

# RV34x Series 라우터에서 사용자 계정 구성 및 관리

## 목표

이 문서의 목적은 RV34x Series 라우터에서 로컬 및 원격 사용자 계정을 구성하고 관리하는 방법을 보여 주는 것입니다. 여기에는 로컬 사용자 비밀번호 복잡성 구성, 로컬 사용자 구성/편집/가져오기, RADIUS, Active Directory 및 LDAP를 사용하여 원격 인증 서비스를 구성하는 방법이 포함됩니다.

## 적용 가능한 디바이스 | 펌웨어 버전

- RV34x 시리즈 | 1.0.01.16([최신 다운로드](#))

## 소개

RV34x Series Router는 설정을 보고 관리하기 위한 사용자 계정을 제공합니다. 사용자는 서로 다른 그룹의 사용자이거나 인증 도메인, LAN(Local Area Network) 및 서비스 액세스 규칙, 유휴 시간 제한 설정을 공유하는 SSL(Secure Sockets Layer) VPN(Virtual Private Networks)의 논리적 그룹에 속할 수 있습니다. 사용자 관리는 어떤 유형의 사용자가 특정 유형의 시설을 활용할 수 있는지, 어떻게 할 수 있는지를 정의합니다.

외부 데이터베이스 우선 순위는 항상 RADIUS(Remote Authentication Dial-In User Service)/LDAP(Lightweight Directory Access Protocol)/AD(Active Directory)/Local입니다. 라우터에 RADIUS 서버를 추가하면 웹 로그인 서비스 및 기타 서비스에서 RADIUS 외부 데이터베이스를 사용하여 사용자를 인증합니다.

웹 로그인 서비스에만 외부 데이터베이스를 사용하도록 설정하고 다른 서비스에 대해 다른 데이터베이스를 구성하는 옵션은 없습니다. 라우터에서 RADIUS를 생성하고 활성화하면 라우터는 웹 로그인, 사이트 대 사이트 VPN, EzVPN/타사 VPN, SSL VPN, PPTP(Point-to-Point Transport Protocol)/L2TP(Layer 2 Transport Protocol) VPN 및 802.1x에 대한 외부 데이터베이스로 RADIUS 서비스를 사용합니다.

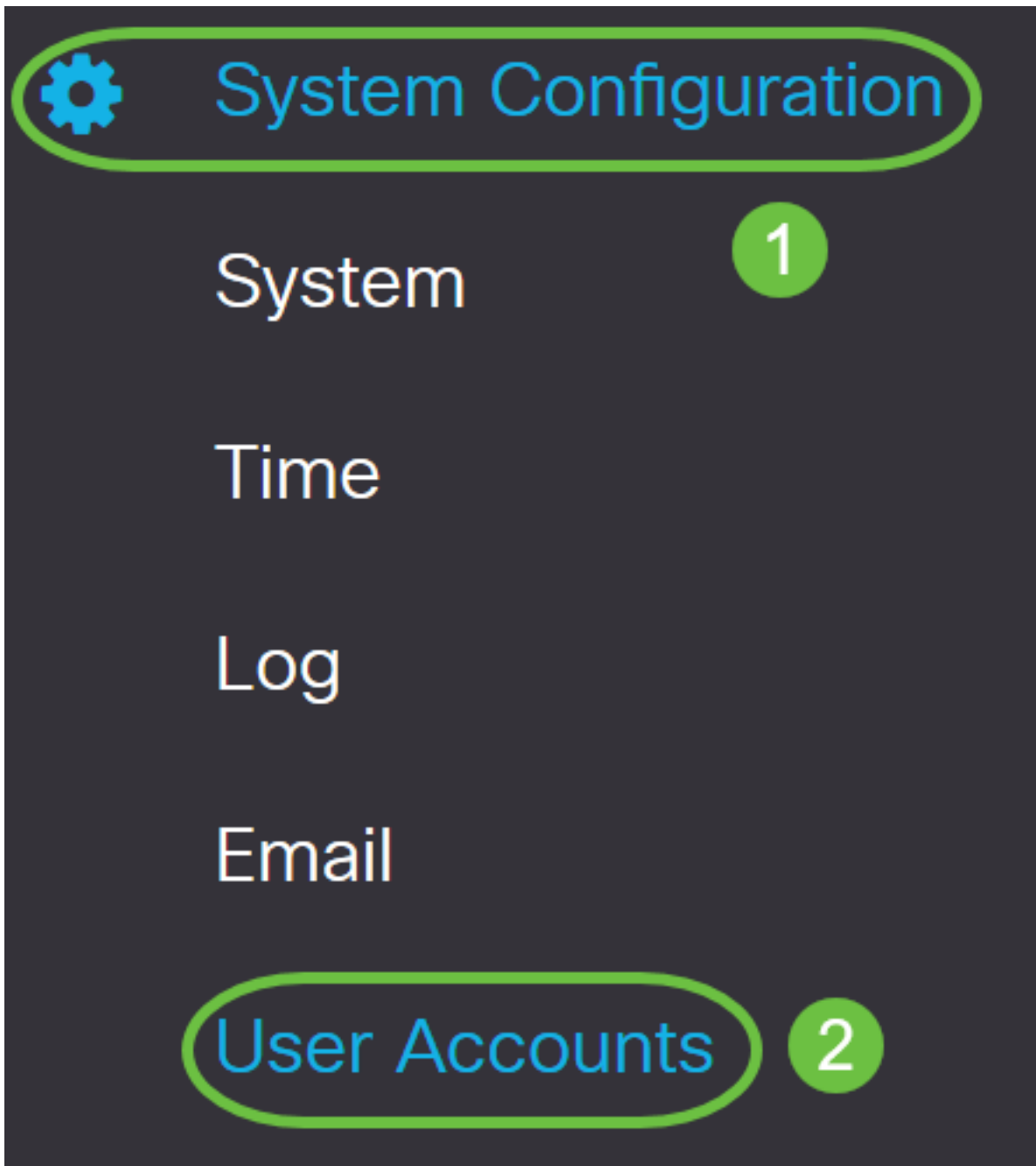
## 목차

- [로컬 사용자 계정 구성](#)
- [로컬 사용자 비밀번호 복잡성](#)
- [로컬 사용자 구성](#)
- [로컬 사용자 편집](#)
- [로컬 사용자 가져오기](#)
- [원격 인증 서비스 구성](#)
- [RADIUS](#)
- [Active Directory 구성](#)
- [Active Directory 통합](#)
- [Active Directory 통합 설정](#)
- [LDAP](#)

## 로컬 사용자 계정 구성

## 로컬 사용자 비밀번호 복잡성

1단계. 라우터의 웹 기반 유틸리티에 로그인하고 System Configuration(시스템 컨피그레이션) > User Accounts(사용자 계정)를 선택합니다.



2단계. 비밀번호 복잡성 매개변수를 활성화하려면 **Enable Password Complexity Settings**(비밀번호 복잡성 설정 활성화) 확인란을 선택합니다.

이 옵션을 선택하지 않은 상태이면 Configure Local [Users](#)(로컬 사용자 구성)로 건너됩니다.

# Local Users Password Complexity

Password Complexity Settings:

Enable

3단계. *최소 비밀번호 길이* 필드에 0~127의 숫자를 입력하여 비밀번호에 포함해야 할 최소 문자 수를 설정합니다. 기본값은 8입니다.

이 예에서는 최소 문자 수가 **10**으로 설정됩니다.

## Local Users Password Complexity

Password Complexity Settings:

Enable

Minimal password length:

10

(Range: 0 - 127, Default: 8)

4단계. *최소 문자 클래스 수* 필드에 0에서 4 사이의 숫자를 입력하여 클래스를 설정합니다. 입력한 숫자는 다른 클래스의 최소 또는 최대 문자 수를 나타냅니다.

