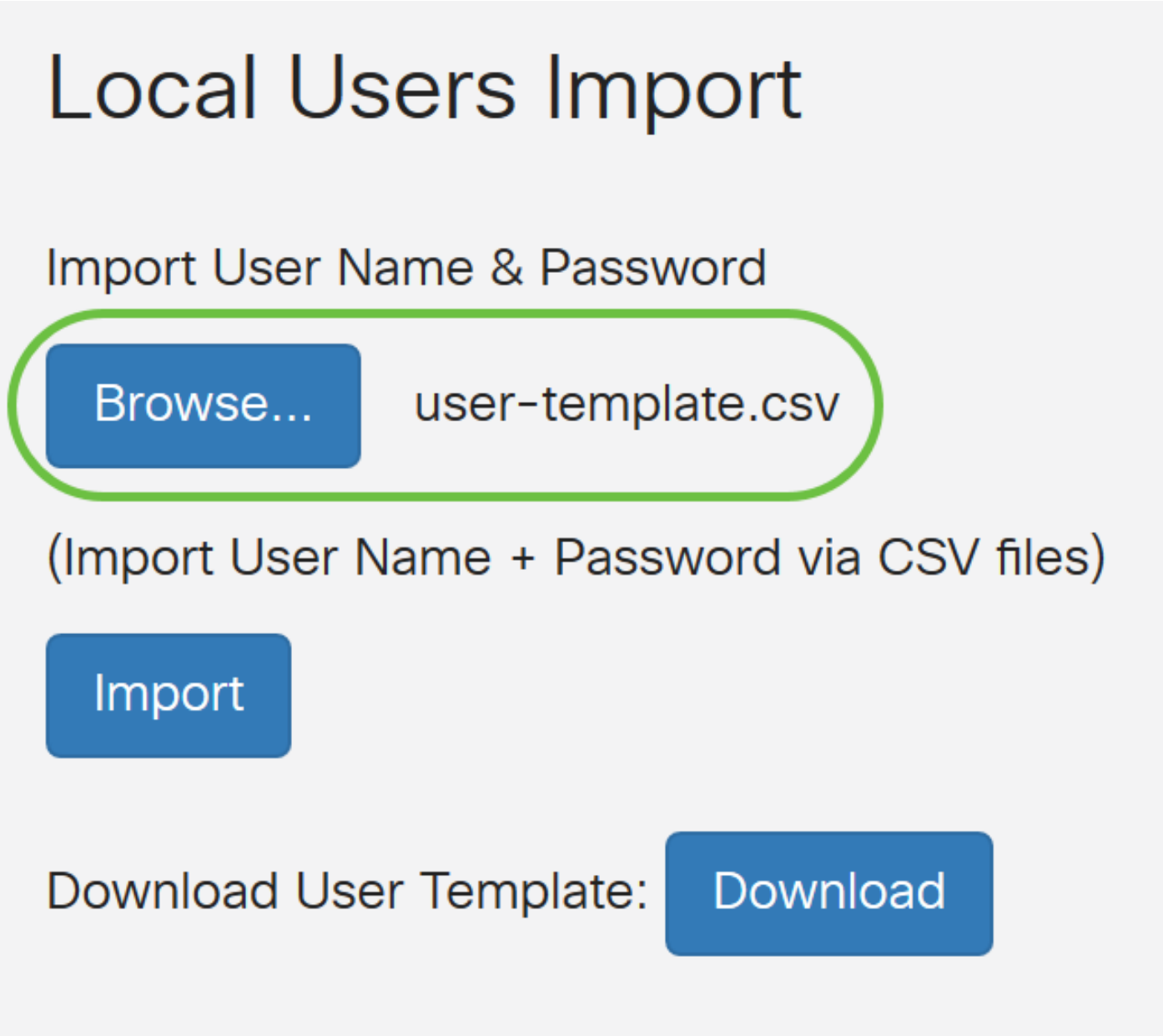


Importar usuarios locales

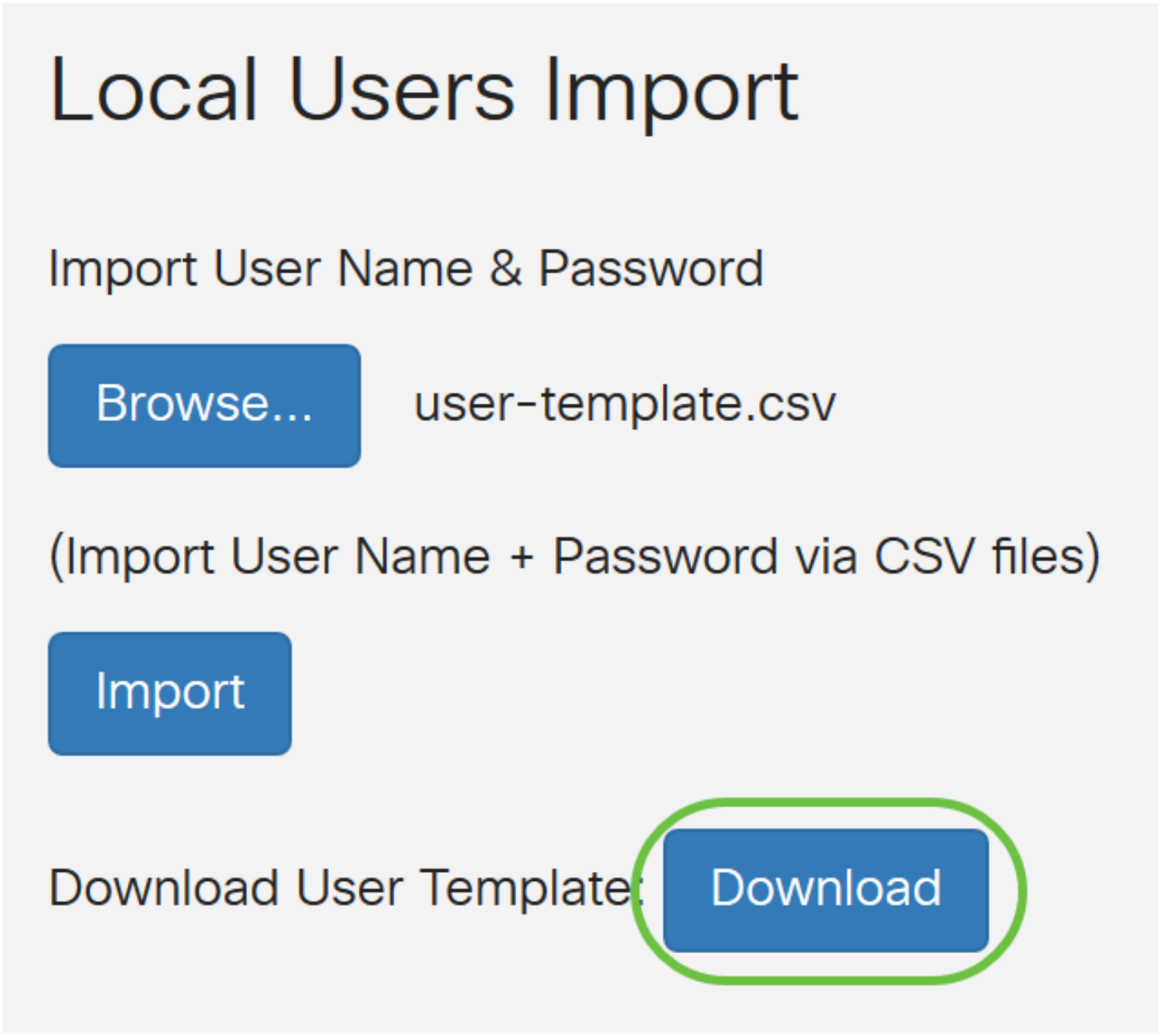
Paso 1. En el área Importación de usuarios locales, haga clic  .

Paso 2. En Importar nombre de usuario y contraseña, haga clic en **Examinar...** para importar una lista de usuarios. Este archivo suele ser una hoja de cálculo guardada en formato de valor separado por comas (.CSV).

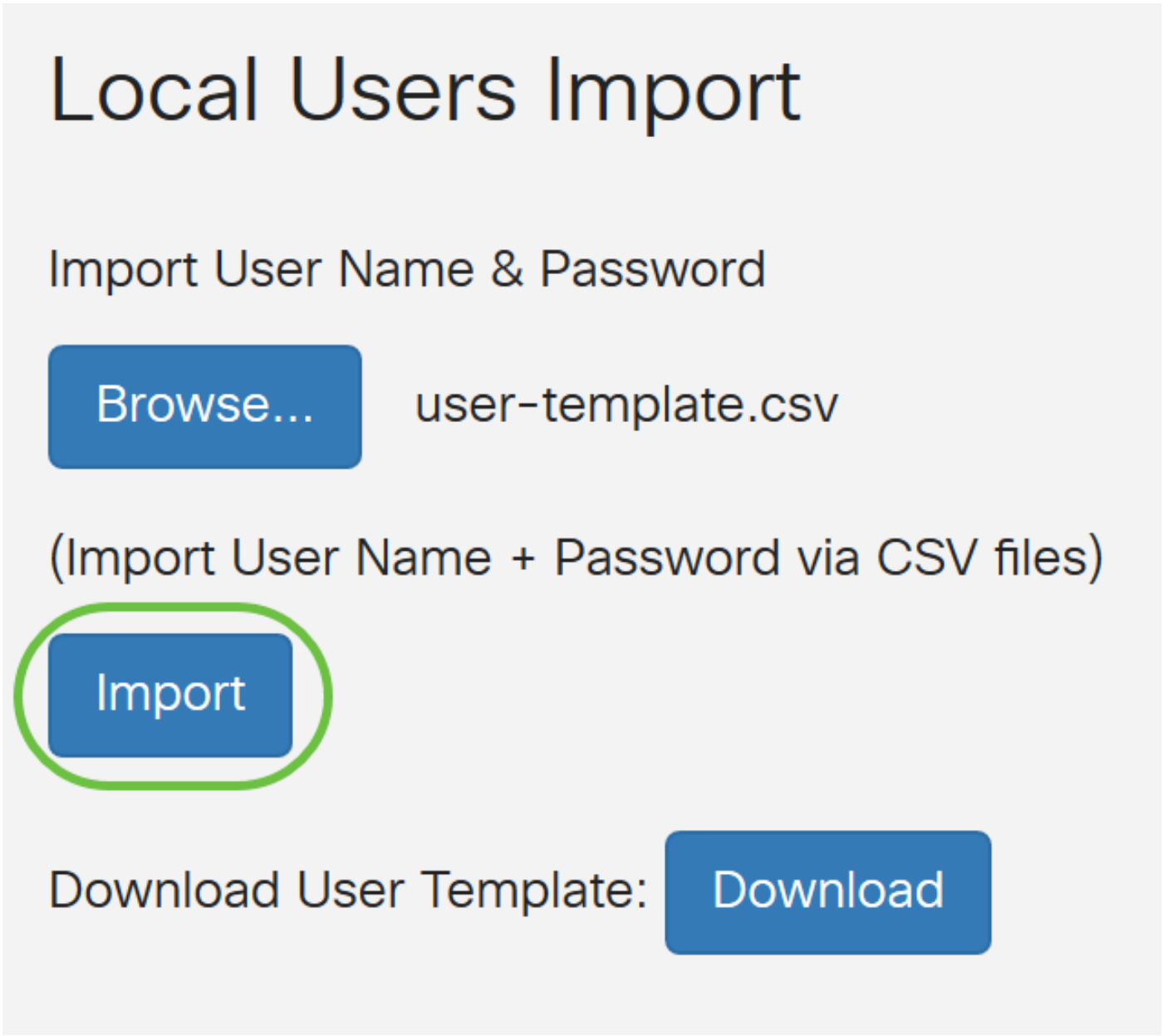
En este ejemplo, se elige **user-template.csv**.



Paso 3. (Opcional) Si no tiene una plantilla, haga clic en **Descargar** en el área Descargar plantilla de usuario.



Paso 4. Haga clic en **Importar**.



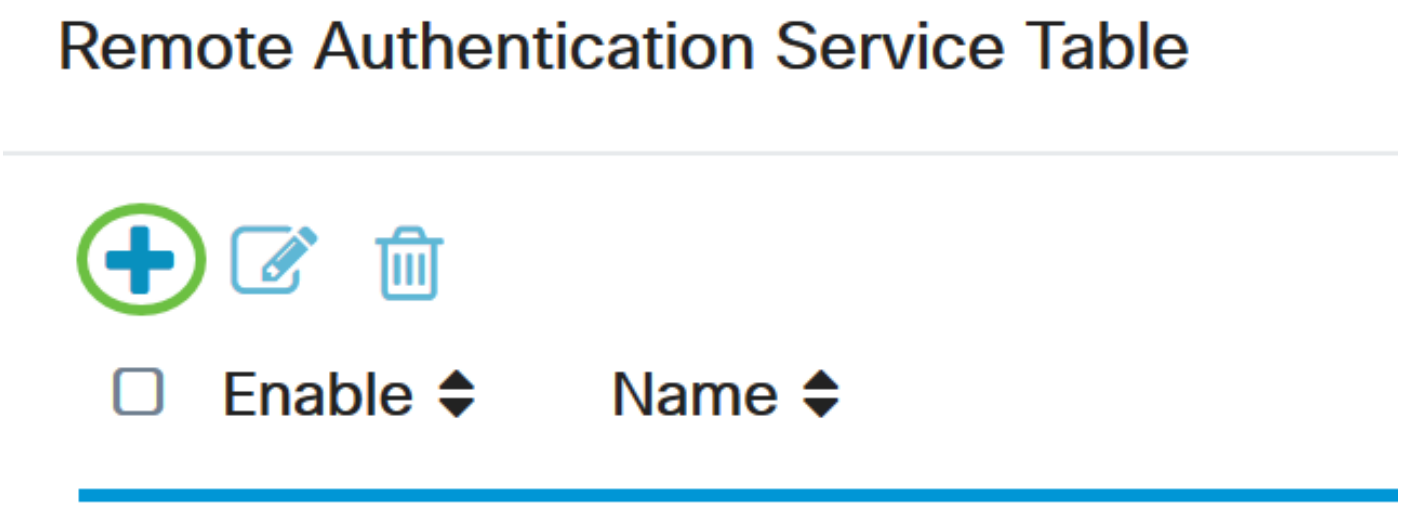
Aparecerá un mensaje junto al botón de importación que indica que la importación se ha realizado correctamente.

