

Configurazione e gestione di account utente su un router serie RV34x

Obiettivo

In questo articolo viene spiegato come configurare e gestire gli account utente locali e remoti su un router serie RV34x. Tra queste vi sono le modalità per configurare la complessità della password degli utenti locali, configurare/modificare/importare utenti locali, configurare il servizio di autenticazione remota utilizzando RADIUS, Active Directory e LDAP.

Dispositivi interessati | Versione firmware

- Serie RV34x | 1.0.01.16 ([scarica la versione più recente](#))

Introduzione

I router serie RV34x dispongono di account utente per visualizzare e amministrare le impostazioni. Gli utenti possono appartenere a gruppi diversi o a gruppi logici di reti VPN (Virtual Private Network) SSL (Secure Sockets Layer) che condividono il dominio di autenticazione, le regole di accesso ai servizi e alla rete locale (LAN) e le impostazioni di timeout di inattività. La gestione degli utenti definisce il tipo di utenti che possono utilizzare un determinato tipo di struttura e le modalità di utilizzo.

La priorità del database esterno è sempre RADIUS (Remote Authentication Dial-In User Service)/LDAP (Lightweight Directory Access Protocol)/AD (Active Directory)/Local. Se si aggiunge il server RADIUS al router, il servizio Accesso Web e altri servizi utilizzeranno il database esterno RADIUS per autenticare l'utente.

Non è disponibile alcuna opzione per abilitare un database esterno solo per il servizio Accesso Web e configurare un altro database per un altro servizio. Dopo aver creato e abilitato RADIUS sul router, questo utilizzerà il servizio RADIUS come database esterno per il login al Web, la VPN da sito a sito, la VPN EzVPN/di terze parti, la VPN SSL, il protocollo PPTP (Point-to-Point Transport Protocol)/il protocollo L2TP (Layer 2 Transport Protocol) e la VPN 802.1x.

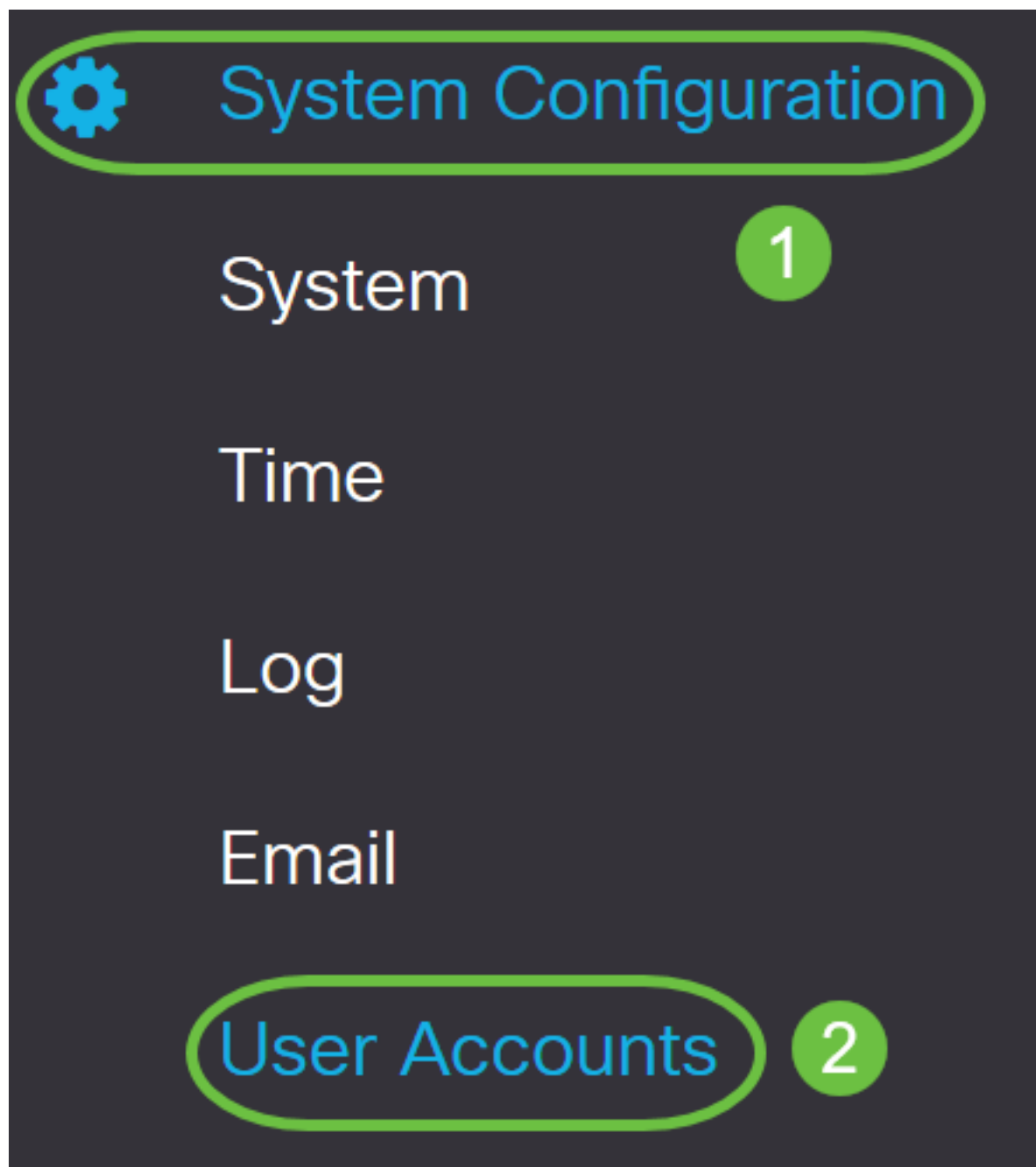
Sommario

- [Configurare un account utente locale](#)
- [Complessità password utenti locali](#)
- [Configura utenti locali](#)
- [Modifica utenti locali](#)
- [Importa utenti locali](#)
- [Configura servizio di autenticazione remota](#)
- [RAGGIO](#)
- [Configurazione di Active Directory](#)
- [Integrazione con Active Directory](#)
- [Impostazioni integrazione Active Directory](#)
- [LDAP](#)

Configurare un account utente locale

Complessità password utenti locali

Passaggio 1. Accedere all'utility basata sul Web del router e scegliere **Configurazione di sistema > Account utente**.



Passaggio 2. Selezionare la casella di controllo **Abilita impostazioni complessità password** per abilitare i parametri di complessità della password.

Se l'opzione è deselezionata, passare alla sezione [Configurazione utenti locali](#).

Local Users Password Complexity

Password Complexity Settings:



Enable

Passaggio 3. Nel campo *Lunghezza minima password*, immettere un numero compreso tra 0 e 127 per impostare il numero minimo di caratteri che una password deve contenere. Il valore predefinito è 8.

Per questo esempio, il numero minimo di caratteri è impostato su 10.

