

# Configurar e gerenciar contas de usuário em um roteador RV34x Series

## Objetivo

O objetivo deste artigo é mostrar a você como configurar e gerenciar as contas de usuário local e remoto em um RV34x Series Router. Isso inclui como configurar a complexidade de senha de usuários locais, configurar/editar/importar usuários locais, configurar o serviço de autenticação remota usando RADIUS, Ative Directory e LDAP.

## Dispositivos aplicáveis | Versão do firmware

- Série RV34x | 1.0.01.16 ([Baixe o mais recente](#))

## Introduction

O RV34x Series Router fornece contas de usuário para exibir e administrar configurações. Os usuários podem ser de grupos diferentes ou pertencer a grupos lógicos de Redes virtuais privadas (VPN - Virtual Private Networks) SSL (Secure Sockets Layer) que compartilham o domínio de autenticação, a rede local (LAN) e as regras de acesso a serviços e as configurações de timeout de ociosidade. O gerenciamento de usuários define que tipo de usuário pode utilizar um determinado tipo de instalação e como isso pode ser feito.

A prioridade externa do banco de dados é sempre RADIUS (Remote Authentication Dial-In User Service)/LDAP (Lightweight Directory Access Protocol)/AD (Ative Directory)/Local. Se você adicionar o servidor RADIUS ao roteador, o serviço de login da Web e outros serviços usarão o banco de dados externo RADIUS para autenticar o usuário.

Não há opção para habilitar um banco de dados externo somente para o serviço de login da Web e configurar outro banco de dados para outro serviço. Depois que o RADIUS for criado e ativado no roteador, ele usará o serviço RADIUS como um banco de dados externo para Web Login, Site to Site VPN, EzVPN/3rd Party VPN, SSL VPN, Point-to-Point Transport Protocol (PPTP)/Layer 2 Transport Protocol (L2TP) VPN e 802.1x.

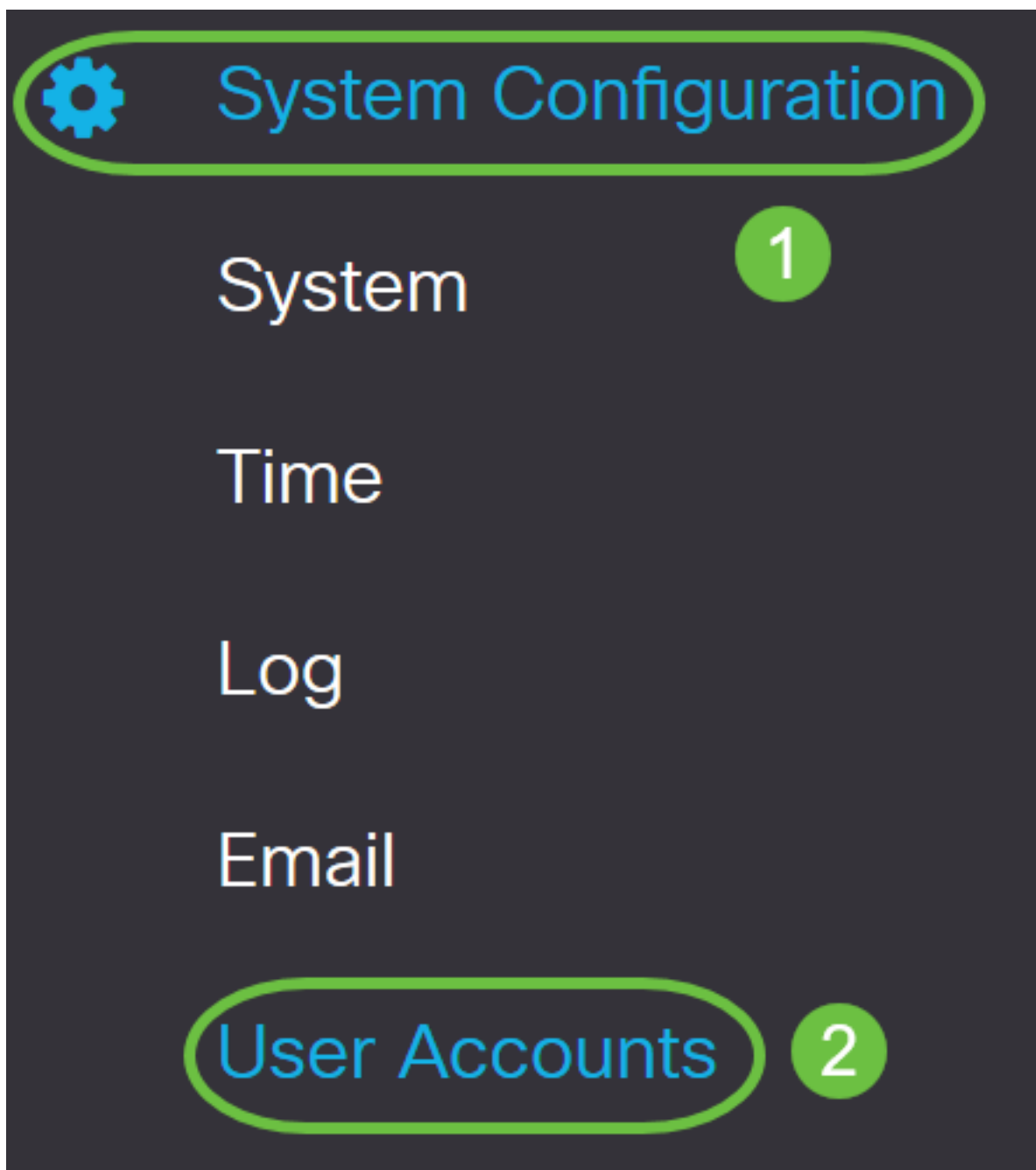
## Table Of Contents

- [Configurar uma conta de usuário local](#)
- [Complexidade de senha de usuários locais](#)
- [Configurar usuários locais](#)
- [Editar usuários locais](#)
- [Importar usuários locais](#)
- [Configurar serviço de autenticação remota](#)
- [RADIUS](#)
- [Configuração do Ative Directory](#)
- [Integração com o Ative Directory](#)
- [Configurações de integração do Ative Directory](#)
- [LDAP](#)

# Configurar uma conta de usuário local

## Complexidade de senha de usuários locais

Etapa 1. Faça login no utilitário baseado na Web do roteador e escolha **Configuração do sistema** > **Contas de usuário**.



Etapa 2. Marque a caixa de seleção **Enable Password Complexity Settings** para ativar os parâmetros de complexidade de senha.

Se esta opção estiver desmarcada, vá para [Configurar usuários locais](#).

# Local Users Password Complexity

Password Complexity Settings:



Enable

Etapa 3. No campo *Tamanho mínimo da senha*, insira um número que varie de 0 a 127 para definir o número mínimo de caracteres que uma senha deve conter. O padrão é 8.

Para este exemplo, o número mínimo de caracteres é definido como 10.

