

配置和管理RV34x系列路由器上的使用者帳戶

目標

本文的目的是展示如何在RV34x系列路由器上配置和管理本地和遠端使用者帳戶。這包括如何配置本地使用者的密碼複雜性、配置/編輯/匯入本地使用者、使用RADIUS、Active Directory和LDAP配置遠端身份驗證服務。

適用裝置 | 韌體版本

- RV34x系列 | 1.0.01.16(下載[最新版本](#))

簡介

RV34x系列路由器提供使用者帳戶以便檢視和管理設定。使用者可能來自不同的組，或者屬於共用身份驗證域、區域網(LAN)和服務訪問規則以及空閒超時設定的安全套接字層(SSL)虛擬專用網路(VPN)的邏輯組。使用者管理定義哪些型別的使用者可以使用特定型別的合作室以及如何使用。

外部資料庫優先順序始終為遠端身份驗證撥入使用者服務(RADIUS)/輕量級目錄訪問協定(LDAP)/Active Directory(AD)/本地。如果在路由器上新增RADIUS伺服器，Web登入服務和其他服務將使用RADIUS外部資料庫驗證使用者。

沒有選項可以單獨為Web登入服務啟用外部資料庫並為其他服務配置另一個資料庫。在路由器上建立並啟用RADIUS後，路由器將使用RADIUS服務作為外部資料庫進行網路登入、站點到站點VPN、EzVPN/第三方VPN、SSL VPN、點對點傳輸協定(PPTP)/第2層傳輸協定(L2TP)VPN和802.1x。

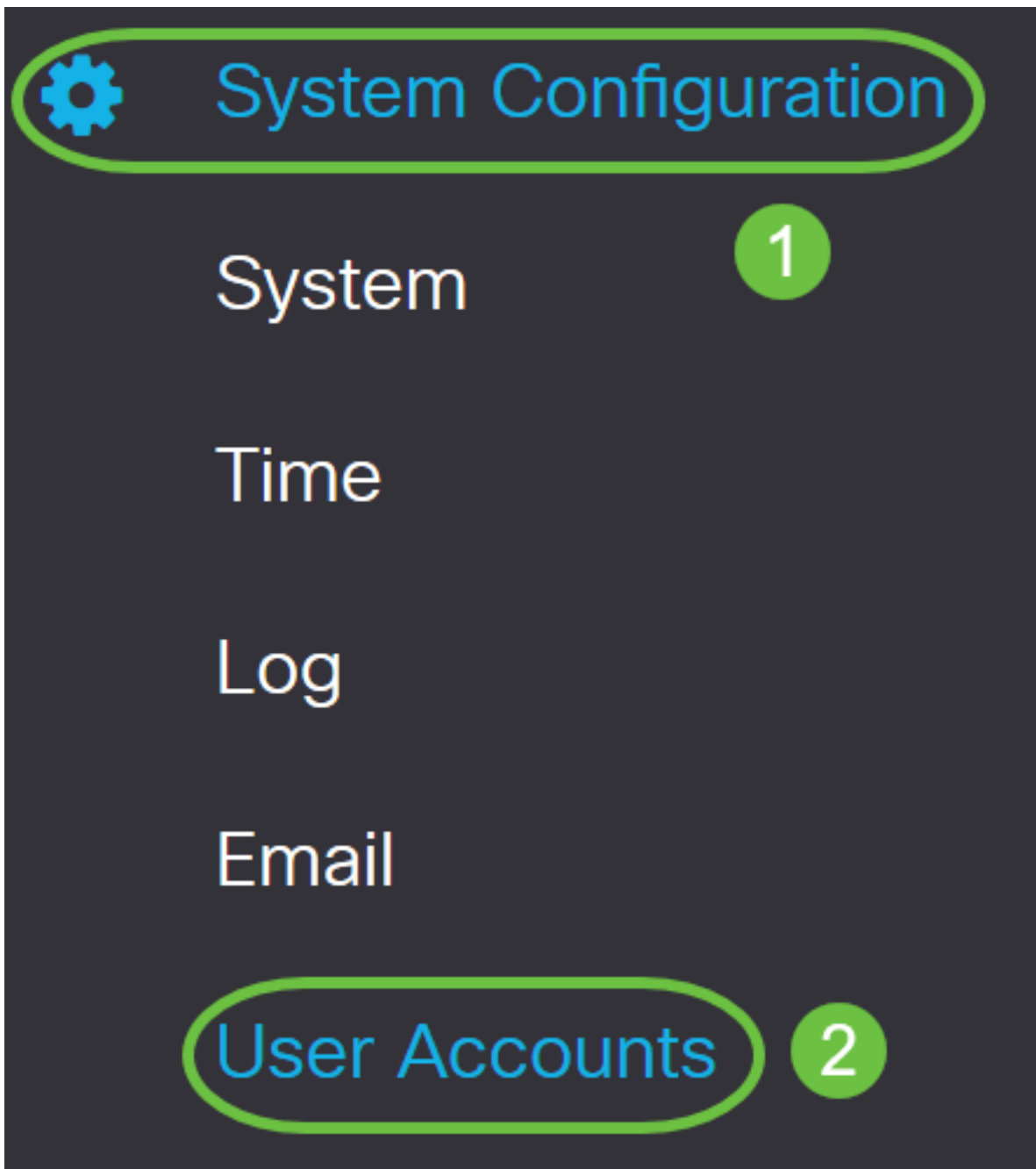
目錄

- [配置本地使用者帳戶](#)
- [本地使用者密碼複雜性](#)
- [配置本地使用者](#)
- [編輯本地使用者](#)
- [匯入本地使用者](#)
- [配置遠端身份驗證服務](#)
- [RADIUS](#)
- [Active Directory配置](#)
- [Active Directory整合](#)
- [Active Directory整合設定](#)
- [LDAP](#)