Local Users Password Complexity

Password Complexity Settings:



Enable

Minimal password length:

(Range: 0 - 127, Default: 8)

Passaggio 4. Nel campo *Numero minimo di classi di caratteri*, immettere un numero compreso tra 0 e 4 per impostare la classe. Il numero immesso rappresenta il numero minimo o massimo di caratteri delle diverse classi:

- La password è composta da caratteri maiuscoli (ABCD).
- La password è composta da caratteri minuscoli (abcd).
- La password è composta da caratteri numerici (1234).
- La password è composta da caratteri speciali (!@#\$).

Nell'esempio, viene usato il valore 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(!@#\$...).

Passaggio 5. Selezionare la casella di controllo **Abilita** per la nuova password deve essere diversa da quella corrente.

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

Passaggio 6. Nel campo *Scadenzario password*, immettere il numero di giorni (0 - 365) per la scadenza della password. Nell'esempio, sono stati immessi **180** giorni.

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)

Configurazione delle impostazioni di complessità della password degli utenti locali sul router completata.

Configura utenti locali

Passaggio 1. Nella tabella Elenco appartenenza utenti locali fare clic su **Aggiungi** per creare un nuovo account utente. Verrà visualizzata la pagina Aggiungi account utente.

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

Nell'intestazione *Aggiungi account utente* vengono visualizzati i parametri definiti nei passaggi Complessità password locale.

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

Passaggio 2. Nel campo *Nome utente*, immettere un nome utente per l'account.


Nell'esempio viene utilizzato **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"/>	

Passaggio 3. Nel campo *Nuova password*, immettere una password con i parametri definiti. In questo esempio, la lunghezza minima della password deve essere composta da 10 caratteri con una combinazione di lettere maiuscole, lettere minuscole, numeri e caratteri speciali.

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"/>	

Passaggio 4. Nel campo *Conferma nuova password*, immettere nuovamente la password per confermare. Se le password non corrispondono, verrà visualizzato un testo accanto al campo.

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"/>	▼


Il Misuratore dell'intensità della password varia a seconda dell'intensità della password.



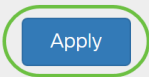
Passaggio 5. Dall'elenco a discesa *Gruppo*, scegliere un gruppo a cui assegnare un privilegio a un account utente. Le opzioni sono:

- admin: privilegi di lettura e scrittura.
- guest - Privilegi di sola lettura.

Per questo esempio, viene scelto **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"/>	

Passaggio 6. Fare clic su **Applica**.



Cancel

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"/>	▼

Configurazione dell'appartenenza dell'utente locale su un router serie RV34x completata.

Modifica utenti locali

Passaggio 1. Selezionare la casella di controllo accanto al nome dell'utente locale nella tabella Elenco appartenenza utente locale.

Per questo esempio, viene scelto **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

Passaggio 2. Fare clic su **Modifica**.

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

Impossibile modificare il nome utente.

Passaggio 3. Nel campo *Vecchia password*, immettere la password precedentemente configurata per l'account utente locale.

Edit User Account

User Name

Old Password

Passaggio 4. Nel campo *Nuova password*, immettere una nuova password. La nuova password deve soddisfare i requisiti minimi.

Edit User Account

User Name

Old Password

New Password

(Range: 0 - 127)

Passaggio 5. Immettere la nuova password ancora una volta nel campo *Conferma nuova password* per confermare. Queste password devono corrispondere.

Edit User Account

User Name

Old Password

New Password

(Range: 0 - 127)

New Password Confirm

Passaggio 6. (Facoltativo) Dall'elenco a discesa Gruppo scegliere un gruppo per assegnare un privilegio a un account utente.

Nell'esempio viene scelto **guest**.

Edit User Account

User Name

Old Password

New Password

(Range: 0 - 127)

New Password Confirm

Group

admin

guest

Passaggio 7. Fare clic su **Applica**.

User Accounts

Apply

Cancel

Edit User Account

User Name

Old Password

New Password

(Range: 0 - 127)

New Password Confirm

Group

A questo punto è necessario aver modificato un account utente locale.

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

Importa utenti locali



Passaggio 1. Nell'area Importazione utenti locali, fare clic su

Passaggio 2. In Importa nome utente e password fare clic su **Sfogliare...** per importare un elenco di utenti. Questo file è in genere un foglio di calcolo salvato in formato CSV (Comma Separated Value).

In questo esempio viene scelto **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

Passaggio 3. (Facoltativo) Se non si dispone di un modello, fare clic su **Download** nell'area Download del modello utente.

Local Users Import

Import User Name & Password

Browse...

user-template.csv

(Import User Name + Password via CSV files)

Import

Download User Template:

Download

Passaggio 4. Fare clic su **Importa**.

Local Users Import

Import User Name & Password

Browse...

user-template.csv

(Import User Name + Password via CSV files)

Import

Download User Template:

Download

Accanto al pulsante di importazione viene visualizzato un messaggio che indica che l'importazione è stata completata correttamente.

È stato importato un elenco di utenti locali.

Configura servizio di autenticazione remota

RAGGIO

Passaggio 1. Nella tabella Servizio di autenticazione remota fare clic su **Aggiungi** per creare una voce.

Remote Authentication Service Table



Enable ⇅ Name ⇅

Passaggio 2. Nel campo *Nome*, creare un nome utente per l'account.

Per questo esempio viene utilizzato **Administrator**.

Add/Edit New Domain

Name

Administrator

Passaggio 3. Dal menu a discesa Tipo di autenticazione, scegliere **Raggio**. Ciò significa che l'autenticazione utente verrà eseguita tramite un server RADIUS.

È possibile configurare un solo account utente remoto in RADIUS.

Authentication Type

RADIUS

Primary Server

RADIUS

Active Directory

Backup Server

LDAP

Passaggio 4. Nel campo *Server primario*, immettere l'indirizzo IP del server RADIUS primario.

Nell'esempio, il server principale è **192.168.3.122**.

Primary Server Port

Passaggio 5. Nel campo *Porta* immettere il numero di porta del server RADIUS primario.

Nell'esempio, il numero di porta è **1645**.

Primary Server Port

Passaggio 6. Nel campo *Server di backup*, immettere l'indirizzo IP del server RADIUS di backup. Questa funzionalità funge da failover in caso di interruzione del server principale.

Nell'esempio, l'indirizzo del server di backup è **192.168.4.122**.

Backup Server Port

Passaggio 7. Nel campo *Port (Porta)*, immettere il numero di server RADIUS di backup.

Backup Server Port

Nell'esempio, il numero di porta è **1646**.

Passaggio 8. Nel campo *Preshared-Key*, immettere la chiave precondivisa configurata sul server RADIUS.

Pre-shared Key

Passaggio 9. Nel campo *Confirm Preshared-key*, reimmettere la chiave già condivisa da confermare.

Confirm Pre-shared Key

Passaggio 10. Fare clic su **Applica**.