## Local Users Password Complexity

Password Complexity Settings:



Enable

Minimal password length:

10

(Range: 0 - 127, Default: 8)

Etapa 4. No campo *Número mínimo de classes de caracteres*, insira um número de 0 a 4 para definir a classe. O número inserido representa o número mínimo ou máximo de caracteres das diferentes classes:

- A senha é composta por caracteres maiúsculos (ABCD).
- A senha é composta por caracteres minúsculos (abcd).
- A senha é composta por caracteres numéricos (1234).
- A senha é composta por caracteres especiais (!@#\$).

Neste exemplo, 4 é usado.

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

Etapa 5. Marque a caixa de seleção **Habilitar** para a nova senha deve ser diferente da atual.

## 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

Etapa 6. No campo *Password Aging Time*, insira o número de dias (0 a 365) para a expiração da senha. Neste exemplo, **180** dias foram inseridos.

## 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)

Agora você configurou com êxito as configurações de Complexidade de Senha de Usuários Locais no roteador.

## Configurar usuários locais

Etapa 1. Na tabela Lista de associação de usuário local, clique em **Adicionar** para criar uma nova conta de usuário. Você será levado à página Adicionar conta de usuário.

# 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

No cabeçalho *Adicionar conta de usuário*, os parâmetros definidos nas etapas Complexidade da senha local são exibidos.

# 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

Etapa 2. No campo *Nome de usuário*, insira um nome de usuário para a conta.


Neste exemplo, **Administrator\_Noah** é usado.

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"/>	

Etapa 3. No campo *Nova senha*, insira uma senha com os parâmetros definidos. Neste exemplo, o comprimento mínimo da senha deve ser composto de 10 caracteres com uma combinação de letras maiúsculas, minúsculas, numéricas e caracteres especiais.

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"/>	

Etapa 4. No campo *Nova confirmação de senha*, digite novamente a senha para confirmá-la. Um texto ao lado do campo aparecerá se as senhas não coincidirem.

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"/>	▼


O Password Strength Meter (Medidor de força da senha) é alterado dependendo da força da sua senha.



Etapa 5. Na lista suspensa *Grupo*, escolha um grupo para atribuir um privilégio a uma conta de usuário. As opções são:

- admin - Privilégios de leitura e gravação.
- convidado - Privilégios somente leitura.

Para este exemplo, **admin** é escolhido.

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"/>	

Etapa 6. Clique em 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"/>	▼

Você agora configurou com êxito a Associação de usuário local em um roteador RV34x Series.

## Editar usuários locais

Etapa 1. Marque a caixa de seleção ao lado do nome de usuário local na tabela Lista de associação de usuário local.

Para este exemplo, **Administrator\_Noah** é escolhido.



# 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

Etapa 2. Clique em **Editar**.

# 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

O nome de usuário não pode ser editado.

Etapa 3. No campo *Senha antiga*, digite a senha que foi configurada anteriormente para a conta de usuário local.

## Edit User Account

User Name

Old Password

Etapa 4. No campo *Nova senha*, digite uma nova senha. A nova senha deve atender aos requisitos mínimos.

## Edit User Account

User Name

Old Password

New Password

( Range: 0 - 127 )

Etapa 5. Insira a nova senha novamente no campo *Nova confirmação de senha* para confirmá-la. Essas senhas devem corresponder.

## Edit User Account

User Name

Old Password

New Password

( Range: 0 - 127 )

New Password Confirm

Etapa 6. (Opcional) Na lista suspensa Grupo, escolha um grupo para atribuir um privilégio a uma conta de usuário.

Neste exemplo, **convidado** é escolhido.

## Edit User Account

User Name

Old Password

New Password

( Range: 0 - 127 )

New Password Confirm

Group

admin

guest

Passo 7. Clique em Apply.

User Accounts

Apply

Cancel

## Edit User Account

User Name

Old Password

New Password

( Range: 0 - 127 )

New Password Confirm

Group

Agora você deve ter editado com êxito uma conta de usuário local.

# 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

## Importar usuários locais



Etapa 1. Na área Importação de usuários locais, clique em  .

Etapa 2. Em Importar nome de usuário e senha, clique em **Procurar...** para importar uma lista de usuários. Normalmente, esse arquivo é uma planilha salva no formato Valor separado por vírgula (.CSV).

Neste exemplo, **user-template.csv** é escolhido.

# Local Users Import

Import User Name & Password

Browse...

user-template.csv

(Import User Name + Password via CSV files)

Import

Download User Template:

Download

Etapa 3. (Opcional) Se você não tiver um modelo, clique em **Download** na área Download User Template.

# Local Users Import

Import User Name & Password

Browse...

user-template.csv

(Import User Name + Password via CSV files)

Import

Download User Template:

Download

Etapa 4. Clique em **Importar**.

# Local Users Import

Import User Name & Password

Browse...

user-template.csv

(Import User Name + Password via CSV files)

Import

Download User Template:

Download

Uma mensagem ao lado do botão importar será exibida informando que a importação foi bem-sucedida.

Agora você importou com êxito uma lista de usuários locais.

## Configurar serviço de autenticação remota

### RADIUS

Etapa 1. Na Tabela de serviços de autenticação remota, clique em **Adicionar** para criar uma entrada.



# Remote Authentication Service Table



Enable ⇅      Name ⇅

Etapa 2. No campo *Nome*, crie um nome de usuário para a conta.

Para este exemplo, é usado **Administrador**.

## Add/Edit New Domain

Name

Administrator

Etapa 3. No menu suspenso Authentication Type (Tipo de autenticação), escolha **RADIUS**. Isso significa que a autenticação do usuário será feita através de um servidor RADIUS.

Somente uma única conta de usuário remoto no RADIUS pode ser configurada.

Authentication Type

RADIUS



RADIUS

Active Directory

LDAP

Primary Server

Backup Server

Etapa 4. No campo *Servidor primário*, insira o endereço IP do servidor RADIUS primário.

Neste exemplo, **192.168.3.122** é usado como o servidor primário.

Primary Server  Port

Etapa 5. No campo *Porta*, insira o número da porta do servidor RADIUS primário.

Para este exemplo, **1645** é usado como o número da porta.

Primary Server  Port

Etapa 6. No campo *Backup Server*, insira o endereço IP do servidor RADIUS de backup. Isso serve como um failover caso o servidor primário fique inoperante.

Neste exemplo, o endereço do servidor de backup é **192.168.4.122**.

Backup Server  Port

Passo 7. No campo *Porta*, digite o número do servidor RADIUS de backup.

Backup Server  Port

Neste exemplo, **1646** é usado como o número da porta.

Etapa 8. No campo *chave pré-compartilhada*, insira a chave pré-compartilhada configurada no servidor RADIUS.

Pre-shared Key

Etapa 9. No campo *Confirmar chave pré-compartilhada*, insira novamente a chave pré-compartilhada para confirmar.

Confirm Pre-shared Key

Etapa 10. Clique em Apply.

