

# User and Domain Management Configuration on RV320 and RV325 VPN Router Series

## Objective

The *User Management* page is used to configure domains and users. A domain is a subnetwork that consists of a group of clients and servers. Authentication to a domain is controlled by a local security server. The RV32x VPN Router Series supports authentication through the local database, a RADIUS server, an active directory server, or an LDAP server.

This article explains how to manage domains and users on the RV32x VPN Router Series.

## Applicable Devices

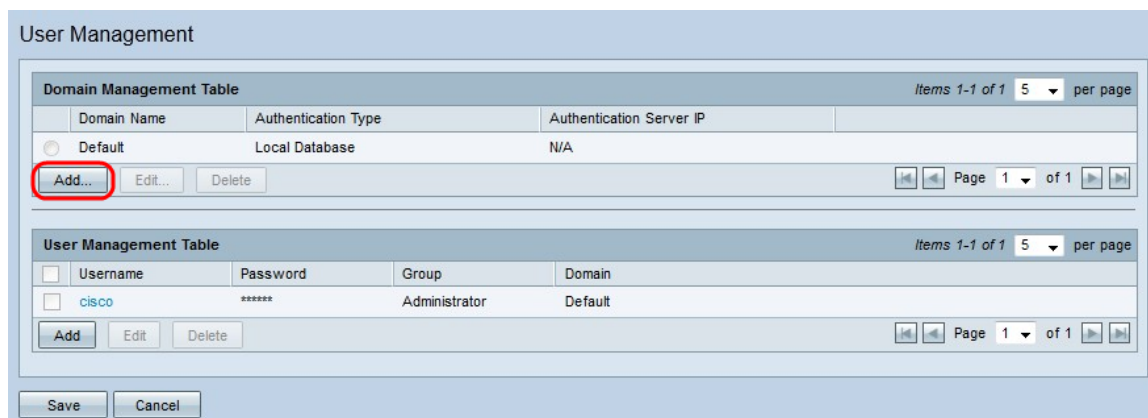
- RV320 Dual WAN VPN Router
- RV325 Gigabit Dual WAN VPN Router

## Software Version

- v1.1.0.09

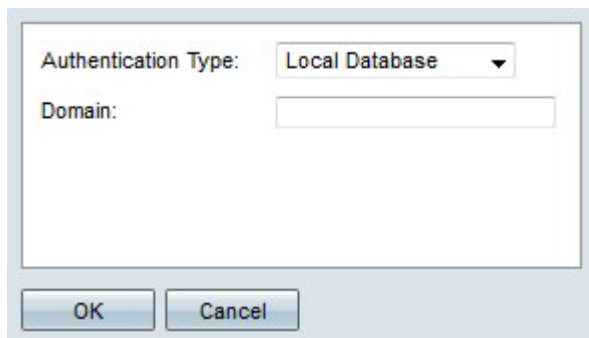
## Domain Management

Step 1. Log in to the Web Configuration Utility and choose **User Management**. The *User Management* page opens:



The screenshot displays the 'User Management' interface. At the top, there is a 'Domain Management Table' with columns for 'Domain Name', 'Authentication Type', and 'Authentication Server IP'. A single entry 'Default' is listed with 'Local Database' as the authentication type and 'N/A' as the server IP. Below this table, the 'Add...' button is circled in red. Below the domain table is a 'User Management Table' with columns for 'Username', 'Password', 'Group', and 'Domain'. A single entry 'cisco' is listed with '\*\*\*\*\*' as the password, 'Administrator' as the group, and 'Default' as the domain. At the bottom of the page, there are 'Save' and 'Cancel' buttons.

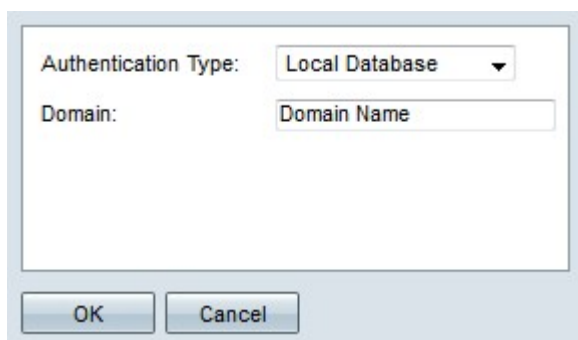
Step 2. Click **Add** in the Domain Management Table to configure a new domain. The *Add Domain* window appears.



