

# 在RV34x系列路由器上配置和管理用户帐户

## 目标

本文旨在向您展示如何配置和管理RV34x系列路由器上的本地和远程用户帐户。这包括如何配置本地用户密码复杂性、配置/编辑/导入本地用户、使用RADIUS、Active Directory和LDAP配置远程身份验证服务。

## 适用设备 | 固件版本

- RV34x系列 | 1.0.01.16(下载[最新版](#))

## 简介

RV34x系列路由器提供用户帐户，以便查看和管理设置。用户可以来自不同的组或属于共享身份验证域、局域网(LAN)和服务访问规则以及空闲超时设置的安全套接字层(SSL)虚拟专用网络(VPN)的逻辑组。用户管理定义了哪种类型的用户可以使用特定类型的设施，以及如何实现。

外部数据库优先级始终为远程身份验证拨入用户服务(RADIUS)/轻量目录访问协议(LDAP)/Active Directory(AD)/本地。如果在路由器上添加RADIUS服务器，Web登录服务和其他服务将使用RADIUS外部数据库对用户进行身份验证。

没有为Web登录服务单独启用外部数据库并为其他服务配置其他数据库的选项。在路由器上创建并启用RADIUS后，路由器将使用RADIUS服务作为外部数据库进行Web登录、站点到站点VPN、EzVPN/第三方VPN、SSL VPN、点对点传输协议(PPTP)/第2层传输协议(L2TP)VPN、和802.1x。

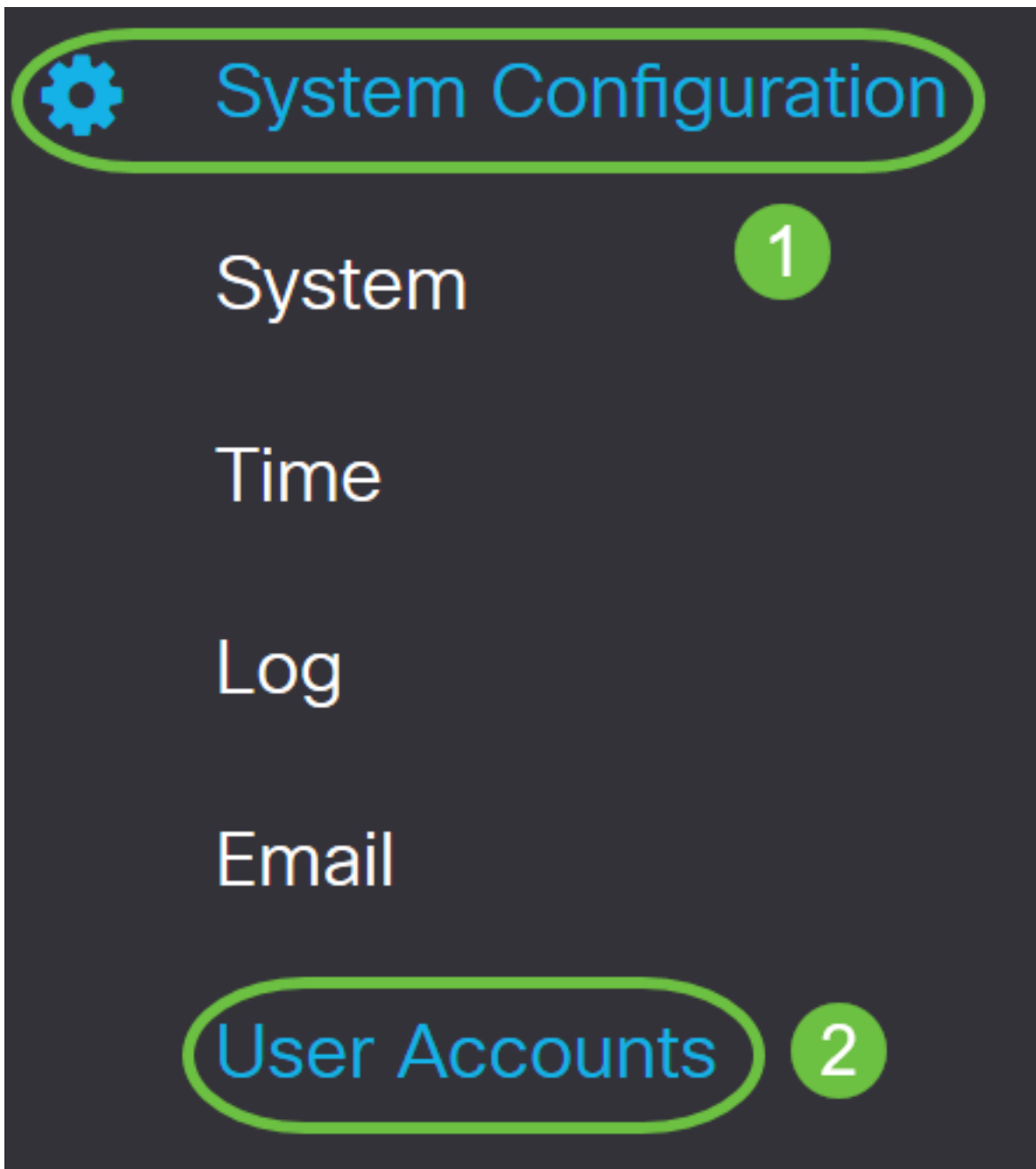
## 目录

- [配置本地用户帐户](#)
- [本地用户密码复杂性](#)
- [配置本地用户](#)
- [编辑本地用户](#)
- [导入本地用户](#)
- [配置远程身份验证服务](#)
- [RADIUS](#)
- [Active Directory配置](#)
- [Active Directory集成](#)
- [Active Directory集成设置](#)
- [LDAP](#)