Ahora ha importado correctamente una lista de usuarios locales.

Configuración del servicio de autenticación remota

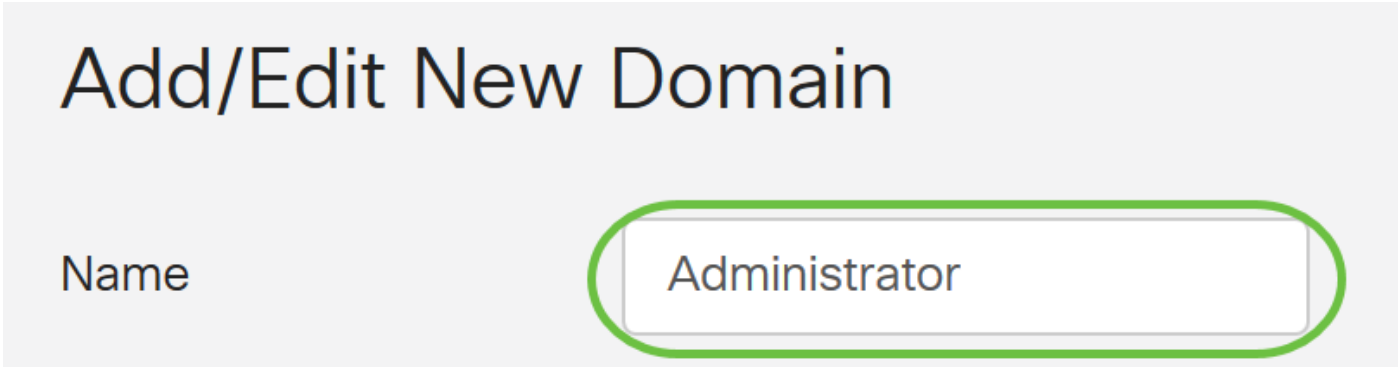
RADIUS

Paso 1. En la tabla Remote Authentication Service, haga clic en **Add** para crear una entrada.



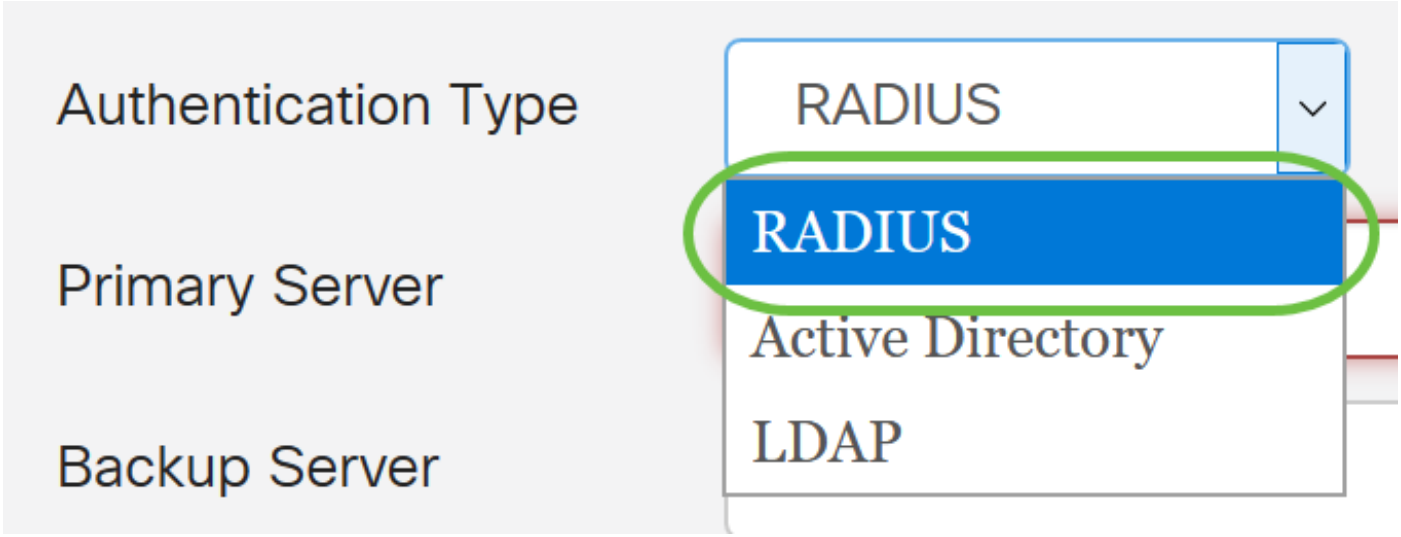
Paso 2. En el campo *Nombre*, cree un nombre de usuario para la cuenta.

Para este ejemplo, se utiliza **Administrator**.



Paso 3. En el menú desplegable Authentication Type , elija **Radius**. Esto significa que la autenticación de usuario se realizará a través de un servidor RADIUS.

Sólo se puede configurar una sola cuenta de usuario remota en RADIUS.



Paso 4. En el campo *Primary Server*, ingrese la dirección IP del servidor RADIUS primario.

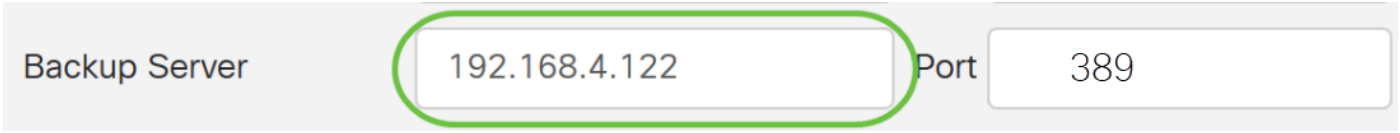
En este ejemplo, **192.168.3.122** se utiliza como servidor primario.

Paso 5. En el campo *Port*, ingrese el número de puerto del servidor RADIUS primario.

Para este ejemplo, **1645** se utiliza como número de puerto.

Paso 6. En el campo *Backup Server*, ingrese la dirección IP del servidor RADIUS de respaldo. Esto funciona como una conmutación por fallas en caso de que el servidor primario se desactive.

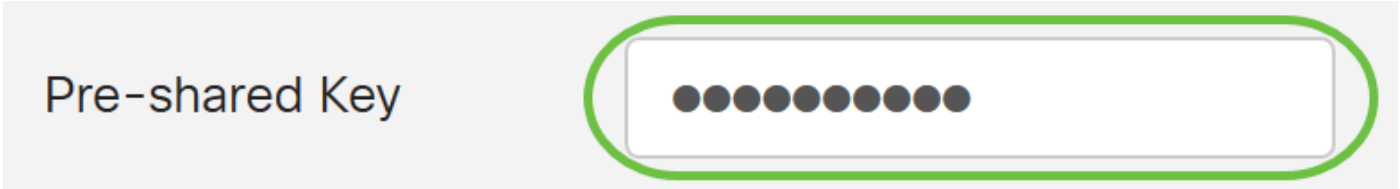
En este ejemplo, la dirección del servidor de respaldo es **192.168.4.122**.



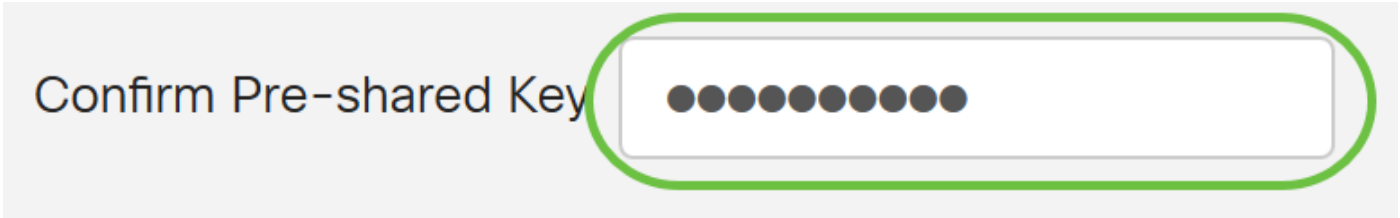
Paso 7. En el campo *Port*, ingrese el número de servidor RADIUS de respaldo.

En este ejemplo, **1646** se utiliza como número de puerto.

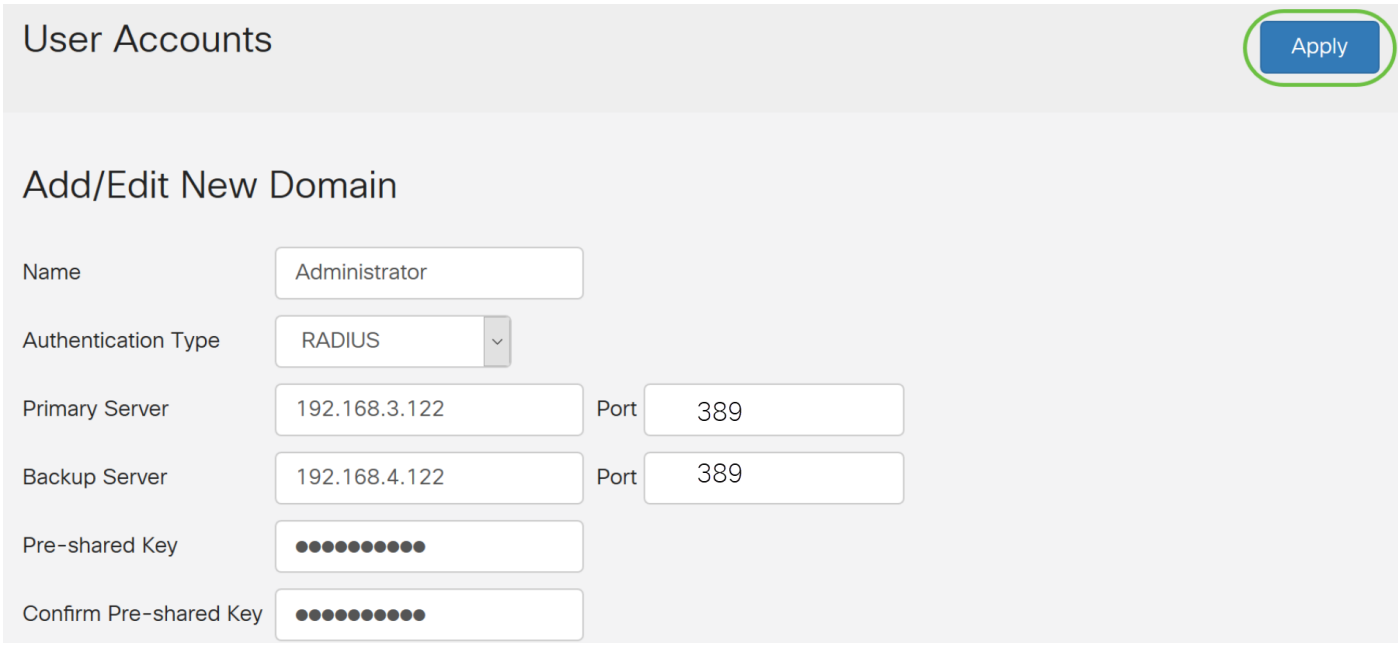
Paso 8. En el campo *Preshared -Key*, ingrese la clave previamente compartida que se configuró en el servidor RADIUS.



Paso 9. En el campo *Confirmar clave precompartida-key*, vuelva a ingresar la clave precompartida para confirmar.



Paso 10. Haga clic en Apply (Aplicar).

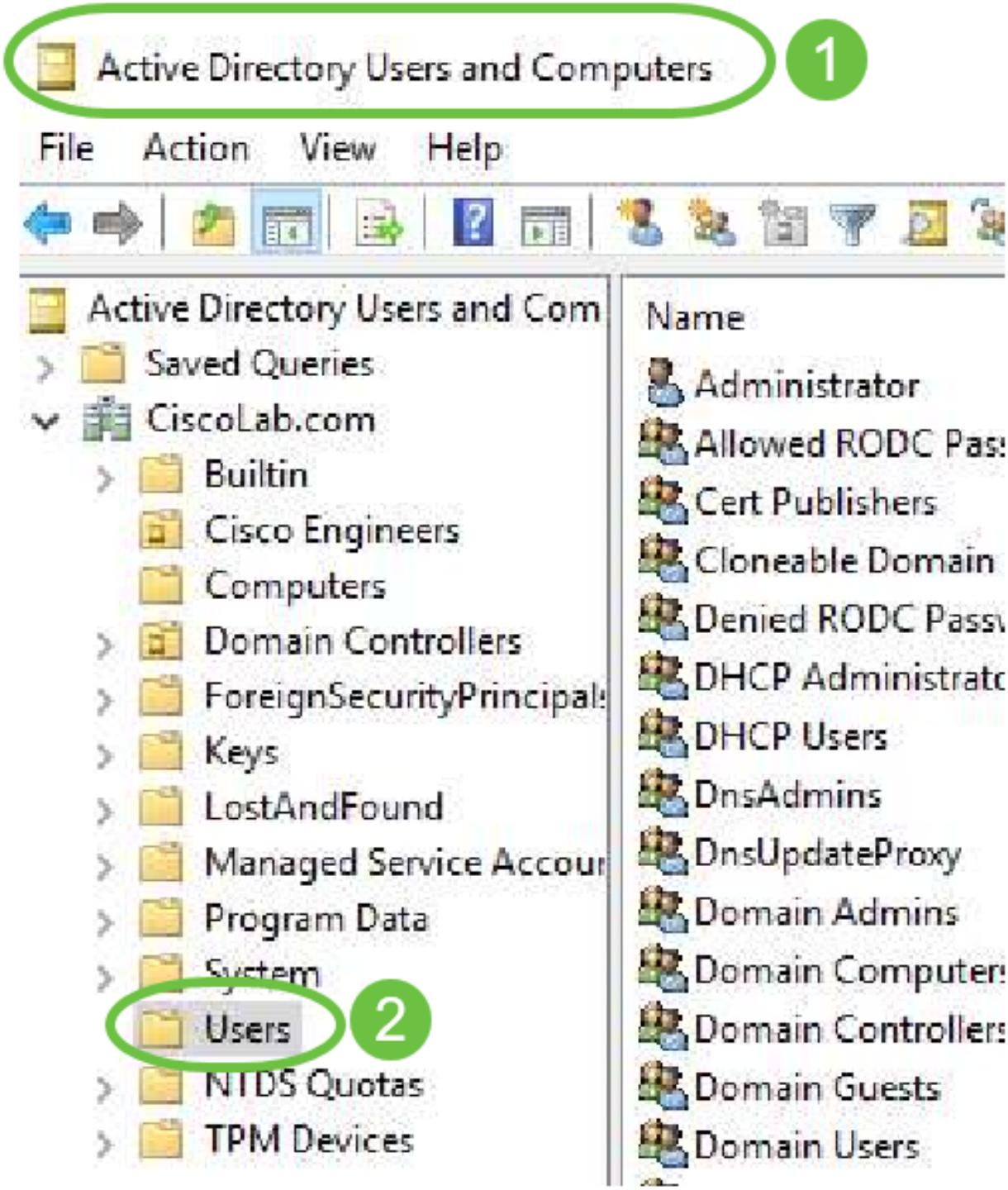


Se le dirigirá a la página principal de la cuenta de usuario. La cuenta configurada recientemente aparece ahora en la tabla Servicio de autenticación remota.

