Remote Authentication and Login Guidance Using Active Directory and RV34x Routers

Objective

This article explains how to configure remote authentication using Windows Active Directory (AD) on Cisco RV34x series routers. In addition, information will be provided to avoid a potential login error.

Introduction

When you configure the service authentication settings on the RV34x router, you need to select an external authentication method.

By default, the external database priority on the RV34x series router is RADIUS/LDAP/AD/Local. If you add the RADIUS server on the router, the Web Login Service and other services will use the RADIUS external database to authenticate the user. There is no option to enable an external database for Web Login Service alone and configure another database for another service. Once RADIUS is created and enabled on the router, the router will use the RADIUS service as an external database for Web Login, Site-to-Site VPN, EzVPN/3rd Party VPN, SSL VPN, PPTP/L2TP VPN, and 802.1x.

If you use Windows, Microsoft provides an internal AD Service. AD stores all of the essential information for the network including users, devices, and policies. Administrators use AD as a single place to create and manage the network. It facilitates working with interconnected, complex, and different network resources in a unified manner.

Once configured, anyone authorized can authenticate using the external AD option (present in Windows server OS) to use any specific service on the RV34x router. Authorized users can use the features provided, as long as they have the required hardware and software to use that type of authentication.

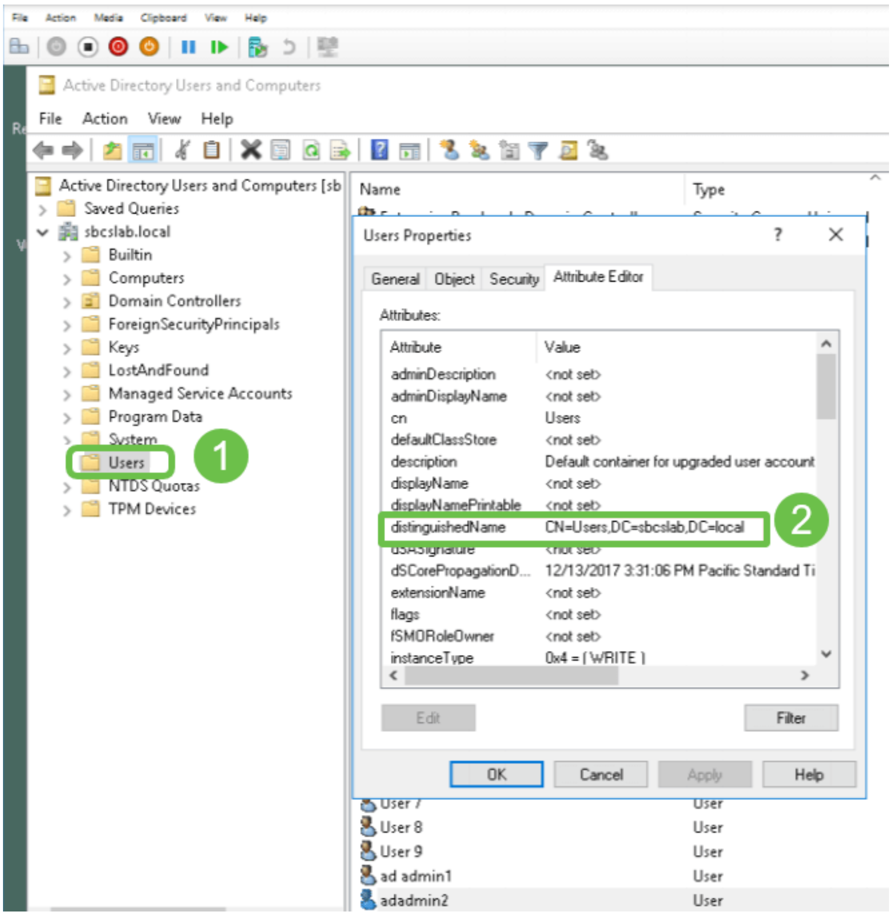
Applicable Devices | Software Version

- RV340 | 1.0.03.16
- RV340W | 1.0.03.16
- RV345 | 1.0.03.16
- RV345P | 1.0.03.16

Table of Contents

Identify the Distinguished Name Value

Access the *Active Directory Users and Computers* management interface on the Windows 2016 server. Select the **Users** container folder, right-click the mouse, and open **Properties**. Take note of the *DistinguishedName* value that will be used later in the RV34x router *User Container Path* field.



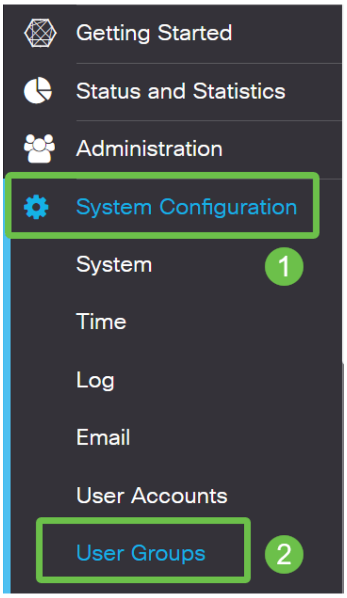
Attribute	Value
adminDescription	<not set>
adminDisplayName	<not set>
cn	Users
defaultClassStore	<not set>
description	Default container for upgraded user account
displayName	<not set>
displayNamePrintable	<not set>
distinguishedName	CN=Users,DC=sbcslab,DC=local
dSASignature	<not set>
dSCorePropagationD...	12/13/2017 3:31:06 PM Pacific Standard Ti
extensionName	<not set>
flags	<not set>
fSMORoleOwner	<not set>
instanceType	0x4 = (WRITE)

Name	Type
User 7	User
User 8	User
User 9	User
ad admin1	User
adadmin2	User

Create a User Group for Active Directory

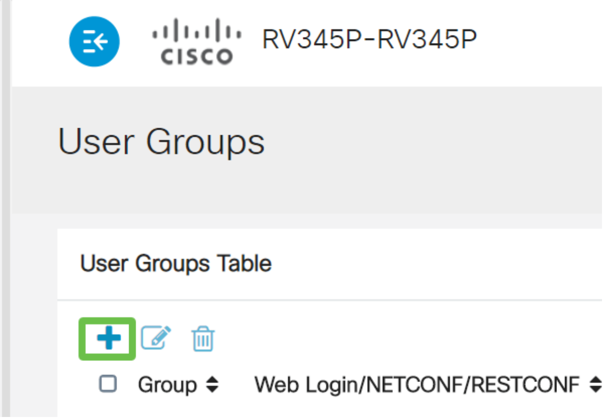
Step 1

Log into the RV34x series router. Navigate to **System Configuration > User Groups**.