- 비밀번호는 대문자(ABCD)로 구성됩니다.
- 비밀번호는 소문자(abcd)로 구성됩니다.
- 암호는 숫자 문자(1234)로 구성됩니다.
- 암호는 특수 문자(!@#\$)로 구성됩니다.

이 예에서는 **4**가 사용됩니다.

## Local Users Password Complexity

Password Complexity Settings:

Enable

Minimal password length:

10

(Range: 0 - 127, Default: 8)

Minimal number of character classes:

4

(Range: 0 - 4, Default: 3)

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

5단계. 새 비밀번호에 대한 **Enable** 확인란을 현재 비밀번호와 달라야 합니다.

## 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

6단계. Password *Aging Time*(비밀번호 에이징 시간) 필드에 비밀번호 만료에 대한 일 수(0 - 365)를 입력합니다. 이 예에서는 **180**일이 입력되었습니다.

## 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)

이제 라우터에서 로컬 사용자 비밀번호 복잡성 설정을 성공적으로 구성했습니다.

## 로컬 사용자 구성

1단계. Local User Membership List(로컬 사용자 구성원 목록) 테이블에서 **Add(추가)**를 클릭하여 새 사용자 계정을 생성합니다. 사용자 계정 추가 페이지로 이동합니다.

# 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

Add *User Account* header 아래 Local Password Complexity(로컬 비밀번호 복잡성) 단계에서 정의된 매개변수가 표시됩니다.

# 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

2단계. 사용자 이름 필드에 계정의 사용자 이름을 입력합니다.


이 예에서는 **Administrator\_Noah**가 사용됩니다.

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"/>	

3단계. *New Password*(새 비밀번호) 필드에 정의된 매개변수를 사용하여 비밀번호를 입력합니다 .이 예에서 최소 비밀번호 길이는 대문자, 소문자, 숫자 및 특수 문자의 조합으로 10자로 구성되어야 합니다.

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: 25%; background-color: red;"></div><div style="width: 25%; background-color: yellow;"></div><div style="width: 50%; background-color: gray;"></div></div>	
Group	<input type="text" value="admin"/>	

4단계. *New Password Confirm*(새 비밀번호 확인) 필드에 확인할 비밀번호를 다시 입력합니다.비밀번호가 일치하지 않으면 필드 옆에 텍스트가 나타납니다.

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"/>	▼


비밀번호 강도 측정기는 비밀번호의 강도에 따라 변경됩니다.



5단계. *Group* 드롭다운 목록에서 사용자 계정에 권한을 할당할 그룹을 선택합니다.옵션은 다음과 같습니다.

- admin - 읽기 및 쓰기 권한
- guest - 읽기 전용 권한입니다.

이 예에서는 **admin**이 선택됩니다.

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"/>	

6단계. 적용을 클릭합니다.

## 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: 33%; background-color: gray;"></div></div>	
Group	<input type="text" value="admin"/>	▼

이제 RV34x Series 라우터에서 로컬 사용자 멤버십을 성공적으로 구성했습니다.

## 로컬 사용자 편집

1단계. Local User Membership List(로컬 사용자 구성원 목록) 테이블에서 로컬 사용자의 사용자 이름 옆에 있는 확인란을 선택합니다.

이 예에서는 **Administrator\_Noah**가 선택됩니다.



# 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

2단계. Edit(수정)를 클릭합니다.

# 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

사용자 이름을 편집할 수 없습니다.

3단계. 이전 *비밀번호* 필드에 로컬 사용자 계정에 대해 이전에 구성한 비밀번호를 입력합니다.

## Edit User Account

User Name

Old Password

4단계. *New Password* 필드에 새 비밀번호를 입력합니다. 새 암호는 최소 요구 사항을 충족해야 합니다.

## Edit User Account

User Name

Old Password

New Password

( Range: 0 - 127 )

5단계. 새 비밀번호 확인 필드에 새 비밀번호를 한 번 더 입력하여 확인합니다. 이러한 비밀번호는 일치해야 합니다.

## Edit User Account

User Name

Old Password

New Password

( Range: 0 - 127 )

New Password Confirm

6단계. (선택 사항) Group(그룹) 드롭다운 목록에서 사용자 계정에 권한을 할당할 그룹을 선택합니다.

이 예에서는 게스트가 선택됩니다.

# Edit User Account

User Name

Administrator\_Noah

Old Password

●●●●●●●●

New Password

●●●●●●●●

( Range: 0 - 127 )

New Password Confirm

●●●●●●●●

Group

guest

admin

guest

7단계. 적용을 클릭합니다.

User Accounts

Apply

Cancel

## Edit User Account

User Name

Administrator\_Noah

Old Password

●●●●●●●●

New Password

●●●●●●●●

( Range: 0 - 127 )

New Password Confirm

●●●●●●●●

Group

guest

이제 로컬 사용자 계정을 편집했습니다.

# 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

## 로컬 사용자 가져오기



1단계. Local Users Import(로컬 사용자 가져오기) 영역에서 을 클릭합니다 .

2단계. Import User Name & Password(사용자 이름 및 비밀번호 가져오기)에서 **Browse...**를 클릭하여 사용자 목록을 가져옵니다. 이 파일은 일반적으로 쉼표로 구분된 값(.CSV) 형식으로 저장된 스프레드시트입니다.

이 예에서는 **user-template.csv**가 선택됩니다.

# Local Users Import

Import User Name & Password

Browse...

user-template.csv

(Import User Name + Password via CSV files)

Import

Download User Template:

Download

3단계. (선택 사항) 템플릿이 없는 경우 Download User Template(사용자 템플릿 다운로드) 영역에서 Download(다운로드)를 클릭합니다.

# Local Users Import

Import User Name & Password

Browse...

user-template.csv

(Import User Name + Password via CSV files)

Import

Download User Template:

Download

4단계. 가져오기를 클릭합니다.

# Local Users Import

Import User Name & Password

Browse...

user-template.csv

(Import User Name + Password via CSV files)

Import

Download User Template:

Download

가져오기 버튼 옆에 가져오기가 성공했다는 메시지가 나타납니다.

로컬 사용자 목록을 성공적으로 가져왔습니다.

## 원격 인증 서비스 구성

### RADIUS

1단계. Remote Authentication Service Table(원격 인증 서비스 테이블)에서 Add(추가)를 클릭하여 항목을 생성합니다.



# Remote Authentication Service Table



Enable       Name 

2단계. *Name* 필드에서 계정의 사용자 이름을 생성합니다.

이 예에서는 **관리자**가 사용됩니다.

## Add/Edit New Domain

Name

Administrator

3단계. Authentication Type(인증 유형) 드롭다운 메뉴에서 **Radius**를 선택합니다. 즉, RADIUS 서버를 통해 사용자 인증이 수행됩니다.

RADIUS의 단일 원격 사용자 계정만 구성할 수 있습니다.

Authentication Type

RADIUS



**RADIUS**

Active Directory

LDAP

Primary Server

Backup Server

4단계. *Primary Server* 필드에 기본 RADIUS 서버의 IP 주소를 입력합니다.

이 예에서 **192.168.3.122**는 기본 서버로 사용됩니다.

Primary Server

192.168.3.122

Port

389

5단계. Port(포트) 필드에 기본 RADIUS 서버의 포트 번호를 입력합니다.

이 예에서 **1645**는 포트 번호로 사용됩니다.

Primary Server

192.168.3.122

Port

389

6단계. Backup Server(백업 서버) 필드에 백업 RADIUS 서버의 IP 주소를 입력합니다. 이는 기본 서버가 다운될 경우 장애 조치 역할을 합니다.

