# Gebruikersrekeningen configureren en beheren op een RV34x Series router

## Doel

Het doel van dit artikel is om u te tonen hoe u de lokale en afstandsbediening van uw gebruikersrekeningen op een RV34x Series router kunt configureren en beheren. Dit omvat, hoe u de complexiteit van het lokale gebruikerswachtwoord kunt configureren, bewerken/importeren, lokale gebruikers configureren, externe verificatieservice configureren met behulp van RADIUS, Active Directory en LDAP.

### Toepasselijke apparaten | Versie firmware

- RV34x Series | 1.0.01.16 (laatste download)

### Inleiding

De RV34x Series router biedt gebruikersrekeningen om instellingen te bekijken en te beheren. De gebruikers kunnen uit verschillende groepen bestaan of behoren tot logische groepen Secure Socket Layer (SSL) Virtual Private Networks (VPN's) die het verificatiedomein, Local Area Network (LAN) en de regels voor servicetoegang delen, en instellingen voor onbelaste tijd. Het gebruikersbeheer definieert welk type gebruikers een bepaald type faciliteit kunnen gebruiken en hoe dat kan worden gedaan.

De externe prioriteit van de database is altijd de inbel-gebruikersservice (RADIUS)/lichtgewicht Directory Access Protocol (LDAP)/Active Directory (AD)/Local. Als u de RADIUS-server op de router toevoegt, gebruiken de Web Login Service (Web Login Service) en andere services de externe RADIUS-database om de gebruiker voor authentiek te verklaren.

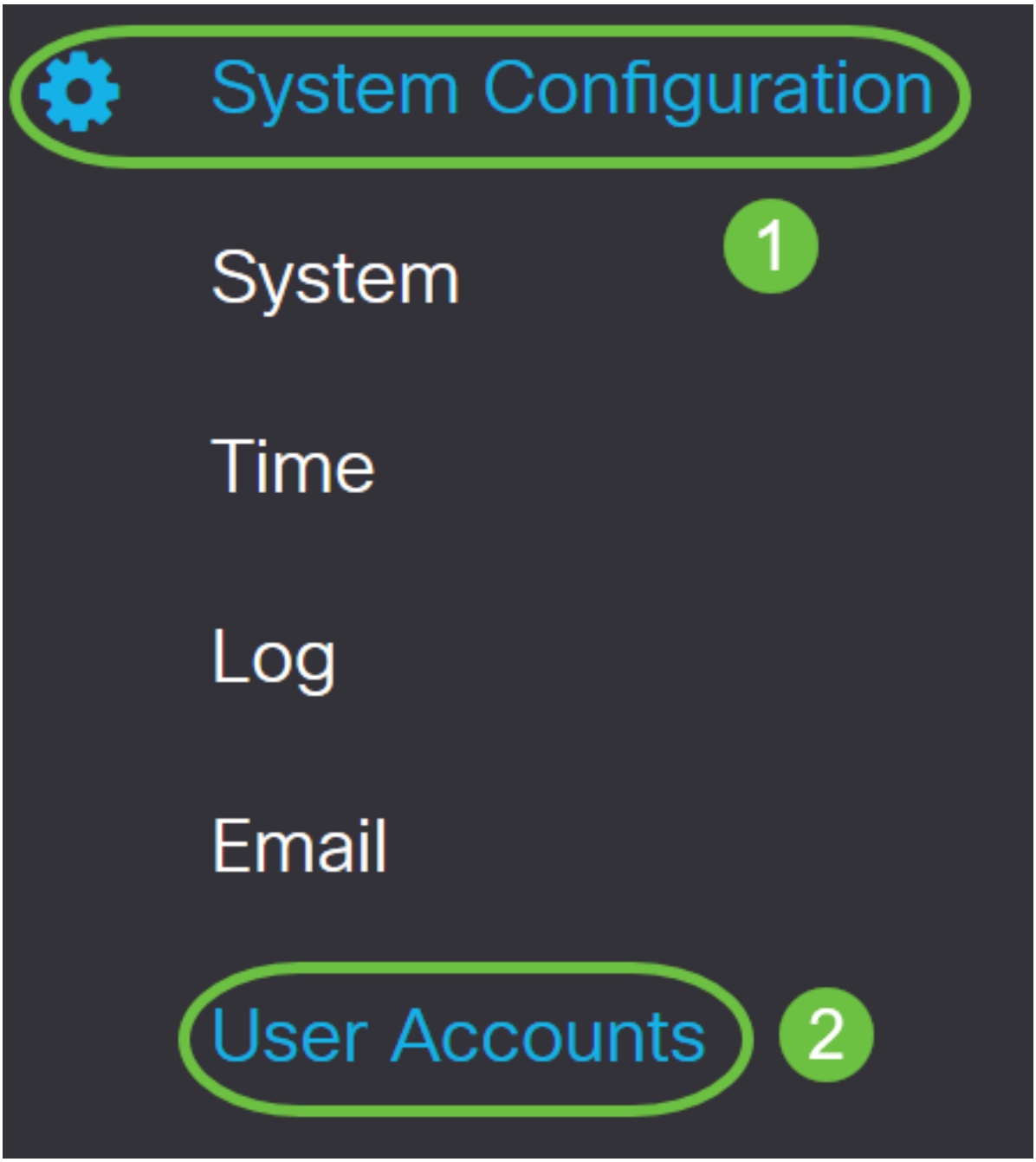
Er is geen optie om een externe database voor Web Login Service alleen in te schakelen en een andere database voor een andere service te configureren. Zodra RADIUS op de router is gemaakt en ingeschakeld, zal de router de RADIUS-service gebruiken als een externe database voor webvastlegging, Site to Site VPN, EzVPN/3rd Party VPN, SSL VPN, Point-to-Point Transport Protocol (PPTP)/Layer 2 Transport Protocol (L2TP) VPN en 802.1x.

### Inhoud

# Een lokale gebruikersaccount configureren

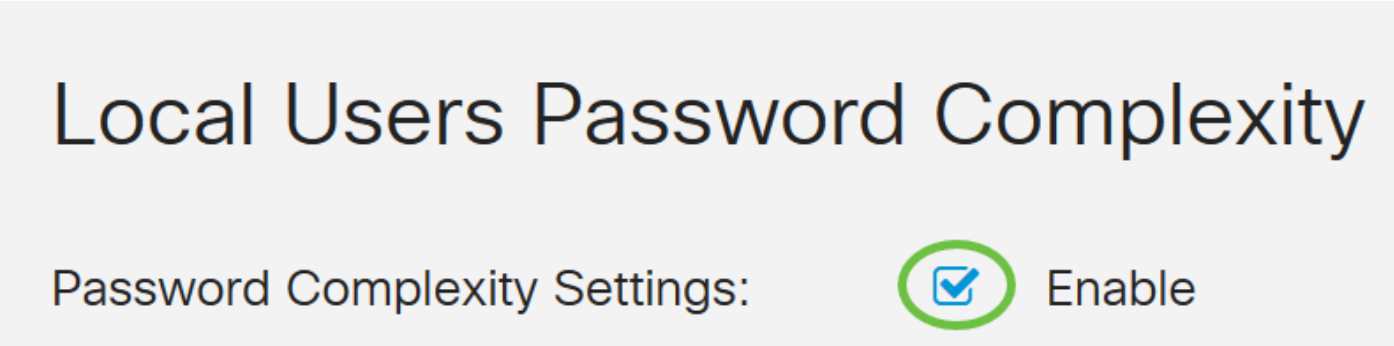
## Wachtwoord voor lokale gebruikers

Stap 1. Meld u aan bij het op web gebaseerde hulpprogramma van de router en kies **Systeemconfiguratie > Gebruikersrekeningen**.



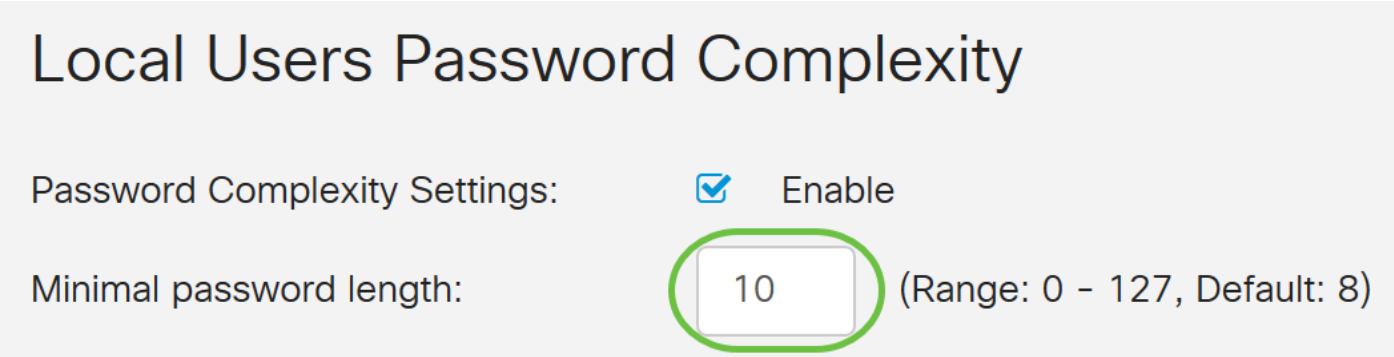

Stap 2. Controleer het vakje **Wachtwoord** complexiteit **inschakelen** om de parameters voor wachtwoordcomplexiteit in te schakelen.

Als dit niet is ingeschakeld, slaat u de knop over om lokale gebruikers te configureren.




Stap 3. In het veld *Minimale wachtwoordlengte* voert u een aantal in dat varieert van 0 tot 127 om het minimale aantal tekens in te stellen dat een wachtwoord moet bevatten. De standaard is 8.

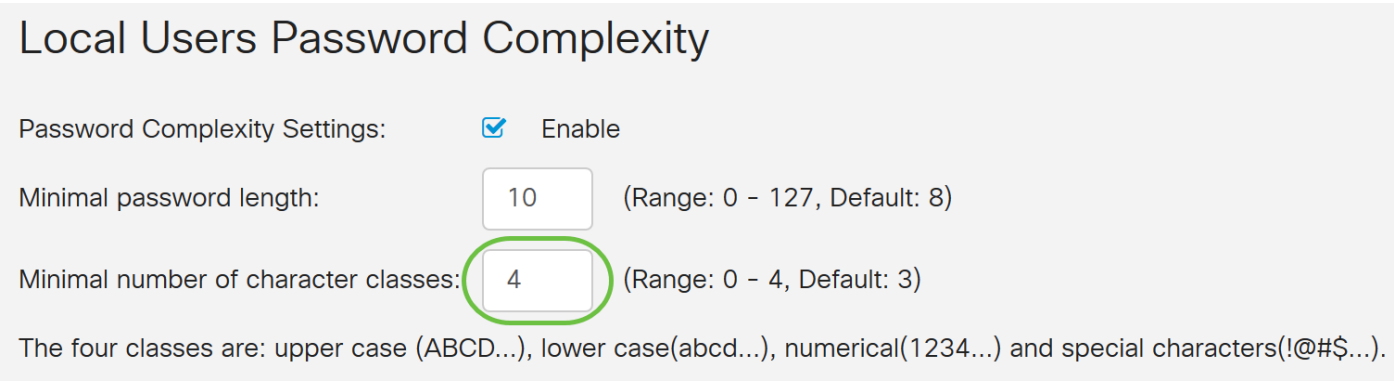
In dit voorbeeld is het minimumaantal tekens ingesteld op **10**.



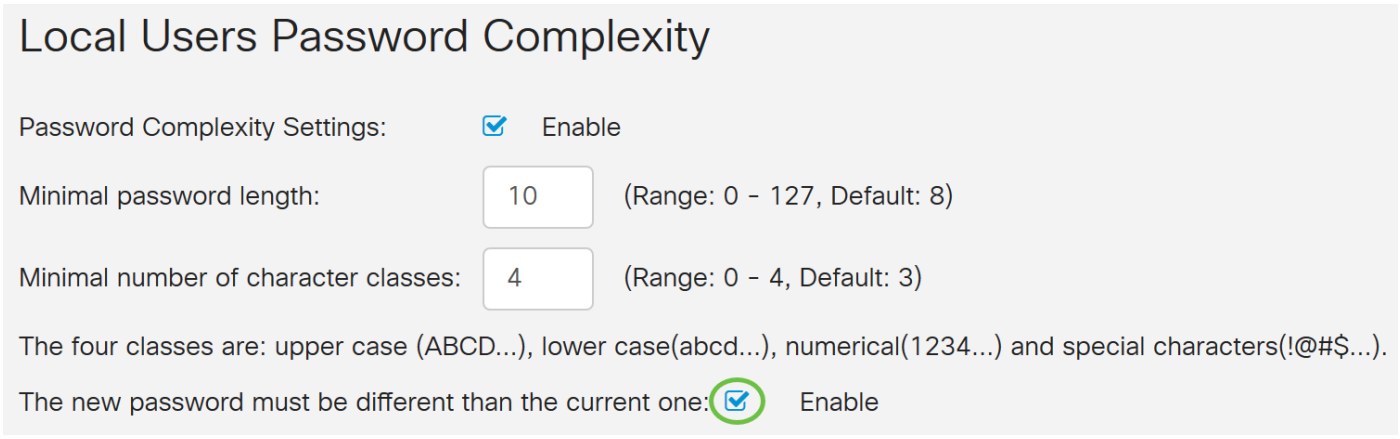

Stap 4. Voer in het veld *Minimale aantal tekenklassen* een aantal van 0 tot 4 in om de klasse in te stellen. Het opgegeven nummer vertegenwoordigt het minimum- of maximum aantal tekens van de verschillende klassen:

- Het wachtwoord bestaat uit hoofdletters (ABCD).
- Het wachtwoord bestaat uit kleine letters (abcd).
- Wachtwoord bestaat uit numerieke tekens (1234).
- Wachtwoord bestaat uit speciale tekens (!@#$).

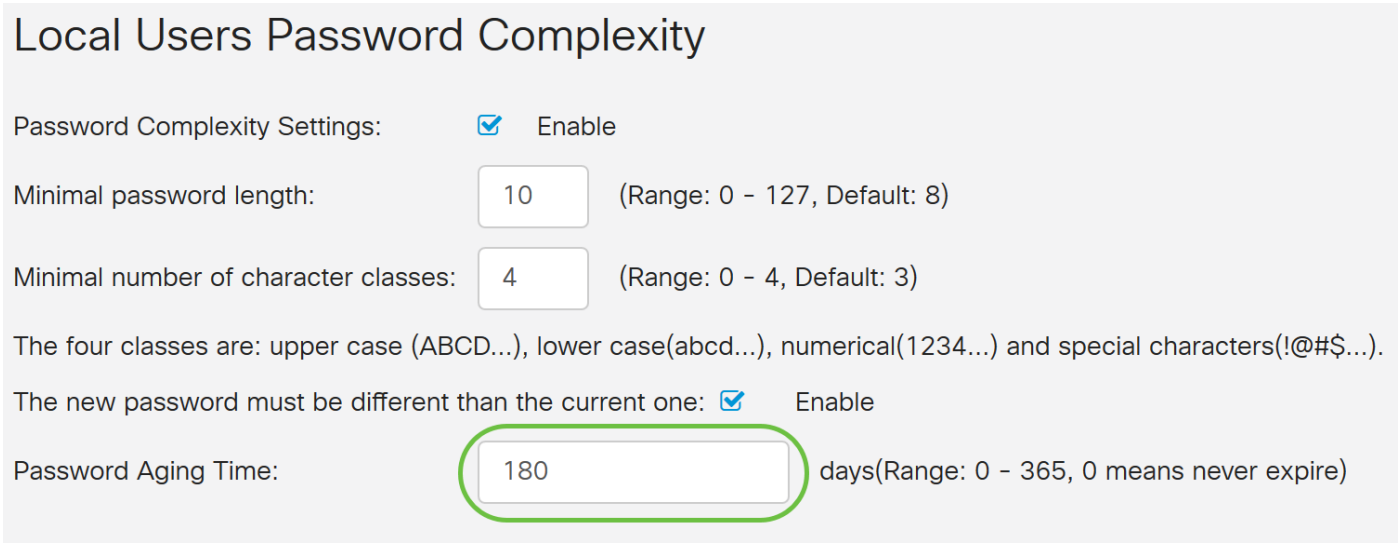
In dit voorbeeld wordt **4** gebruikt.




Stap 5. Controleer het vakje **Enable** om het nieuwe wachtwoord in te voeren.



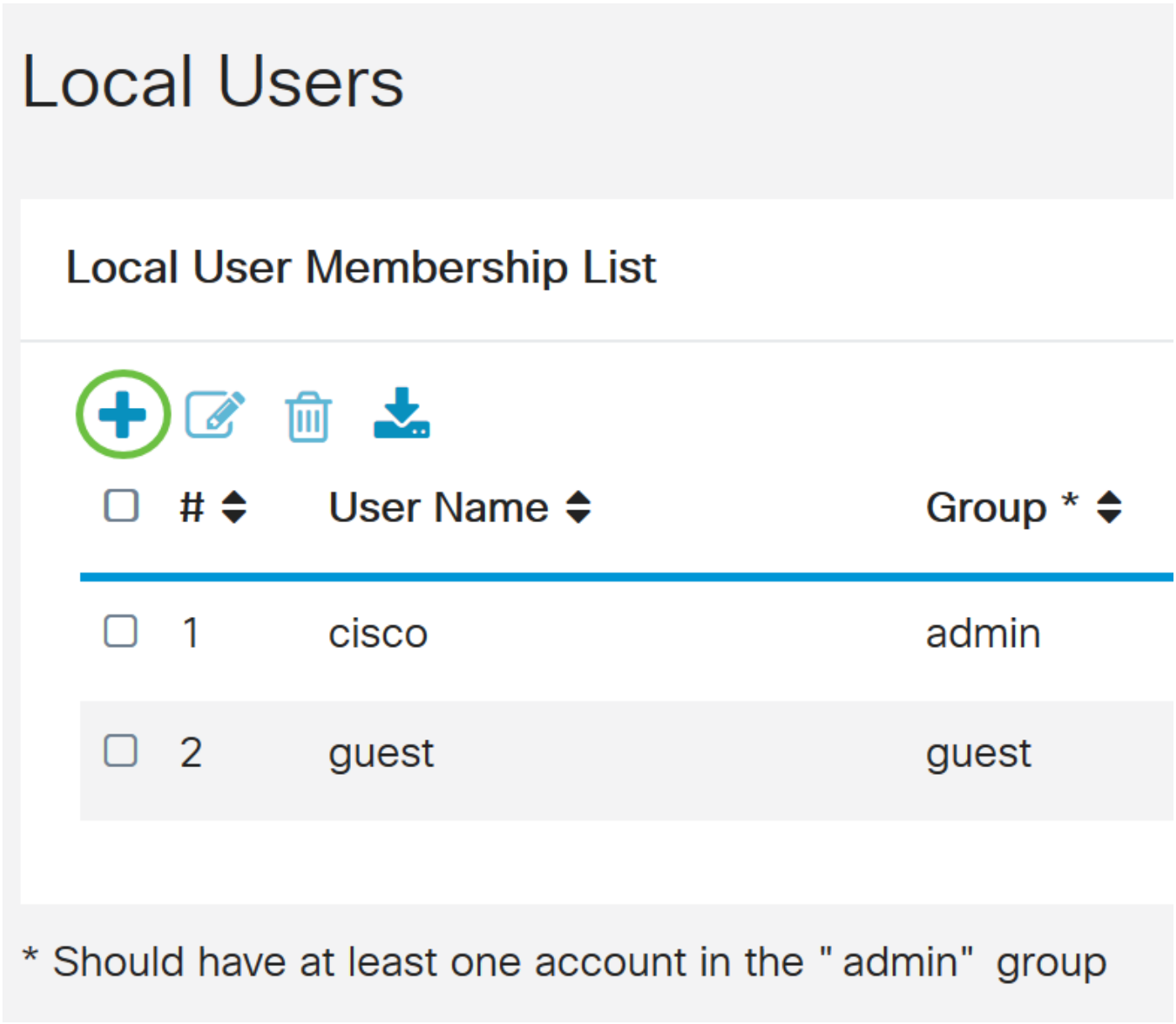

Stap 6. Voer in het veld *Wachtwoord ouder* in het aantal dagen (0 - 365) voor het verlopen van het wachtwoord. In dit voorbeeld zijn **180** dagen aangegeven.



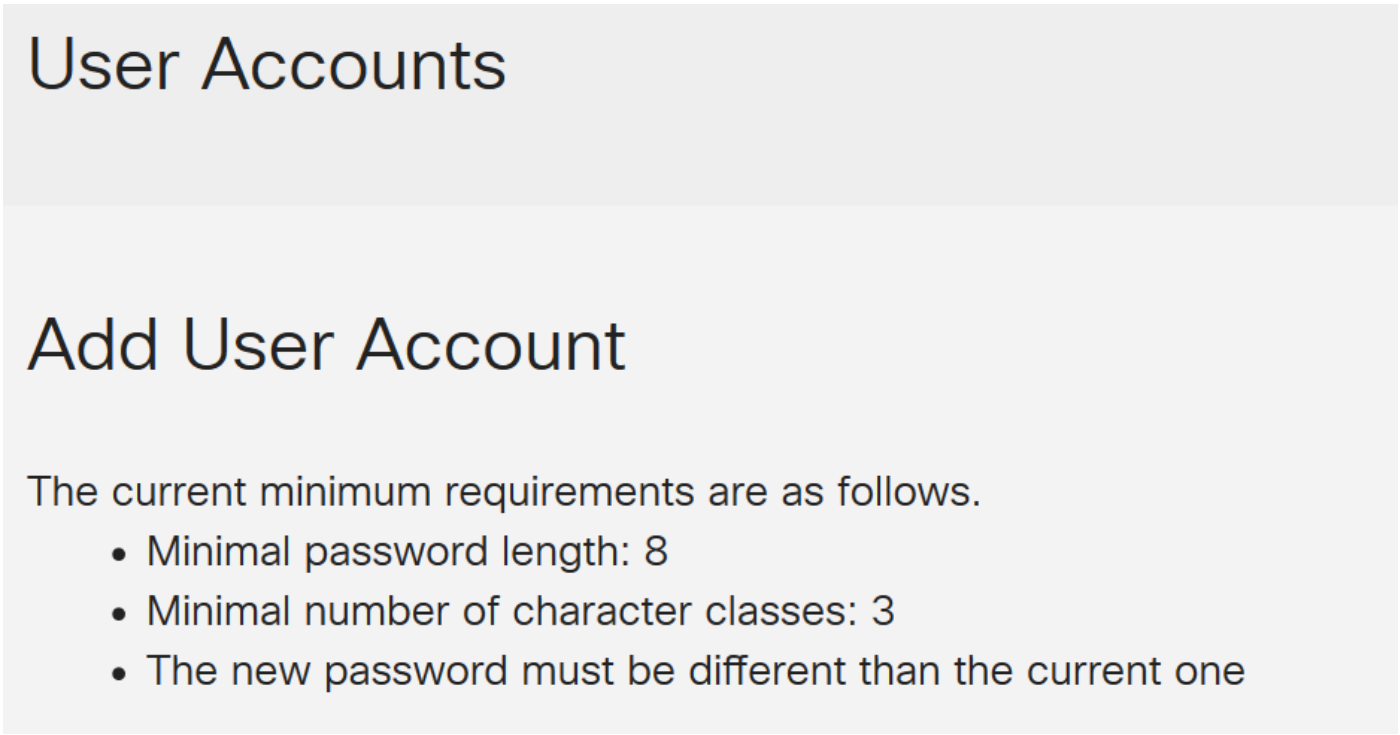

U hebt nu met succes de instellingen voor de complexiteit van het wachtwoord van lokale gebruikers op uw router ingesteld.