配置本地使用者帳戶

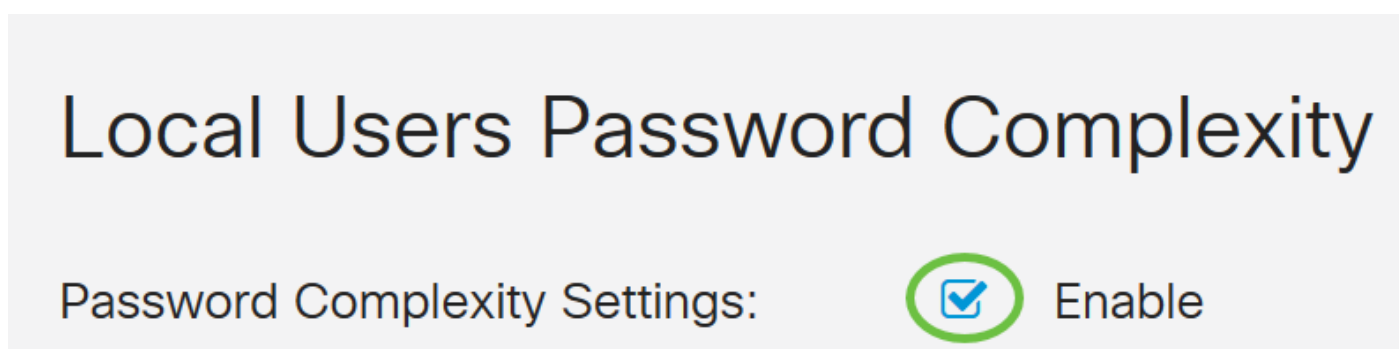
本地使用者密碼複雜性

步驟1.登入到路由器的基於Web的實用程式，然後選擇System Configuration > User Accounts。



步驟2.選中Enable Password Complexity Settings覈取方塊以啟用密碼複雜性引數。

如果未選中此覈取方塊，請跳至[配置本地使用者](#)。



步驟3.在**最小密碼長度**欄位中，輸入範圍從0到127的數字，以設定密碼必須包含的最小字元數。預設值為8。

在本示例中，最小字元數設定為10。

Local Users Password Complexity

Password Complexity Settings: Enable

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

步驟4.在「最小字元類數」字段中，輸入0到4之間的數字以設定類。輸入的數字表示不同類別的最小或最大字元數：

- 密碼由大寫字元(ABCD)組成。
- 密碼由小寫字元(abcd)組成。
- 密碼由數字字元(1234)組成。
- 密碼由特殊字元(!@#\$)組成。

在此範例中，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(!@#\$...).

步驟5.選中**Enable**竅取方塊，新密碼必須不同於當前密碼。

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

步驟6.在 *Password Aging Time* 欄位中，輸入密碼到期的天數(0 - 365)。在此示例中，已輸入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)

現在，您已成功在路由器上配置本地使用者密碼複雜性設定。

配置本地使用者

步驟1.在「本地使用者成員資格清單」(Local User Membership List)表格中，按一下**Add**建立新的使用者帳戶。您將進入「新增使用者帳戶」頁。

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 *Add User Account* 標題下，顯示 Local Password Complexity 步驟下定義的引數。

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

步驟2. 在 *User Name* 欄位中輸入帳戶的使用者名稱。

在本示例中，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"/>	

步驟3. 在 *New Password* 欄位中，輸入具有已定義引數的密碼。在本例中，最小密碼長度必須由 10 個字元組成，並包括大寫字母、小寫字母、數字和特殊字元。

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"/>	

步驟4. 在 *New Password Confirm* 欄位中，重新輸入密碼以進行確認。如果密碼不匹配，欄位旁將顯

示文本。

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	<div><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"/>	▼

密碼強度計根據密碼強度而變化。



步驟5.從Group下拉選單中選擇一個組，以向使用者帳戶分配許可權。選項包括：

- admin — 讀寫許可權。
- guest — 只讀許可權。

在本例中，選擇了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	<div><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	<div><input type="text" value="admin"/> ▼ admin guest</div>	

步驟6.按一下Apply。

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"/>	

現在，您已在RV34x系列路由器上成功配置本地使用者成員資格。

編輯本地使用者

步驟1.選中Local User Membership List表中本地使用者使用者名稱旁邊的竅取方塊。

在本示例中，選擇了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

步驟2. 按一下「Edit」。

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

無法編輯使用者名稱。

步驟3.在 *Old Password* 欄位中，輸入先前為本地使用者帳戶設定的密碼。

Edit User Account

User Name

Administrator_Noah

Old Password

●●●●●●●●

步驟4.在 *New Password* 欄位中，輸入新密碼。新密碼必須符合最低要求。

Edit User Account

User Name

Old Password

New Password

(Range: 0 - 127)

步驟5.在 *New Password Confirm* 欄位中再次輸入新密碼進行確認。這些密碼必須匹配。

Edit User Account

User Name

Old Password

New Password

(Range: 0 - 127)

New Password Confirm

步驟6. (可選) 從「組」下拉選單中，選擇一個組，以向使用者帳戶分配許可權。

在此範例中，選擇 **guest**。

Edit User Account

User Name

Old Password

New Password

(Range: 0 - 127)

New Password Confirm

Group

admin

guest

步驟7.按一下Apply。

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"/>	▼

您現在應該已成功編輯本地使用者帳戶。

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

匯入本地使用者



步驟1. 在Local Users Import區域中，按一下 。

步驟2. 在Import User Name & Password下，按一下 **Browse...** 匯入使用者清單。此檔案通常是以逗號分隔值(.CSV)格式儲存的電子表格。

在本示例中，選擇了 **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

步驟3. (可選) 如果您沒有模板，請按一下Download User Template區域中的**Download**。

Local Users Import

Import User Name & Password

Browse...

user-template.csv

(Import User Name + Password via CSV files)

Import

Download User Template:

Download

步驟4.按一下「Import」。

Local Users Import

Import User Name & Password

Browse...

user-template.csv

(Import User Name + Password via CSV files)

Import

Download User Template:

Download

匯入按鈕旁會顯示一條消息，說明匯入成功。

您現在已成功匯入本地使用者清單。

配置遠端身份驗證服務

RADIUS

步驟1.在「遠端身份驗證服務」表中，按一下Add以建立條目。

Remote Authentication Service Table



Enable  Name 

步驟2. 在 *Name* 欄位中，為帳戶建立使用者名稱。

在本例中，使用 **Administrator**。

Add/Edit New Domain

Name

Administrator

步驟3. 從「Authentication Type」下拉選單中選擇 **Radius**。這表示將透過 RADIUS 伺服器進行使用者驗證。

只能在 RADIUS 下配置單個遠端使用者帳戶。

Authentication Type

RADIUS

Primary Server

RADIUS

Active Directory

Backup Server

LDAP

步驟4. 在 *Primary Server* 欄位中，輸入主 RADIUS 伺服器的 IP 位址。

在本示例中，**192.168.3.122** 用作主伺服器。

Primary Server Port

步驟5.在「Port」欄位中，輸入主RADIUS伺服器的連線埠號碼。

在本例中，**1645**用作埠號。

Primary Server Port

步驟6.在Backup Server欄位中，輸入備份RADIUS伺服器的IP位址。這用作主伺服器關閉時的故障轉移。

在本示例中，備份伺服器地址為**192.168.4.122**。

Backup Server Port

步驟7.在Port欄位中，輸入備份RADIUS伺服器的數量。

Backup Server Port

在本例中，**1646**用作埠號。

步驟8.在Preshared-Key欄位中，輸入在RADIUS伺服器上設定的預共用金鑰。

Pre-shared Key