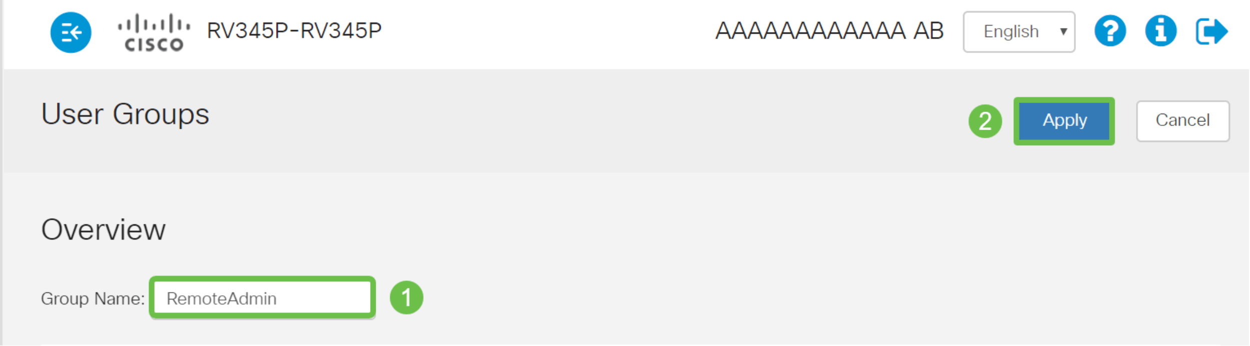
Step 2

Click on the **plus icon**.



Step 3

Enter a *Group Name*. Click **Apply**.

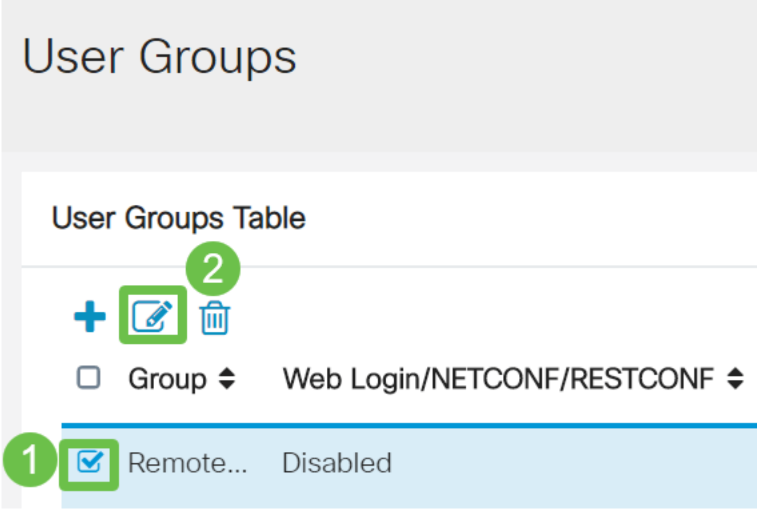


Group Name: RemoteAdmin

In this example, a *RemoteAdmin* User Group has been created.

Step 4

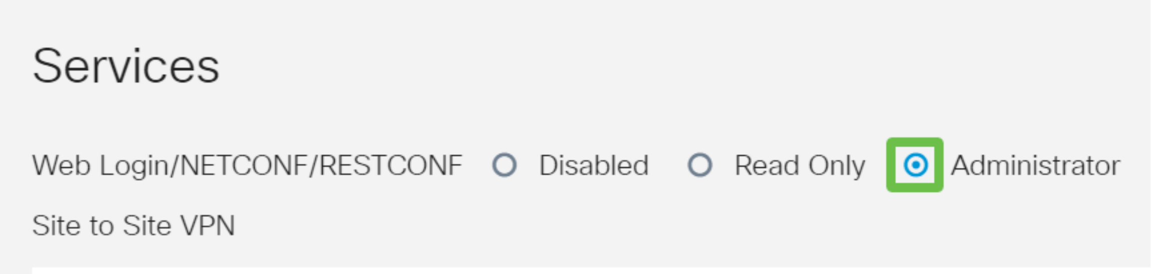
Click the checkbox next to the new User Group. Click the **edit icon**.



□	Group	Web Login/NETCONF/RESTCONF
☑	Remote...	Disabled

Step 5

Scroll down the page to *Services*. Click the **Administrator** radio button.



