

# Konfigurieren und Verwalten von Benutzerkonten auf einem Router der Serie RV34x

## Ziel

In diesem Artikel erfahren Sie, wie Sie lokale und Remote-Benutzerkonten auf einem Router der Serie RV34x konfigurieren und verwalten. Dazu gehören die Konfiguration der Kennwortkomplexität für lokale Benutzer, das Konfigurieren/Bearbeiten/Importieren lokaler Benutzer, das Konfigurieren des Remote-Authentifizierungsdienstes mithilfe von RADIUS, Active Directory und LDAP.

## Unterstützte Geräte | Firmware-Version

- Serie RV34x | 1.0.01.16 ([aktueller Download](#))

## Einführung

Der Router der Serie RV34x stellt Benutzerkonten zum Anzeigen und Verwalten von Einstellungen bereit. Die Benutzer können aus verschiedenen Gruppen bestehen oder zu logischen Gruppen von SSL (Secure Sockets Layer) Virtual Private Networks (VPN) gehören, die die Authentifizierungsdomäne, LAN (Local Area Network)- und Service-Zugriffsregeln sowie Timeout-Einstellungen für Inaktivität gemeinsam nutzen. Die Benutzerverwaltung definiert, welche Benutzertypen eine bestimmte Einrichtung nutzen können und wie dies möglich ist.

Die Priorität der externen Datenbank ist immer RADIUS (Remote Authentication Dial-In User Service)/LDAP (Lightweight Directory Access Protocol)/Active Directory (AD)/Local. Wenn Sie den RADIUS-Server auf dem Router hinzufügen, authentifizieren der Weblogin-Dienst und andere Dienste den Benutzer mithilfe der externen RADIUS-Datenbank.

Es gibt keine Option, eine externe Datenbank nur für den Weblogin-Dienst zu aktivieren und eine andere Datenbank für einen anderen Dienst zu konfigurieren. Sobald RADIUS erstellt und auf dem Router aktiviert ist, verwendet der Router den RADIUS-Service als externe Datenbank für die Webanmeldung, Site-to-Site-VPN, EzVPN/Drittanbieter-VPN, SSL VPN, Point-to-Point Transport Protocol (PPTP)/Layer 2 Transport Protocol (L2TP)-VPN und 802.1x.

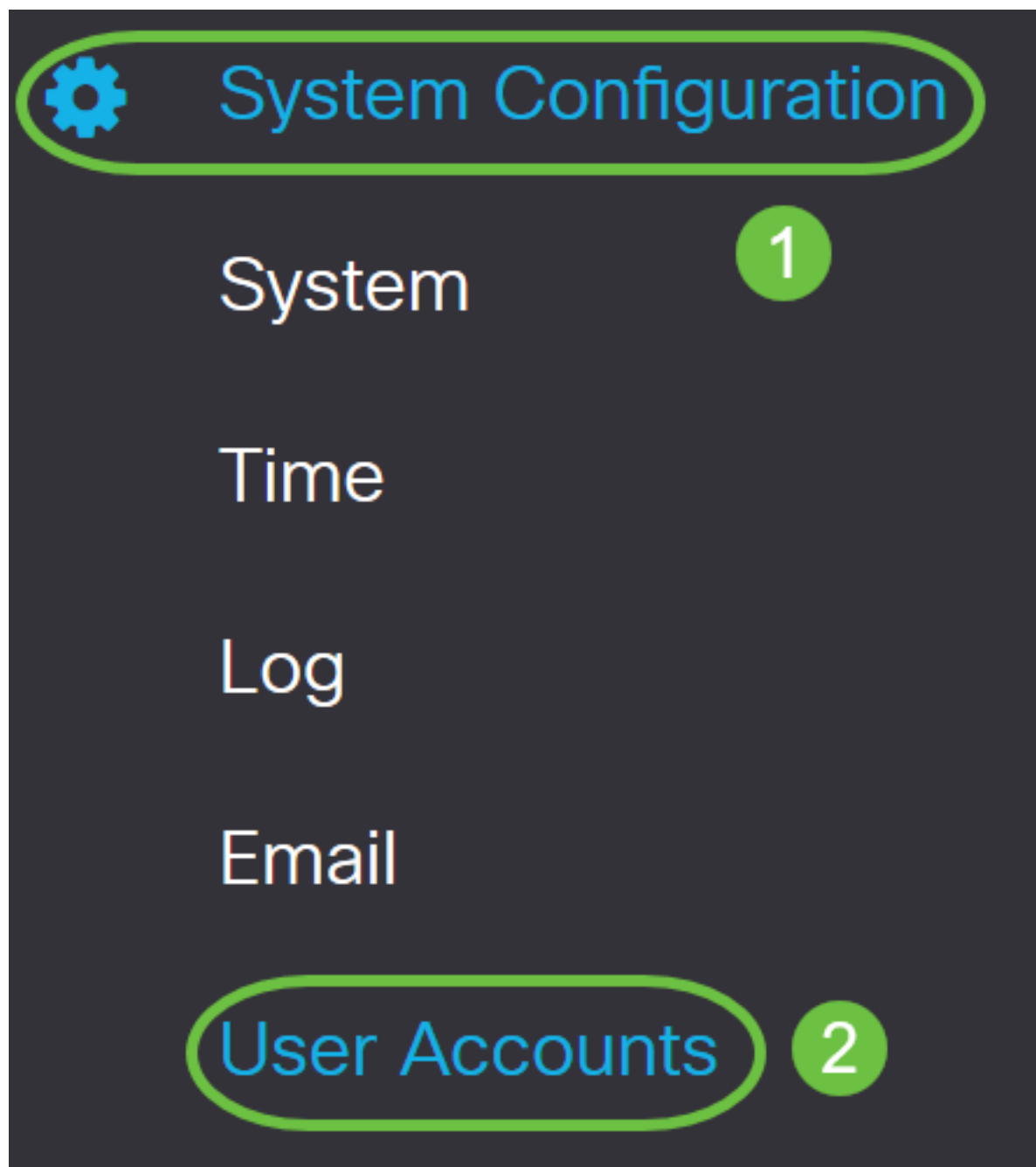
## Inhalt

- [Konfigurieren eines lokalen Benutzerkontos](#)
- [Komplexität des lokalen Benutzerkennworts](#)
- [Lokale Benutzer konfigurieren](#)
- [Lokale Benutzer bearbeiten](#)
- [Lokale Benutzer importieren](#)
- [Konfigurieren des Remote-Authentifizierungsdienstes](#)
- [RADIUS](#)
- [Active Directory-Konfiguration](#)
- [Active Directory-Integration](#)
- [Active Directory-Integrationseinstellungen](#)
- [LDAP](#)

# Konfigurieren eines lokalen Benutzerkontos

## Komplexität des lokalen Benutzerkennworts

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des Routers an, und wählen Sie **Systemkonfiguration > Benutzerkonten** aus.



Schritt 2: Aktivieren Sie das Kontrollkästchen **Einstellungen für die Kennwortkomplexität aktivieren**, um Parameter für die Kennwortkomplexität zu aktivieren.

Wenn diese Option nicht markiert ist, fahren Sie mit [Konfigurieren lokaler Benutzer fort](#).

# Local Users Password Complexity

Password Complexity Settings:



Enable

Schritt 3: Geben Sie im Feld *Minimale Kennwortlänge* eine Zahl zwischen 0 und 127 ein, um die Mindestanzahl von Zeichen festzulegen, die ein Kennwort enthalten muss. Der Standardwert ist 8.

In diesem Beispiel ist die Mindestanzahl von Zeichen auf **10** festgelegt.

## Local Users Password Complexity

Password Complexity Settings:



Enable

Minimal password length:

(Range: 0 - 127, Default: 8)

Schritt 4: Geben Sie im Feld *Minimale Anzahl von Zeichenklassen* eine Zahl zwischen 0 und 4 ein, um die Klasse festzulegen. Die eingegebene Nummer stellt die Mindest- oder Höchstzeichen der einzelnen Klassen dar:

- Das Passwort besteht aus Großbuchstaben (ABCD).
- Das Kennwort besteht aus Kleinbuchstaben (abcd).
- Das Kennwort besteht aus numerischen Zeichen (1234).
- Das Kennwort besteht aus Sonderzeichen (!@#\$).

