

RV34xシリーズルータでのユーザアカウントの設定と管理

目的

この記事の目的は、RV34xシリーズルータでローカルおよびリモートユーザアカウントを設定および管理する方法を説明することです。これには、ローカルユーザのパスワードの複雑度の設定方法、ローカルユーザの設定/編集/インポート、RADIUS、Active Directory、およびLDAPを使用したリモート認証サービスの設定方法が含まれます。

該当するデバイス | ファームウェアのバージョン

- RV34xシリーズ | 1.0.01.16 (最新の[ダウンロード](#))

概要

RV34xシリーズルータは、設定を表示および管理するためのユーザアカウントを提供します。ユーザは、異なるグループのユーザにすることも、認証ドメイン、ローカルエリアネットワーク(LAN)、サービスアクセスルール、およびアイドルタイムアウト設定を共有するSecure Sockets Layer(SSL)仮想プライベートネットワーク(VPN)の論理グループに属することもできます。ユーザ管理は、特定のタイプの機能を利用できるユーザのタイプと、その方法を定義します。

外部データベースの優先順位は、常にRemote Authentication Dial-In User Service(RADIUS)/Lightweight Directory Access Protocol(LDAP)/Active Directory(AD)/Localです。ルータにRADIUSサーバを追加すると、Webログインサービスやその他のサービスは、RADIUS外部データベースを使用してユーザを認証します。

Webログインサービス専用の外部データベースを有効にし、別のサービス用に別のデータベースを設定するオプションはありません。ルータでRADIUSが作成され、有効になると、ルータはRADIUSサービスをWebログイン、サイト間VPN、EzVPN/3rd Party VPN、SSL VPN、Point-to-Point Transport Protocol(PPTP)/レイヤ2 Transport Protocol(L2TP) VPN)、および802.1x

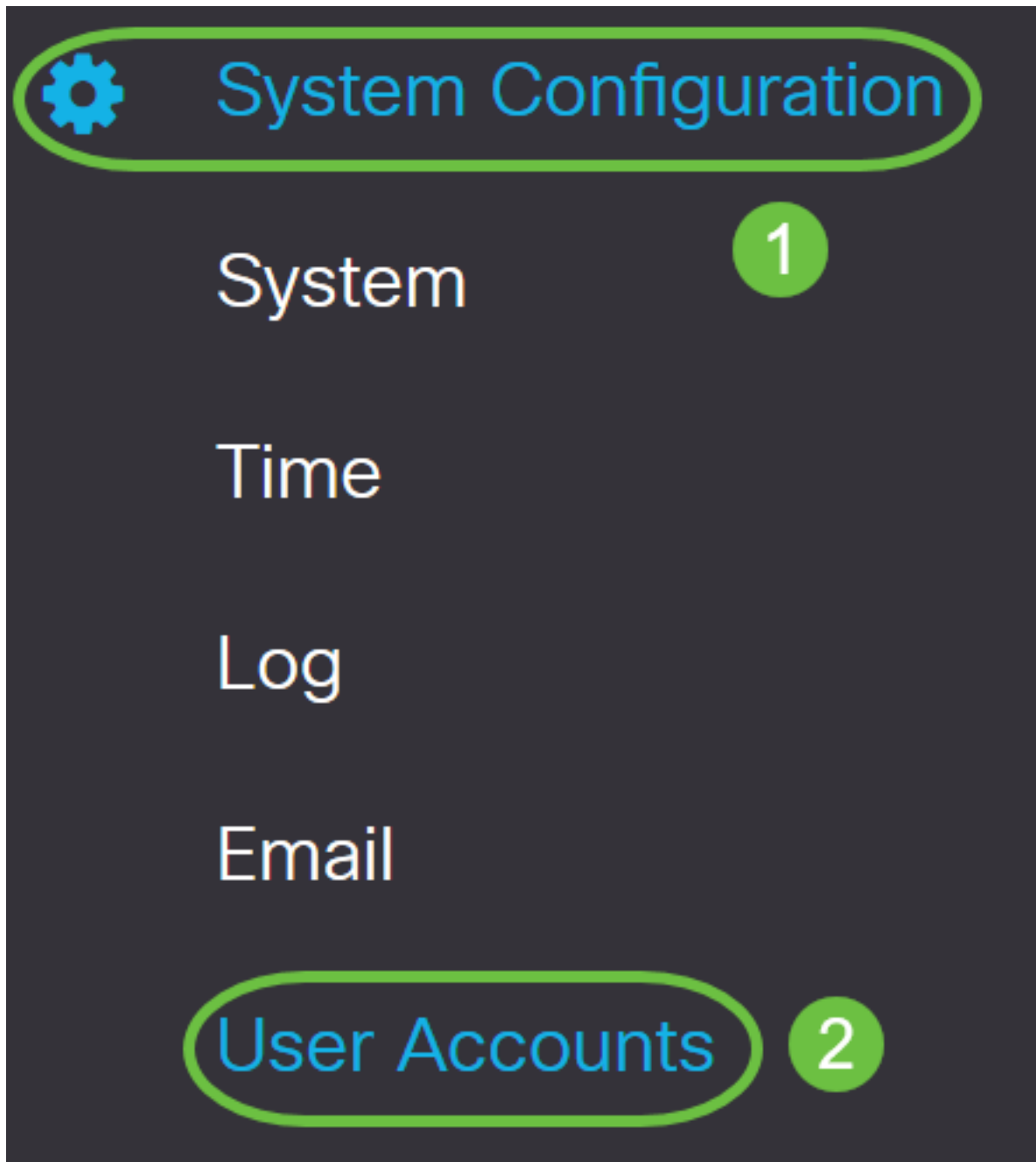
目次

- [ローカルユーザアカウントの設定](#)
- [ローカルユーザのパスワードの複雑度](#)
- [ローカルユーザの設定](#)
- [ローカルユーザの編集](#)
- [ローカルユーザのインポート](#)
- [リモート認証サービスの設定](#)
- [RADIUS](#)
- [Active Directoryの設定](#)
- [Active Directory統合](#)
- [Active Directory統合設定](#)
- [\[LDAP\]](#)

ローカルユーザアカウントの設定

ローカルユーザのパスワードの複雑度

ステップ1：ルータのWebベースのユーティリティにログインし、[System Configuration] > [User Accounts]を選択します。



ステップ2：パスワードの複雑さパラメータを有効にするには、[パスワードの複雑さ設定を有効にする]チェックボックスをオンにします。

このチェックボックスをオフのままにした場合は、「[ローカルユーザの構成](#)」に進みます。

Local Users Password Complexity

Password Complexity Settings:



Enable

ステップ3:[Minimal password length]フィールドに、0 ~ 127の範囲の数字を入力して、パスワードに含める必要がある最小文字数を設定します。デフォルト値は8です。

この例では、最小文字数を10に設定します。

Local Users Password Complexity

Password Complexity Settings:



Enable

Minimal password length:

10

(Range: 0 - 127, Default: 8)

ステップ4:[Minimal number of character classes]フィールドに、クラスを設定するために0 ~ 4の数値を入力します。入力した数値は、異なるクラスの最小文字数または最大文字数を表します。

- パスワードは、大文字(ABCD)で構成されます。
- パスワードは、小文字(abcd)で構成されます。
- パスワードは数字で構成される(1234)。
- パスワードは特殊文字(!@#\$)で構成されています。

この例では、4が使用されます。

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(!@#\$...).