## Add/Edit New Domain

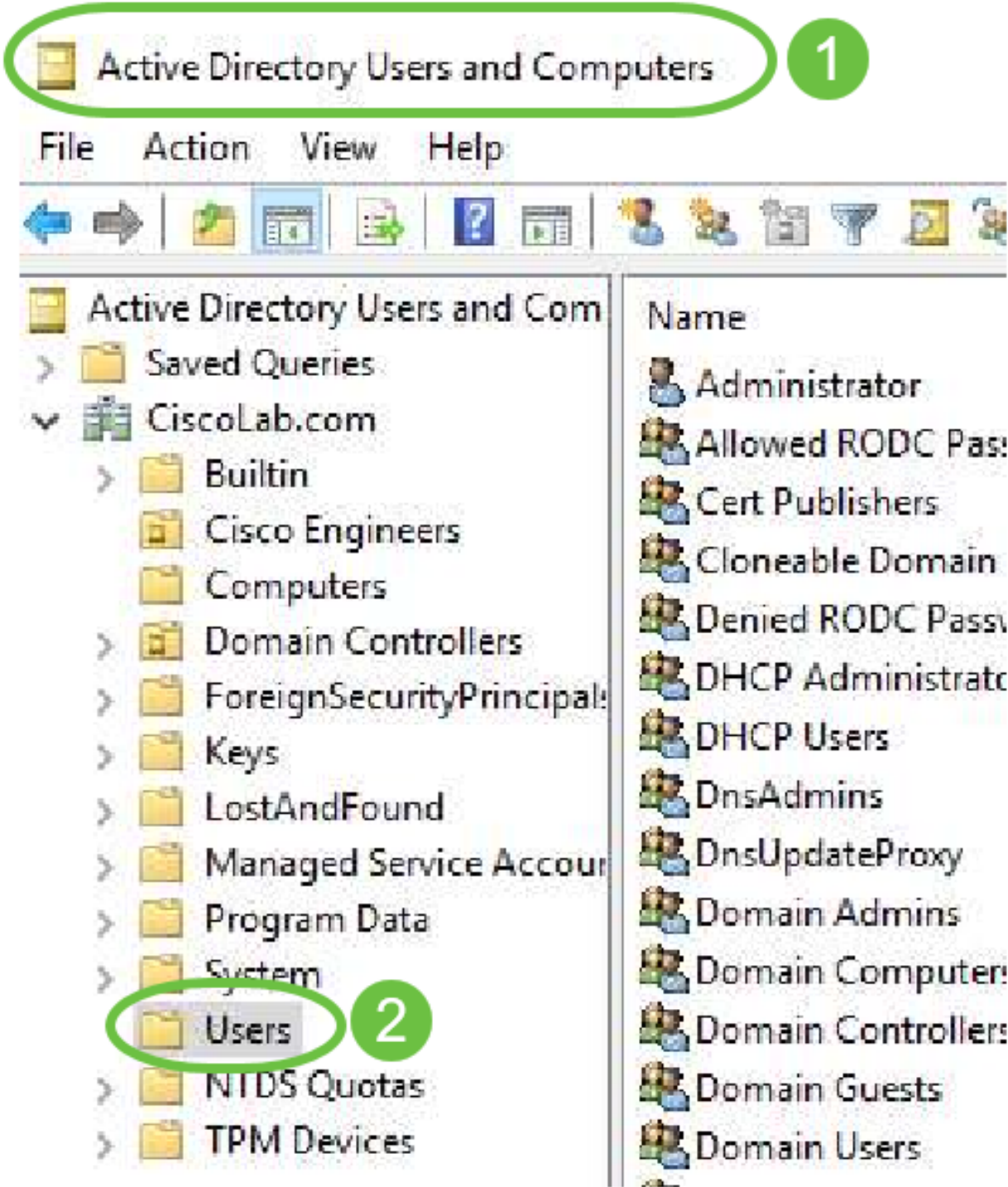
Name	<input type="text" value="Administrator"/>		
Authentication Type	<input type="text" value="RADIUS"/>		
Primary Server	<input type="text" value="192.168.3.122"/>	Port	<input type="text" value="389"/>
Backup Server	<input type="text" value="192.168.4.122"/>	Port	<input type="text" value="389"/>
Pre-shared Key	<input type="password" value="●●●●●●●●"/>		
Confirm Pre-shared Key	<input type="password" value="●●●●●●●●"/>		

Você será levado à página principal da conta de usuário. A conta recentemente configurada aparece agora na tabela Remote Authentication Service.

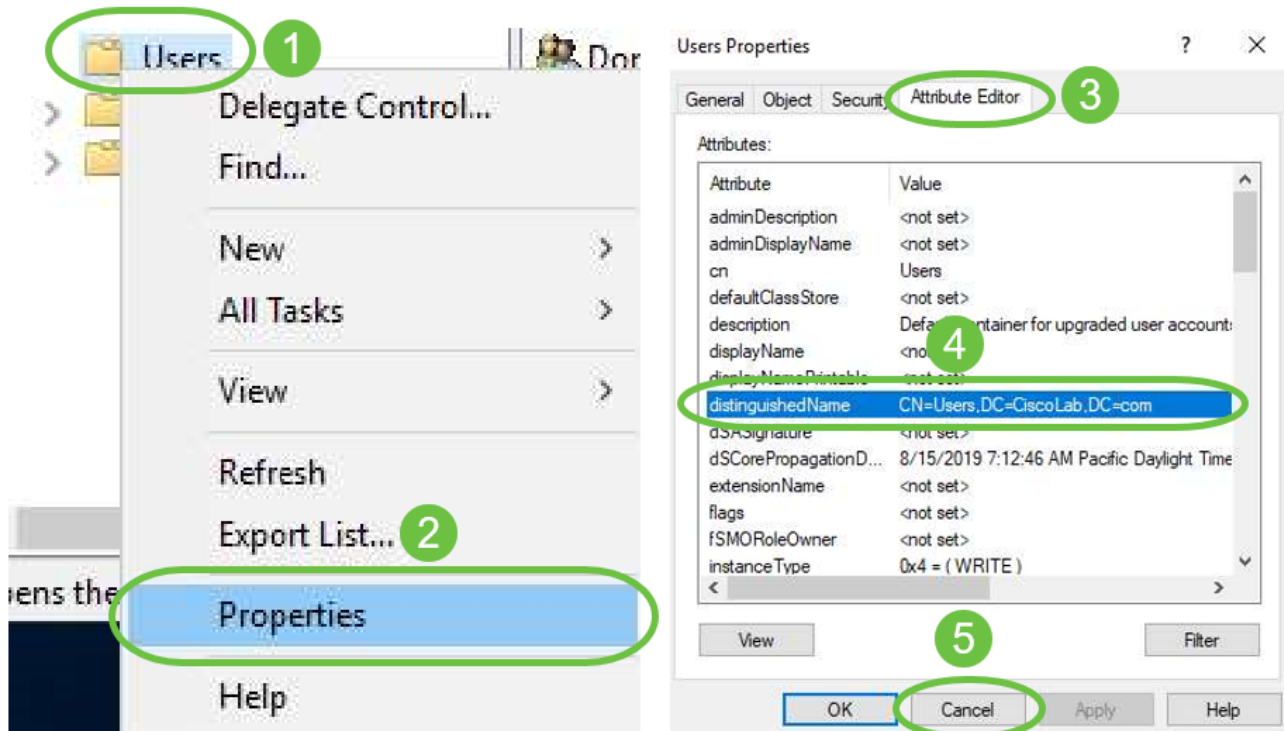
Você agora configurou com êxito a autenticação RADIUS em um RV34x Series Router.