## 配置本地用户帐户

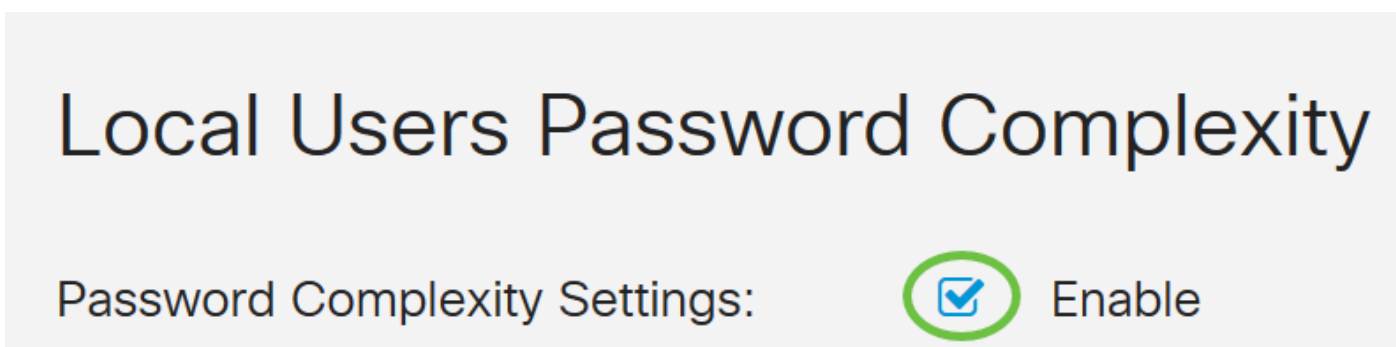
### 本地用户密码复杂性

步骤1.登录到路由器的基于Web的实用程序，然后选择System Configuration > User Accounts。



步骤2.选中Enable Password Complexity Settings复选框以启用密码复杂性参数。

如果未选中此复选框，请跳至[配置本地用户](#)。



步骤3.在“最小密码长度”字段中，输入一个介于0和127之间的数字，以设置密码必须包含的最小字符数。默认值为8。

在本例中，最小字符数设置为10。

# Local Users Password Complexity

Password Complexity Settings:  Enable

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

步骤4.在“最小字符类数”字段中，输入0到4之间的数字以设置类。输入的数字表示不同类的最小或最大字符数：

- 密码由大写字符(ABCD)组成。
- 密码由小写字符(abcd)组成。
- 密码由数字字符(1234)组成。
- 密码由特殊字符(!@#\$)组成。

在本例中，使用4。

## 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(!@#\$...).

步骤5.选中Enable复选框，新密码必须与当前密码不同。

## 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

步骤6.在“密码老化时间”字段中，输入密码到期的天数(0 - 365)。在本例中，已输入180天。

## 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)

您现在已成功配置路由器上的本地用户密码复杂性设置。

### 配置本地用户

步骤1.在Local User Membership List表中，单击**Add**以创建新用户帐户。您将进入“添加用户帐户”页面。

# 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

在“添加用户帐户”标题下，将显示在“本地密码复杂性”步骤下定义参数。

# 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

步骤2.在“用户名”字段中，输入帐户的用户名。


在本例中，使用Administrator\_Noah。

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"/>	

步骤3.在New Password字段中，输入带有已定义参数的密码。在本例中，最小密码长度必须由10个字符组成，并结合大小写、小写、数字和特殊字符。

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"/>	

步骤4.在“新密码确认”字段中，重新输入要确认的密码。如果密码不匹配，将显示字段旁边的文本。

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"/>	▼


密码强度计会根据密码的强度而改变。



步骤5.从组下拉列表中，选择要向用户帐户分配权限的组。选项有：

- admin — 读写权限。
- guest — 只读权限。

在本例中，选择admin。

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"/>	

步骤6.单击“应用”。

## 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"/>	▼

您现在已成功配置RV34x系列路由器上的本地用户成员资格。

## 编辑本地用户

步骤1.选中Local User Membership List表中本地用户用户名旁的复选框。

在本例中，选择Administrator\_Noah。



# 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

步骤2. 单击“编辑”。

# 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

无法编辑用户名。

步骤3.在“旧密码”字段中，输入之前为本地用户帐户配置的密码。

## Edit User Account

User Name

Administrator\_Noah

Old Password

●●●●●●●●

步骤4.在“新密码”字段中，输入新密码。新密码必须满足最低要求。

## Edit User Account

User Name

Old Password

New Password

( Range: 0 - 127 )

步骤5.在New Password Confirm字段中再次输入新密码以进行确认。这些密码必须匹配。

## Edit User Account

User Name

Old Password

New Password

( Range: 0 - 127 )

New Password Confirm

第6步。(可选)从Group下拉列表中,选择要向用户帐户分配权限的组。

在本例中,选择访客。

## Edit User Account

User Name

Old Password

New Password

( Range: 0 - 127 )

New Password Confirm

Group

admin

guest

步骤7.单击“应用”。

User Accounts

### Edit User Account

User Name	<input type="text" value="Administrator_Noah"/>	
Old Password	<input type="password" value="●●●●●●"/>	
New Password	<input type="password" value="●●●●●●"/>	( Range: 0 - 127 )
New Password Confirm	<input type="password" value="●●●●●●"/>	
Group	<input type="text" value="guest"/>	▼

您现在应该已成功编辑本地用户帐户。

# 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

### 导入本地用户



步骤1.在Local Users Import区域中，单击 。

步骤2.在“导入用户名和密码”下，单击“浏览.....”以导入用户列表。此文件通常是以逗号分隔值 (.CSV)格式保存的电子表格。

在本示例中，选择user-template.csv。

# Local Users Import

Import User Name & Password

Browse...

user-template.csv

(Import User Name + Password via CSV files)

Import

Download User Template:

Download

步骤3. ( 可选 ) 如果您没有模板 , 请点击Download User Template ( 下载用户模板 ) 区域中的Download ( 下载 ) 。

# Local Users Import

Import User Name & Password

Browse...

user-template.csv

(Import User Name + Password via CSV files)

Import

Download User Template:

Download

步骤4.单击Import。

# Local Users Import

Import User Name & Password

Browse...

user-template.csv

(Import User Name + Password via CSV files)

Import

Download User Template:

Download

导入按钮旁边将显示一条消息，表明导入成功。

您现在已成功导入本地用户列表。

## 配置远程身份验证服务

### RADIUS

步骤1.在远程身份验证服务表中，单击**添加**以创建条目。



# Remote Authentication Service Table



Enable  Name 

步骤2.在Name字段中，为帐户创建用户名。

在本例中，使用**管理员**。

## Add/Edit New Domain

Name

Administrator

步骤3.从Authentication Type下拉菜单中，选择**Radius**。这意味着用户身份验证将通过RADIUS服务器进行。

只能配置RADIUS下的单个远程用户帐户。

Authentication Type

RADIUS



**RADIUS**

Active Directory

LDAP

Primary Server

Backup Server

步骤4.在Primary Server字段中，输入主RADIUS服务器的IP地址。

在本例中，**192.168.3.122**用作主服务器。

Primary Server  Port

步骤5.在Port字段中，输入主RADIUS服务器的端口号。

在本例中，1645用作端口号。

Primary Server  Port

步骤6.在“备份服务器”字段中，输入备份RADIUS服务器的IP地址。当主服务器发生故障时，这将用作故障切换。

在本例中，备份服务器地址为192.168.4.122。

Backup Server  Port

步骤7.在Port字段中，输入备份RADIUS服务器的数量。

Backup Server  Port

在本例中，1646用作端口号。

步骤8.在预共享密钥字段中，输入在RADIUS服务器上配置的预共享密钥。

Pre-shared Key

步骤9.在确认预共享密钥字段中，重新输入预共享密钥进行确认。

Confirm Pre-shared Key

步骤10.单击“应用”。

## 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="●●●●●●●●"/>		

您将进入主用户帐户页面。最近配置的帐户现在显示在远程身份验证服务表中。

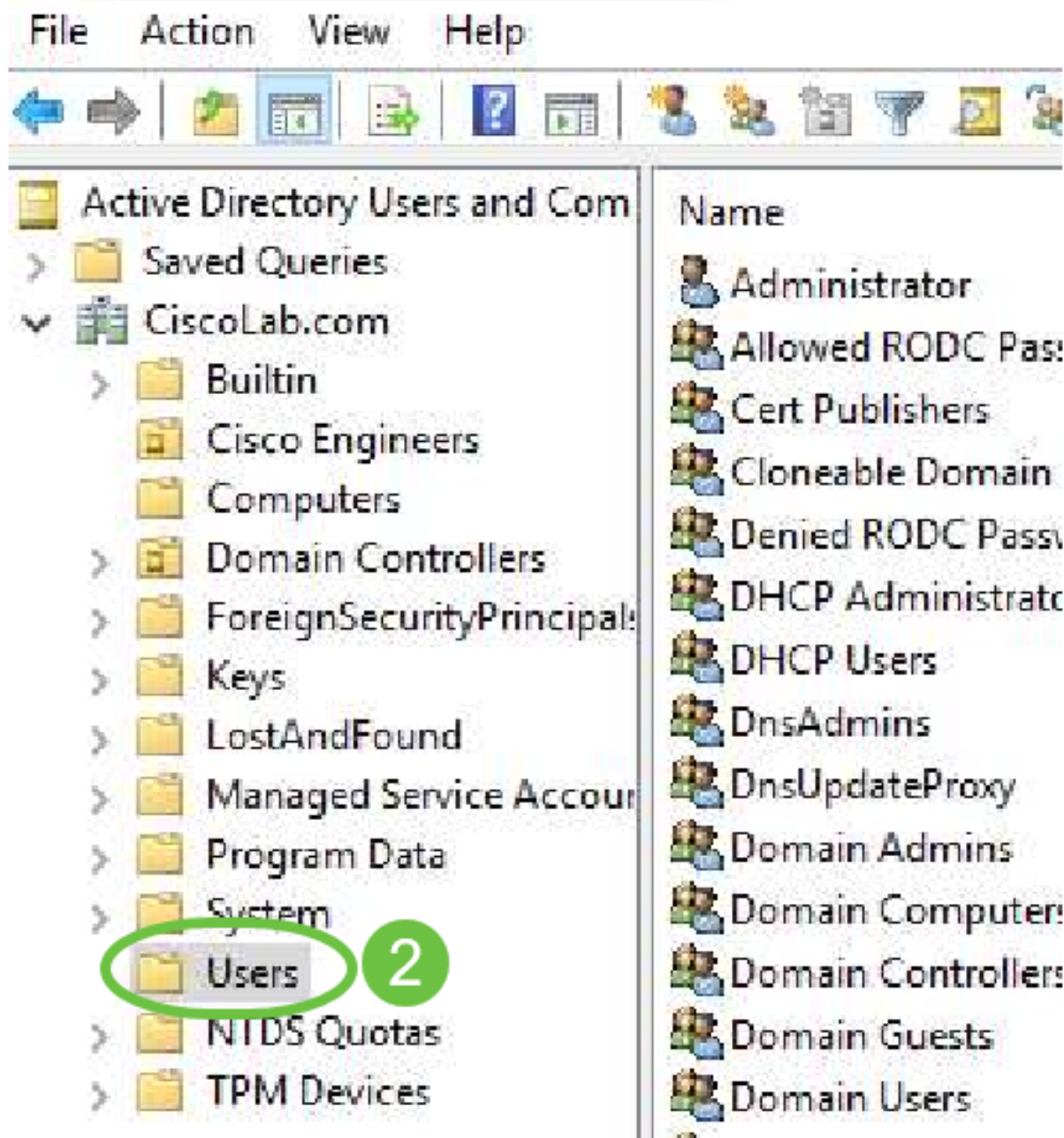
您现在已成功在RV34x系列路由器上配置RADIUS身份验证。

## Active Directory配置

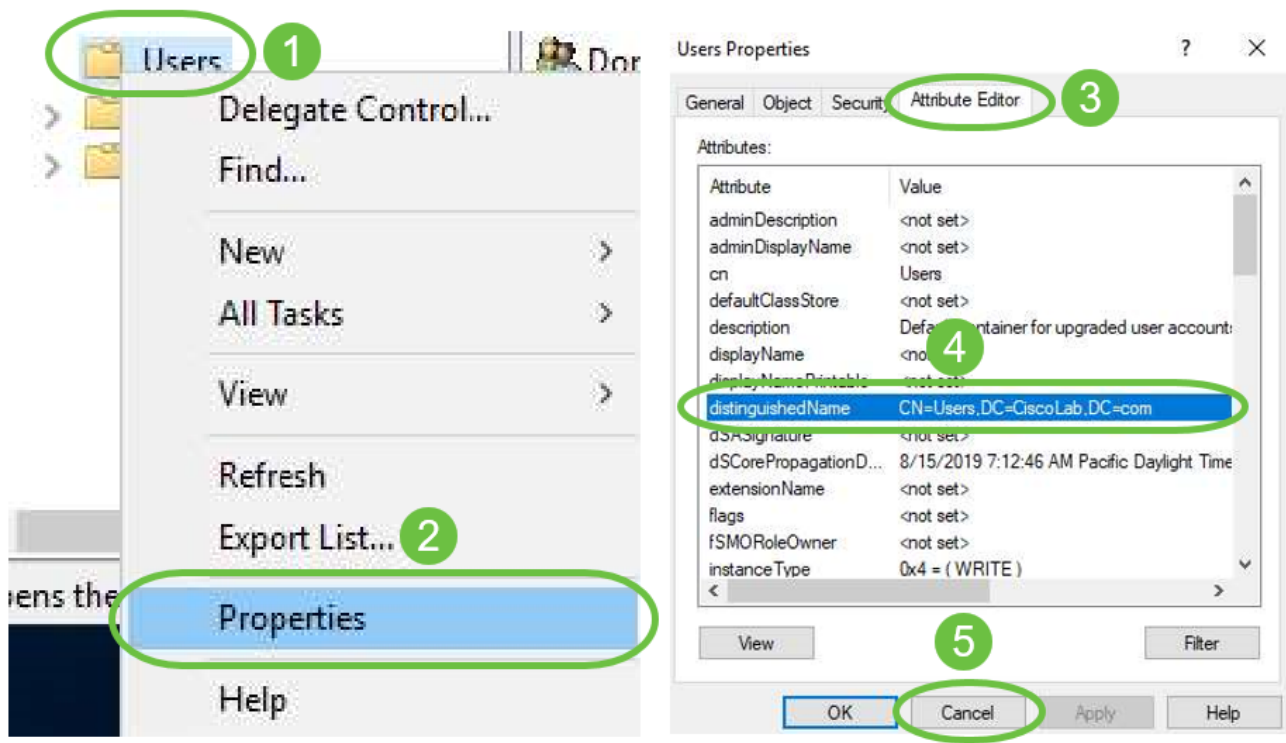
步骤1.要完成Active Directory配置，您需要登录到Active Directory服务器。在PC上，打开**Active Directory用户和计算机**，并导航至将具有用于远程登录的用户帐户的容器。在本例中，我们将使用“用户”容器。

# Active Directory Users and Computers

1



步骤2. 右键单击容器并选择属性。导航至“属性编辑器”选项卡并查找可分辨名称字段。如果此选项卡不可见，则需要先在Active Directory用户和计算机中启用高级功能视图并重新开始。记下此字段，然后单击“取消”。这是用户容器路径。配置RV340时也需要此字段，且必须完全匹配。



