

Configurer et gérer des comptes d'utilisateurs sur un routeur de la gamme RV34x

Objectif

L'objectif de cet article est de vous montrer comment configurer et gérer les comptes d'utilisateurs locaux et distants sur un routeur de la gamme RV34x. Cela inclut : comment configurer la complexité des mots de passe des utilisateurs locaux, configurer/modifier/importer des utilisateurs locaux, configurer le service d'authentification à distance à l'aide de RADIUS, Active Directory et LDAP.

Périphériques pertinents | Version du micrologiciel

- Gamme RV34x | 1.0.01.16 ([Télécharger la dernière version](#))

Introduction

Le routeur de la gamme RV34x fournit des comptes d'utilisateurs afin d'afficher et d'administrer les paramètres. Les utilisateurs peuvent provenir de différents groupes ou appartenir à des groupes logiques de réseaux privés virtuels (VPN) SSL (Secure Sockets Layer) qui partagent le domaine d'authentification, les règles d'accès au réseau local (LAN) et aux services, ainsi que les paramètres de délai d'inactivité. La gestion des utilisateurs définit le type d'utilisateurs pouvant utiliser un certain type d'installation et la manière de le faire.

La priorité de la base de données externe est toujours RADIUS (Remote Authentication Dial-In User Service)/LDAP (Lightweight Directory Access Protocol)/Active Directory (AD)/Local. Si vous ajoutez le serveur RADIUS sur le routeur, le service de connexion Web et d'autres services utiliseront la base de données externe RADIUS pour authentifier l'utilisateur.

Il n'existe aucune option permettant d'activer une base de données externe pour le service de connexion Web seul et de configurer une autre base de données pour un autre service. Une fois RADIUS créé et activé sur le routeur, le routeur utilise le service RADIUS comme base de données externe pour la connexion Web, le VPN site à site, le VPN EzVPN/tiers, le VPN SSL, le protocole PPTP (Point-to-Point Transport Protocol)/le VPN L2TP (Layer 2 Transport Protocol) et 802.1x.

Table des matières

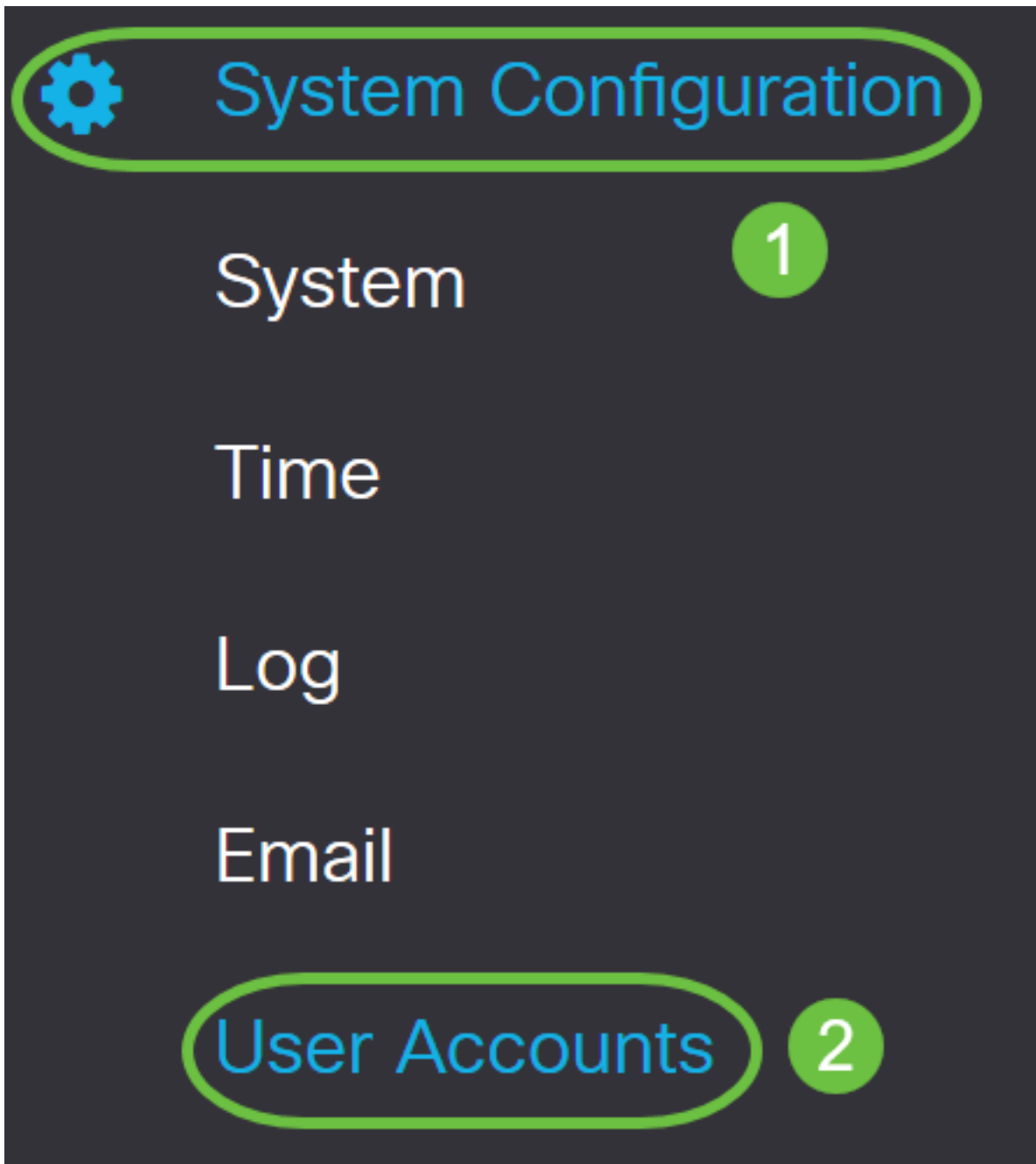
- [Configurer un compte d'utilisateur local](#)
- [Complexité des mots de passe des utilisateurs locaux](#)
- [Configurer les utilisateurs locaux](#)
- [Modifier les utilisateurs locaux](#)
- [Importer les utilisateurs locaux](#)
- [Configurer le service d'authentification à distance](#)
- [RADIUS](#)
- [Configuration Active Directory](#)
- [Intégration Active Directory](#)
- [Paramètres d'intégration Active Directory](#)

- [LDAP](#)

Configurer un compte d'utilisateur local

Complexité des mots de passe des utilisateurs locaux

Étape 1. Connectez-vous à l'utilitaire Web du routeur et sélectionnez **Configuration système > Comptes d'utilisateurs**.



Étape 2. Cochez la case **Activer les paramètres de complexité du mot de passe** pour activer les paramètres de complexité du mot de passe.

Si cette case n'est pas cochée, passez à [Configurer les utilisateurs locaux](#).

Local Users Password Complexity

Password Complexity Settings:



Enable

Étape 3. Dans le champ *Longueur minimale du mot de passe*, saisissez un nombre compris entre 0 et 127 pour définir le nombre minimal de caractères qu'un mot de passe doit contenir. Il est défini par défaut à 8.