## Configuração do Ative Directory

Etapa 1. Para concluir a configuração do Ative Directory, você precisará estar conectado ao Servidor do Ative Directory. No PC, abra **usuários e computadores do Ative Directory** e navegue até o contêiner que terá as contas de usuário usadas para fazer login remotamente. Neste exemplo, usaremos o contêiner **Usuários**.



Etapa 2. Clique com o botão direito do mouse no contêiner e selecione **Propriedades**. Navegue até a guia *Editor de atributos* e localize o campo *uniqueName*. Se esta guia não estiver visível, você precisará ativar a exibição de recursos avançados em Usuários e computadores do Ative Directory e iniciá-la novamente. Anote este campo e clique em **Cancelar**. Esse será o caminho do contêiner do usuário. Esse campo também será necessário ao configurar o RV340 e deve corresponder exatamente.



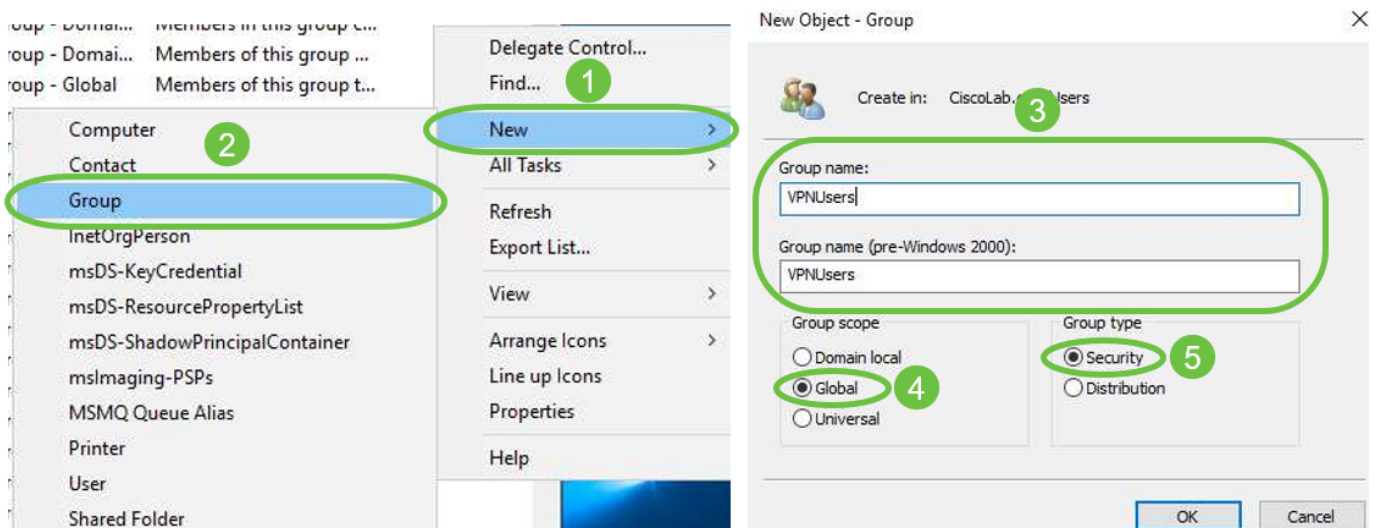
Etapa 3. Crie um Grupo de Segurança Global no mesmo contêiner das Contas de Usuário que serão usadas.

No contêiner selecionado, clique com o botão direito do mouse em uma área em branco e selecione **Novo > Grupo**.

Select the following:

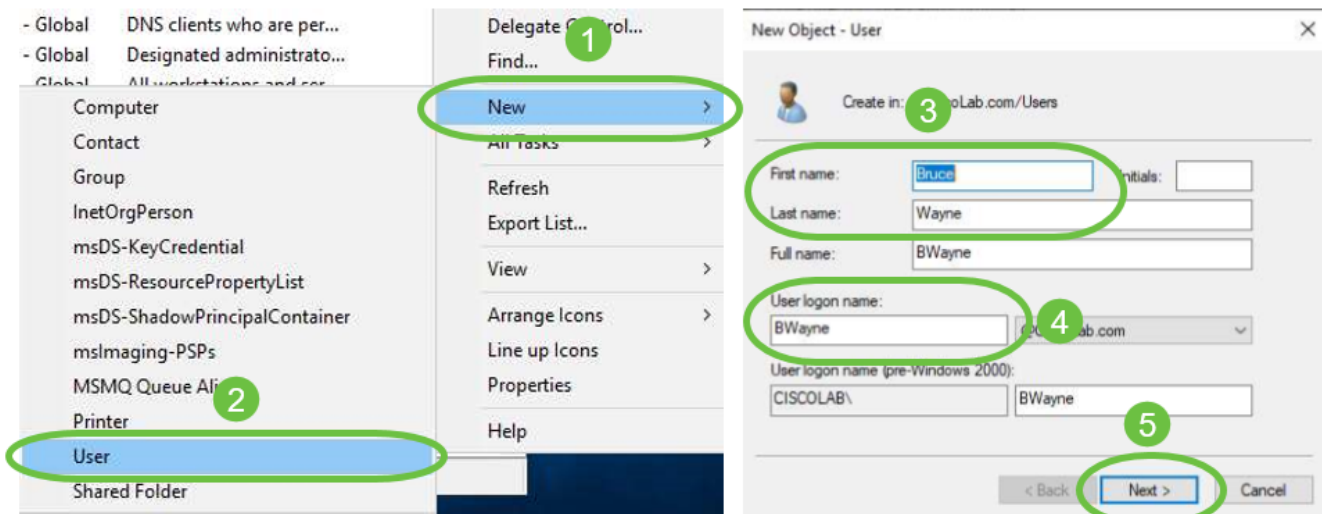
- Nome do grupo - Este nome deverá ser uma correspondência exata com o nome do grupo de usuários criado no RV340. Neste exemplo, usaremos **VPNUsers**.
- Escopo do grupo - Global
- Tipo de grupo - Segurança

Click **OK**.



Etapa 4. Para criar novas contas de usuário, faça o seguinte:

- Clique com o botão direito do mouse em um espaço vazio no Contêiner e selecione **Novo > Usuário**.
- Digite *Nome, Sobrenome*.
- Digite o *Nome de logon do usuário*.
- Clique em Next.