Step 3. Choose the type of authentication that is used for the domain from the Authentication Type drop-down list.

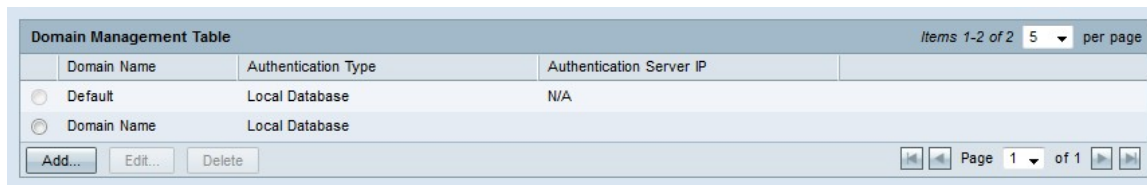
- Local Database — Authentication is performed by the router.
- RADIUS — A remote RADIUS server performs authentication for the domain.
  - RADIUS-PAP — Password Authentication Protocol (PAP) is an authentication protocol which only uses a simple password for authentication. This authentication is considered insecure and should only be used if the remote RADIUS server does not support a stronger authentication method.
  - RADIUS-CHAP — Challenge Handshake Authentication Protocol (CHAP) is an authentication protocol that verifies authentication through a three way handshake. This handshake takes place at the time of initial connection and at random intervals after the initial connection.
  - RADIUS-MSCHAP — MS-CHAP is the Microsoft version of CHAP. The MS-CHAP format was designed to be compatible with Windows NT products.
  - RADIUS-MSCHAPV2 — MS-CHAPV2 is an extension of MS-CHAP that provides a stronger encryption key.
- Active Directory — A server that runs active directory performs authentication for the domain. Active directory is a service that provides network security on a Windows domain network.
- LDAP — A remote server that runs a directory service performs authentication for the domain. Lightweight Directory Access Protocol (LDAP) is an access protocol that is used to access the directory service.

## Local Database Authentication



Step 1. Enter a name for the domain in the Domain field.

Step 2. Click **OK**. The domain is created.

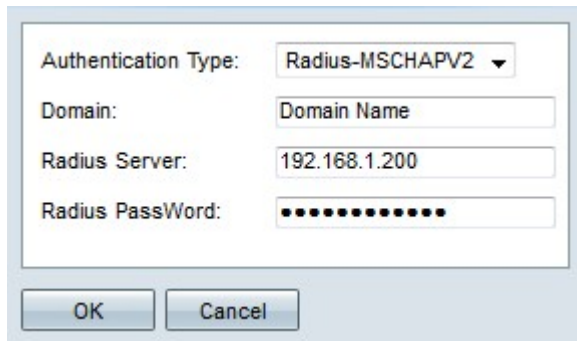


Domain Name	Authentication Type	Authentication Server IP
<input type="radio"/> Default	Local Database	N/A
<input type="radio"/> Domain Name	Local Database	

Items 1-2 of 2 5 per page

Add... Edit... Delete Page 1 of 1

## RADIUS Authentication



Authentication Type: Radius-MSCHAPV2

Domain: Domain Name

Radius Server: 192.168.1.200

Radius PassWord: .....

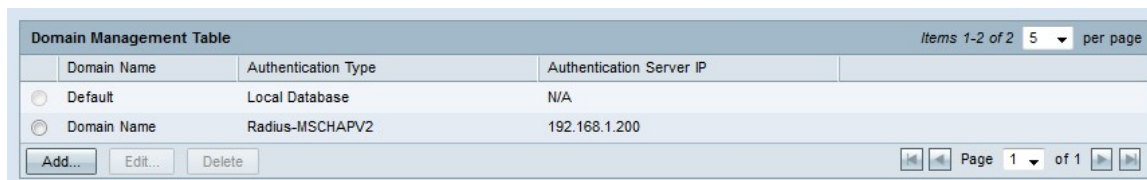
OK Cancel

Step 1. Enter a name for the domain in the Domain field.