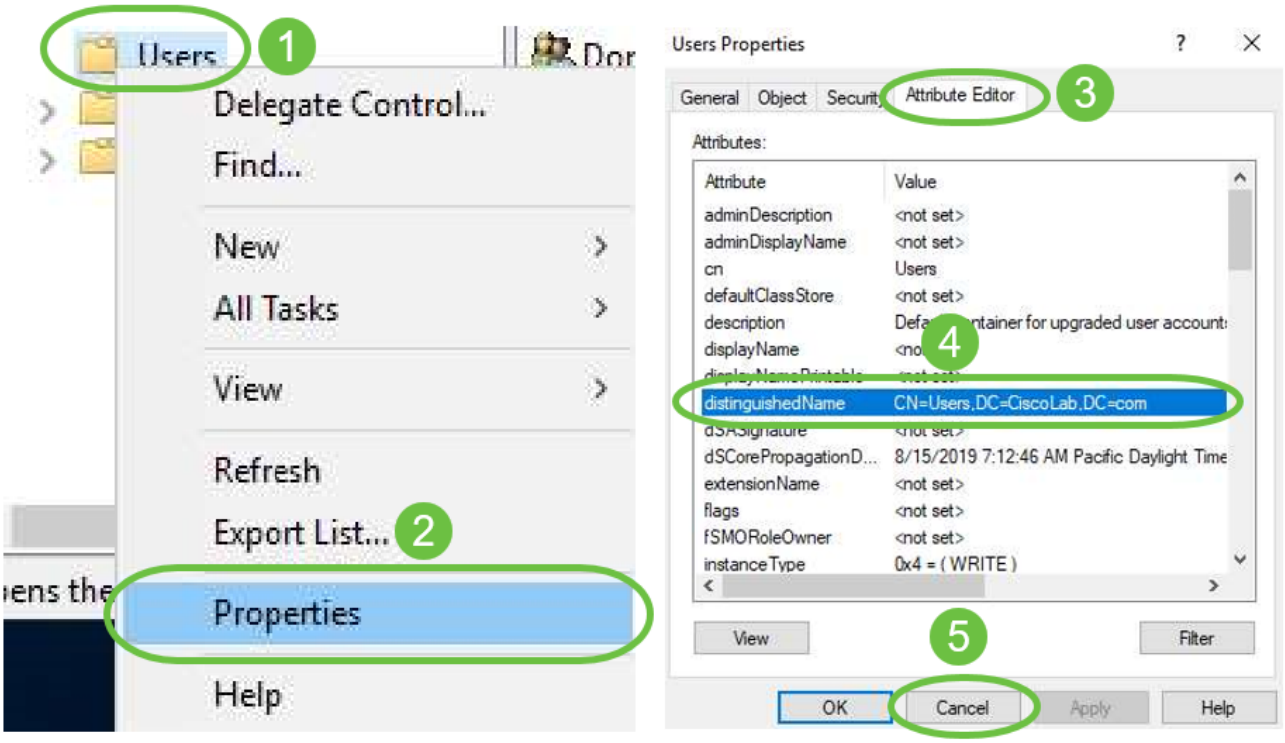
Ahora ha configurado correctamente la autenticación RADIUS en un router serie RV34x.

Configuración de Active Directory

Paso 1. Para completar la configuración de Active Directory, deberá iniciar sesión en el servidor de Active Directory. En su PC, abra **Usuarios y equipos de Active Directory** y desplácese al contenedor que utilizará las cuentas de usuario para iniciar sesión de forma remota. En este ejemplo, usaremos el contenedor **Users**.



Paso 2. Haga clic con el botón derecho del ratón en el contenedor y seleccione **Propiedades**. Navegue hasta la ficha *Editor de atributos* y busque el campo *Nombre distinguido*. Si esta ficha no está visible, deberá activar la vista de funciones avanzadas en los usuarios y equipos de Active Directory y volver a empezar. Anote este campo y haga clic en **Cancelar**. Esta será la ruta del contenedor del usuario. Este campo también será necesario al configurar el RV340 y debe coincidir exactamente.



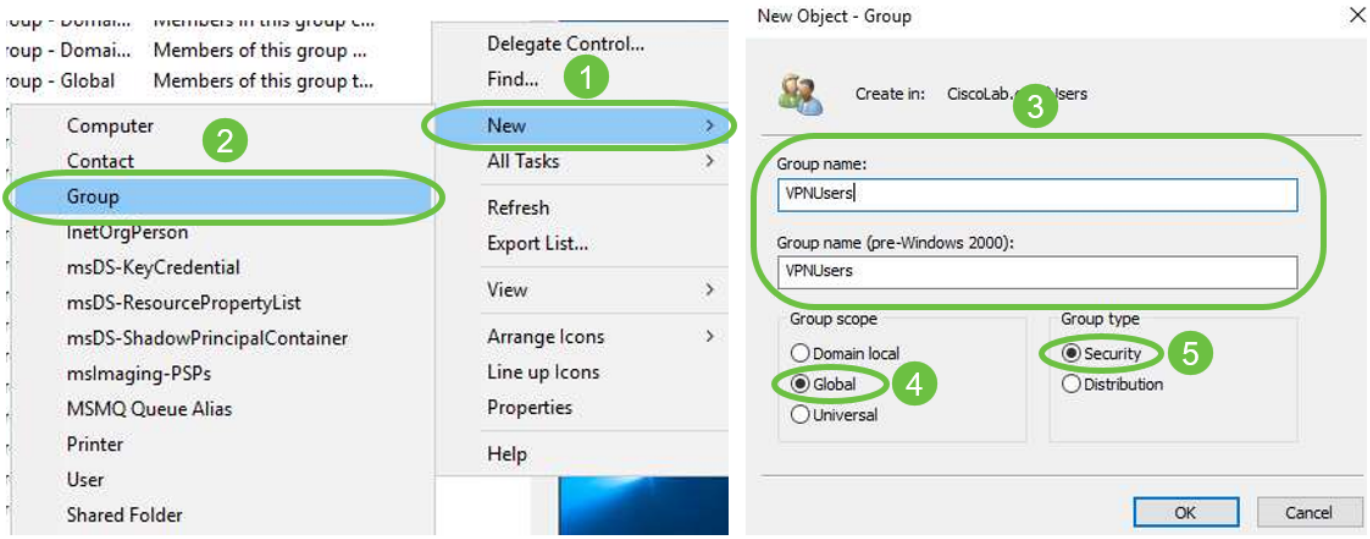
Paso 3. Cree un grupo de seguridad global en el mismo contenedor que las cuentas de usuario que se utilizarán.

En el contenedor seleccionado, haga clic con el botón derecho del ratón en un área en blanco y seleccione **Nuevo > Grupo**.

Select the following:

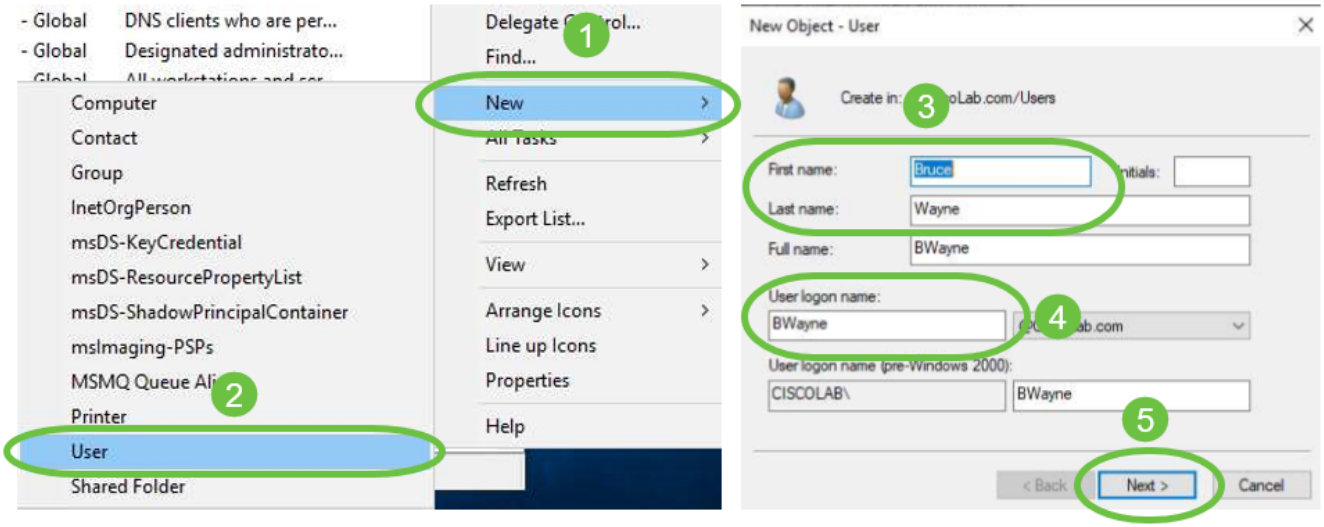
- Group Name (Nombre de grupo): este nombre deberá coincidir exactamente con el nombre de grupo de usuarios creado en el RV340. En este ejemplo, usaremos **VPNU**.
- Ámbito del grupo: global
- Tipo de grupo - Seguridad

Click OK.



Paso 4. Para crear nuevas cuentas de usuario, realice lo siguiente:

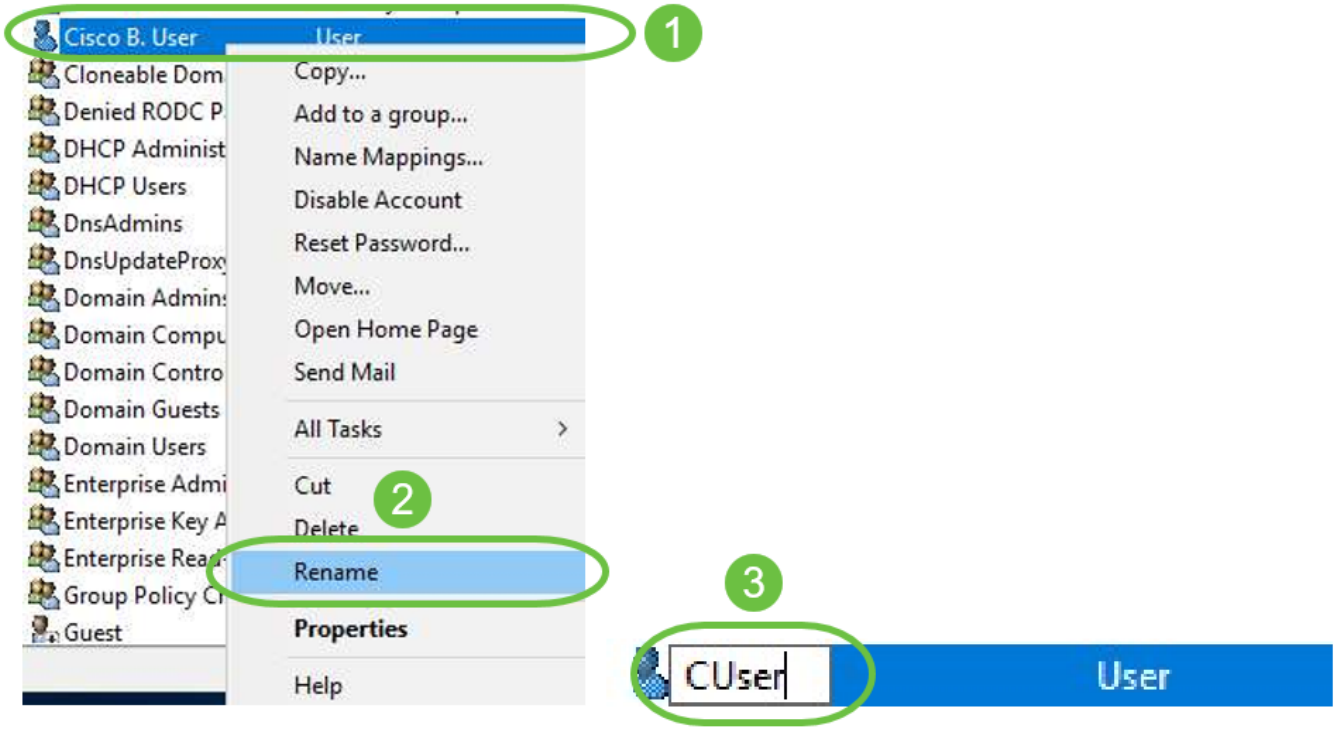
- Haga clic con el botón derecho en un espacio vacío en Container y seleccione **New > User**.
- Introduzca *Nombre*, *Apellidos*.
- Introduzca el *nombre de inicio de sesión de usuario*.
- Haga clic en Next (Siguiente).



Se le solicitará que introduzca una contraseña para el usuario. Si la casilla *El usuario debe cambiar la contraseña en el siguiente inicio de sesión* está marcada, el usuario tendrá que iniciar sesión localmente y cambiar la contraseña ANTES de iniciar sesión de forma remota.