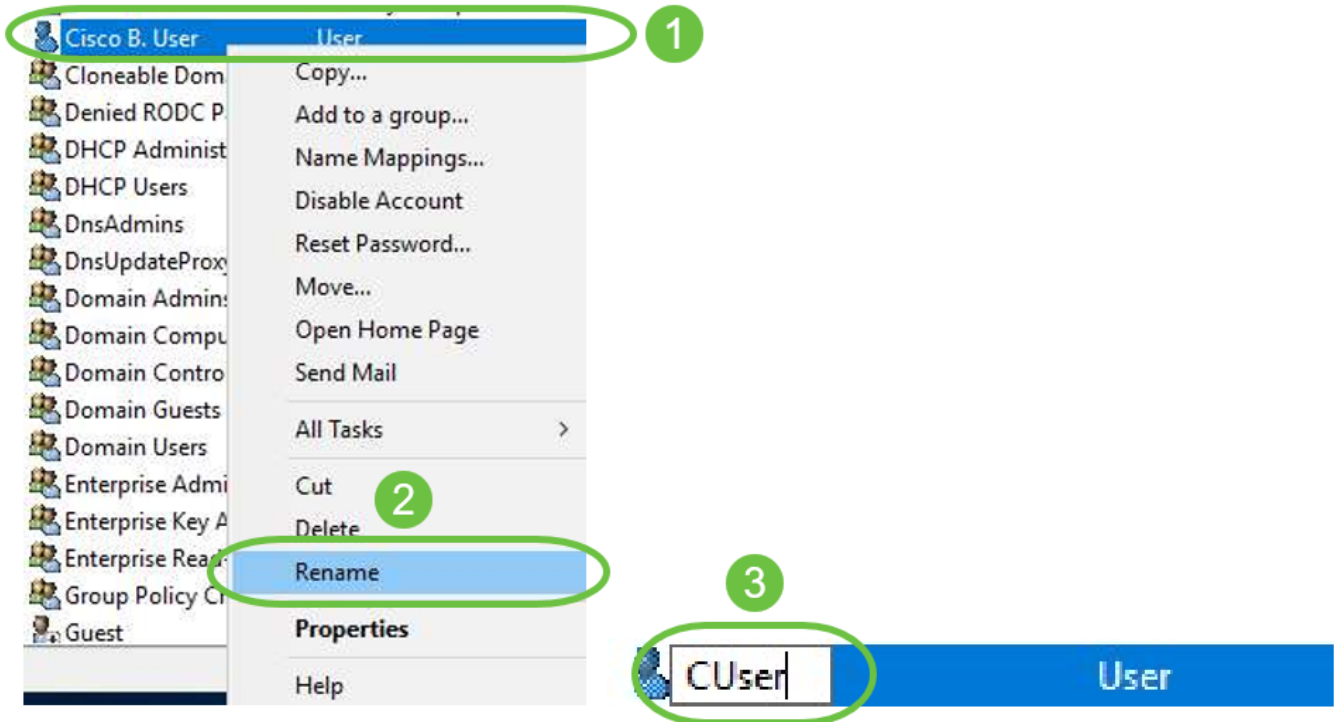


Você será solicitado a inserir uma senha para o usuário. Se o usuário precisar alterar a senha na próxima caixa de login estiver marcada, o usuário terá que fazer login localmente e alterar a senha ANTES de fazer login remotamente.

Clique em Finish.

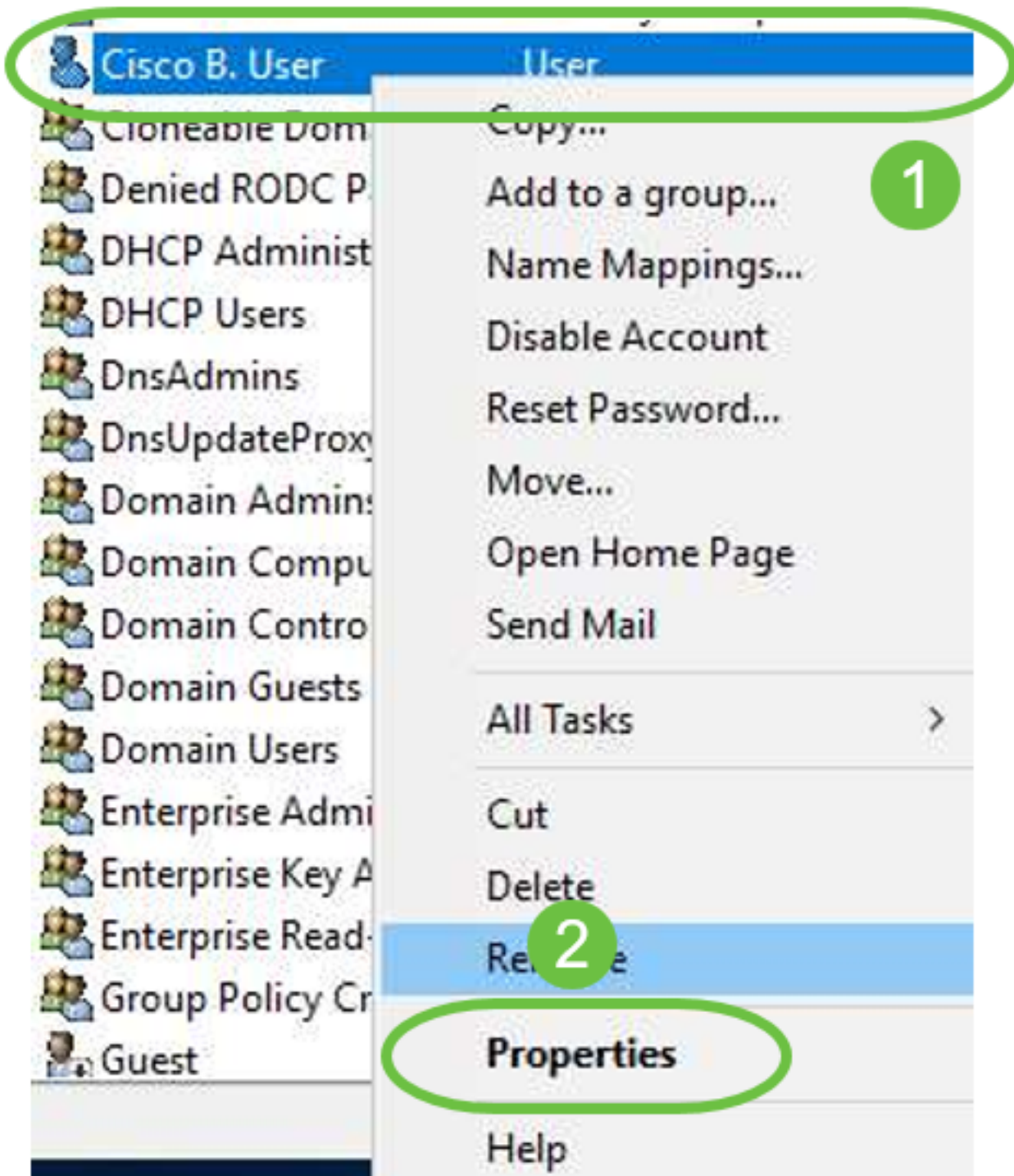
Se já forem criadas contas de usuário que precisam ser usadas, talvez seja necessário fazer ajustes. Para ajustar o nome canônico de um usuário, selecione-o, clique com o botão direito do mouse e selecione **Renomear**. Verifique se todos os espaços foram removidos e se eles correspondem ao Nome de logon do usuário. Isso NÃO alterará o nome de exibição dos usuários. Click **OK**.