Web Login/NETCONF/RESTCONF ○ Disabled ○ Read Only ● Administrator

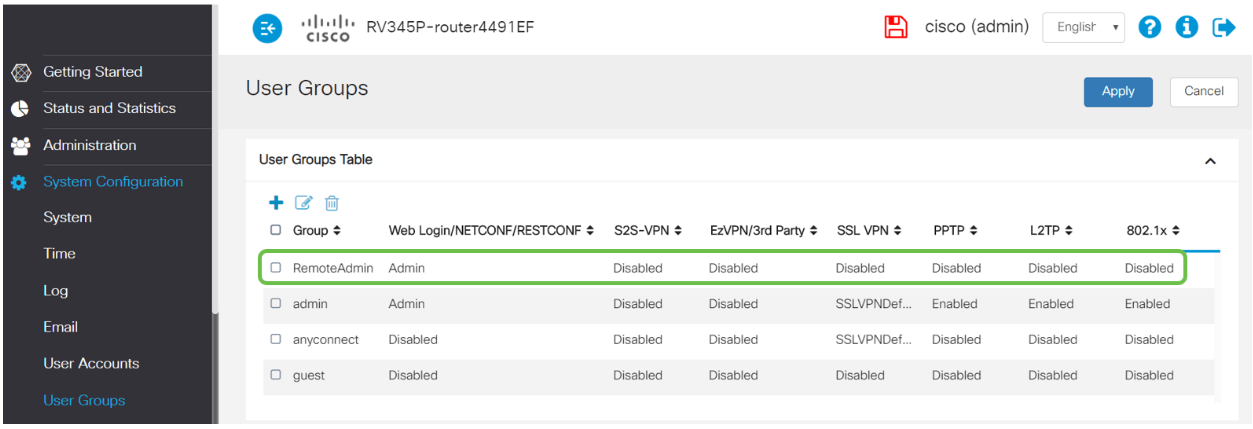
Site to Site VPN

Step 6

Click **Apply**.

Step 7

You will now see the new User Group showing with Admin privileges.



User Groups

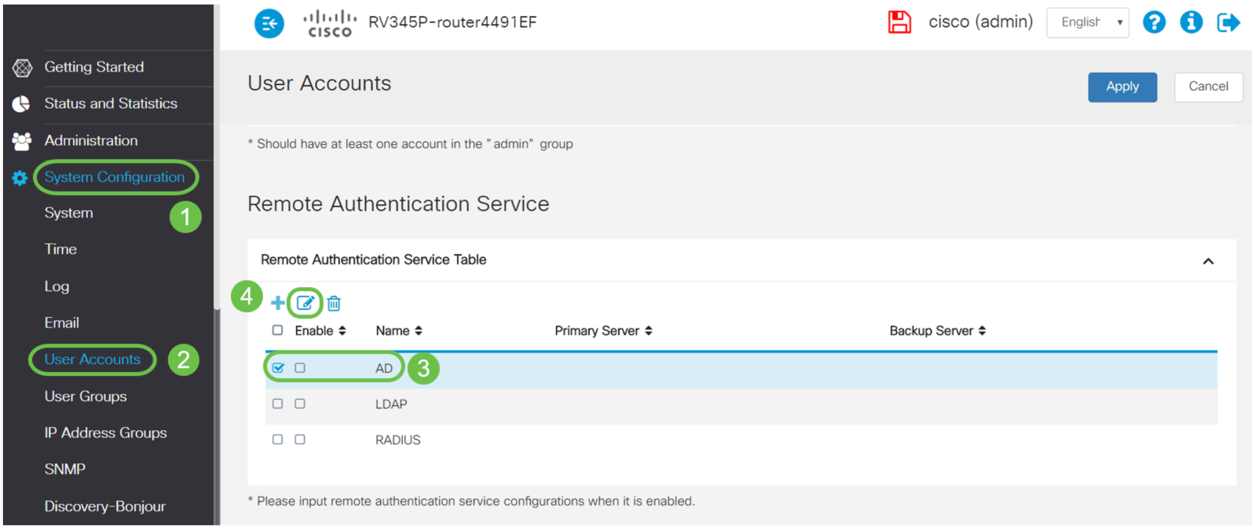
User Groups Table

□ Group	Web Login/NETCONF/RESTCONF	S2S-VPN	EzVPN/3rd Party	SSL VPN	PPTP	L2TP	802.1x
□ RemoteAdmin	Admin	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
□ admin	Admin	Disabled	Disabled	SSLVPNDef...	Enabled	Enabled	Enabled
□ anyconnect	Disabled	Disabled	Disabled	SSLVPNDef...	Disabled	Disabled	Disabled
□ guest	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled

Add Active Directory Details on the RV34x Router

Step 1

Navigate to **System Configuration > User Accounts.** Select the *AD* option and click the **edit icon** to add the details for the AD server.



User Accounts

* Should have at least one account in the " admin" group

Remote Authentication Service

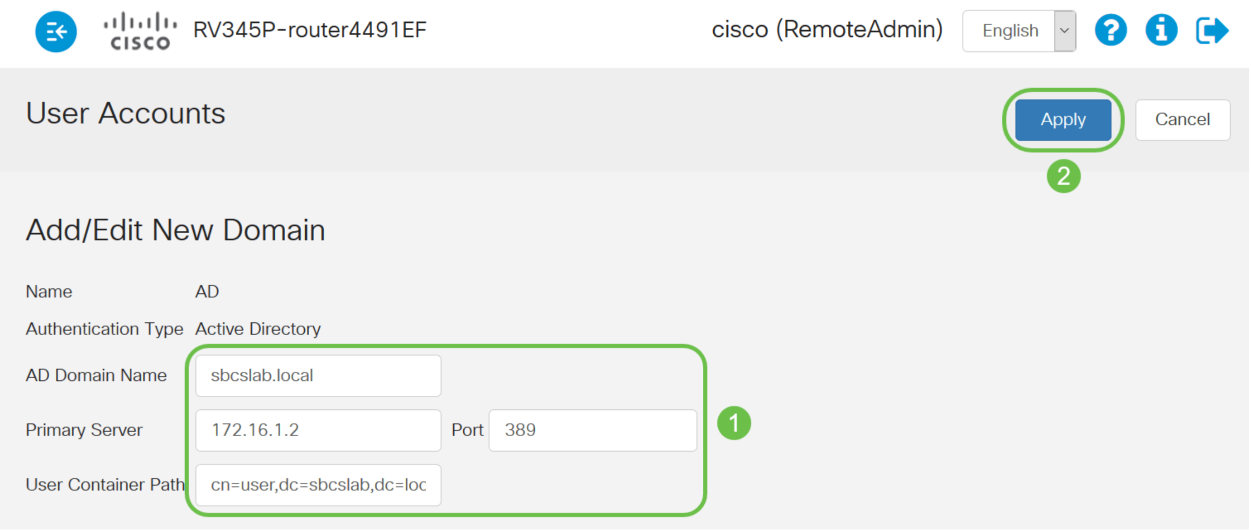
Remote Authentication Service Table

□	Enable	Name	Primary Server	Backup Server
☑	□	AD		
□	□	LDAP		
□	□	RADIUS		

* Please input remote authentication service configurations when it is enabled.