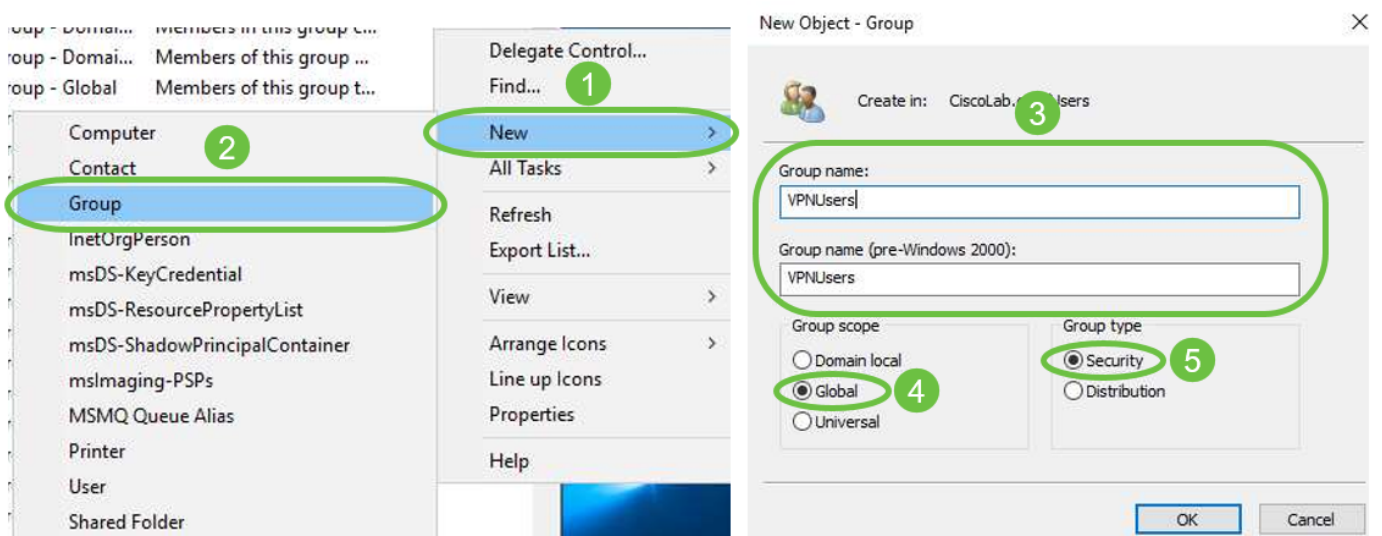
步骤3.在将要使用的用户帐户所在的容器中创建全局安全组。

在选定的容器中，右键单击空白区域并选择“新建”>“组”。

请依次选择以下选项：

- 组名 — 此名称必须与在RV340上创建的用户组名称完全匹配。在本例中，我们将使用 **VPNUsers**。
- 组范围 — 全球
- 组类型 — 安全

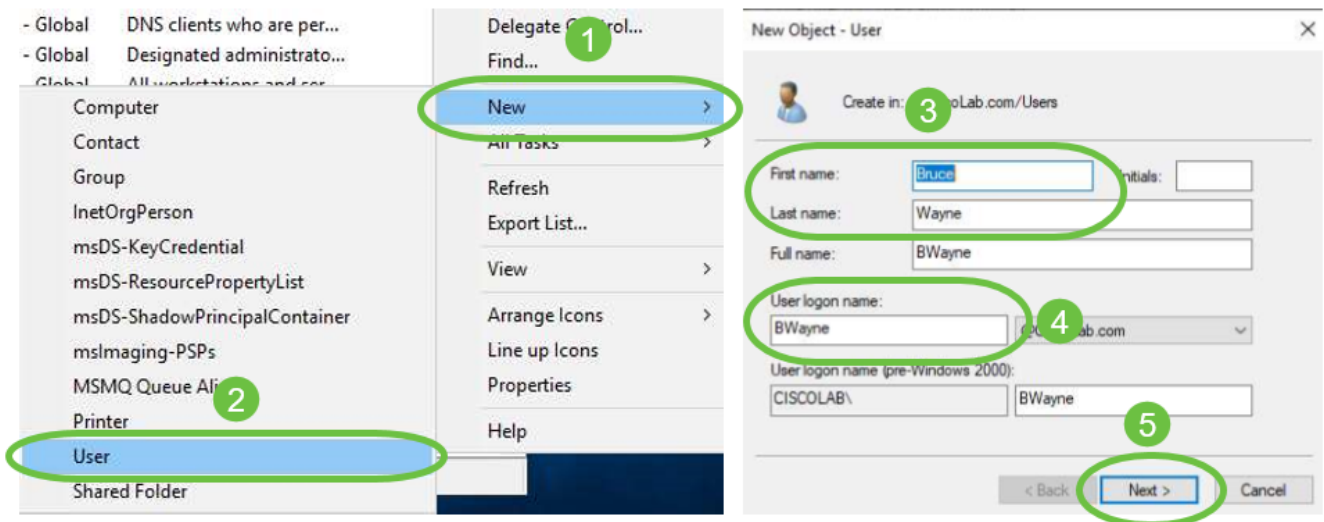
Click OK.