Etapa 5. Depois que as contas de usuário forem estruturadas corretamente, precisarão receber direitos para fazer login remotamente.

Para fazer isso, selecione a conta de usuário, clique com o botão direito do mouse e selecione **Propriedades**.



Em *Propriedades do usuário*, selecione a guia **Editor de atributos** e role para baixo até *DistinguishedName*. Certifique-se de que o primeiro *CN=* tem o nome de início de sessão de utilizador correto sem espaços.



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 <b>3</b>
displaynamePrintable	<not set>
distinguishedName	CN=CUser,CN=Users,DC=CiscoLab,DC=com
division	<not set>

Selecione a guia **Membro de** e clique em **Adicionar**.

# 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	

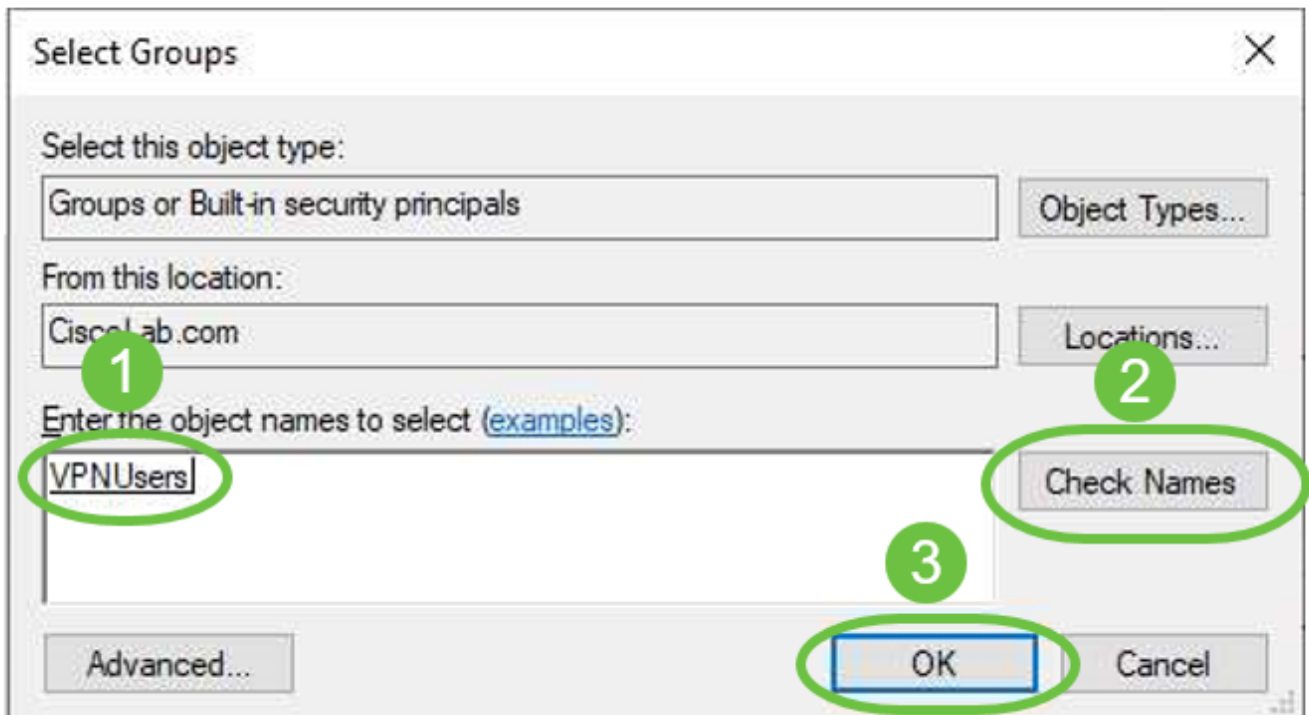
Member of:

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

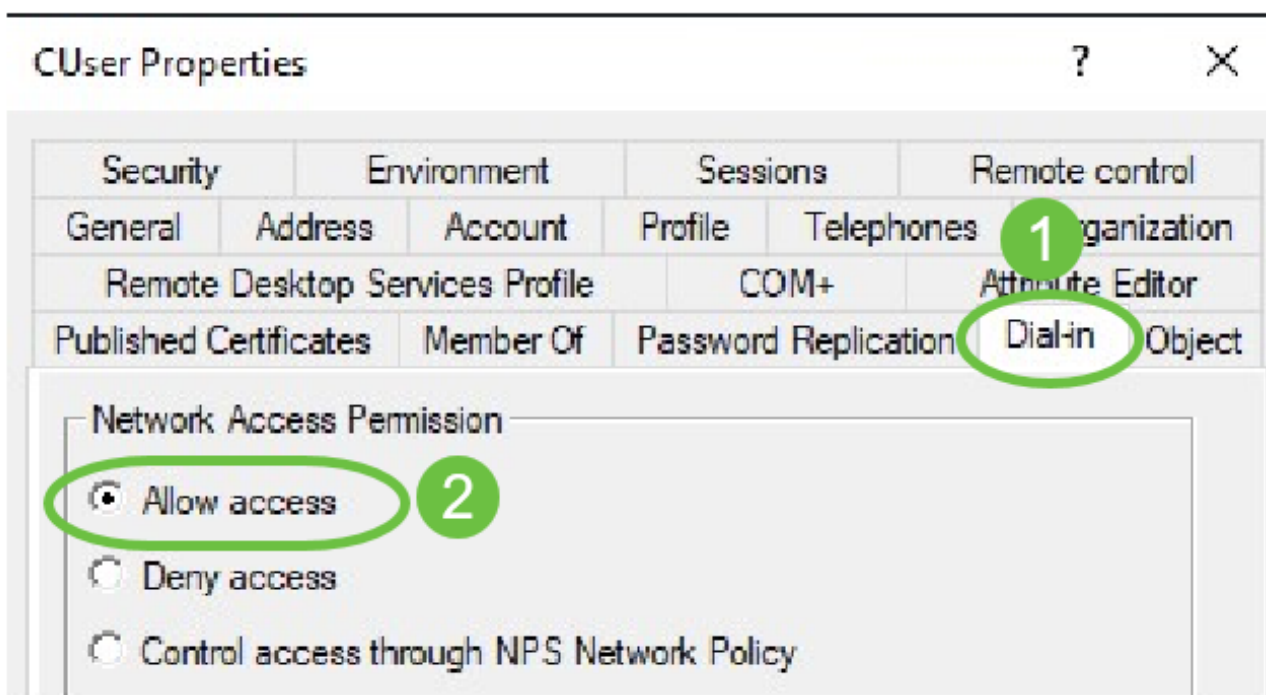
2

Add... Remove

Digite o nome do *Grupo de Segurança Global* e selecione **Verificar nome**. Se a entrada estiver sublinhada, clique em **OK**.



Selecione a guia **Discar**. Na seção *Permissão de Acesso à Rede*, selecione **Permitir Acesso** e deixe o restante como padrão.