Dans cet exemple, le nombre minimal de caractères est défini sur 10.

Local Users Password Complexity

Password Complexity Settings:



Enable

Minimal password length:

10

(Range: 0 - 127, Default: 8)

Étape 4. Dans le champ *Nombre minimal de classes de caractères*, entrez un nombre compris entre 0 et 4 pour définir la classe. Le nombre entré représente le nombre de caractères minimum ou maximum des différentes classes :

- Le mot de passe est composé de caractères majuscules (ABCD).
- Le mot de passe est composé de caractères en minuscules (abcd).
- Le mot de passe est composé de caractères numériques (1234).
- Le mot de passe est composé de caractères spéciaux (!@#\$.).

Dans cet exemple, 4 est utilisé.

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(!@#\$.).

Étape 5. Cochez la case **Activer** pour que le nouveau mot de passe soit différent de celui en cours.

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

Étape 6. Dans le champ *Délai d'expiration du mot de passe*, saisissez le nombre de jours (0 - 365) pour l'expiration du mot de passe. Dans cet exemple, **180** jours ont été saisis.

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)

Vous avez maintenant correctement configuré les paramètres de complexité du mot de passe des utilisateurs locaux sur votre routeur.

Configurer les utilisateurs locaux

Étape 1. Dans le tableau Liste des membres des utilisateurs locaux, cliquez sur **Ajouter** pour créer un nouveau compte d'utilisateur. Vous accédez à la page Ajouter un compte d'utilisateur.

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

Sous l'en-tête *Ajouter un compte d'utilisateur*, les paramètres définis sous les étapes Complexité du mot de passe local s'affichent.

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

Étape 2. Dans le champ *Nom d'utilisateur*, saisissez un nom d'utilisateur pour le compte.


Dans cet exemple, **Administrator_Noah** est utilisé.

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"/>	

Étape 3. Dans le champ *Nouveau mot de passe*, saisissez un mot de passe avec les paramètres définis. Dans cet exemple, la longueur minimale du mot de passe doit être composée de 10 caractères avec une combinaison de majuscules, minuscules, chiffres et caractères spéciaux.

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"/>	

Étape 4. Dans le champ *Nouveau mot de passe*, saisissez à nouveau le mot de passe pour le confirmer. Un texte en regard du champ apparaît si les mots de passe ne correspondent pas.

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"/>	▼


Le compteur de puissance du mot de passe change en fonction de la force de votre mot de passe.



Étape 5. Dans la liste déroulante *Groupe*, sélectionnez un groupe pour attribuer un privilège à un compte d'utilisateur. Les options sont les suivantes :

- admin : privilèges de lecture et d'écriture.
- guest : privilèges en lecture seule.

Dans cet exemple, **admin** est sélectionné.

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"/>	

Étape 6. Cliquez sur 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"/>	▼

Vous avez maintenant correctement configuré l'appartenance de l'utilisateur local sur un routeur de la gamme RV34x.

Modifier les utilisateurs locaux

Étape 1. Cochez la case en regard du nom d'utilisateur de l'utilisateur local dans le tableau Liste des membres d'utilisateurs locaux.

Pour cet exemple, **Administrator_Noah** est sélectionné.

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

Étape 2. Cliquez sur **Edit**.

Local Users

Local User Membership List



<input type="checkbox"/>	#	User Name	Group *
<input checked="" type="checkbox"/>	1	Administrator_Noah	admin
<input type="checkbox"/>	2	cisco	admin
<input type="checkbox"/>	3	guest	guest

Impossible de modifier le nom d'utilisateur.

Étape 3. Dans le champ *Ancien mot de passe*, saisissez le mot de passe précédemment configuré pour le compte d'utilisateur local.

Edit User Account

User Name

Old Password

Étape 4. Dans le champ *Nouveau mot de passe*, saisissez un nouveau mot de passe. Le nouveau mot de passe doit répondre aux exigences minimales.

Edit User Account

User Name

Old Password

New Password

(Range: 0 - 127)

Étape 5. Entrez à nouveau le nouveau mot de passe dans le champ *Nouveau mot de passe* à confirmer. Ces mots de passe doivent correspondre.

Edit User Account

User Name

Old Password

New Password

(Range: 0 - 127)

New Password Confirm

Étape 6. (Facultatif) Dans la liste déroulante Groupe, sélectionnez un groupe pour attribuer un privilège à un compte d'utilisateur.

Dans cet exemple, **guest** est choisi.

Edit User Account

User Name

Old Password

New Password

(Range: 0 - 127)

New Password Confirm

Group

admin

guest

Étape 7. Cliquez sur Apply.

User Accounts

Apply

Cancel

Edit User Account

User Name

Old Password

New Password

(Range: 0 - 127)

New Password Confirm

Group

Vous devez maintenant avoir correctement modifié un compte d'utilisateur 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

Importer les utilisateurs locaux



Étape 1. Dans la zone Importation d'utilisateurs locaux, cliquez sur

Étape 2. Sous Importer le nom d'utilisateur et le mot de passe, cliquez sur **Parcourir...** pour importer une liste d'utilisateurs. Ce fichier est généralement une feuille de calcul enregistrée dans un format de valeur séparée par des virgules (.CSV).

Dans cet exemple, **user-template.csv** est sélectionné.

Local Users Import

Import User Name & Password

Browse...

user-template.csv

(Import User Name + Password via CSV files)

Import

Download User Template:

Download

Étape 3. (Facultatif) Si vous n'avez pas de modèle, cliquez sur **Télécharger** dans la zone Télécharger le modèle utilisateur.

Local Users Import

Import User Name & Password

Browse...

user-template.csv

(Import User Name + Password via CSV files)

Import

Download User Template:

Download

Étape 4. Cliquez sur **Import**.

Local Users Import

Import User Name & Password

Browse...

user-template.csv

(Import User Name + Password via CSV files)

Import

Download User Template:

Download

Un message s'affiche en regard du bouton d'importation pour indiquer que l'importation a réussi.

Vous avez maintenant importé une liste d'utilisateurs locaux.

Configurer le service d'authentification à distance

RADIUS

Étape 1. Dans la table Remote Authentication Service, cliquez sur **Add** pour créer une entrée.

Remote Authentication Service Table



Enable ⇅

Name ⇅

Étape 2. Dans le champ *Nom*, créez un nom d'utilisateur pour le compte.

Dans cet exemple, **Administrator** est utilisé.

Add/Edit New Domain

Name

Administrator

Étape 3. Dans le menu déroulant Type d'authentification, sélectionnez **Radius**. Cela signifie que l'authentification de l'utilisateur sera effectuée via un serveur RADIUS.

Seul un seul compte d'utilisateur distant sous RADIUS peut être configuré.

Authentication Type

RADIUS



RADIUS

Active Directory

LDAP

Primary Server

Backup Server

Étape 4. Dans le champ *Serveur principal*, saisissez l'adresse IP du serveur RADIUS principal.