## Lokale gebruikers configureren

Stap 1. Klik in de tabel Local User Membership List op **Add** om een nieuwe gebruikersaccount te maken. U wordt naar de pagina Toevoegen gebruikersaccount gehouden.

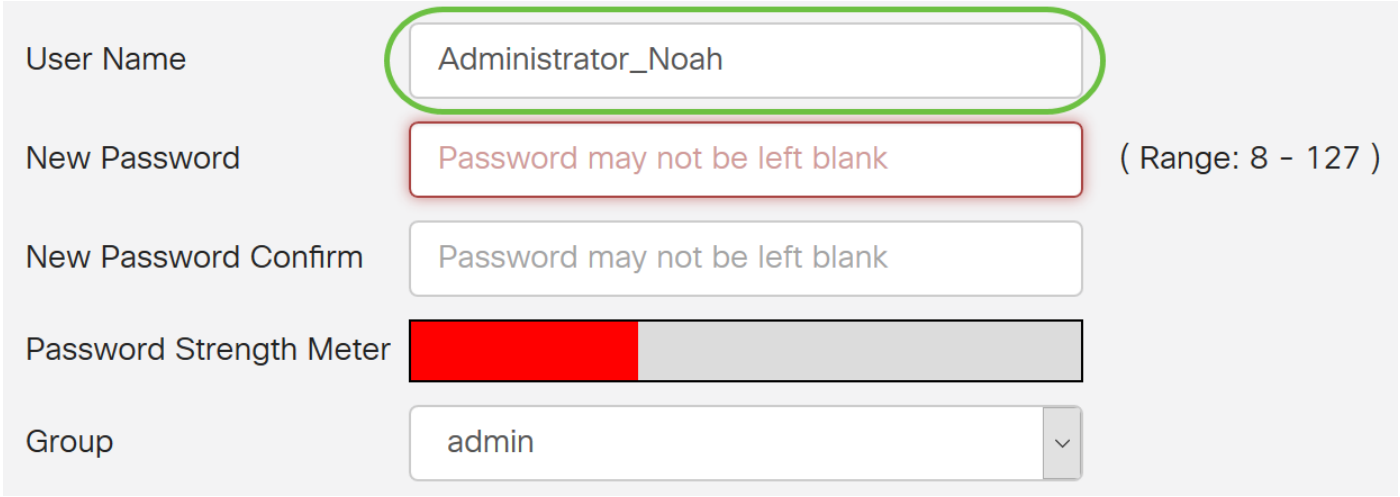



Onder de kop *gebruikersaccount toevoegen* worden de parameters weergegeven die zijn gedefinieerd onder de stappen Local Wachtwoord Complexity.

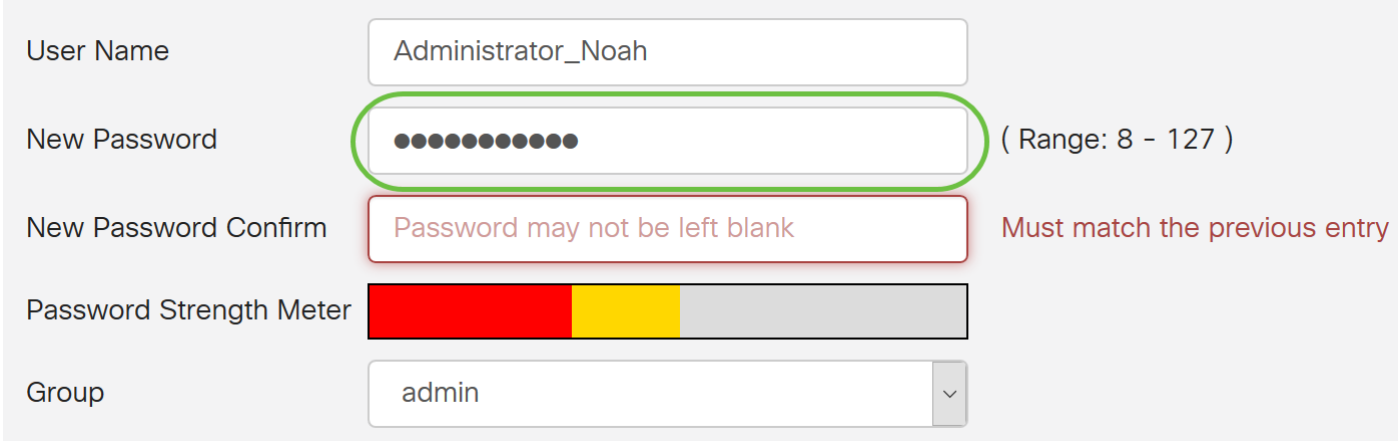



Stap 2. Voer in het veld *Gebruikersnaam* een gebruikersnaam voor de account in.

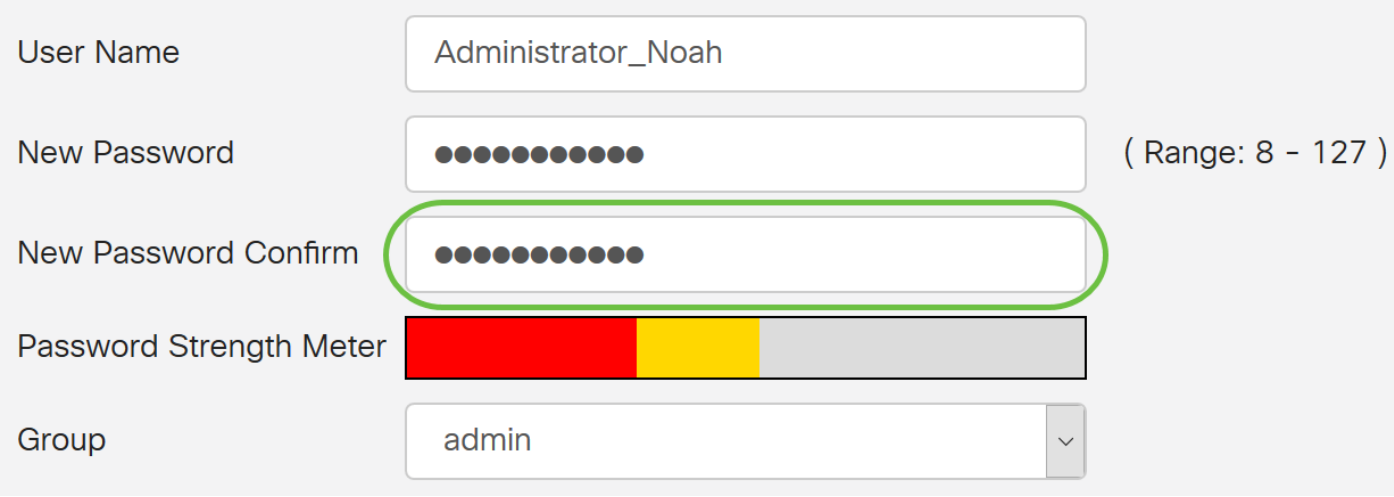
In dit voorbeeld wordt **Administrator_Noah** gebruikt.




Stap 3. Voer in het veld *Nieuw wachtwoord* een wachtwoord in met de gedefinieerde parameters. In dit voorbeeld moet de minimum wachtwoordlengte bestaan uit 10 tekens met een combinatie van hoofdletters, kleine letters, numerieke en speciale tekens.



Stap 4. Voer in het veld *Nieuw wachtwoord* opnieuw in om het wachtwoord te bevestigen. Als de wachtwoorden niet overeenkomen, verschijnt er een tekst naast het veld.

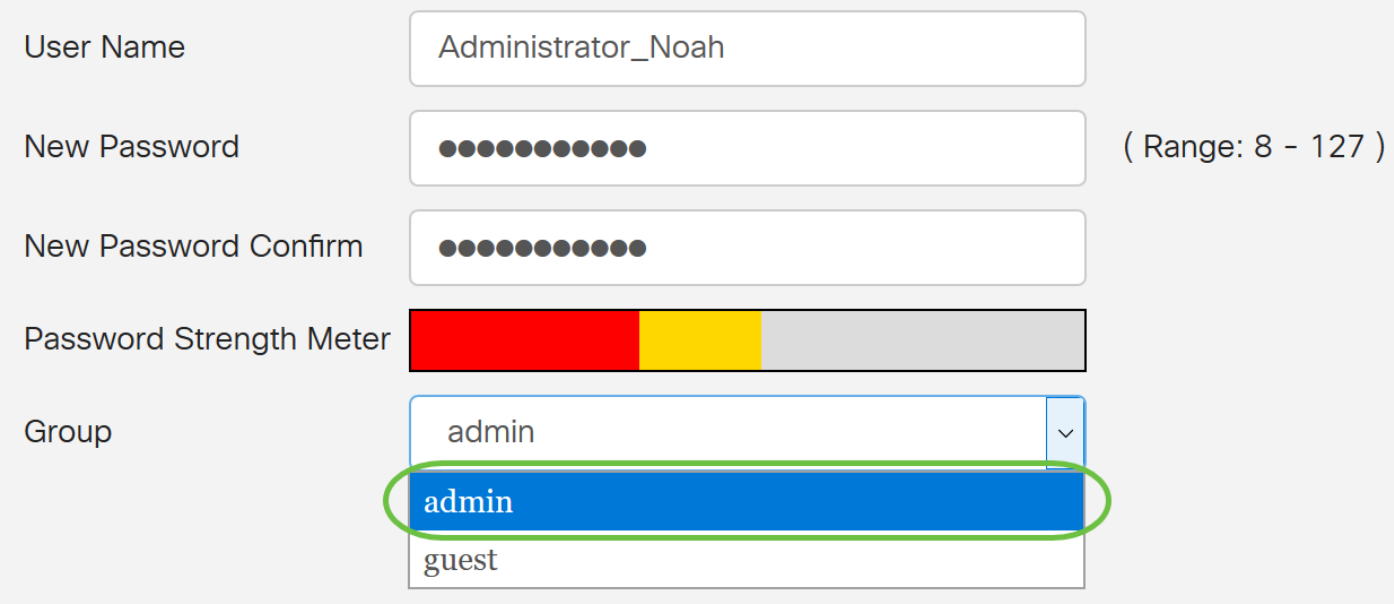



De wachtwoordversterking verandert afhankelijk van de sterkte van het wachtwoord.

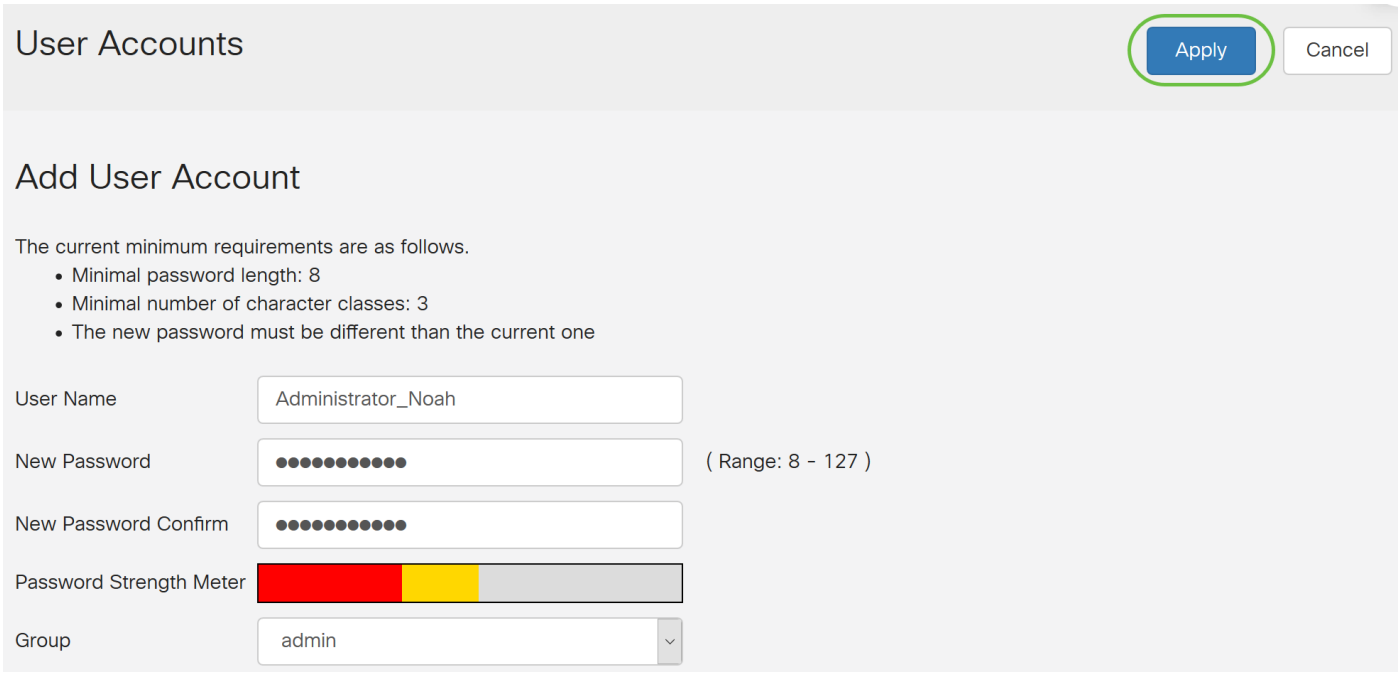

Stap 5. Kies in de vervolgkeuzelijst *Groep* een groep om een voorrecht aan een gebruikersaccount toe te wijzen. De opties zijn:

- admin - Lees- en schrijfrechten.
- gast - Lees-only privileges.

U hebt bijvoorbeeld **admin** gekozen.




Stap 6. Klik op **Toepassen**.

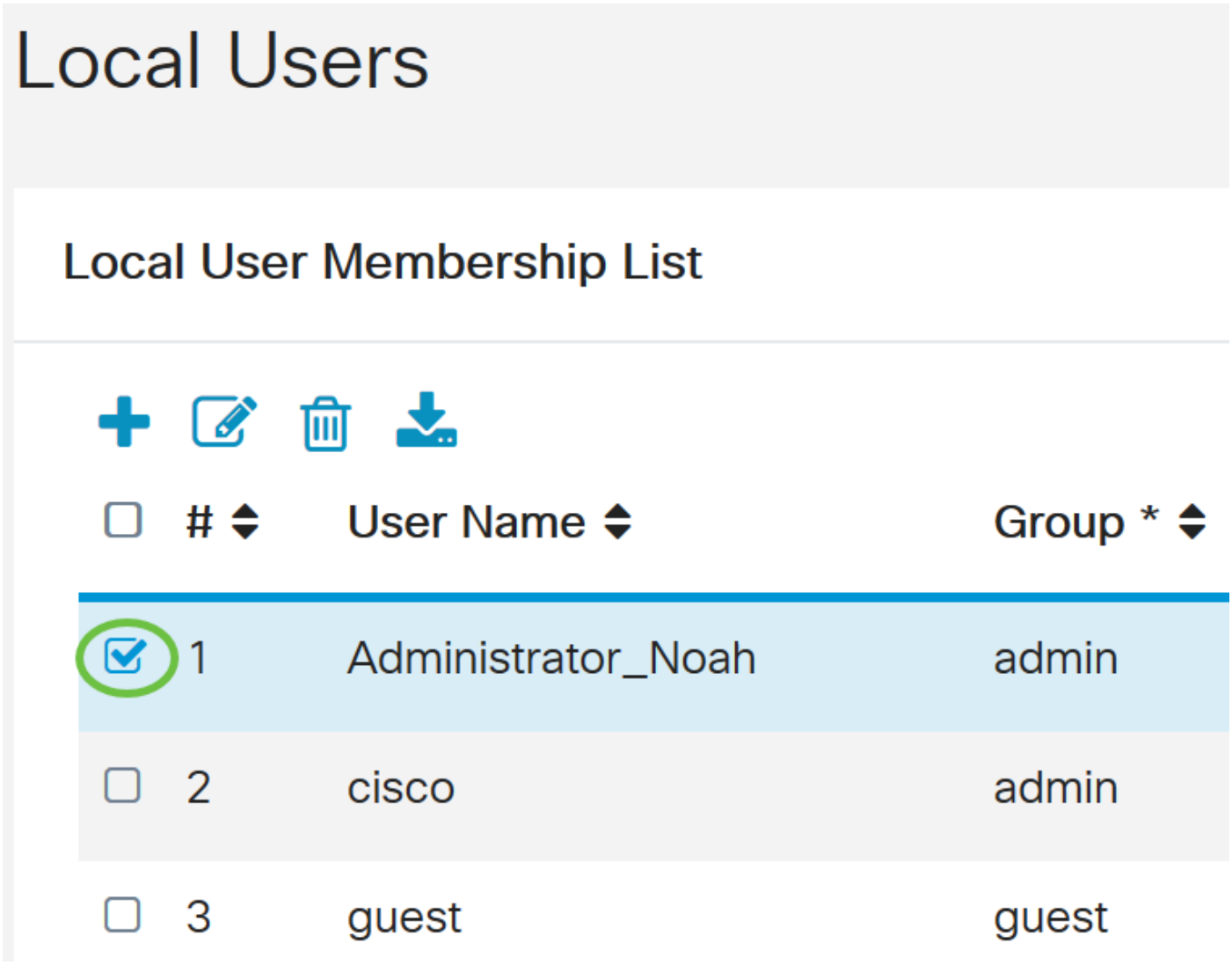



U hebt nu met succes het Lokale Gebruiker Membership op een RV34x Series router ingesteld.

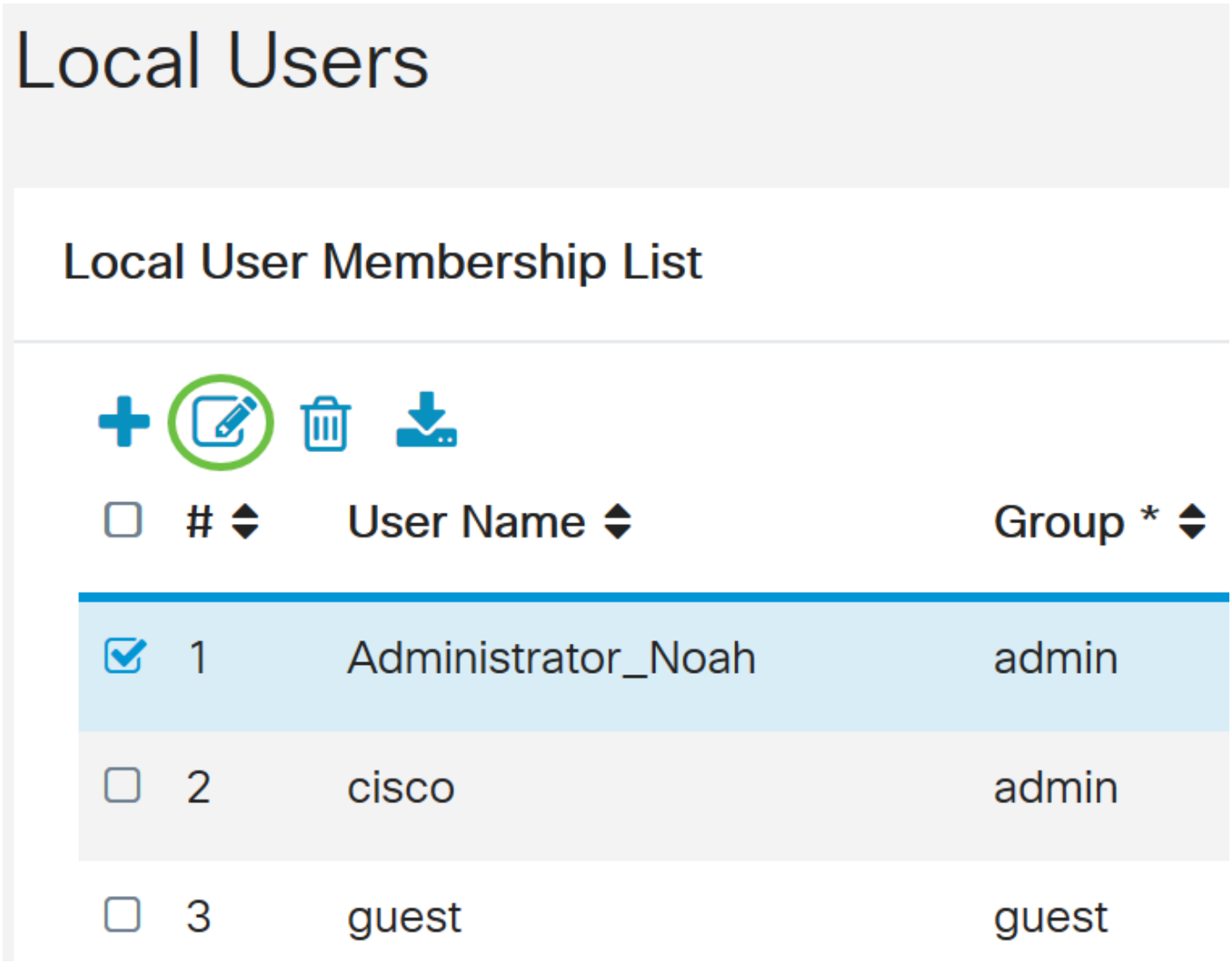
## Lokale gebruikers bewerken

Stap 1. Controleer het aankruisvakje naast de gebruikersnaam van de lokale gebruiker in de tabel met lokale gebruikers die lid zijn van de lijst.

Om dit voorbeeld te geven, wordt **Administrator_Noah** geselecteerd.