In diesem Beispiel wird **4** verwendet.

## Local Users Password Complexity

Password Complexity Settings:



Enable

Minimal password length:

(Range: 0 - 127, Default: 8)

Minimal number of character classes:

(Range: 0 - 4, Default: 3)

The four classes are: upper case (ABCD...), lower case(abcd...), numerical(1234...) and special characters(!@#\$...).

Schritt 5: Aktivieren Sie das Kontrollkästchen **Aktivieren** für das neue Kennwort muss sich vom aktuellen unterscheiden.

## Local Users Password Complexity

Password Complexity Settings:  Enable

Minimal password length:  (Range: 0 - 127, Default: 8)

Minimal number of character classes:  (Range: 0 - 4, Default: 3)

The four classes are: upper case (ABCD...), lower case(abcd...), numerical(1234...) and special characters(!@#\$...).

The new password must be different than the current one:  Enable

Schritt 6: Geben Sie im Feld *Password Aging Time (Passwortveralterung)* die Anzahl der Tage (0 - 365) für das Kennwortablaufen ein. In diesem Beispiel wurden **180** Tage eingegeben.

## Local Users Password Complexity

Password Complexity Settings:  Enable

Minimal password length:  (Range: 0 - 127, Default: 8)

Minimal number of character classes:  (Range: 0 - 4, Default: 3)

The four classes are: upper case (ABCD...), lower case(abcd...), numerical(1234...) and special characters(!@#\$...).

The new password must be different than the current one:  Enable

Password Aging Time:  days(Range: 0 - 365, 0 means never expire)

Sie haben jetzt die Einstellungen für die lokale Benutzerkennwortkomplexität auf Ihrem Router erfolgreich konfiguriert.

## Lokale Benutzer konfigurieren

Schritt 1: Klicken Sie in der Tabelle "Lokale Benutzermitgliedschaft" auf **Hinzufügen**, um ein neues Benutzerkonto zu erstellen. Sie werden zur Seite "Benutzerkonto hinzufügen" weitergeleitet.

# Local Users

## Local User Membership List



<input type="checkbox"/>	#	User Name	Group *
<input type="checkbox"/>	1	cisco	admin
<input type="checkbox"/>	2	guest	guest

\* Should have at least one account in the "admin" group

Unter dem Header *Benutzerkonto hinzufügen* werden die Parameter angezeigt, die unter Schritte zur Komplexität des lokalen Kennworts definiert sind.

# User Accounts

## Add User Account

The current minimum requirements are as follows.

- Minimal password length: 8
- Minimal number of character classes: 3
- The new password must be different than the current one

Schritt 2: Geben Sie im Feld *Benutzername* einen Benutzernamen für das Konto ein.


In diesem Beispiel wird **Administrator\_Noah** verwendet.

User Name	<input type="text" value="Administrator_Noah"/>	
New Password	<input type="password" value="Password may not be left blank"/>	( Range: 8 - 127 )
New Password Confirm	<input type="password" value="Password may not be left blank"/>	
Password Strength Meter	<div><div style="width: 25%; background-color: red;"></div><div style="width: 75%; background-color: gray;"></div></div>	
Group	<input type="text" value="admin"/>	

Schritt 3: Geben Sie im Feld *Neues Kennwort* ein Kennwort mit den definierten Parametern ein. In diesem Beispiel muss die Mindestlänge des Kennworts aus 10 Zeichen bestehen, wobei Groß-, Kleinschreibung, Zahlen und Sonderzeichen miteinander kombiniert werden.

User Name	<input type="text" value="Administrator_Noah"/>	
New Password	<input type="password" value="●●●●●●●●●●"/>	( Range: 8 - 127 )
New Password Confirm	<input type="password" value="Password may not be left blank"/>	Must match the previous entry
Password Strength Meter	<div><div style="width: 33%; background-color: red;"></div><div style="width: 17%; background-color: yellow;"></div><div style="width: 50%; background-color: gray;"></div></div>	
Group	<input type="text" value="admin"/>	

Schritt 4: Geben Sie im Feld *Neue Kennwortbestätigung* das Kennwort zur Bestätigung erneut ein. Wenn die Kennwörter nicht übereinstimmen, wird ein Text neben dem Feld angezeigt.

User Name	<input type="text" value="Administrator_Noah"/>	
New Password	<input type="password" value="●●●●●●●●"/>	( Range: 8 - 127 )
New Password Confirm	<input type="password" value="●●●●●●●●"/>	
Password Strength Meter		
Group	<input type="text" value="admin"/>	


Die Kennwortstärkeregelung ändert sich je nach Kennwortstärke.



Schritt 5: Wählen Sie aus der Dropdown-Liste *Gruppe* eine Gruppe aus, um einem Benutzerkonto eine Berechtigung zuzuweisen. Folgende Optionen sind verfügbar:

- admin - Lese- und Schreibberechtigungen.
- guest - schreibgeschützte Berechtigungen.

In diesem Beispiel wird **admin** ausgewählt.

User Name	<input type="text" value="Administrator_Noah"/>	
New Password	<input type="password" value="●●●●●●●●"/>	( Range: 8 - 127 )
New Password Confirm	<input type="password" value="●●●●●●●●"/>	
Password Strength Meter		
Group	<input type="text" value="admin"/>	
	<input type="text" value="admin"/>	
	<input type="text" value="guest"/>	

Schritt 6: Klicken Sie auf **Apply** (Anwenden).

## Add User Account

The current minimum requirements are as follows.

- Minimal password length: 8
- Minimal number of character classes: 3
- The new password must be different than the current one

User Name	<input type="text" value="Administrator_Noah"/>	
New Password	<input type="password" value="●●●●●●●●"/>	( Range: 8 - 127 )
New Password Confirm	<input type="password" value="●●●●●●●●"/>	
Password Strength Meter	<div style="width: 100%;"><div style="width: 33%; background-color: red;"></div><div style="width: 33%; background-color: yellow;"></div><div style="width: 34%; background-color: gray;"></div></div>	
Group	<input type="text" value="admin"/>	▼

Sie haben jetzt die lokale Benutzermitgliedschaft auf einem Router der Serie RV34x erfolgreich konfiguriert.

## Lokale Benutzer bearbeiten

Schritt 1: Aktivieren Sie das Kontrollkästchen neben dem Benutzernamen des lokalen Benutzers in der Tabelle "Liste der lokalen Benutzer".

In diesem Beispiel wird **Administrator\_Noah** ausgewählt.



# Local Users

## Local User Membership List



#  User Name  Group \*

<input checked="" type="checkbox"/>	1	Administrator_Noah	admin
<input type="checkbox"/>	2	cisco	admin
<input type="checkbox"/>	3	guest	guest

Schritt 2: Klicken Sie auf **Bearbeiten**.

# Local Users

## Local User Membership List



<input type="checkbox"/>	#	User Name	Group *
<input checked="" type="checkbox"/>	1	Administrator_Noah	admin
<input type="checkbox"/>	2	cisco	admin
<input type="checkbox"/>	3	guest	guest

Der Benutzername kann nicht bearbeitet werden.

Schritt 3: Geben Sie im Feld *Altes Kennwort* das Kennwort ein, das zuvor für das lokale Benutzerkonto konfiguriert wurde.

## Edit User Account

User Name

Old Password

Schritt 4: Geben Sie im Feld *Neues Kennwort* ein neues Kennwort ein. Das neue Kennwort muss die Mindestanforderungen erfüllen.

## Edit User Account

User Name

Old Password

New Password

( Range: 0 - 127 )

Schritt 5: Geben Sie das neue Kennwort erneut im Feld *Neue Kennwortbestätigung* zur Bestätigung ein. Diese Kennwörter müssen übereinstimmen.

## Edit User Account

User Name

Old Password

New Password

( Range: 0 - 127 )

New Password Confirm

Schritt 6: (Optional) Wählen Sie in der Dropdown-Liste Gruppe eine Gruppe aus, um einem Benutzerkonto eine Berechtigung zuzuweisen.

In diesem Beispiel wird **guest** ausgewählt.

# Edit User Account

User Name

Old Password

New Password

( Range: 0 - 127 )

New Password Confirm

Group

admin

guest

Schritt 7: Klicken Sie auf **Apply** (Anwenden).