ステップ5 : 新しいパスワードの[Enable] チェックボックスをオンにします。これは、現在のパスワードと異なるパスワードである必要があります。

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

ステップ6:[パスワード・エージングタイム(Password Aging Time)]フィールドに、パスワード期限切れの日数(0 ~ 365)を入力します。この例では、180日が入力されています。

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)

これで、ルータの[Local Users Password Complexity]設定が正常に設定されました。

ローカルユーザの設定

ステップ1:[Local User Membership List]テーブルで、[Add]をクリックして新しいユーザアカウントを作成します。[Add User Account]ページが表示されます。

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

[Add User Account]ヘッダーの下に、[Local Password Complexity]ステップで定義したパラメータが表示されます。

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

ステップ2:[ユーザー名]フィールドに、アカウントのユーザー名を入力します。


この例では、Administrator_Noahが使用されます。

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"/>	

ステップ3:[新しいパスワード]フィールドに、定義されたパラメータを持つパスワードを入力します。この例では、パスワードの最小長は10文字で構成され、大文字、小文字、数字、特殊文字が組み合わされている必要があります。

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"/>	

ステップ4:[新しいパスワードの確認(New Password Confirm)]フィールドで、確認するパスワードを再入力します。パスワードが一致しない場合は、フィールドの横にテキストが表示されます。

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"/>	▼


パスワード強度メーターは、パスワードの強度に応じて変化します。



ステップ5:[グループ(Group)]ドロップダウンリストから、権限をユーザアカウントに割り当てるグループを選択します。次のオプションがあります。

- admin : 読み取り/書き込み権限。
- guest : 読み取り専用権限。

この例では、[admin]が選択されています。

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"/>	

ステップ6:[Apply]をクリックします。

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"/>	▼

これで、RV34xシリーズルータのローカルユーザメンバーシップが正常に設定されました。

ローカルユーザの編集

ステップ1:[Local User Membership List]テーブルで、ローカルユーザのユーザ名の横にあるチェックボックスをオンにします。

この例では、Administrator_Noahが選択されます。

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

ステップ2:[Edit]をクリックします。

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

ユーザー名を編集できません。

ステップ3:[*Old Password* (古いパスワード)]フィールドに、ローカルユーザアカウント用に以前に設定したパスワードを入力します。

Edit User Account

User Name

Old Password

ステップ4:[新しいパスワード]フィールドに、新しいパスワードを入力します。新しいパスワードは最小要件を満たしている必要があります。

Edit User Account

User Name

Old Password

New Password

(Range: 0 - 127)

ステップ5:[New Password Confirm]フィールドにもう一度新しいパスワードを入力して確認します。これらのパスワードは一致している必要があります。

Edit User Account

User Name

Old Password

New Password

(Range: 0 - 127)

New Password Confirm

ステップ6: (オプション) [Group]ドロップダウンリストから、権限をユーザアカウントに割り当てるグループを選択します。

この例では、[guest]が選択されています。

Edit User Account

User Name

Old Password

New Password

(Range: 0 - 127)

New Password Confirm

Group

ステップ7:[Apply]をクリックします。

User Accounts

Edit User Account

User Name

Old Password

New Password

(Range: 0 - 127)

New Password Confirm

Group

これで、ローカルユーザアカウントが正常に編集されました。

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

ローカルユーザのインポート

ステップ1:[Local Users Import (ローカルユーザのインポート)]領域で、をクリックします



ステップ2:[Import User Name & Password]で[Browse...]をクリックして、ユーザのリストをインポートします。このファイルは通常、カンマ区切り値(.CSV)形式で保存されたスプレッドシートです。

この例では、user-template.csvが選択されています。

Local Users Import

Import User Name & Password

Browse...

user-template.csv

(Import User Name + Password via CSV files)

Import

Download User Template:

Download

ステップ3: (オプション) テンプレートがない場合は、[Download User Template]領域の[Download]をクリックします。

Local Users Import

Import User Name & Password

Browse...

user-template.csv

(Import User Name + Password via CSV files)

Import

Download User Template:

Download

ステップ 4 : [Import] をクリックします。

Local Users Import

Import User Name & Password

Browse...

user-template.csv

(Import User Name + Password via CSV files)

Import

Download User Template:

Download

インポートが成功したことを示すメッセージがインポートボタンの横に表示されます。

これで、ローカルユーザのリストが正常にインポートされました。

リモート認証サービスの設定

RADIUS

ステップ1:[Remote Authentication Service Table]で、[Add]をクリックしてエントリを作成します。
。

Remote Authentication Service Table



Enable  Name 

ステップ2:[Name]フィールドで、アカウントのユーザ名を作成します。

この例では、管理者が使用されます。

Add/Edit New Domain

Name

Administrator

ステップ3:[Authentication Type]ドロップダウンメニューから[RADIUS]を選択します。つまり、ユーザ認証はRADIUSサーバを介して行われます。

RADIUSで設定できるリモートユーザアカウントは1つだけです。

Authentication Type

RADIUS



RADIUS

Active Directory

LDAP

Primary Server

Backup Server

ステップ4:[プライマリ・サーバ]フィールドに、プライマリRADIUSサーバのIPアドレスを入力します。

この例では、プライマリサーバとして192.168.3.122が使用されています。

Primary Server	<input type="text" value="192.168.3.122"/>	Port	<input type="text" value="389"/>
----------------	--	------	----------------------------------

ステップ5:[Port] フィールドに、プライマリRADIUSサーバのポート番号を入力します。

この例では、ポート番号として1645が使用されます。

Primary Server	<input type="text" value="192.168.3.122"/>	Port	<input type="text" value="389"/>
----------------	--	------	----------------------------------

ステップ6:[Backup Server]フィールドに、バックアップRADIUSサーバのIPアドレスを入力します。これは、プライマリサーバがダウンした場合のフェールオーバーとして機能します。

この例では、バックアップサーバのアドレスは192.168.4.122です。

Backup Server	<input type="text" value="192.168.4.122"/>	Port	<input type="text" value="389"/>
---------------	--	------	----------------------------------

ステップ7:[Port]フィールドに、バックアップRADIUSサーバの数を入力します。

Backup Server	<input type="text" value="192.168.4.122"/>	Port	<input type="text" value="389"/>
---------------	--	------	----------------------------------

この例では、ポート番号として1646が使用されます。

ステップ8:[Preshared-Key] フィールドに、RADIUSサーバで設定された事前共有キーを入力します。

Pre-shared Key	<input type="password" value="●●●●●●●●"/>
----------------	---

ステップ9:[Confirm Preshared-key]フィールドで、事前共有キーを再入力して確認します。

Confirm Pre-shared Key	<input type="password" value="●●●●●●●●"/>
------------------------	---