Dans cet exemple, **192.168.3.122** est utilisé comme serveur principal.

Primary Server Port

Étape 5. Dans le champ *Port*, saisissez le numéro de port du serveur RADIUS principal.

Dans cet exemple, **1645** est utilisé comme numéro de port.

Primary Server Port

Étape 6. Dans le champ *Backup Server*, saisissez l'adresse IP du serveur RADIUS de sauvegarde. Ceci sert de basculement en cas de panne du serveur principal.

Dans cet exemple, l'adresse du serveur de sauvegarde est **192.168.4.122**.

Backup Server Port

Étape 7. Dans le champ *Port*, saisissez le nombre de serveurs RADIUS de sauvegarde.

Backup Server Port

Dans cet exemple, **1646** est utilisé comme numéro de port.

Étape 8. Dans le champ *Preshared-Key*, saisissez la clé pré-partagée qui a été configurée sur le serveur RADIUS.

Pre-shared Key

Étape 9. Dans le champ *Confirmer la clé prépartagée*, saisissez à nouveau la clé prépartagée pour confirmer.

Confirm Pre-shared Key

Étape 10. Cliquez sur 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="●●●●●●●●"/>		

Vous accéderez à la page du compte d'utilisateur principal. Le compte récemment configuré apparaît maintenant dans la table Remote Authentication Service.

Vous avez maintenant correctement configuré l'authentification RADIUS sur un routeur de la gamme RV34x.

Configuration Active Directory

Étape 1. Pour terminer la configuration Active Directory, vous devez être connecté au serveur Active Directory. Sur votre ordinateur, ouvrez **Utilisateurs et ordinateurs Active Directory** et naviguez jusqu'au conteneur dans lequel les comptes utilisateur seront utilisés pour se connecter à distance. Dans cet exemple, nous allons utiliser le conteneur **Utilisateurs**.

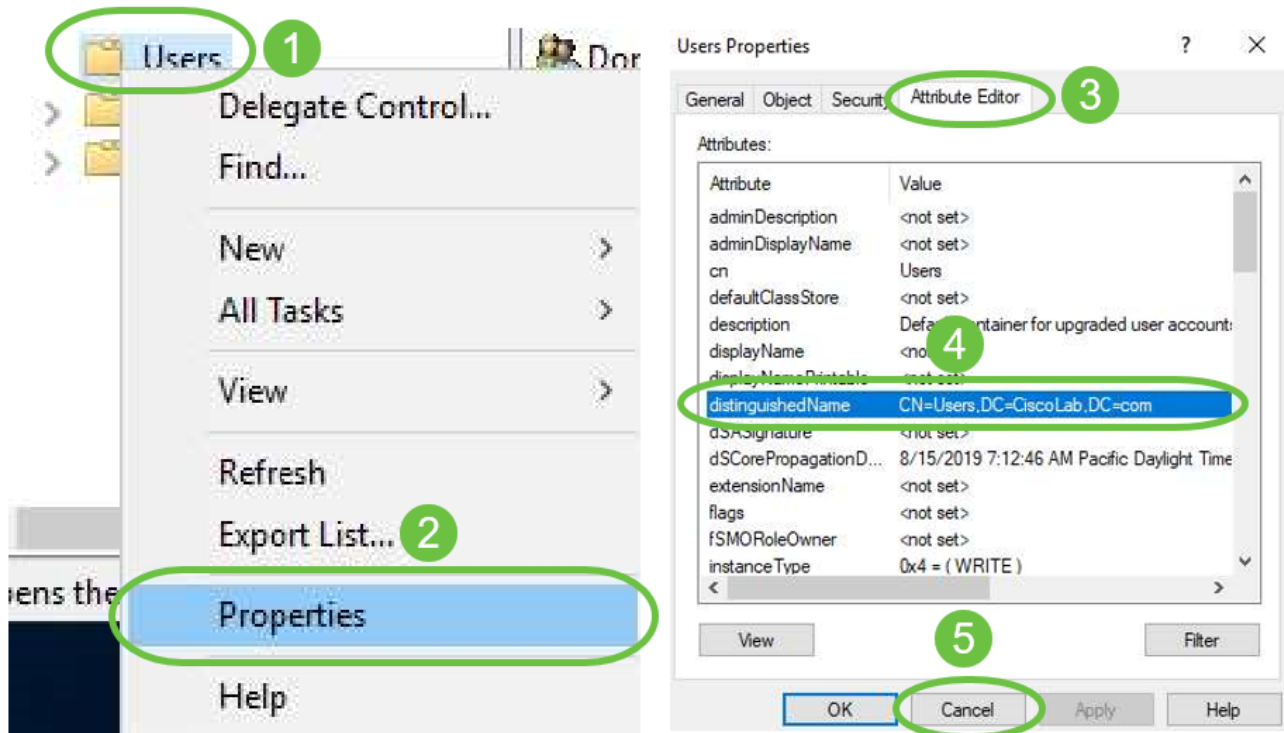
Active Directory Users and Computers

1

The screenshot shows the Active Directory Users and Computers console. The left pane displays a tree view of the directory structure. The 'Users' folder is selected and highlighted with a green oval, with a green circle containing the number '2' next to it. The right pane shows a list of users and groups, including Administrator, Allowed RODC Passwords, Cert Publishers, Cloneable Domain, Denied RODC Passwords, DHCP Administrators, DHCP Users, DnsAdmins, DnsUpdateProxy, Domain Admins, Domain Computers, Domain Controllers, Domain Guests, and Domain Users.

Name
Administrator
Allowed RODC Passwords
Cert Publishers
Cloneable Domain
Denied RODC Passwords
DHCP Administrators
DHCP Users
DnsAdmins
DnsUpdateProxy
Domain Admins
Domain Computers
Domain Controllers
Domain Guests
Domain Users

Étape 2. Cliquez avec le bouton droit sur le conteneur et sélectionnez **Propriétés**. Accédez à l'onglet *Éditeur d'attributs* et recherchez le champ *distinguéName*. Si cet onglet n'est pas visible, vous devez activer l'affichage des fonctionnalités avancées dans Utilisateurs et ordinateurs Active Directory et recommencer. Notez ce champ et cliquez sur **Annuler**. Il s'agit du chemin d'accès du conteneur utilisateur. Ce champ est également nécessaire lors de la configuration du RV340 et doit correspondre exactement.