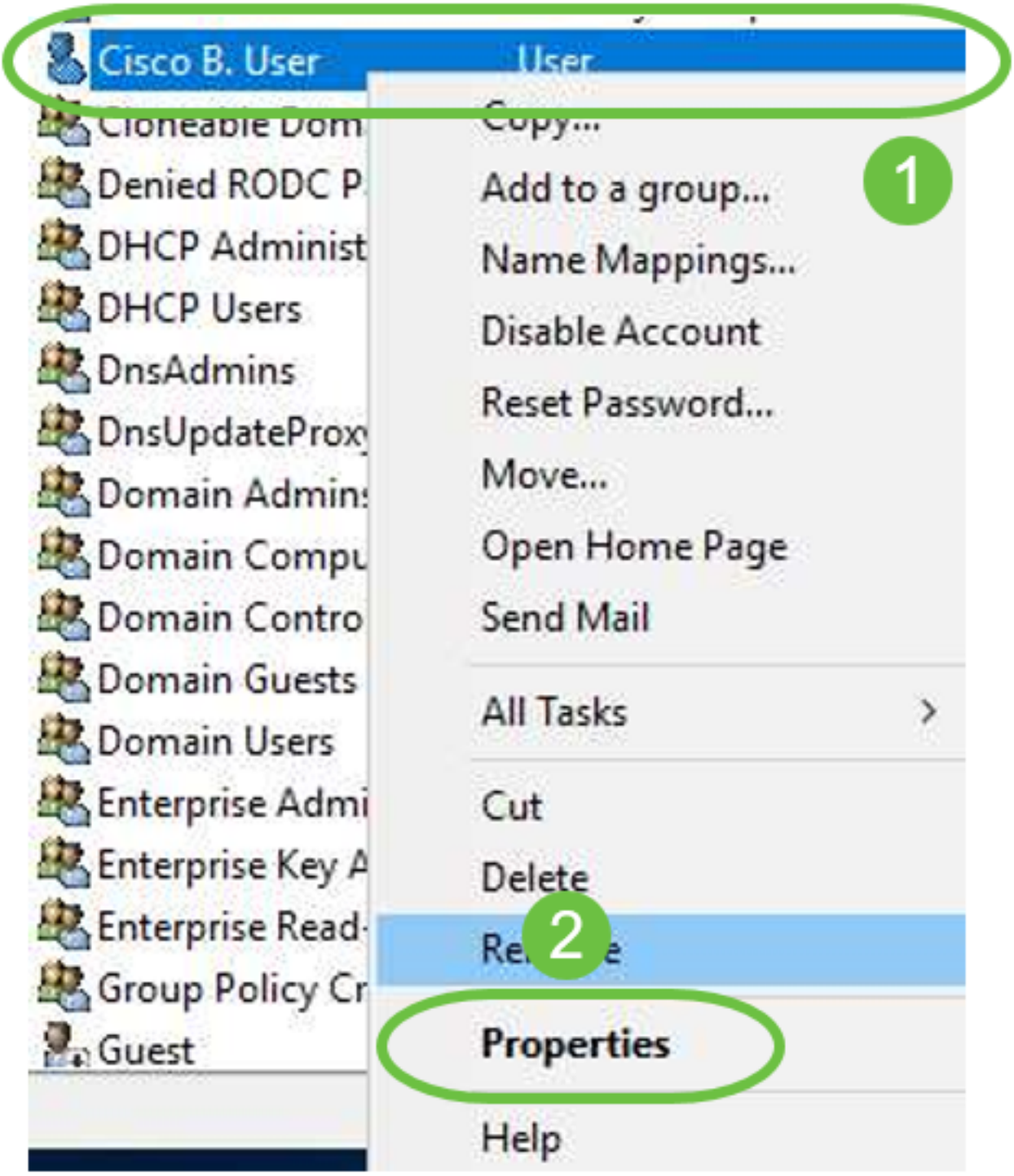
Haga clic en Finish (Finalizar).

Si ya se han creado cuentas de usuario que deben utilizarse, es posible que sea necesario realizar ajustes. Para ajustar el nombre canónico de un usuario, seleccione el usuario, haga clic con el botón derecho y seleccione **Cambiar nombre**. Asegúrese de que todos los espacios se quitan y que coincidan con el nombre de inicio de sesión del usuario. Esto NO cambiará el nombre mostrado de los usuarios. Click OK.

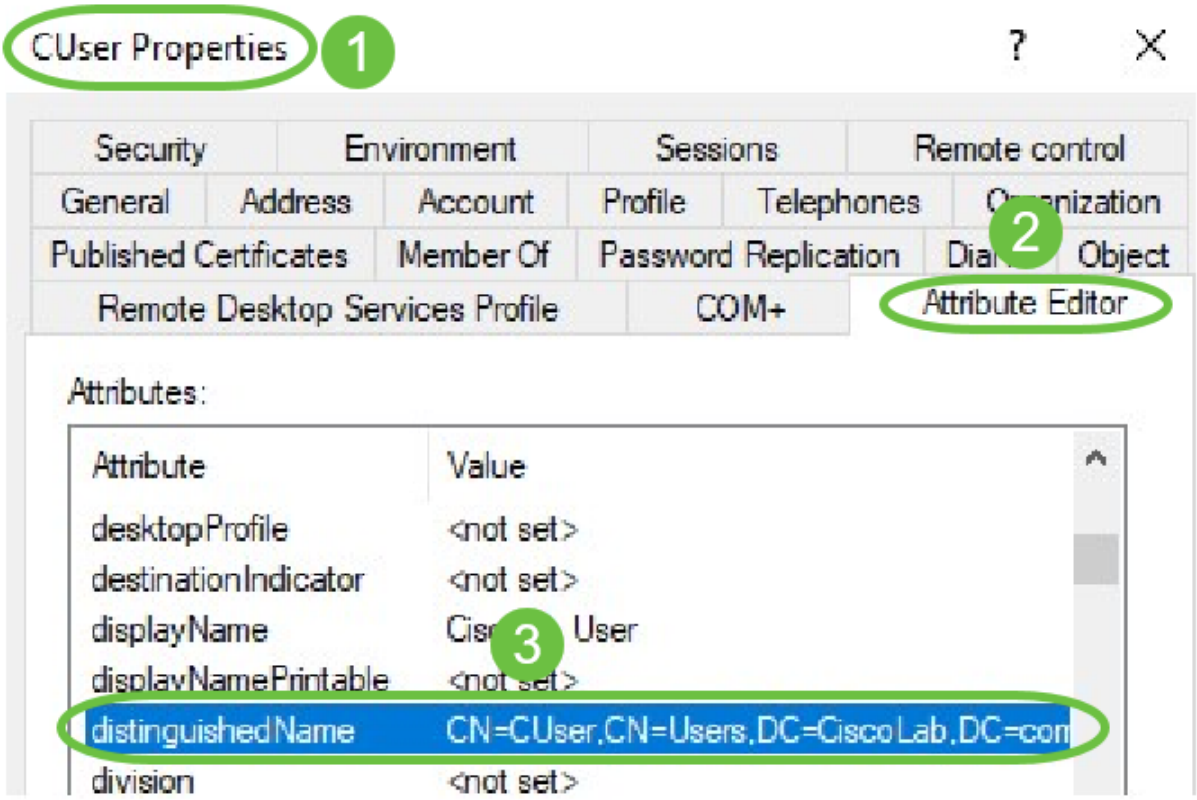


Paso 5. Una vez que las cuentas de usuario estén estructuradas correctamente, se les deberán conceder derechos para iniciar sesión de forma remota.

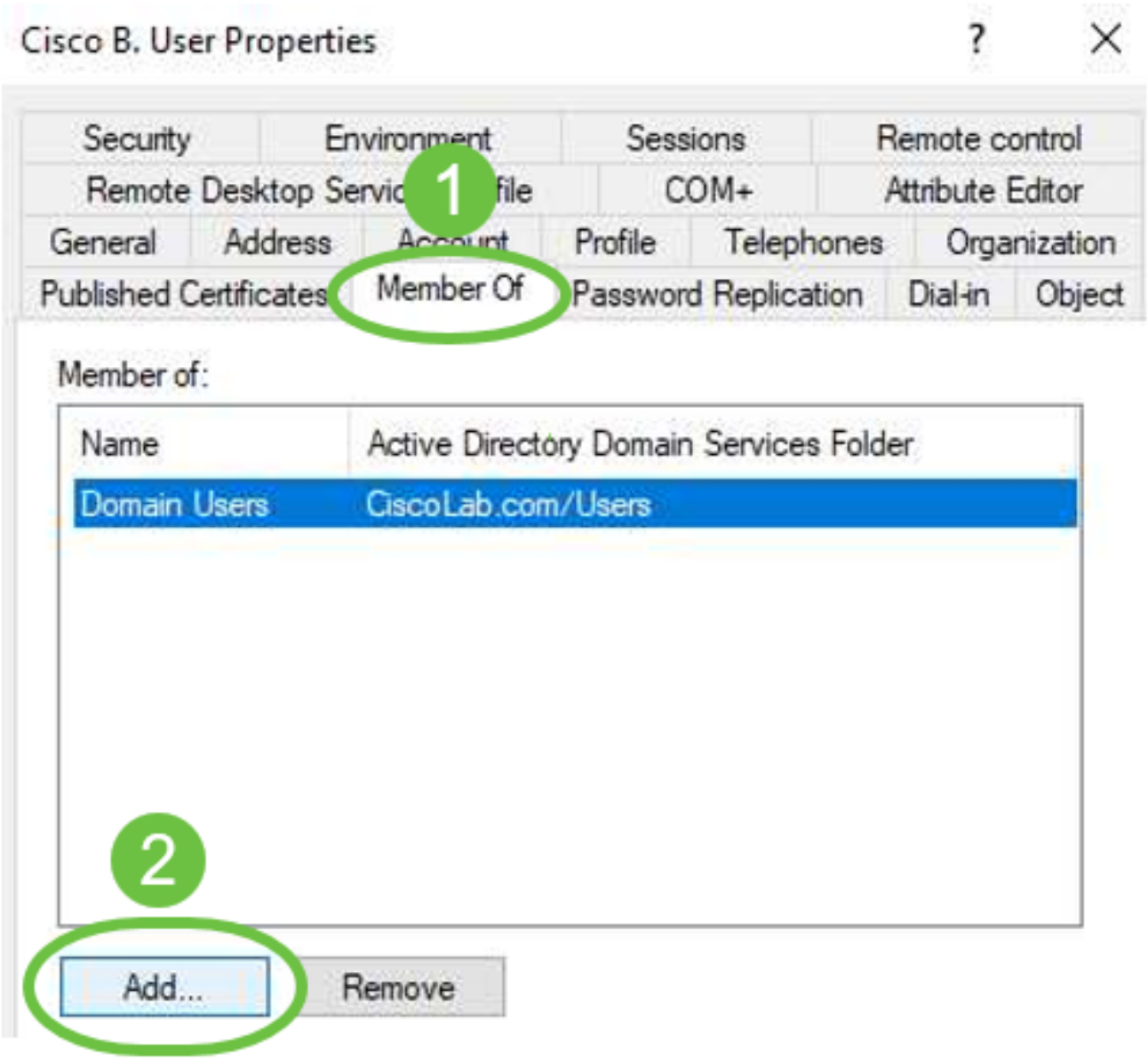
Para hacerlo, seleccione la cuenta de usuario, haga clic con el botón derecho y seleccione **Propiedades**.



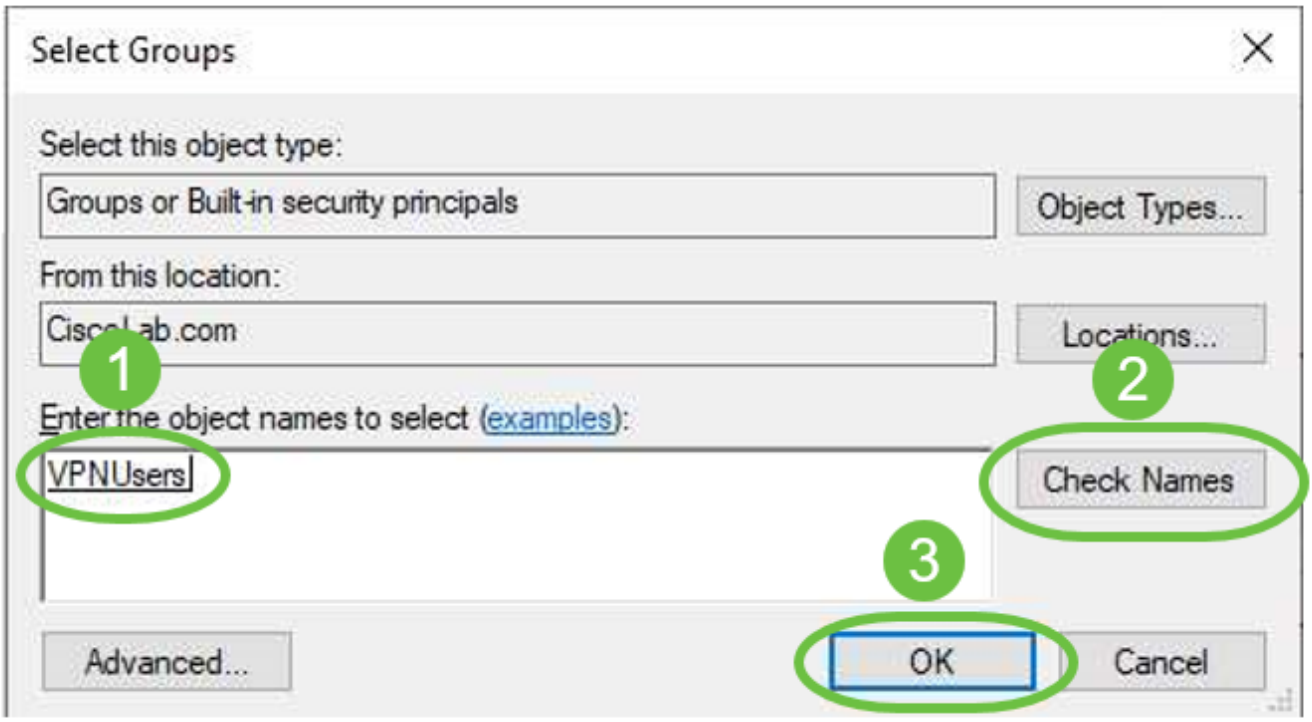
En la pestaña *Propiedades de usuario* seleccione **Editor de atributos** y desplácese hacia abajo hasta *Nombre distinguido*. Asegúrese de que el primer *CN=* tenga el nombre de inicio de sesión de usuario correcto sin espacios.