Step 2

Enter the *AD Domain Name*, *Primary Server*, *Port*, and *User Container Path* details. Click **Apply**.



User Accounts

Add/Edit New Domain

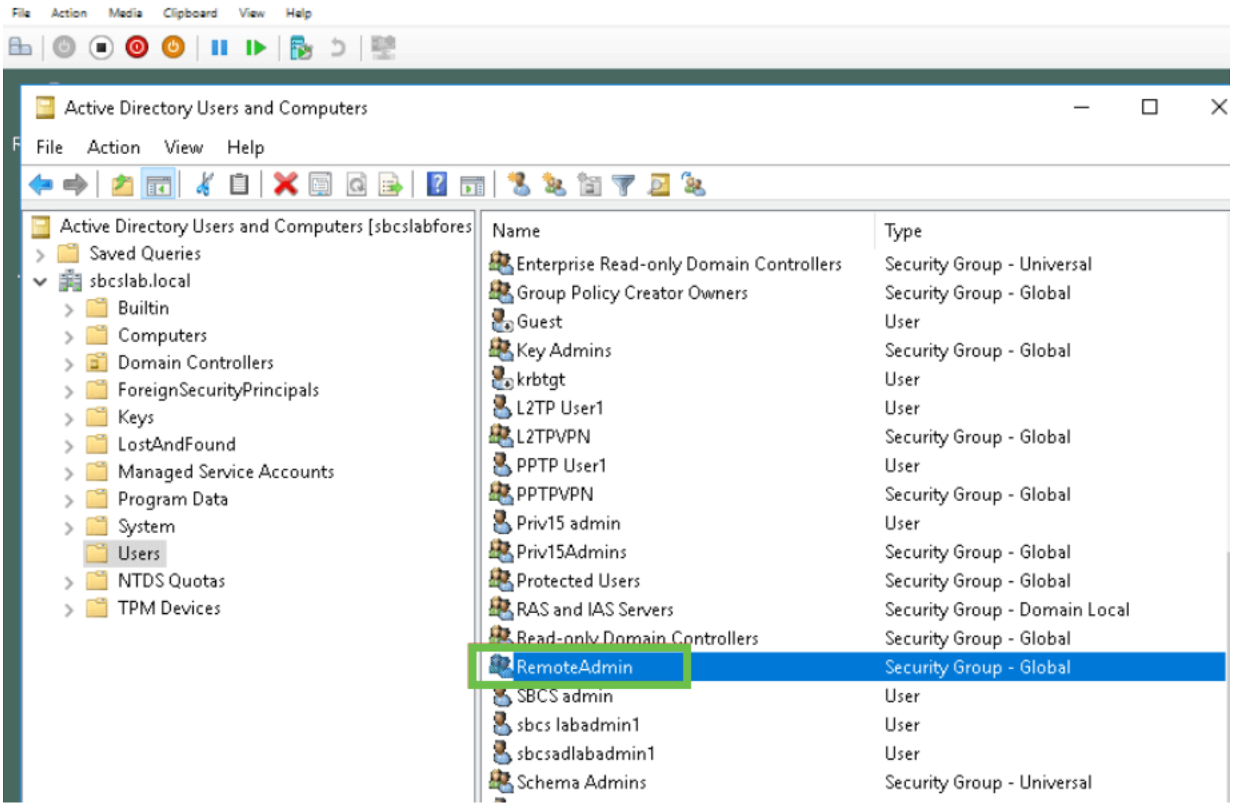
Name	AD
Authentication Type	Active Directory
AD Domain Name	sbcslab.local
Primary Server	172.16.1.2 Port 389
User Container Path	cn=user,dc=sbcslab,dc=loc

Note: You need to enter the *User Container Path* details captured from the Windows server in the **Identify the Distinguished Name Value** section of this article.

In this example, the details are *Cn=user,dc=sbcslab,dc=local*. The Lightweight Directory Access Protocol (LDAP) server default listening port is 389.

Step 3

In the AD, verify that the *User Group* is configured, and it matches router's *User Group* name.



- Active Directory Users and Computers [sbcslabfores
  - Saved Queries
  - sbcslab.local
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Keys
    - LostAndFound
    - Managed Service Accounts
    - Program Data
    - System
    - Users
    - NTDS Quotas
    - TPM Devices