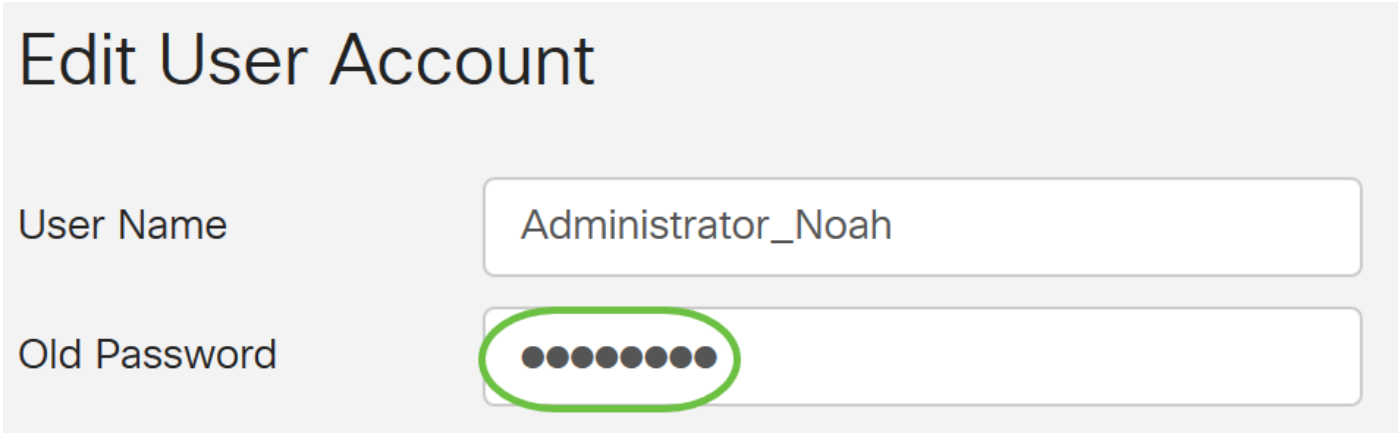



Stap 2. Klik op **Bewerken**.

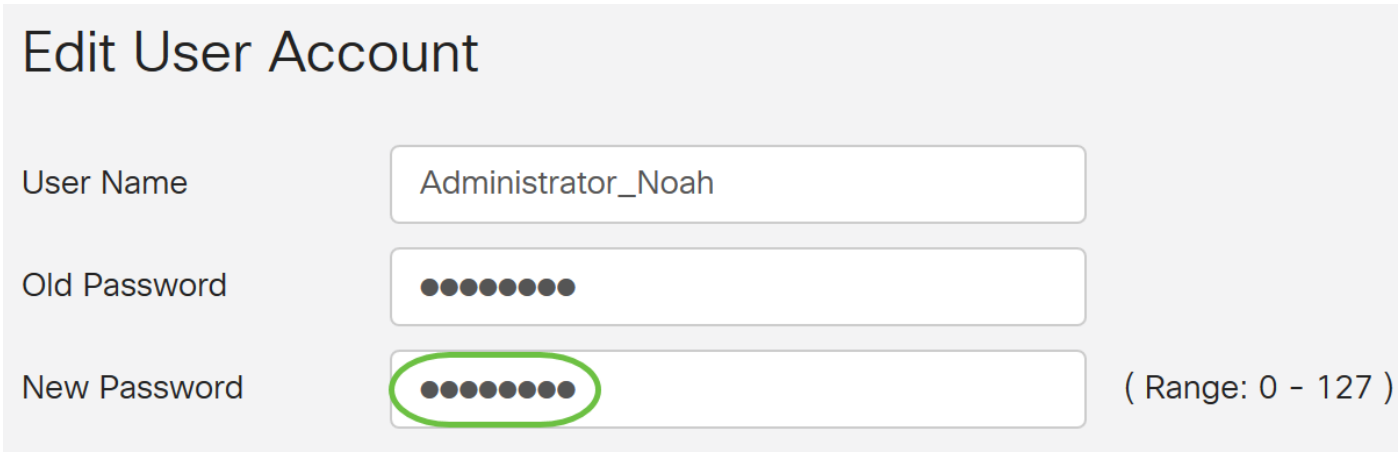



De gebruikersnaam kan niet worden bewerkt.

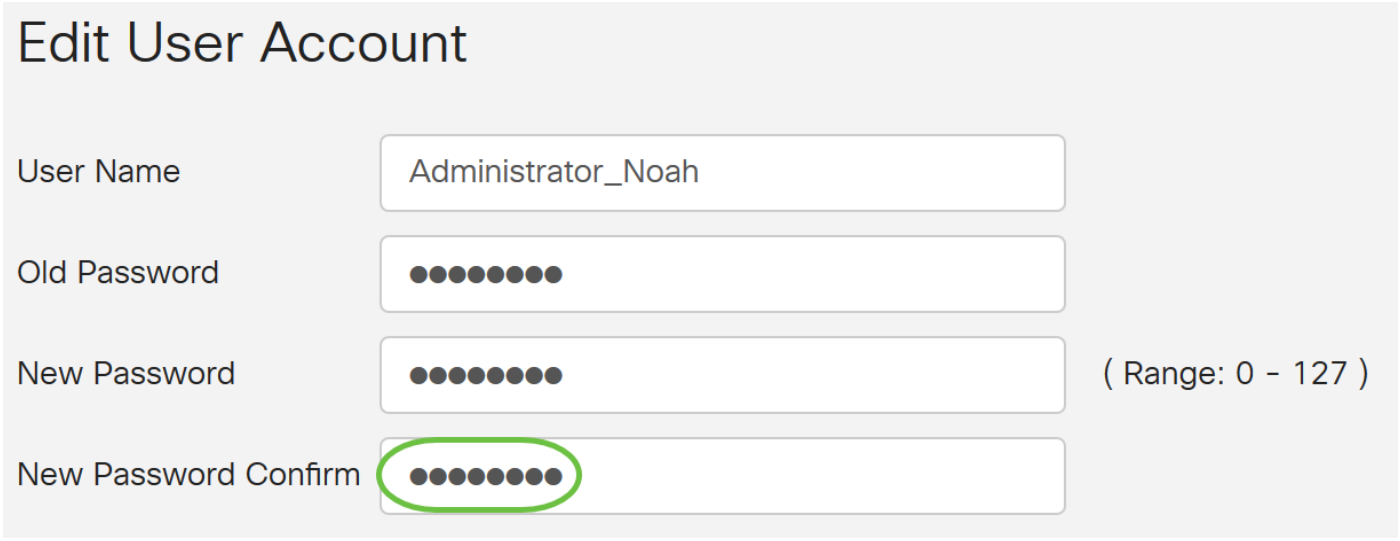
Stap 3. Voer in het veld *Oude wachtwoord* in dat eerder voor de lokale gebruikersaccount is ingesteld.




Stap 4. Voer in het veld *Nieuw wachtwoord* in. Het nieuwe wachtwoord moet aan de minimumvereisten voldoen.

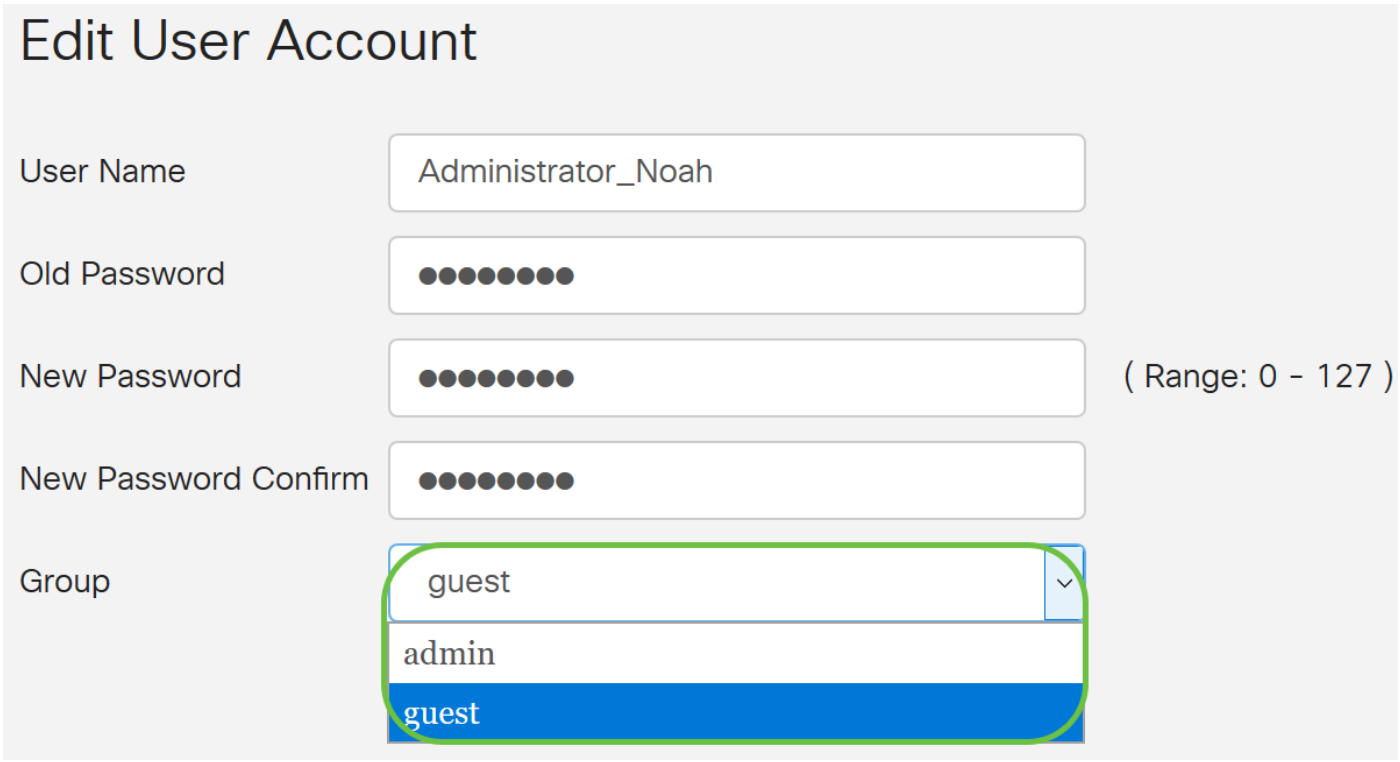



Stap 5. Voer het nieuwe wachtwoord nogmaals in het veld *Wachtwoord bevestigen*. Deze wachtwoorden moeten overeenkomen.

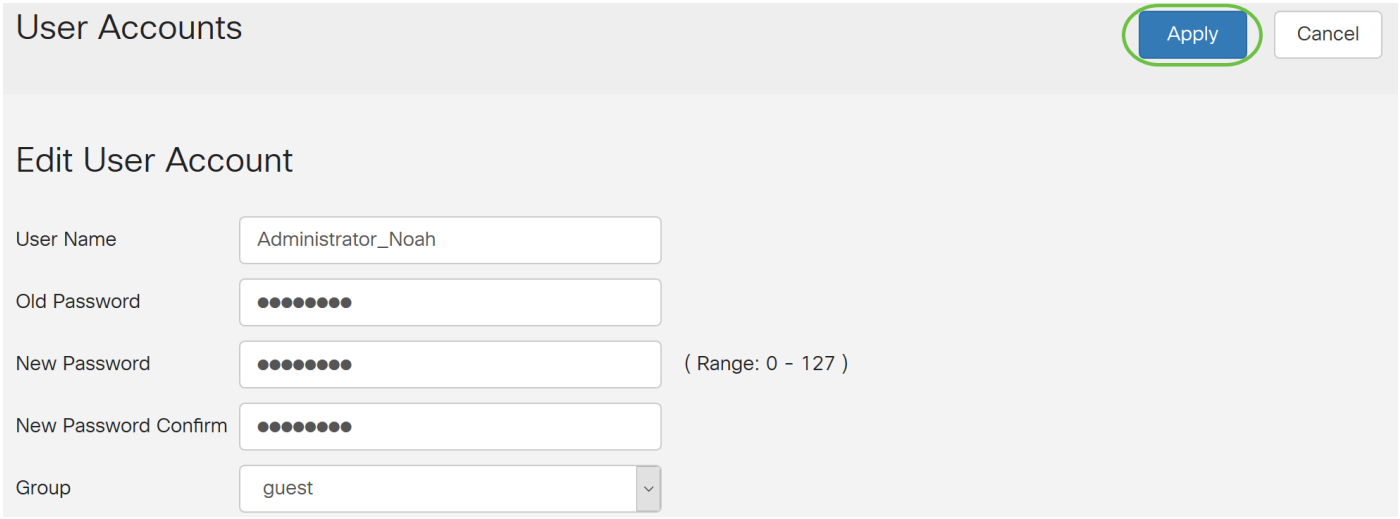



Stap 6. (Optioneel) Kies een groep in de vervolgkeuzelijst Groep om een voorrecht aan een gebruikersaccount toe te wijzen.

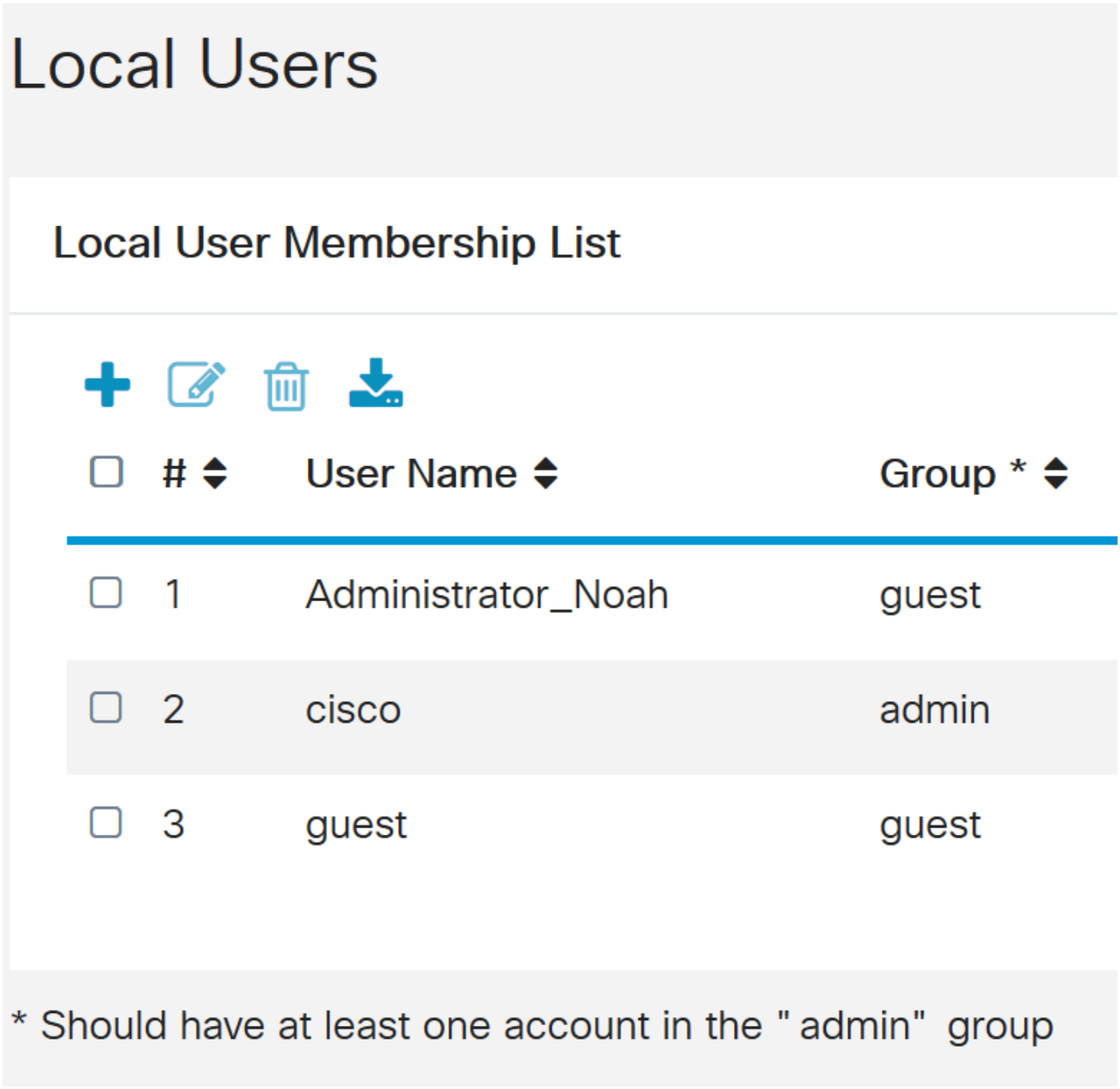
In dit voorbeeld wordt de **gast** gekozen.




Stap 7. Klik op **Toepassen**.




U moet nu een lokale gebruikersaccount hebben bewerkt.

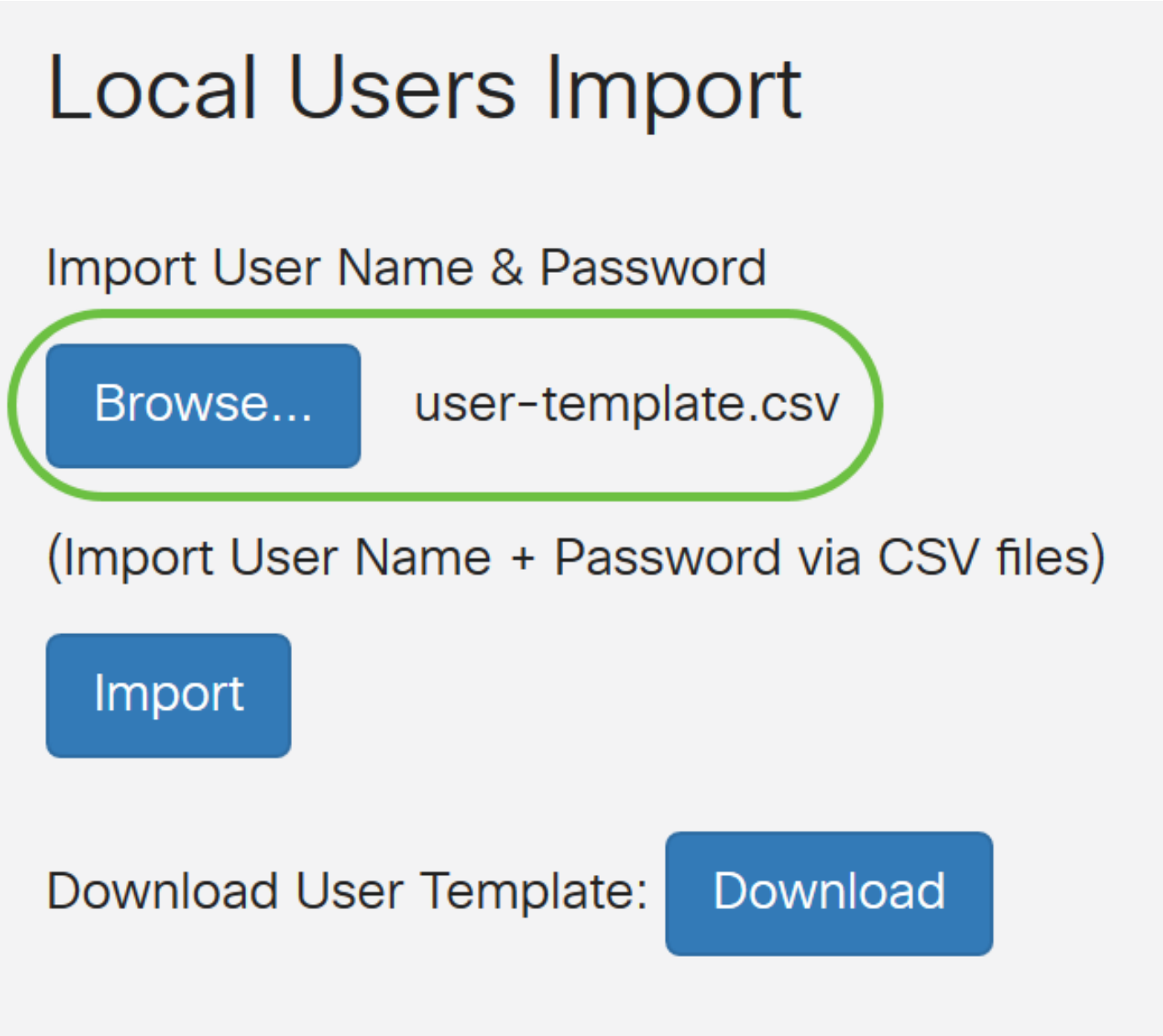



## Lokale gebruikers importeren

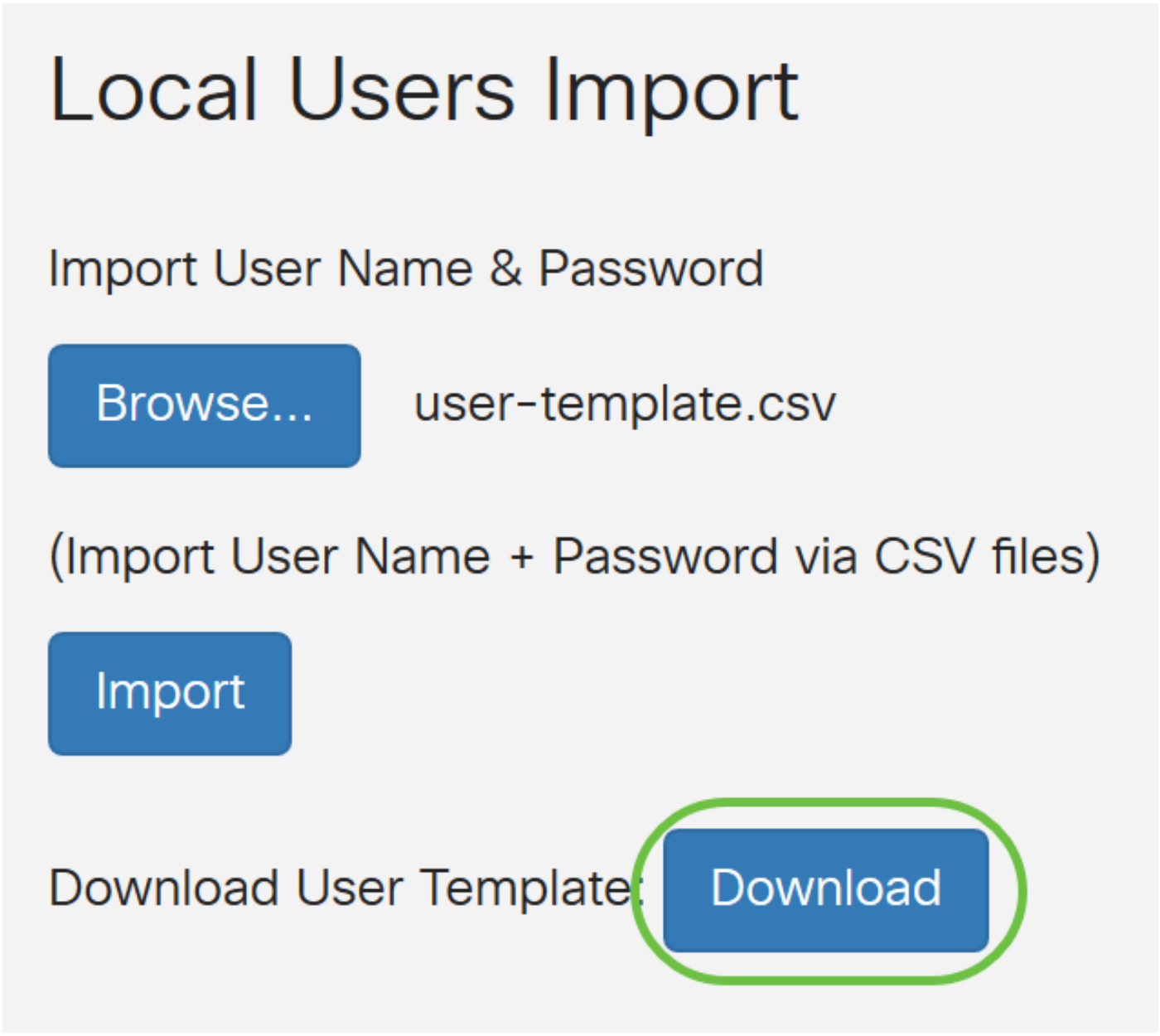
Stap 1. Klik in het gedeelte Local Gebruikers Importeren op  .