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="●●●●●●●●"/>		

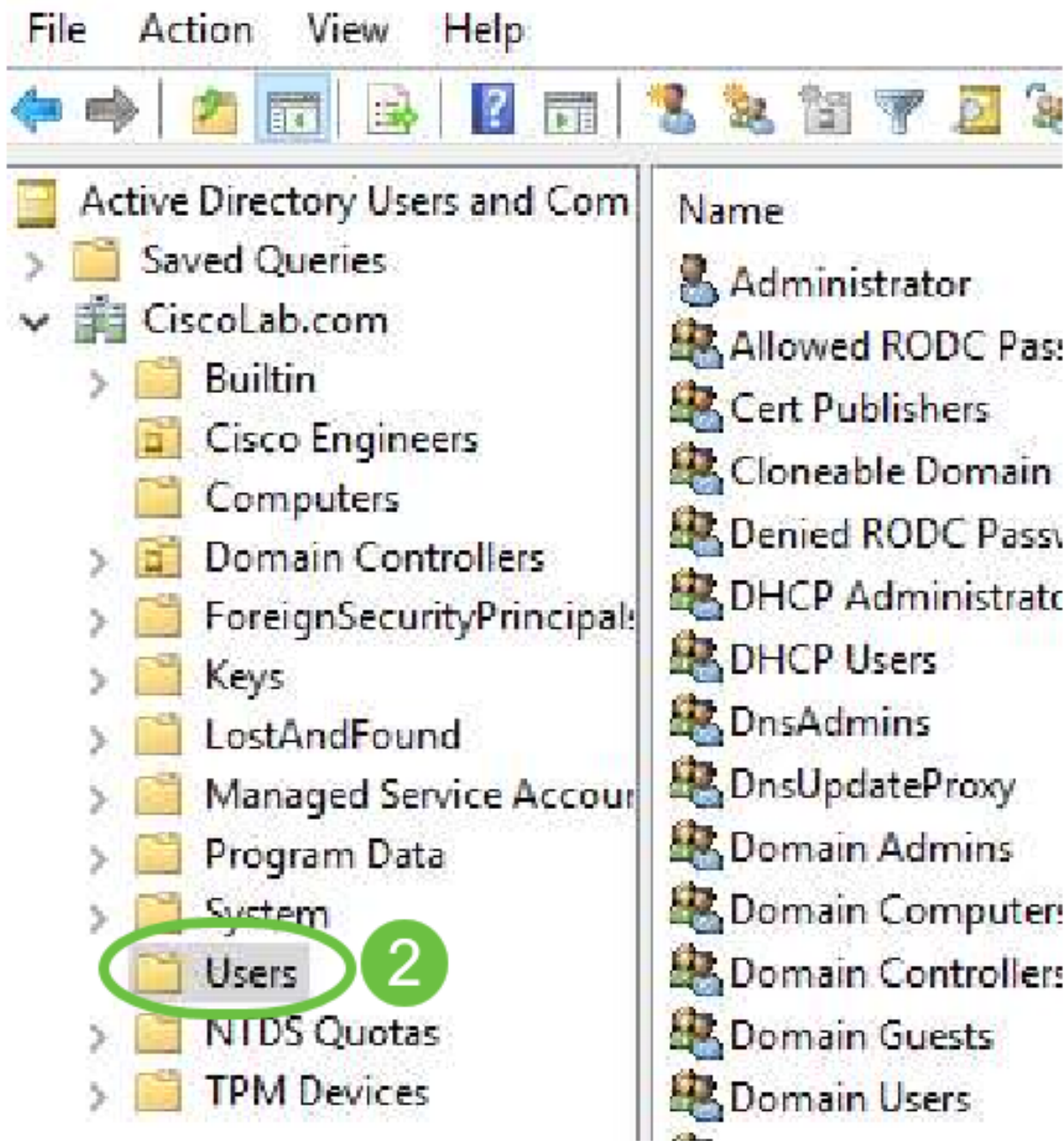
Verrà visualizzata la pagina dell'account utente principale. L'account configurato di recente verrà visualizzato nella tabella Servizio di autenticazione remota.

L'autenticazione RADIUS su un router serie RV34x è stata configurata correttamente.

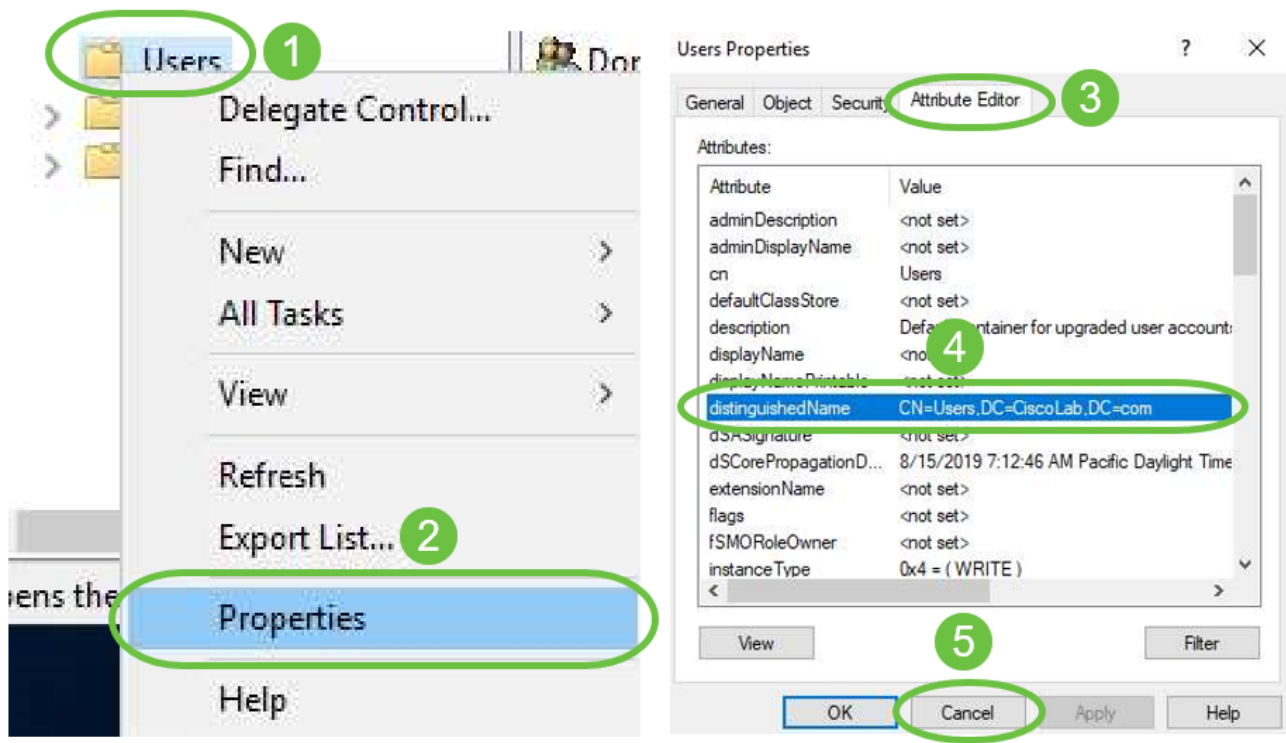
Configurazione di Active Directory

Passaggio 1. Per completare la configurazione di Active Directory, è necessario accedere al server Active Directory. Nel PC aprire **Utenti e computer di Active Directory** e passare al contenitore in cui verranno utilizzati gli account utente per l'accesso remoto. In questo esempio verrà utilizzato il contenitore **Users**.