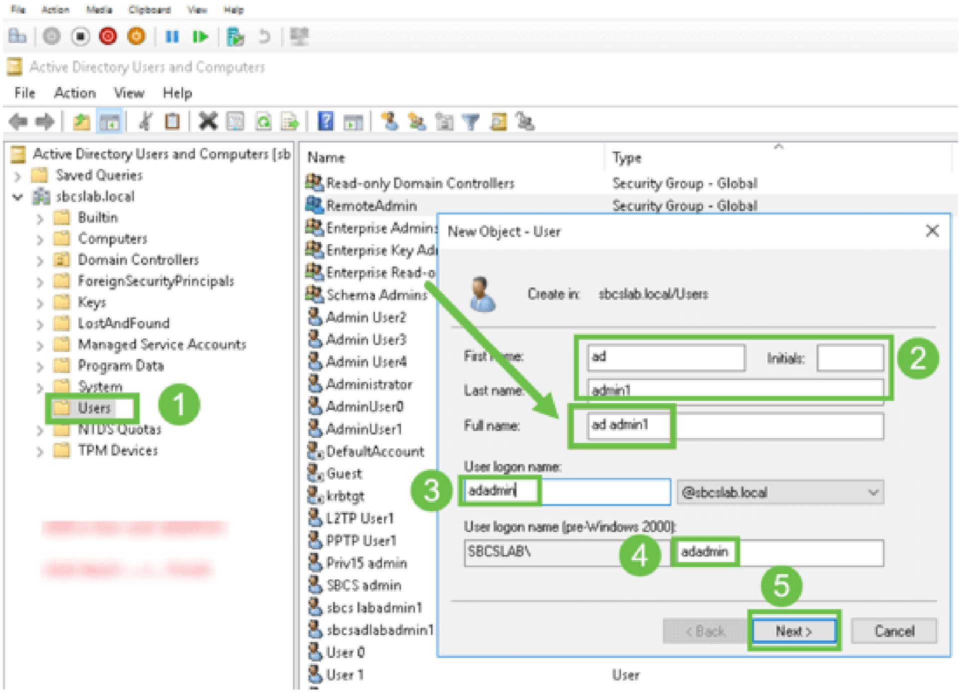
Name	Type
Enterprise Read-only Domain Controllers	Security Group - Universal
Group Policy Creator Owners	Security Group - Global
Guest	User
Key Admins	Security Group - Global
krbtgt	User
L2TP User1	User
L2TPVPN	Security Group - Global
PPTP User1	User
PPTPVPN	Security Group - Global
Priv15 admin	User
Priv15Admins	Security Group - Global
Protected Users	Security Group - Global
RAS and IAS Servers	Security Group - Domain Local
Read-only Domain Controllers	Security Group - Global
RemoteAdmin	Security Group - Global
SBCS admin	User
sbcs labadmin1	User
sbcsadlabadmin1	User
Schema Admins	Security Group - Universal

Step 4

Under *New Object – User*, fill in *First name*, *Initials* and *Last name*, The *Full name* field will be populated automatically, showing a space between the first and last name.

The space between the first and last name in the *Full name* box must be deleted or it will not login properly.

This image shows the space in the Full name that must be deleted:



[redacted]

Name	Type
Read-only Domain Controllers	Security Group - Global
RemoteAdmin	Security Group - Global
Enterprise Admins	
Enterprise Key Ad	
Enterprise Read-o	
Schema Admins	
Admin User2	
Admin User3	
Admin User4	
Administrator	
AdminUser0	
AdminUser1	
DefaultAccount	
Guest	
krbtgt	
L2TP User1	
PPTP User1	
Priv15 admin	
SBCS admin	
sbcs labadmin1	
sbcsadlabadmin1	
User 0	
User 1	User

New Object - User

Create in: sbcslab.local/Users

First name: ad Initials:

Last name: admin1

Full name: ad admin1

User logon name: adadmin @sbcslab.local

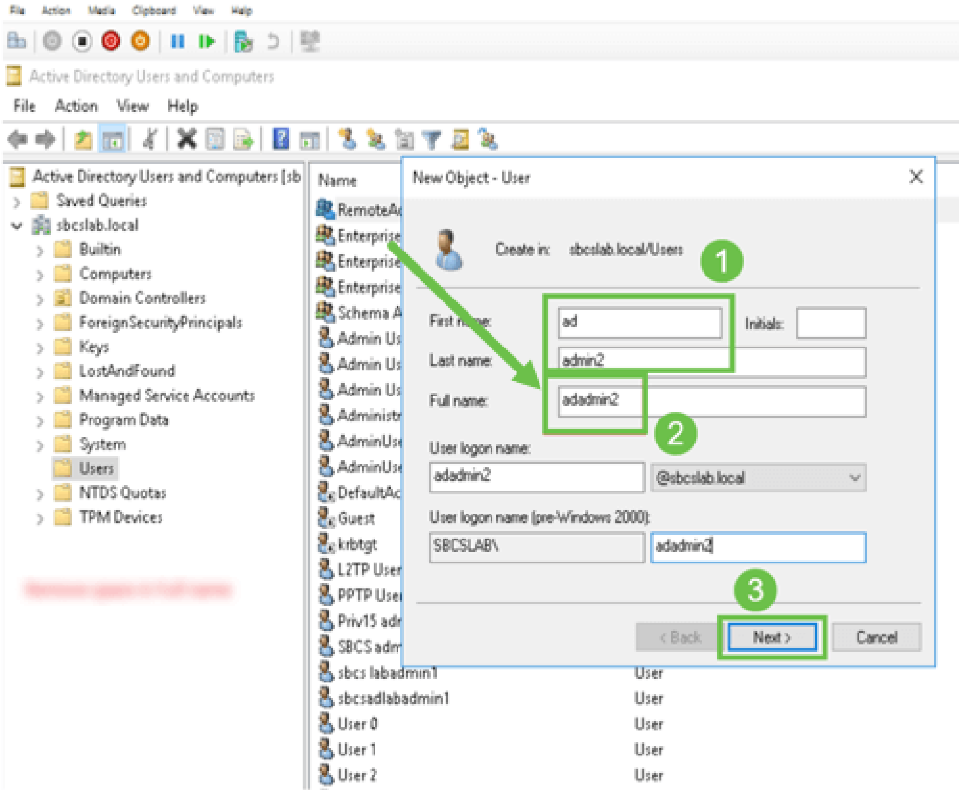
User logon name (pre-Windows 2000): SBCSLAB\ adadmin

< Back Next > Cancel

Step 5

Repeat the steps to create another user. Once again, you need to modify the *Full Name* field by removing any spaces automatically created. Click **Next** to set up the password and finish creating the user.