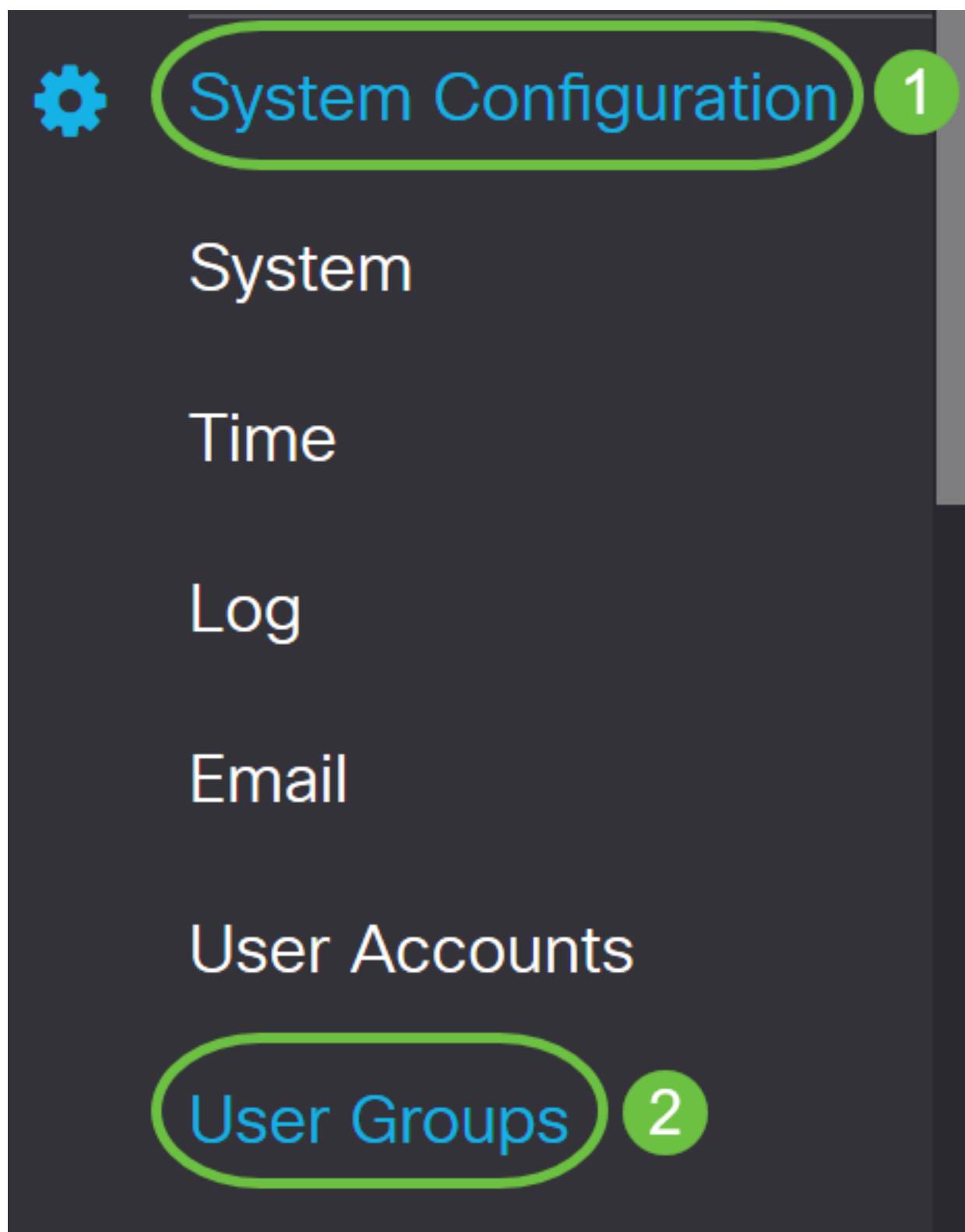


## Integração com o Active Directory

O Active Directory exige que a hora do roteador RV34x corresponda à do servidor AD. Para obter etapas sobre como configurar as configurações de tempo em um roteador RV34x Series, clique [aqui](#).

O AD também exige que o RV340 tenha um Grupo de Usuários que corresponda ao Grupo de Segurança Global do AD.

Etapa 1. Navegue até **Configuração do sistema > Grupos de usuários**.



Etapa 2. Clique no ícone **de mais** para adicionar um grupo de usuários.

# User Groups

## User Groups Table



Etapa 3. Digite o *nome do grupo*. Neste exemplo, são **VPNUsers**.

Group Name:

O nome do grupo deve ser exatamente o mesmo do Grupo de Segurança Global do AD.

Etapa 4. Em *Services*, *Web Login/NETCONF/RESTCONF* deve ser marcado como **Disabled**. Se a Integração do AD não funcionar imediatamente, você ainda poderá acessar o RV34x.

## Services

Web Login/NETCONF/RESTCONF  Disabled  Read Only  Administrator

Etapa 5. Você pode adicionar os túneis VPN que usarão a Integração do AD para registrar seus usuários.

1. Para adicionar uma VPN Cliente a Site que já tenha sido configurada, vá até a seção *EZVPN/Terceiros* e clique no ícone **mais**. Selecione o perfil VPN no menu suspenso e clique em **Adicionar**.

## 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 - Se um túnel SSL VPN for usado, selecione a política no menu suspenso ao lado de *Select a Profile* (*Selecionar um perfil*).

SSL VPN

Select a Profile

SSLVPNDefaultPolicy



6. PPTP/L2TP/802.1x - Para permitir que eles usem o AD, basta clicar na caixa de seleção ao lado deles para *permitir*.

PPTP VPN



Permit

L2TP



Permit

802.1x



Permit

Etapa 6. Clique em **Apply** para salvar suas alterações.

## User Groups

Apply

---

Site to Site VPN Profile Member In-use Table

+ 🗑️

<input type="checkbox"/>	#	Connection Name
--------------------------	---	-----------------

---

EzVPN/3rd Party

EzVPN/3rd Party Profile Member In-use Table

+ 🗑️

<input type="checkbox"/>	#	Group Name
--------------------------	---	------------

---

SSL VPN Select a Profile SSLVPNDefaultPolicy ▾

PPTP VPN  Permit

L2TP  Permit

802.1x  Permit

## Configurações de integração do Active Directory

Etapa 1. Navegue até **Configuração do sistema > Contas de usuário** .



## System Configuration

System

1

Time

Log

Email

User Accounts

2

Etapa 2. Na Tabela de serviços de autenticação remota, clique em **Adicionar** para criar uma entrada.



# Remote Authentication Service Table



Enable ⇅

Name ⇅

Etapa 3. No campo *Nome*, crie um nome de usuário para a conta. Neste exemplo, é usado *Jorah\_Admin*.

## Add/Edit New Domain

Name

Jorah\_Admin

Etapa 4. No menu suspenso *Authentication Type*, escolha **Active Directory**. O AD é usado para atribuir políticas abrangentes a todos os elementos da rede, implantar programas em muitos computadores e aplicar atualizações críticas a toda a organização.

Authentication Type

Active Directory

AD Domain Name

RADIUS

Active Directory

Primary Server

LDAP

Etapa 5. No campo *AD Domain Name*, insira o nome de domínio totalmente qualificado do AD.