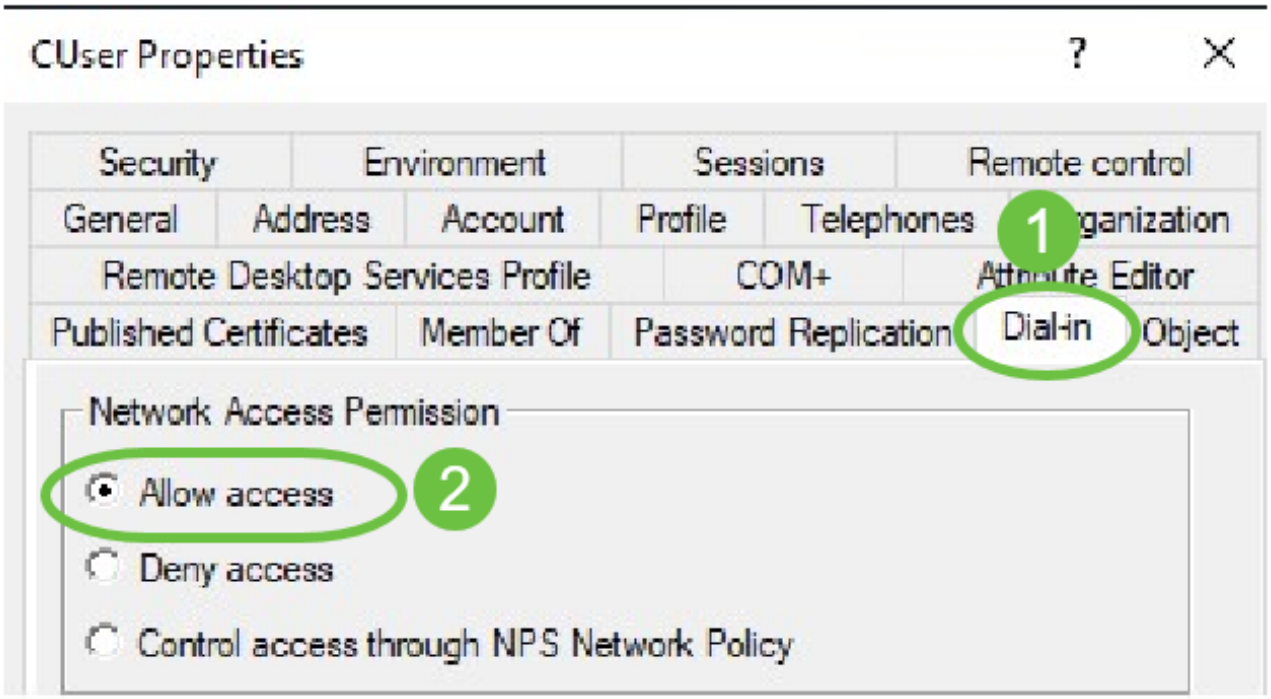
Seleccione la ficha **Miembro de y haga clic en Agregar**.



Ingrese el nombre del *Grupo de Seguridad Global* y seleccione **Check Name**. Si la entrada está subrayada, haga clic en **Aceptar**.



Seleccione la pestaña **Marcado de entrada**. En la sección *Permiso de acceso a la red*, seleccione **Permitir acceso** y deje el resto como predeterminado.

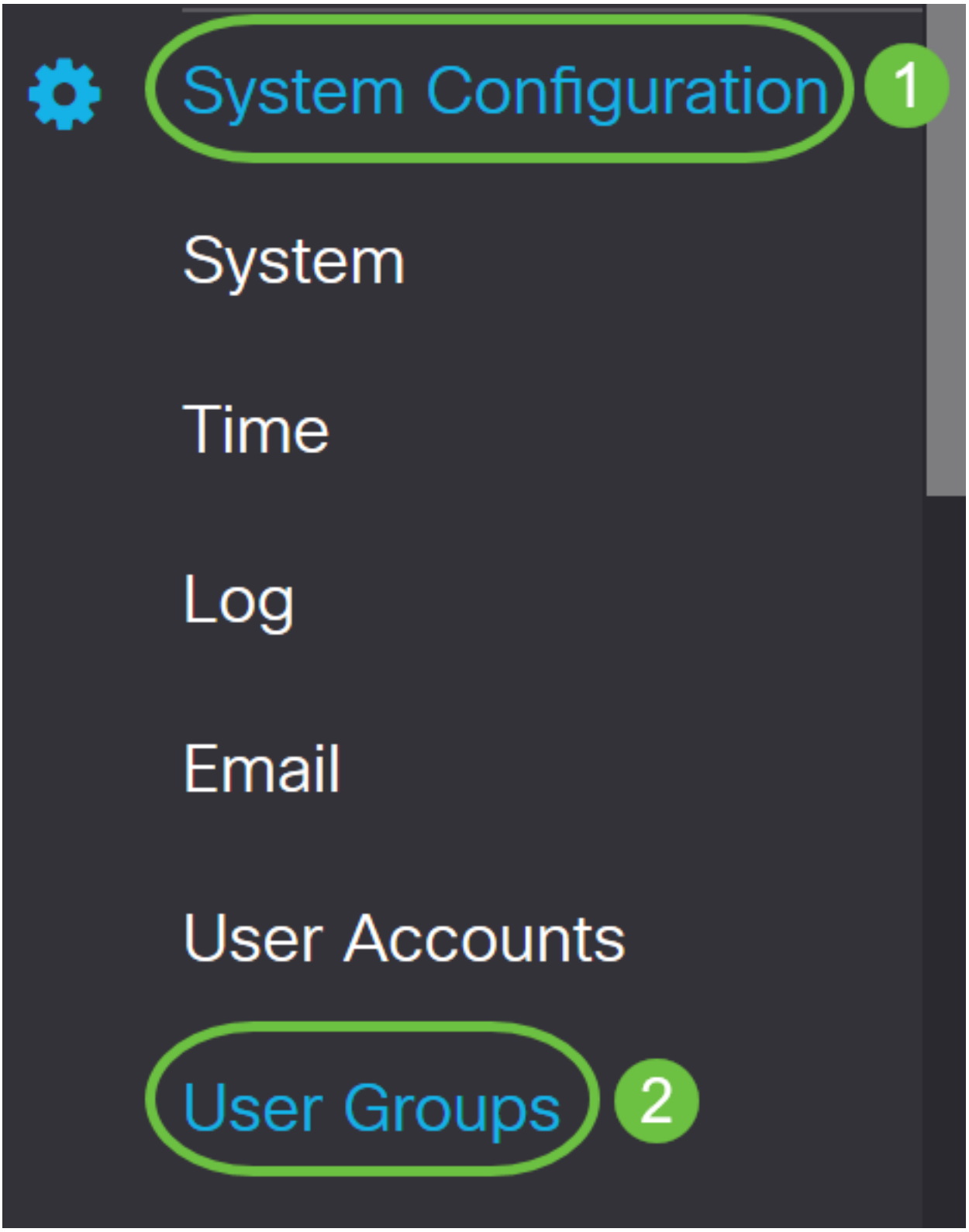


Integración de Active Directory

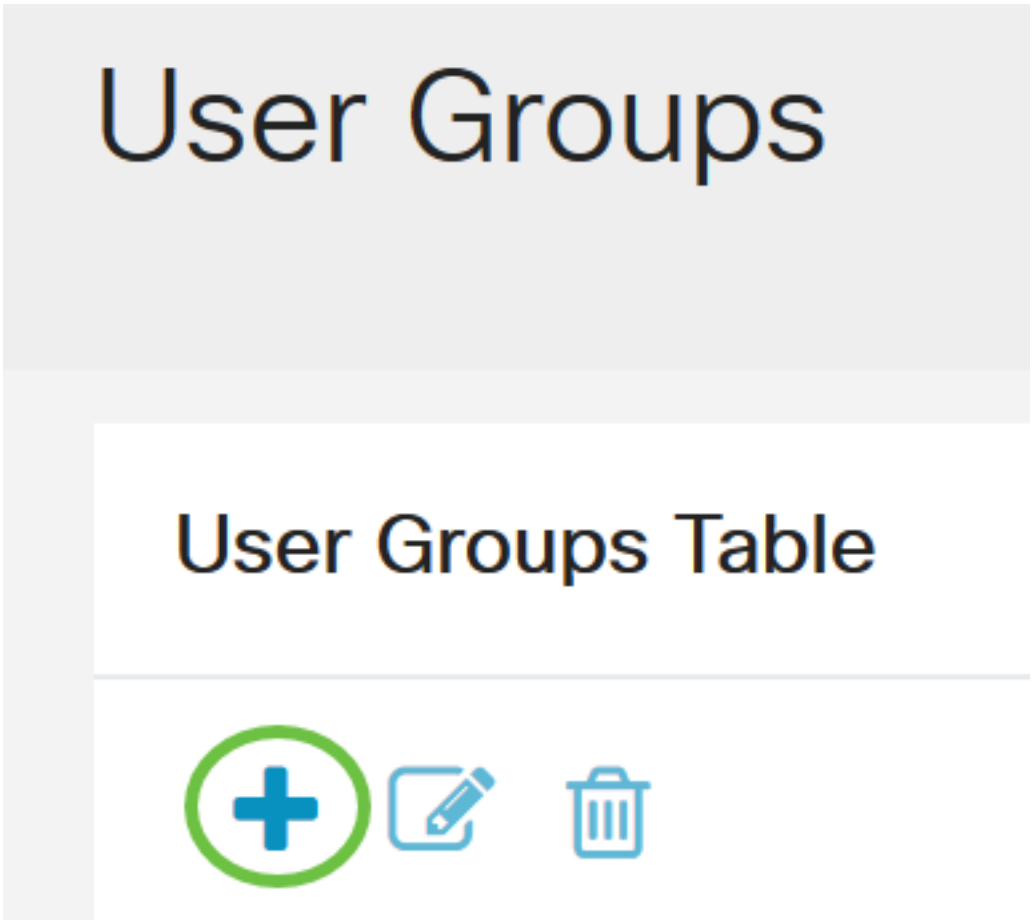
Active Directory requiere que la hora del router RV34x coincida con la del servidor AD. Para ver los pasos sobre cómo configurar la configuración de la hora en un RV34x Series Router, haga clic aquí.

AD también requiere que el RV340 tenga un grupo de usuarios que coincida con el grupo de seguridad global de AD.

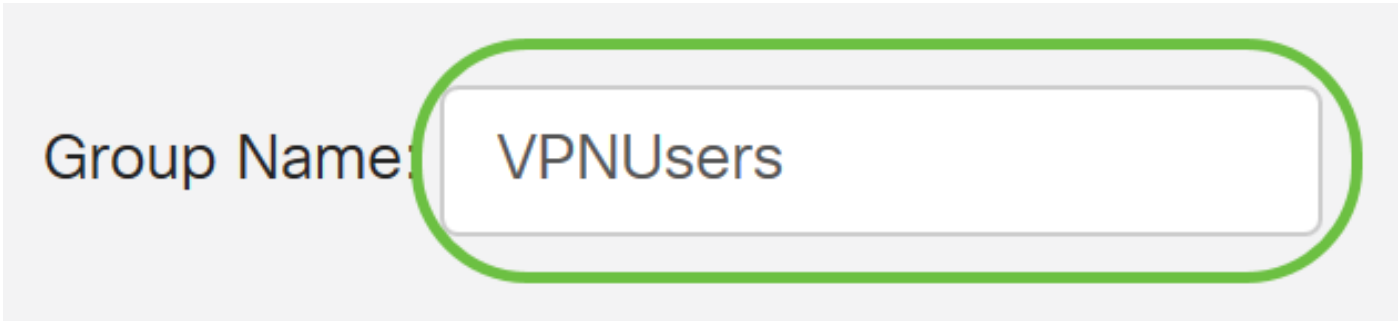
Paso 1. Vaya a **Configuración del sistema > Grupos de usuarios**.



Paso 2. Haga clic en el icono **más** para agregar un grupo de usuarios.

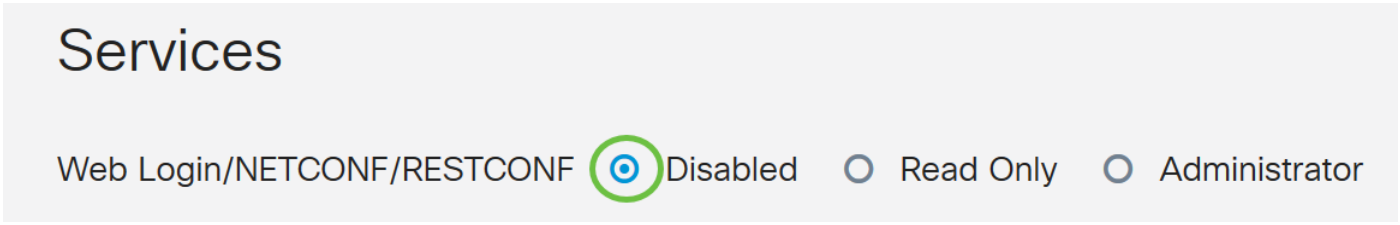


Paso 3. Introduzca el *nombre del grupo*. En este ejemplo, son **usuarios VPNU**.



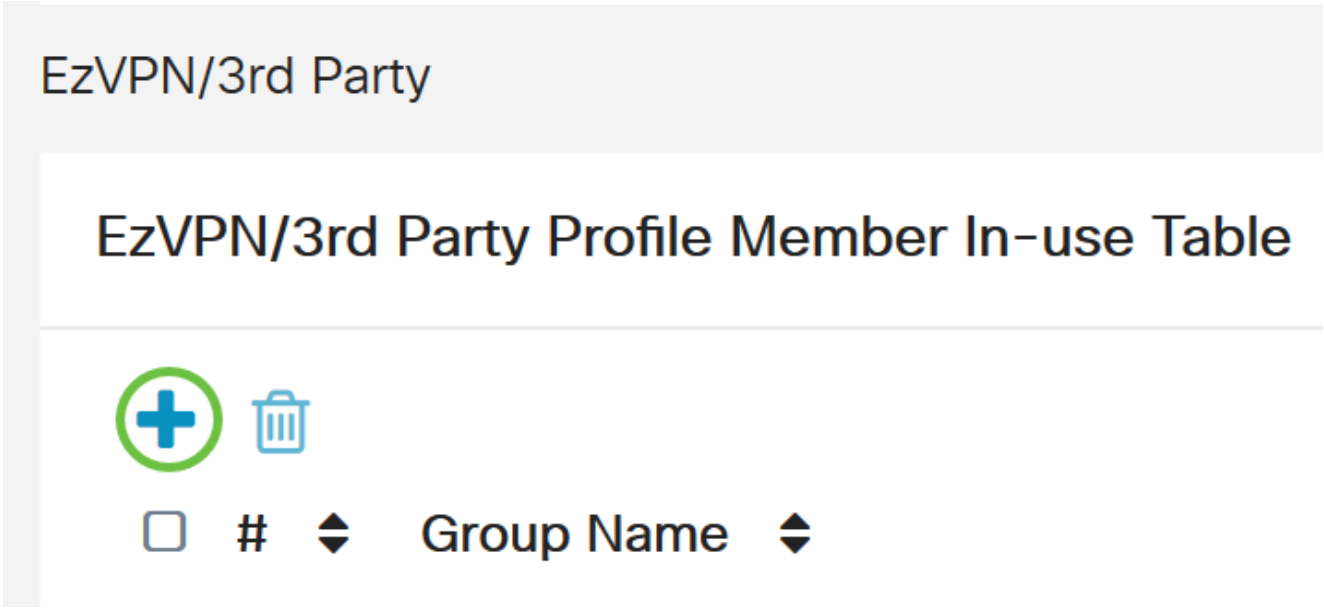
El nombre de grupo debe ser exactamente igual que el grupo de seguridad global de AD.

