## 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<u>最新版本)</u>)

## 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
- <u>匯入本地使用者</u>
- <u>配置遠端身份驗證服務</u>
- RADIUS
- <u>Active Directory</u>配置
- <u>Active Directory整合</u>
- Active Directory整合設定
- <u>LDAP</u>

## 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<mark>配置本地使用者</mark>。

# Local Users Password Complexity

Password Complexity Settings:

![](_page_1_Picture_5.jpeg)

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:	10 (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:	🗹 Enab	le
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 (ABC	D), Iowe	r case(abcd), numerical(1234) and special characters(!@#\$).

#### 步驟5.選中Enable覈取方塊,新密碼必須不同於當前密碼。

## Local Users Password Complexity

Password Complexity Settings:	S Enable	9	
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(!@#\$).			
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:	🗹 Enabl	e	
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(!@#\$).			
The new password must be different than the current one: 🗹 Enable			
Password Aging Time:	180	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

	<u>i</u>	
□ # \$	User Name 🖨	Group * 🖨
□ 1	cisco	admin
□ 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	Administrator_Noah	
New Password	Password may not be left blank	( Range: 8 - 127 )
New Password Confirm	Password may not be left blank	
Password Strength Meter		
Group	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	Administrator_Noah	
New Password	••••••	( Range: 8 - 127 )
New Password Confirm	Password may not be left blank	Must match the previous entry
Password Strength Meter		]
Group	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	Administrator_Noah	]
New Password	•••••	( Range: 8 - 127 )
New Password Confirm	•••••	
Password Strength Meter		
Group	admin	

## 密碼強度計根據密碼強度而變化。

![](_page_6_Figure_3.jpeg)

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	Administrator_Noah	
New Password	••••••	( Range: 8 - 127 )
New Password Confirm	••••••	
Password Strength Meter		
Group	admin ~	
	admin	
	guest	

步驟6.按一下Apply。

User Accounts			Apply Cancel
Add User Acco	unt		
The current minimum requi Minimal password le Minimal number of c The new password r	irements are as follows. ngth: 8 haracter classes: 3 nust be different than the current one		
User Name	Administrator_Noah		
New Password	••••••	( Range: 8 - 127 )	
New Password Confirm	•••••		
Password Strength Meter			
Group	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覈取方塊。

在本示例中,選擇了Administrator\_Noah。

# Local Users

## Local User Membership List

+ 🗷	🔟 📥	
□ # \$	User Name 🖨	Group * 🖨
1	Administrator_Noah	admin
□ 2	cisco	admin
□ 3	guest	guest

步驟2.按一下**「Edit**」。

# Local Users

## Local User Membership List

+ 🕜 🛍 📥		
□ #\$	User Name 🖨	Group * 🖨
<b>I</b>	Administrator_Noah	admin
□ 2	cisco	admin
□ 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 Acco	ount
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	Administrator_Noah	
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 Acco	unt	
User Name	Administrator_Noah	
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 Acco	ount	
User Name	Administrator_Noah	
Old Password	••••••	
New Password	••••••	( Range: 0 - 127 )
New Password Confirm	••••••	
Group	guest	
	admin	
	guest	

## 步驟7.按一下Apply。

User Accounts			Apply	Cancel
Edit User Acco	punt			
User Name	Administrator_Noah			
Old Password	•••••			
New Password	•••••	( Range: 0 - 127 )		
New Password Confirm	•••••			
Group	guest ~			

您現在應該已成功編輯本地使用者帳戶。

# Local Users

## Local User Membership List

+ 🗷	<u>iii</u>	
□ #\$	User Name 🖨	Group * 🖨
□ 1	Administrator_Noah	guest
□ 2	cisco	admin
□ 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。

![](_page_13_Figure_0.jpeg)

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

![](_page_14_Picture_0.jpeg)

![](_page_15_Figure_0.jpeg)

## **Remote Authentication Service Table**

![](_page_16_Picture_1.jpeg)

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。

![](_page_16_Picture_9.jpeg)

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	192.168.3.122	Port	389

步驟5.在「Port」欄位中,輸入主RADIUS伺服器的連線埠號碼。

Primary Server	192.168.3.122	Port	389	)
Primary Server	192.168.3.122	Port	389	

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	192.168.4.122	Port	389	
步驟7.在Port欄位中,輸入	備份RADIUS伺服器的數量。	,		
Backup Server	192.168.4.122	Port	389	
在本例中, <b>1646</b> 用作埠號。				
步驟8.在Preshared-Key欄位	立中,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	d-key欄位中,重新輸入預共	用金鑰以進行確認。	0	
Confirm Pre-sh	ared Key			