步驟9.在Confirm Preshared-key欄位中，重新輸入預共用金鑰以進行確認。

Confirm Pre-shared Key

步驟10.按一下Apply。

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="●●●●●●●●"/>		

您將進入主使用者帳戶頁面。最近配置的帳戶現在顯示在遠端身份驗證服務表中。

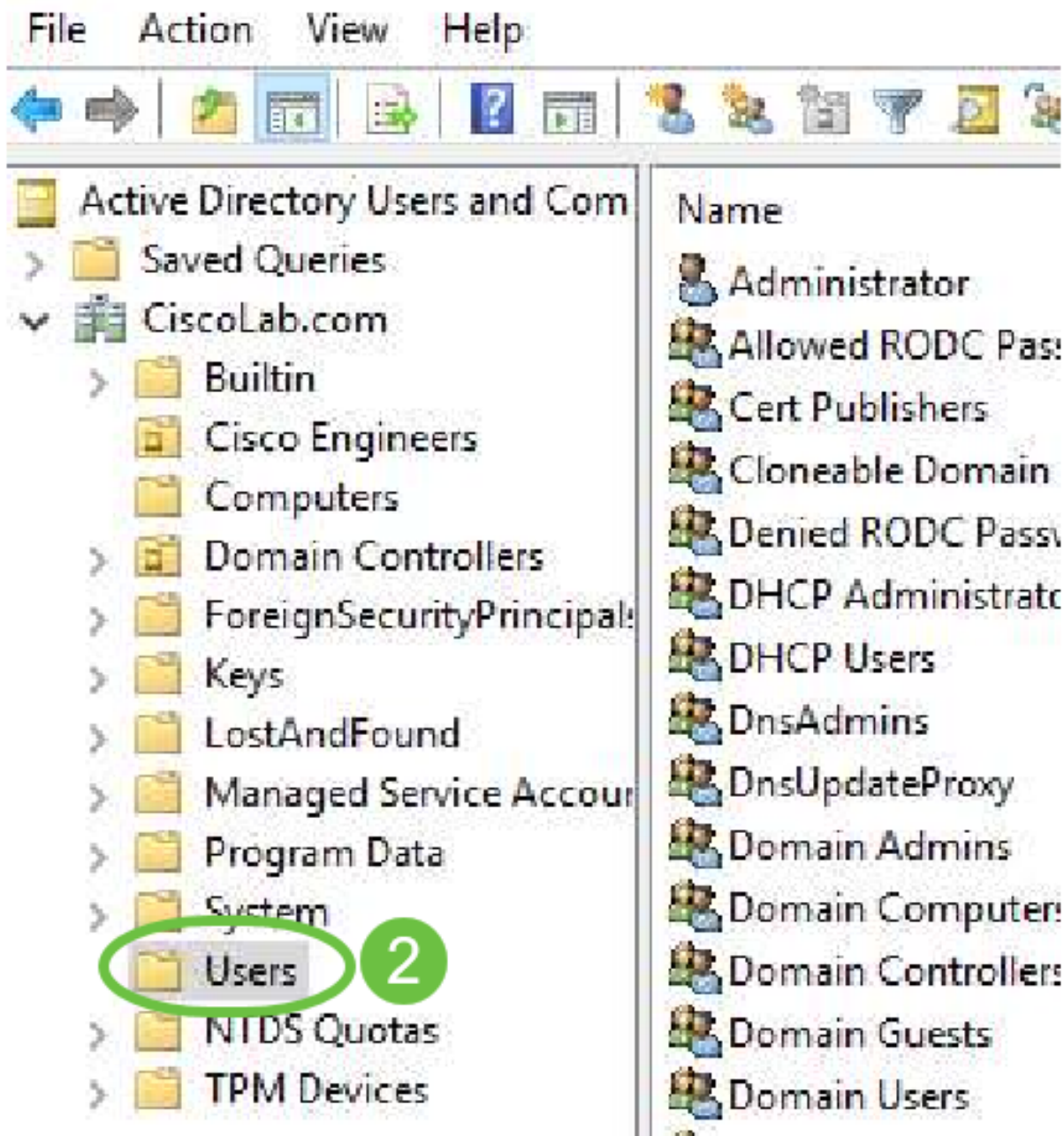
您現在已在RV34x系列路由器上成功配置RADIUS身份驗證。

Active Directory配置

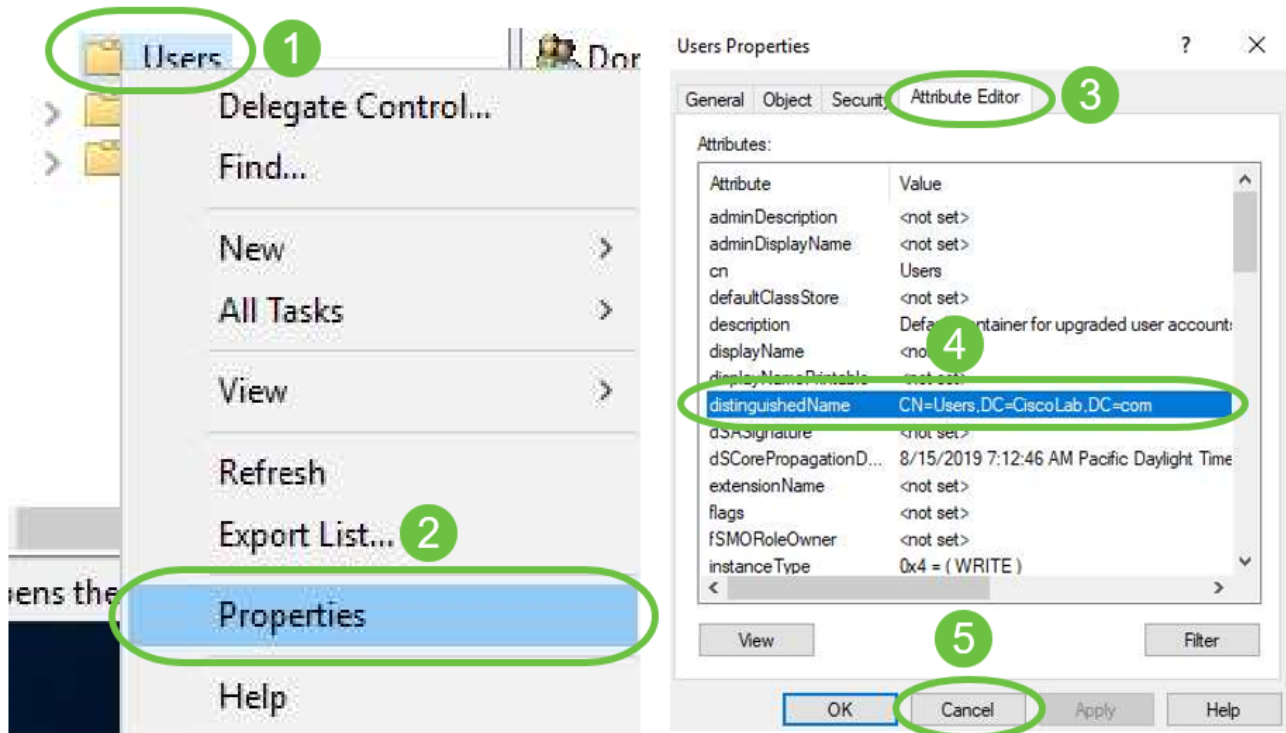
步驟1.要完成Active Directory配置，您需要登入到Active Directory伺服器。在PC上，開啟**Active Directory使用者和電腦**，然後導航到包含用於遠端登入的使用者帳戶的容器。在本例中，我們將使用**Users**容器。

Active Directory Users and Computers

1



步驟2. 按一下右鍵容器並選擇屬性。導航到Attribute Editor頁籤並找到distinguishedName欄位。如果此頁籤不可見，則需要在Active Directory使用者和電腦中啟用高級功能檢視並重新開始。請記下此欄位，然後按一下Cancel。這將是使用者容器路徑。配置RV340時也需要此欄位，並且必須完全匹配。



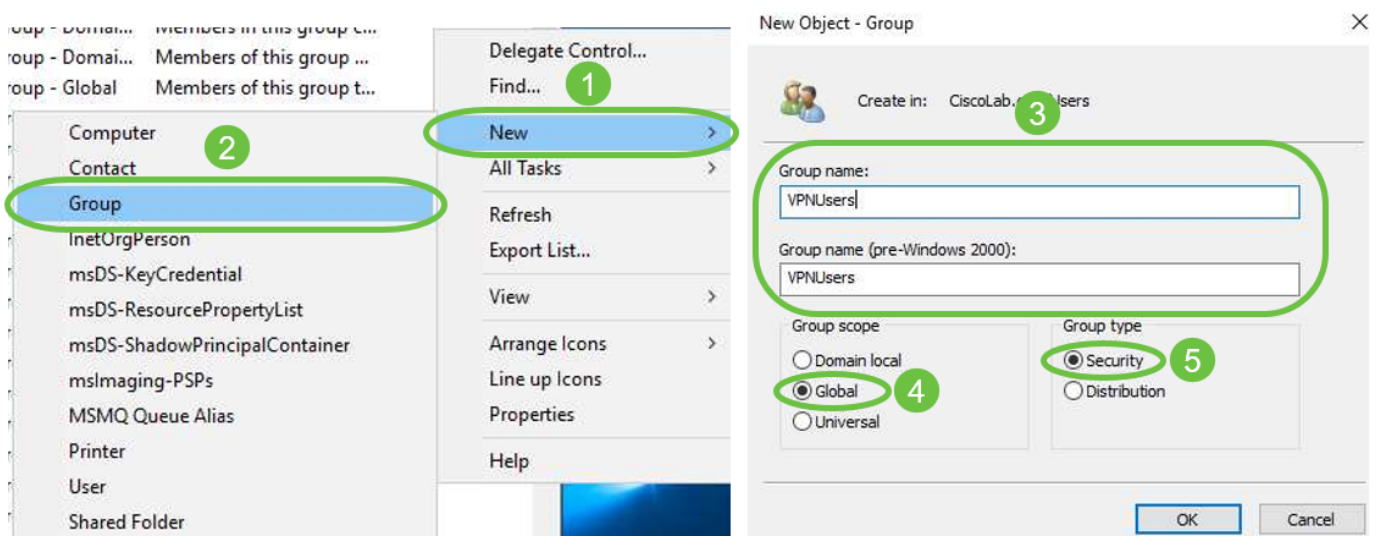
步驟3.在將要使用的使用者帳戶所在的容器中建立全域性安全組。

在選定的容器中，按一下右鍵空白區域，然後選擇「新建」>「組」。

選擇以下內容：

- 組名 — 此名稱必須與RV340上建立的使用者組名完全匹配。在本示例中，我們將使用 **VPNUsers**。
- 組範圍 — 全域性
- 組型別 — 安全性