Step 2. Enter the IP address of the RADIUS server in the Radius Server field.

Step 3. Enter the password that the router uses to authenticate to the RADIUS server in the Radius PassWord field. The password allows the router and RADIUS server to encrypt passwords and exchange responses. This field should match the configured password on the RADIUS server.

Step 4. Click **OK**. The domain is created.

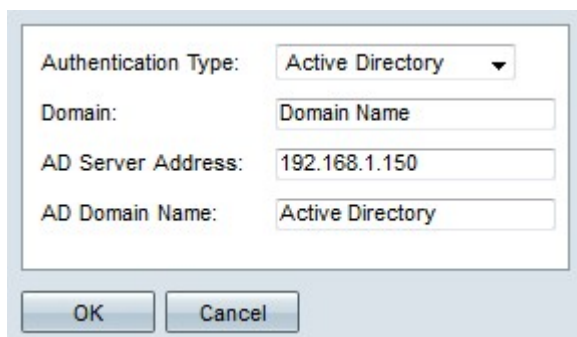


Domain Name	Authentication Type	Authentication Server IP
<input type="radio"/> Default	Local Database	N/A
<input type="radio"/> Domain Name	Radius-MSCHAPV2	192.168.1.200

Items 1-2 of 2 5 per page

Add... Edit... Delete Page 1 of 1

## Active Directory Authentication



Authentication Type: Active Directory

Domain: Domain Name

AD Server Address: 192.168.1.150

AD Domain Name: Active Directory

OK Cancel

Step 1. Enter a name for the domain in the Domain field.

Step 2. Enter the IP address of the active directory server in the AD Server Address field.

Step 3. Enter the domain name of the active directory server in the AD Domain Name field.

Step 4. Click **OK**. The domain is created.

Domain Management Table			Items 1-2 of 2 5 per page
Domain Name	Authentication Type	Authentication Server IP	
<input type="radio"/> Default	Local Database	N/A	
<input type="radio"/> Domain Name	Active Directory	192.168.1.150	

Add... Edit... Delete Page 1 of 1

## LDAP Authentication

Authentication Type:	LDAP
Domain:	Domain Name
LDAP Server Address:	192.168.1.150
LDAP Base DN:	LDAP Distinguished Name

OK Cancel

Step 1. Enter a name for the domain in the Domain field.

Step 2. Enter the IP address of the LDAP server in the LDAP Server Address field.

Step 3. Enter the base distinguished name of the LDAP server in the LDAP Base DN field. The base DN is the location where the LDAP server searches for users when it receives an authorization request. This field should match the base DN that is configured on the LDAP server.

Step 4. Click **OK**. The domain is created.

Domain Management Table			Items 1-2 of 2 5 per page
Domain Name	Authentication Type	Authentication Server IP	
<input type="radio"/> Default	Local Database	N/A	
<input checked="" type="radio"/> Domain Name	LDAP	192.168.1.100	

Add... Edit... Delete Page 1 of 1

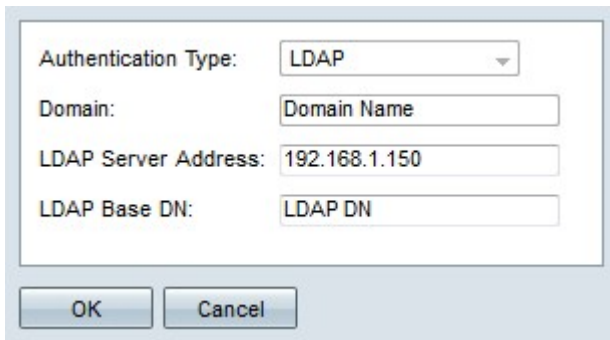
## Edit Domain Configuration

Domain Management Table			Items 1-2 of 2 5 per page
Domain Name	Authentication Type	Authentication Server IP	
<input type="radio"/> Default	Local Database	N/A	
<input checked="" type="radio"/> Domain Name	LDAP	192.168.1.100	

Add... Edit... Delete Page 1 of 1

Step 1. Click the radio button of the domain you want to edit.