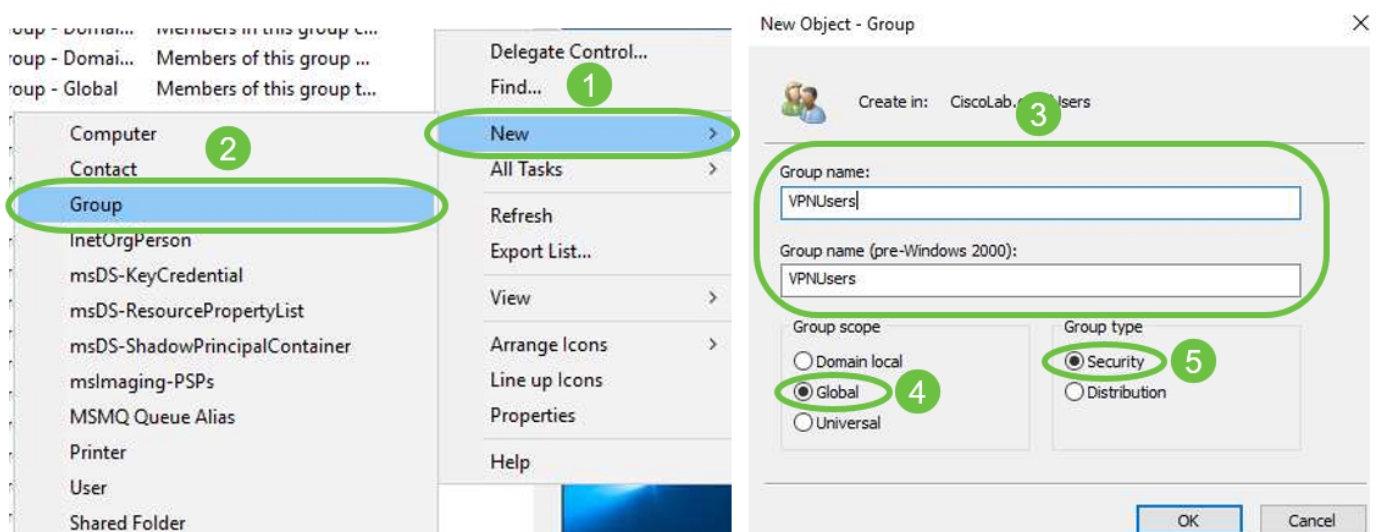
Étape 3. Créez un groupe de sécurité globale dans le même conteneur que les comptes d'utilisateurs qui seront utilisés.

Dans le conteneur sélectionné, cliquez avec le bouton droit sur une zone vide et sélectionnez **Nouveau > Groupe**.

Suivez le chemin suivant :

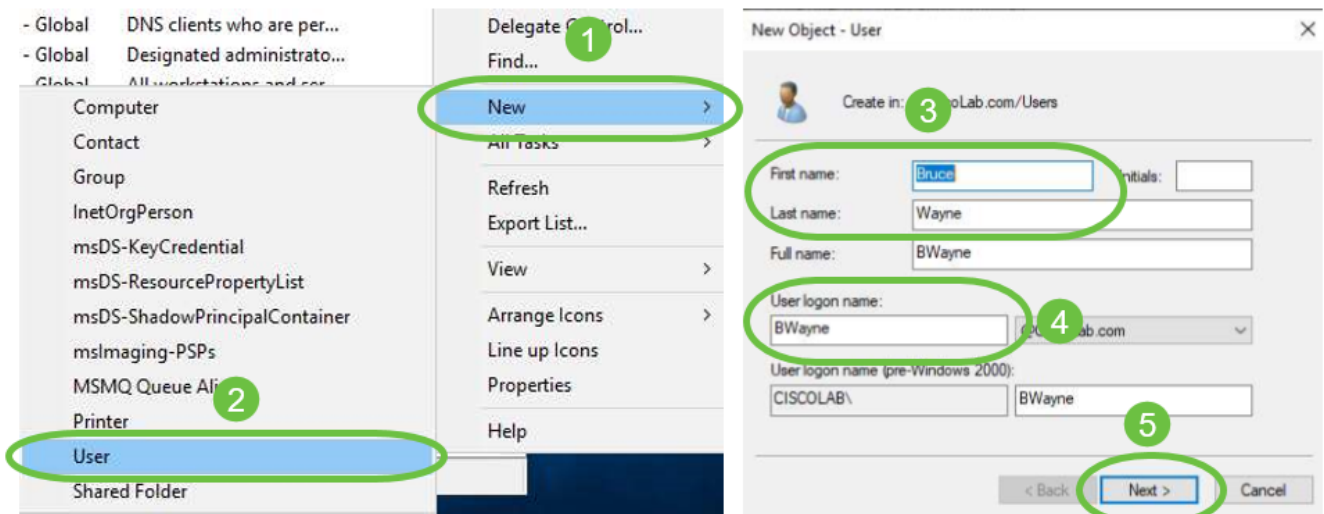
- Nom du groupe : ce nom doit correspondre exactement au nom du groupe d'utilisateurs créé sur le routeur RV340. Dans cet exemple, nous allons utiliser **des VPNUsers**.
- Portée du groupe - Globale
- Type de groupe - Sécurité

Click OK.



Étape 4. Pour créer de nouveaux comptes d'utilisateurs, procédez comme suit :

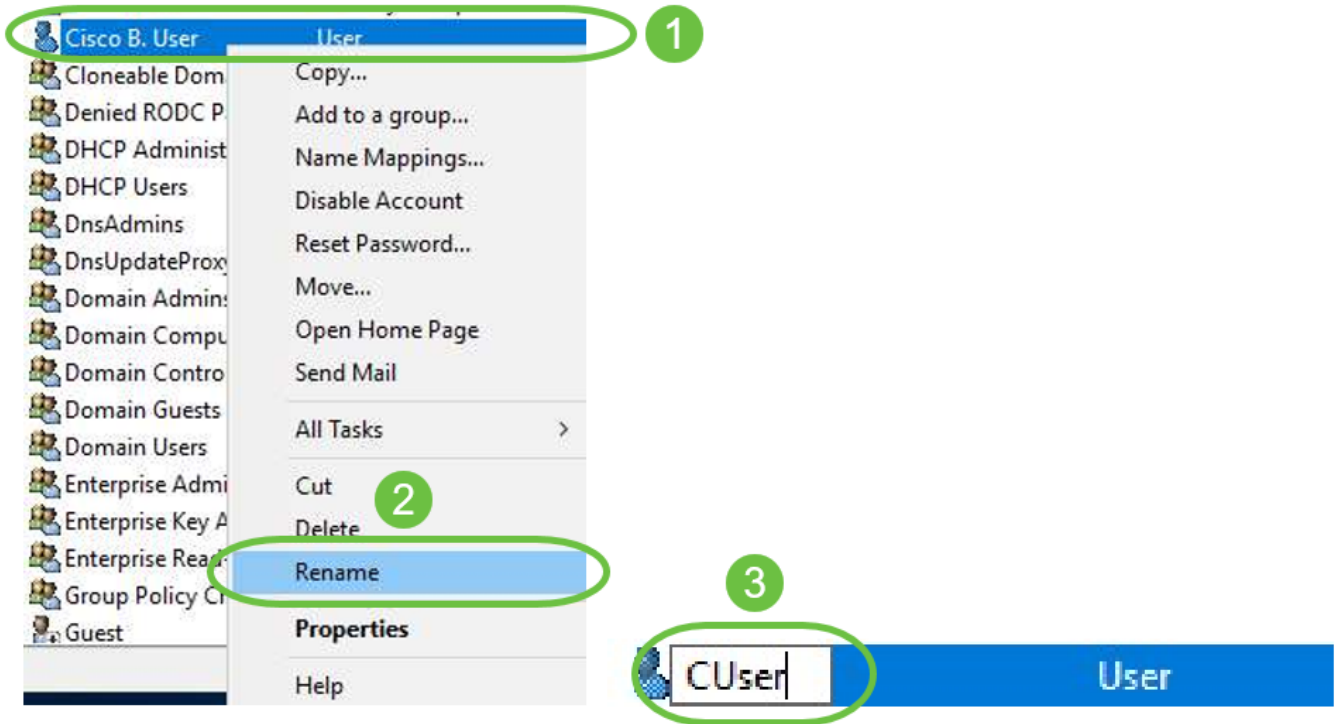
- Cliquez avec le bouton droit sur un espace vide dans le conteneur et sélectionnez **Nouveau > Utilisateur**.
- Entrez *Prénom, Nom*.
- Entrez le *nom de connexion de l'utilisateur*.
- Cliquez sur **Next** (Suivant).