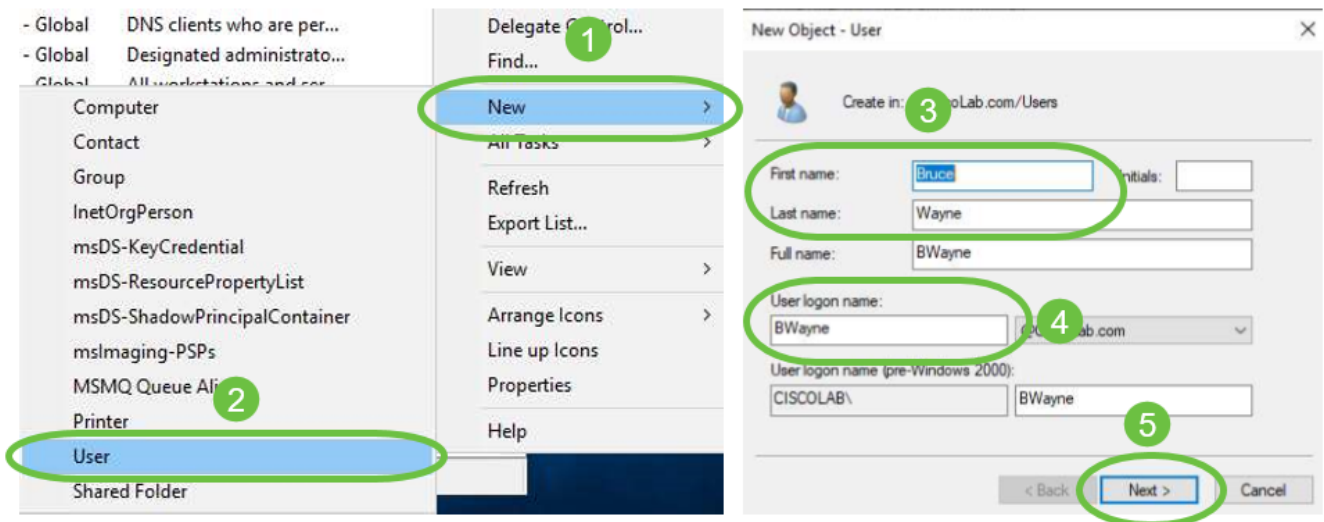
按一下「OK」（確定）。



步驟4.要建立新的使用者帳戶，請執行以下操作：

- 按一下右鍵容器中的空白區域，然後選擇「新建」>「使用者」。

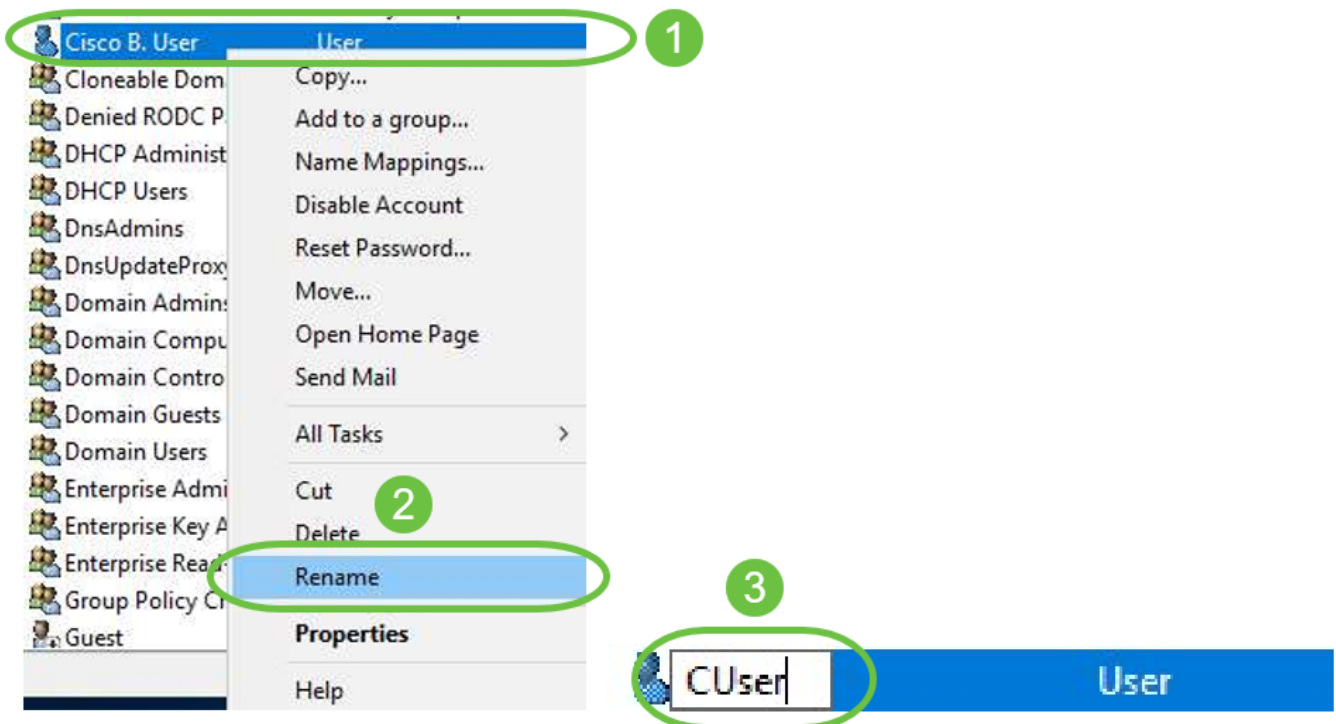
- 輸入名字、姓氏。
- 輸入使用者登入名。
- 按「Next」（下一步）。



系統將提示您輸入使用者的密碼。如果選中 *User must change password at next logon* 框，則使用者必須在本地登入並在遠端登入之前更改密碼。

