

# Password Complexity Configuration on the RV315W VPN Router

## Objective

A user created password is used to enter the web configuration utility and manage the settings on the router. Password complexity is used to ensure that a password is sufficiently secure for network access. This article explains how to configure the password settings on the RV315W.

## Applicable Device

- RV315W

## Software Version

- 1.01.03

## Password Complexity Configuration

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

**Password Complexity**

Password Complexity Settings: ☒ Enable ☐ Disable

Minimal password length: 8 (Range: 0 - 64, Default: 8)

Minimal number of character classes: 3 (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 ☐ Disable

Password Aging: ☒ Enable ☐ Disable

Password Aging time: 180 days (Range: 1 - 365, Default: 180)

Save Cancel

Step 2. Click the **Enable** radio button in the Password Complexity Settings field to enable the complexity rules.

**Timesaver:** If you click the **Disable** radio button in the Password Complexity Settings field skip to step 8. It is not recommended that you disable the Password Complexity Settings.

Step 3. Enter the minimal length of the password that the administrator would like to apply to the password in the Minimal Password Length field.

Step 4. Enter the minimal number of character classes that the password has to contain in the Minimal number of character classes field. The four classes of characters are:

- Upper Case — The alpha characters are in upper case (A,B,C ,etc).
- Lower Case — The alpha characters are in lower case (a,b,c ,etc).

- Numerical — Numerical characters are used in the password (1,2,3 ,etc).
- Special — Special characters are used in the password (#,\$.& ,etc).

Step 5. (Optional) To ensure that the new password must be different from the old password, click the **Enable** radio button in the New Password must be different than the current one field.

Step 6. (Optional) To give the password an expiration date, click the **Enable** radio button in the Password Aging field.

Step 7. If Password Aging is enabled, enter how long a password lasts (in days) before it expires in the Password Aging Time field. The default value is 180 days.

Step 8. Click **Save** to save the changes.