Active Directory Users and Computers 1



Passaggio 2. Fare clic con il pulsante destro del mouse sul contenitore e selezionare **Proprietà**. Passare alla scheda *Editor attributi* e individuare il campo *distinguishedName*. Se questa scheda non è visibile, sarà necessario attivare la visualizzazione delle funzionalità avanzate in Utenti e computer di Active Directory e ricominciare. Prendere nota di questo campo e fare clic su **Annulla**. Si tratta del percorso del contenitore utente. Questo campo è necessario anche per la configurazione della RV340 e deve corrispondere esattamente.



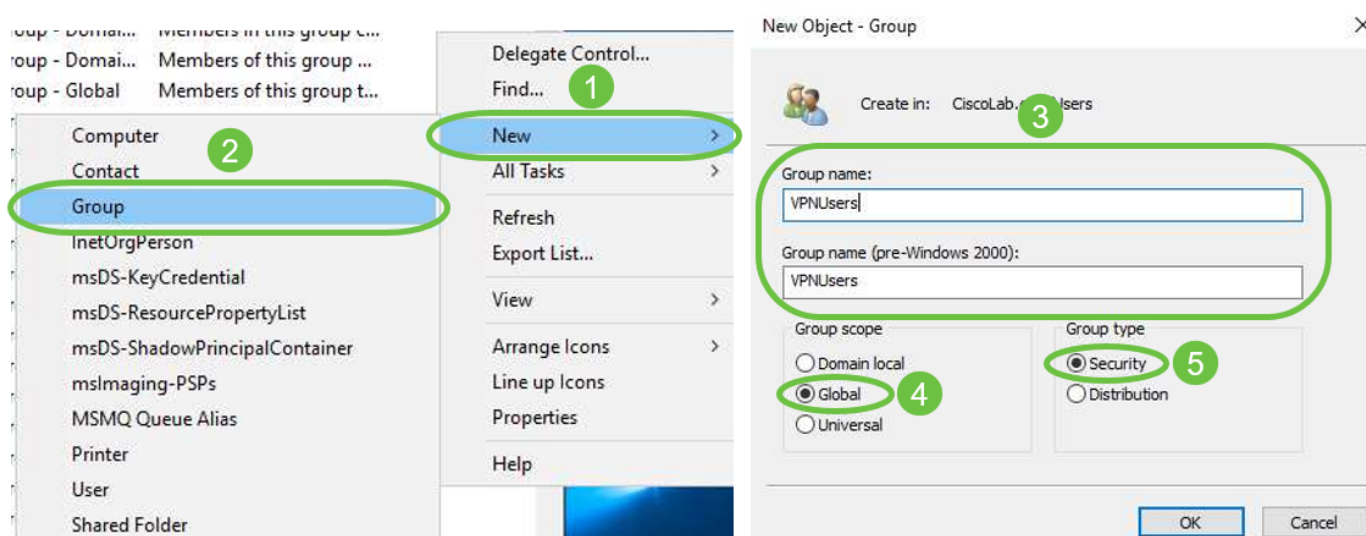
Passaggio 3. Creare un gruppo di sicurezza globale nello stesso contenitore degli account utente che verranno utilizzati.

Nel Contenitore selezionato, fare clic con il pulsante destro del mouse su un'area vuota e selezionare **Nuovo > Gruppo**.

Selezionare quanto segue:

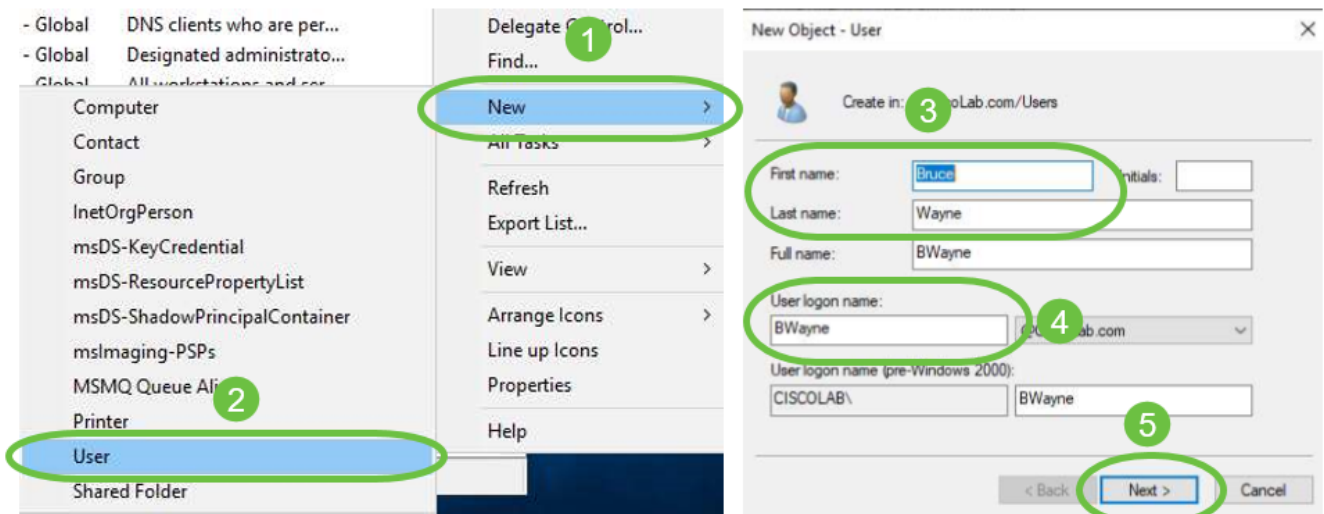
- Nome gruppo: questo nome deve corrispondere esattamente al nome del gruppo di utenti creato sulla RV340. In questo esempio, verranno utilizzati **gli utenti VPN**.
- Ambito gruppo - Globale
- Tipo di gruppo - Sicurezza

Fare clic su **OK**.



Passaggio 4. Per creare nuovi account utente, eseguire le operazioni seguenti:

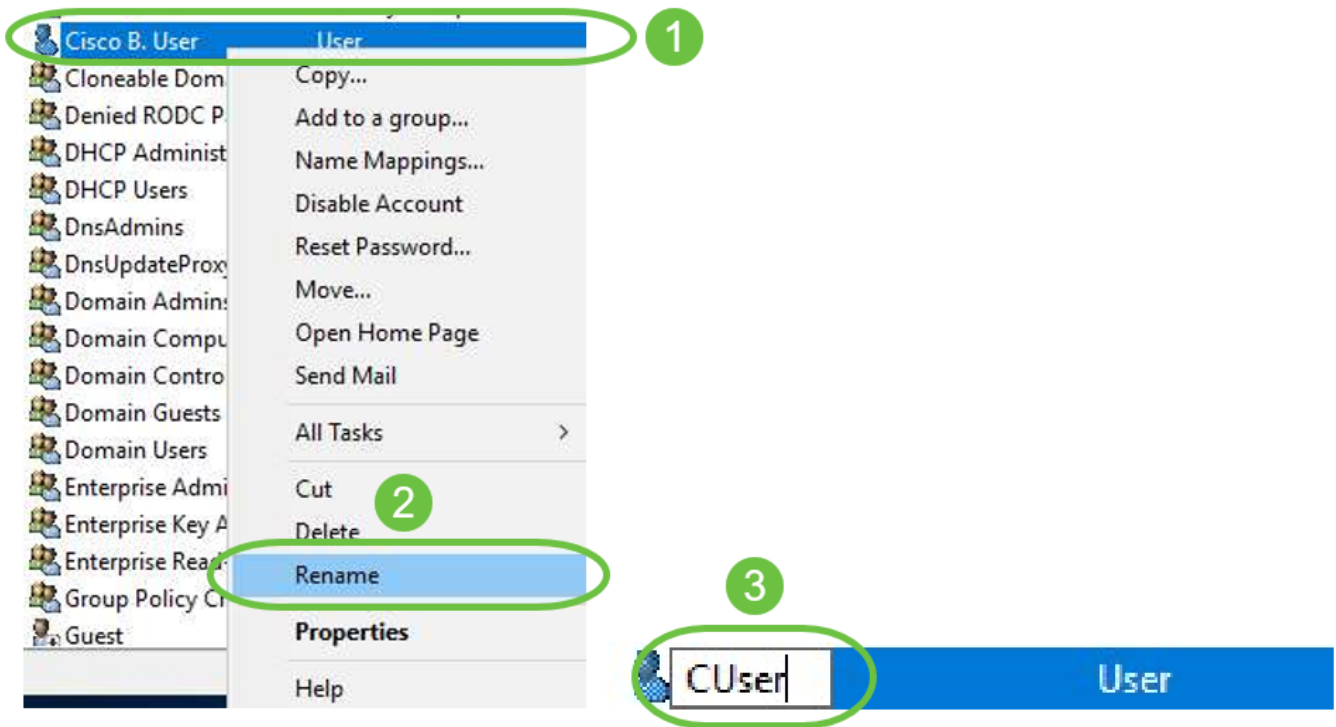
- Fare clic con il pulsante destro del mouse su uno spazio vuoto nel contenitore e selezionare **Nuovo > Utente**.
- Immettere *Nome, Cognome*.
- Immettere il *nome di accesso dell'utente*.
- Fare clic su **Next** (Avanti).



Verrà richiesto di immettere una password per l'utente. Se la casella di controllo *Cambiamento obbligatorio password all'accesso successivo* è selezionata, l'utente dovrà eseguire l'accesso localmente e cambiare la password PRIMA di accedere in remoto.

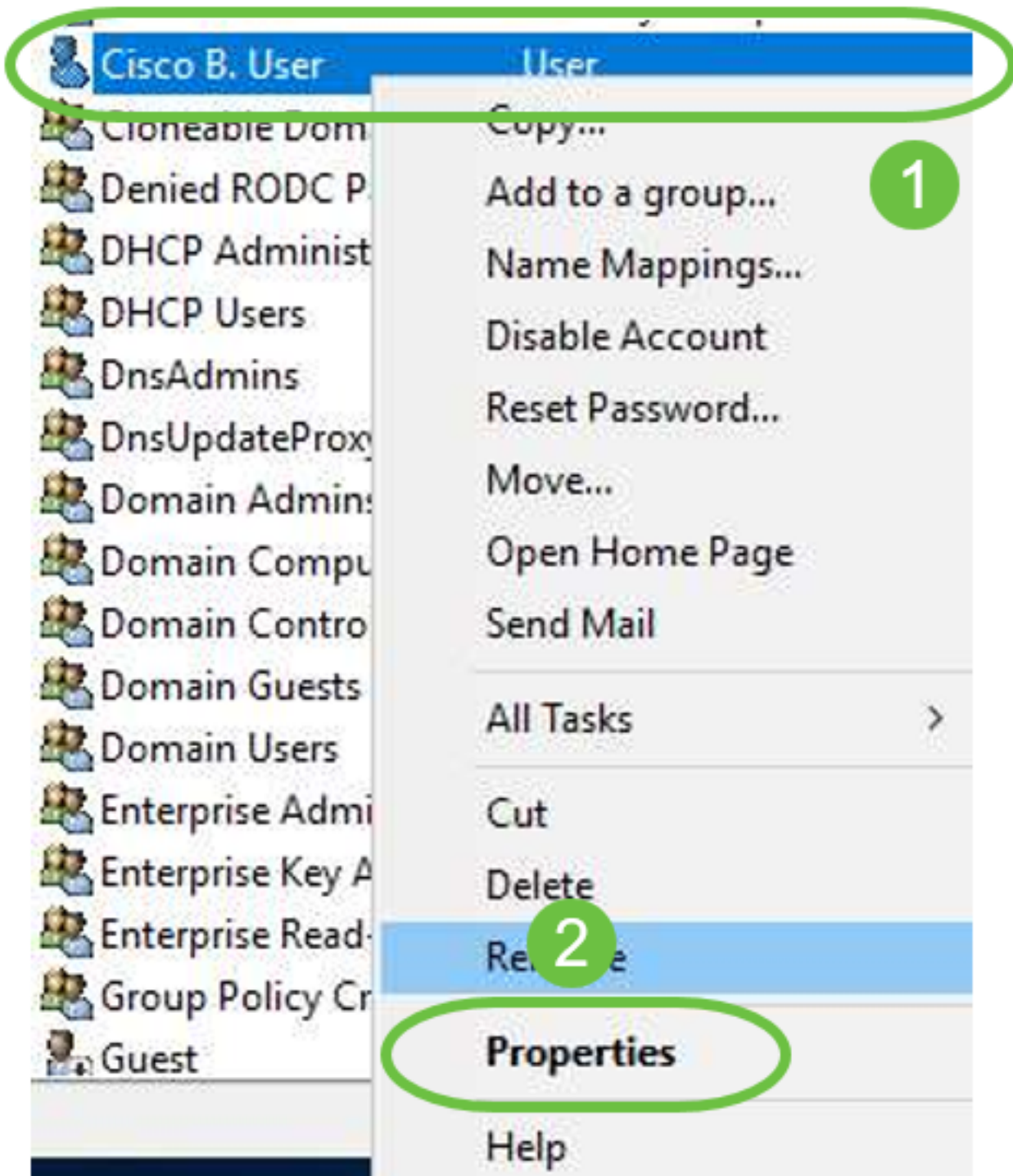
Fare clic su **Finish** (Fine).

Se sono già stati creati account utente da utilizzare, potrebbe essere necessario apportare modifiche. Per modificare il nome canonico di un utente, selezionare l'utente, fare clic con il pulsante destro del mouse e selezionare **Rinomina**. Assicurarsi che tutti gli spazi vengano rimossi e che corrispondano al Nome di accesso dell'utente. Il nome visualizzato dell'utente NON verrà modificato. Fare clic su **OK**.



Passaggio 5. Una volta strutturati correttamente gli account utente, è necessario concedere loro i diritti di accesso remoto.