This image shows that the space in the Full name was deleted. This is the correct way to add the user:



[redacted]

Name	
RemoteA	
Enterprise	
Enterprise	
Enterprise	
Schema A	
Admin Us	
Admin Us	
Admin Us	
Administr	
AdminUse	
AdminUse	
DefaultAc	
Guest	
krbtgt	
L2TP User	
PPTP User	
Priv15 adr	
SBCS adm	
sbcs labadmin1	User
sbcsadlabadmin1	User
User 0	User
User 1	User
User 2	User

New Object - User

Create in: sbcslab.local/Users

First name: ad Initials:

Last name: admin2

Full name: adadmin2

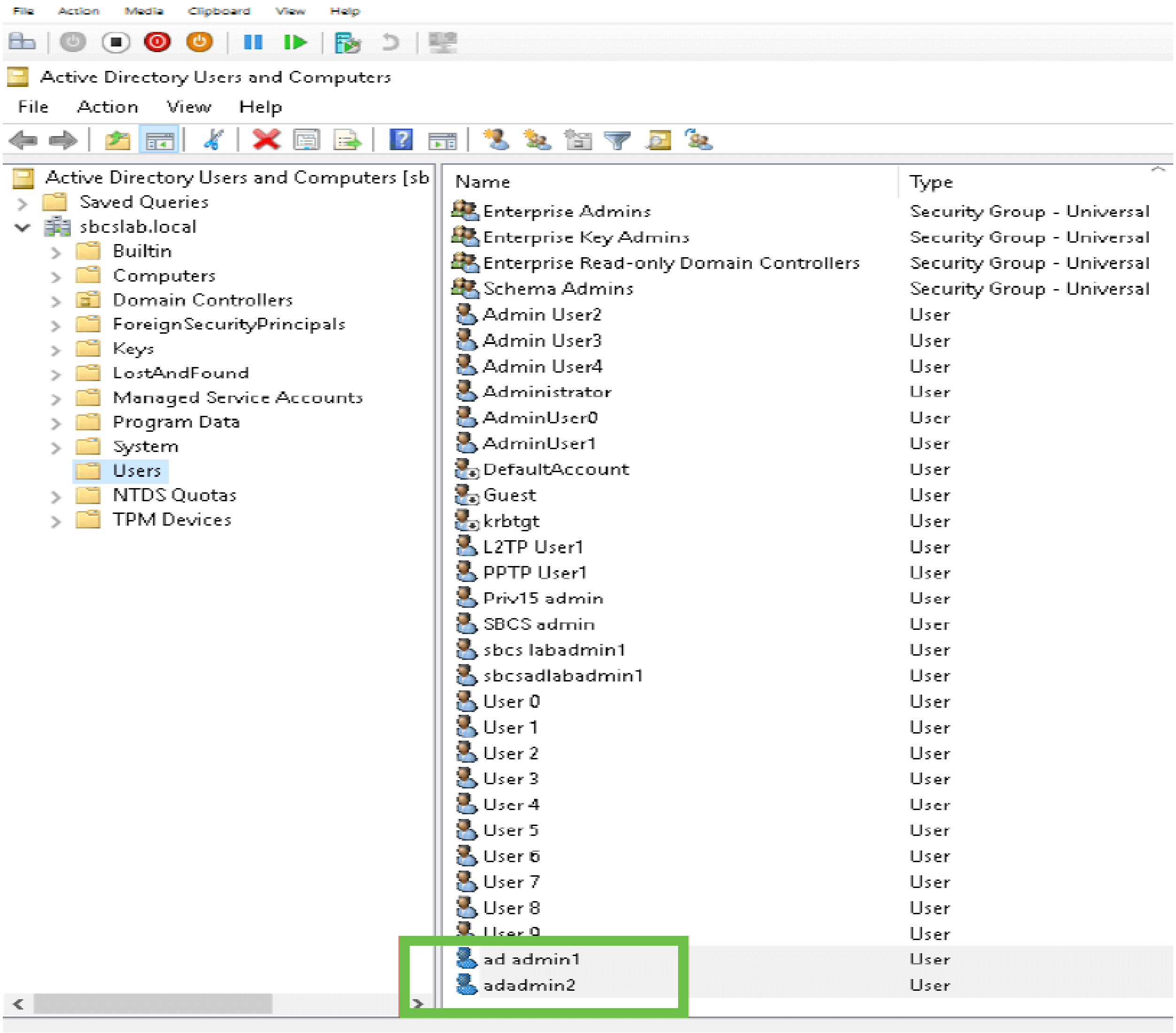
User logon name: adadmin2 @sbcslab.local

User logon name (pre-Windows 2000): SBCSLAB\ adadmin2

< Back Next > Cancel

Step 6

The Users list will show both of the newly added user details.


File Action Media Clipboard View Help
Active Directory Users and Computers
File Action View Help

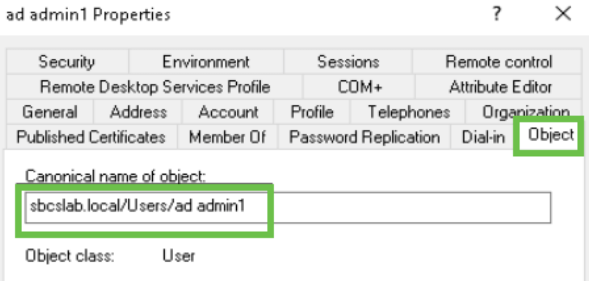
- Active Directory Users and Computers [sb
  - Saved Queries
  - sbcslab.local
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Keys
    - LostAndFound
    - Managed Service Accounts
    - Program Data
    - System
    - Users
    - NTDS Quotas
    - TPM Devices

Name	Type
Enterprise Admins	Security Group - Universal
Enterprise Key Admins	Security Group - Universal
Enterprise Read-only Domain Controllers	Security Group - Universal
Schema Admins	Security Group - Universal
Admin User2	User
Admin User3	User
Admin User4	User
Administrator	User
AdminUser0	User
AdminUser1	User
DefaultAccount	User
Guest	User
krbtgt	User
L2TP User1	User
PPTP User1	User
Priv15 admin	User
SBCS admin	User
sbcs labadmin1	User
sbcsadlabadmin1	User
User 0	User
User 1	User
User 2	User
User 3	User
User 4	User
User 5	User
User 6	User
User 7	User
User 8	User
User 9	User
ad admin1	User
adadmin2	User

Step 7

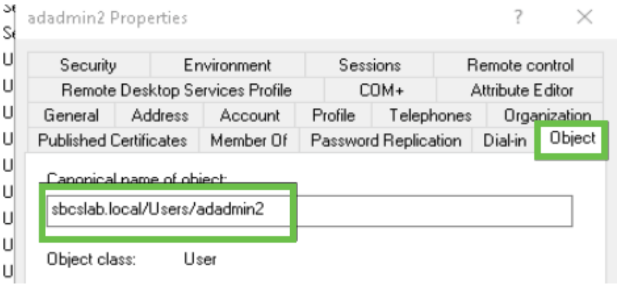
You will notice that the *ad admin1* shows a space between the first and last name, if this is not fixed, login will fail. This error is being left in for demonstration purposes, do not leave the space there! The *adadmin2* example is correct.