步骤4.要创建新用户帐户，请执行以下操作：

- 右键单击容器中的空格，然后选择“新建”>“用户”。

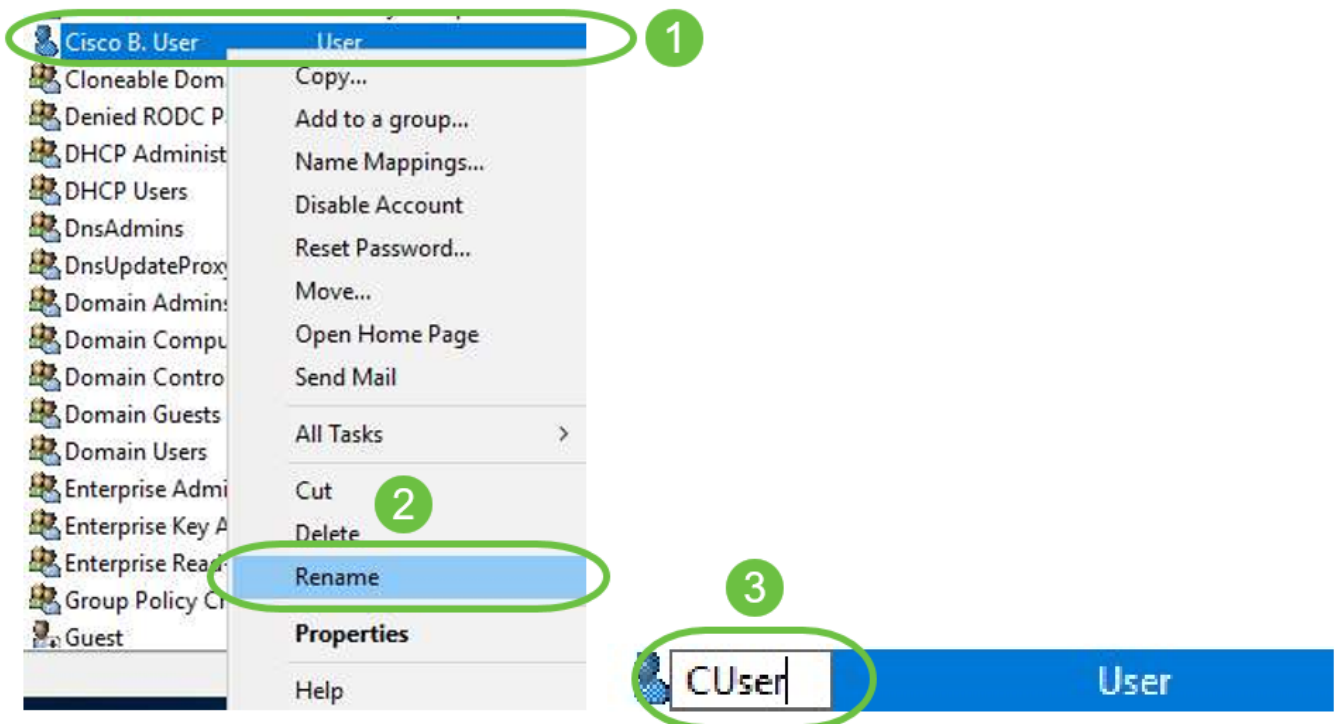
- 输入名字,姓氏。
- 输入用户登录名。
- 单击 **Next**。



系统将提示您输入用户的密码。如果选中 *User must change password at next logon* 框，则用户必须在本地登录并更改密码BEFORE远程登录。

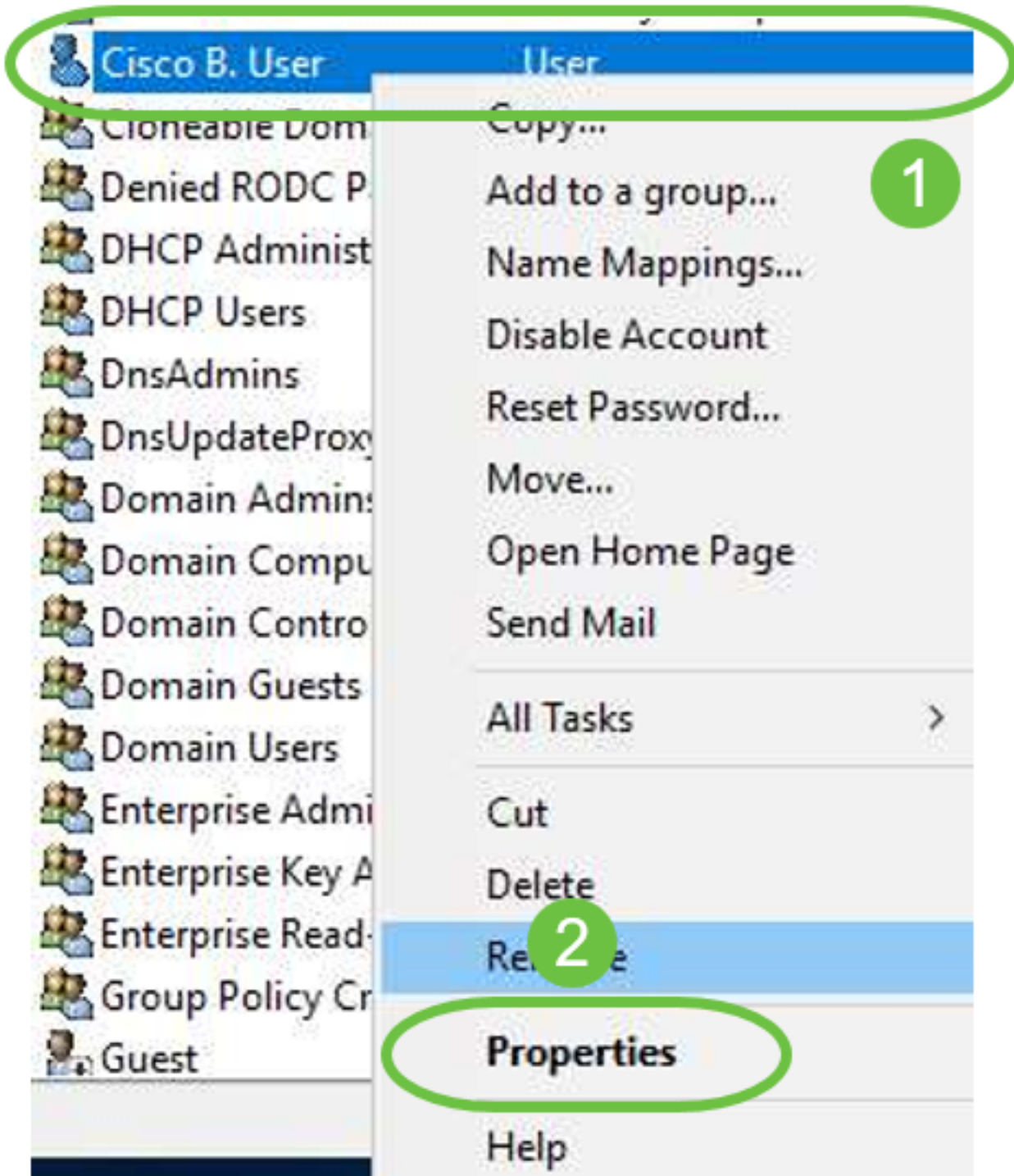
单击 **完成**。

如果已创建需要使用的用户帐户，则可能需要进行调整。要调整用户的规范名称，请选择用户，右键单击并选择“重命名”。确保删除所有空格，并确保其与用户的登录名匹配。这不会更改用户的显示名称。Click **OK**。