이 예에서 백업 서버 주소는 **192.168.4.122**입니다.

Backup Server

192.168.4.122

Port

389

7단계. Port 필드에 백업 RADIUS 서버의 수를 입력합니다.

Backup Server

192.168.4.122

Port

389

이 예에서 **1646**은 포트 번호로 사용됩니다.

8단계. Preshared-Key 필드에 RADIUS 서버에 구성된 사전 공유 키를 입력합니다.

Pre-shared Key

●●●●●●●●●●

9단계. Confirm Preshared-key 필드에서 확인할 사전 공유 키를 다시 입력합니다.

Confirm Pre-shared Key

●●●●●●●●●●

10단계. 적용을 누릅니다.

## 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="text" value="●●●●●●●●"/>		
Confirm Pre-shared Key	<input type="text" value="●●●●●●●●"/>		

기본 사용자 계정 페이지로 이동합니다. 최근에 구성된 어카운트가 Remote Authentication Service 테이블에 나타납니다.

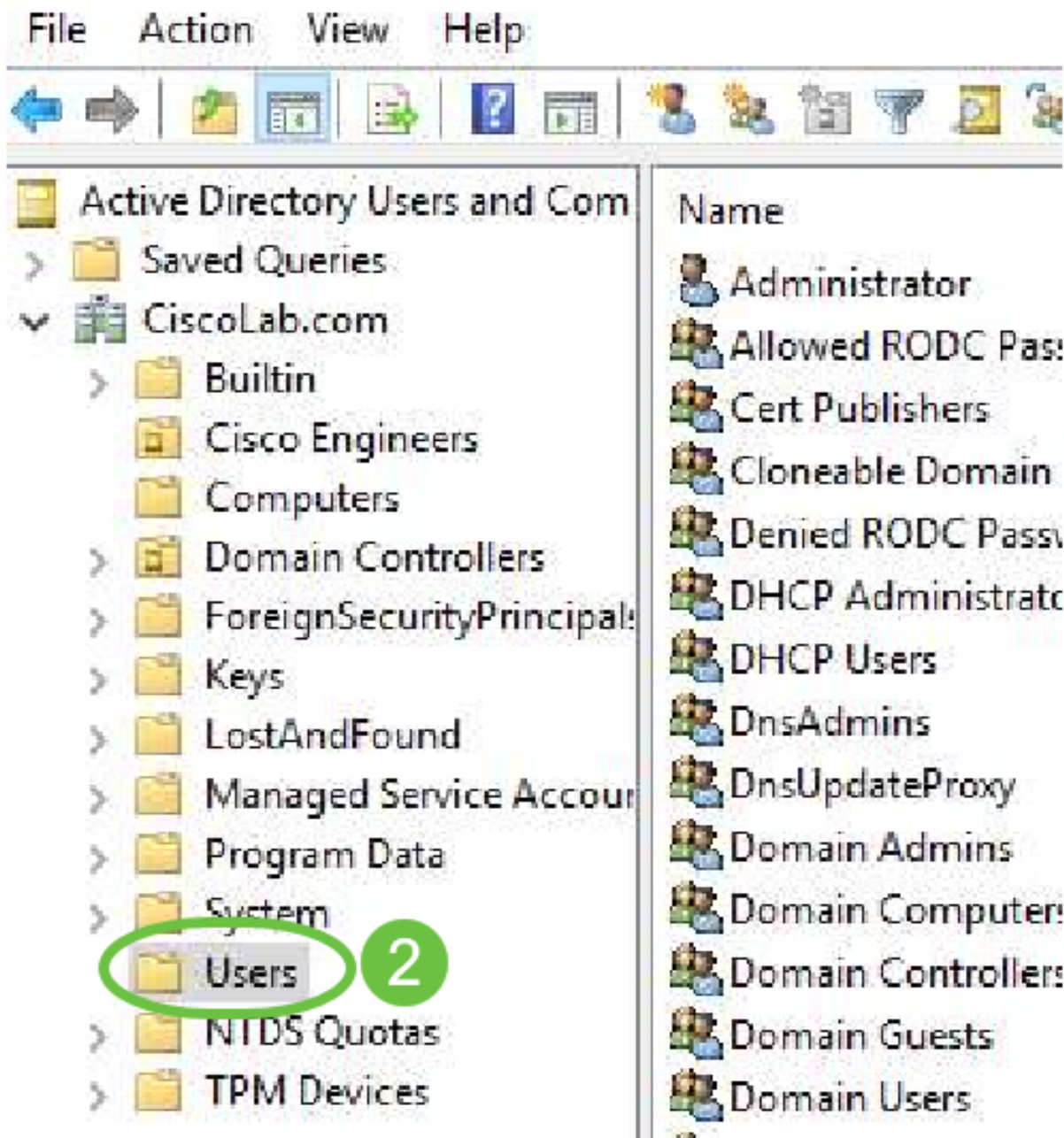
이제 RV34x Series 라우터에서 RADIUS 인증을 성공적으로 구성했습니다.

## Active Directory 구성

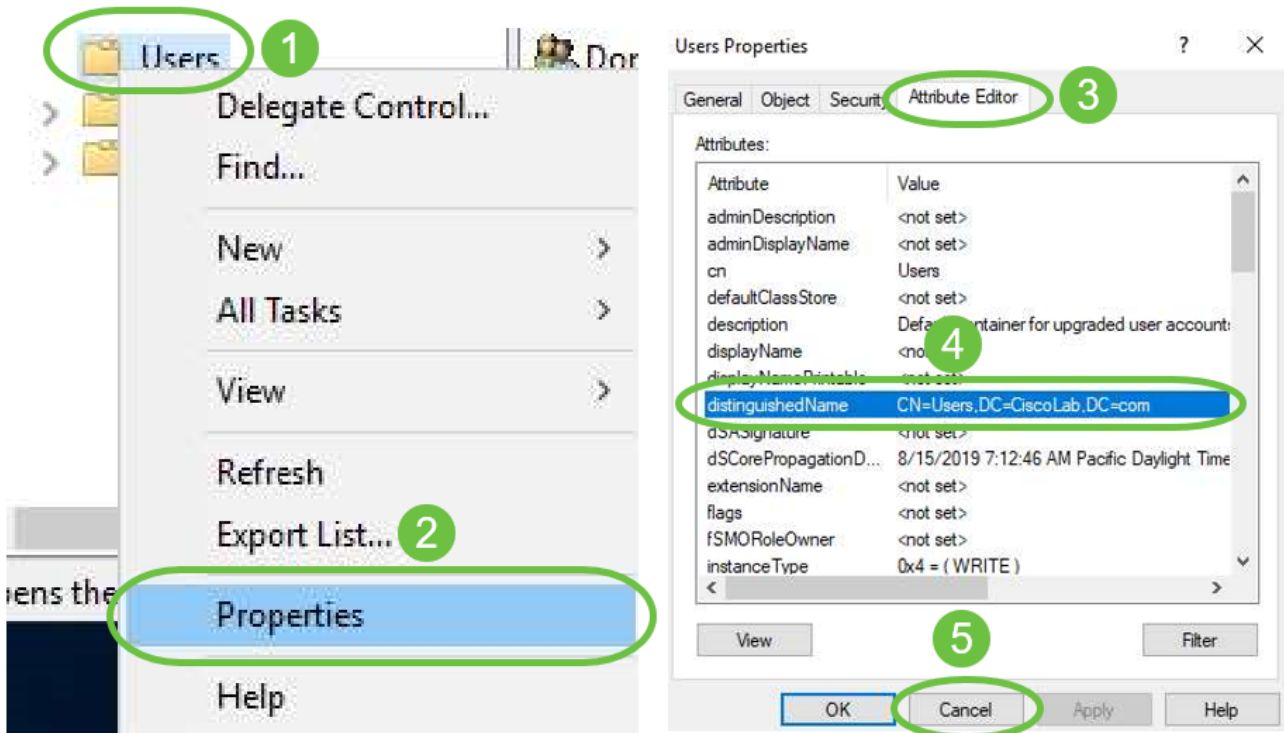
1단계. Active Directory 구성을 완료하려면 Active Directory 서버에 로그인해야 합니다. PC에서 **Active Directory 사용자 및 컴퓨터**를 열고 원격으로 로그인하는 데 사용되는 사용자 계정이 있는 컨테이너로 이동합니다. 이 예에서는 **Users** 컨테이너를 사용합니다.

