Password Configuration on RV320 and RV325 VPN Router Series

Objective

A password is a string of characters that is used for authentication. The default username/password for the RV32x VPN Router Series is cisco/cisco. For security purposes, it is highly recommended that the password be changed from the default. If the username or password is forgotten, there is no way for them to be recovered. At this point, the device must be reset to factory default settings.

This article explains how to configure a new password on the RV32x VPN Router Series.

Applicable Devices

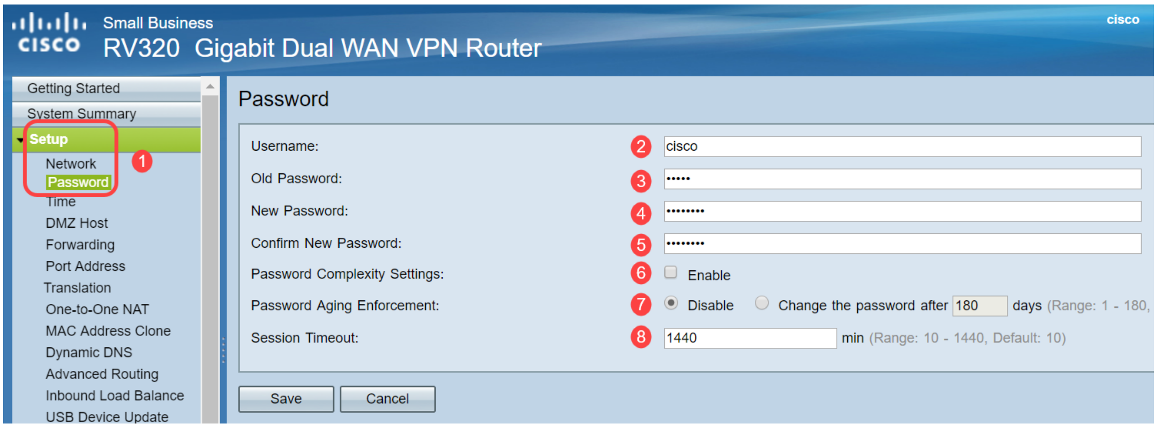
- RV320 Dual WAN VPN Router
- RV325 Gigabit Dual WAN VPN Router

Software Version

- v1.1.0.09

Password Configuration

Step 1. Log in to the web configuration utility and choose **Setup > Password**. The *Password* page opens:



Password

Username: cisco

Old Password: •••••

New Password: ••••••••

Confirm New Password: ••••••••

Password Complexity Settings: □ Enable

Password Aging Enforcement: ● Disable ○ Change the password after 180 days (Range: 1 - 180,

Session Timeout: 1440 min (Range: 10 - 1440, Default: 10)

Step 2. Enter the desired username in the Username field. The username can consists of uppercase letters, lowercase letters, numbers, and special characters.

Step 3. Enter the previous password used in the Old Password field.

Step 4. Enter the new desired password in the New Password field. The password can consists of uppercase letters, lowercase letters, numbers, and special characters.

Step 5. Re-enter the new password in the Confirm New Password field.

Step 6. (Optional) To enable the password strength feature, check the **Enable** check box in the Password Complexity Settings field. This is used to ensure that the password is complex enough. With this option enabled, the Minimal password length and the Minimal number of character classes fields become available.

- Minimal password length — Enter the minimum password length (0-64 characters). By default, the minimum length is 8.

- Minimal number of character classes — Enter the number of classes that the password must include. By default, the password must contain characters from at least three of these classes: Uppercase letters (ABCD...), Lowercase letters (abcd...), Numbers (1234...), Special characters available on a standard keyboard (!@#$...).

Note: The Password Strength Meter field displays a meter that gauges how strong the new password is.

Step 7. Click the radio button that corresponds to the desired password time in the Password Aging Enforcement field.

- Disable — The password is always valid.

- Change the Password — Enter the amount of days that the password is valid. After this time the RV320 will prompt the user for a new password. The range of the password aging enforcement feature is from 1 day to 180 days.

Step 8. Enter a timeout value in minutes in the Session Timeout value. This is the amount of time that the user can be allowed to be idle in the GUI until the RV32x returns to the log in screen. The range of the session timeout value is from 10 to 1440 minutes.

Step 9. Click **Save**. The new password is configured.