WiFi Protected Access Pre-Shared Key (WPA-PSK) Complexity Configuration on WAP551 and WAP561 Access Points

Objective

If WiFi Protected Access (WPA) is configured on the access point , a WPA pre-shared key can be chosen to securely authenticate clients. When WPA-PSK Complexity is enabled, complexity requirements for the key used in the authentication process can be configured. More complex keys provide increased security.

This article explains how to configure WPA Pre-Shared Key Complexity on the WAP5551 and WAP561 access points.
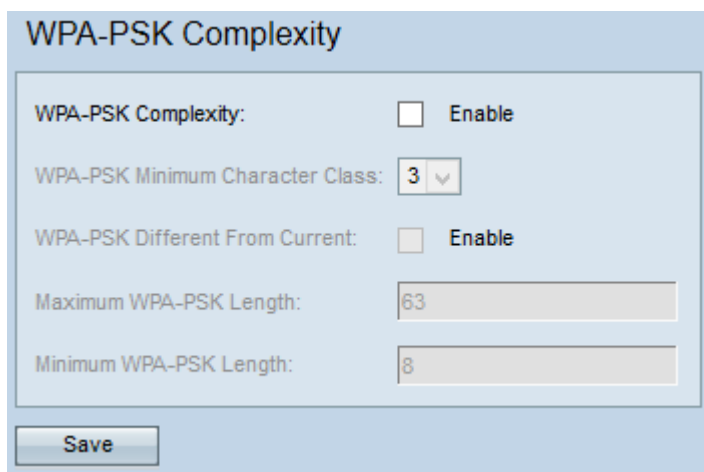
Applicable Devices

- WAP551
- WAP561

Software Version

- v1.0.4.2

Configuration of WPA-PSK Complexity

Step 1. Log in to the web configuration utility and choose **System Security > WPA-PSK Complexity**. The *WPA-PSK Complexity* page opens:

Step 2. Check the **Enable** check box in the WPA-PSK Complexity field to enable the AP to check the new WPA pre-shared keys for complexity.

Step 3. Choose the minimum number of character classes that must be represented in the key string from the WPA-PSK Minimum Character Class drop-down list. If two character classes are chosen, then the pre-shared key should contain at least two character classes, such as uppercase letters, lowercase letters, numbers, and special characters.

Step 4. (Optional) To enter a different pre-shared key when the current key has expired, check the **Enable** check box in the WPA-PSK Different From Current field. If disabled, you can reenter the same key which you used earlier.

Step 5. Enter the maximum number of characters for a key in the Maximum WPA-PSK Length field. The range is from 64 to 80.

Step 6. Enter the minimum number of characters that a key can have in the Minimum WPA-PSK Length field. The range is from 8 to 32.

Step 7. Click **Save** to save the settings.