步驟10.按一下Apply。

## Add/Edit New Domain

Name	Administrator		
Authentication Type	RADIUS ~		
Primary Server	192.168.3.122	Port	389
Backup Server	192.168.4.122	Port	389
Pre-shared Key	••••••		
Confirm Pre-shared Key	•••••		

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。

![](_page_19_Figure_0.jpeg)

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。

>	Delegate Control Find		General Object Security Attributes:	Attribute Editor	
	New All Tasks	>	Attribute adminDescription adminDisplayName cn defaultClassStore description displayName	Value <not set=""> <not set=""> Users <not set=""> Defate that the for upgraded user according to the for upgraded user according to the for upgraded user according to the formula to the for</not></not></not>	Aunt:
	View	>	display Name Drintsbla distinguished Name	CN=Users.DC=CiscoLab.DC=com	
	Refresh Export List <b>2</b>		dSASignature dSCorePropagationD extensionName flags fSMORoleOwner instanceType	<pre><not set=""> 8/15/2019 7:12:46 AM Pacific Daylight T <not set=""> <not set=""> cnot set&gt; 0x4 = (WRITE)</not></not></not></pre>	Time
ens the	Properties		<		>

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)。

roup - Domai Members in this group c roup - Domai Members of this group roup - Global Members of this group t	Delegate Control Find	New Object - Group
Computer 2	New	
Contact	All Tasks	Group name:
Group	Refresh	VPNUsers
InetOrgPerson	Export List	Group name (pre-Windows 2000):
msDS-ResourcePropertyList	View	> VPNUsers
msDS-ShadowPrincipalContainer	Arrange Icons	Group scope     Group type     Opomain local     Security
msImaging-PSPs	Line up Icons	Global     A     Distribution
, MSMQ Queue Alias	Properties	OUniversal
, Printer	Help	
User		
Shared Folder		OK Cancel

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」。

ilobal DNS clients who are per ilobal Designated administrato	Delegate Trol Find	New Object - User
Computer	New	Create in: 3 oLab.com/Users
Contact	All Tasks	·
Group InetOrgPerson	Refresh Export List	First name:     Bruce     Initials:       Last name:     Wayne
msDS-ResourcePropertyList	View	Full name: BWayne
msDS-ShadowPrincipalContainer msImaging-PSPs MSMQ Queue Ali	Arrange Icons Line up Icons Properties	User logon name:     BWayne     User logon name (pre-Windows 2000):     CISCOLAB\     BWayne
Printer	Help	5
User		

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)。

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

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)。

🖁 Cisco B. User 🔛	User			
Cloneable Dom	Сору			
RODC P	Add to a group			
Rep Administ	Name Mappings			
DHCP Users	Disable Account			
DnsUpdateProx	Reset Password			
Domain Admin	Move			
Bomain Compu	Open Hom <mark>e Pag</mark> e			
Bomain Contro	Send Mail			
🐮 Domain Guests 💐 Domain Users	All Tasks	>		
🕂 Enterprise Admi	Cut			
Enterprise Key A	Delete			
Conterprise Read Conterprise Read	Rename		3	
Guest	Properties			
	Help		🚳 CUser 📄	User

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**。

Cisco B. User	User	
Cioneable Dom	Сору	
RODC P	Add to a group	
BHCP Administ	Name Mappings	
CHCP Users	Disable Account	
R DnsAdmins	Reset Password	
ConsUpdateProx	Move	
Bomain Admin:	wove	
Bomain Compu	Open Home Page	
Real Domain Contro	Send Mail	
Comain Guests	All Tasks >	
🕂 Enterprise Admi	Cut	
😤 Enterprise Key A	Delete	
🗟 Enterprise Read	Re 2 e	
Roup Policy Cr		
Guest	Properties	
	Help	