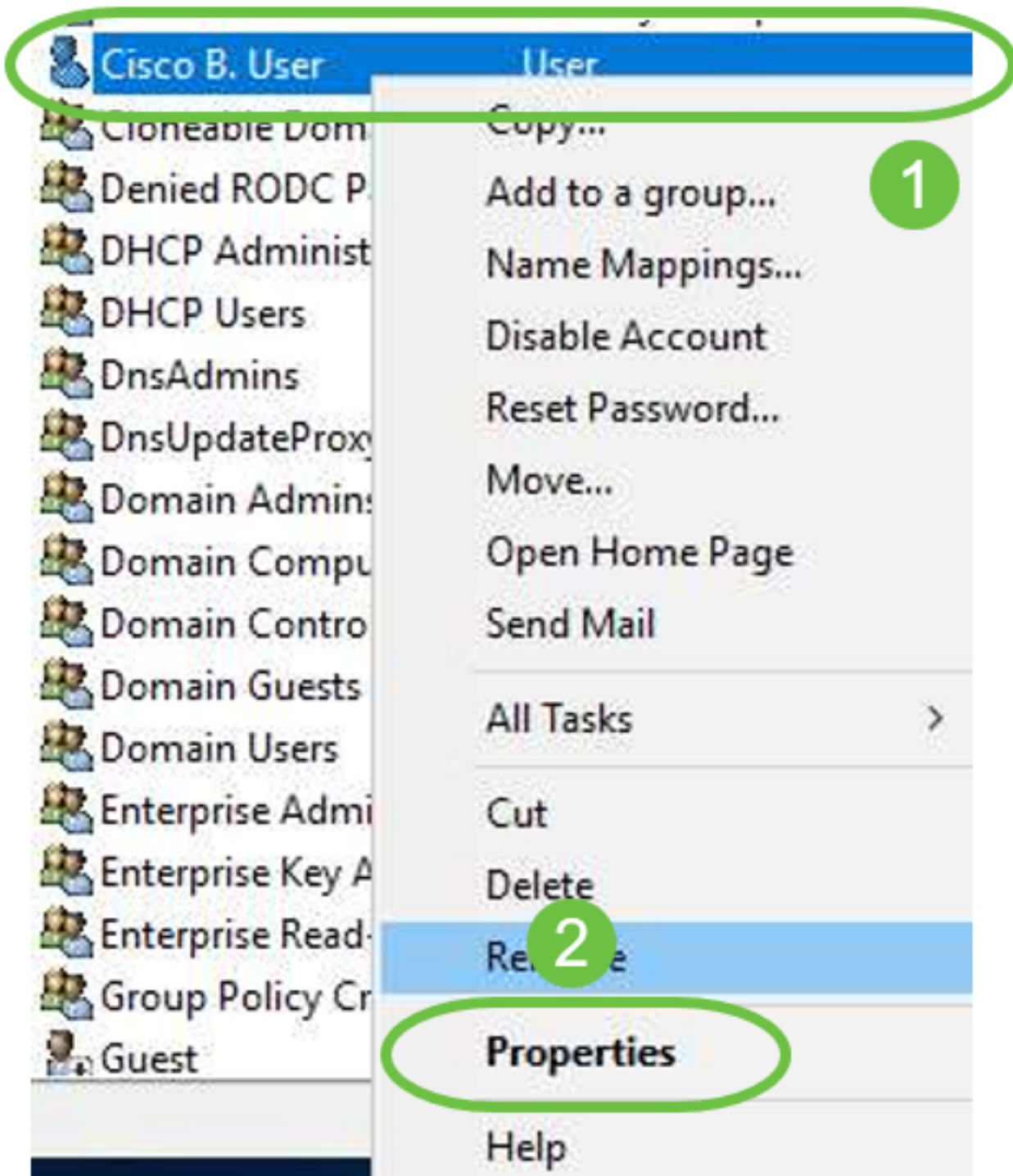
按一下「Finish」（結束）。

如果已建立了需要使用的使用者帳戶，則可能需要進行調整。要調整使用者的規範名稱，請選擇使用者，按一下右鍵並選擇**重新命名**。確保所有空格都已刪除，並且與使用者的登入名相匹配。這不會更改使用者的顯示名稱。按一下「OK」（確定）。



步驟5. 正確構建使用者帳戶後，需要授予其遠端登入許可權。

為此，請選擇使用者帳戶，按一下右鍵並選擇**屬性**。



在 *User Properties* 中選擇 **Attribute Editor** 頁籤，向下滾動到 **distinguishedName**。確保第一個 **CN=** 的使用者登入名正確且沒有空格。

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 3
displayableNamePrintable	<not set>
distinguishedName	CN=CUser,CN=Users,DC=CiscoLab,DC=com
division	<not set>

選擇Member Of頁籤，然後按一下Add。

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	

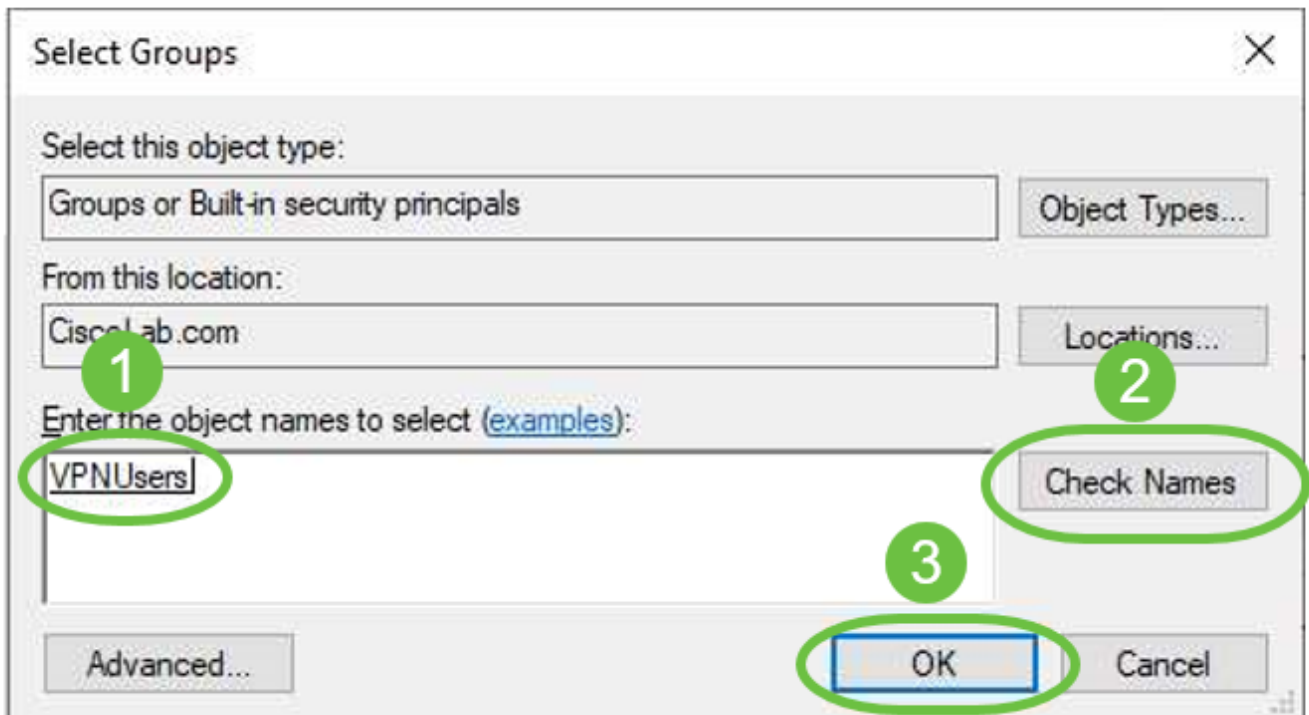
Member of:

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

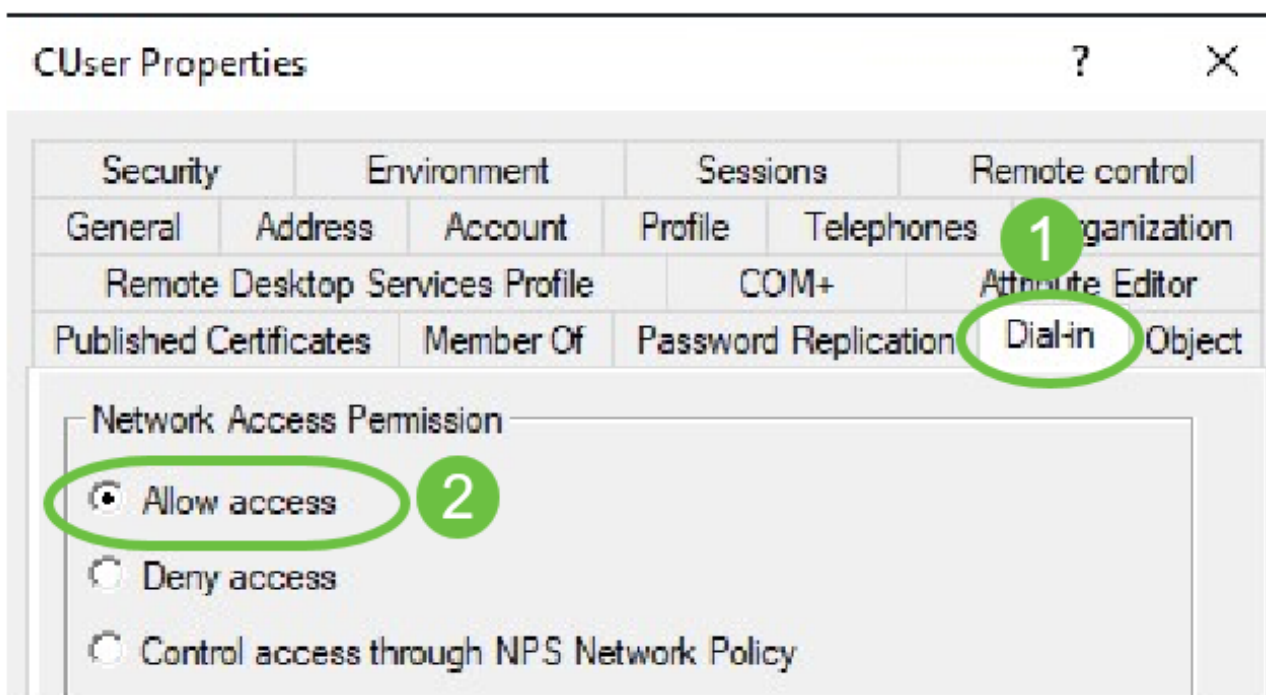
2

Add... Remove

輸入全域性安全組的名稱，然後選擇**檢查名稱**。如果條目帶有下列線，請按一下OK。



選擇Dial-In頁籤。在Network Access Permission部分下，選擇Allow Access，保留其餘部分為預設值。

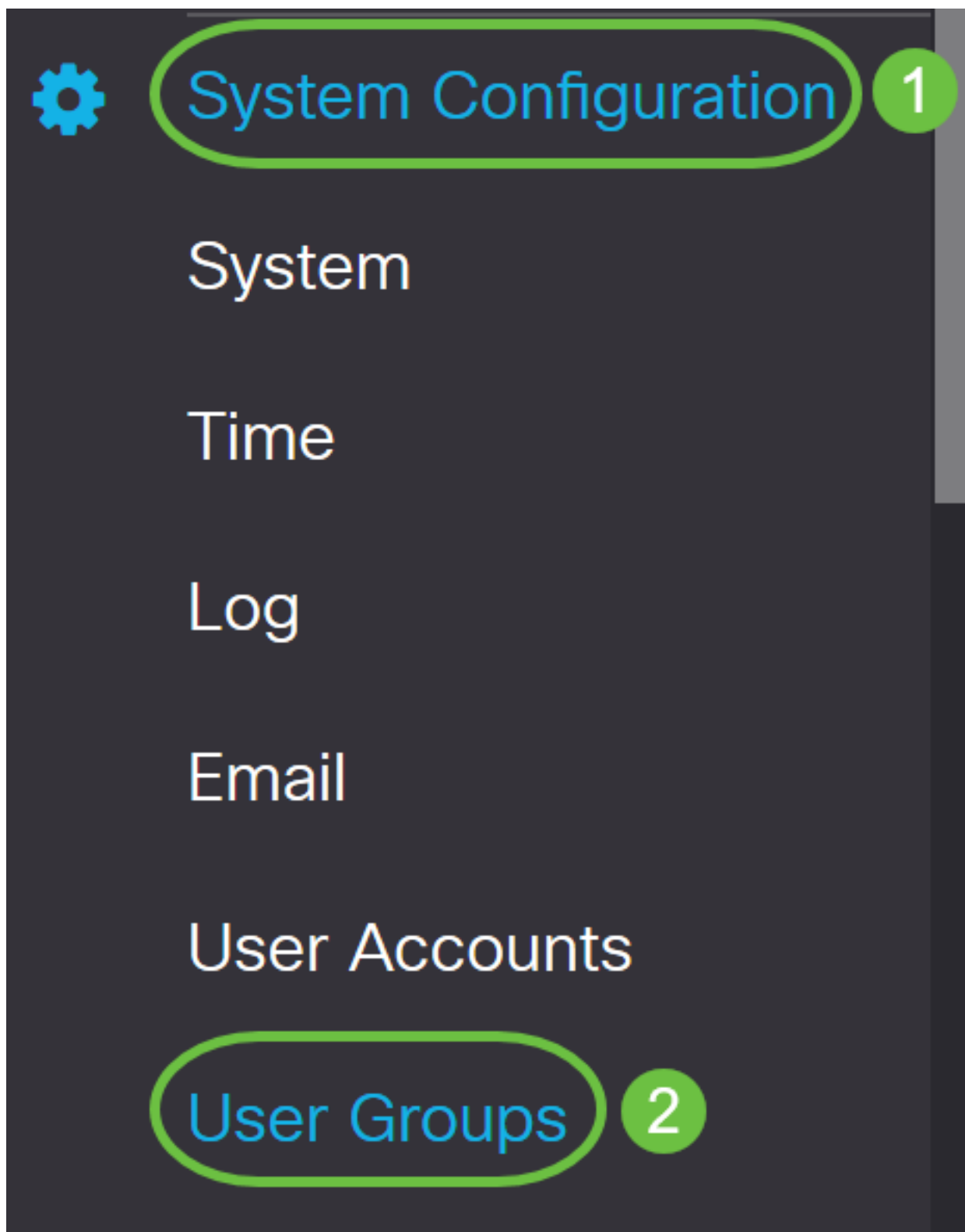


Active Directory整合

Active Directory要求RV34x路由器的時間與AD伺服器的時間相匹配。有關如何在RV34x系列路由器上配置時間設定的步驟，請按一下[此處](#)。

AD還要求RV340具有與AD全域性安全組匹配的使用者組。

步驟1.導覽至System Configuration > User Groups。



步驟2.點選plus圖示新增使用者組。

User Groups

User Groups Table



步驟3.輸入組名。在本例中，它是VPNUsers。

Group Name:

組名稱必須與AD全域性安全組完全相同。

步驟4.在 *Services* 下，*Web Login/NETCONF/RESTCONF* 應標籤為 **Disabled**。如果AD整合不能立即運行，您仍可以訪問RV34x。

Services

Web Login/NETCONF/RESTCONF Disabled Read Only Administrator

步驟5.您可以新增將使用AD整合登入其使用者的VPN隧道。

1. 要新增已配置的客戶端到站點VPN，請轉到EZVPN/第三方部分，然後按一下 **plus** 圖標。從下拉選單中選擇VPN配置檔案，然後按一下 **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 — 如果使用SSL VPN隧道，請從選擇配置檔案旁邊的下拉選單中選擇策略。

SSL VPN

Select a Profile

SSLVPNDefaultPolicy

6. PPTP/L2TP/802.1x — 要允許這些裝置使用AD，只需按一下它們旁邊的覈取方塊 *Permit*。

PPTP VPN



Permit

L2TP



Permit

802.1x



Permit

步驟6. 按一下 **Apply** 以儲存變更。

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整合設定

步驟1. 導覽至System Configuration > User Accounts。



System Configuration

System

1

Time

Log

Email

User Accounts

2

步驟2.在「遠端身份驗證服務」表中，按一下Add以建立條目。

Remote Authentication Service Table



Enable ⇅

Name ⇅

步驟3.在Name欄位中，為帳戶建立使用者名稱。在本示例中，使用Jorah_Admin。

Add/Edit New Domain

Name

Jorah_Admin

步驟4.從Authentication Type下拉選單中選擇Active Directory。AD用於向網路的所有元素分配寬泛的策略，將程式部署到多台電腦，並將關鍵更新應用到整個組織。

Authentication Type

Active Directory

AD Domain Name

RADIUS

Active Directory

Primary Server

LDAP

步驟5.在AD域名欄位中，輸入AD的完全限定域名。

本示例使用sampledomain.com。

AD Domain Name

sampledomain.com

步驟6.在 *Primary Server* 欄位中，輸入AD的地址。

在本例中，使用 **192.168.2.122**。

Primary Server

192.168.2.122

Port

1234

步驟7.在 *Port* 欄位中輸入主伺服器的埠號。

在本例中，**1234** 用作埠號。

Primary Server

192.168.2.122