A tale scopo, selezionare l'account utente, fare clic con il pulsante destro del mouse e selezionare **Proprietà**.



Nella scheda *Proprietà utente* selezionare **Editor attributi** e scorrere verso il basso fino a *distinguishedName*. Assicurarsi che il primo *CN=* abbia il nome di accesso utente corretto senza spazi.

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 2	

Attributes:

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

Selezionare la scheda **Membro di** e fare clic su **Aggiungi**.

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	

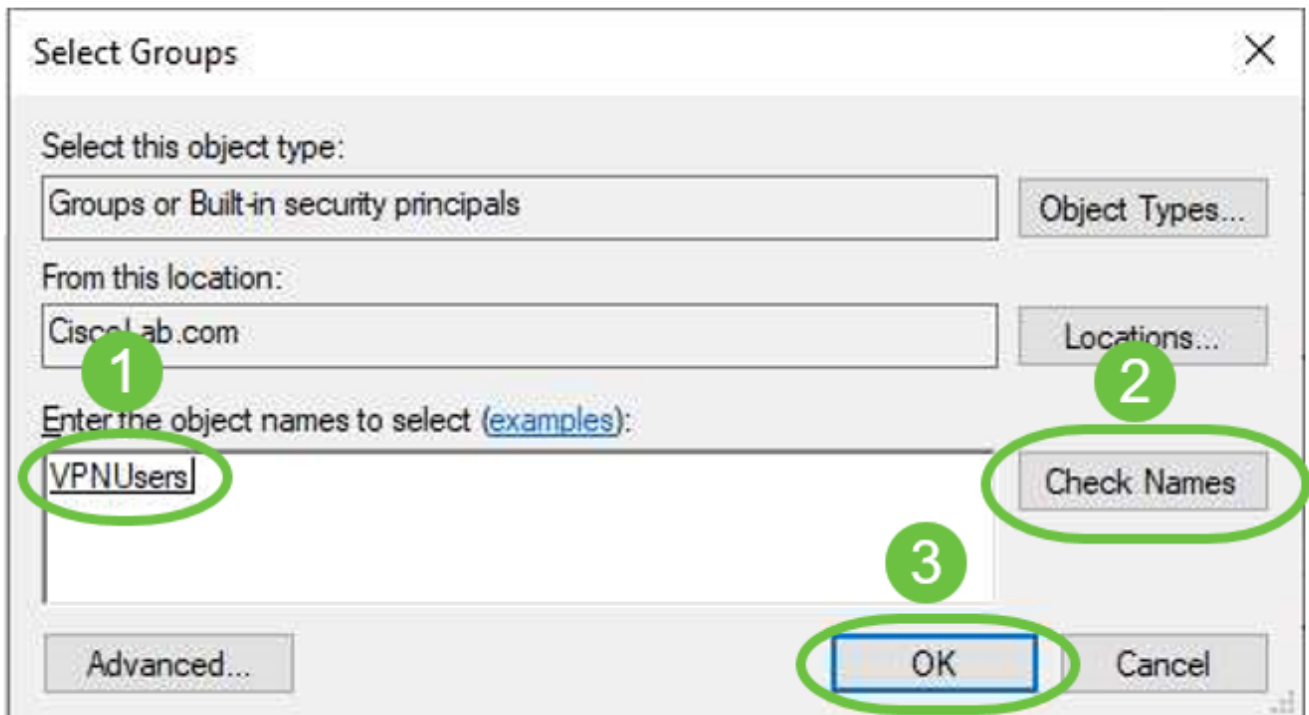
Member of:

Name	
Domain Users	CiscoLab.com/Users

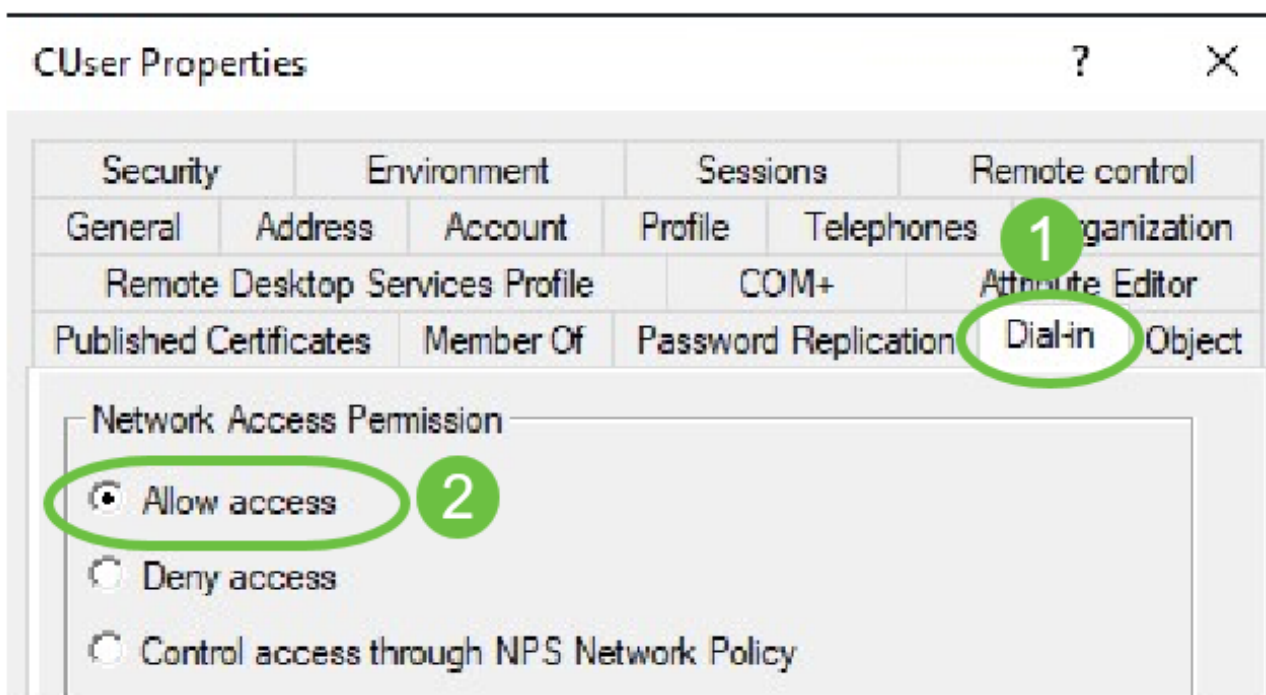
2

Add... Remove

Immettere il nome del *gruppo di sicurezza globale* e selezionare **Controlla nome**. Se la voce è sottolineata, fare clic su **OK**.



Selezionare la scheda **Dial-In**. Nella sezione *Autorizzazioni di accesso alla rete*, selezionare **Consenti accesso**, quindi lasciare le altre opzioni predefinite.