To view, right-click on the *ad admin 1* username and select the **Properties** option. Then navigate to the **Object** tab to see the *Canonical name of Object* details.



Canonical name of object:
sbcslab.local/Users/ad admin1

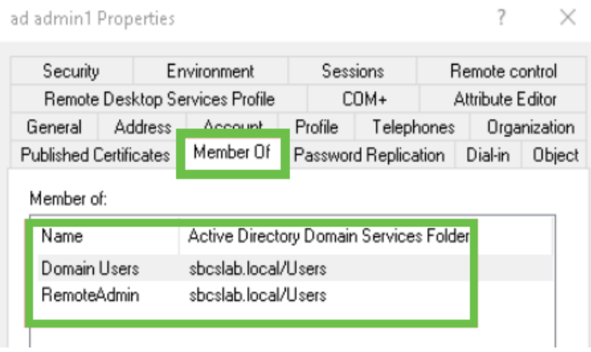
Object class: User



Canonical name of object:
sbcslab.local/Users/adadmin2

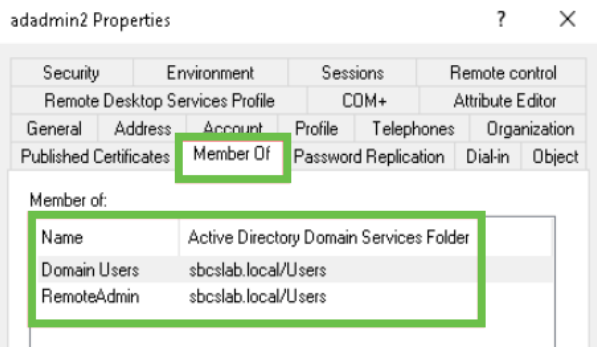
Object class: User

Also, you can verify the *Domain Users* and *RemoteAdmin* details for those usernames by navigating to the *Member Of* tab under the **Properties** option.



Member of:

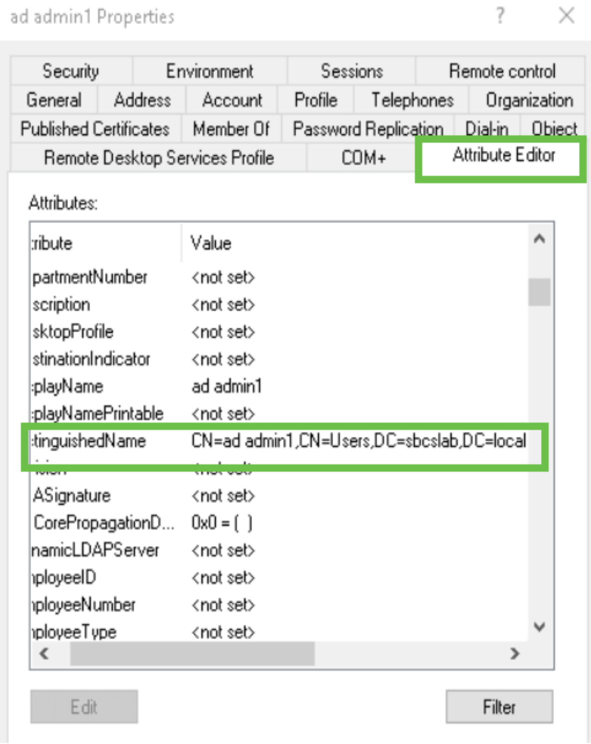
Name	Active Directory Domain Services Folder
Domain Users	sbcslab.local/Users
RemoteAdmin	sbcslab.local/Users



Member of:

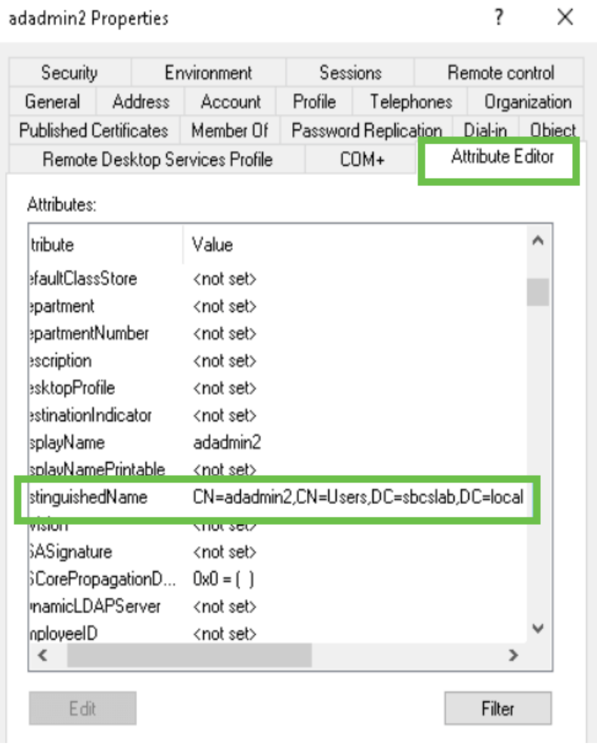
Name	Active Directory Domain Services Folder
Domain Users	sbcslab.local/Users
RemoteAdmin	sbcslab.local/Users

Navigate to the*Attribute Editor* tab to verify the *DistinguishedName* values for those usernames.