Step 2. Click **Edit** in the Domain Management Table to edit the domain.



Authentication Type: LDAP

Domain: Domain Name

LDAP Server Address: 192.168.1.150

LDAP Base DN: LDAP DN

OK Cancel

Step 3. Edit the desired fields.

Step 4. Click **OK**. The domain configuration is updated.

## Delete Domain Configuration

Domain Management Table				Items 1-2 of 2 5 per page
Domain Name	Authentication Type	Authentication Server IP		
<input type="radio"/> Default	Local Database	N/A		
<input checked="" type="radio"/> Domain Name	LDAP	192.168.1.150		

Add... Edit... Delete Page 1 of 1

Step 1. Click the radio button of the domain you want to delete.

Step 2. Click **Delete** in the Domain Management Table to delete the domain. A warning window appears.



Step 3. Click **Yes**. The domain configuration is deleted.

## User Management

Step 1. Log in to the Router Configuration Utility and choose **User Management**. The *User Management* page opens:

User Management

Domain Management Table			
Domain Name	Authentication Type	Authentication Server IP	
Default	Local Database	N/A	

Add... Edit... Delete Page 1 of 1

User Management Table			
Username	Password	Group	Domain
<input type="checkbox"/> cisco	*****	Administrator	Default

**Add** Edit Delete Page 1 of 1

Save Cancel

Step 2. Click **Add** in the User Management Table to add a new user.

User Management Table			
Username	Password	Group	Domain
<input type="checkbox"/> cisco	*****	Administrator	Default
<input type="text" value="Username"/>	<input type="password" value="*****"/>	<input type="text" value="Group 1"/>	<input type="text" value="Default"/>

Add Edit Delete Page 1 of 1

Step 3. Enter the desired username in the Username field.

Step 4. Enter a password for the username in the Password field. The password is used to authenticate the user to the configured local database domain.

Step 5. Choose the group that the user is to be a part of from the Group drop-down list. Groups are used to further divide domains into smaller sub-domains. The administrator group can only contain one user. The default username/password of the administrator is cisco/cisco.

**Note:** Groups can be configured on the *Group Management* page. For more information, refer to the article *Group Management on RV320 Routers*.

Step 6. Choose the domain that the user is to be part of from the Domain drop-down list.

Step 7. Click **Save**. The new user is configured.

User Management Table			
Username	Password	Group	Domain
<input type="checkbox"/> cisco	*****	Administrator	Default
<input type="checkbox"/> Username	*****	Group 1	Domain Name

Add Edit Delete Page 1 of 1

## Edit User Management

User Management Table			
Username	Password	Group	Domain
<input type="checkbox"/> cisco	*****	Administrator	Default
<input checked="" type="checkbox"/> Username	*****	Group 1	Default

Add Edit Delete Page 1 of 1

Step 1. Check the check box of the username you want to edit.

Step 2. Click **Edit** in the User Management Table to edit the username.

User Management Table				Items 1-2 of 2 5 per page
<input type="checkbox"/>	Username	Password	Group	Domain
<input type="checkbox"/>	cisco	*****	Administrator	Default
<input type="checkbox"/>	Username	*****	Mobile User	Default

Add Edit Delete Page 1 of 1

Step 3. Edit the desired fields.

Step 4. Click **Save**. The username configuration is updated.

## Delete User Management

User Management Table				Items 1-2 of 2 5 per page
<input type="checkbox"/>	Username	Password	Group	Domain
<input type="checkbox"/>	cisco	*****	Administrator	Default
<input checked="" type="checkbox"/>	Username	*****	Mobile User	Default

Add Edit Delete Page 1 of 1

Step 1. Check the check box of the username you want to delete.

Step 2. Click **Delete** in the User Management Table to delete the username.

Step 3. Click **Save**. The username configuration is deleted.