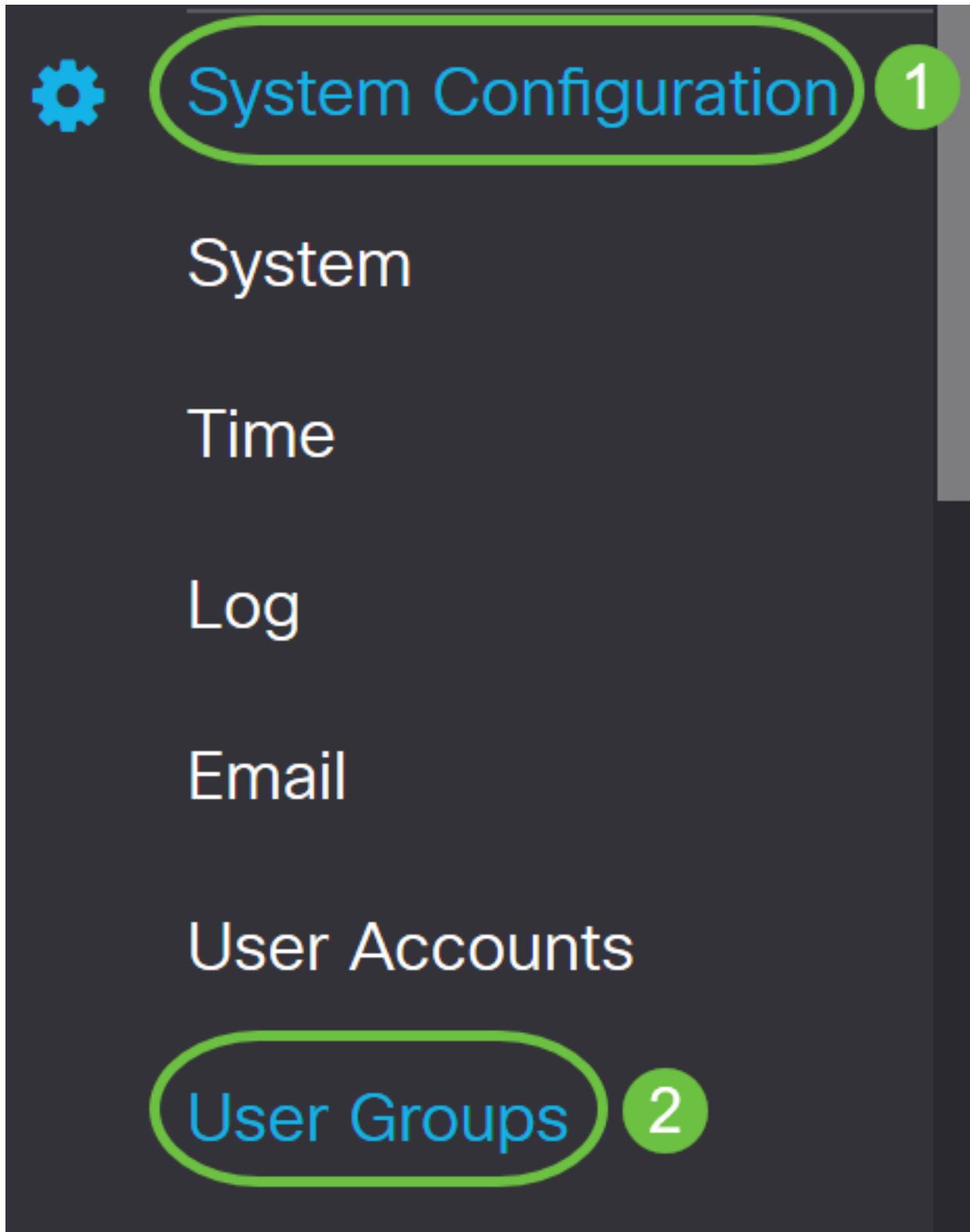
Integrazione con Active Directory

Active Directory richiede che l'ora del router RV34x corrisponda a quella del server AD. Per la procedura di configurazione delle impostazioni temporali su un router serie RV34x, fare clic [qui](#).

Active Directory richiede inoltre che RV340 disponga di un gruppo di utenti corrispondente al

gruppo di sicurezza globale AD.

Passaggio 1. Passare a **Configurazione di sistema > Gruppi di utenti**.



Passaggio 2. Fare clic sull'icona **più** per aggiungere un gruppo di utenti.

User Groups

User Groups Table



Passaggio 3. Inserire il *nome* del *gruppo*. Nell'esempio, questo valore è **VPNUsers**.

Group Name:

Il nome del gruppo deve corrispondere esattamente al gruppo di sicurezza globale di Active Directory.

Passaggio 4. In *Servizi*, *Accesso Web/NETCONF/RESTCONF* deve essere contrassegnato come **Disabilitato**. Se l'integrazione AD non funziona immediatamente, sarà comunque possibile accedere alla RV34x.

Services

Web Login/NETCONF/RESTCONF Disabled Read Only Administrator



Passaggio 5. È possibile aggiungere i tunnel VPN che utilizzeranno l'integrazione AD per accedere ai relativi utenti.



1. Per aggiungere una VPN da client a sito già configurata, andare alla sezione *EZVPN/terze*

parti e fare clic sull'icona **più**. Selezionare il profilo VPN dal menu a discesa e fare clic su **Aggiungi**.


EzVPN/3rd Party


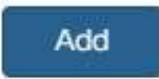

EzVPN/3rd Party Profile Member In-use Table

 **Group Name** 



Add Feature List

Select a Profile: ShrewVPN 

4. VPN SSL: se verrà utilizzato un tunnel VPN SSL, selezionare il criterio dal menu a discesa accanto a *Seleziona un profilo*.

SSL VPN

Select a Profile  SSLVPNDefaultPolicy 

6. PPTP/L2TP/802.1x: per consentire l'utilizzo di Active Directory da parte di questi utenti, è sufficiente selezionare la casella di controllo accanto a essi per *Autorizzare*.

PPTP VPN

Permit

L2TP

Permit

802.1x

Permit

Passaggio 6. Fare clic su **Applica** per salvare le modifiche.

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 ▼

PPTP VPN

Permit

L2TP

Permit

802.1x

Permit

Impostazioni integrazione Active Directory

Passaggio 1. Passare a **Configurazione di sistema > Account utente**.



System Configuration

System

1

Time

Log

Email

User Accounts

2

Passaggio 2. Nella tabella Servizio di autenticazione remota fare clic su **Aggiungi** per creare una voce.

Remote Authentication Service Table



Enable ⇅

Name ⇅

Passaggio 3. Nel campo *Nome*, creare un nome utente per l'account. Nell'esempio viene utilizzato *Jorah_Admin*.

Add/Edit New Domain

Name

Jorah_Admin

Passaggio 4. Dal menu a discesa *Tipo di autenticazione*, scegliere **Active Directory**. AD viene utilizzato per assegnare criteri estesi a tutti gli elementi della rete, distribuire programmi a molti computer e applicare aggiornamenti critici a un'intera organizzazione.

Authentication Type

Active Directory

AD Domain Name

RADIUS

Active Directory

Primary Server

LDAP

Passaggio 5. Nel campo *Nome dominio AD*, immettere il nome di dominio completo di AD.

Nell'esempio viene usato **sampledomain.com**.

AD Domain Name

Passaggio 6. Nel campo *Server primario*, immettere l'indirizzo di Active Directory.

nell'esempio viene usato **192.168.2.122**.