Vous serez invité à saisir un mot de passe pour l'utilisateur. Si *l'utilisateur doit changer de mot de passe à la prochaine case de connexion* est cochée, il devra se connecter localement et changer de mot de passe AVANT de se connecter à distance.

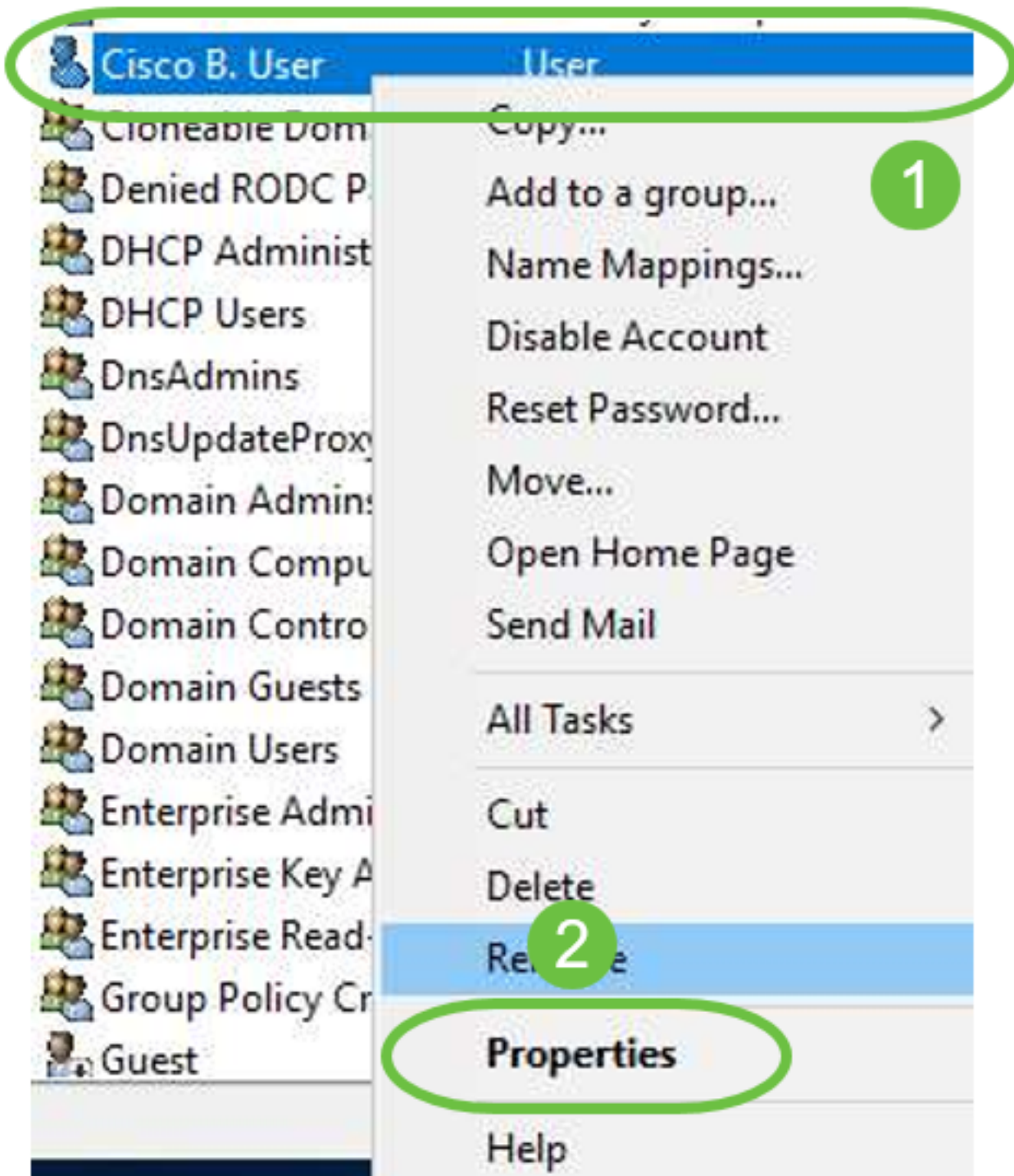
Cliquez sur Finish.

Si des comptes d'utilisateurs sont déjà créés et qu'ils doivent être utilisés, des ajustements peuvent être nécessaires. Pour ajuster le nom canonique d'un utilisateur, sélectionnez-le, cliquez avec le bouton droit de la souris et sélectionnez **Renommer**. Vérifiez que tous les espaces sont supprimés et qu'ils correspondent au nom de connexion de l'utilisateur. Ceci NE modifiera PAS le nom d'affichage des utilisateurs. Click OK.



Étape 5. Une fois que les comptes d'utilisateurs sont structurés correctement, ils doivent se voir accorder des droits de connexion à distance.

Pour ce faire, sélectionnez le compte d'utilisateur, cliquez avec le bouton droit de la souris et sélectionnez **Propriétés**.



Dans l'onglet *Propriétés utilisateur*, sélectionnez **Éditeur d'attributs** et faites défiler jusqu'à **Nom unique**. Assurez-vous que le premier **CN=** a le nom d'ouverture de session utilisateur correct sans espace.

CUser Properties 1 ? X

Security	Environment		Sessions		Remote control	
General	Address	Account	Profile	Telephones	Organization	
Published Certificates		Member Of	Password Replication		Dial	Object
Remote Desktop Services Profile			COM+		Attribute Editor	

Attributes:

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

Sélectionnez l'onglet **Membre de** et cliquez sur **Ajouter**.