# Active Directory Users and Computers

1



2단계. 컨테이너를 마우스 오른쪽 버튼으로 클릭하고 속성을 선택합니다.속성 편집기 탭으로 이동하여 *distinguishedName* 필드를 찾습니다.이 탭이 표시되지 않으면 Active Directory 사용자 및 컴퓨터에서 고급 기능 보기를 사용하도록 설정하고 다시 시작해야 합니다.이 필드를 기록하고 취소를 클릭합니다.사용자 컨테이너 경로가 됩니다.이 필드는 RV340을 구성할 때도 필요하며 정확히 일치해야 합니다.



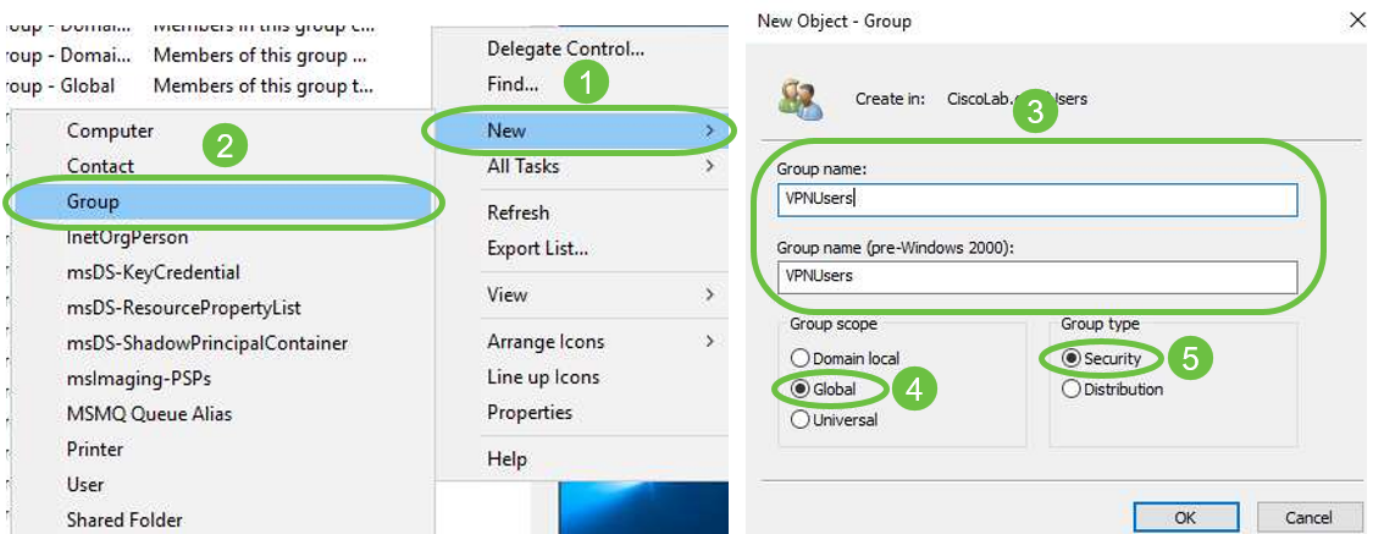
3단계. 사용할 사용자 계정과 동일한 컨테이너에 글로벌 보안 그룹을 생성합니다.

선택한 컨테이너에서 빈 영역을 마우스 오른쪽 단추로 클릭하고 새로 만들기 > 그룹을 선택합니다.

다음을 선택합니다.

- Group Name(그룹 이름) - 이 이름은 RV340에 생성된 사용자 그룹 이름과 정확히 일치해야 합니다. 이 예에서는 VPNUsers를 사용합니다.
- 그룹 범위 - 전역
- 그룹 유형 - 보안

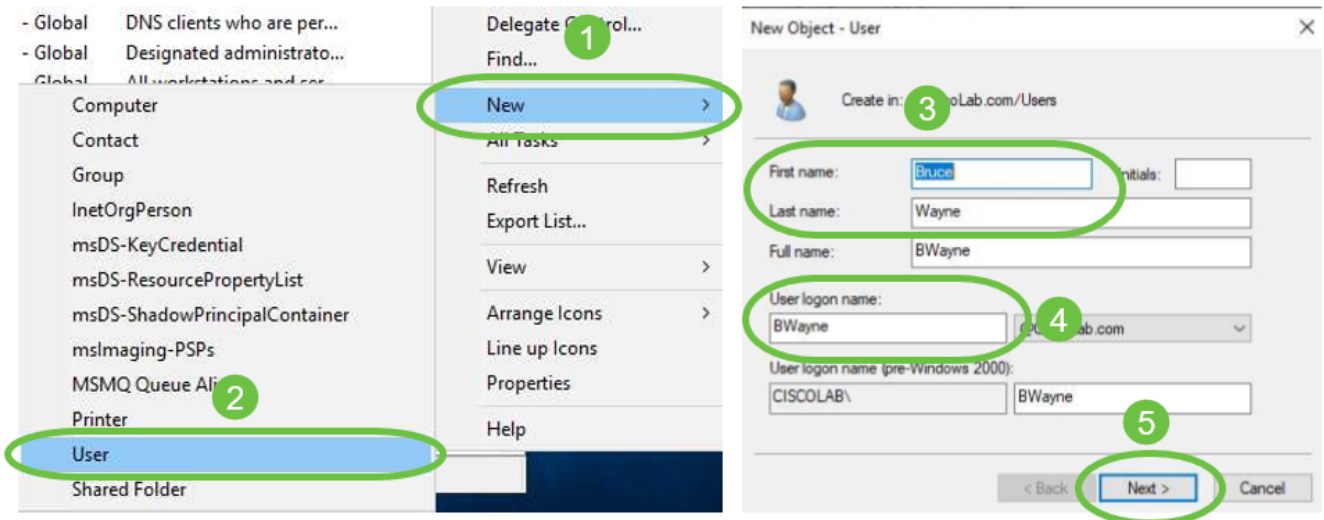
확인을 클릭합니다.



4단계. 새 사용자 계정을 생성하려면 다음을 수행합니다.

- 컨테이너에서 빈 공간을 마우스 오른쪽 단추로 클릭하고 새로 만들기 > 사용자 를 선택합니다.