ステップ10:[Apply]をクリックします。

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="●●●●●●●●"/>		

メインユーザアカウントのページが表示されます。最近設定したアカウントが[Remote Authentication Service]テーブルに表示されます。

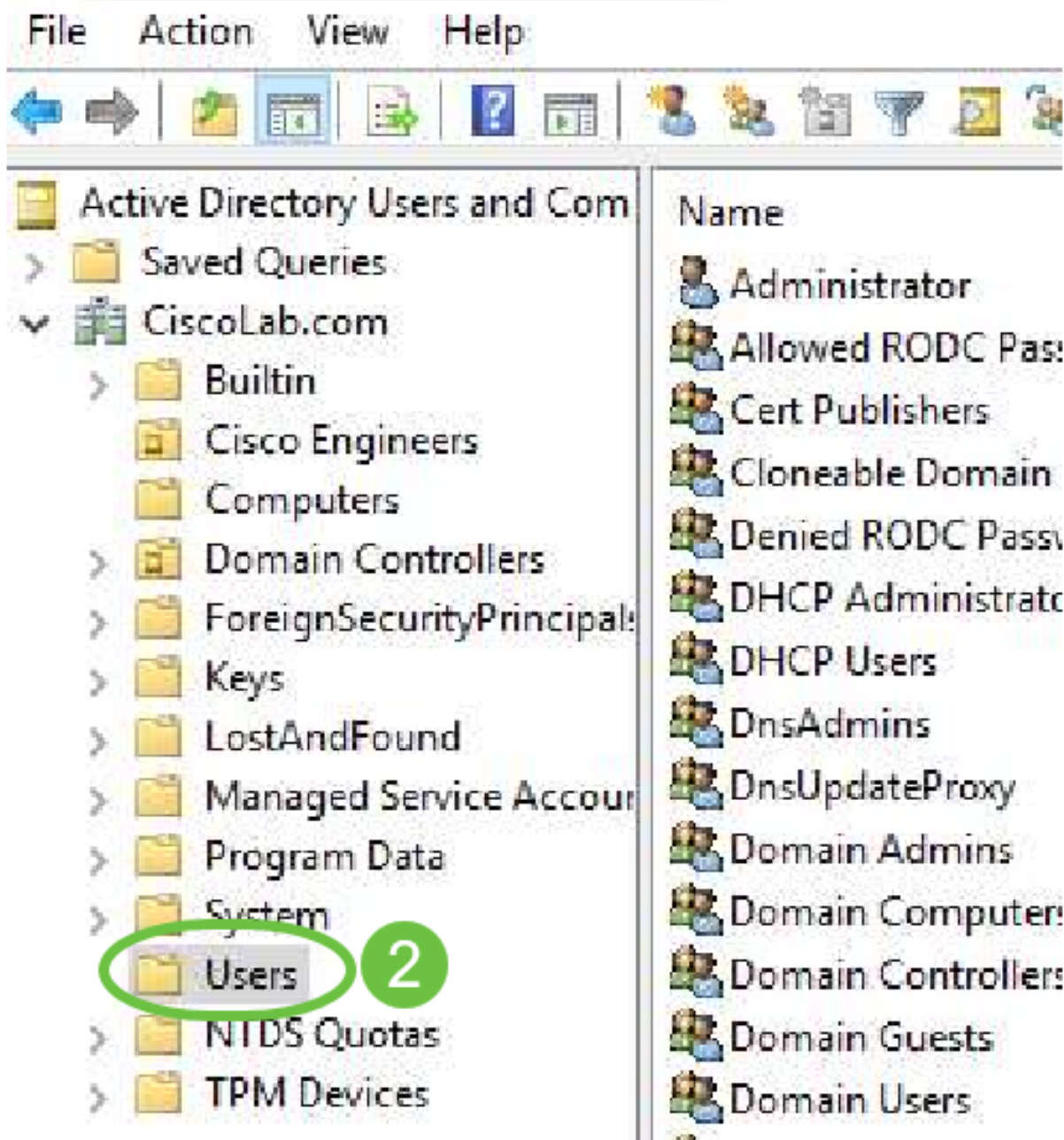
これで、RV34xシリーズルータでRADIUS認証が正常に設定されました。

Active Directoryの設定

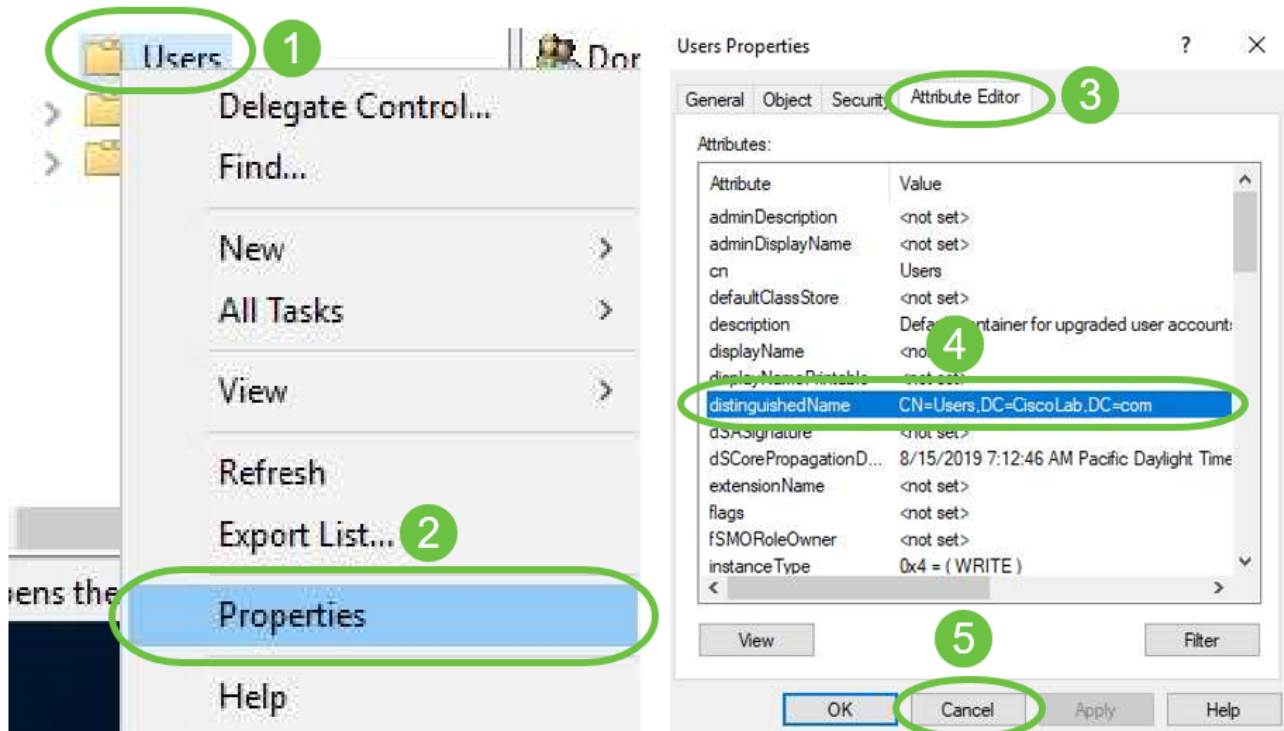
ステップ1:Active Directoryの設定を完了するには、Active Directoryサーバにログインする必要があります。PCでActive Directoryのユーザーとコンピュータを開き、リモートでログインするために使用するユーザーアカウントがあるコンテナに移動します。この例では、Usersコンテナを使用します。

Active Directory Users and Computers

1



ステップ2 : コンテナを右クリックし、[Properties]を選択します。[Attribute Editor]タブに移動し、[distinguishedName]フィールドを探します。このタブが表示されていない場合は、Active Directoryユーザーとコンピューターで拡張機能ビューを有効にし、やり直す必要があります。このフィールドをメモし、[キャンセル]をクリックします。これはユーザコンテナパスになります。このフィールドは、RV340を設定する際にも必要であり、正確に一致する必要があります。