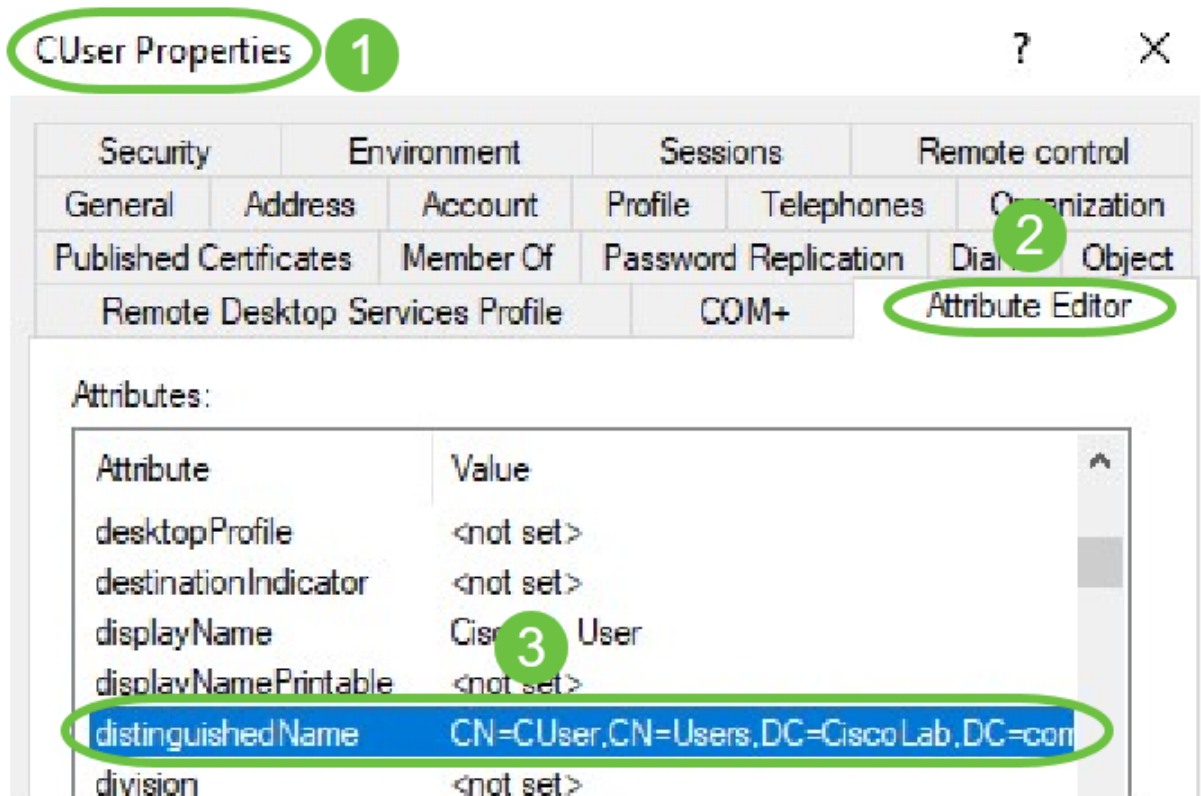


步骤5.一旦用户帐户结构正确，就需要授予其远程登录权限。

为此，请选择用户帐户，右键单击并选择“属性”。



在“用户属性”中，选择属性编辑器选项卡，并向下滚动到distinguishedName。确保第一个CN=具有正确的用户登录名，不带空格。



选择“成员”选项卡，然后单击添加。



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	

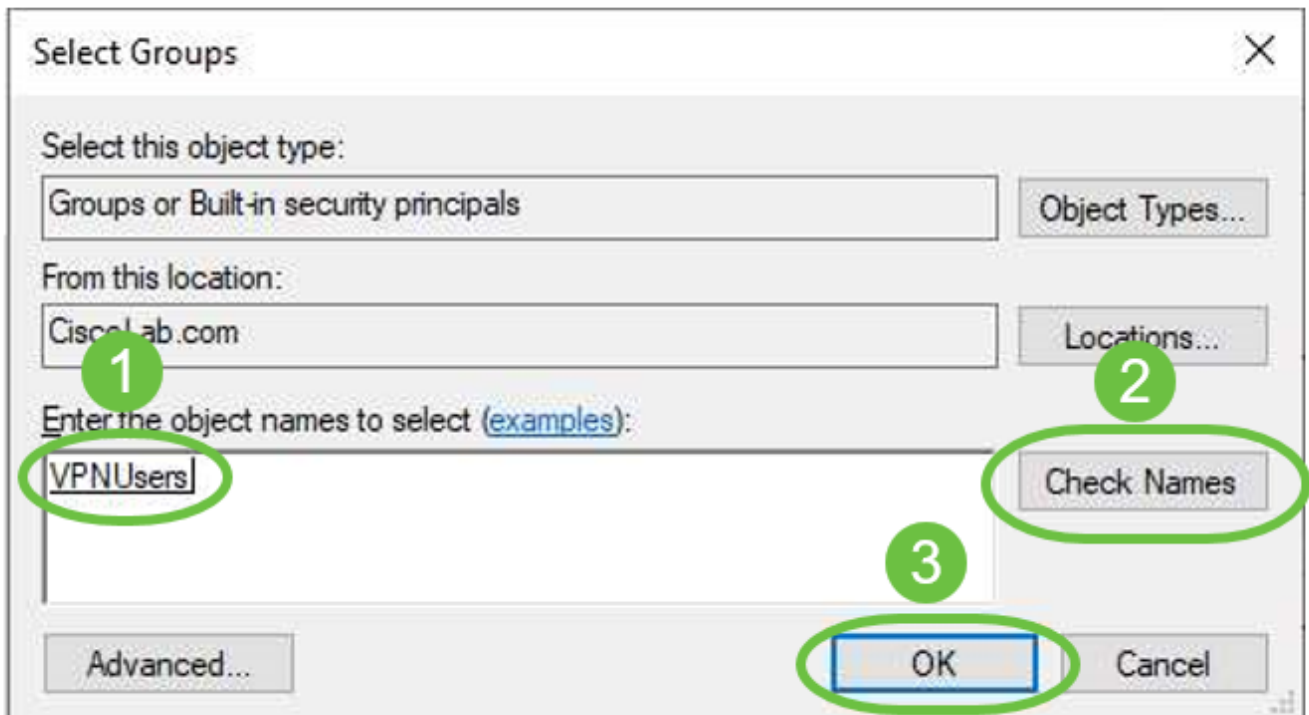
Member of:

Name	Active Directory Domain Services Folder
<u>Domain Users</u>	CiscoLab.com/Users