User Accounts

Apply

Cancel

## Edit User Account

User Name

Old Password

New Password

( Range: 0 - 127 )

New Password Confirm

Group

Sie sollten jetzt ein lokales Benutzerkonto erfolgreich bearbeitet haben.

# Local Users

## Local User Membership List



<input type="checkbox"/>	#	User Name	Group *
<input type="checkbox"/>	1	Administrator_Noah	guest
<input type="checkbox"/>	2	cisco	admin
<input type="checkbox"/>	3	guest	guest

\* Should have at least one account in the "admin" group

## Lokale Benutzer importieren



Schritt 1: Klicken Sie im Bereich Lokaler Benutzerimport auf  .

Schritt 2: Klicken Sie unter Benutzername und Kennwort importieren auf **Durchsuchen...** um eine Benutzerliste zu importieren. Diese Datei ist in der Regel eine Tabelle, die im CSV-Format (Comma Separated Value) gespeichert wird.

In diesem Beispiel wird **user-template.csv** ausgewählt.

# Local Users Import

Import User Name & Password

Browse...

user-template.csv

(Import User Name + Password via CSV files)

Import

Download User Template:

Download

Schritt 3: (Optional) Wenn Sie keine Vorlage haben, klicken Sie im Bereich Benutzervorlage herunterladen auf **Download**.

# Local Users Import

Import User Name & Password

Browse...

user-template.csv

(Import User Name + Password via CSV files)

Import

Download User Template:

Download

Schritt 4: Klicken Sie auf **Importieren**.

# Local Users Import

Import User Name & Password

Browse...

user-template.csv

(Import User Name + Password via CSV files)

Import

Download User Template:

Download

Neben der Importschaltfläche wird eine Meldung angezeigt, dass der Import erfolgreich war.

Sie haben nun erfolgreich eine Liste von lokalen Benutzern importiert.

## Konfigurieren des Remote-Authentifizierungsdiensts

### RADIUS

Schritt 1: Klicken Sie in der Tabelle für den Dienst für die Remoteauthentifizierung auf **Hinzufügen**, um einen Eintrag zu erstellen.



# Remote Authentication Service Table



Enable ⇅

Name ⇅

Schritt 2: Erstellen Sie im Feld *Name* einen Benutzernamen für das Konto.

In diesem Beispiel wird **Administrator** verwendet.

## Add/Edit New Domain

Name

Administrator

Schritt 3: Wählen Sie im Dropdown-Menü *Authentication Type* (Authentifizierungstyp) die Option **RADIUS aus**. Dies bedeutet, dass die Benutzerauthentifizierung über einen RADIUS-Server erfolgt.

Es kann nur ein einziges Remote-Benutzerkonto unter RADIUS konfiguriert werden.

Authentication Type

RADIUS



RADIUS

Active Directory

LDAP

Primary Server

Backup Server

Schritt 4: Geben Sie im Feld *Primärserver* die IP-Adresse des primären RADIUS-Servers ein.

In diesem Beispiel wird **192.168.3.122** als Primärserver verwendet.

Primary Server

192.168.3.122

Port

389

Schritt 5: Geben Sie im Feld *Port* die Portnummer des primären RADIUS-Servers ein.

In diesem Beispiel wird **1645** als Portnummer verwendet.

Primary Server

192.168.3.122

Port

389

Schritt 6: Geben Sie im Feld *Backup-Server* die IP-Adresse des Backup-RADIUS-Servers ein. Dies dient als Failover, falls der primäre Server ausfällt.

In diesem Beispiel lautet die Adresse des Sicherungsservers **192.168.4.122**.

Backup Server

192.168.4.122

Port

389

Schritt 7: Geben Sie im Feld *Port* die Anzahl der Backup-RADIUS-Server ein.

Backup Server

192.168.4.122

Port

389

In diesem Beispiel wird **1646** als Portnummer verwendet.

Schritt 8: Geben Sie im Feld *Preshared-Key* (Vorinstallierter Schlüssel) den Pre-Shared Key ein, der auf dem RADIUS-Server konfiguriert wurde.

Pre-shared Key

●●●●●●●●●●

Schritt 9: Geben Sie im Feld *Confirm Preshared-key* (Vorinstallierten Schlüssel bestätigen) den vorinstallierten Schlüssel zur Bestätigung erneut ein.

Confirm Pre-shared Key

●●●●●●●●●●

Schritt 10: Klicken Sie auf **Apply** (Anwenden).

## Add/Edit New Domain

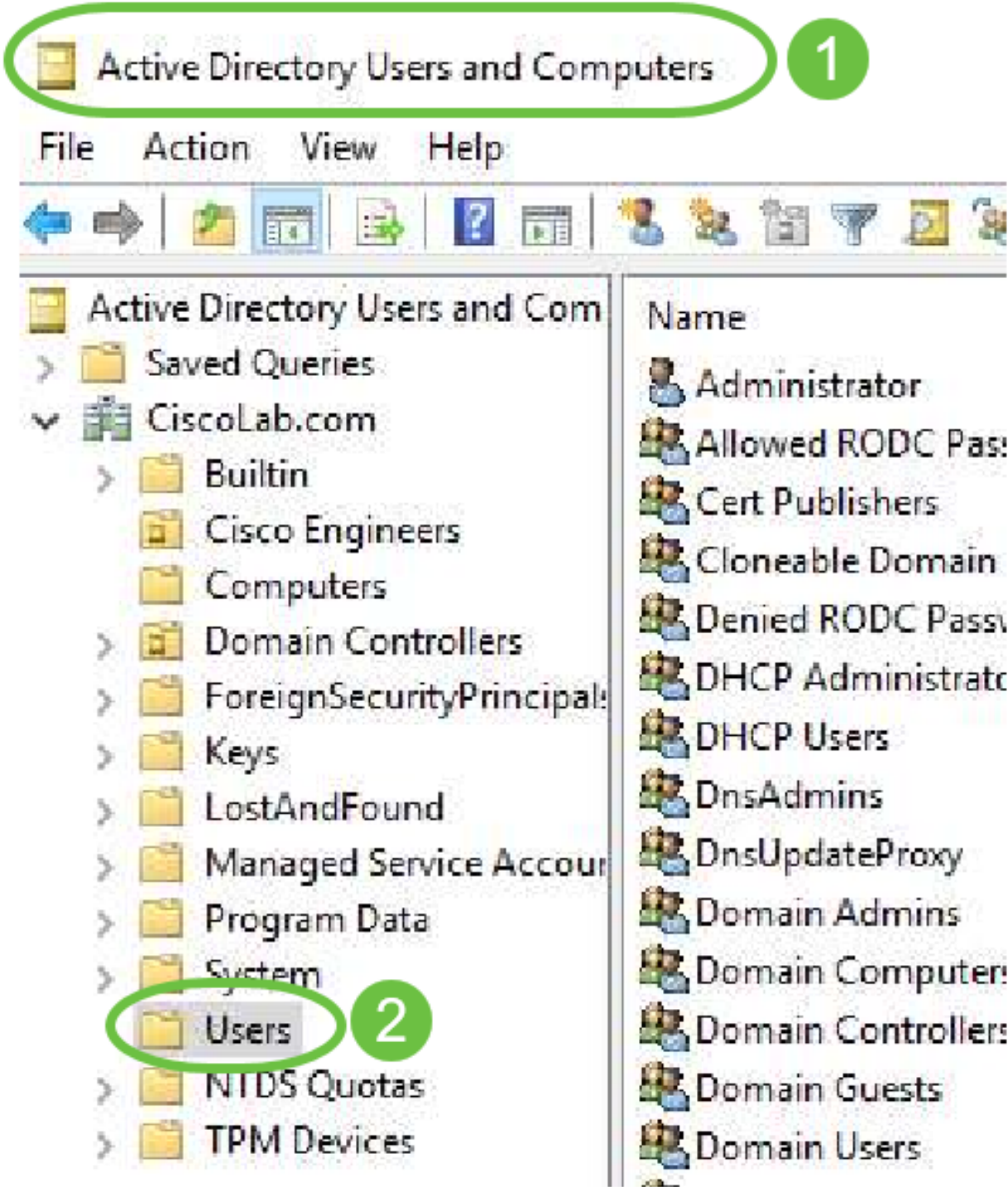
Name	<input type="text" value="Administrator"/>		
Authentication Type	<input type="text" value="RADIUS"/>		
Primary Server	<input type="text" value="192.168.3.122"/>	Port	<input type="text" value="389"/>
Backup Server	<input type="text" value="192.168.4.122"/>	Port	<input type="text" value="389"/>
Pre-shared Key	<input type="password" value="●●●●●●●●"/>		
Confirm Pre-shared Key	<input type="password" value="●●●●●●●●"/>		

Sie werden zur Haupt-Benutzerkontenseite weitergeleitet. Das kürzlich konfigurierte Konto wird jetzt in der Tabelle für den Remote-Authentifizierungsdienst angezeigt.