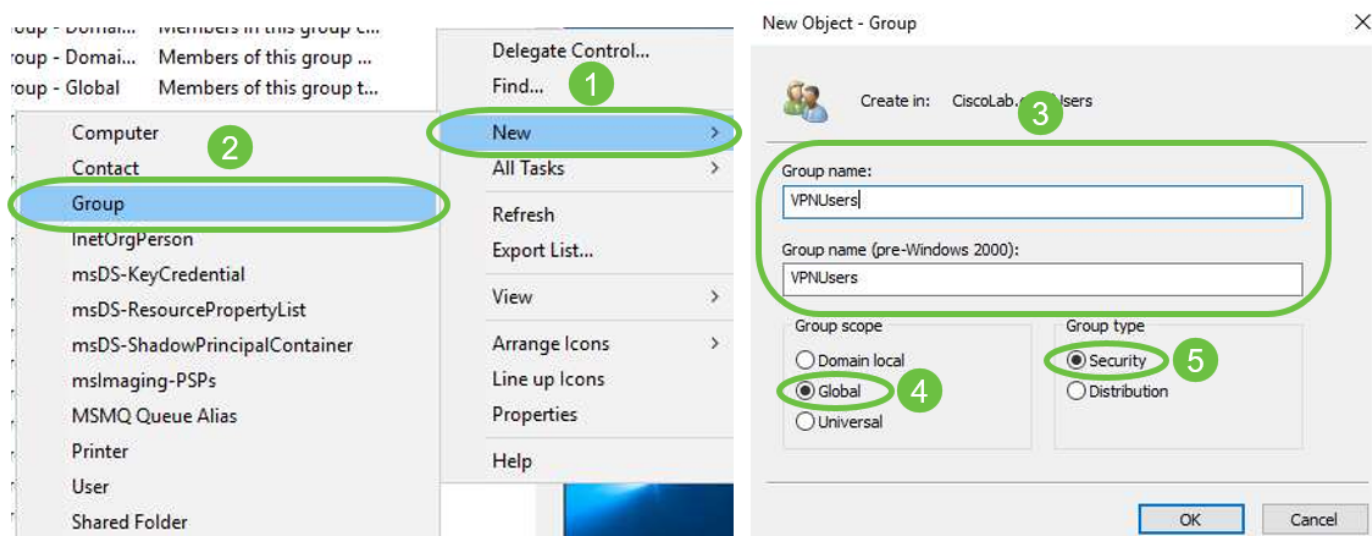
ステップ3：使用するユーザアカウントと同じコンテナにグローバルセキュリティグループを作成します。

選択したコンテナで、空白の領域を右クリックし、「新規」>「グループ」を選択します。

次の項目を選択してください。

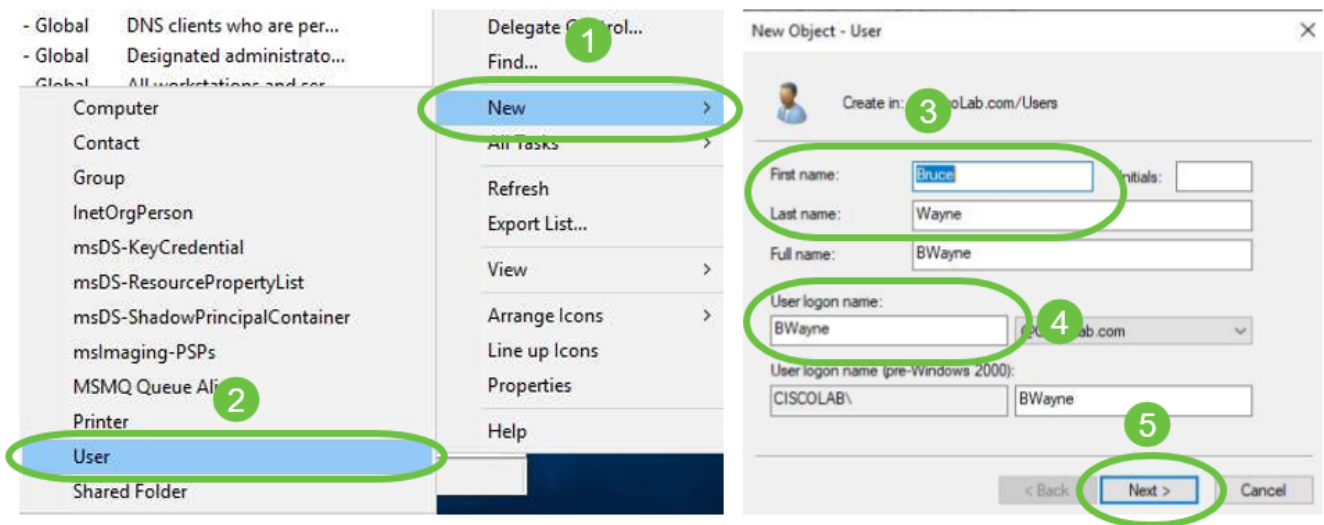
- グループ名：この名前は、RV340で作成されたユーザグループ名と完全に一致している必要があります。この例では、VPNUsersを使用します。
- グループスコープ – グローバル
- グループタイプ：セキュリティ

[OK] をクリックします。



ステップ4：新しいユーザアカウントを作成するには、次の手順を実行します。

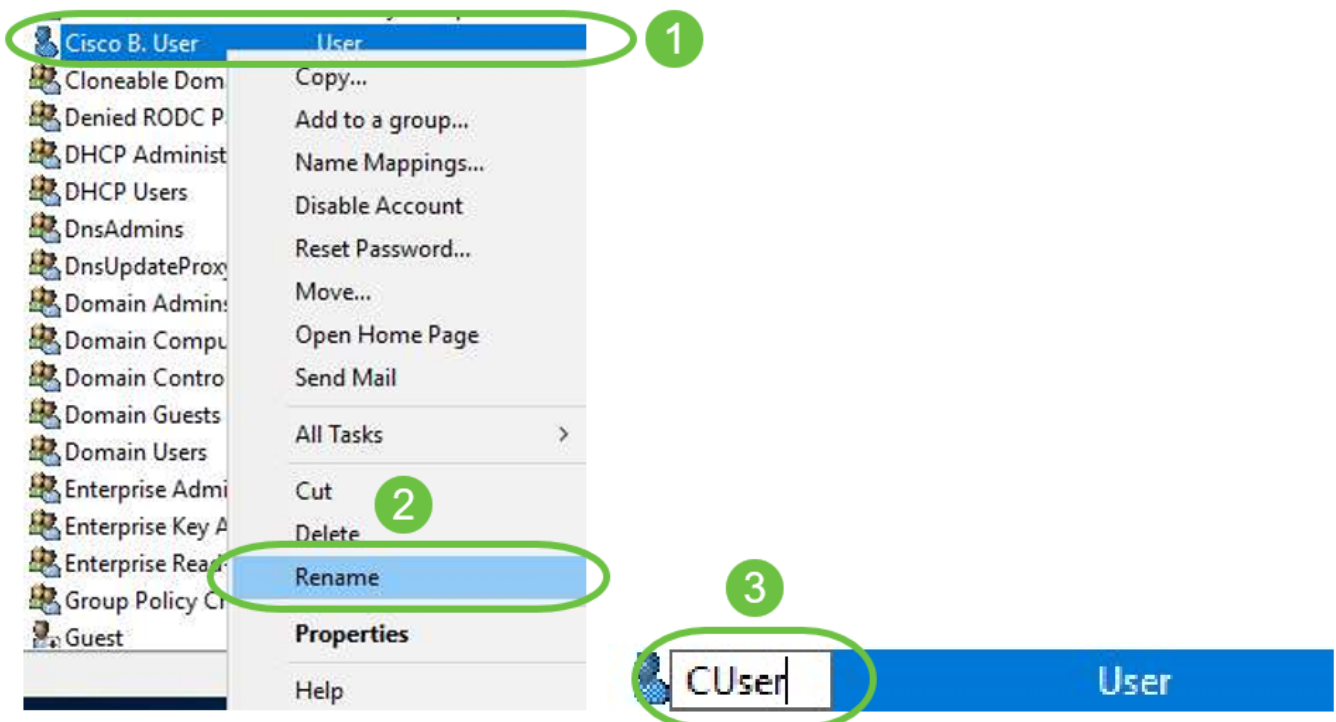
- コンテナ内の空のスペースを右クリックし、「新規」>「ユーザー」を選択します。
- [名前]、[名前]を入力します。
- ユーザー・ ログオン名を入力します。
- [next] をクリックします。