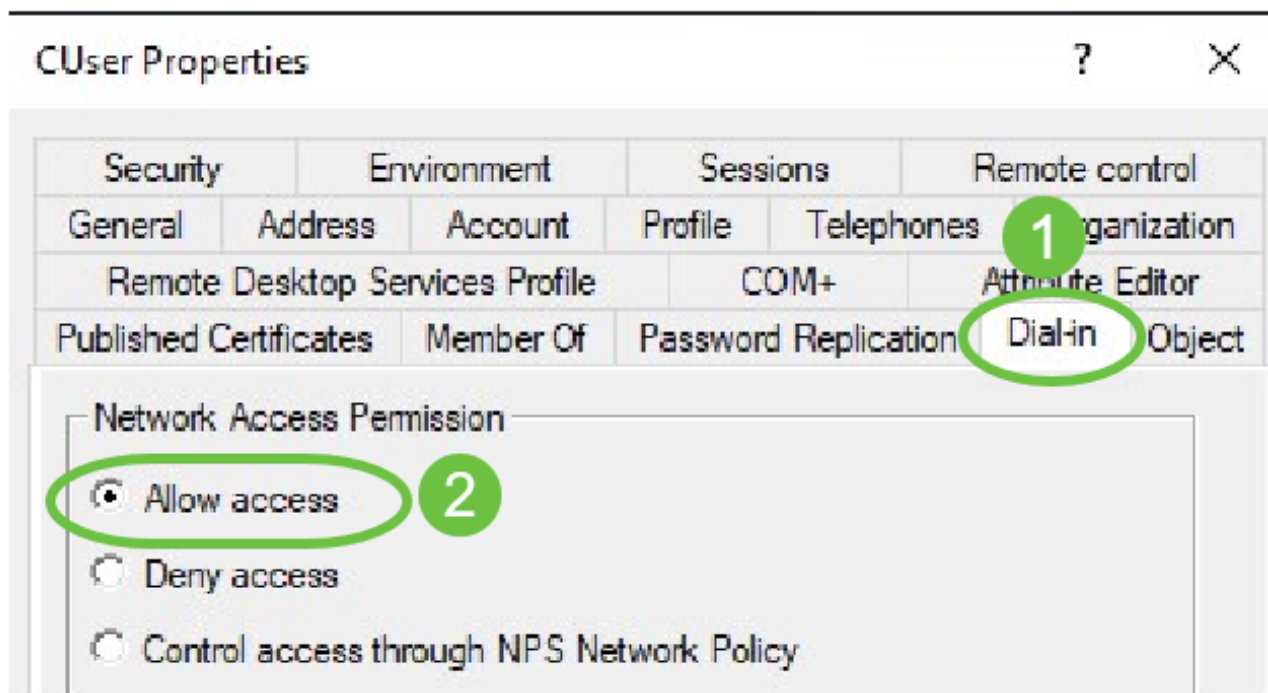
2

Add... Remove

输入全局安全组的名称，然后选择**检查名称**。如果条目带下划线，请单击**OK**。



选择“拨入”选项卡。在“网络访问权限”部分下，选择“允许访问”，将其余保留为默认值。

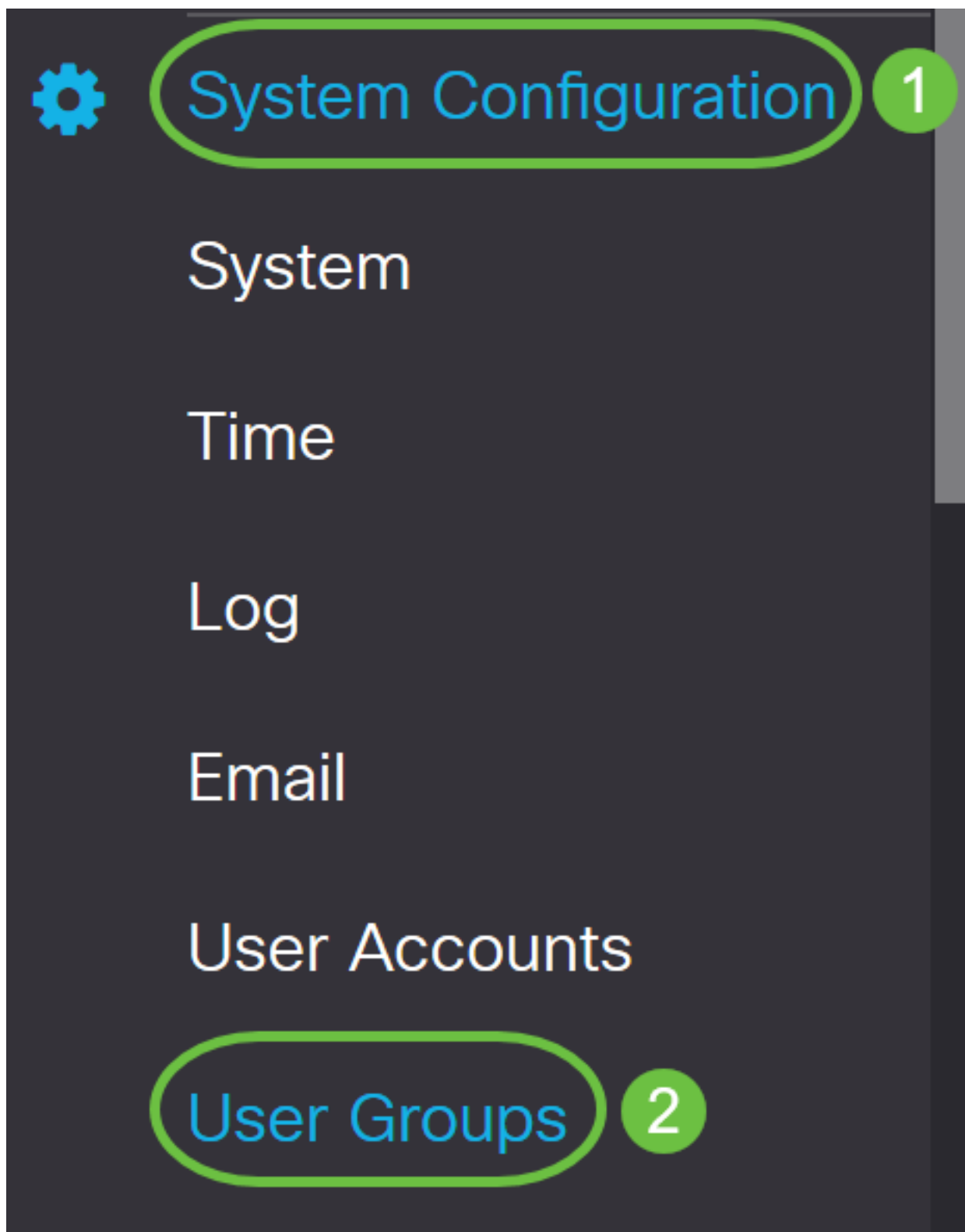


## Active Directory集成

Active Directory要求RV34x路由器的时间与AD服务器的时间匹配。有关如何在RV34x系列路由器上配置时间设置的步骤，请单击[此处](#)。

AD还要求RV340具有与AD全局安全组匹配的用户组。

步骤1. 导航至System Configuration > User Groups。



步骤2. 单击加号图标添加用户组。

# User Groups

## User Groups Table



步骤3.输入组名称。在本例中，它是VPNUsers。

Group Name:

组名称必须与AD全局安全组完全相同。

步骤4.在“服务”下，*Web Login/NETCONF/RESTCONF*应标记为“禁用”。如果AD集成不能立即运行，您仍可以访问RV34x。

## Services

Web Login/NETCONF/RESTCONF  Disabled  Read Only  Administrator

步骤5.您可以添加将使用AD集成登录其用户的VPN隧道。

1. 要添加已配置的客户端到站点VPN，请转到EZVPN/第3方部分并单击加号图标。从下拉菜单中选择VPN配置文件，然后单击Add。

## 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 — 如果将使用SSL VPN隧道，请从Select a Profile旁的下拉菜单中选择策略。

SSL VPN

Select a Profile

SSLVPNDefaultPolicy

6. PPTP/L2TP/802.1x — 要允许这些设备使用AD，只需单击它们旁边的复选框即可允许。

PPTP VPN



Permit

L2TP



Permit

802.1x



Permit

步骤6.单击“应用”保存更改。

# 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集成设置

步骤1. 导航至 System Configuration > User Accounts。



## System Configuration

System

1

Time

Log

Email

User Accounts

2

步骤2.在远程身份验证服务表中，单击**添加**以创建条目。

# Remote Authentication Service Table



Enable ⇅

Name ⇅

步骤3.在Name字段中，为帐户创建用户名。在本示例中，使用Jorah\_Admin。

## Add/Edit New Domain

Name

Jorah\_Admin

步骤4.从Authentication Type下拉菜单中，选择**Active Directory**。AD用于为网络的所有元素分配策略，将程序部署到许多计算机，并将关键更新应用到整个组织。