Stap 2. Klik onder Gebruikersnaam en wachtwoord importeren op **Bladeren...** om een lijst met gebruikers te importeren. Dit bestand is doorgaans een spreadsheet die in een Comma Separated Value (.CSV)-formaat is opgeslagen.

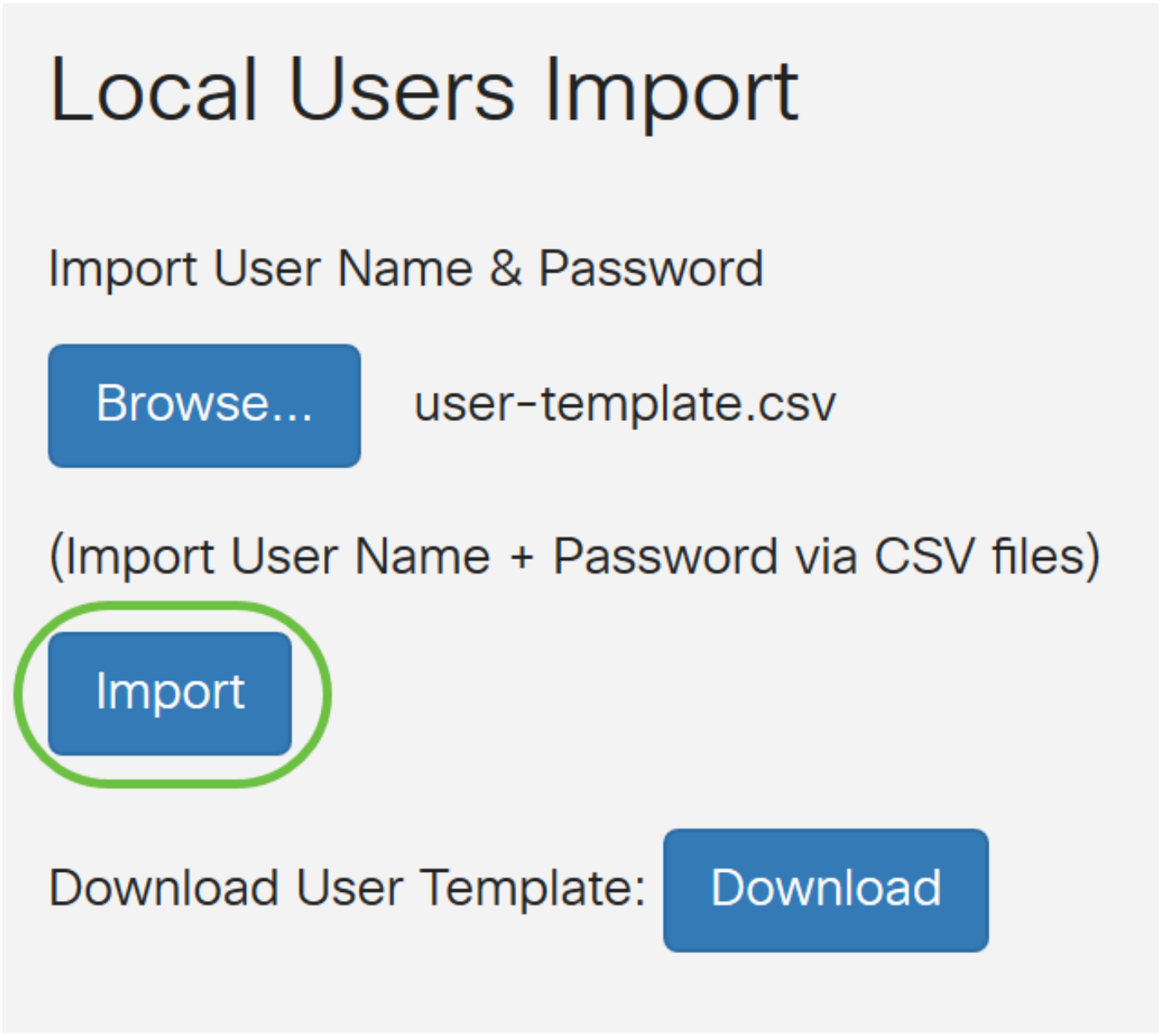
In dit voorbeeld wordt **user-sjabloon.csv** gekozen.




Stap 3. (Optioneel) Als u geen sjabloon hebt, klikt u op in het gedeelte met **Downloadsjabloon**.




Stap 4. Klik op **Importeren**.



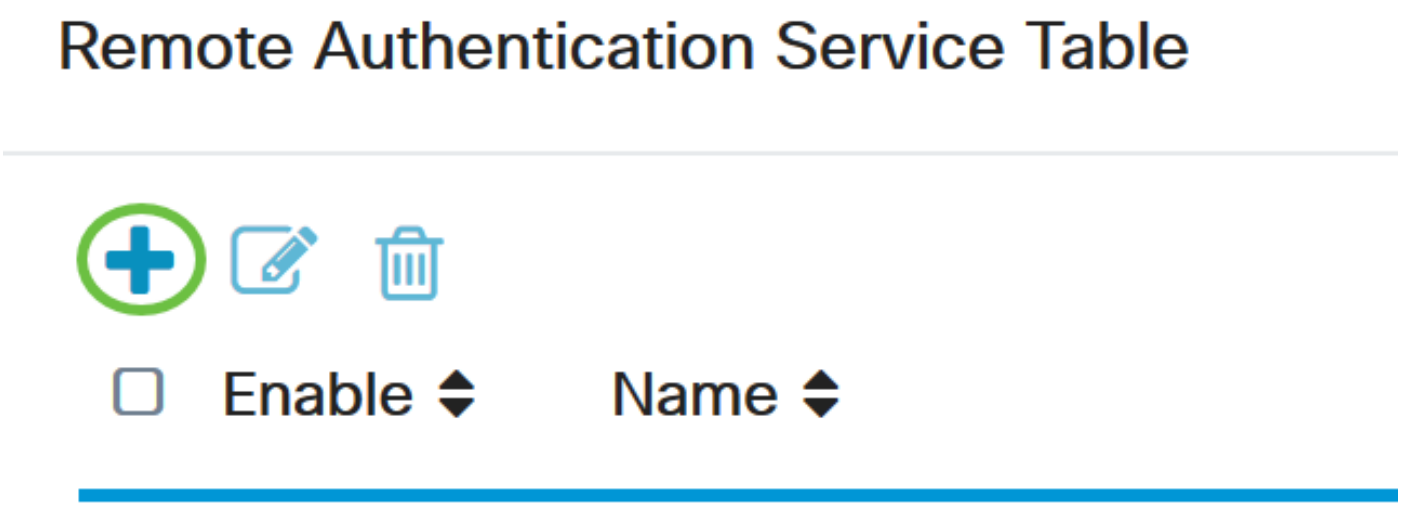

Er verschijnt een bericht naast de knop Importeren dat de import is geslaagd.

U hebt nu met succes een lijst met lokale gebruikers geïmporteerd.

## Remote-verificatieservice

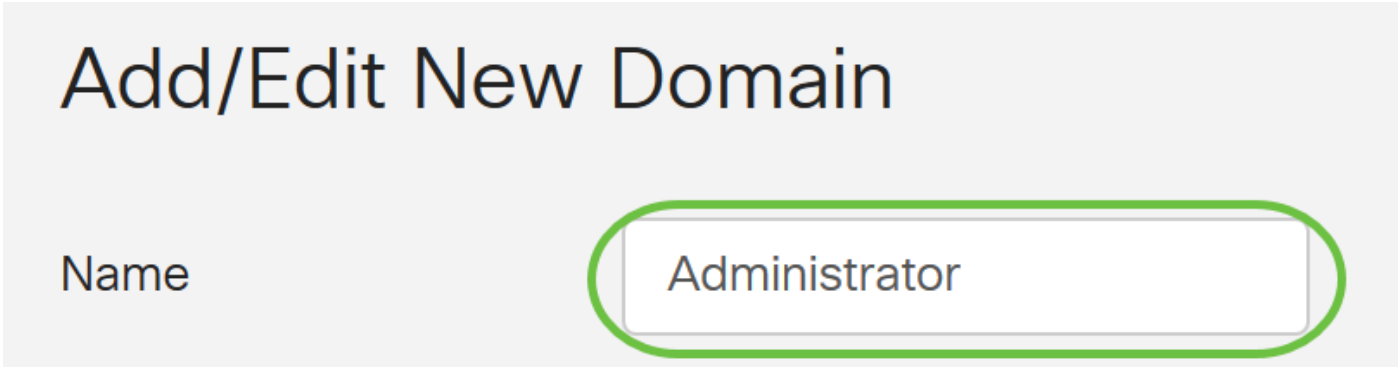
### RADIUS

Stap 1. In de tabel met afstandsverificatie klikt u op **Add** om een ingang te maken.



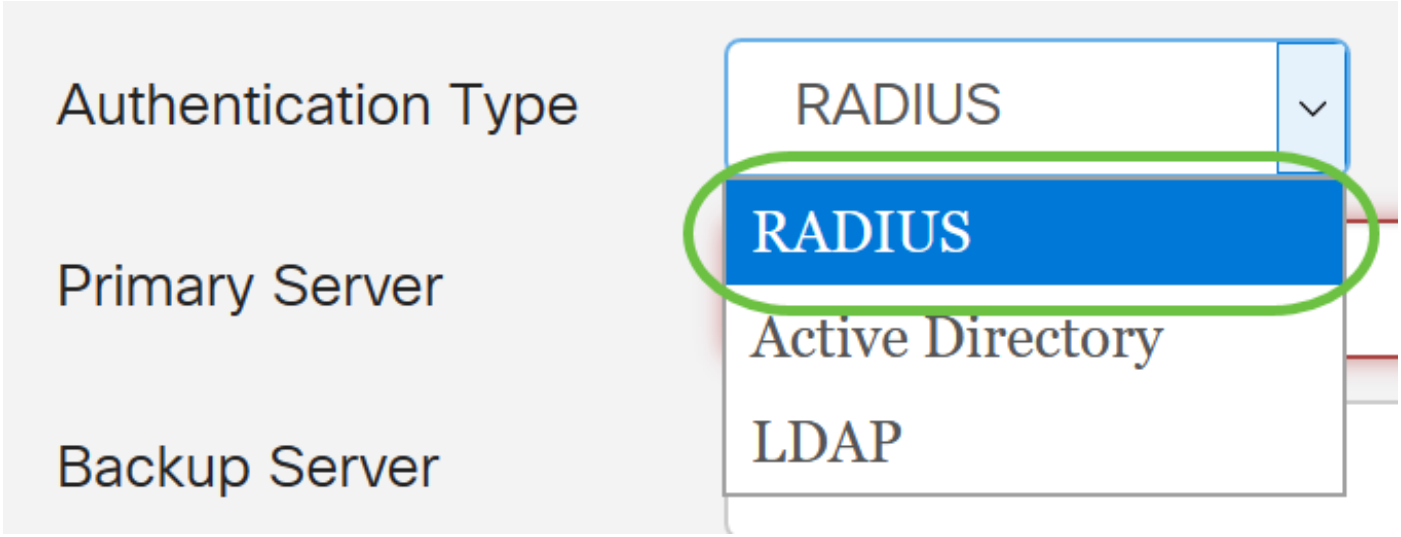

Stap 2. Voer in het veld *Naam* een gebruikersnaam voor de account in.

De **beheerder** wordt bijvoorbeeld gebruikt.




Stap 3. Kies in het vervolgkeuzemenu Verificatietype **Straal**. Dit betekent dat de gebruikersverificatie via een RADIUS-server wordt uitgevoerd.

Er kan slechts één externe gebruikersaccount onder RADIUS worden ingesteld.

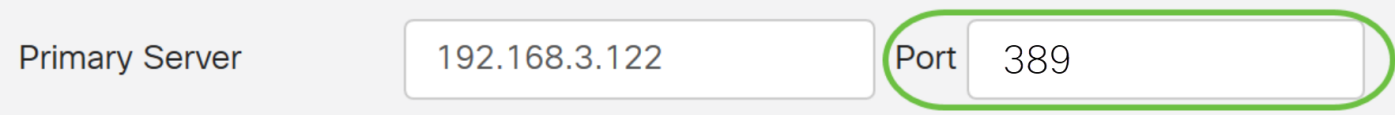



Stap 4. Voer in het veld *Primaire server* het IP-adres van de primaire RADIUS-server in.

In dit voorbeeld wordt **192.168.3.122** gebruikt als primaire server.

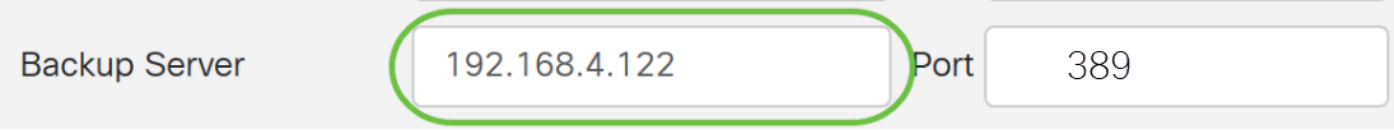

Stap 5. Voer in het veld *Port* het poortnummer van de primaire RADIUS-server in.

Bijvoorbeeld, **1645** wordt gebruikt als havennummer.




Stap 6. Voer in het veld *Backup Server* het IP-adres in van de RADIUS-server op de back-up. Dit dient als een failover voor het geval de primaire server uitvalt.

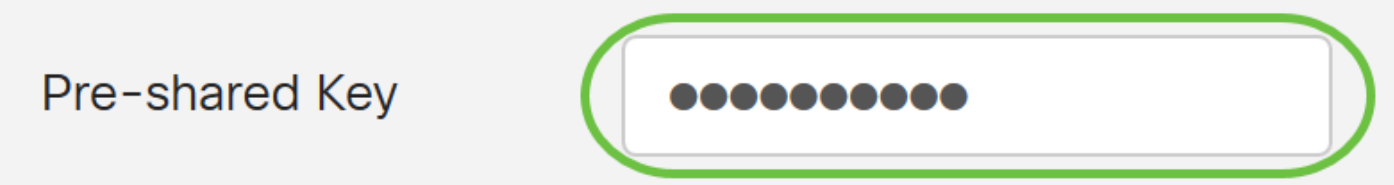
In dit voorbeeld is het adres van de reserveserver **192.168.4.122**.



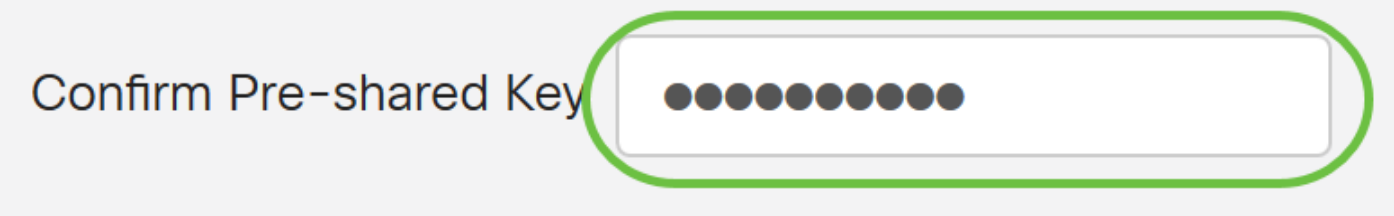

Stap 7. Voer in het veld *Port* het aantal RADIUS-back-upservers in.


In dit voorbeeld wordt **1646** gebruikt als havennummer.

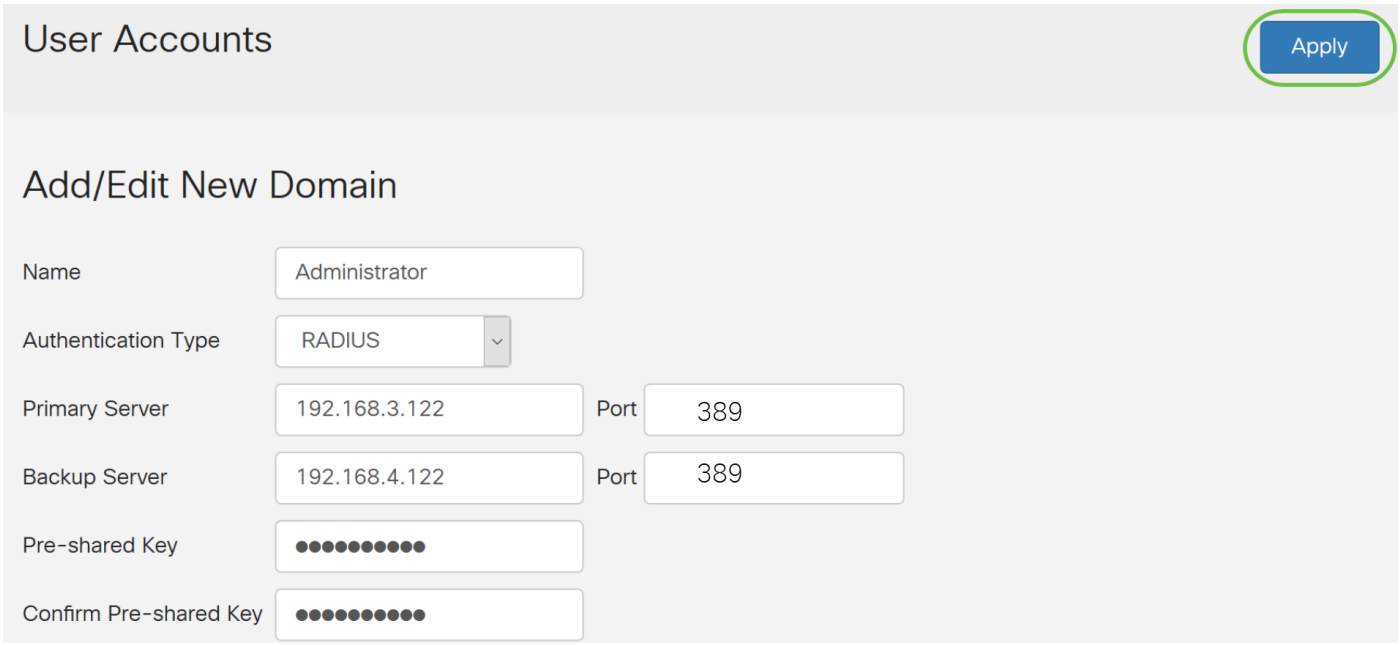
Stap 8. In het veld *PreShared-Key* voert u de vooraf gedeelde toets in die op de RADIUS-server is geconfigureerd.




Stap 9. Voer in het veld Geavanceerd *bevestigen* de voorgedeelde toets opnieuw in om te bevestigen.




Stap 10. Klik op **Toepassen**.

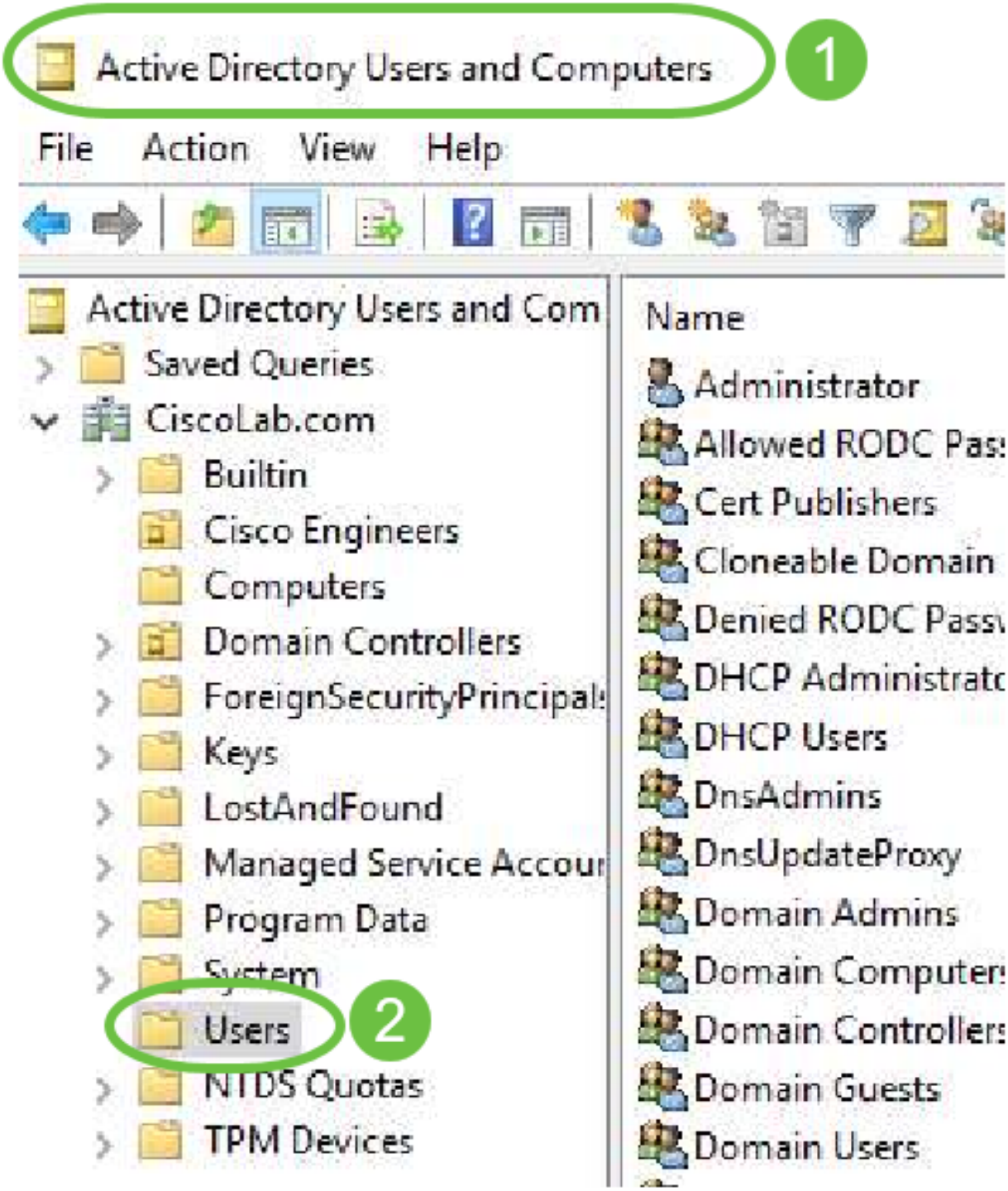



U wordt naar de pagina met de hoofdgebruikersaccount gebracht. De onlangs gevormde account verschijnt nu in de tabel met de afstandsbediening.