Primary Server Port

Passaggio 7. Nel campo *Porta*, immettere un numero di porta per il server principale.

Nell'esempio, il numero di porta è **1234**.

Primary Server Port

Passaggio 8. (Facoltativo) Nel campo *Percorso contenitore utenti*, immettere un percorso radice in cui sono contenuti gli utenti.

Nota: Nell'esempio viene utilizzato **file:Documents/manage/containers**.

User Container Path

Passaggio 9. Fare clic su **Applica**.

User Accounts

Add/Edit New Domain

Name

Authentication Type

AD Domain Name

Primary Server Port

User Container Path

Passaggio 10. Scorrere fino alla *sequenza di autenticazione del servizio* per impostare il metodo

di login per le varie opzioni.

- Web Login/NETCONF/RESTCONF - Ecco come accedere al router RV34x. Deselezionare la casella di controllo *Utilizza predefinito* e impostare il metodo Primary su **Local DB**. In questo modo, l'utente non verrà disconnesso dal router anche se l'integrazione di Active Directory non riesce.
- VPN da sito a sito/EzVPN&VPN da client a sito di terze parti - Consente di impostare il tunnel VPN da client a sito per l'utilizzo di AD. Deselezionare la casella di controllo *Utilizza predefinito* e impostare il metodo Primary su **Active Directory** e il metodo secondario su **DB locale**.

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

Passaggio 11. Fare clic su **Applica**.

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

Passaggio 12. Salvare la configurazione in esecuzione nella configurazione di avvio.

Le impostazioni di Active Directory su un router serie RV34x sono state configurate correttamente.

LDAP

Passaggio 1. Nella tabella Servizio di autenticazione remota fare clic su **Aggiungi** per creare una voce.

Remote Authentication Service Table



Enable ⇅

Name ⇅

Passaggio 2. Nel campo *Nome*, creare un nome utente per l'account.

È possibile configurare un solo account utente remoto in LDAP.

Nell'esempio viene utilizzato Dany_Admin.

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

Passaggio 3. Dal menu a discesa Tipo di autenticazione, scegliere **LDAP**. Lightweight Directory Access Protocol è un protocollo di accesso utilizzato per accedere a un servizio directory. Si tratta di un server remoto che esegue un server di directory per eseguire l'autenticazione per il dominio.

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"/>

Passaggio 4. Nel campo *Server primario*, immettere l'indirizzo del server LDAP.

nell'esempio viene usato 192.168.7.122.

Primary Server Port

Passaggio 5. Nel campo *Porta*, immettere un numero di porta per il server principale.

Nell'esempio, il numero di porta è **122**.

Primary Server Port

Passaggio 6. Immettere il nome distinto di base del server LDAP nel campo *DN di base*. Il DN di base è la posizione in cui il server LDAP cerca gli utenti quando riceve una richiesta di autorizzazione. Questo campo deve corrispondere al DN di base configurato nel server LDAP.

Nell'esempio viene utilizzato **Dept101**.

Base DN

Passaggio 7. Fare clic su **Applica**. Verrà visualizzata la tabella Servizio di autenticazione remota.



User Accounts

Add/Edit New Domain

Name:

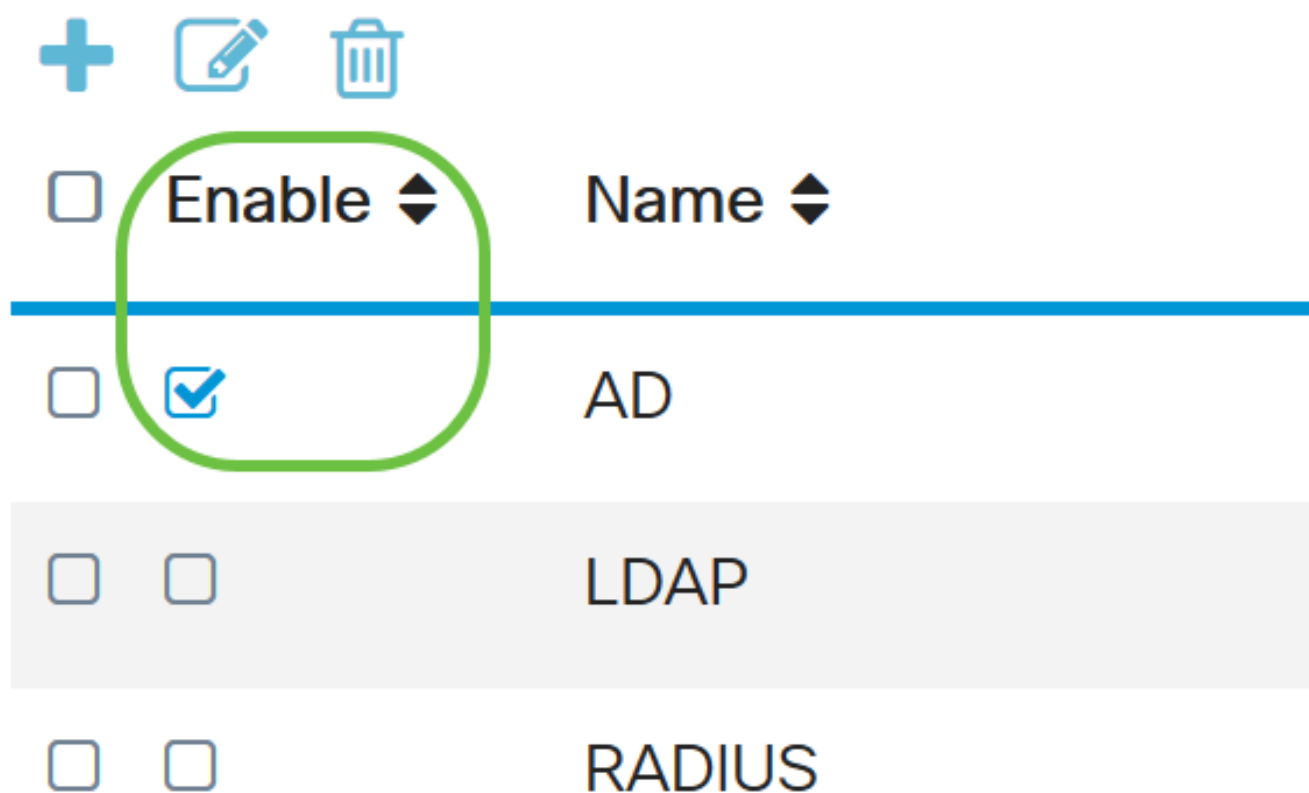
Authentication Type:



Primary Server: Port:

Base DN:

Passaggio 8. (Facoltativo) Se si desidera attivare o disattivare il servizio di autenticazione remota, selezionare o deselezionare la casella di controllo accanto al servizio che si desidera attivare o disattivare.

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

Passaggio 9. Fare clic su **Applica**.

User Accounts

Apply

La configurazione del protocollo LDAP su un router serie RV34x è stata completata.

Qui è disponibile un video relativo a questo articolo...

[Fare clic qui per visualizzare altre Tech Talks di Cisco](#)