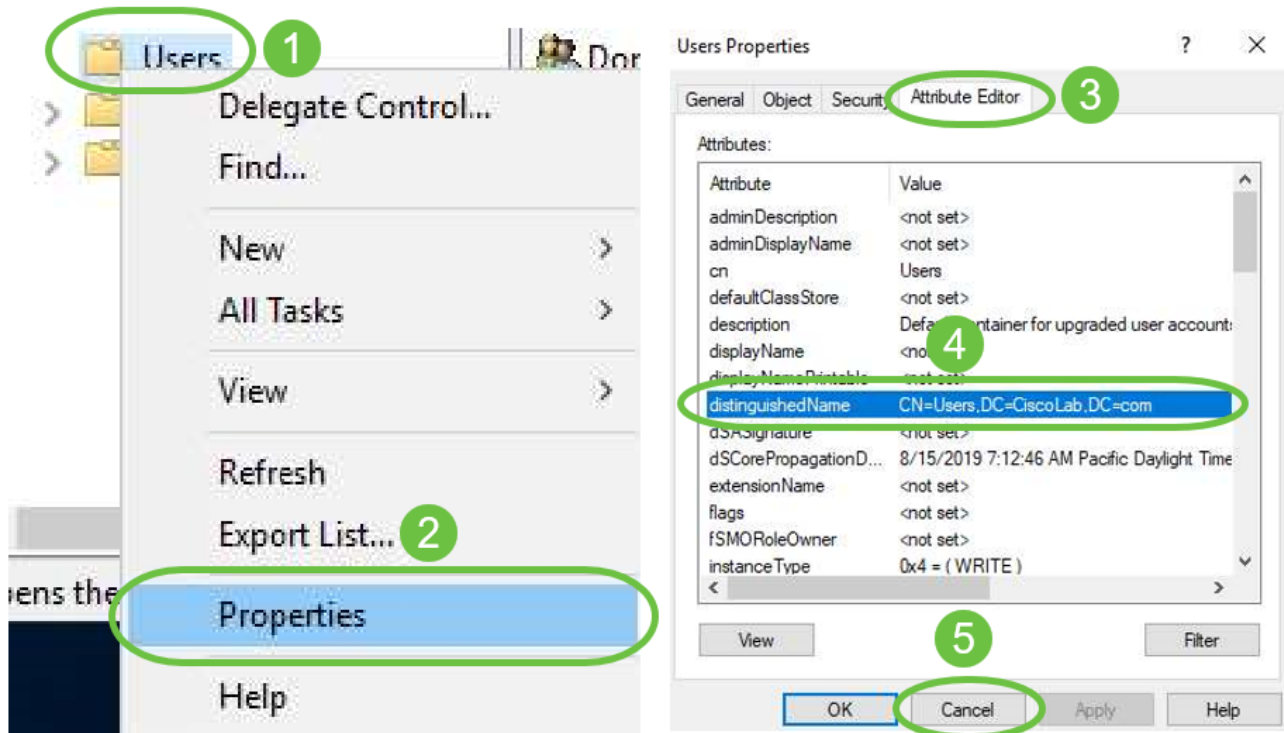
Sie haben jetzt erfolgreich die RADIUS-Authentifizierung auf einem Router der Serie RV34x konfiguriert.

## Active Directory-Konfiguration

Schritt 1: Um die Active Directory-Konfiguration abzuschließen, müssen Sie beim Active Directory-Server angemeldet sein. Öffnen Sie auf Ihrem PC **Active Directory-Benutzer und -Computer**, und navigieren Sie zu dem Container, in dem die Benutzerkonten für die Remote-Anmeldung verwendet werden. In diesem Beispiel wird der **Benutzer**-Container verwendet.



Schritt 2: Klicken Sie mit der rechten Maustaste auf den Container, und wählen Sie **Eigenschaften aus**. Navigieren Sie zur Registerkarte *Attributeditor*, und suchen Sie das *DistinguishedName*-Feld. Wenn diese Registerkarte nicht sichtbar ist, müssen Sie die Ansicht der erweiterten Funktionen in Active Directory-Benutzern und -Computern aktivieren und von vorne beginnen. Notieren Sie sich dieses Feld, und klicken Sie auf **Abbrechen**. Dies ist der Benutzercontainerpfad. Dieses Feld wird auch bei der Konfiguration des RV340 benötigt und muss genau übereinstimmen.



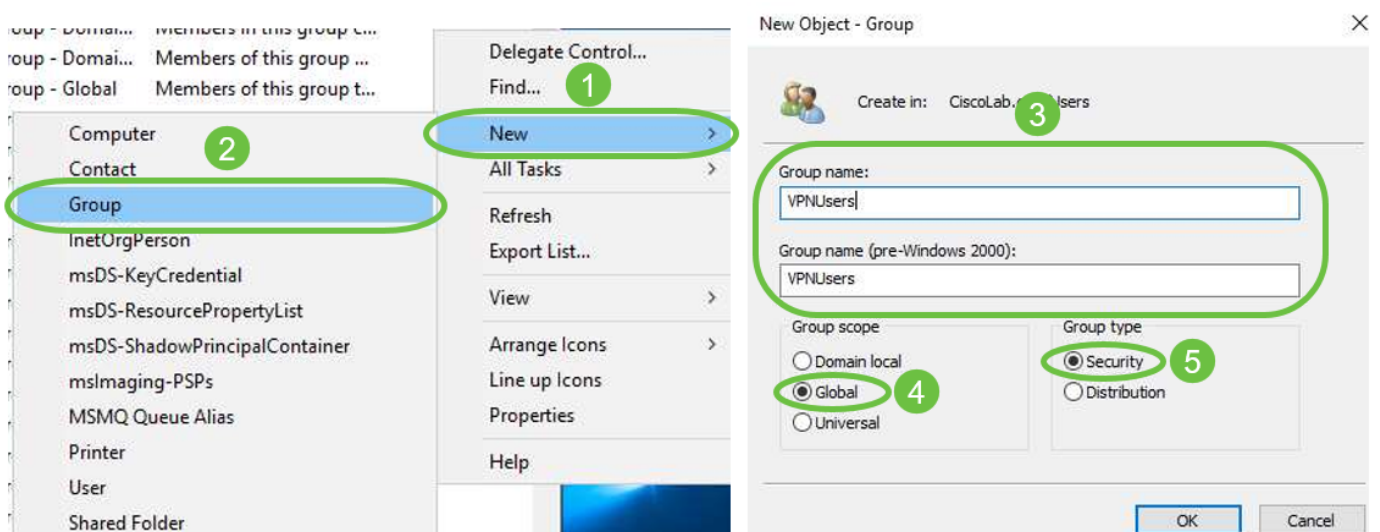
Schritt 3: Erstellen Sie eine globale Sicherheitsgruppe im gleichen Container wie die Benutzerkonten, die verwendet werden sollen.

Klicken Sie im ausgewählten Container mit der rechten Maustaste auf einen leeren Bereich, und wählen Sie **Neu > Gruppe**.