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。

Security	Er	nvironment	Ses	sions	R	emote co	ontrol
General	Address	Account	Profile	Teleph	ones	201	nization
Published (	Certificates	Member Of	Passwor	rd Replicat	tion	Dia	Objec
Remote	Desktop Se	ervices Profile	0	COM+	A	ttribute E	ditor
desktop	Profile	<not set=""></not>	>				and the second second
destinati	ionIndicator	<not set=""></not>	>				
displayN	lame	Cisr 2	User				
displavN	lamePrintabl	e <not set=""></not>	,				
distingui	shedName	CN=CUs	er,CN=Use	ers,DC=Cis	scoLat	DC=co	
			<not set=""></not>				

選擇Member Of頁籤,然後按一下Add。

Cisco B. User Properties

Security	/ Er	vironment	Sess	ions f	Remote c	ontrol
Remote	e Desktop Se	ervic file	C	OM+	Attribute	Editor
General	Address	Account	Profile	Telephones	Orga	nization
Published	Certificates	Member Of	Password Replication		Dial-in	Object
Member of	of:					
Name		Active Direct	ory Domain	Services Fold	er	
Domain	Users	CiscoLab.com	n/Users			
Contain	03010	0.300 200.001	in Coolio			
Add.	F	Remove				

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

?

Select Groups	
Select this object type:	
Groups or Built-in security principals	Object Types
From this location:	
Ciscol ab.com	Locations Des):
VPNUsers	Check Names

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。

User Prop	erties				? ×
Security	Er	nvironment	Sess	ions	Remote control
General	Address	Account	Profile	Telephone	es ganization
Remote	Desktop Se	ervices Profile	C	OM+	Attracte Editor
Published (	Certificates	Member Of	Passwon	d Replication	Dial-in Object
Network	Access Per access	mission			
C Deny	access				
C Contr	ol access th	rough NPS Ne	twork Poli	cv	

## 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<u>此處</u>。

AD還要求RV340具有與AD全域性安全組匹配的使用者組。

![](_page_26_Picture_1.jpeg)

步驟2.點選plus圖示新增使用者組。

![](_page_27_Picture_0.jpeg)

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。

![](_page_27_Picture_2.jpeg)

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 Mem	ber In-use Table
<b>⊕</b> <sup>†</sup>	
#  Group Name	
Add Easture List	×
Salact a Profile: Strow//PNL +	
Select a Prome. ShrewvPN	2
	Add Cancel

- 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

   SSL VPN

   Select a Profile

   SSL VPN
- 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。

![](_page_28_Picture_4.jpeg)

User Groups				Apply
Site to Site VPN Profile Mem	per In-use Table			
	÷			
EzVPN/3rd Party				
EzVPN/3rd Party Profile Mem	ber In-use Table			
<ul> <li></li></ul>				
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。

![](_page_30_Picture_0.jpeg)

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**

![](_page_31_Picture_1.jpeg)

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	~	
	RADIUS		
AD Domain Name	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 <i>Primary</i> 在本例中,使用 <sup>-</sup>	<sup>,</sup> <i>Server</i> 欄位中,輸入A 192.168.2.122。	AD的地址。						
Primary Serve	ər (192.168.2	2.122	Port	1234				
步驟7.在 <i>Port</i> 欄位 在本例中, <b>1234</b>	之中輸入主伺服器的埠 用作埠號。	號。						
Primary Serve	er 192.168.2	2.122	Port	1234				
步驟8.(可選)4 <b>附註:</b> 本示例使/	生 <i>User Container Path</i> 用file:Documents/man	欄位中,輸入包含使 age/containers。	更用者的机	<b>退路徑。</b>				
User Cor	ntainer Path	file:Docu	men	ts/manage/co				
步驟9.按一下 <b>Ap</b>	ply₀							
User Accour	its			Apply				
Add/Edit Nev	<i>w</i> 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	Ⅰ至 <i>服務身份驗證序列</i> ,	,設定各種選項的登 <i>」</i>	入方法。					
Web Login/I	NETFCONF/RESTCO	NF — 這是您登入R\	√34x路自	由器的方式。取消選中 <i>Use</i>				

Default覈取方塊,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覈取方塊,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		Local DB	✓ None
Site-to-site/EzVPN&3rd Party Client-to-site VPN		Active Directory	Local DB
AnyConnect SSL VPN		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**

![](_page_34_Picture_1.jpeg)

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

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	LDAP	~	
Drimony Sonyor	RADIUS		
Phinary Server	Active Directory		
Base DN	LDAP		)

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	0	
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 Accour	nts		
Add/Edit Ne	w Domain		
Name	Dany_Admin		
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**

![](_page_36_Figure_1.jpeg)

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