Five tips to Fortify your Wireless Network

Objective

The radio is the physical component of the Wireless Access Point (WAP) that creates a wireless network. The radio settings on the WAP and the wireless router control the behavior of the radio and determine the signals the device transmits. While Wi-Fi networks are convenient, it may become vulnerable to wireless clients using up the bandwidth, and increasing security risks when it is not protected properly. It is recommended to have the following settings for added security:

- Enable Data Encryption
- Allow only known devices to connect to the network with Media Access Control (MAC) Filtering
- Change the Wireless Network Password regularly
- Enable built-in firewalls
- Hide the Service Set Identifier (SSID)

This article aims to provide tips that would be useful in securing your wireless network.

Applicable Devices

- RV Series
- Wireless Access Points
- Cisco Unified Communications

Fortify your Wireless Network

Enable Data Encryption

Wireless network devices typically support some type of encryption to be able to connect to a wireless network securely. Whenever possible, use Wi-Fi Protected Access (WPA) or Wi-Fi Protected Access 2 (WPA2) as they provide better security with the Advanced Encryption Standard (AES) encryption method. Steps in enabling data encryption differ slightly per device. For a guide to enable wireless security on a wireless router, click here. For a guide to enable wireless security on an access point, click here.

Allow Only Known devices with MAC Filtering

MAC Address filtering lets you list down the MAC addresses of the wireless clients connected to your network, effectively creating a known-only devices list. You can then grant or deny the devices access to the network depending on your requirement. MAC addresses not on the list are automatically excluded from the condition. Steps in enabling MAC address filtering differ slightly per device. For a guide to enable MAC filtering on a wireless router, click here. For a guide to enable MAC filtering on a wireless access point, click here.

Change the Wireless Network Password Regularly

Setting up a wireless network password is the easiest way to secure a wireless network.

They often need to be synchronized with other wireless access points in the network, for a seamless wireless connection. Wireless network passwords typically need to changed regularly to ensure that only authorized devices are connected to the network. Steps in setting up a wireless network password differ slightly per device. For a guide on how to configure the wireless settings on a router, click here. For a guide on changing the password on an access point, click here.

Enable Built-in Firewalls

Many wireless routers, such as the RV130W Wireless-N VPN Router, have built-in firewalls that prevent malicious traffic from entering your network. Steps in enabling the firewall differ slightly per device. For a guide on enabling the firewall on a router, click here.

Hide the SSID

Disabling SSID broadcast makes your network invisible to a device when it searches for a wireless network. Like setting up a wireless password, hiding the SSID makes connecting to your wireless network more difficult, since the connection will have to be configured manually on the device. Steps in disabling SSID broadcast differ slightly per device. For a guide on disabling SSID broadcast on an access point, click here. For a guide in disabling SSID broadcast on a wireless router, click here.