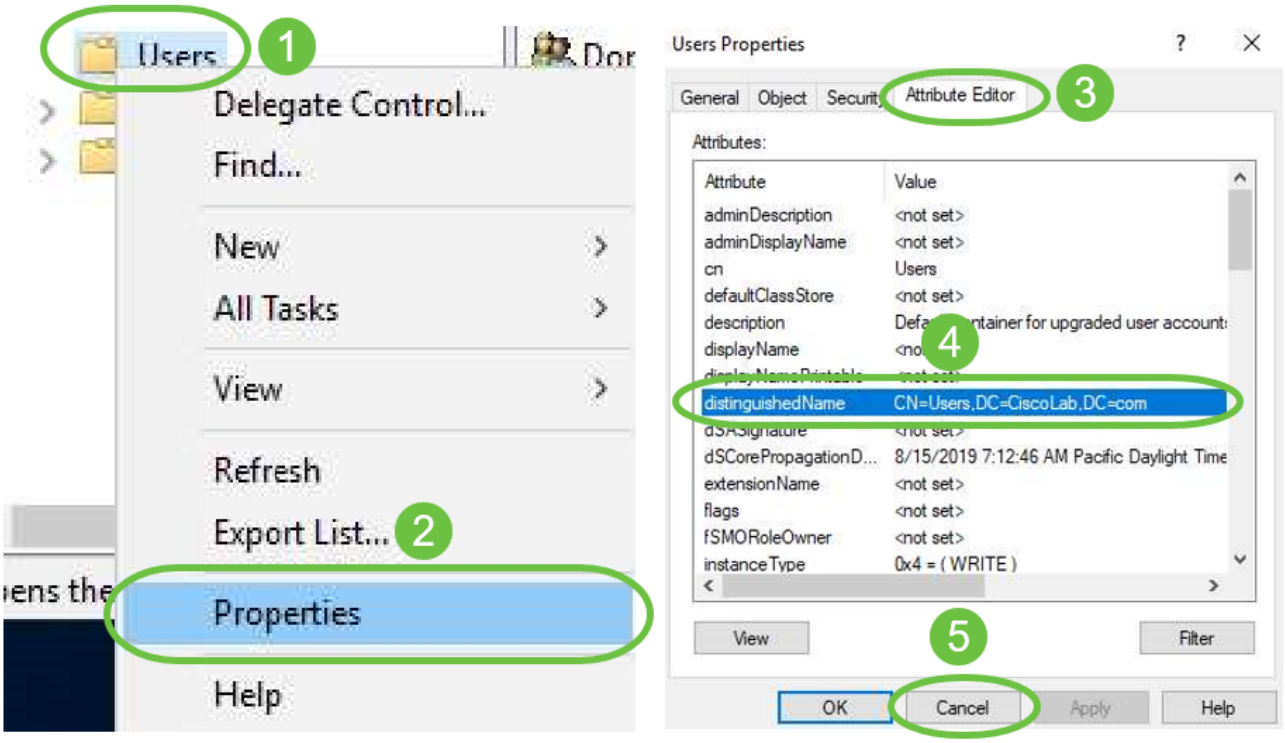
U hebt nu met succes RADIUS-verificatie ingesteld op een RV34x Series router.

## Configuratie actieve map

Stap 1. Om de configuratie van de actieve map te voltooien, moet u inloggen op de Active Directory Server. Op uw PC, open **Actieve de gebruikers en de Computers van de Map** en navigeer naar de container die de gebruikersrekeningen gebruikt zal hebben om extern in te loggen. In dit voorbeeld zullen we de **gebruikerscontainer** gebruiken.




Stap 2. Klik met de rechtermuisknop op de container en selecteer **Eigenschappen**. Blader naar het tabblad *Lijst met eigenschappen* en vind het veld *Naam*. Als dit tabblad niet zichtbaar is, moet u de geavanceerde functieweergave in actieve gebruikers en computers inschakelen en opnieuw starten. Let op dit veld en klik op **Annuleren**. Dit is het gebruikerspatroon. Dit veld zal ook nodig zijn bij het configureren van de RV340 en moet precies overeenkomen.



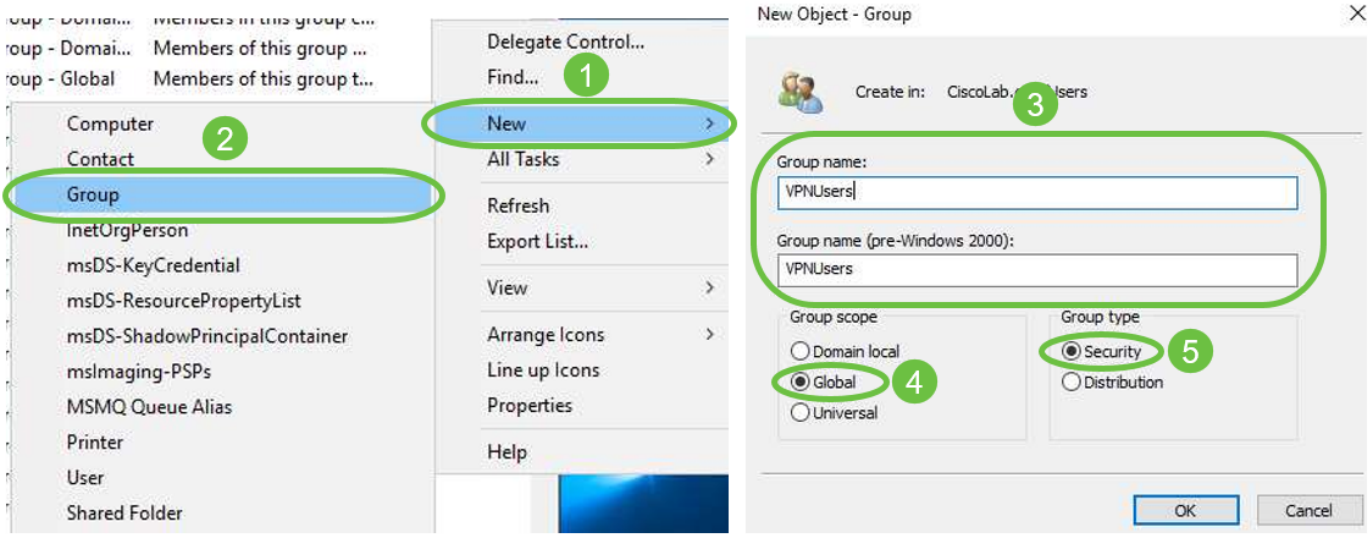

Stap 3. Maak een Global Security Group in dezelfde container als de Gebruikersrekeningen die zullen worden gebruikt.

Klik in de geselecteerde container met de rechtermuisknop op een leeg gebied en selecteer **Nieuw > Groep**.

Selecteer het volgende:

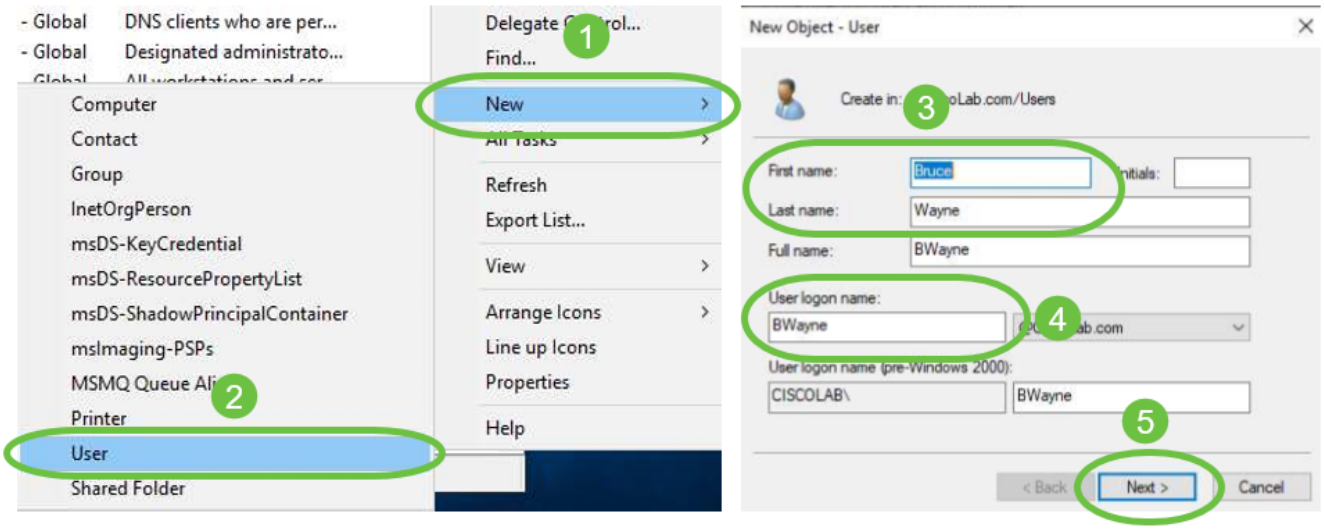
- groepsnaam - Deze naam moet exact overeenkomen met de naam van de gebruikersgroep die op de RV340 is gemaakt. In dit voorbeeld gebruiken we **VPN-gebruikers**.
- Groepstoepassingsgebied - mondiaal
- Type groep - beveiliging

Klik op **OK**.




Stap 4. Voer de volgende handelingen uit om nieuwe gebruikersrekeningen te maken:

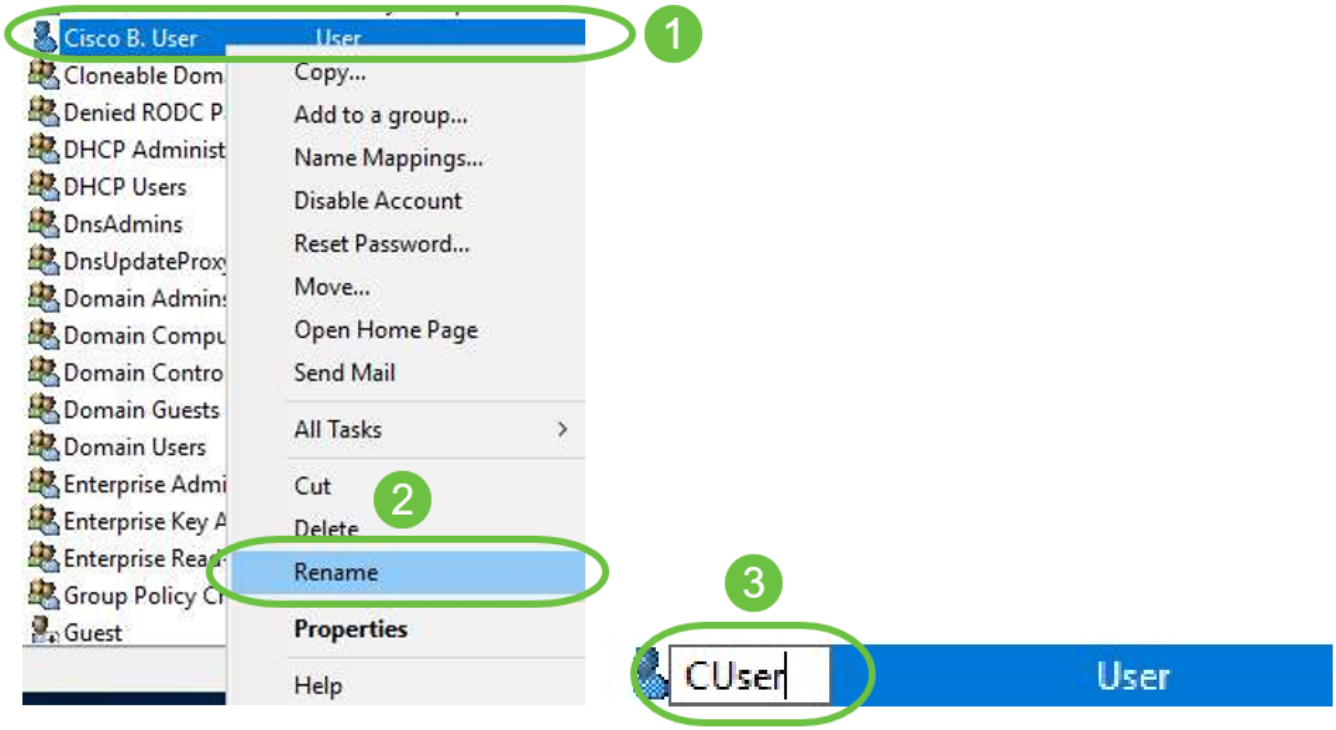
- Klik met de rechtermuisknop op een lege ruimte in de container en selecteer **Nieuw > Gebruiker**.
- Voer *voornaam* en *achternaam in*.
- Voer de *gebruikersnaam in*.
- Klik op **Volgende**.




U wordt gevraagd een wachtwoord voor de gebruiker in te voeren. Als *de gebruiker het wachtwoord moet wijzigen* in het *volgende* aanmelding is ingeschakeld, moet de gebruiker lokaal inloggen en het wachtwoord wijzigen voordat hij zich op afstand inlogt.

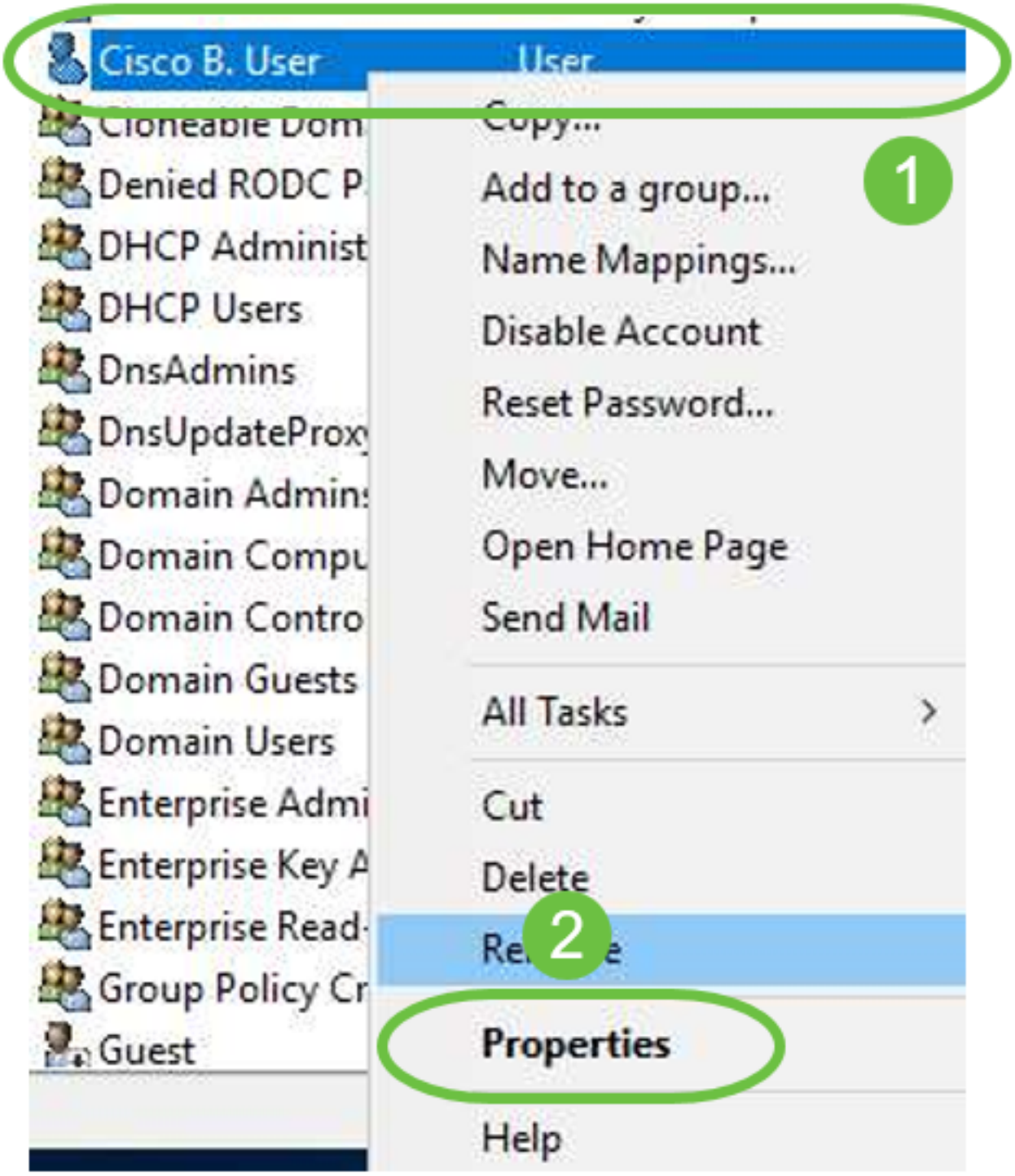
Klik op **Voltooien**.

Als er al gebruikersaccounts zijn gemaakt die moeten worden gebruikt, moeten er mogelijk aanpassingen worden gemaakt. Als u de canonische naam van een gebruiker wilt aanpassen, selecteert u de gebruiker, klikt u met de rechtermuisknop en selecteert u **Hernoemen**. Zorg ervoor dat alle spaties zijn verwijderd en dat deze overeenkomen met de lognaam van de gebruiker. Dit verandert DE naam van het gebruikersdisplay NIET. Klik op **OK**.

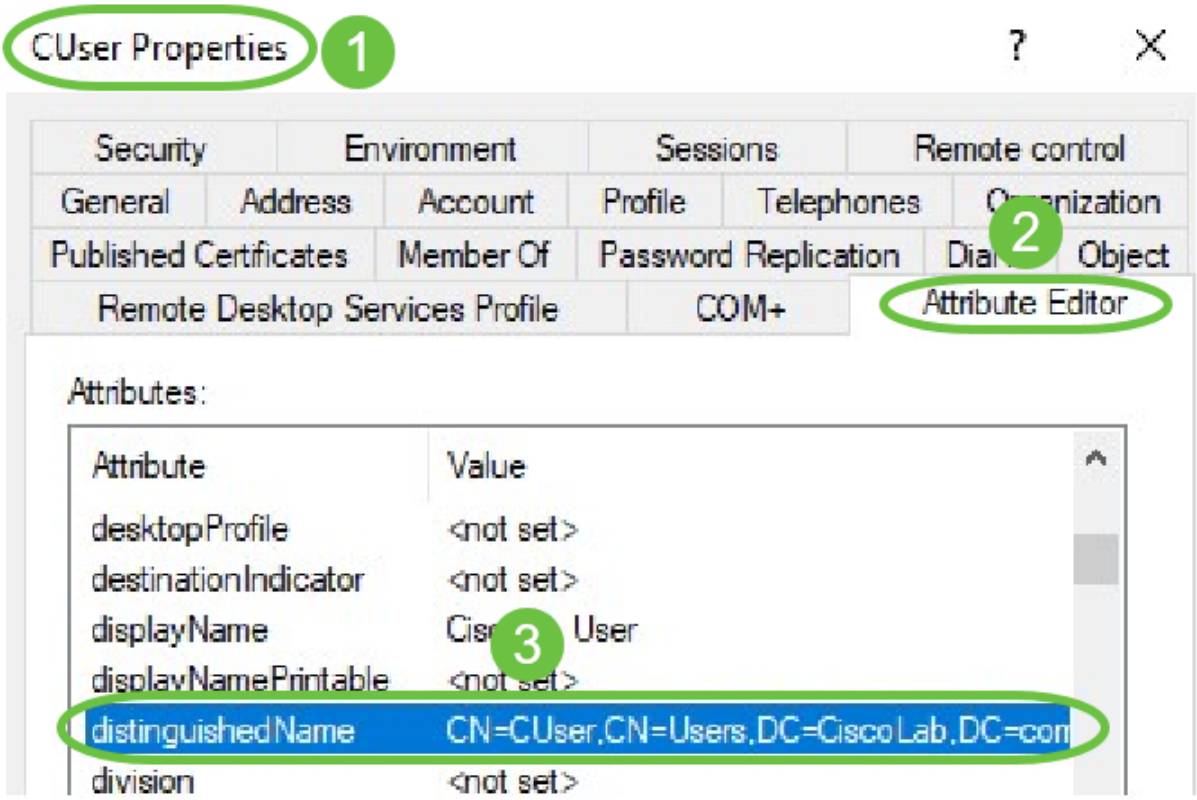



Stap 5. Zodra de gebruikersaccounts correct zijn gestructureerd, moeten ze rechten krijgen om op afstand in te loggen.