Paso 4. En *Servicios*, *Login/NETCONF/RESTCONF* de la Web debe marcarse como **Desactivado** . Si AD Integration no funciona inmediatamente, podrá acceder al RV34x.

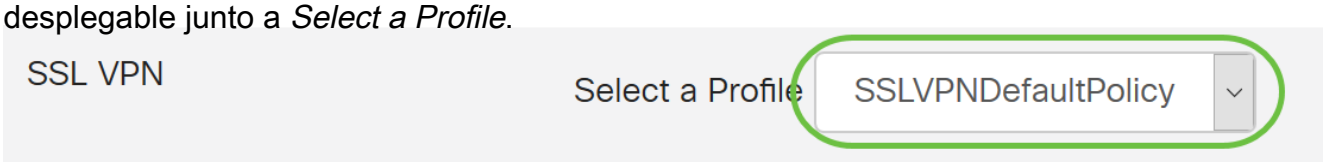


Paso 5. Puede agregar los túneles VPN que utilizarán AD Integration para registrar a sus usuarios.

1. Para agregar una VPN de cliente a sitio que ya se ha configurado, vaya a la sección *EZVPN/terceros* y haga clic en el icono **más**. Seleccione el perfil VPN en el menú desplegable y haga clic en **Agregar**.

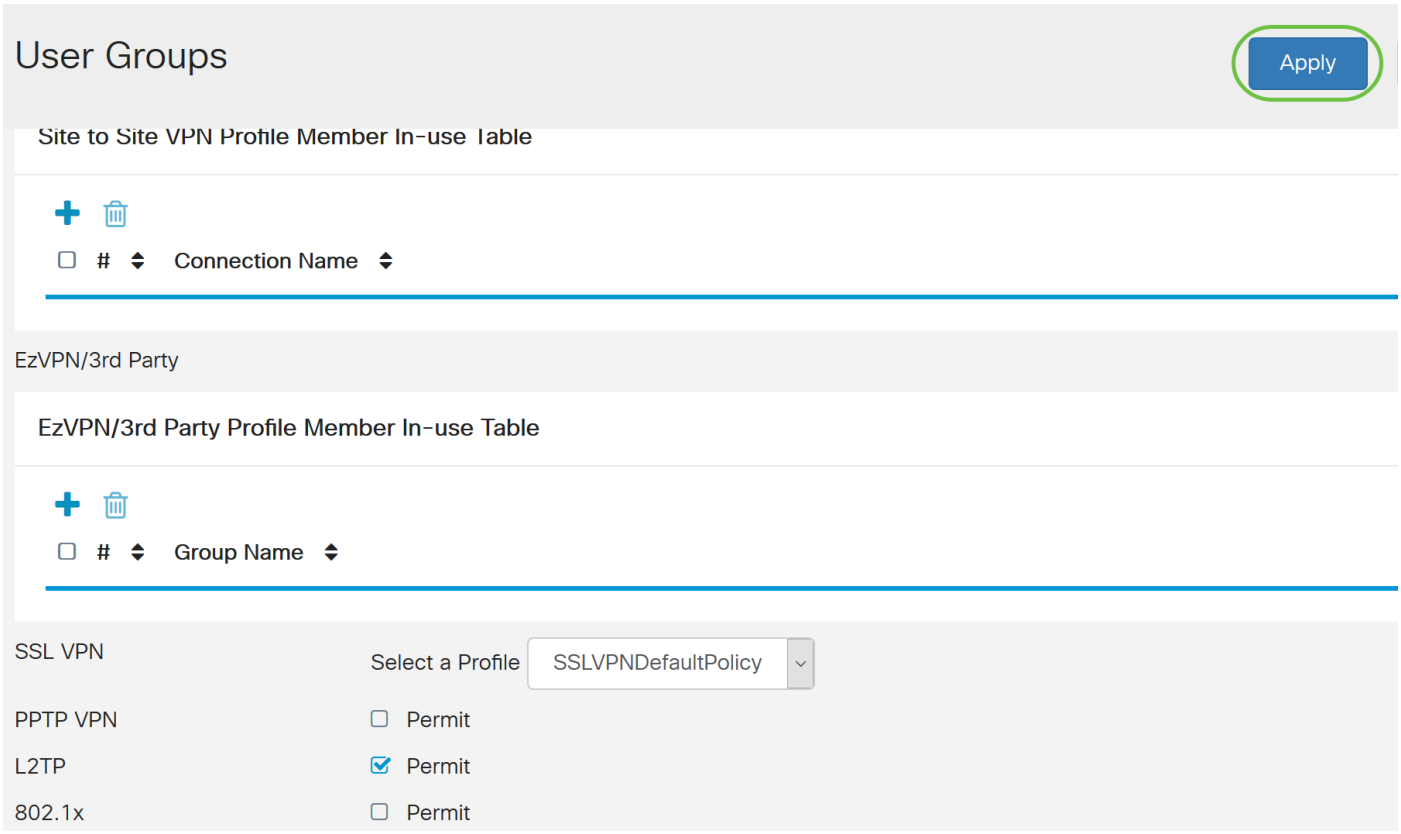


4. SSL VPN - Si se va a utilizar un túnel SSL VPN, seleccione la política en el menú desplegable junto a *Select a Profile*.



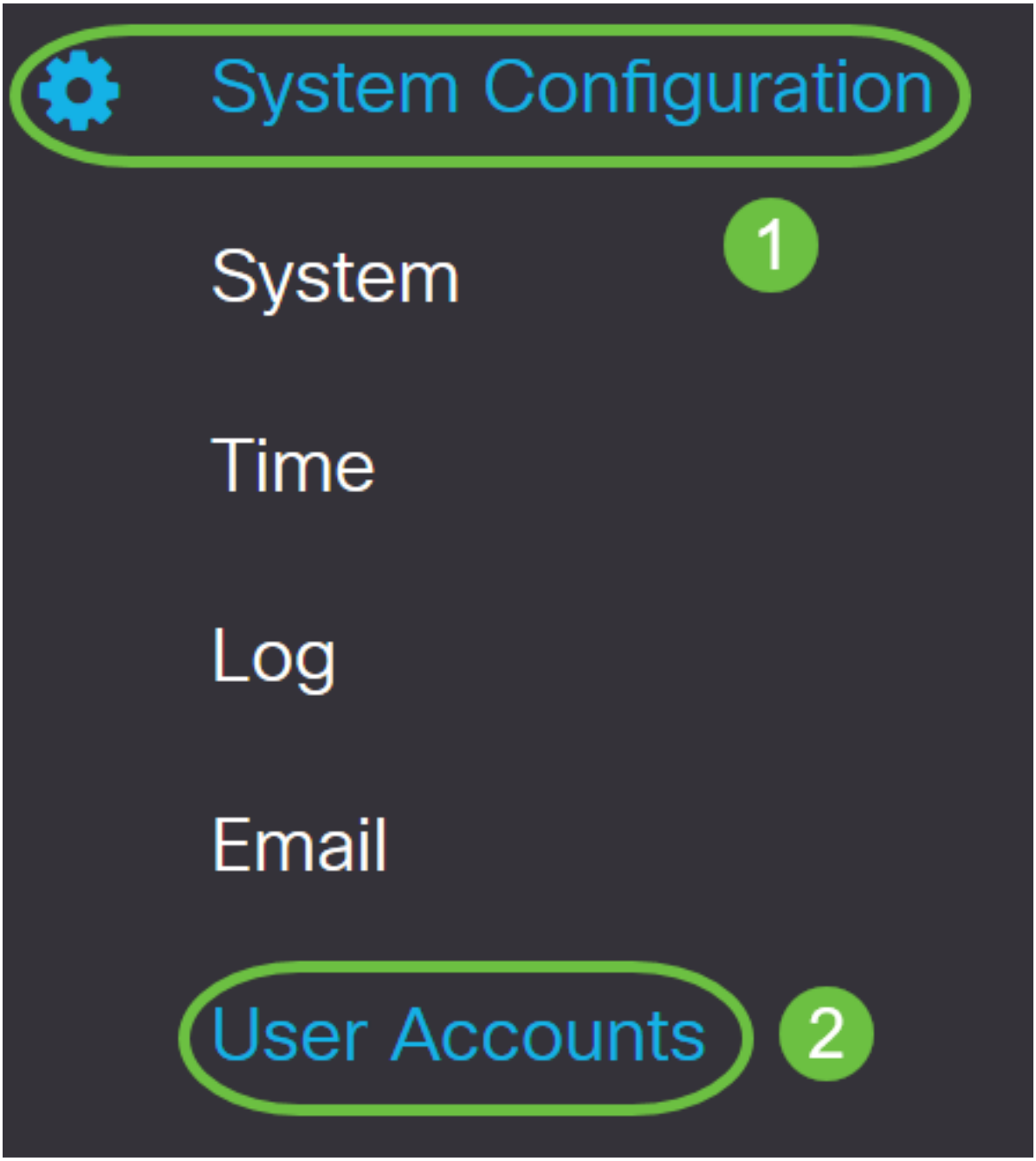
6. PPTP/L2TP/802.1x - Para permitir que estos usuarios utilicen AD, simplemente haga clic en la casilla de verificación junto a ellos para *Permitir*.

Paso 6. Haga clic en **Aplicar** para guardar los cambios.

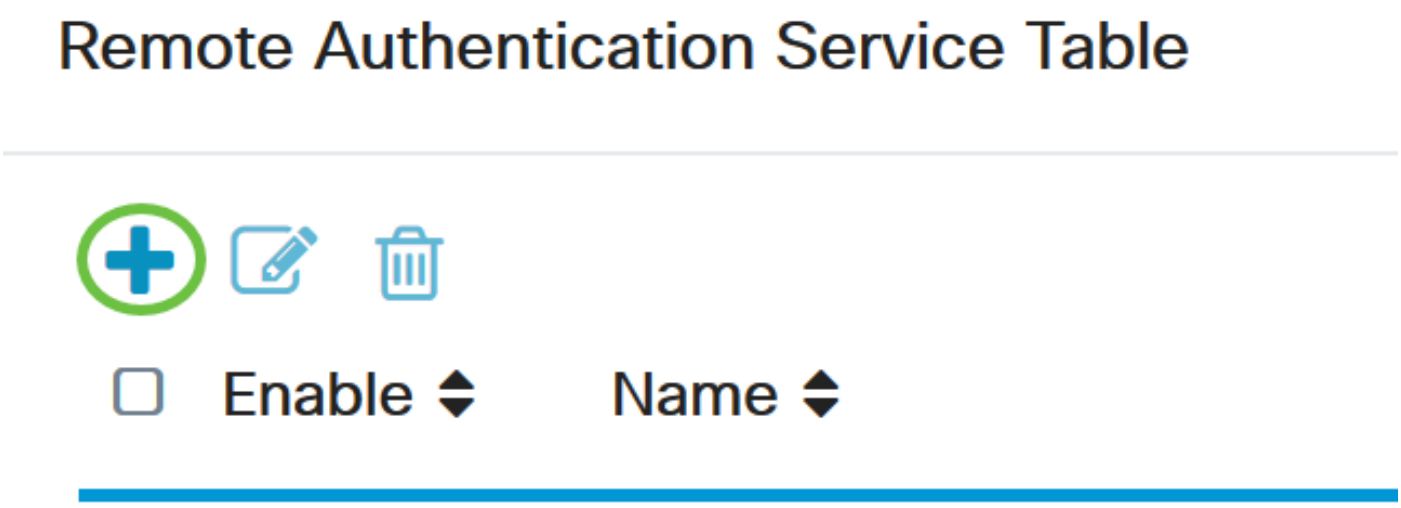


Configuración de integración de Active Directory

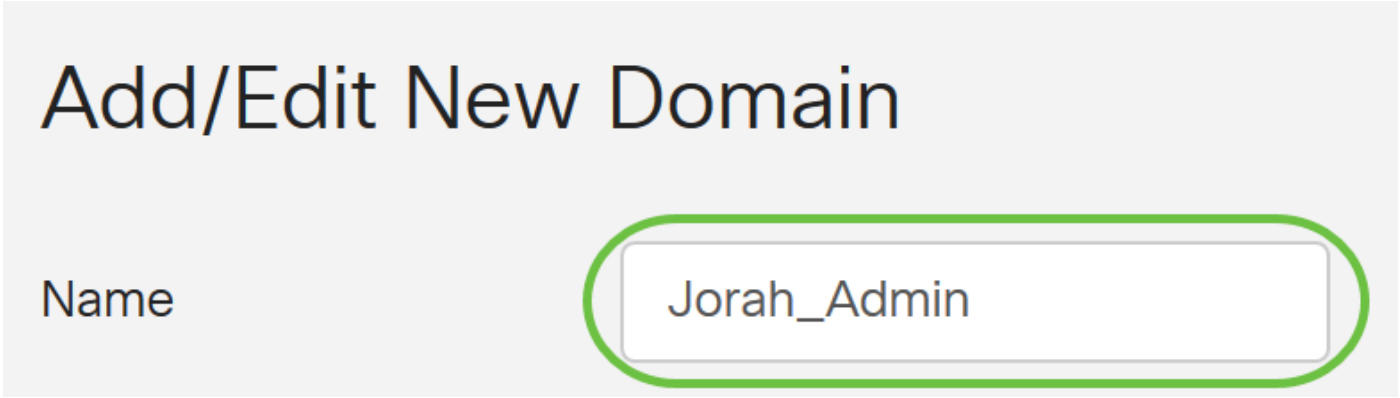
Paso 1. Vaya a **Configuración del sistema > Cuentas de usuario** .