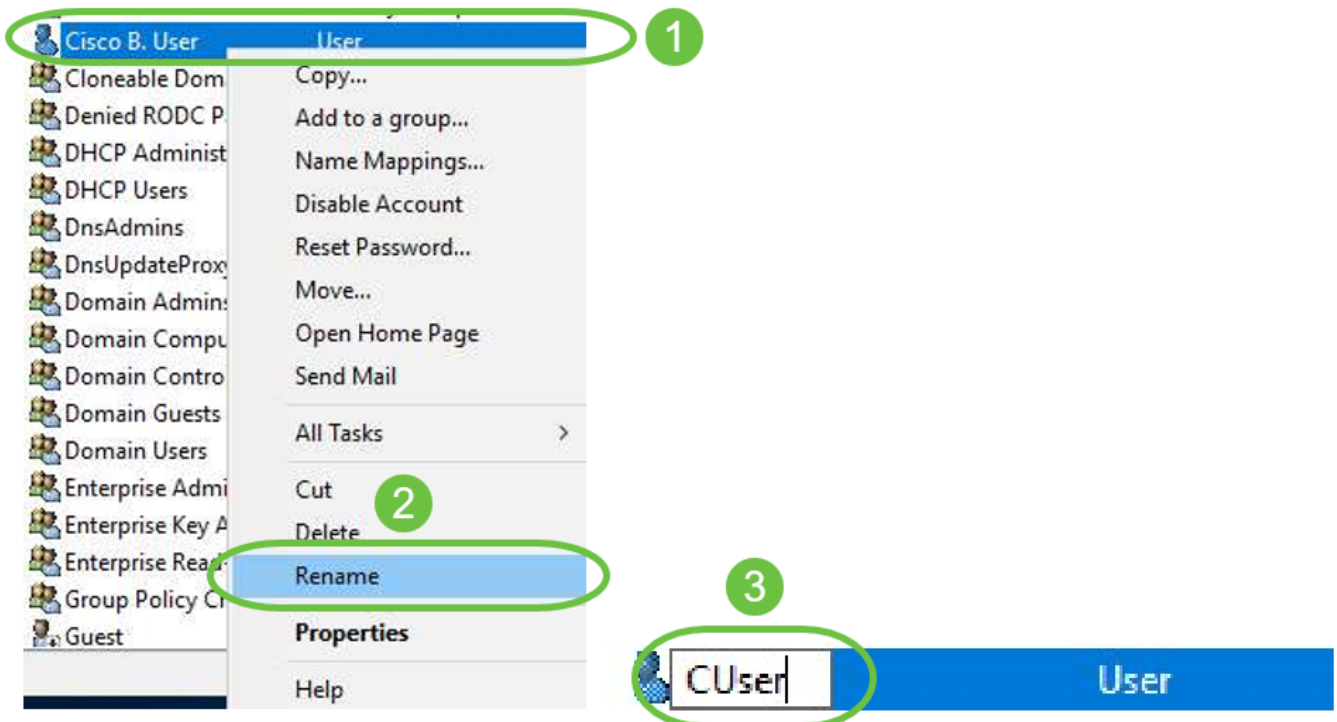
- 이름, 성을 입력합니다.
- 사용자 로그온 이름을 입력합니다.
- Next(다음)를 클릭합니다.



사용자의 비밀번호를 입력하라는 메시지가 표시됩니다. *User must change password at next logon* (다음 로그온 시 사용자가 암호를 변경해야 함) 확인란을 선택하면 사용자가 로컬로 로그인하고 비밀번호를 변경해야 원격으로 로그인할 수 있습니다.

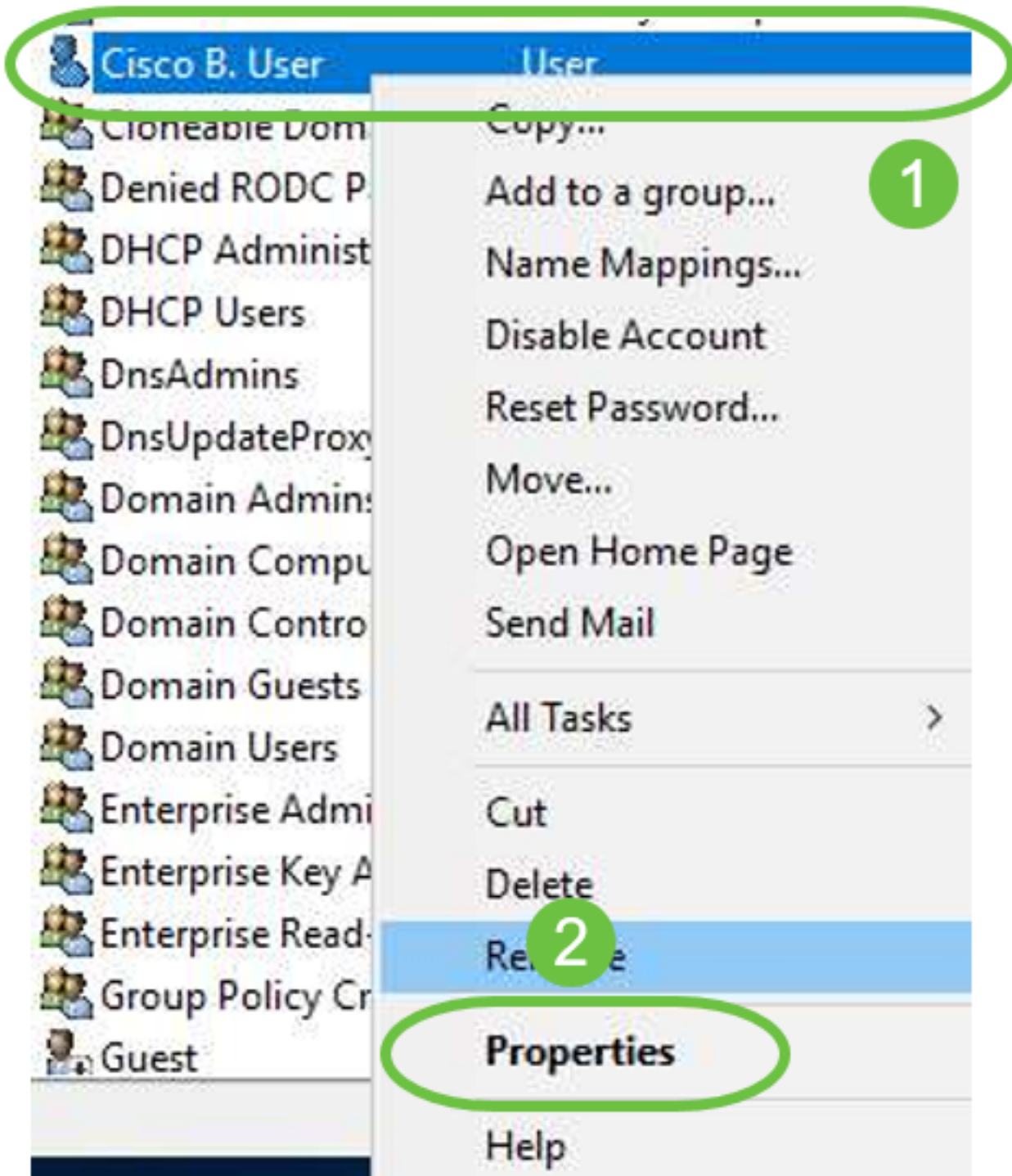
마침을 클릭합니다.

User Accounts(사용자 어카운트)를 사용해야 하는 경우 조정을 수행해야 할 수 있습니다. 사용자의 정식 이름을 조정하려면 사용자를 선택하고 마우스 오른쪽 단추를 클릭한 다음 이름 바꾸기를 선택합니다. 모든 공백을 제거하고 사용자의 로그온 이름과 일치하는지 확인합니다. 사용자 표시 이름은 변경되지 않습니다. 확인을 클릭합니다.



5단계. 사용자 계정이 올바르게 구성되면 원격으로 로그인할 수 있는 권한을 부여받아야 합니다.

이렇게 하려면 사용자 계정을 선택하고 마우스 오른쪽 단추를 클릭한 다음 속성을 선택합니다.



사용자 등록 정보에서 속성 편집기 탭을 선택하고 아래로 스크롤하여 distinguishedName으로 이동합니다. 첫 번째 CN=공백 없이 올바른 사용자 로그인 이름이 있는지 확인합니다.