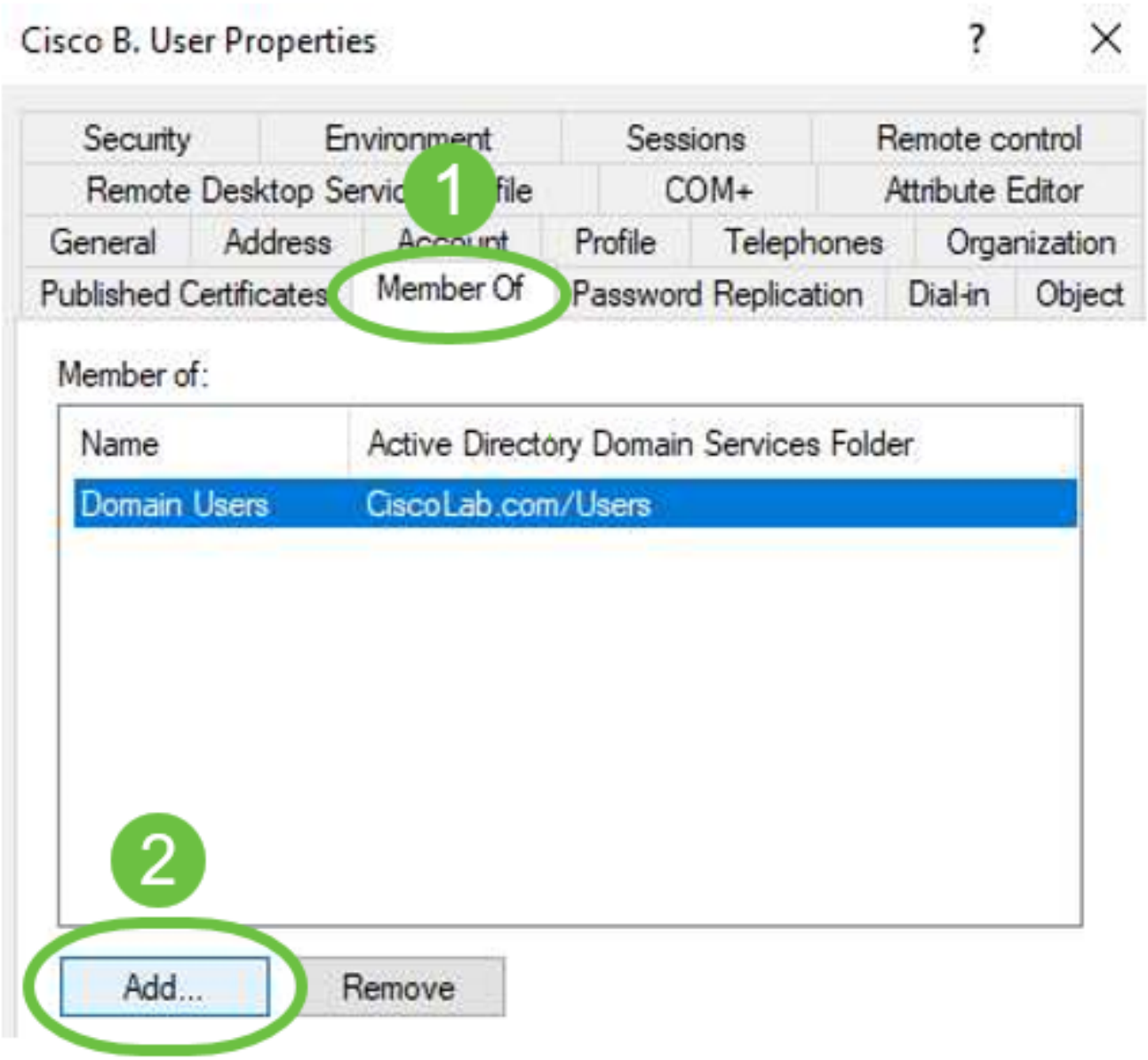
Selecteer de gebruikersaccount, klik met de rechtermuisknop en selecteer **Eigenschappen**.



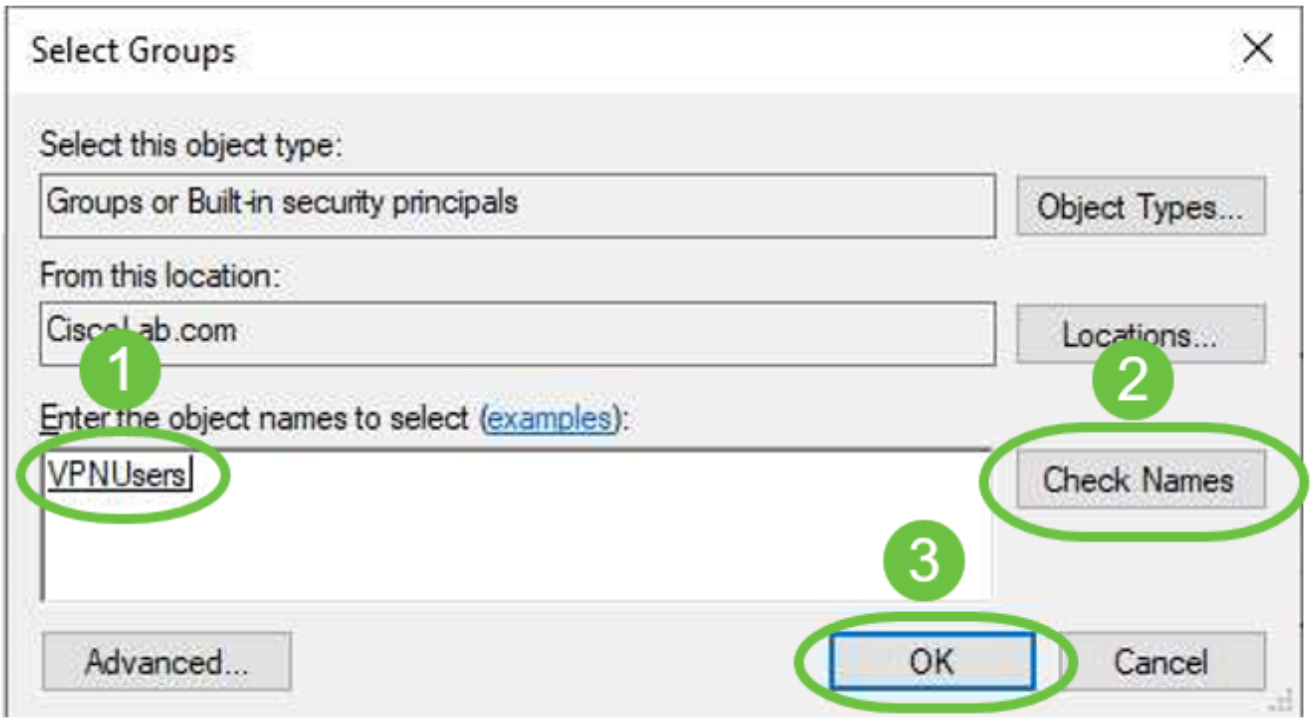

Selecteer in het tabblad *Gebruikerseigenschappen* de optie **Lijst** van **kenmerken** en ga naar *voornaam*. Zorg ervoor dat de eerste *CN=* de juiste naam van de gebruikersaanmelding zonder spaties heeft.



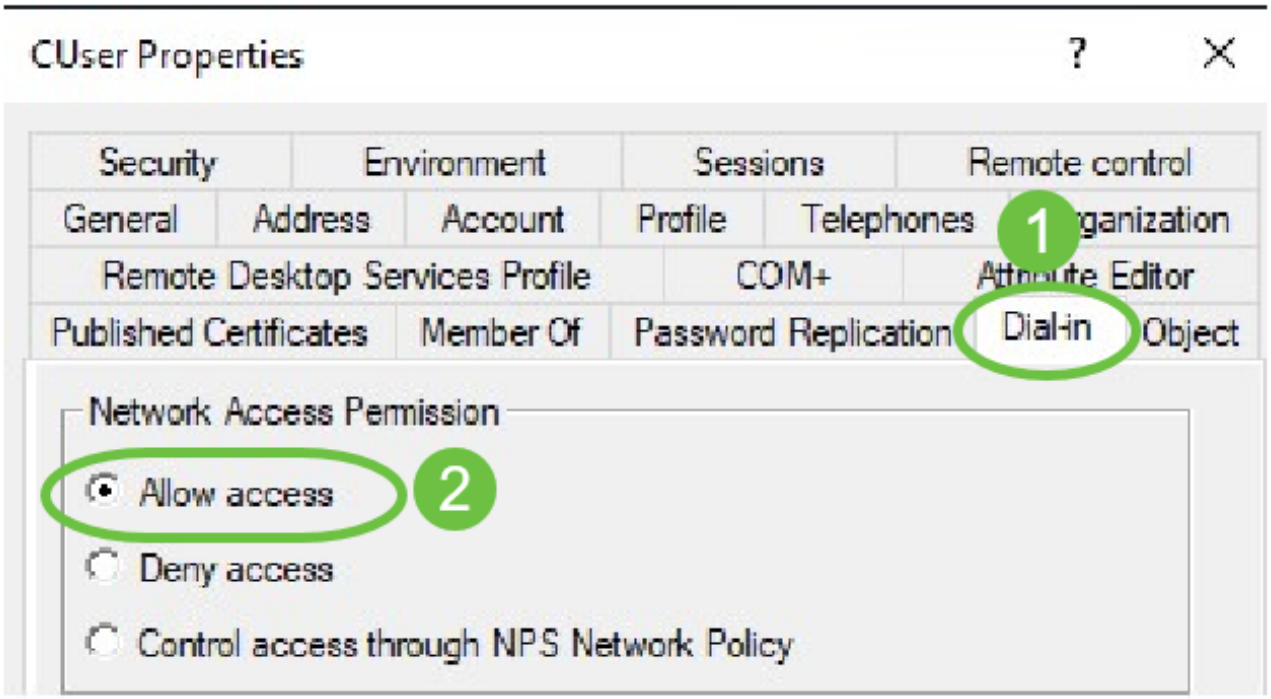

Selecteer het **tabblad Lid** en klik op **Toevoegen**.




Voer de naam van de *wereldwijde beveiligingsgroep in* en selecteer **Naam controleren**. Klik op **OK** als het bericht wordt onderstreept.




Selecteer het tabblad **Inbellen**. Selecteer onder het gedeelte *Network Access* de optie **Toegang toestaan** en laat de rest standaard staan.

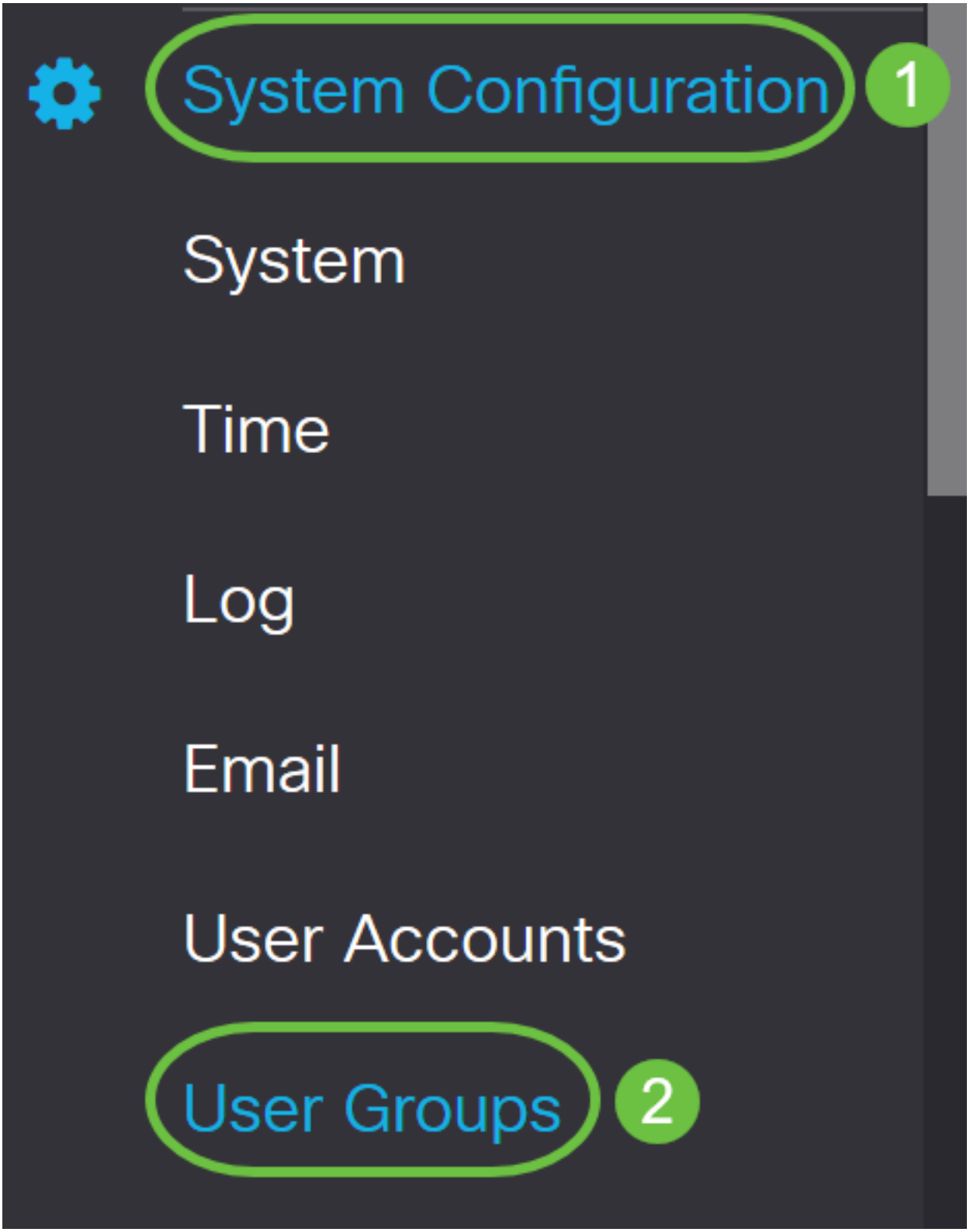



## Integratie met actieve map

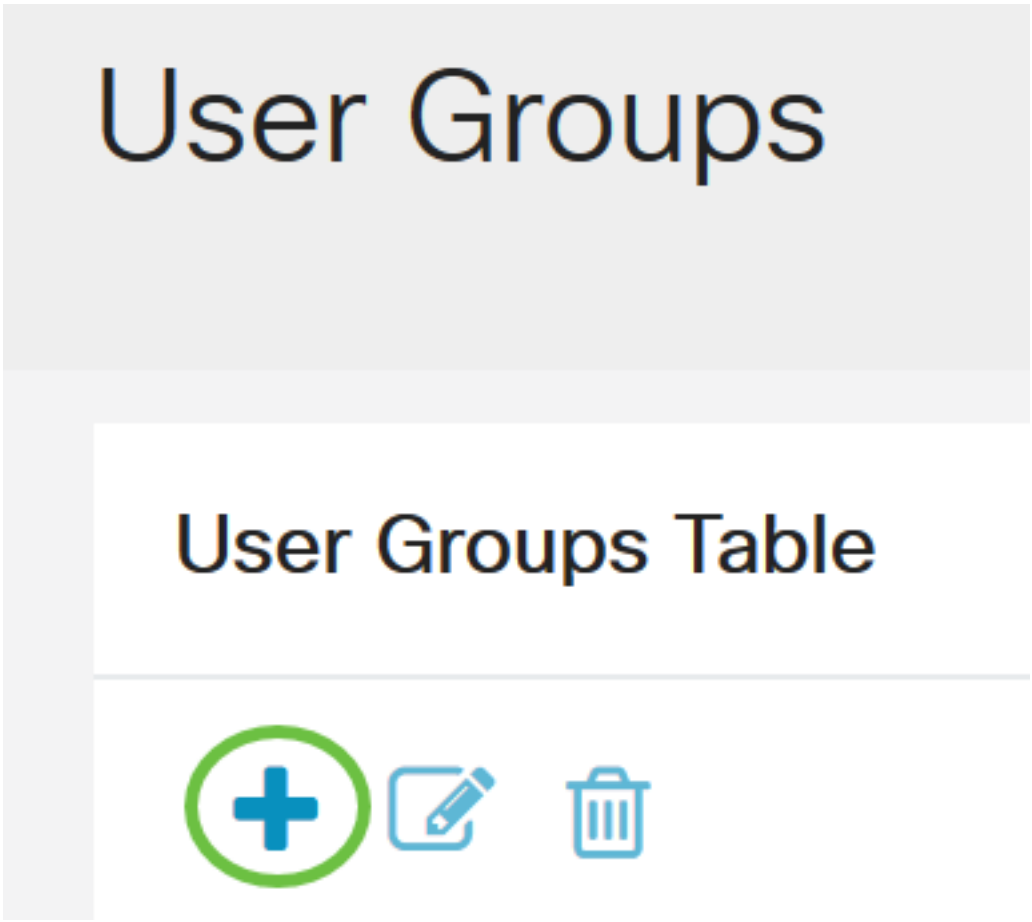
Actieve Map vereist dat de tijd van de RV34x-router overeenkomt met die van de AD-server. Voor stappen op het configureren van tijdinstellingen op een RV34x Series router klikt u hier.

AD vereist ook dat RV340 een gebruikersgroep heeft die AD Global Security Group aansluit.

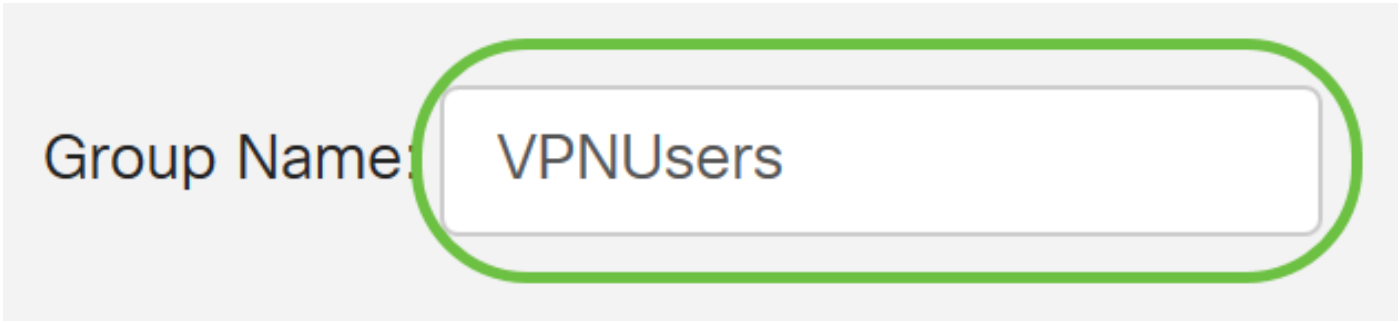
Stap 1. Navigeer naar **systeemconfiguratie > gebruikersgroepen**.




Stap 2. Klik op het pictogram **plus** om een gebruikersgroep toe te voegen.

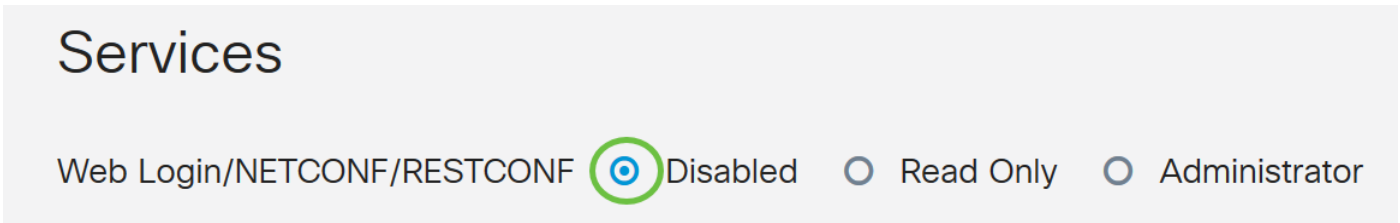



Stap 3. Voer de *groepsnaam in*. In dit voorbeeld zijn het **VPNUsers**.




De groepsnaam moet exact hetzelfde zijn als de AD Global Security Group.

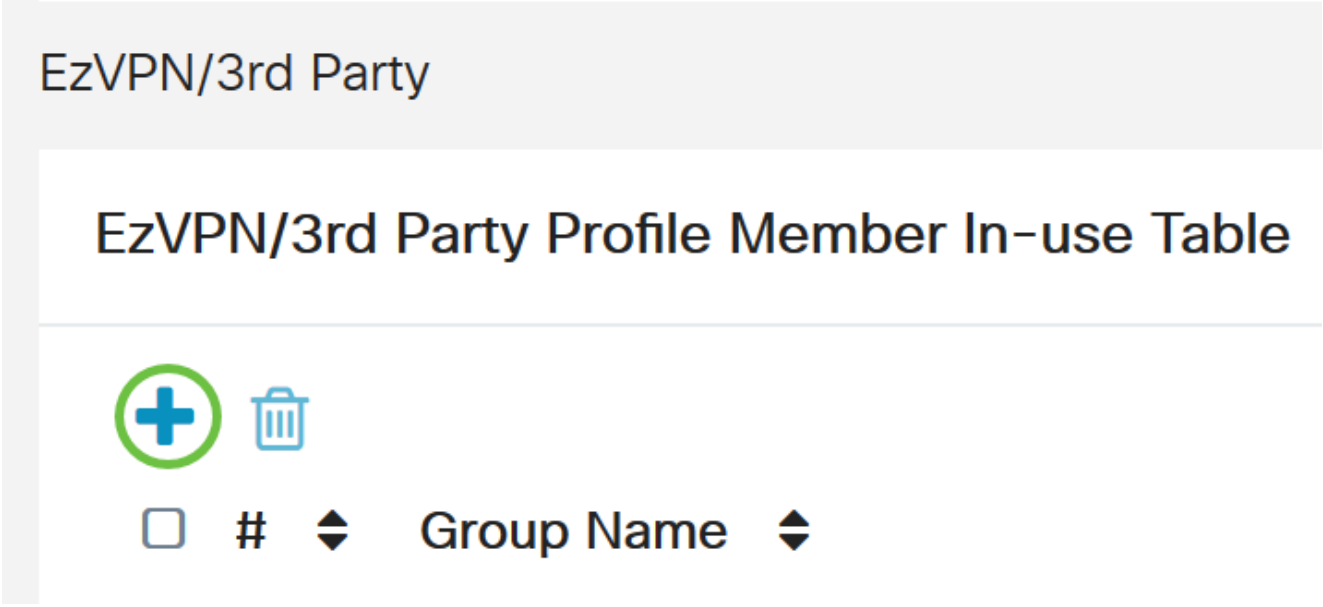
Stap 4. Onder *Services*, dient *Web Login/NETCONF/RESTCONF* te worden gemarkeerd als **Uitgeschakeld**. Als de AD-integratie niet onmiddellijk werkt, kunt u nog steeds toegang krijgen tot de RV34x.