Port

1234

步驟8. (可選) 在 *User Container Path* 欄位中，輸入包含使用者的根路徑。

附註：本示例使用 `file:Documents/manage/containers`。

User Container Path

file:Documents/manage/co

步驟9.按一下 **Apply**。

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

步驟10.向下滾動至 *服務身份驗證序列*，設定各種選項的登入方法。

- Web Login/NETFCNF/RESTCONF — 這是您登入RV34x路由器的方式。取消選中 *Use Default* 覆取方塊，並將Primary方法設定為 **Local DB**。這將確保即使Active Directory整合失敗

，您也不會從路由器註銷。

- 站點到站點/EzVPN第三方客戶端到站點VPN — 這是為了將客戶端到站點VPN隧道設定為使用AD。取消選中*Use Default*覆取方塊，並將Primary方法設定為**Active Directory**，將Secondary方法設定為**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"/>	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

步驟11.按一下**Apply**。

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

步驟12.將運行配置儲存到啟動配置。

現在，您已在RV34x系列路由器上成功配置Active Directory設定。

LDAP

步驟1.在「遠端身份驗證服務」表中，按一下**Add**以建立條目。

Remote Authentication Service Table



Enable  Name 


步驟2. 在 *Name* 欄位中，為帳戶建立使用者名稱。

只能在LDAP下配置單個遠端使用者帳戶。

在此示例中，使用Dany_Admin。

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

步驟3. 從Authentication Type下拉選單中選擇LDAP。輕量型目錄訪問協定是用於訪問目錄服務的訪問協定。它是運行目錄伺服器以對域執行身份驗證的遠端伺服器。

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	

步驟4. 在 *Primary Server* 欄位中，輸入LDAP的伺服器地址。

在本示例中，使用192.168.7.122。

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

步驟5.在 *Port* 欄位中，輸入主要伺服器的連線埠號碼。

在本例中，122 用作埠號。

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

步驟6.在 *Base DN* 欄位中輸入LDAP伺服器的基本可分辨名稱。基本DN是LDAP伺服器在收到授權請求時搜尋使用者的位置。此欄位應與LDAP伺服器上配置的基本DN匹配。

在本示例中，使用Dept101。

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

步驟7.按一下 **Apply**。您將轉到遠端身份驗證服務表。



User Accounts

Add/Edit New Domain

Name	Client_Accounts		
Authentication Type	LDAP		
Primary Server	192.168.7.122	Port	122
Base DN	Dept101		

步驟8. (可選) 如果要啟用或禁用遠端身份驗證服務，請選中或取消選中要啟用或禁用的服務旁邊的覈取方塊。

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

步驟9.按一下「Apply」。

User Accounts

Apply

現在，您已在RV34x系列路由器上成功配置LDAP。

檢視與本文相關的影片.....

[按一下此處檢視思科的其他技術對話](#)