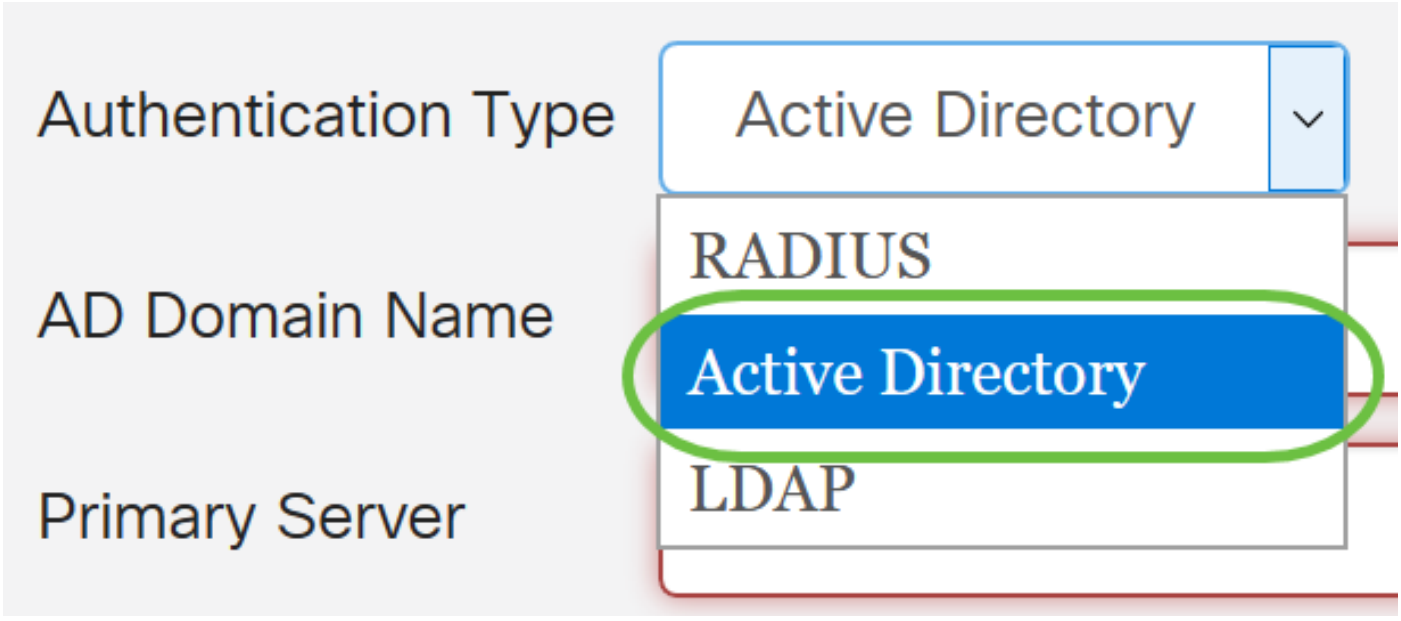
Paso 2. En la tabla Remote Authentication Service, haga clic en **Add** para crear una entrada.



Paso 3. En el campo *Nombre*, cree un nombre de usuario para la cuenta. En este ejemplo, se utiliza **Jorah_Admin**.

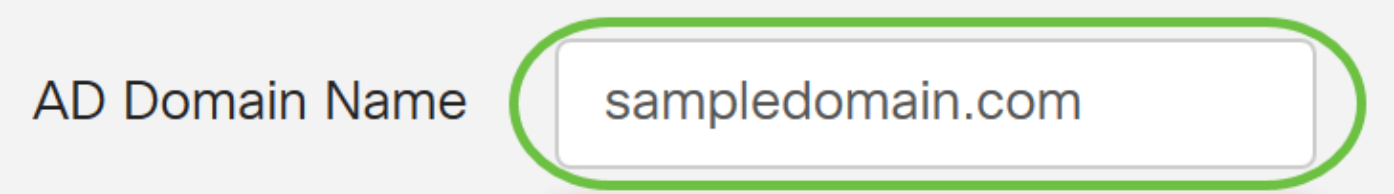


Paso 4. En el menú desplegable *Tipo de autenticación*, elija **Active Directory**. AD se utiliza para asignar políticas amplias a todos los elementos de la red, implementar programas en muchos equipos y aplicar actualizaciones críticas a toda una organización.



Paso 5. En el campo *AD Domain Name*, ingrese el nombre de dominio completo del AD.

En este ejemplo, se utiliza **samcompromeomain.com**.

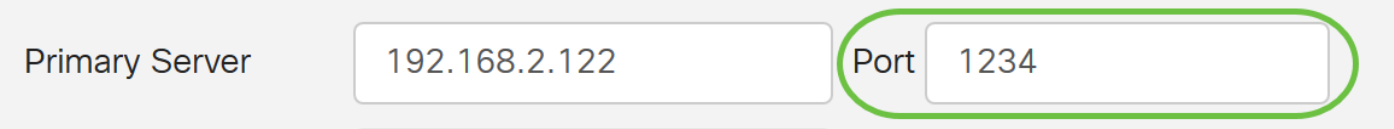


Paso 6. En el campo *Servidor primario*, ingrese la dirección del AD.

En este ejemplo, se utiliza **192.168.2.122**.

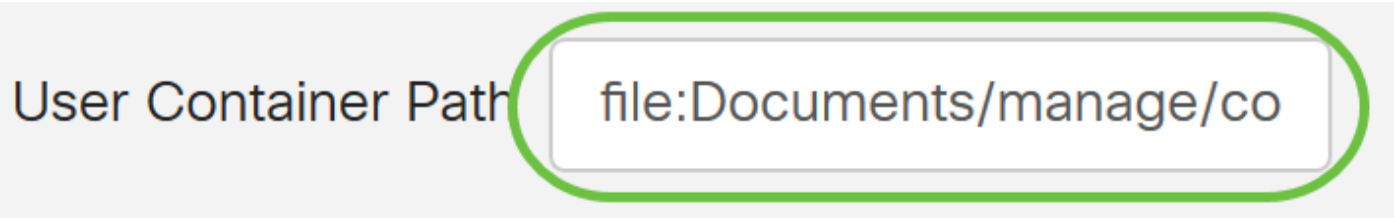
Paso 7. En el campo *Port*, ingrese un número de puerto para el Servidor Primario.

En este ejemplo, **1234** se utiliza como número de puerto.

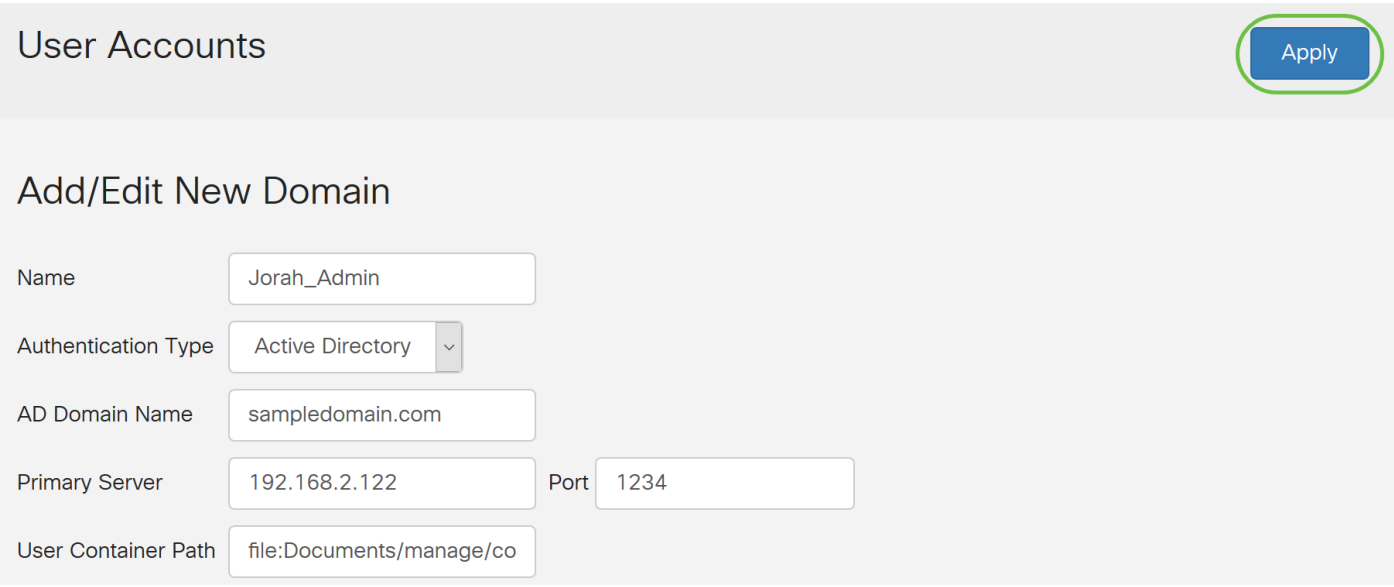


Paso 8. (Opcional) En el campo *User Container Path*, ingrese una ruta de acceso raíz donde se encuentran los usuarios.

Nota: En este ejemplo, se utiliza **file:Documents/manage/containers**.



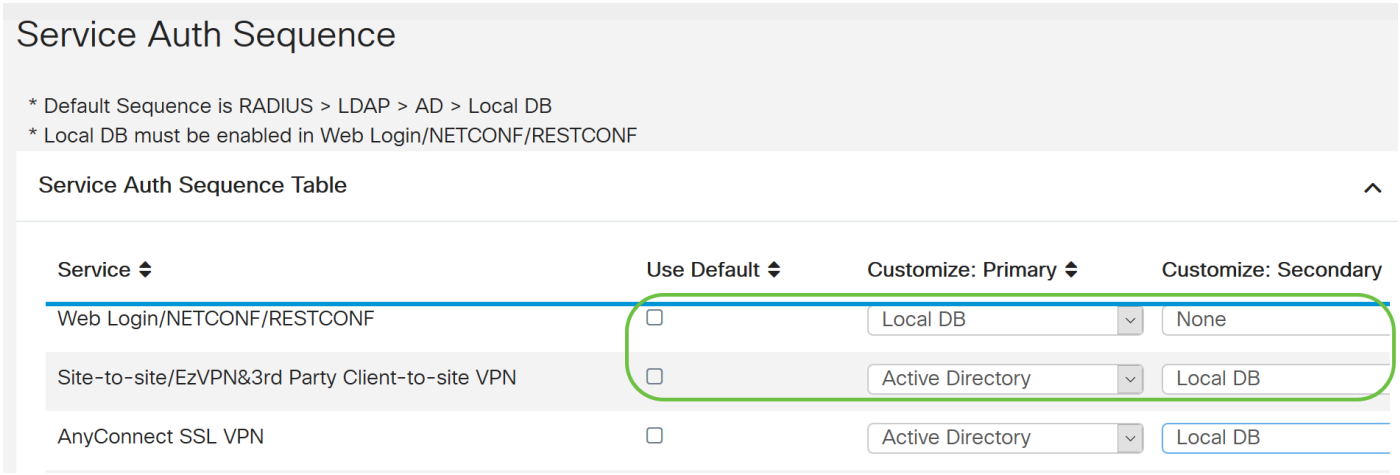
Paso 9. Haga clic en Apply (Aplicar).



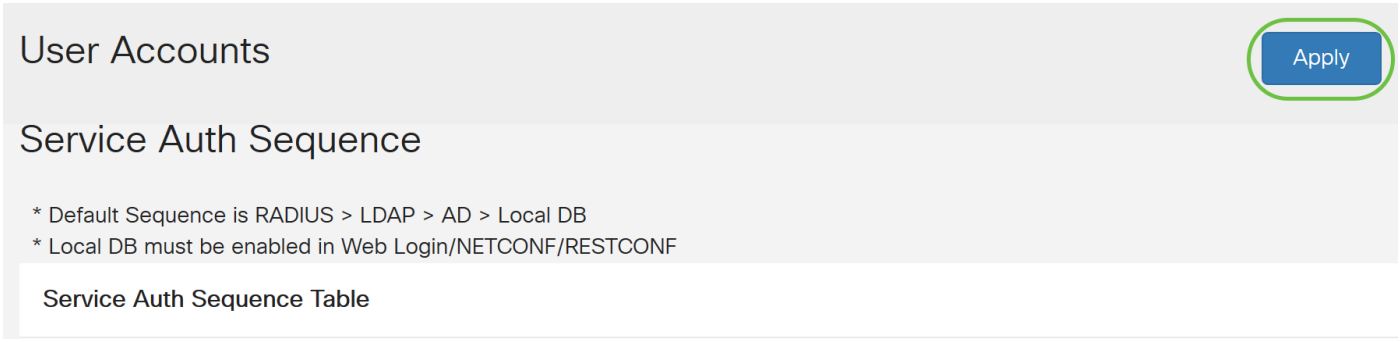
Paso 10. Desplácese hacia abajo hasta *Secuencia de autenticación de servicio* para establecer el

método de inicio de sesión para las diversas opciones.

- Inicio de sesión en la Web/NETFCONF/RESTCONF - Así es como inicia sesión en el router RV34x. Desmarque la casilla *Usar valor predeterminado* y establezca el método principal en **Base de datos local**. Esto garantizará que no se cierre la sesión del router incluso si falla la integración de Active Directory.
- VPN de sitio a sitio/EzVPN&VPN de cliente a sitio de terceros: se establece el túnel VPN de cliente a sitio para utilizar AD. Desmarque la casilla de verificación *Usar valor predeterminado* y establezca el método principal en **Active Directory** y Método secundario en **Local DB**.



Paso 11. Haga clic en Apply (Aplicar).