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 <b>2</b>	

Attributes:

Attribute	Value
desktopProfile	<not set>
destinationIndicator	<not set>
displayName	Cisco <b>3</b> User
displaynamePrintable	<not set>
distinguishedName	CN=CUser,CN=Users,DC=Cisco Lab,DC=com
division	<not set>

Member Of 탭을 선택하고 Add를 클릭합니다.



# 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	

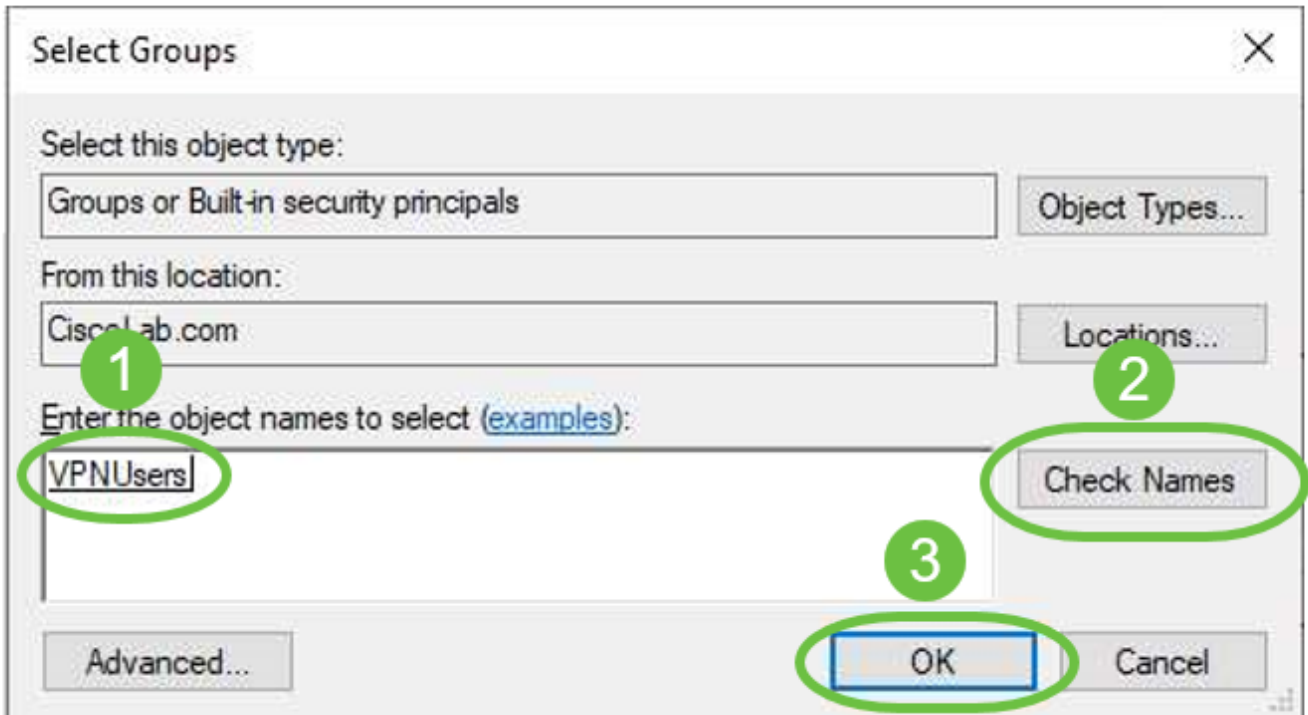
Member of:

Name	Active Directory Domain Services Folder
Domain Users	CiscoLab.com/Users

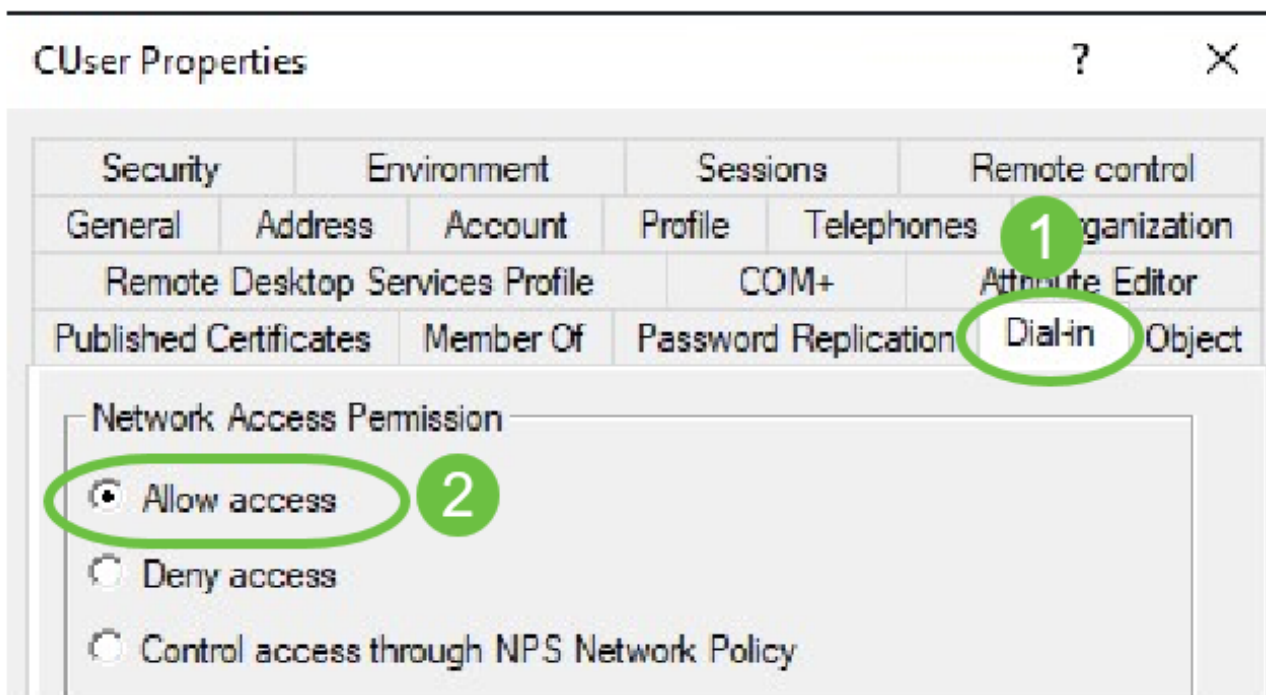
2

Add... Remove

글로벌 보안 그룹의 이름을 입력하고 이름 **확인**을 선택합니다. 항목에 밑줄이 그어져 있으면 **확인**을 클릭합니다.



전화 접속 탭을 선택합니다. Network Access Permission(네트워크 액세스 권한) 섹션에서 Allow Access(액세스 허용)를 선택하고 나머지는 기본값으로 둡니다.