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	

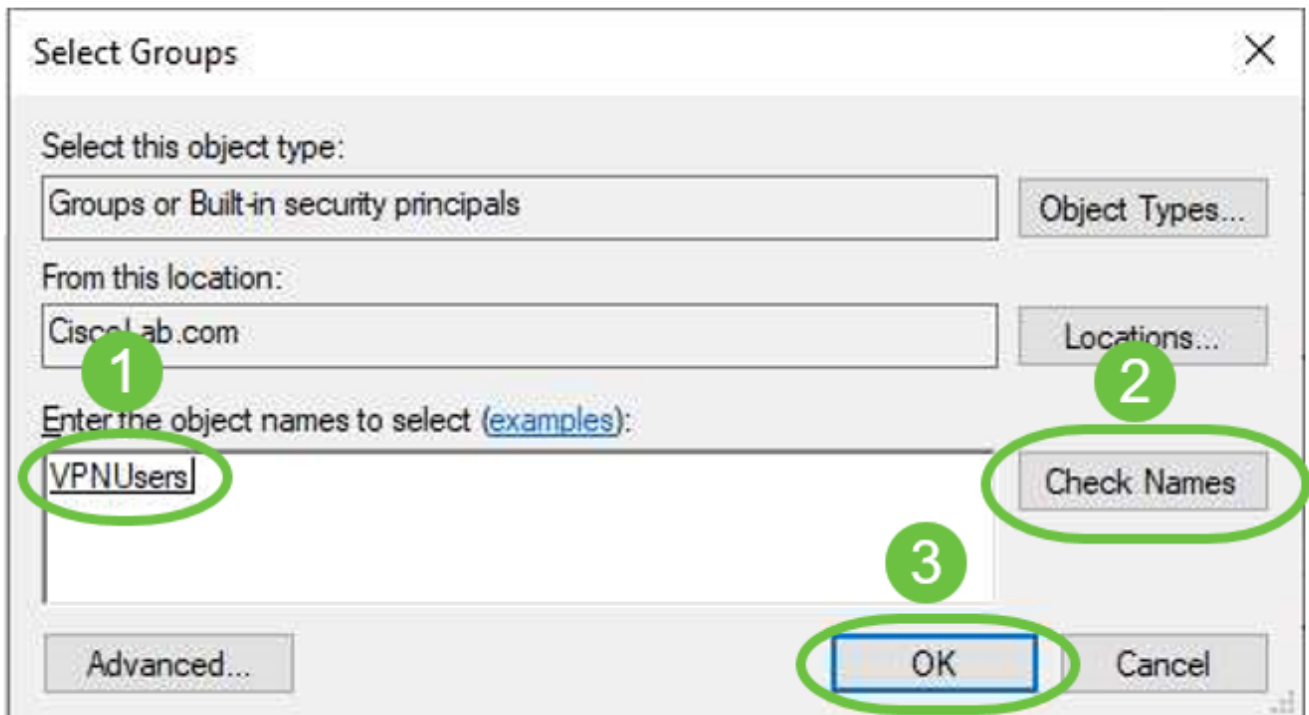
Member of:

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

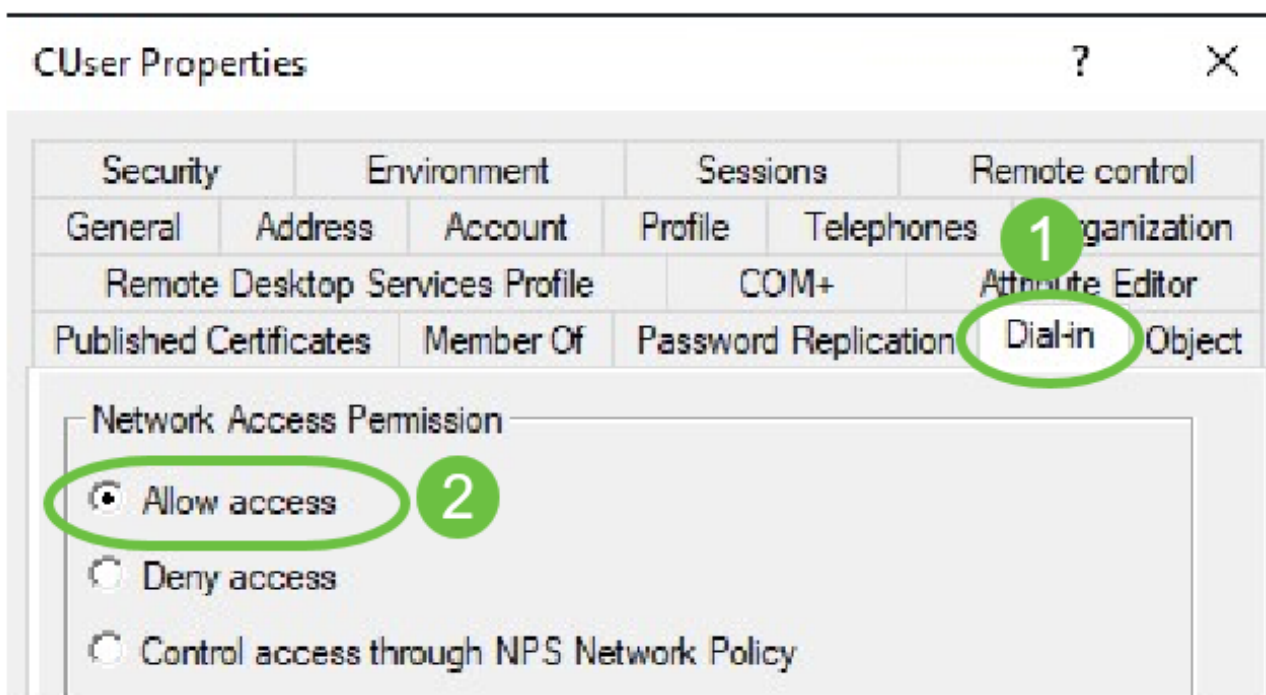
2

Add... Remove

Entrez le nom du *groupe de sécurité globale* et sélectionnez **Vérifier le nom**. Si l'entrée est soulignée, cliquez sur **OK**.



Sélectionnez l'onglet **Appel entrant**. Dans la section *Autorisation d'accès au réseau*, sélectionnez **Autoriser l'accès** et laissez le reste comme valeur par défaut.