Wählen Sie Folgendes aus:

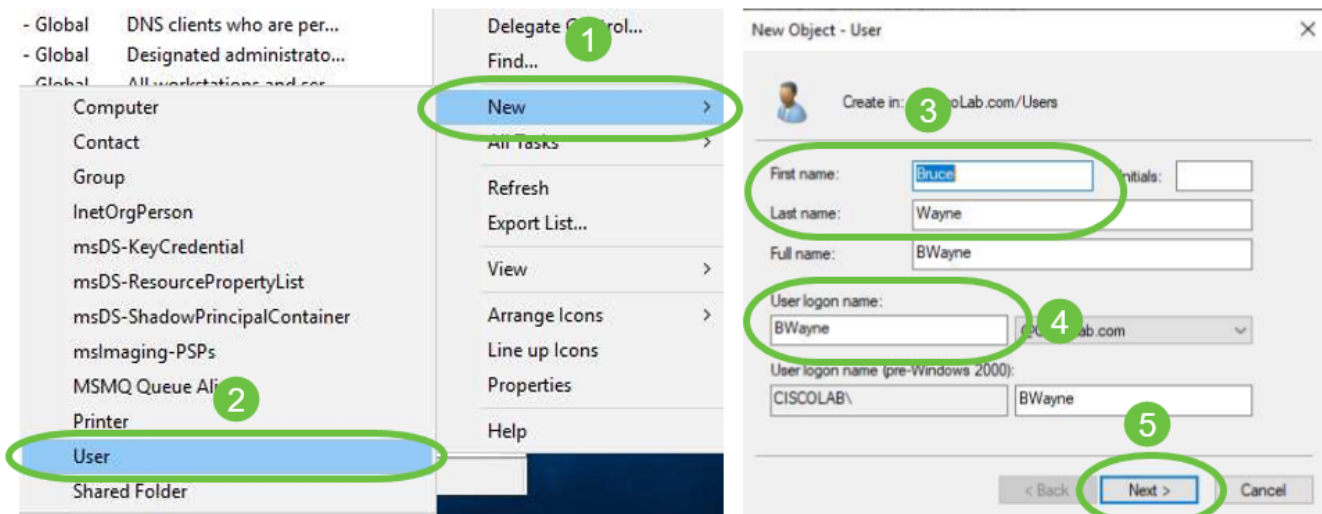
- Gruppenname: Dieser Name muss exakt mit dem auf dem RV340 erstellten Benutzernamen für die Gruppe übereinstimmen. In diesem Beispiel verwenden wir **VPNUsers**.
- Gruppenbereich - Global
- Gruppentyp - Sicherheit

Klicken Sie auf **OK**.



Schritt 4: Gehen Sie wie folgt vor, um neue Benutzerkonten zu erstellen:

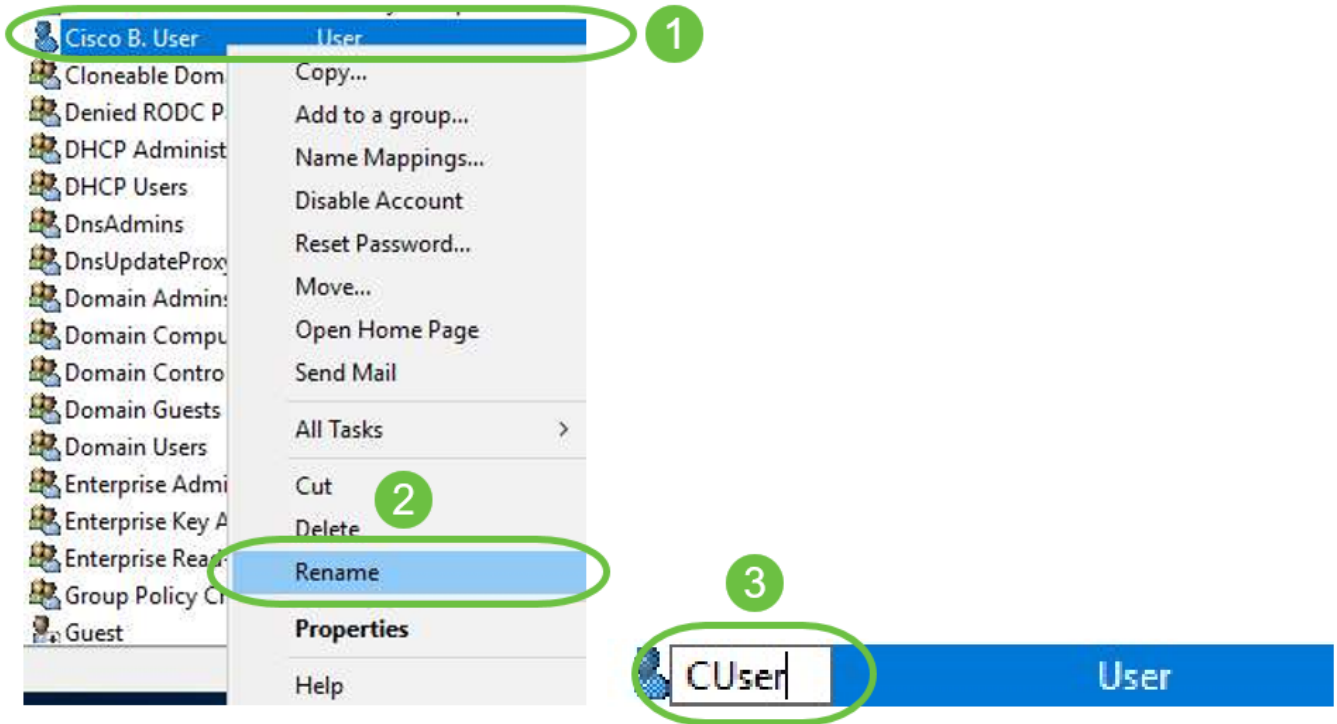
- Klicken Sie mit der rechten Maustaste auf einen leeren Bereich im Container, und wählen Sie **Neu > Benutzer aus**.
- Geben Sie *Vorname, Nachname* ein.
- Geben Sie den *Benutzernamen für die Anmeldung* ein.
- Klicken Sie auf **Weiter**.



Sie werden aufgefordert, ein Kennwort für den Benutzer einzugeben. Wenn *der Benutzer das Kennwort ändern muss, wenn das nächste Anmeldefeld aktiviert ist*, muss sich der Benutzer lokal anmelden und das Kennwort ändern, BEVOR er sich remote anmeldet.

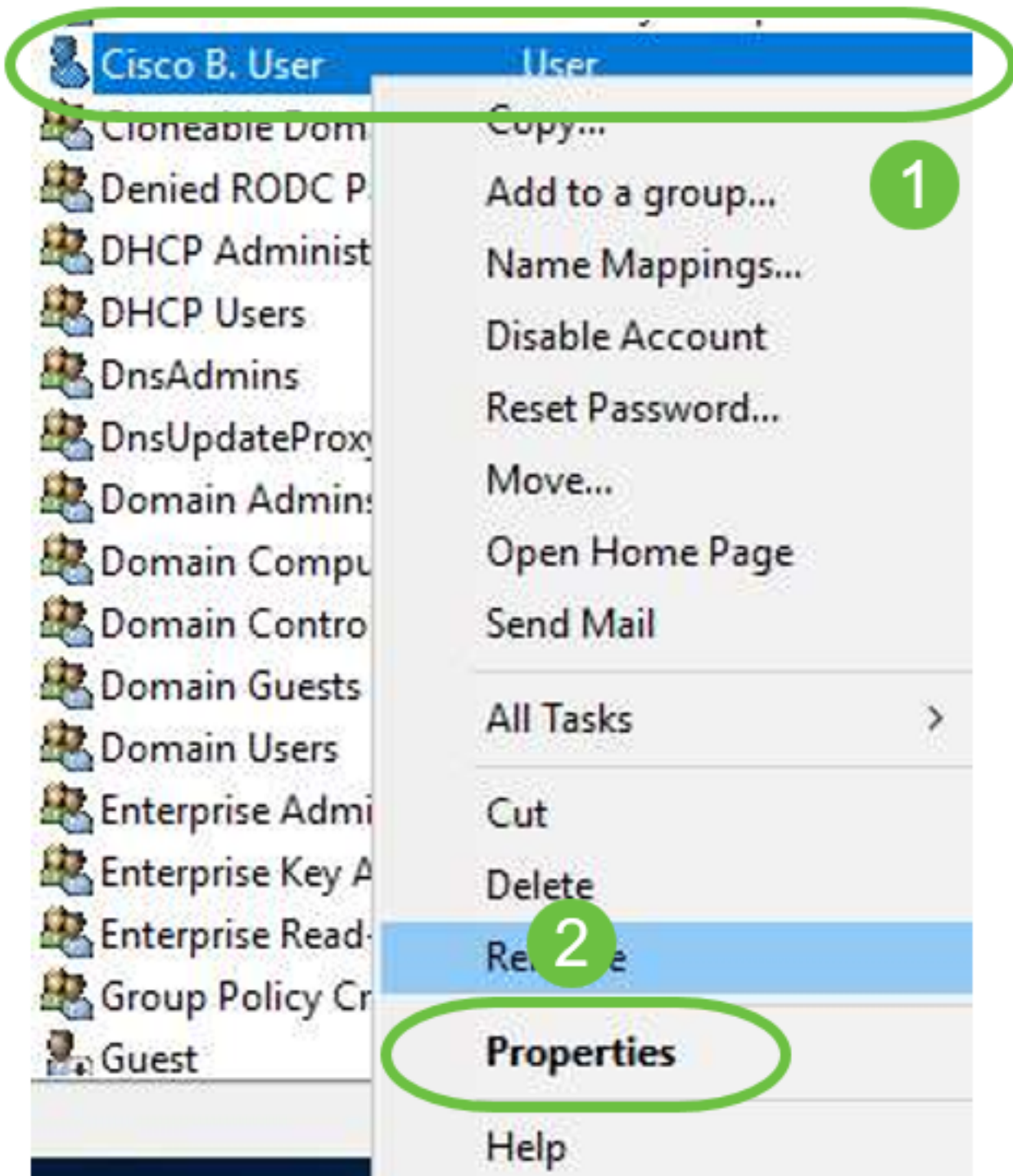
Klicken Sie auf **Fertig stellen**.