Neste exemplo, **sampledomain.com** é usado.

AD Domain Name

Etapa 6. No campo *Servidor primário*, digite o endereço do AD.

Neste exemplo, é usado **192.168.2.122**.

Primary Server  Port

Passo 7. No campo *Porta*, insira um número de porta para o Servidor Primário.

Neste exemplo, **1234** é usado como o número da porta.

Primary Server  Port

Etapa 8. (Opcional) No campo *Caminho do contêiner do usuário*, insira um caminho raiz onde os usuários estão contidos.

**Note:** Neste exemplo, **file:Documents/manage/containers** é usado.

User Container Path

Etapa 9. Clique em Apply.

User Accounts

Add/Edit New Domain

Name

Authentication Type

AD Domain Name

Primary Server  Port

User Container Path

Etapa 10. Role para baixo até *Service Auth Sequence* para definir o método de login para as

várias opções.

- Login na Web/NETCONF/RESTCONF - É assim que você faz login no roteador RV34x. Desmarque a caixa de seleção *Usar padrão* e defina o método principal como **BD local**. Isso garantirá que você não será desconectado do roteador, mesmo se a Integração com o Ative Directory falhar.
- VPN de cliente para site/EzVPN&VPN de terceiros - Esta é a configuração do túnel VPN de cliente para site para usar AD. Desmarque a caixa de seleção *Usar padrão* e defina o método primário como **Ative Directory** e Método secundário como **DB local**.

### 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

Etapa 11. Clique em 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

Etapa 12. Salve sua configuração atual na configuração de inicialização.

Agora você configurou com êxito as configurações do Ative Directory em um RV34x Series Router.

## LDAP

Etapa 1. Na Tabela de serviços de autenticação remota, clique em **Adicionar** para criar uma entrada.

# Remote Authentication Service Table



Enable ⇅

Name ⇅

Etapa 2. No campo *Nome*, crie um nome de usuário para a conta.

Somente uma única conta de usuário remoto no LDAP pode ser configurada.

Neste exemplo, Dany\_Admin é usado.

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

Etapa 3. No menu suspenso Authentication Type (Tipo de autenticação), escolha **LDAP**. O Lightweight Directory Access Protocol é um protocolo de acesso usado para acessar um serviço de diretório. É um servidor remoto que executa um servidor de diretório para executar a autenticação para o domínio.

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

RADIUS

Active Directory

**LDAP**

Etapa 4. No *campo Servidor primário*, insira o endereço do servidor do LDAP.

Neste exemplo, é usado **192.168.7.122**.

Primary Server  Port

Etapa 5. No campo *Porta*, insira um número de porta para o Servidor Primário.

Neste exemplo, **122** é usado como o número da porta.

Primary Server  Port

Etapa 6. Insira o nome diferenciado base do servidor LDAP no campo *DN base*. O DN base é o local onde o servidor LDAP procura usuários quando recebe uma solicitação de autorização. Esse campo deve corresponder ao DN base configurado no servidor LDAP.

Neste exemplo, é usado **Dept101**.

Base DN

Passo 7. Clique em Apply. Você será levado à Tabela de serviços de autenticação remota.



User Accounts

Add/Edit New Domain

Name:

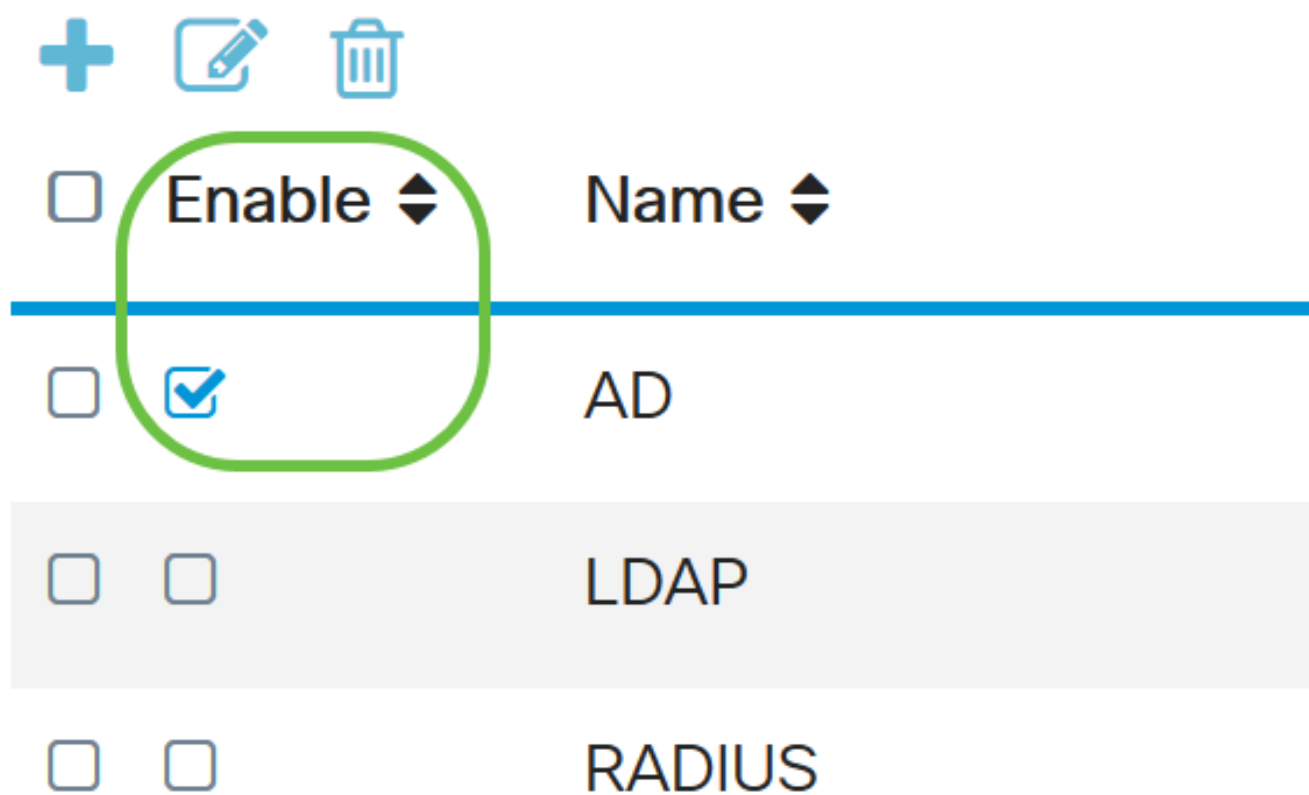
Authentication Type:

Primary Server:  Port:

Base DN:

Etapa 8. (Opcional) Se quiser ativar ou desativar o serviço de autenticação remota, marque ou desmarque a caixa de seleção ao lado do serviço que deseja ativar ou desativar.

# 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 is 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'.

<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

Etapa 9. Clique em Apply.

User Accounts

Apply

Agora você configurou com êxito o LDAP em um RV34x Series Router.

**Exibir um vídeo relacionado a este artigo...**

[Clique aqui para ver outras palestras técnicas da Cisco](#)