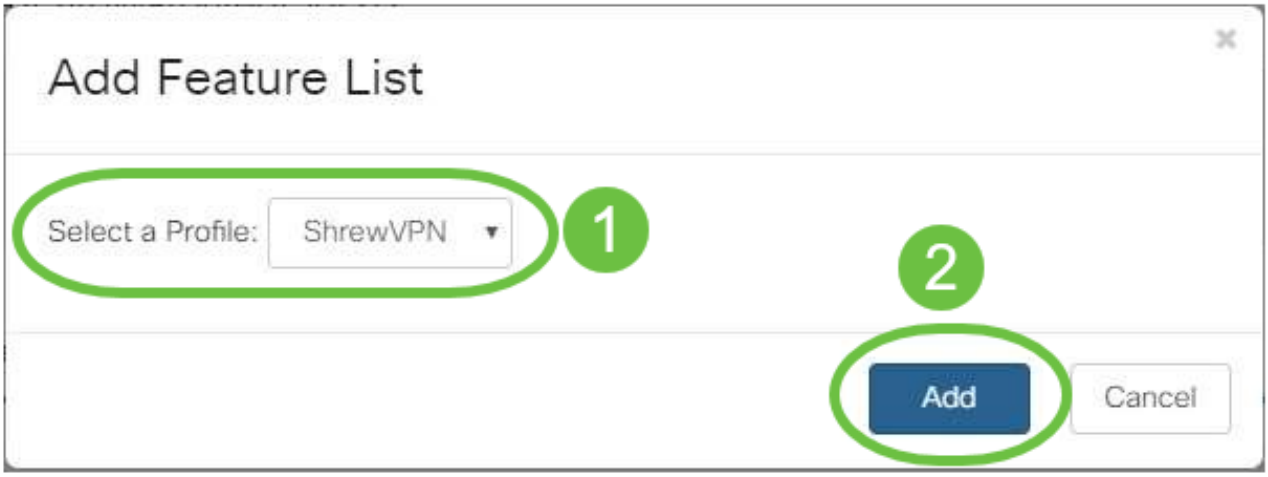



Stap 5. U kunt de VPN-tunnels toevoegen die AD-integratie gebruiken om hun gebruikers in te loggen.

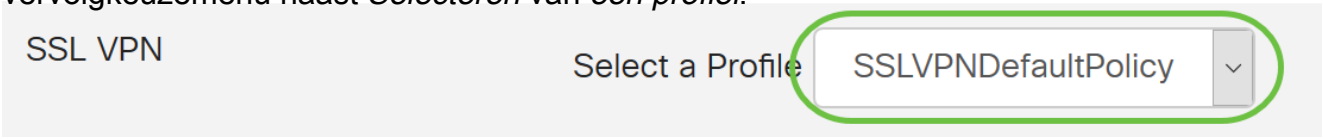
1. Als u een client-to-Site VPN wilt toevoegen dat al is geconfigureerd, gaat u naar het gedeelte *EZVPN/3rd* en vervolgens klikt u op het pictogram **plus**. Selecteer het VPN-profiel in het

vervolgkeuzemenu en klik op **Toevoegen**.

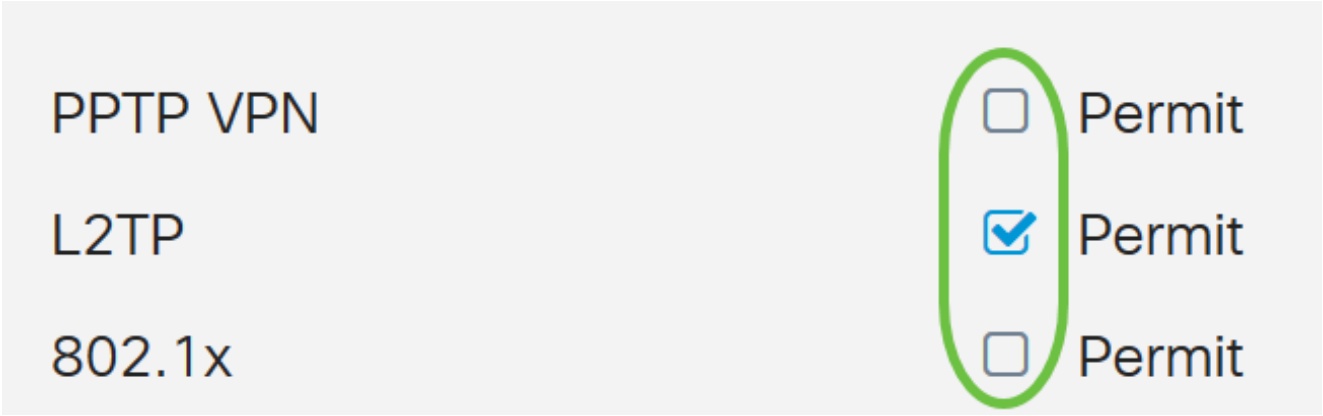


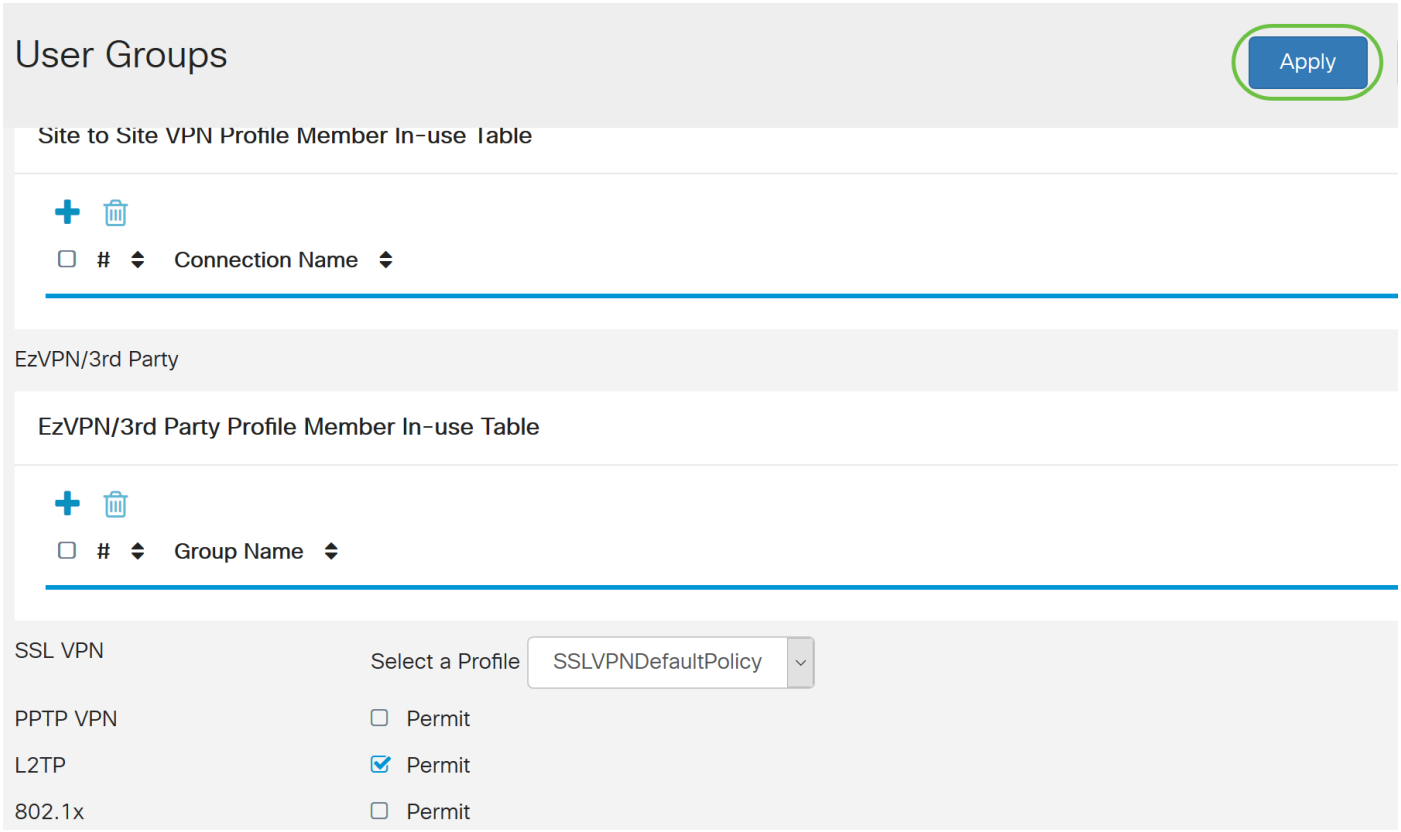

4. SSL VPN - Als een SSL VPN-tunnel wordt gebruikt, selecteert u het beleid in het vervolgkeuzemenu naast *Selecteren* van *een profiel*.




6. PPTP/L2TP/802.1x - Om deze toe te staan om AD te gebruiken, klik eenvoudig op het aankruisvakje naast hen om *vergunning* te *verlenen*.

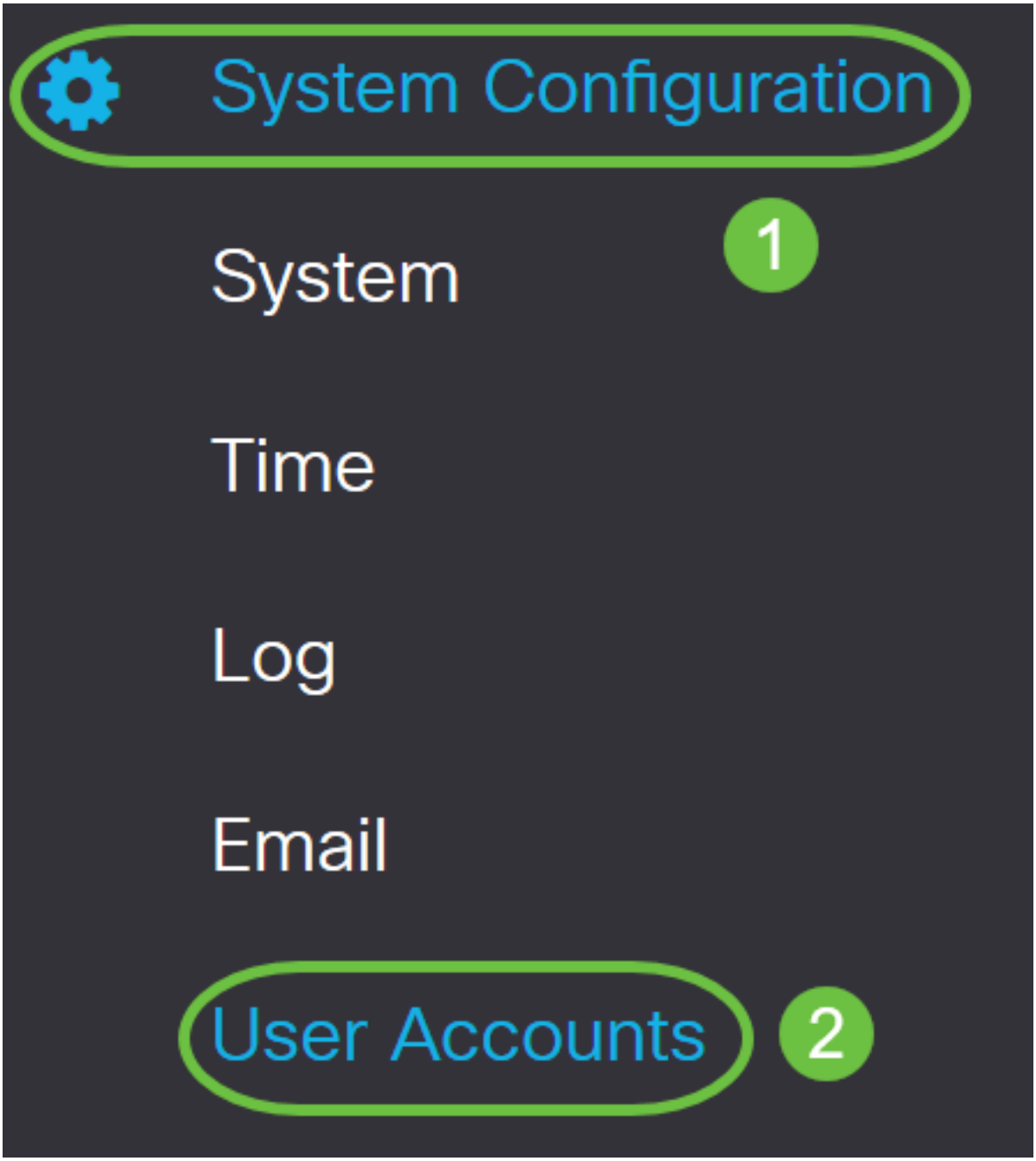



Stap 6. Klik op **Toepassen** om uw wijzigingen op te slaan.

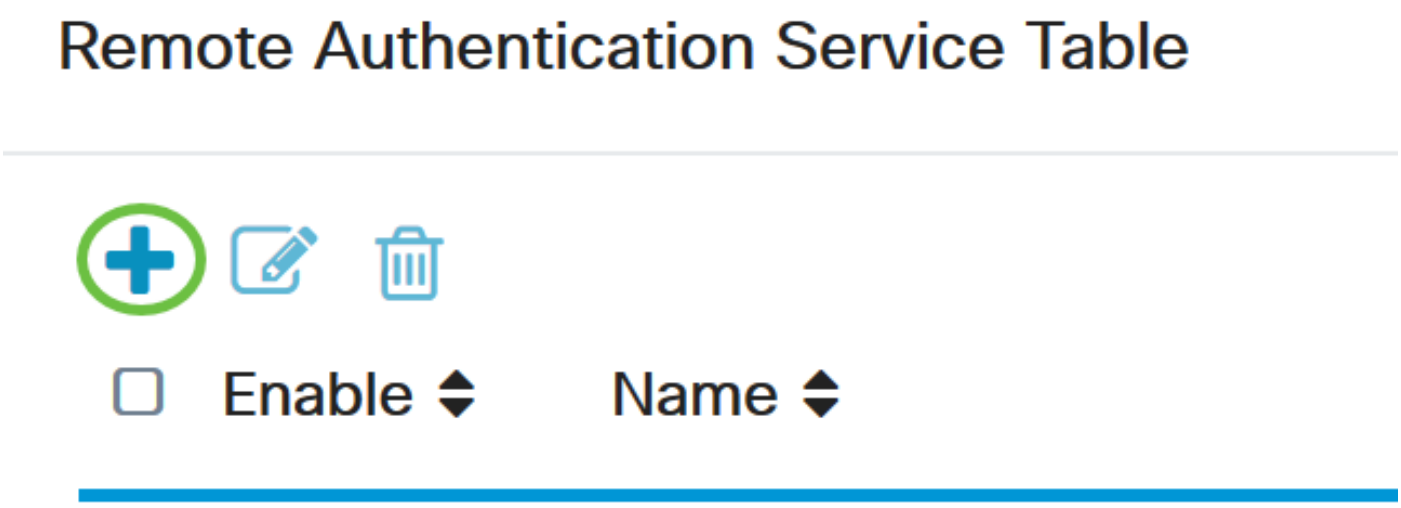



## Integratie-instellingen met actieve map

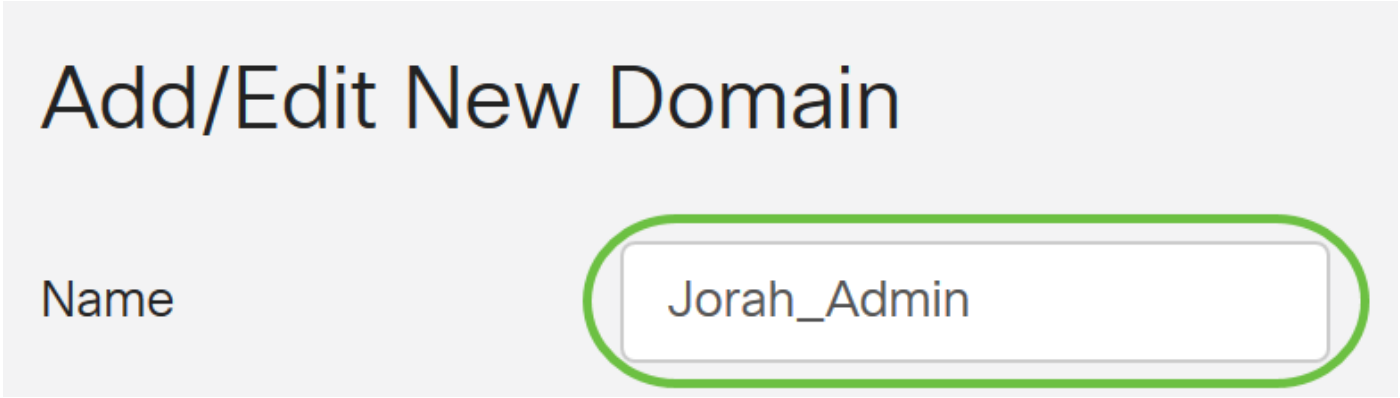
Stap 1. Navigeer naar **systeemconfiguratie > Gebruikersrekeningen**.



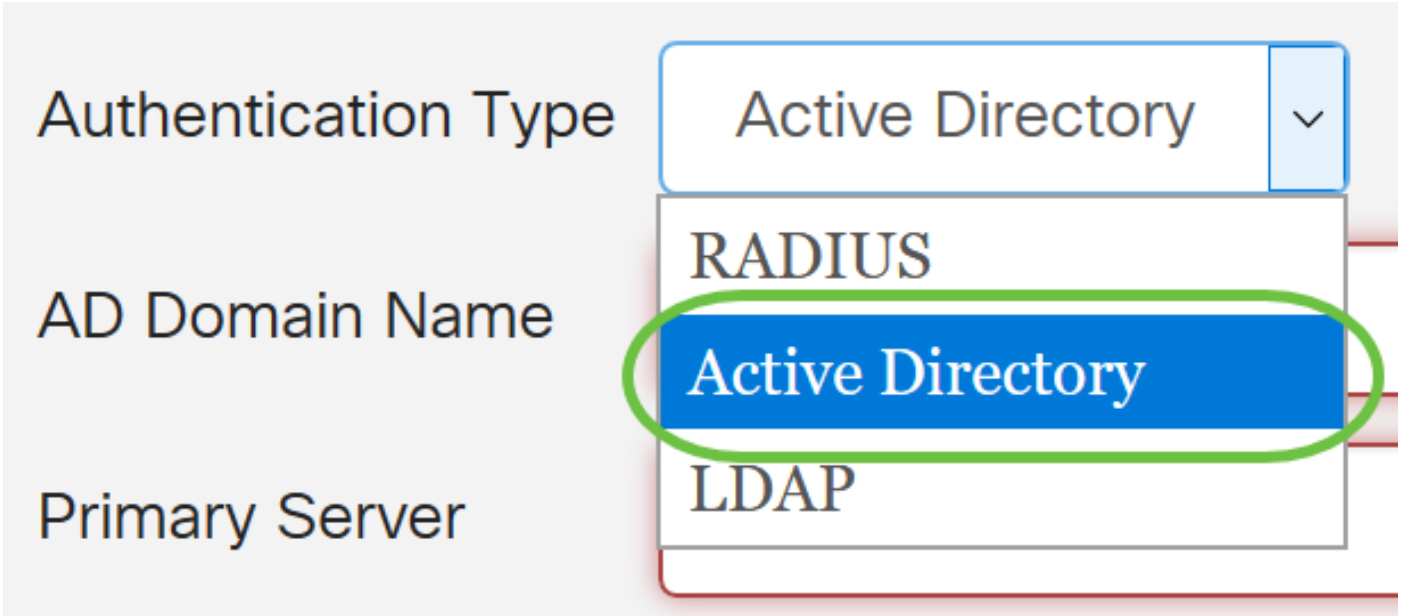

Stap 2. In de tabel met afstandsverificatie klikt u op **Add** om een ingang te maken.




Stap 3. Voer in het veld *Naam* een gebruikersnaam voor de account in. In dit voorbeeld wordt **Jorah_Admin** gebruikt.

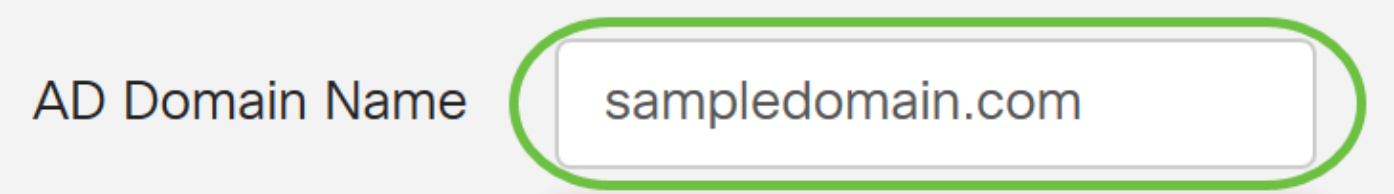



Stap 4. Kies in het vervolgkeuzemenu *Verificatietype*, **Active Directory**. AD wordt gebruikt om breed beleid aan alle elementen van het netwerk toe te wijzen, programma's op vele computers op te stellen en kritieke updates op een gehele organisatie toe te passen.




Stap 5. Voer in het veld *Naam* AD-*domein* de volledig gekwalificeerde domeinnaam van de AD in.

In dit voorbeeld wordt **sampledomain.com** gebruikt.

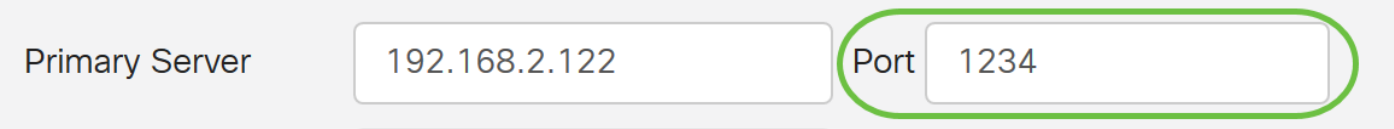



Stap 6. Voer in het veld *Primaire server* het adres van de AD in.

In dit voorbeeld wordt **192.168.2.122** gebruikt.

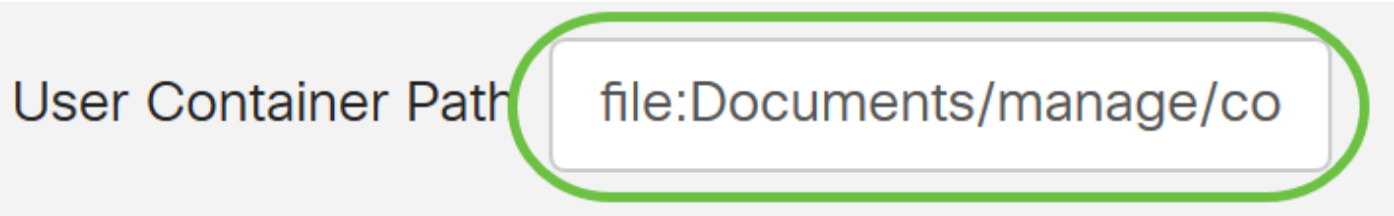

Stap 7. Voer in het veld *Port* een poortnummer in voor de primaire server.