Attributes:

ribute	Value
partmentNumber	<not set>
scription	<not set>
sktopProfile	<not set>
stinationIndicator	<not set>
playName	ad admin1
playNamePrintable	<not set>
tinguishedName	CN=ad admin1,CN=Users,DC=sbcslab,DC=local
ASignature	<not set>
CorePropagationD...	0x0 = ( )
namicLDAPServer	<not set>
ployeeID	<not set>
ployeeNumber	<not set>
ployeeType	<not set>



Attributes:

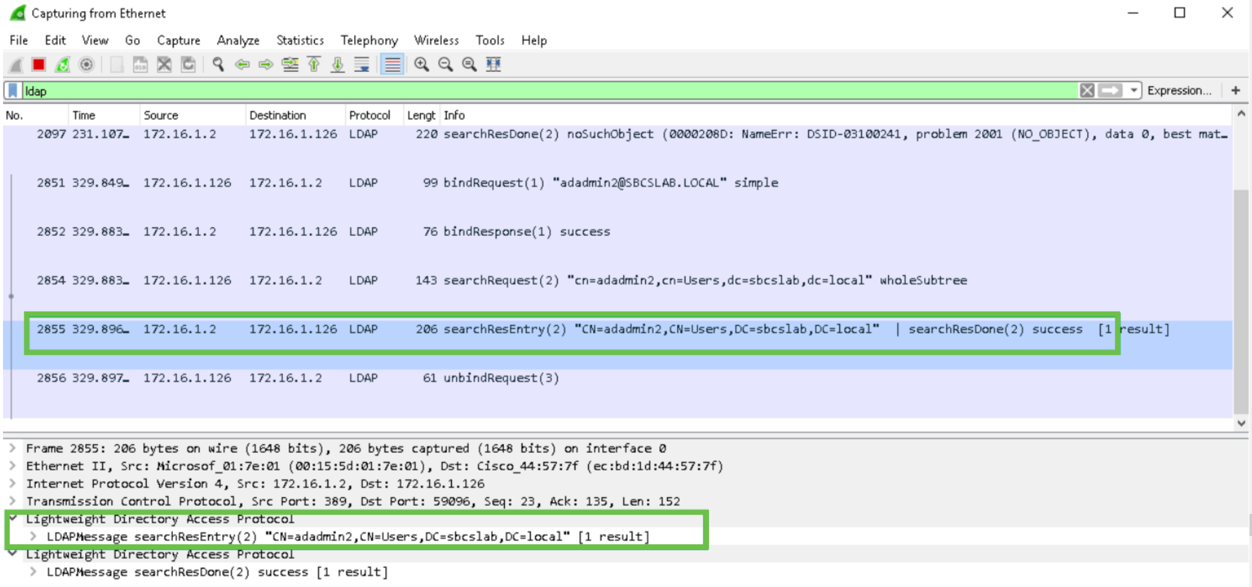
tribute	Value
faultClassStore	<not set>
partment	<not set>
partmentNumber	<not set>
scription	<not set>
sktopProfile	<not set>
stinationIndicator	<not set>
splayName	adadmin2
splayNamePrintable	<not set>
stinguishedName	CN=adadmin2,CN=Users,DC=sbcslab,DC=local
SASignature	<not set>
CorePropagationD...	0x0 = ( )
namicLDAPServer	<not set>
nployeeID	<not set>

Step 8

Log in with the *User logon name*, in this case, *adadmin2*, you will see that the login is successful.

Step 9

You can see the details on the packet capture as shown in the following screenshot.



```
No.   Time      Source        Destination   Protocol Lengt Info
2097 231.107…  172.16.1.2    172.16.1.126  LDAP     220 searchResDone(2) noSuchObject (0000208D: NameErr: DSID-03100241, problem 2001 (NO_OBJECT), data 0, best mat…
2851 329.849…  172.16.1.126  172.16.1.2    LDAP      99 bindRequest(1) "adadmin2@SBCSLAB.LOCAL" simple
2852 329.883…  172.16.1.2    172.16.1.126  LDAP      76 bindResponse(1) success
2854 329.883…  172.16.1.126  172.16.1.2    LDAP     143 searchRequest(2) "cn=adadmin2,cn=Users,dc=sbcslab,dc=local" wholeSubtree
2855 329.896…  172.16.1.2    172.16.1.126  LDAP     206 searchResEntry(2) "CN=adadmin2,CN=Users,DC=sbcslab,DC=local"  | searchResDone(2) success  [1 result]
2856 329.897…  172.16.1.126  172.16.1.2    LDAP      61 unbindRequest(3)
```

```
> Frame 2855: 206 bytes on wire (1648 bits), 206 bytes captured (1648 bits) on interface 0
> Ethernet II, Src: Microsof_01:7e:01 (00:15:5d:01:7e:01), Dst: Cisco_44:57:7f (ec:bd:1d:44:57:7f)
> Internet Protocol Version 4, Src: 172.16.1.2, Dst: 172.16.1.126
> Transmission Control Protocol, Src Port: 389, Dst Port: 59096, Seq: 23, Ack: 135, Len: 152
v Lightweight Directory Access Protocol
  > LDAPMessage searchResEntry(2) "CN=adadmin2,CN=Users,DC=sbcslab,DC=local" [1 result]
v Lightweight Directory Access Protocol
  > LDAPMessage searchResDone(2) success [1 result]
```

What happens if you don’t take the space out of the full name field?

If you try using the *User logon name,* in this case *adadmin*, you will see that login fails as Lightweight Directory Access Protocol (LDAP) server cannot return object because *Full name,* in this case, *ad admin1,* has a space. You will be able to see that details upon capturing the packets as shown on the following screenshot.

Conclusion

You have now successfully completed and avoided a failed login for remote authentication via Active Directory on RV34x Router.