ユーザのパスワードを入力するように求められます。[User must change password at next logon]ボックスがオンになっている場合は、リモートでログインする前に、ローカルでログインし、パスワードを変更する必要があります。

[Finish] をクリックします。

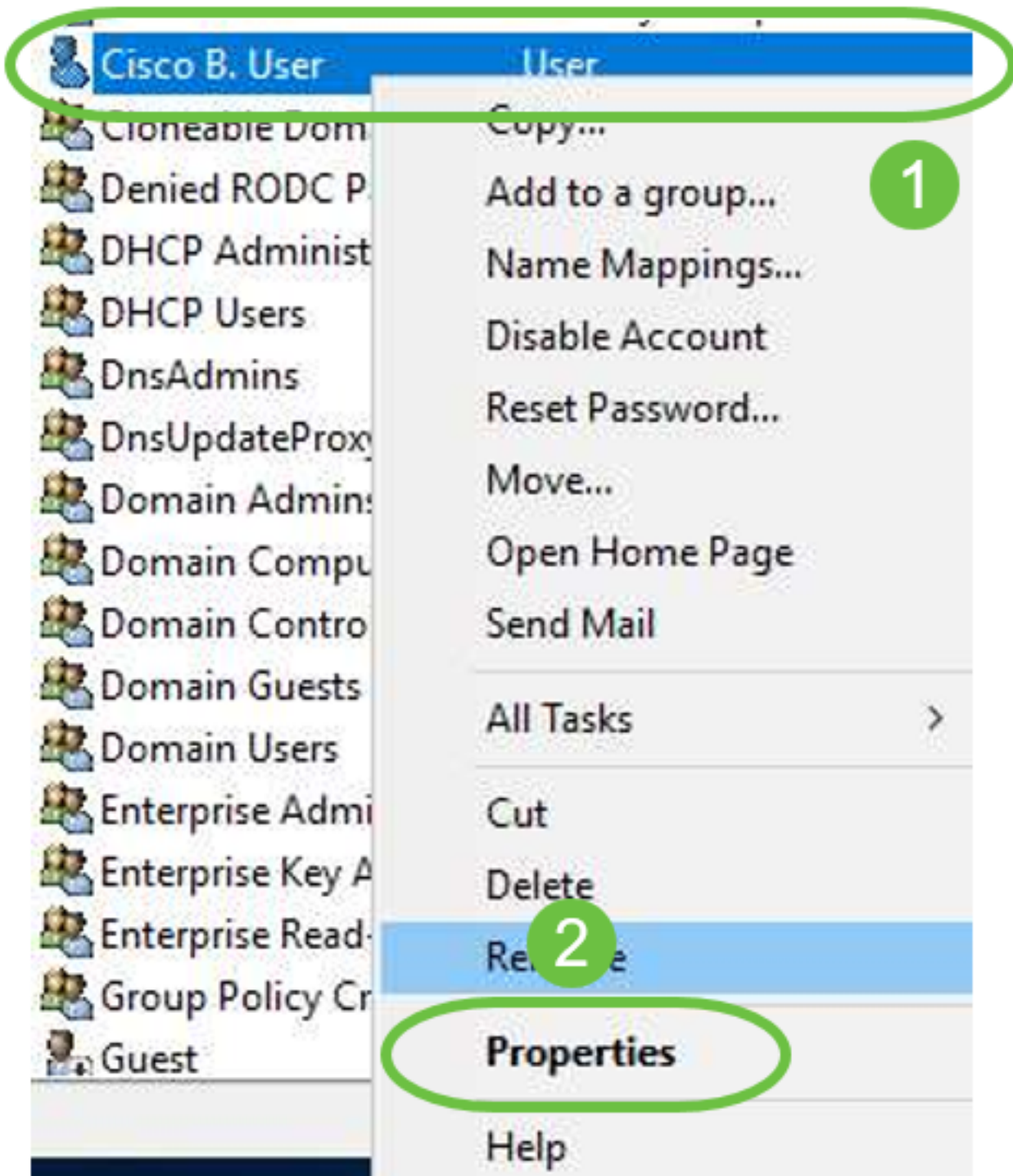
使用する必要のあるユーザーアカウントがすでに作成されている場合は、調整が必要な場合があります。ユーザーの正規名を調整するには、ユーザーを選択し、右クリックして「名前の変更」を選択します。すべてのスペースが削除され、ユーザのログオン名と一致していることを確認します。ユーザの表示名は変更されません。[OK] をクリックします。



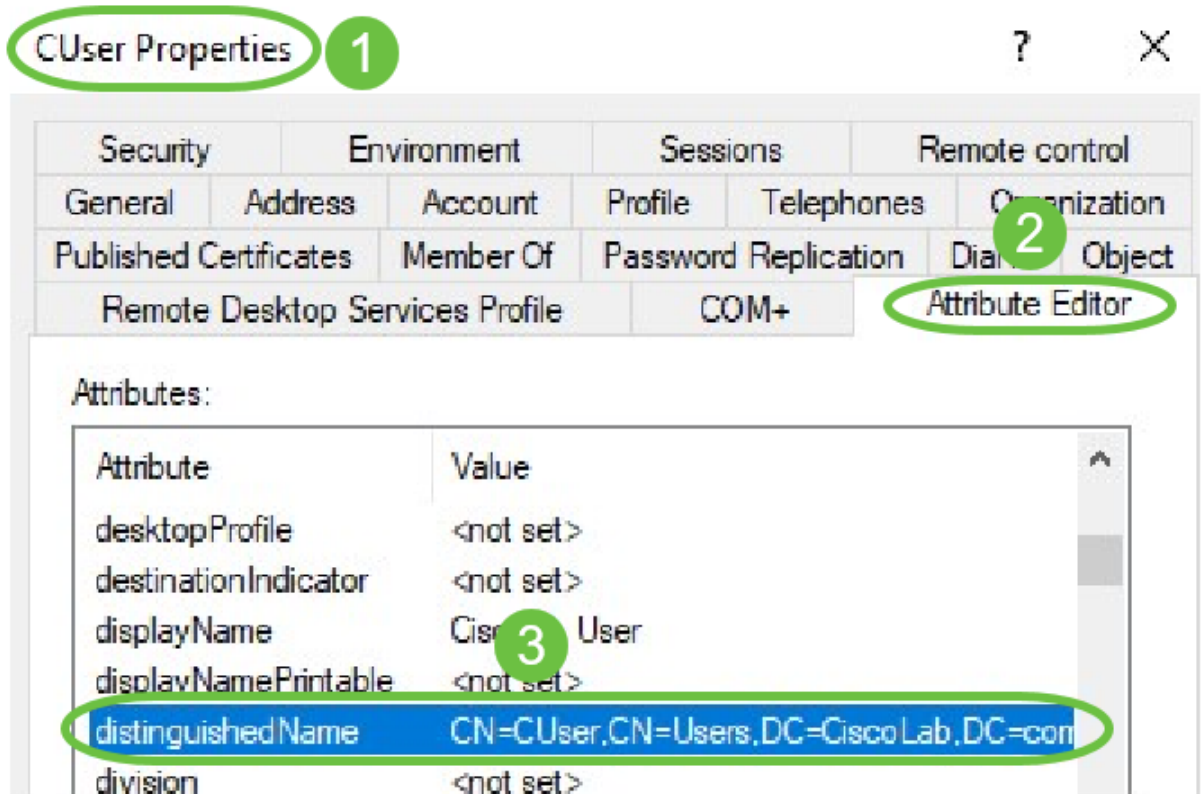
ステップ5 : ユーザアカウントが正しく構成されたら、リモートでログインする権限を付与する必