In dit voorbeeld wordt **1234** gebruikt als havennummer.

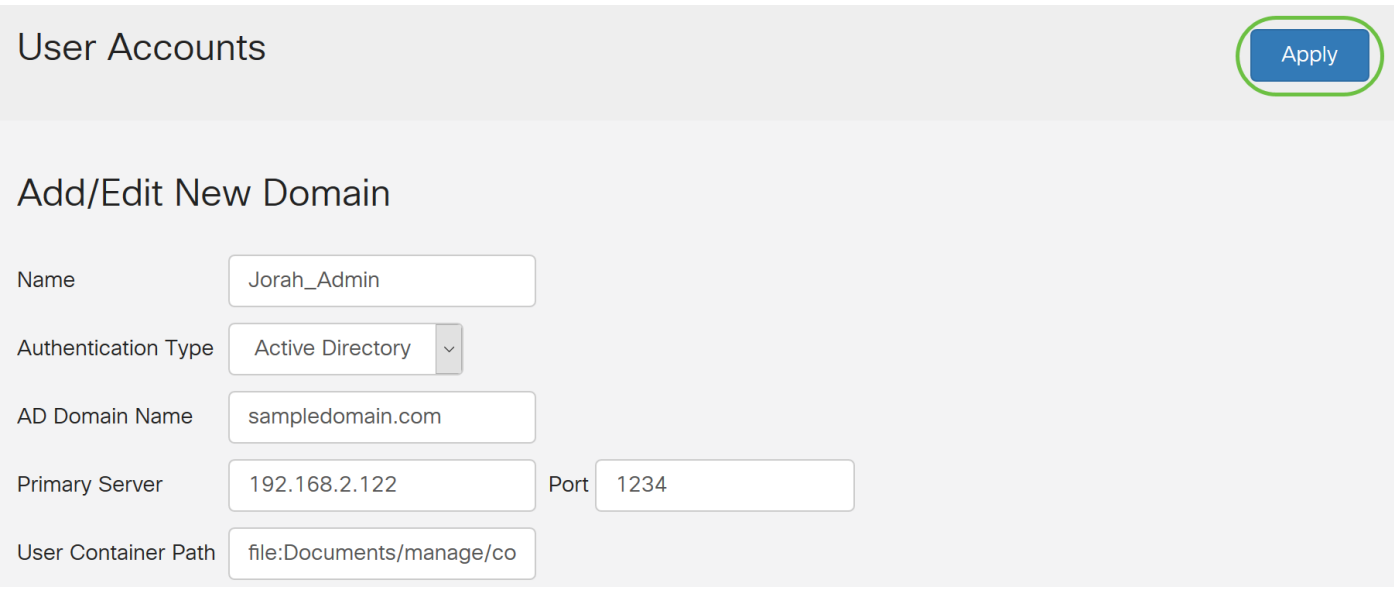



Stap 8. (Optioneel) Voer in het veld *User container Path* een wortelpad in waar de gebruikers zich beperken.

**Opmerking:** In dit voorbeeld wordt **file:Documents/manage/containers** gebruikt.



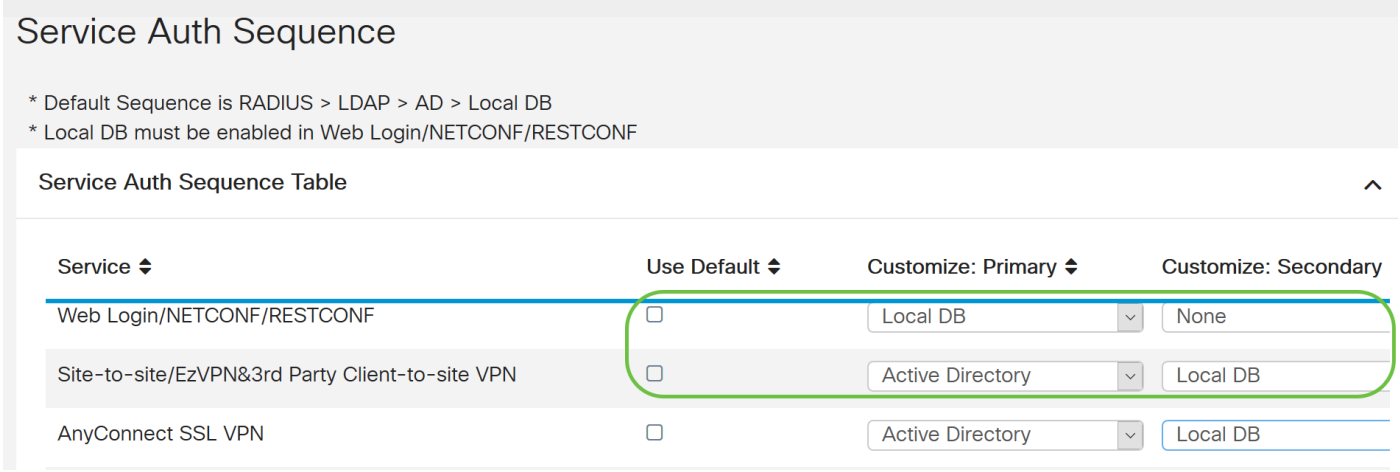

Stap 9. Klik op **Toepassen**.



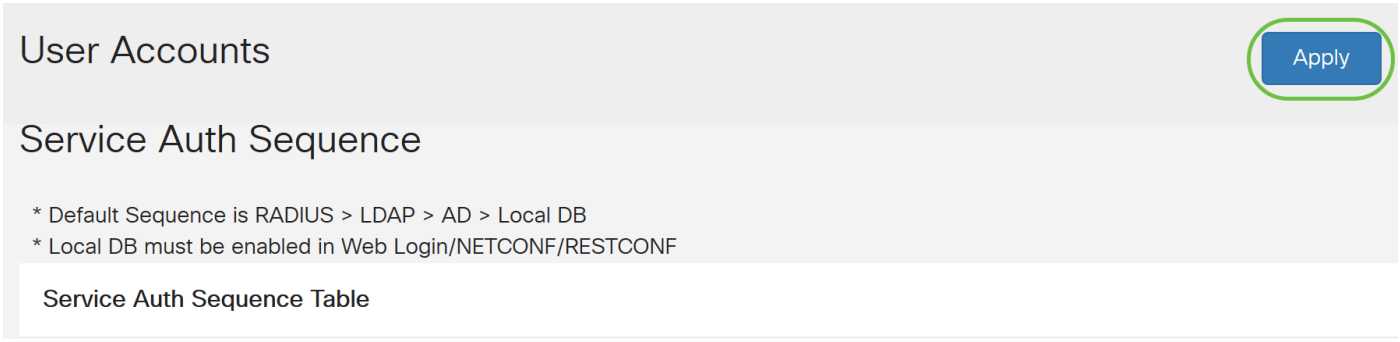

Stap 10. Scroll naar *Service Auth Sequence* om de inlogmethode voor de verschillende opties in

te stellen.

- Webex Login/NETFCONF/RESTCONF - Dit is de manier waarop u inlogt op de RV34x-router. Schakel het aanvinkvakje *Default* uit en stel de primaire methode in op **Local DB**. Dit zal verzekeren dat u niet uit de router zult worden ingelogd zelfs als de Actieve Integratie van de Map faalt.
- Site-to-site/EzVPN&3rd Party client-naar-site VPN - Dit is om client-naar-site VPN-tunnel in te stellen voor gebruik van AD. Schakel het vakje *Default* uit en stel de primaire methode in op **Active Directory** en de secundaire methode op **Local DB**.




Stap 1. Klik op **Toepassen**.

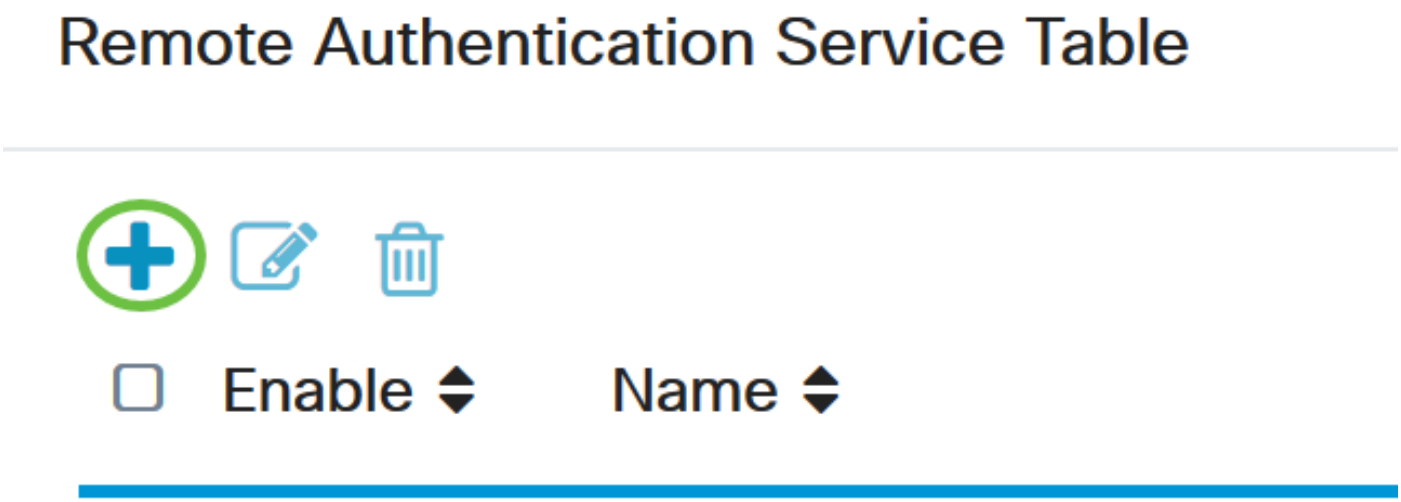



Stap 12. Sla de draaiende configuratie op naar de opstartconfiguratie.

U hebt nu met succes de instellingen voor actieve map op een RV34x Series router ingesteld.

## LDAP

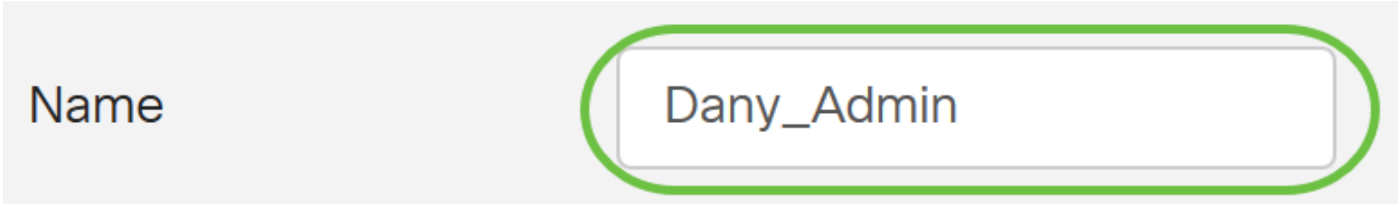
Stap 1. In de tabel met afstandsverificatie klikt u op **Add** om een ingang te maken.



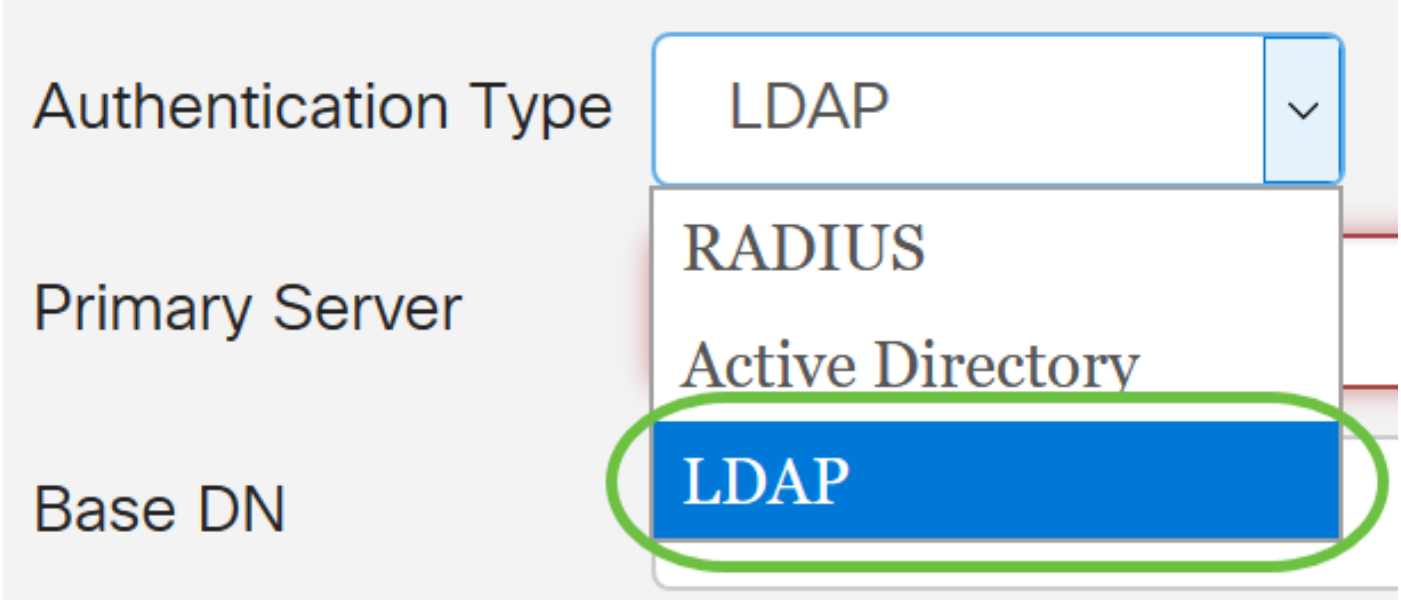

Stap 2. Voer in het veld *Naam* een gebruikersnaam voor de account in.

Er kan slechts één externe gebruikersaccount onder LDAP worden ingesteld.

In dit voorbeeld wordt Dany_Admin gebruikt.

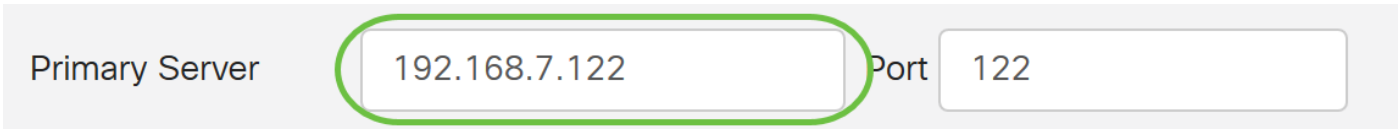



Stap 3. Kies in het vervolgkeuzemenu Verificatietype **LDAP**. Lichtgewicht Directory Access Protocol is een toegangsprotocol dat wordt gebruikt om toegang te krijgen tot een directory service. Het is een externe server die een directory server runt om authenticatie voor het domein uit te voeren.



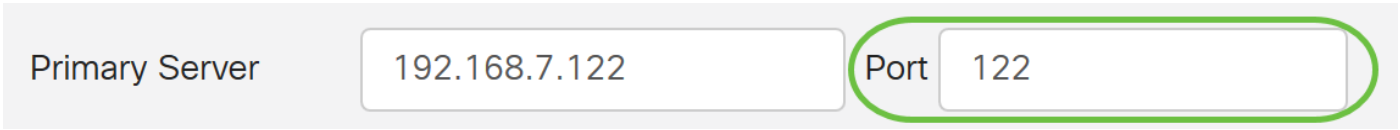

Stap 4. Voer in het *veld Primaire server* het serveradres van de LDAP in.

In dit voorbeeld wordt **192.168.7.122** gebruikt.



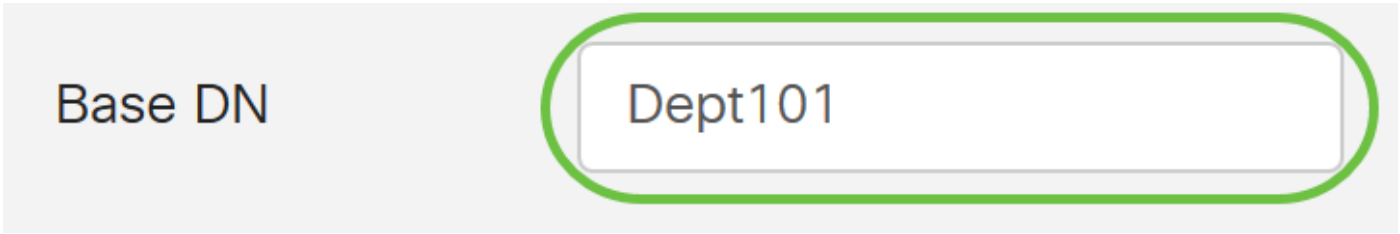

Stap 5. Voer in het veld *Port* een poortnummer in voor de primaire server.

In dit voorbeeld wordt **122** gebruikt als poortnummer.



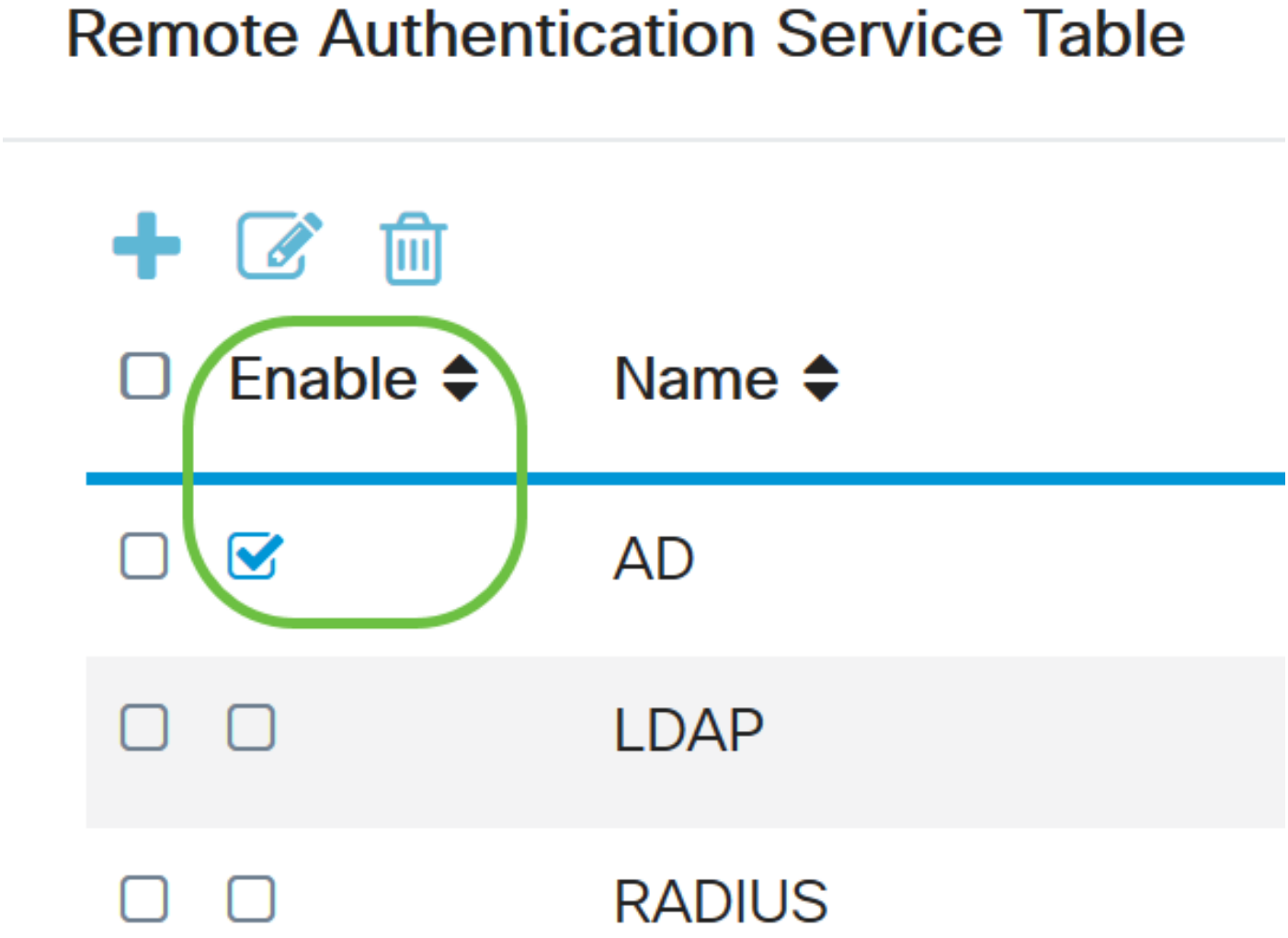

Stap 6. Voer de basisnaam van de LDAP-server in in het veld *Base DN*. De basis DN is de locatie waar de LDAP server naar gebruikers zoekt wanneer het een vergunningsaanvraag ontvangt. Dit veld dient overeen te komen met de standaard DNA die op de LDAP server is ingesteld.

In dit voorbeeld wordt **Dept101** gebruikt.

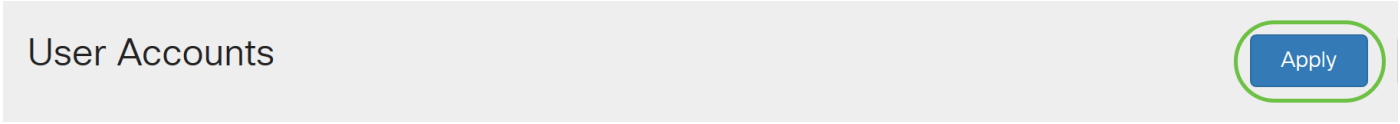



Stap 7. Klik op **Toepassen**. U wordt opgenomen in de tabel met de afstandsbediening.


Stap 8. (Optioneel) Als u de externe authenticatieservice wilt in- of uitschakelen, schakelt u het aankruisvakje naast de service in of uit.




Stap 9. Klik op **Toepassen**.




U hebt nu met succes de LDAP op een RV34x Series router ingesteld.

## Bekijk een video gerelateerd aan dit artikel...

[Klik hier om andere Tech Talks uit Cisco te bekijken]