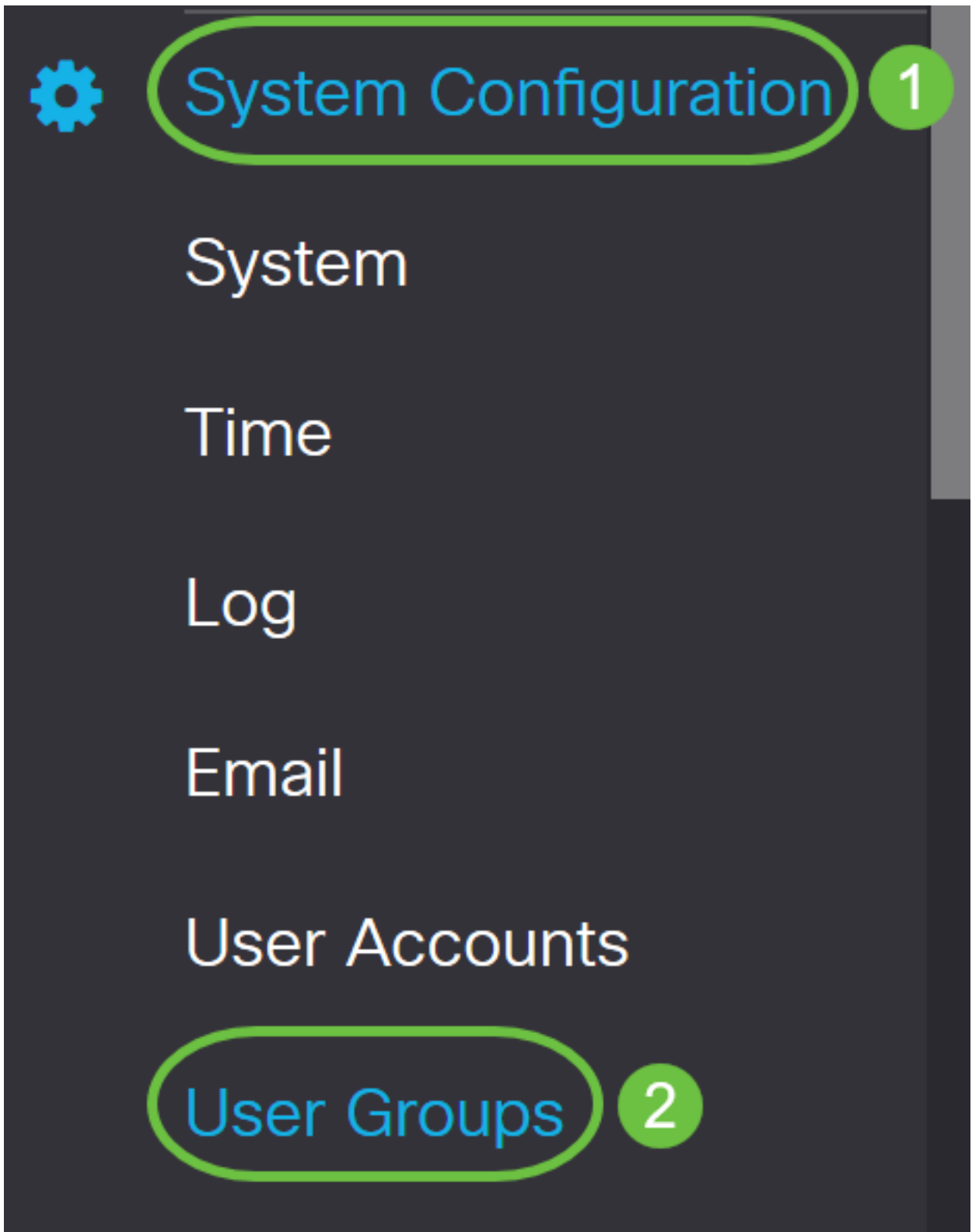


## Active Directory 통합

Active Directory를 사용하려면 RV34x 라우터의 시간이 AD 서버의 시간과 일치해야 합니다. RV34x 시리즈 라우터에서 시간 설정을 구성하는 방법에 대한 단계를 보려면 [여기](#)를 클릭하십시오.

또한 AD는 RV340에 AD Global Security Group과 일치하는 사용자 그룹이 있어야 합니다.

1단계. System Configuration(시스템 컨피그레이션) > User Groups(사용자 그룹)로 이동합니다.



2단계. 더하기 아이콘을 클릭하여 사용자 그룹을 추가합니다.

# User Groups

## User Groups Table



3단계. 그룹 이름을 입력합니다. 이 예에서는 VPNUsers입니다.

Group Name:

그룹 이름은 AD 글로벌 보안 그룹과 정확히 같아야 합니다.

4단계. 서비스에서 Web Login/NETCONF/RESTCONF는 Disabled로 표시되어야 합니다. AD 통합이 즉시 작동하지 않으면 RV34x에 액세스할 수 있습니다.

## Services

Web Login/NETCONF/RESTCONF  Disabled  Read Only  Administrator

5단계. AD 통합을 사용하여 사용자를 로그인하는 VPN 터널을 추가할 수 있습니다.

1. 이미 구성된 Client-to-Site VPN을 추가하려면 EZVPN/3rd Party(EZVPN/타사) 섹션으로 이동하여 더하기 아이콘을 클릭합니다. 드롭다운 메뉴에서 VPN 프로필을 선택하고 Add(추가)를 클릭합니다.

## 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 - SSL VPN 터널을 사용할 경우 Select a Profile(프로필 선택) 옆의 드롭다운 메뉴에서 정책을 선택합니다.

SSL VPN

Select a Profile

SSLVPNDefaultPolicy ▾

6. PPTP/L2TP/802.1x - AD를 사용하도록 허용하려면 Permit(허용) 옆의 확인란을 클릭하면 됩니다.

PPTP VPN



Permit

L2TP



Permit

802.1x




Permit



6단계. 적용을 클릭하여 변경 사항을 저장합니다.

## 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 통합 설정

1단계. System Configuration(시스템 컨피그레이션) > User Accounts(사용자 계정)로 이동합니다.



## System Configuration

System

1

Time

Log

Email

User Accounts

2

2단계. Remote Authentication Service Table(원격 인증 서비스 테이블)에서 Add(추가)를 클릭하여 항목을 생성합니다.

# Remote Authentication Service Table



Enable ⇅

Name ⇅

3단계. *Name* 필드에서 계정에 대한 사용자 이름을 생성합니다. 이 예에서는 **Jorah\_Admin**이 사용됩니다.

## Add/Edit New Domain

Name

Jorah\_Admin

4단계. *Authentication Type*(인증 유형) 드롭다운 메뉴에서 **Active Directory**를 선택합니다. AD는 네트워크의 모든 요소에 광범위한 정책을 할당하고, 여러 컴퓨터에 프로그램을 배포하고, 조직 전체에 중요한 업데이트를 적용하는 데 사용됩니다.

Authentication Type

Active Directory

AD Domain Name

RADIUS

Active Directory

Primary Server

LDAP

5단계. *AD Domain Name*(AD 도메인 이름) 필드에 AD의 정규화된 도메인 이름을 입력합니다.



이 예에서는 **sampledomain.com**이 사용됩니다.

AD Domain Name

6단계. Primary Server(기본 서버) 필드에 AD의 주소를 입력합니다.

이 예에서는 **192.168.2.122**가 사용됩니다.

Primary Server  Port

7단계. Port 필드에 기본 서버의 포트 번호를 입력합니다.

이 예에서 **1234**는 포트 번호로 사용됩니다.

Primary Server  Port

8단계. (선택 사항) User Container Path 필드에 사용자가 포함된 루트 경로를 입력합니다.

**참고:**이 예에서는 **file:Documents/manage/containers**가 사용됩니다.

User Container Path

9단계. **적용**을 클릭합니다.

User Accounts Apply

Add/Edit New Domain

Name

Authentication Type

AD Domain Name

Primary Server  Port

User Container Path

10단계. 아래로 스크롤하여 **서비스 인증 시퀀스**로 이동하여 다양한 옵션에 대한 로그인 방법을 설정합니다.