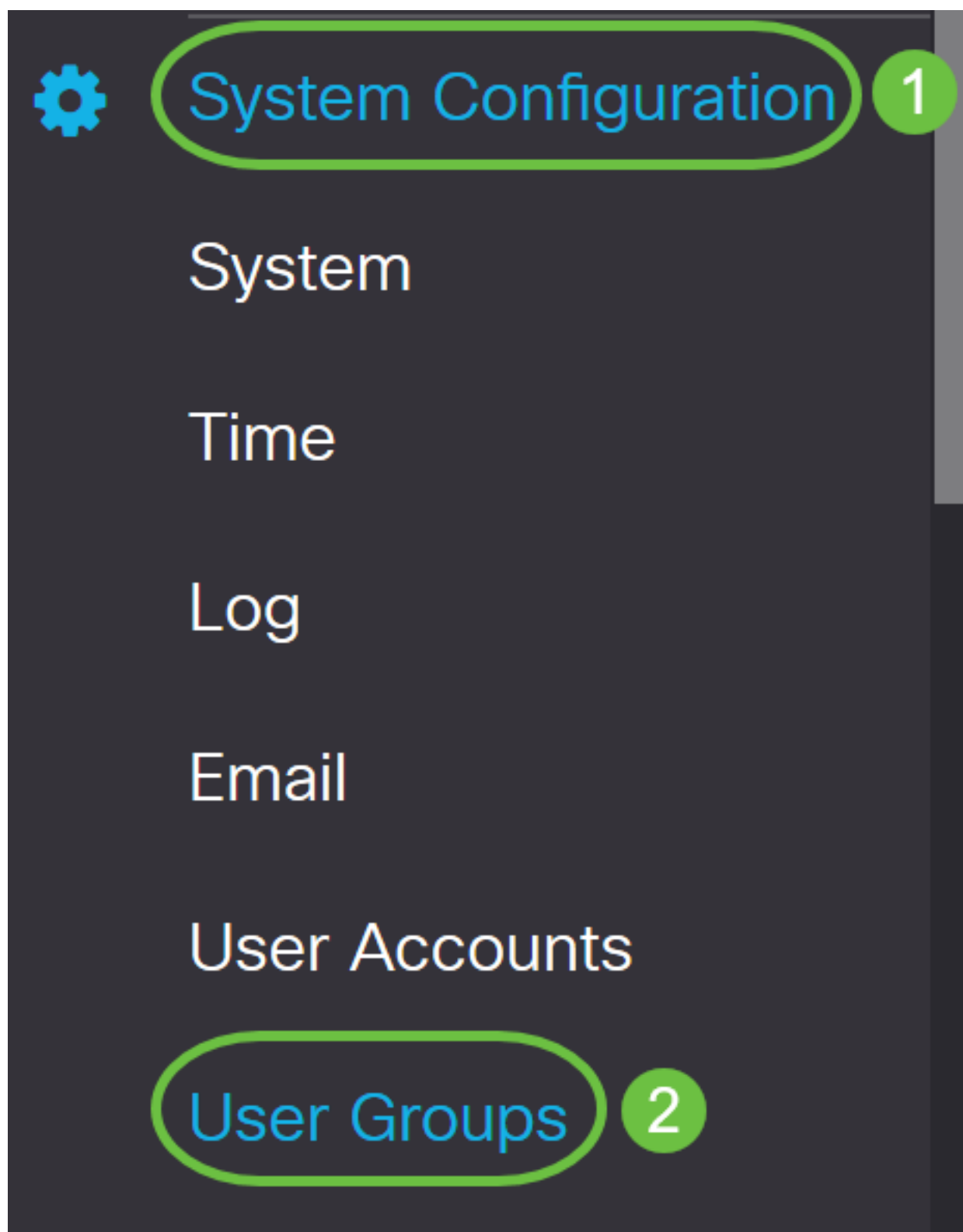


Intégration Active Directory

Active Directory nécessite que l'heure du routeur RV34x corresponde à celle du serveur AD. Pour savoir comment configurer les paramètres temporels sur un routeur de la gamme RV34x, cliquez [ici](#).

AD nécessite également que le RV340 dispose d'un groupe d'utilisateurs correspondant au groupe de sécurité globale AD.

Étape 1. Accédez à **Configuration système > Groupes d'utilisateurs**.



Étape 2. Cliquez sur l'icône **plus** pour ajouter un groupe d'utilisateurs.

User Groups

User Groups Table



Étape 3. Entrez le *nom du groupe*. Dans cet exemple, il s'agit de **VPNUsers**.

Group Name:

Le nom du groupe doit être identique au groupe de sécurité globale AD.

Étape 4. Sous *Services*, *Web Login/NETCONF/RESTCONF* doit être marqué comme **Disabled**. Si l'intégration AD ne fonctionne pas immédiatement, vous pourrez toujours accéder au RV34x.

Services

Web Login/NETCONF/RESTCONF Disabled Read Only Administrator

Étape 5. Vous pouvez ajouter les tunnels VPN qui utiliseront l'intégration AD pour connecter leurs utilisateurs.

1. Pour ajouter un VPN client à site déjà configuré, accédez à la section *EZVPN/tiers* et cliquez sur l'icône **plus**. Sélectionnez le profil VPN dans le menu déroulant et cliquez sur **Ajouter**.

EzVPN/3rd Party

EzVPN/3rd Party Profile Member In-use Table



#



Group Name



Add Feature List

Select a Profile: ShrewVPN 1

2

4. VPN SSL : si un tunnel VPN SSL est utilisé, sélectionnez la stratégie dans le menu déroulant en regard de *Sélectionner un profil*.

SSL VPN

Select a Profile

SSLVPNDefaultPolicy

6. PPTP/L2TP/802.1x - Pour autoriser ces utilisateurs à utiliser AD, cochez simplement la case en regard de ceux-ci pour *autoriser*.

PPTP VPN



Permit

L2TP



Permit

802.1x



Permit

Étape 6. Cliquez sur **apply** pour enregistrer vos modifications.

User Groups

Apply

Site to Site VPN Profile Member In-use Table

+ 🗑️

⌵ Connection Name ⌵

EzVPN/3rd Party

EzVPN/3rd Party Profile Member In-use Table

+ 🗑️

⌵ Group Name ⌵

SSL VPN Select a Profile SSLVPNDefaultPolicy ⌵

PPTP VPN Permit

L2TP Permit

802.1x Permit

Paramètres d'intégration Active Directory

Étape 1. Accédez à **Configuration système > Comptes d'utilisateurs**.



System Configuration

System

1

Time

Log

Email

User Accounts

2

Étape 2. Dans la table Remote Authentication Service, cliquez sur **Add** pour créer une entrée.

Remote Authentication Service Table



Enable ⇅

Name ⇅

Étape 3. Dans le champ *Nom*, créez un nom d'utilisateur pour le compte. Dans cet exemple, **Jorah_Admin** est utilisé.

Add/Edit New Domain

Name

Jorah_Admin

Étape 4. Dans le menu déroulant *Type d'authentification*, sélectionnez **Active Directory**. AD est utilisé pour affecter des stratégies étendues à tous les éléments du réseau, déployer des programmes sur de nombreux ordinateurs et appliquer des mises à jour critiques à l'ensemble de l'organisation.

Authentication Type

Active Directory

AD Domain Name

RADIUS

Active Directory

Primary Server

LDAP

Étape 5. Dans le champ *Nom de domaine AD*, saisissez le nom de domaine complet de l'AD.

Dans cet exemple, **sampledomain.com** est utilisé.

AD Domain Name

Étape 6. Dans le champ *Serveur principal*, saisissez l'adresse de la distance administrative.

Dans cet exemple, **192.168.2.122** est utilisé.

Primary Server Port

Étape 7. Dans le champ *Port*, saisissez un numéro de port pour le serveur principal.

Dans cet exemple, **1234** est utilisé comme numéro de port.

Primary Server Port

Étape 8. (Facultatif) Dans le champ *Chemin du conteneur utilisateur*, entrez un chemin racine où les utilisateurs sont contenus.

Note: Dans cet exemple, **file:Documents/manage/containers** est utilisé.

User Container Path

Étape 9. Cliquez sur Apply.