必要があります。

そのためには、ユーザーアカウントを選択し、右クリックして[プロパティ]を選択します。



[ユーザープロパティ]で[属性エディタ]タブを選択し、[distinguishedName]までスクロールダウンします。最初のCN=にスペースを含まない正しいユーザーログオン名があることを確認してください。



[メンバーの]タブを選択し、[追加]をクリックします。

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	

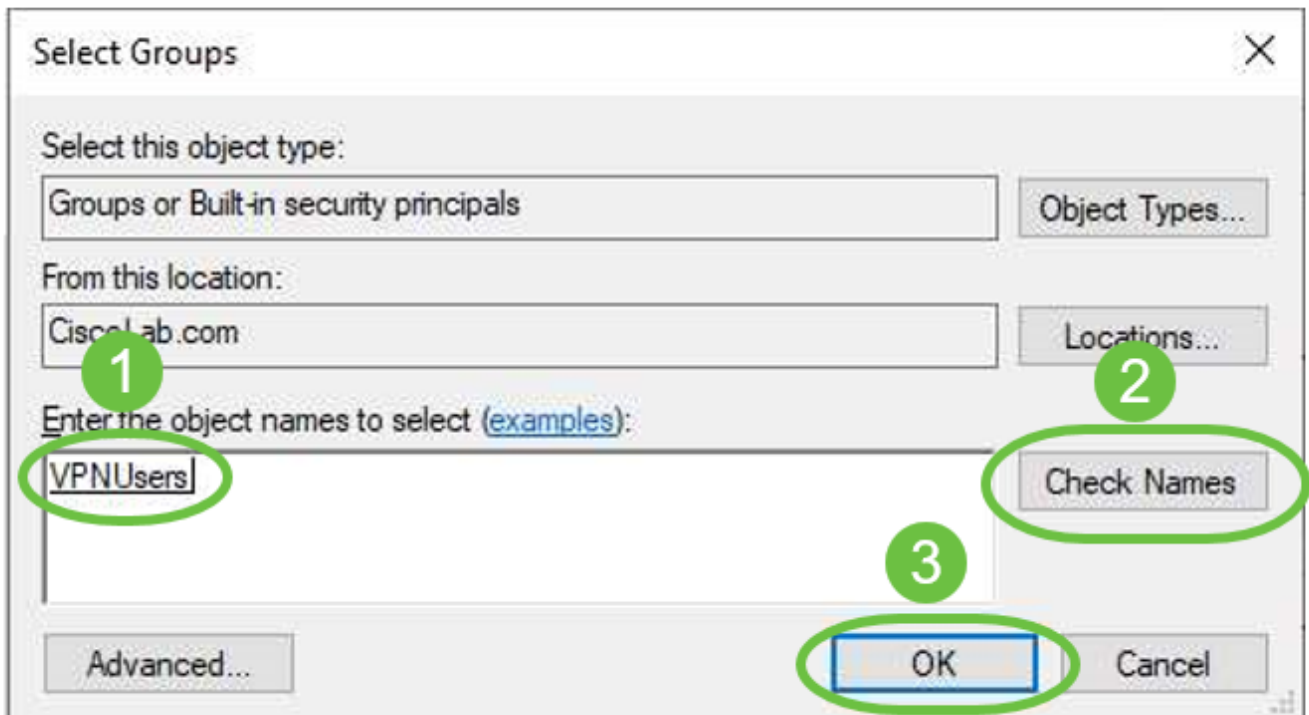
Member of:

Name	
Domain Users	CiscoLab.com/Users

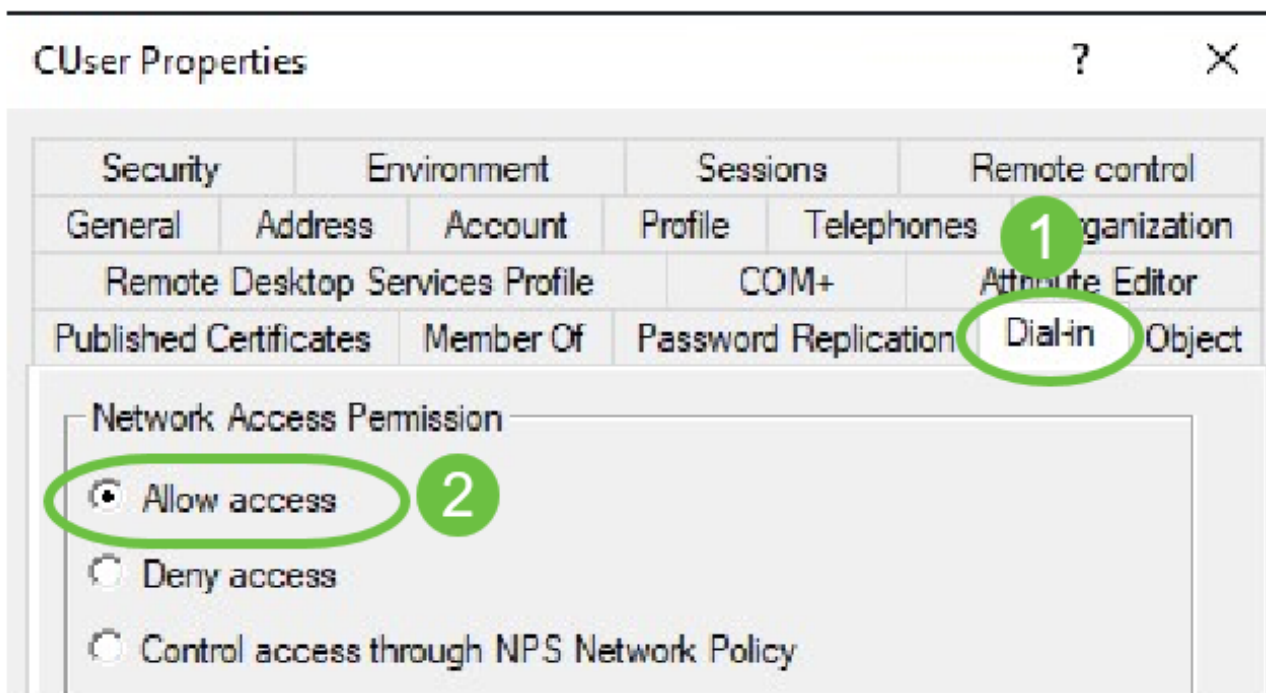
2

Add... Remove

グローバルセキュリティグループの名前を入力し、[Check Name]を選択します。エントリに下線が引かれている場合は、「OK」をクリックします。



[ダイヤルイン]タブを選択します。[ネットワークアクセス許可]セクションの[アクセスを許可]を選択し、残りの項目は既定のままにします。

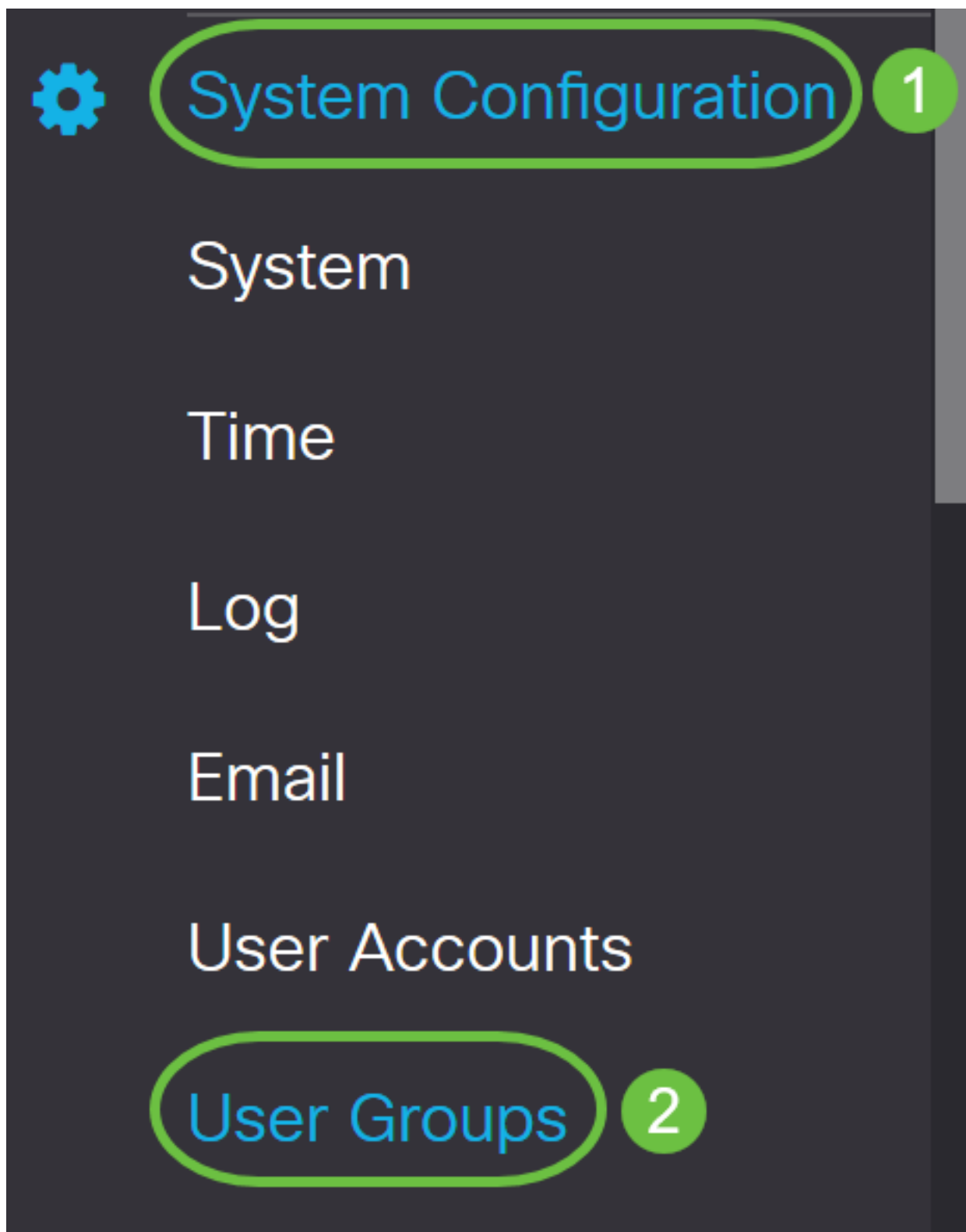


Active Directory統合

Active Directoryでは、RV34xルータの時刻がADサーバの時刻と一致している必要があります。RV34xシリーズルータの時刻設定の手順については、[ここをクリックしてください](#)。

ADでは、RV340にADグローバルセキュリティグループと一致するユーザグループが必要です。

ステップ1:[System Configuration] > [User Groups]に移動します。



ステップ2:[+]アイコンをクリックしてユーザグループを追加します。

User Groups

User Groups Table



ステップ3: グループ名を入力します。この例では、VPNUsersです。

Group Name:

グループ名は、ADグローバルセキュリティグループとまったく同じでなければなりません。

ステップ4:[Services]の[Web Login/NETCONF/RESTCONF]を[Disabled]とマークする必要があります。AD統合がすぐに機能しない場合でも、RV34xにアクセスできます。

Services

Web Login/NETCONF/RESTCONF Disabled Read Only Administrator

ステップ5:AD統合を使用してユーザをログインするVPNトンネルを追加できます。

1. すでに設定されているクライアントからサイトへのVPNを追加するには、[EZVPN/3rd Party]セクションに移動し、プラスのアイコンをクリックします。ドロップダウンメニューからVPNプロファイルを選択し、[Add]をクリックします。

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 - SSL VPNトンネルを使用する場合は、[プロファイルの選択]の横にあるドロップダウンメニューからポリシーを選択します。

SSL VPN

Select a Profile

SSLVPNDefaultPolicy



6. PPTP/L2TP/802.1x:ADの使用を許可するには、[Permit]の横にあるチェックボックスをクリックします。

PPTP VPN



Permit

L2TP



Permit

802.1x



Permit

ステップ6:[Apply]をクリックして変更を保存します。

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

PPTP VPN Permit

L2TP Permit

802.1x Permit

Active Directory統合設定

ステップ1:[System Configuration] > [User Accounts]に移動します。



System Configuration

System

1

Time

Log

Email

User Accounts

2

ステップ2:[Remote Authentication Service Table]で、[Add]をクリックしてエントリを作成します。

Remote Authentication Service Table



Enable ⇅ Name ⇅

ステップ3:[Name]フィールドで、アカウントのユーザ名を作成します。この例では、**Jorah_Admin**が使用されています。

Add/Edit New Domain

Name

Jorah_Admin

ステップ4:[Authentication Type]ドロップダウンメニューから、**[Active Directory]**を選択します。ADは、ネットワークのすべての要素に幅広いポリシーを割り当て、多くのコンピュータにプログラムを展開し、組織全体に重要な更新を適用するために使用されます。