Wenn bereits Benutzerkonten erstellt wurden, die verwendet werden müssen, müssen ggf. Anpassungen vorgenommen werden. Um den kanonischen Namen eines Benutzers anzupassen, wählen Sie den Benutzer aus, klicken Sie mit der rechten Maustaste, und wählen Sie **Umbenennen** aus. Stellen Sie sicher, dass alle Leerzeichen entfernt werden und dass sie mit dem Anmeldenamen des Benutzers übereinstimmen. Dadurch wird der Anzeigename des Benutzers NICHT geändert. Klicken Sie auf **OK**.



Schritt 5: Wenn Benutzerkonten korrekt strukturiert sind, müssen ihnen Rechte für die Remote-Anmeldung gewährt werden.

Wählen Sie dazu das Benutzerkonto aus, klicken Sie mit der rechten Maustaste, und wählen Sie **Eigenschaften** aus.



Wählen Sie in den *Benutzereigenschaften* die Registerkarte **Attributeditor** aus, und führen Sie einen Bildlauf nach unten zu *DistinguishedName* durch. Stellen Sie sicher, dass der erste CN= den richtigen Benutzernamen ohne Leerzeichen hat.



CUser Properties 1 ? X

Security	Environment		Sessions	Remote control	
General	Address	Account	Profile	Telephones	Organization
Published Certificates	Member Of		Password Replication	Dial	Object
Remote Desktop Services Profile			COM+	Attribute Editor	

Attributes:

Attribute	Value
desktopProfile	<not set>
destinationIndicator	<not set>
displayName	Cisco User <span style="border: 1px solid green; border-radius: 50%; padding: 2px 5px;">3</span>
displayableNamePrintable	<not set>
distinguishedName	CN=CUser,CN=Users,DC=Cisco Lab,DC=com
division	<not set>

Wählen Sie die Registerkarte **Mitglied von** aus und klicken Sie auf **Hinzufügen**.

# Cisco B. User Properties



Security	Environment	Sessions	Remote control		
Remote Desktop Service	file	COM+	Attribute Editor		
General	Address	Account	Profile	Telephones	Organization
Published Certificates	Member Of	Password Replication	Dial-in	Object	

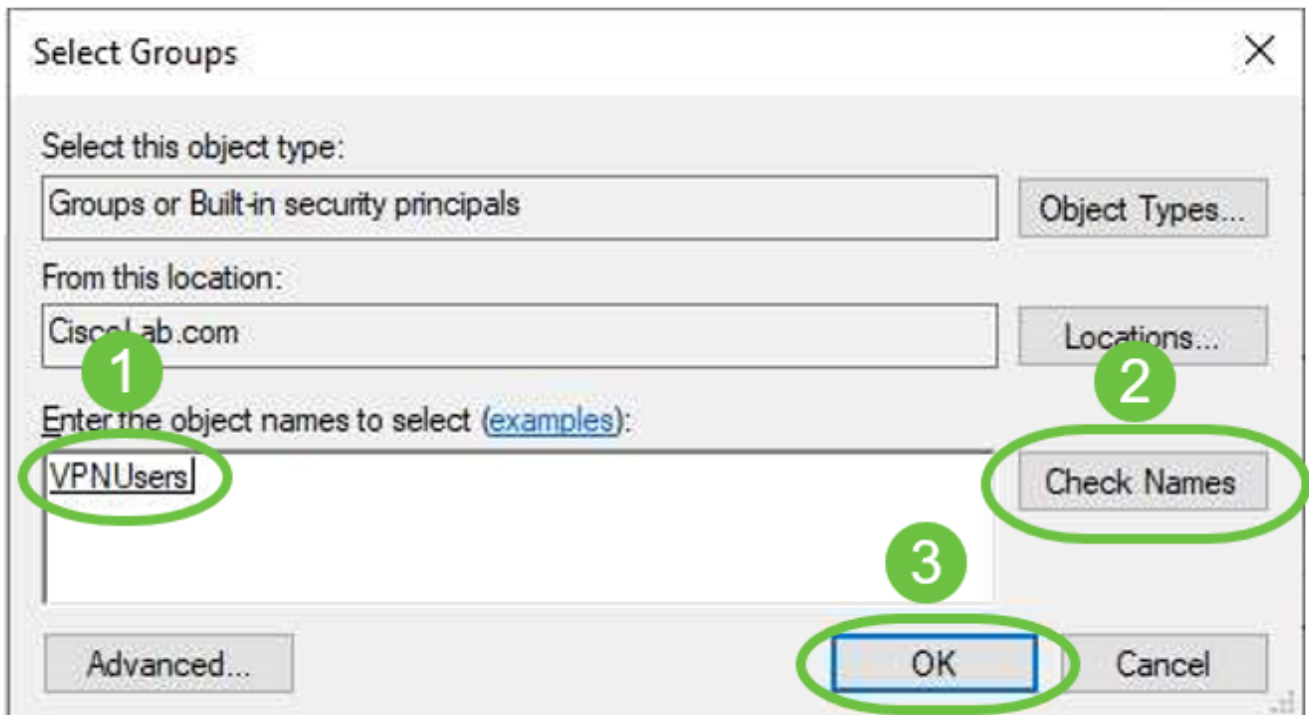
Member of:

Name	
Domain Users	CiscoLab.com/Users

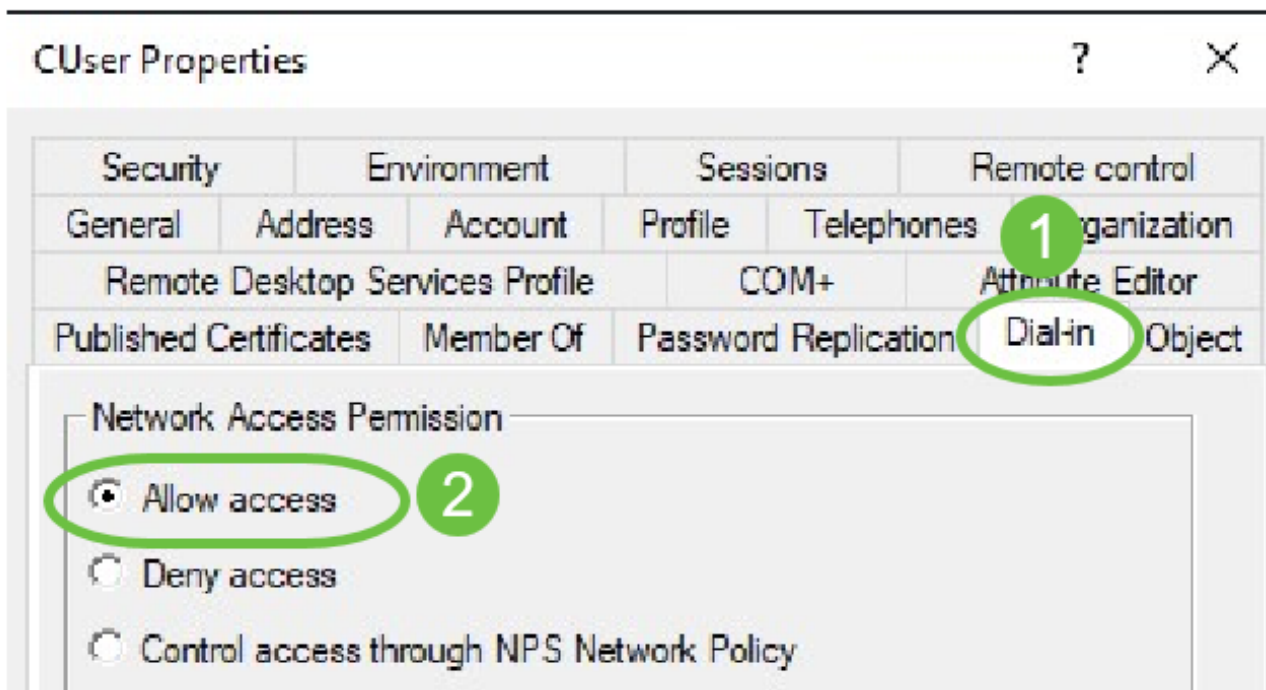
2

Add... Remove

Geben Sie den Namen der *Global Security Group* ein, und wählen Sie **Check Name aus**. Wenn der Eintrag unterstrichen ist, klicken Sie auf **OK**.



Wählen Sie die Registerkarte **Dial-In**. Wählen Sie im Abschnitt *Network Access Permission* (Netzwerkzugriffsberechtigung) die Option **Access (Zugriff zulassen)** aus, und belassen Sie den Rest als Standard.

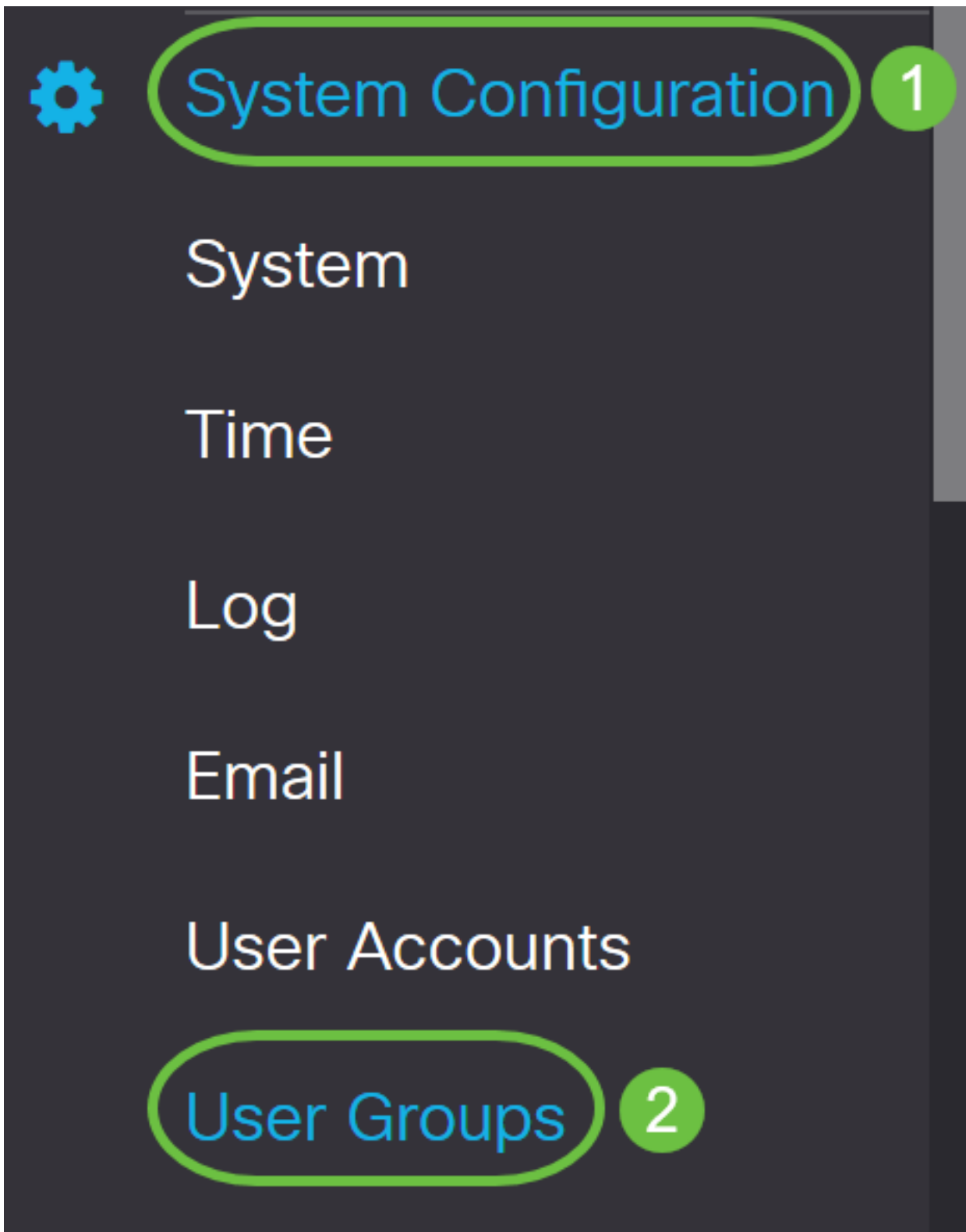


## Active Directory-Integration

Bei Active Directory muss die Uhrzeit des RV34x-Routers mit der des AD-Servers übereinstimmen. Anweisungen zum Konfigurieren von Zeiteinstellungen auf einem Router der Serie RV34x finden Sie [hier](#).

Für AD ist außerdem erforderlich, dass der RV340 über eine Benutzergruppe verfügt, die der AD Global Security Group entspricht.

Schritt 1: Navigieren Sie zu **Systemkonfiguration > Benutzergruppen**.



Schritt 2: Klicken Sie auf das **Plus**-Symbol, um eine Benutzergruppe hinzuzufügen.

# User Groups

## User Groups Table



Schritt 3: Geben Sie den *Gruppennamen ein*. In diesem Beispiel sind es **VPNUsers**.

Group Name:

Der Gruppenname muss mit der AD Global Security Group identisch sein.

Schritt 4: Unter *Dienste* sollte *Web Login/NETCONF/RESTCONF* als **Deaktiviert** markiert werden. Wenn die AD-Integration nicht sofort funktioniert, können Sie weiterhin auf den RV34x zugreifen.

## Services

Web Login/NETCONF/RESTCONF  Disabled  Read Only  Administrator

Schritt 5: Sie können die VPN-Tunnel hinzufügen, die AD-Integration verwenden, um die Benutzer anzumelden.

1. Um ein bereits konfiguriertes Client-to-Site-VPN hinzuzufügen, gehen Sie zum Abschnitt *EZVPN/Drittanbieter* und klicken Sie auf das **Plus**-Symbol. Wählen Sie das VPN-Profil aus dem Dropdown-Menü aus, und klicken Sie auf **Hinzufügen**.

## EzVPN/3rd Party

### EzVPN/3rd Party Profile Member In-use Table



#



Group Name



#### Add Feature List

Select a Profile: ShrewVPN 1

2

4. SSL VPN - Wenn ein SSL VPN-Tunnel verwendet wird, wählen Sie die Richtlinie aus dem Dropdown-Menü neben *Profil auswählen* aus.

SSL VPN

Select a Profile

SSLVPNDefaultPolicy



6. PPTP/L2TP/802.1x - Um die Verwendung von AD zu ermöglichen, aktivieren Sie einfach das Kontrollkästchen neben den Optionen *Zulassen*.