User Accounts

Add/Edit New Domain

Name

Authentication Type

AD Domain Name

Primary Server Port

User Container Path

Étape 10. Faites défiler jusqu'à *Séquence d'authentification* du service pour définir la méthode de

connexion pour les différentes options.

- Web Login/NETCONF/RESTCONF - C'est ainsi que vous vous connectez au routeur RV34x. Décochez la case *Utiliser par défaut* et définissez la méthode principale sur **Base de données locale**. Vous ne serez pas déconnecté du routeur même si l'intégration Active Directory échoue.
- VPN de site à site/EzVPN&de client à site tiers : il s'agit de configurer le tunnel VPN de client à site pour qu'il utilise AD. Décochez la case *Utiliser par défaut* et définissez la méthode principale sur **Active Directory** et la méthode secondaire sur **base de données 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

Étape 11. Cliquez sur 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

Étape 12. Enregistrez votre configuration en cours dans la configuration de démarrage.

Vous avez maintenant correctement configuré les paramètres Active Directory sur un routeur de la gamme RV34x.

LDAP

Étape 1. Dans la table Remote Authentication Service, cliquez sur **Add** pour créer une entrée.

Remote Authentication Service Table



Enable  Name 

Étape 2. Dans le champ *Nom*, créez un nom d'utilisateur pour le compte.

Seul un seul compte d'utilisateur distant sous LDAP peut être configuré.

Dans cet exemple, Dany_Admin est utilisé.

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

Étape 3. Dans le menu déroulant Type d'authentification, sélectionnez **LDAP**. Lightweight Directory Access Protocol est un protocole d'accès utilisé pour accéder à un service d'annuaire. Il s'agit d'un serveur distant qui exécute un serveur de répertoire pour effectuer l'authentification pour le domaine.

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"/>

Étape 4. Dans le *champ Serveur principal*, saisissez l'adresse du serveur LDAP.

Dans cet exemple, 192.168.7.122 est utilisé.

Primary Server Port

Étape 5. Dans le champ *Port*, saisissez un numéro de port pour le serveur principal.

Dans cet exemple, **122** est utilisé comme numéro de port.

Primary Server Port

Étape 6. Entrez le nom unique de base du serveur LDAP dans le champ *DN de base*. Le DN de base est l'emplacement où le serveur LDAP recherche des utilisateurs lorsqu'il reçoit une demande d'autorisation. Ce champ doit correspondre au DN de base configuré sur le serveur LDAP.

Dans cet exemple, **Dept101** est utilisé.

Base DN

Étape 7. Cliquez sur *Apply*. Vous accédez à la table Remote Authentication Service.



User Accounts

Add/Edit New Domain

Name

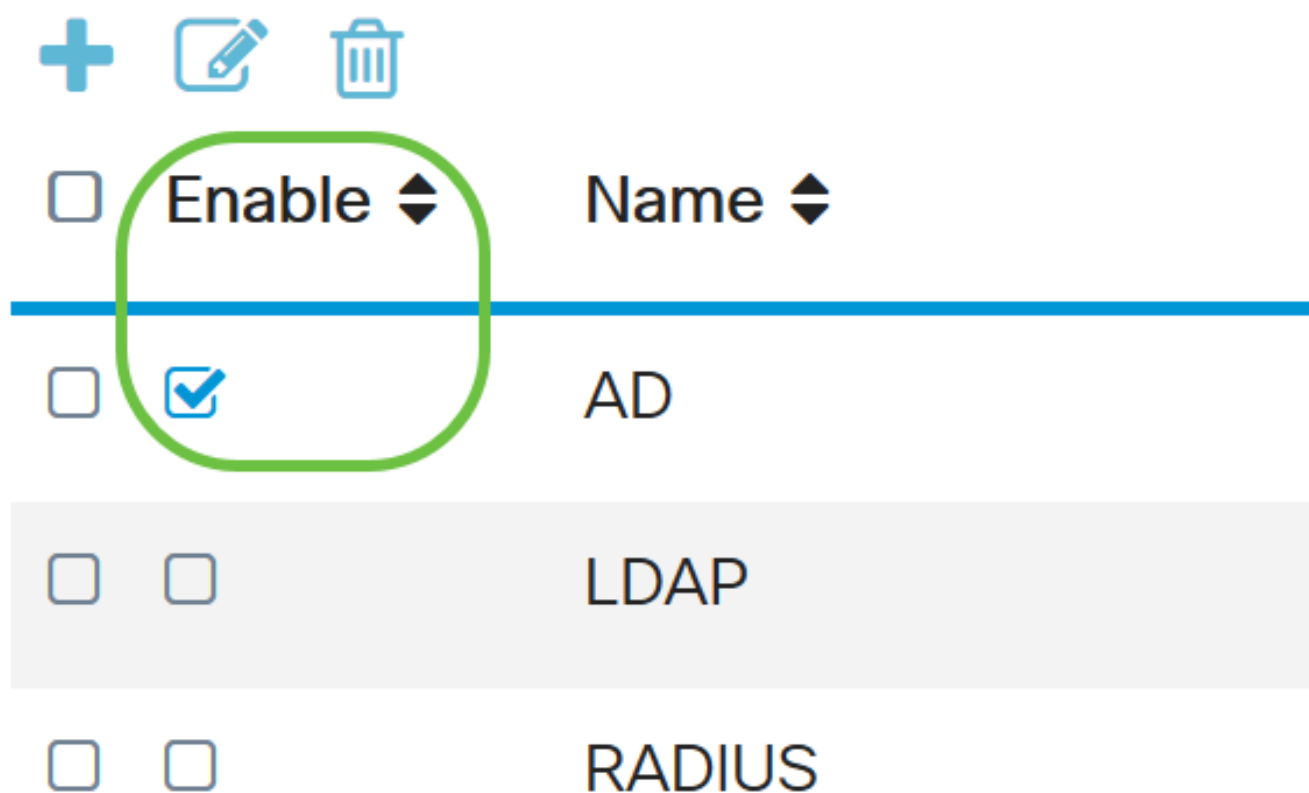
Authentication Type

Primary Server Port

Base DN

Étape 8. (Facultatif) Si vous souhaitez activer ou désactiver le service d'authentification à distance, cochez ou décochez la case en regard du service que vous souhaitez activer ou désactiver.

Remote Authentication Service Table



The image shows a table for configuring Remote Authentication Services. At the top, there are three icons: a plus sign for adding, a pencil for editing, and a trash can for deleting. The table has a header row with a checkbox, a dropdown menu labeled 'Enable', and a column labeled 'Name'. Below the header, there are three rows: 'AD' (with a checked checkbox), 'LDAP' (with an unchecked checkbox), and 'RADIUS' (with an unchecked checkbox). A green circle highlights the 'Enable' dropdown and the checked checkbox for 'AD'.

<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

Étape 9. Cliquez sur Apply.

User Accounts

Apply

Vous avez maintenant correctement configuré LDAP sur un routeur de la gamme RV34x.

[Afficher une vidéo relative à cet article...](#)

[Cliquez ici pour afficher d'autres présentations techniques de Cisco](#)