Authentication Type

Active Directory

AD Domain Name

RADIUS

Active Directory

Primary Server

LDAP

ステップ5:[AD Domain Name]フィールドに、ADの完全修飾ドメイン名を入力します。

この例では、**sampledomain.com**が使用されます。

AD Domain Name

ステップ6:[プライマリ・サーバ]フィールドに、ADのアドレスを入力します。

この例では、**192.168.2.122**が使用されます。

Primary Server Port

ステップ7:[ポート]フィールドに、プライマリサーバのポート番号を入力します。

この例では、ポート番号として**1234**が使用されています。

Primary Server Port

ステップ8: (オプション) [ユーザテナパス(*User Container Path*)]フィールドに、ユーザが含まれるルートパスを入力します。

注：この例では、**file:Documents/manage/containers**が使用されています。

User Container Path

ステップ9:[Apply]をクリックします。

User Accounts

Add/Edit New Domain

Name

Authentication Type

AD Domain Name

Primary Server Port

User Container Path

ステップ10:[Service Auth Sequence]までスクロールダウンして、さまざまなオプションのロガイ

ン方式を設定します。

- Web Login/NETCONF/RESTCONF:RV34xルータへのログイン方法です。[デフォルトを使用]チェックボックスをオフにし、[Primary method]を[Local DB]に設定します。これにより、Active Directory統合が失敗しても、ルータからログアウトされなくなります。
- Site-to-site/EzVPN&Rd Party Client-to-site VPN:ADを使用するようにClient-to-Site VPNトンネルを設定します。[Use Default]チェックボックスをオフにし、[Primary method]を[Active Directory]、[Secondary Method]を[Local DB]に設定します。

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

ステップ11:[Apply]をクリックします。

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

ステップ12 : 実行コンフィギュレーションをスタートアップコンフィギュレーションに保存します。

これで、RV34xシリーズルータのActive Directoryの設定が正常に完了しました。

[LDAP]

ステップ1:[Remote Authentication Service Table]で、[Add]をクリックしてエントリを作成します。

Remote Authentication Service Table



Enable ⇅

Name ⇅

ステップ2:[Name]フィールドで、アカウントのユーザー名を作成します。

LDAPで設定できるリモートユーザアカウントは1つだけです。

この例では、Dany_Adminが使用されています。

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

ステップ3:[Authentication Type]ドロップダウンメニューから、[LDAP]を選択します。Lightweight Directory Access Protocol(LDAP)は、ディレクトリサービスへのアクセスに使用されるアクセスプロトコルです。ドメインの認証を実行するためにディレクトリサーバを実行するリモートサーバです。

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"/>

ステップ4:[プライマリ・サーバ]フィールドに、LDAPのサーバ・アドレスを入力します。

この例では、192.168.7.122が使用されます。

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

ステップ5:[Port]フィールドに、プライマリ・サーバのポート番号を入力します。

この例では、ポート番号として122が使用されています。

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

ステップ6:[Base DN]フィールドにLDAPサーバのベース識別名を入力します。ベースDNは、LDAPサーバが許可要求を受信したときにユーザを検索する場所です。このフィールドは、LDAPサーバに設定されているベースDNと一致している必要があります。

この例では、Dept101が使用されています。

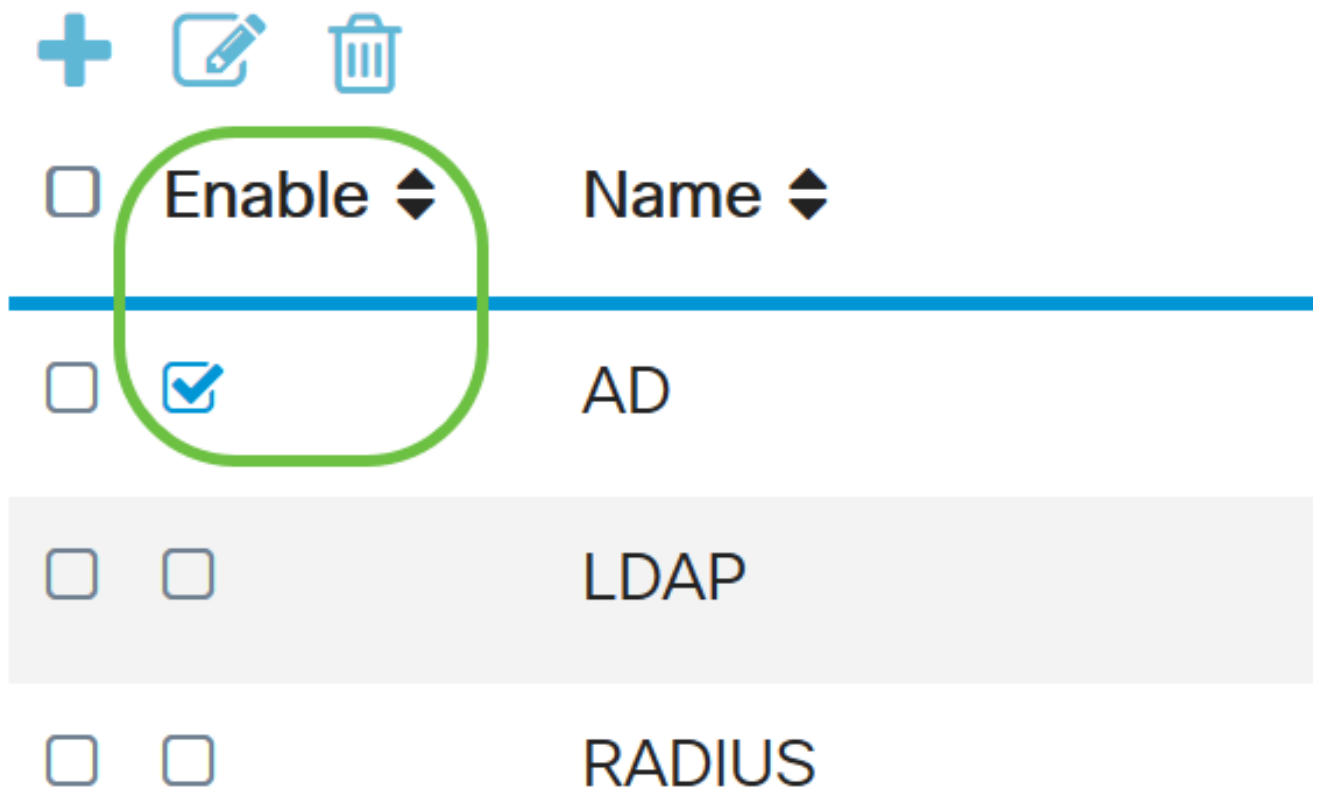
Base DN	Dept101
---------	---------

ステップ7:[Apply]をクリックします。リモート認証サービステーブルに移動します。



ステップ8: (オプション) リモート認証サービスを有効または無効にするには、有効または無効にするサービスの横にあるチェックボックスをオンまたはオフにします。

Remote Authentication Service Table



The image shows a table with three rows. At the top, there are three icons: a plus sign, a pencil, and a trash can. The first row has a header with a checkbox, the text 'Enable' with a double-headed arrow, and the text 'Name' with a double-headed arrow. 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'. A green circle highlights the 'Enable' text and the checked checkbox in the second row.

<input type="checkbox"/>	Enable ⇅	Name ⇅
<input type="checkbox"/>	<input checked="" type="checkbox"/>	AD
<input type="checkbox"/>	<input type="checkbox"/>	LDAP
<input type="checkbox"/>	<input type="checkbox"/>	RADIUS

ステップ9:[Apply]をクリックします。

User Accounts

Apply

これで、RV34xシリーズルータでLDAPが正しく設定されました。

この記事に関連するビデオを表示...

[シスコのその他のテクニカルトークを表示するには、ここをクリックしてください](#)