PPTP VPN



Permit

L2TP



Permit

802.1x





Permit



Schritt 6: Klicken Sie auf **Apply**, um die Änderungen zu speichern.

## User Groups

Apply

Site to Site VPN Profile Member In-use Table



 



#  Connection Name 

---


EzVPN/3rd Party

EzVPN/3rd Party Profile Member In-use Table

#  Group Name 

---

SSL VPN Select a Profile SSLVPNDefaultPolicy 

PPTP VPN  Permit

L2TP  Permit

802.1x  Permit

## Active Directory-Integrationseinstellungen

Schritt 1: Navigieren Sie zu **Systemkonfiguration > Benutzerkonten**.



## System Configuration

System

1

Time

Log

Email

User Accounts

2

Schritt 2: Klicken Sie in der Tabelle für den Dienst für die Remoteauthentifizierung auf **Hinzufügen**, um einen Eintrag zu erstellen.



# Remote Authentication Service Table



Enable ⇅

Name ⇅

Schritt 3: Erstellen Sie im Feld *Name* einen Benutzernamen für das Konto. In diesem Beispiel wird **Jorah\_Admin** verwendet.

## Add/Edit New Domain

Name

Jorah\_Admin

Schritt 4: Wählen Sie im Dropdown-Menü *Authentication Type (Authentifizierungstyp)* die Option **Active Directory (Active Directory)**. AD wird verwendet, um allen Netzwerkelementen umfassende Richtlinien zuzuweisen, Programme auf vielen Computern bereitzustellen und kritische Updates auf das gesamte Unternehmen anzuwenden.

Authentication Type

Active Directory

AD Domain Name

RADIUS

Active Directory

Primary Server

LDAP

Schritt 5: Geben Sie im Feld *AD Domain Name (AD-Domänenname)* den vollqualifizierten

Domännennamen des AD ein.

In diesem Beispiel wird **sampledomain.com** verwendet.

AD Domain Name

Schritt 6: Geben Sie im Feld *Primärserver* die Adresse des AD ein.

In diesem Beispiel wird **192.168.2.122** verwendet.

Primary Server  Port

Schritt 7: Geben Sie im Feld *Port* eine Portnummer für den primären Server ein.

In diesem Beispiel wird **1234** als Portnummer verwendet.

Primary Server  Port

Schritt 8: (Optional) Geben Sie im Feld *User Container Path* einen Stammpfad ein, in dem die Benutzer enthalten sind.

**Hinweis:** In diesem Beispiel wird **file:Documents/manage/containers** verwendet.

User Container Path

Schritt 9: Klicken Sie auf **Apply** (Anwenden).

## User Accounts

Apply

### Add/Edit New Domain

Name	<input type="text" value="Jorah_Admin"/>		
Authentication Type	<input type="text" value="Active Directory"/>		
AD Domain Name	<input type="text" value="sampledomain.com"/>		
Primary Server	<input type="text" value="192.168.2.122"/>	Port	<input type="text" value="1234"/>
User Container Path	<input type="text" value="file:Documents/manage/co"/>		

Schritt 10: Scrollen Sie nach unten zu *Service Auth Sequence*, um die Anmeldemethode für die verschiedenen Optionen festzulegen.

- Web-Anmeldung/NETCONF/RESTCONF - So melden Sie sich beim Router RV34x an. Deaktivieren Sie das Kontrollkästchen *Standard verwenden*, und legen Sie die primäre Methode auf **Lokale DB fest**. Dadurch wird sichergestellt, dass Sie nicht vom Router abgemeldet werden, auch wenn die Active Directory-Integration fehlschlägt.
- Site-to-Site/EzVPN und Drittanbieter-Client-to-Site-VPN - Mit diesem VPN-Tunnel für den Client-to-Site-Zugriff können Sie AD verwenden. Deaktivieren Sie das Kontrollkästchen *Standard verwenden*, und setzen Sie die primäre Methode auf **Active Directory** und Secondary Method auf **Local DB**.

## Service Auth Sequence

\* Default Sequence is RADIUS > LDAP > AD > Local DB

\* Local DB must be enabled in Web Login/NETCONF/RESTCONF

### Service Auth Sequence Table

Service ↕	Use Default ↕	Customize: Primary ↕	Customize: Secondary
Web Login/NETCONF/RESTCONF	<input type="checkbox"/>	<input type="text" value="Local DB"/>	<input type="text" value="None"/>
Site-to-site/EzVPN&3rd Party Client-to-site VPN	<input type="checkbox"/>	<input type="text" value="Active Directory"/>	<input type="text" value="Local DB"/>
AnyConnect SSL VPN	<input type="checkbox"/>	<input type="text" value="Active Directory"/>	<input type="text" value="Local DB"/>

Schritt 11: Klicken Sie auf **Apply** (Anwenden).

## User Accounts

Apply

### Service Auth Sequence

\* Default Sequence is RADIUS > LDAP > AD > Local DB

\* Local DB must be enabled in Web Login/NETCONF/RESTCONF

### Service Auth Sequence Table

Schritt 12: Speichern Sie die aktuelle Konfiguration als Startkonfiguration.

Sie haben jetzt die Active Directory-Einstellungen auf einem Router der Serie RV34x erfolgreich konfiguriert.

## LDAP

Schritt 1: Klicken Sie in der Tabelle für den Dienst für die Remoteauthentifizierung auf **Hinzufügen**, um einen Eintrag zu erstellen.

# Remote Authentication Service Table



Enable 

Name 

Schritt 2: Erstellen Sie im Feld *Name* einen Benutzernamen für das Konto.

Es kann nur ein einziges Remote-Benutzerkonto unter LDAP konfiguriert werden.

In diesem Beispiel wird Dany\_Admin verwendet.

Name

Dany\_Admin

Schritt 3: Wählen Sie im Dropdown-Menü Authentication Type (Authentifizierungstyp) die Option **LDAP aus**. Lightweight Directory Access Protocol ist ein Zugriffsprotokoll, das für den Zugriff auf einen Verzeichnisdienst verwendet wird. Es ist ein Remoteserver, der ein Verzeichnis ausführt, um die Authentifizierung für die Domäne auszuführen.

Authentication Type

Primary Server

Base DN

**LDAP**

RADIUS

Active Directory

Schritt 4: Geben Sie im *Feld Primärserver* die Serveradresse des LDAP ein.

In diesem Beispiel wird **192.168.7.122** verwendet.

Primary Server  Port

Schritt 5: Geben Sie im *Feld Port* eine Portnummer für den primären Server ein.

In diesem Beispiel wird **122** als Portnummer verwendet.

Primary Server  Port

Schritt 6: Geben Sie den unterschieden Basisnamen des LDAP-Servers in das *Feld Basis-DN ein* . Der Basis-DN ist der Ort, an dem der LDAP-Server nach Benutzern sucht, wenn er eine Autorisierungsanfrage empfängt. Dieses Feld sollte mit der Basis-DN übereinstimmen, die auf dem LDAP-Server konfiguriert ist.

In diesem Beispiel wird **Dept101** verwendet.

Base DN

Schritt 7: Klicken Sie auf **Apply** (Anwenden). Sie gelangen zur Servicetabelle für die Remoteauthentifizierung.

User Accounts

Add/Edit New Domain

Name

Authentication Type

Primary Server  Port

Base DN

Schritt 8: (Optional) Wenn Sie den Remote-Authentifizierungsdienst aktivieren oder deaktivieren möchten, aktivieren oder deaktivieren Sie das Kontrollkästchen neben dem Dienst, den Sie

aktivieren oder deaktivieren möchten.

## Remote Authentication Service Table

<input type="checkbox"/>	Enable ▾	Name ▾
<input type="checkbox"/>	<input checked="" type="checkbox"/>	AD
<input type="checkbox"/>	<input type="checkbox"/>	LDAP
<input type="checkbox"/>	<input type="checkbox"/>	RADIUS

Schritt 9: Klicken Sie auf Apply (Anwenden).

User Accounts

Apply

Sie haben jetzt erfolgreich das LDAP auf einem Router der Serie RV34x konfiguriert.

**Sehen Sie sich ein Video zu diesem Artikel an..**

[Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.](#)