Authentication Type

Active Directory

AD Domain Name

RADIUS

Active Directory

Primary Server

LDAP

步骤5.在AD Domain Name字段中，输入AD的完全限定域名。

在本例中，使用sampledomain.com。



AD Domain Name

sampledomain.com

步骤6.在Primary Server字段中，输入AD的地址。

在本例中，使用192.168.2.122。

Primary Server

192.168.2.122

Port

1234

步骤7.在Port字段中，输入主服务器的端口号。

在本例中，1234用作端口号。

Primary Server

192.168.2.122

Port

1234

步骤8. ( 可选 ) 在“用户容器路径”字段中，输入包含用户的根路径。

注意：在本例中，使用file:Documents/manage/containers。

User Container Path

file:Documents/manage/co

步骤9.单击“应用”。

User Accounts

Apply

Add/Edit New Domain

Name

Jorah\_Admin

Authentication Type

Active Directory

AD Domain Name

sampledomain.com

Primary Server

192.168.2.122

Port

1234

User Container Path

file:Documents/manage/co

步骤10.向下滚动到Service Auth Sequence，以设置各种选项的登录方法。

- Web Login/NETFCNF/RESTCONF — 这是您登录RV34x路由器的方式。取消选中“使用默认值”复选框，将“主要”方法设置为“本地数据库”。这将确保即使Active Directory集成失败，您也不

会从路由器注销。

- 站点到站点/EzVPN&第三方客户端到站点VPN — 这是将客户端到站点VPN隧道设置为使用AD。取消选中“使用默认值”复选框，将“主方法”设置为“Active Directory”，将“辅助方法”设置为“本地数据库”。

## 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

步骤11.单击“应用”。

## 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

步骤12.将运行配置保存到启动配置。

您现在已成功配置RV34x系列路由器上的Active Directory设置。

## LDAP

步骤1.在远程身份验证服务表中，单击添加以创建条目。

# Remote Authentication Service Table



Enable  Name 


步骤2.在Name字段中，为帐户创建用户名。

只能配置LDAP下的单个远程用户帐户。

在本例中，使用Dany\_Admin。

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

步骤3.从Authentication Type下拉菜单中，选择LDAP。轻量级目录访问协议是用于访问目录服务的访问协议。它是运行目录服务器以执行域身份验证的远程服务器。

Authentication Type	<div style="border: 1px solid #ccc; padding: 5px;"><div style="border: 1px solid #add8e6; padding: 2px;">LDAP </div><div style="border: 1px solid #add8e6; padding: 2px;">RADIUS</div><div style="border: 1px solid #add8e6; padding: 2px;">Active Directory</div><div style="border: 1px solid #add8e6; padding: 2px; background-color: #0070c0; color: white;">LDAP</div></div>
Primary Server	
Base DN	

步骤4.在Primary Server字段中，输入LDAP的服务器地址。

在本例中，使用192.168.7.122。

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

步骤5.在Port字段中，输入主服务器的端口号。

在本例中，122用作端口号。

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

步骤6.在Base DN字段中输入LDAP服务器的基本可分辨名称。基本DN是LDAP服务器在收到授权请求时搜索用户的位置。此字段应与LDAP服务器上配置的基本DN匹配。

在本例中，使用了Dept101。

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

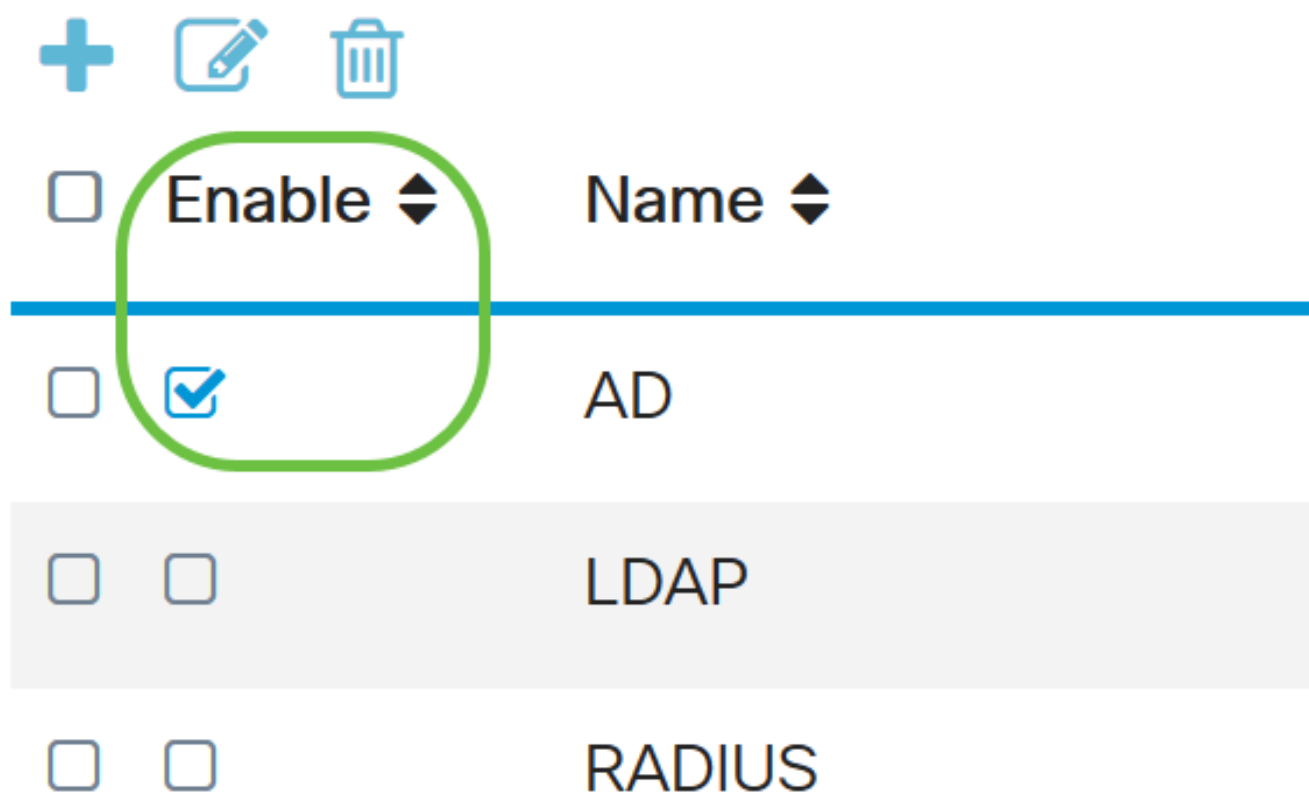
步骤7.单击“应用”。您将进入远程身份验证服务表。



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

第8步。（可选）如果要启用或禁用远程身份验证服务，请选中或取消选中要启用或禁用的服务旁边的复选框。

# Remote Authentication Service Table



The image shows a configuration table for Remote Authentication Services. At the top, there are three icons: a plus sign for adding, a pencil for editing, and a trash can for deleting. The table has a header row with a checkbox, a dropdown menu labeled 'Enable', and a dropdown menu labeled 'Name'. Below the header, there are three rows: 'AD' (with a checked checkbox), 'LDAP' (with an unchecked checkbox), and 'RADIUS' (with an unchecked checkbox). A green circle highlights the 'Enable' dropdown menu in the 'AD' row.

<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

步骤9.单击“应用”。

User Accounts

Apply

您现在已成功在RV34x系列路由器上配置LDAP。

**查看与本文相关的视频.....**

[单击此处查看思科提供的其他技术讲座](#)