- 웹 로그인/NETCONF/RESTCONF - RV34x 라우터에 로그인하는 방법입니다. Use Default(기본값 사용) 확인란의 선택을 취소하고 Primary(기본) 메서드를 **Local DB(로컬 DB)**로 설정합니다. 이렇게 하면 Active Directory 통합이 실패하는 경우에도 라우터에서 로그아웃되지 않습니다.
- Site-to-Site/EzVPN 및 타사 Client-to-Site VPN - AD를 사용하도록 Client-to-Site VPN 터널을 설정합니다. Use Default(기본값 사용) 확인란의 선택을 취소하고 Primary(기본) 방법을 **Active Directory**로, Secondary Method(보조 방법)를 **Local DB**로 설정합니다.

## 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"/>	Local DB	None
Site-to-site/EzVPN&3rd Party Client-to-site VPN	<input type="checkbox"/>	Active Directory	Local DB
AnyConnect SSL VPN	<input type="checkbox"/>	Active Directory	Local DB

11단계. 적용을 클릭합니다.

## 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

12단계. 실행 중인 컨피그레이션을 시작 컨피그레이션에 저장합니다.

이제 RV34x Series 라우터에서 Active Directory 설정을 구성했습니다.

## LDAP

1단계. Remote Authentication Service Table(원격 인증 서비스 테이블)에서 Add(추가)를 클릭하여 항목을 생성합니다.

# Remote Authentication Service Table



Enable ⇅      Name ⇅

2단계. 이름 필드에서 계정의 사용자 이름을 생성합니다.

LDAP에서 단일 원격 사용자 계정만 구성할 수 있습니다.

이 예에서는 Any\_Admin이 사용됩니다.

Name	<input type="text" value="Dany_Admin"/>
------	---

3단계. Authentication Type(인증 유형) 드롭다운 메뉴에서 **LDAP**를 선택합니다.LDS(Lightweight Directory Access Protocol)는 디렉토리 서비스에 액세스하는 데 사용되는 액세스 프로토콜입니다.도메인 인증을 수행하기 위해 디렉토리 서버를 실행하는 원격 서버입니다.

Authentication Type	<input type="text" value="LDAP"/>
Primary Server	<input type="text" value="RADIUS"/>
Base DN	<input type="text" value="Active Directory"/>
	<input type="text" value="LDAP"/>

4단계. Primary Server(기본 서버) 필드에 LDAP의 서버 주소를 입력합니다.

이 예에서는 192.168.7.122가 사용됩니다.

Primary Server	192.168.7.122	Port	122
----------------	---------------	------	-----

5단계. *Port* 필드에 기본 서버의 포트 번호를 입력합니다.

이 예에서 **122**는 포트 번호로 사용됩니다.

Primary Server	192.168.7.122	Port	122
----------------	---------------	------	-----

6단계. *Base DN* 필드에 LDAP 서버의 기본 DN을 입력합니다. 기본 DN은 LDAP 서버가 권한 부여 요청을 받을 때 사용자를 검색하는 위치입니다. 이 필드는 LDAP 서버에 구성된 기본 DN과 일치해야 합니다.

이 예에서는 **Dept101**이 사용됩니다.

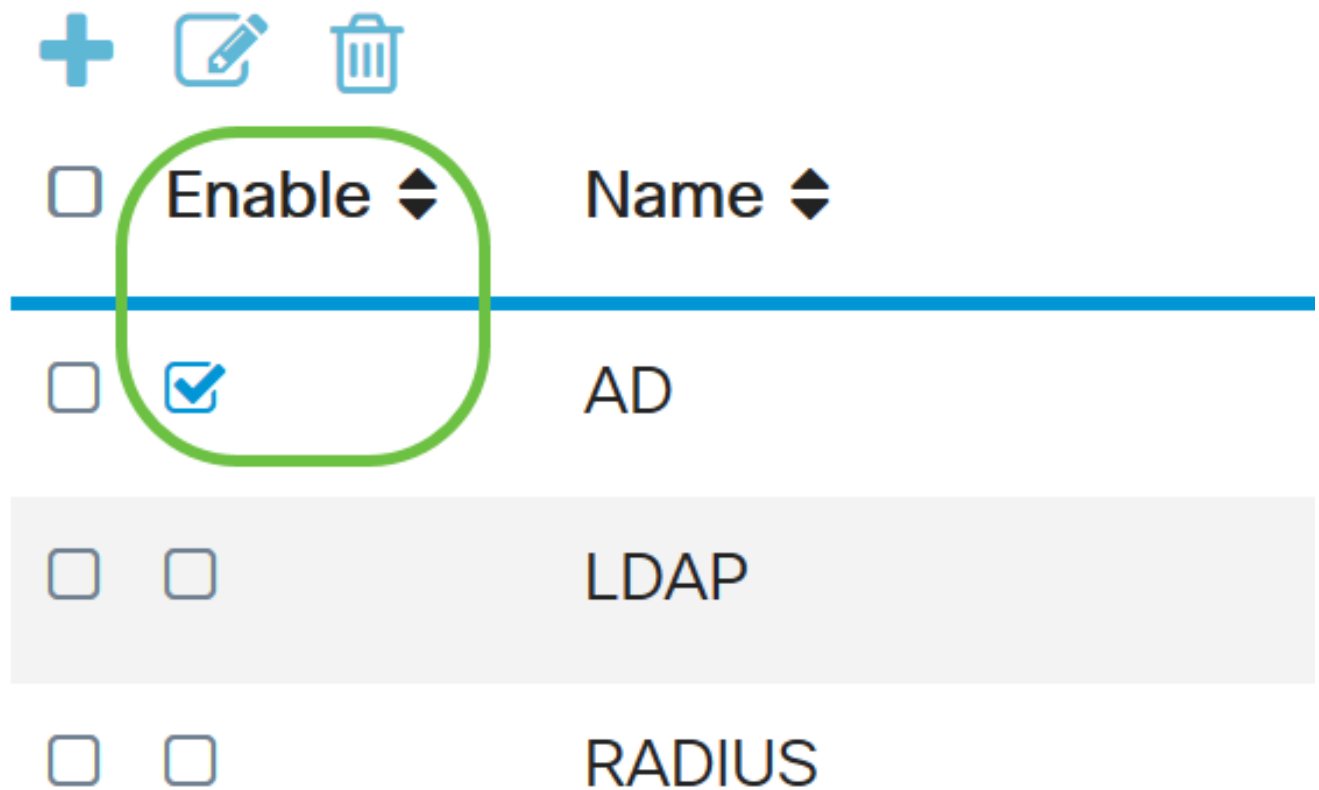
Base DN	Dept101
---------	---------

7단계. 적용을 **클릭**합니다. 원격 인증 서비스 테이블로 이동합니다.

User Accounts		Apply
Add/Edit New Domain		
Name	Dept_Admins	
Authentication Type	LDAP	
Primary Server	192.168.7.122	Port 122
Base DN	Dept101	

8단계. (선택 사항) 원격 인증 서비스를 활성화 또는 비활성화하려면 활성화 또는 비활성화할 서비스 옆의 확인란을 선택 또는 선택 취소합니다.

# Remote Authentication Service Table



The image shows a table with three rows. At the top left, there are three icons: a plus sign, a pencil, and a trash can. The first row has a header with a checkbox, the text 'Enable' with a dropdown arrow, and the text 'Name' with a dropdown arrow. A green circle highlights the 'Enable' text and the checkbox below it. The second row has a checkbox, a checked checkbox, and the text 'AD'. The third row has a checkbox, an unchecked checkbox, and the text 'LDAP'. The fourth row has a checkbox, an unchecked checkbox, and the text 'RADIUS'. A blue horizontal line is positioned between the first and second rows.

<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

9단계. 적용을 클릭합니다.

User Accounts

Apply

이제 RV34x Series 라우터에서 LDAP를 성공적으로 구성했습니다.

**이 문서와 관련된 비디오 보기...**

[여기를 클릭하여 Cisco의 다른 기술 대화를 확인하십시오.](#)