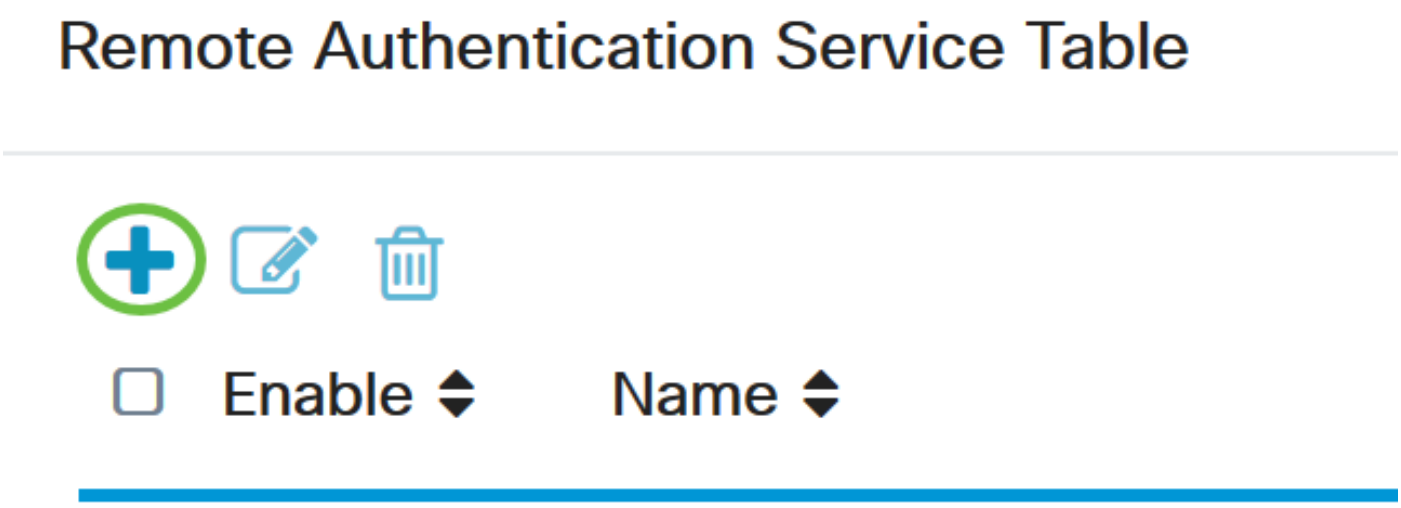


Paso 12. Guarde la configuración en ejecución en la configuración de inicio.

Ahora ha configurado correctamente los parámetros de Active Directory en un router serie RV34x.

LDAP

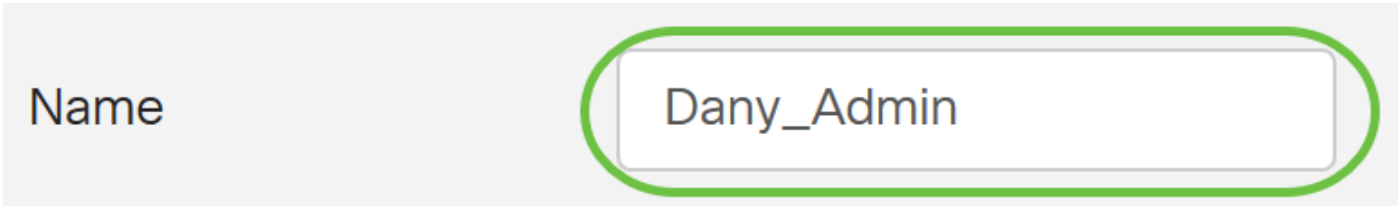
Paso 1. En la tabla Remote Authentication Service, haga clic en **Add** para crear una entrada.



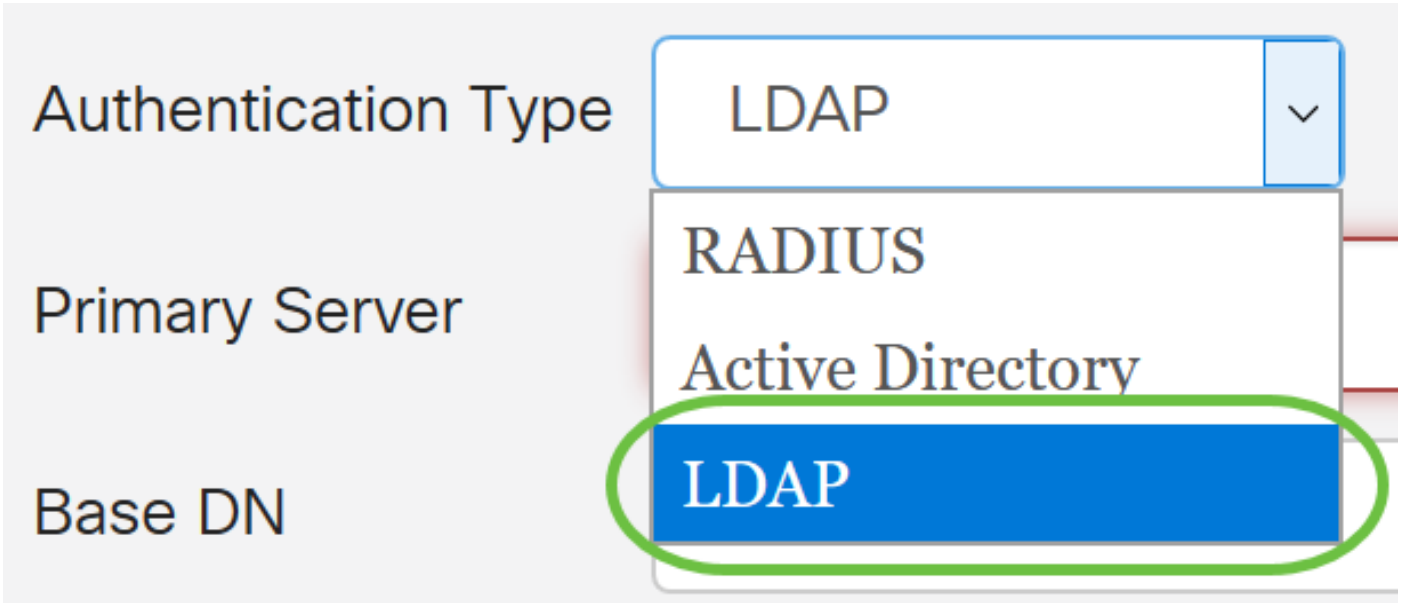
Paso 2. En el campo *Nombre*, cree un nombre de usuario para la cuenta.

Sólo se puede configurar una sola cuenta de usuario remota bajo LDAP.

En este ejemplo, se utiliza Dany_Admin.

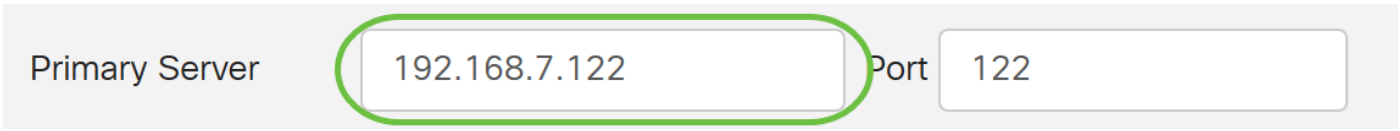


Paso 3. En el menú desplegable Authentication Type , elija **LDAP**. Lightweight Directory Access Protocol es un protocolo de acceso que se utiliza para acceder a un servicio de directorio. Se trata de un servidor remoto que ejecuta un servidor de directorio para realizar la autenticación para el dominio.



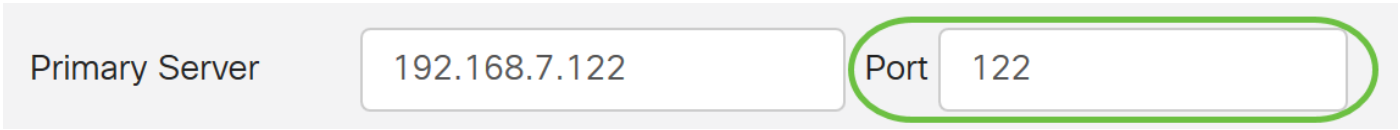
Paso 4. En el *campo Primary Server*, ingrese la dirección del servidor de LDAP.

En este ejemplo, se utiliza **192.168.7.122**.



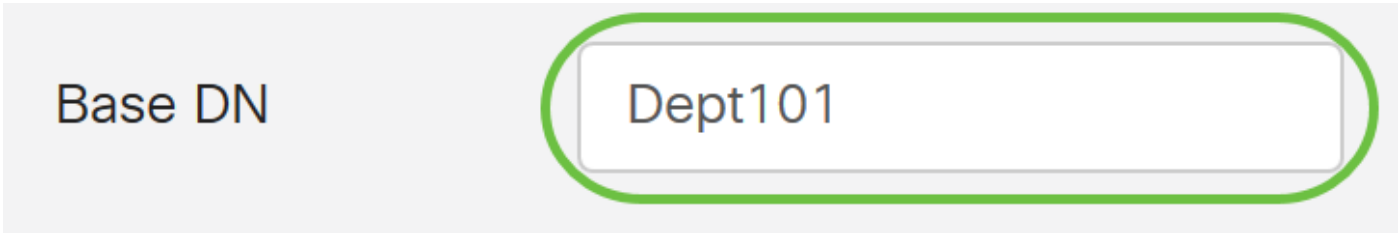
Paso 5. En el campo *Port*, ingrese un número de puerto para el Servidor Primario.

En este ejemplo, **122** se utiliza como número de puerto.



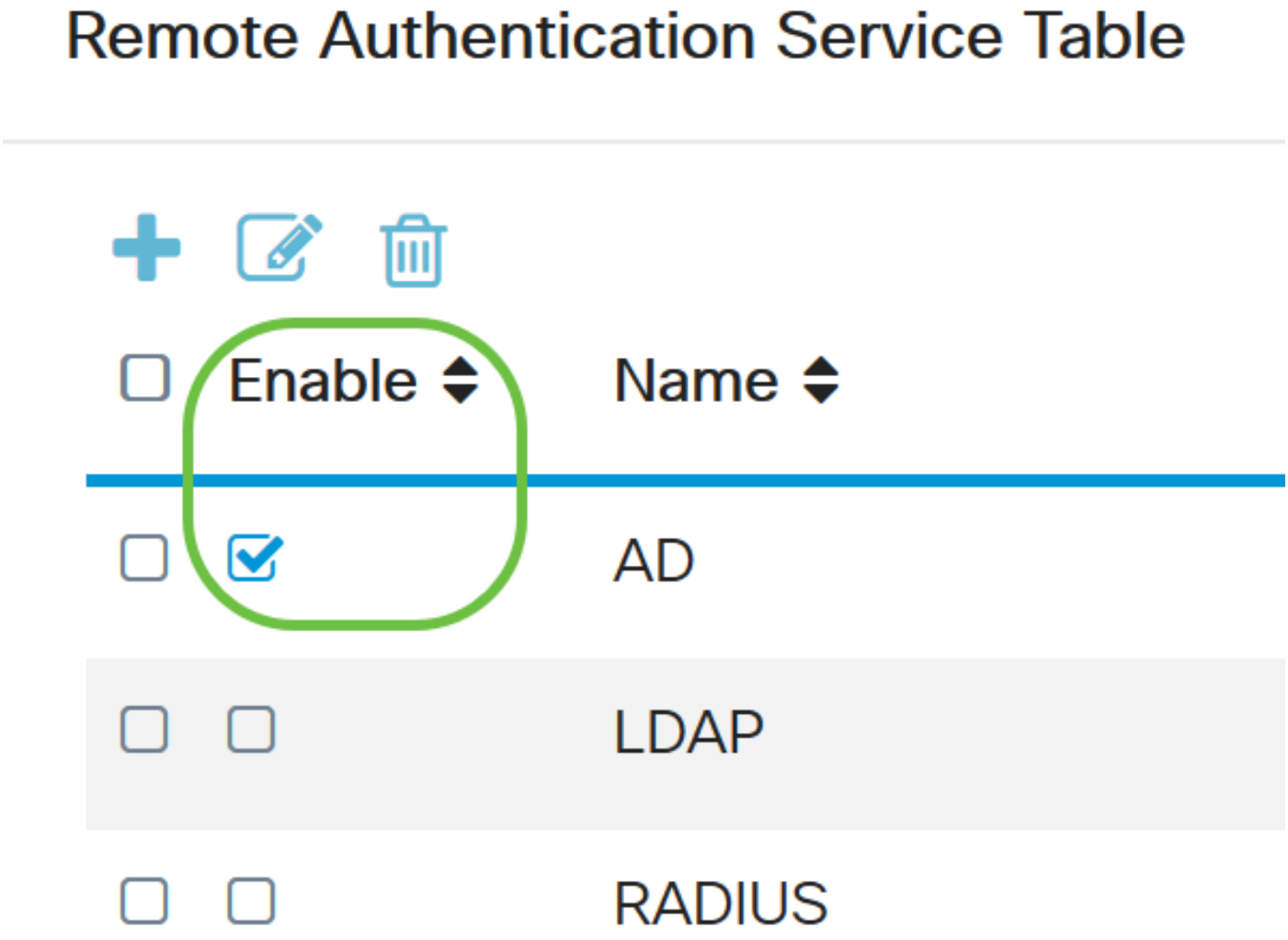
Paso 6. Ingrese el nombre distintivo base del servidor LDAP en el campo *DN base*. El DN base es la ubicación donde el servidor LDAP busca usuarios cuando recibe una solicitud de autorización. Este campo debe coincidir con el DN base configurado en el servidor LDAP.

En este ejemplo, se utiliza **Dept101**.

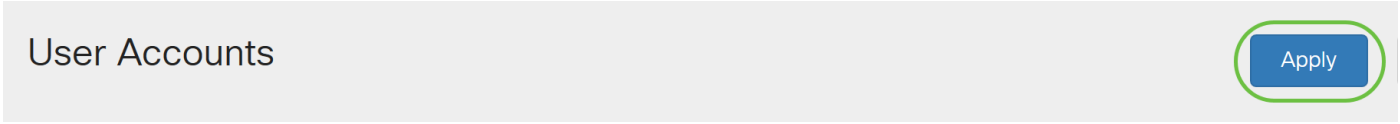


Paso 7. Haga clic en Apply (Aplicar). Se le llevará a la tabla de servicio de autenticación remota.

Paso 8. (Opcional) Si desea activar o desactivar el servicio de autenticación remota, active o desactive la casilla de verificación situada junto al servicio que desea activar o desactivar.



Paso 9. Haga clic en Apply (Aplicar).



Ahora ha configurado correctamente el LDAP en un RV34x Series Router.

Ver un vídeo relacionado con este artículo...

Haga clic aquí para ver otras charlas técnicas de Cisco