Basic Wireless Settings on the CVR100W VPN Router

Objective

A Wireless Local Area Network (WLAN) utilizes radio communication to connect wireless devices to a LAN. An example is a Wi-Fi hotspot at a cafe. Wireless networks are useful as it reduces wiring costs and it is easy to setup.

This article explains how to configure basic wireless settings on the CVR100W VPN router, which includes the configuration of network security. For advanced wireless settings, refer to the article *Advanced Wireless Configuration on the CVR100W VPN Router*.

Applicable Device

- CVR100W VPN Router

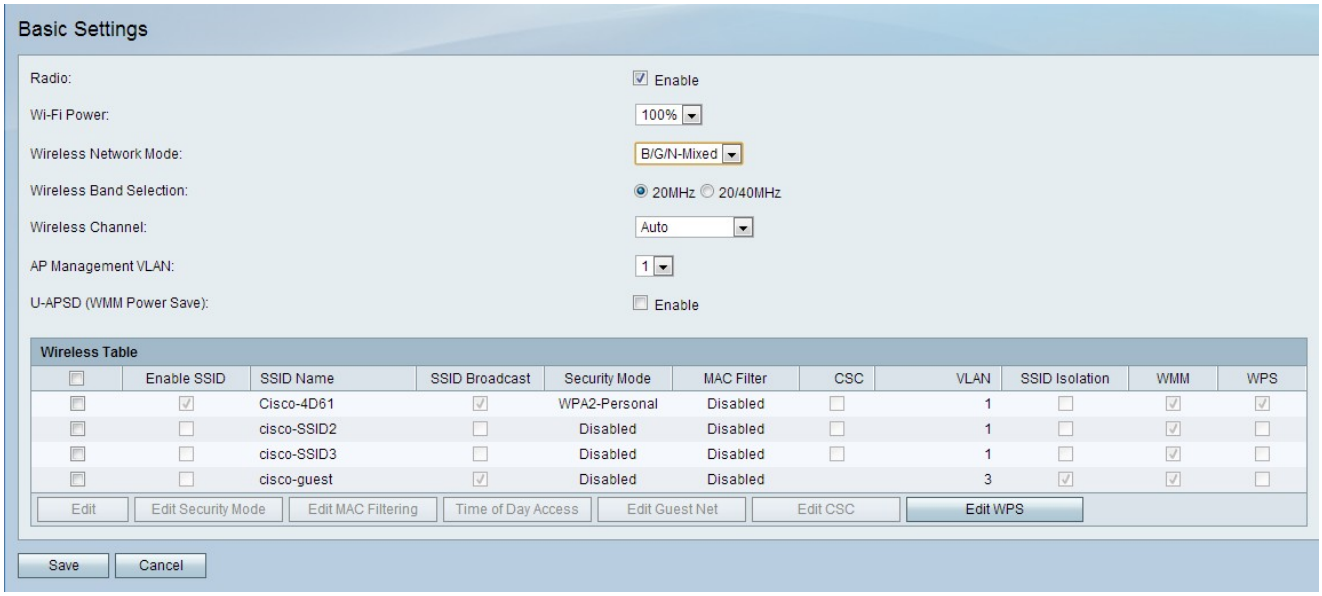
Software Version

- 1.0.1.19

Basic Settings Configuration

General Settings

Step 1. Log in to the web configuration utility and choose **Wireless > Basic Settings**. The *Basic Settings* page opens:



Step 2. Check the **Enable** check box in the Radio field to enable the wireless radio.

Step 3. From the Wi-Fi Power drop-down list choose the wi-fi power. This wi-fi power controls the transmitter power of the wi-fi radio. This feature is useful to reduce or increase the range of the signal. This feature is used to conserve power.

- 100% — This option enables 100% radio transmitter power.
- 50% — This option enables 50% radio transmitter power.

Step 4. From the Wireless Network Mode drop-down list choose the wireless mode. This option is based on the wireless capabilities of the devices in the network.

- B/G/N-Mixed — The network consists a mix of wireless-B, wireless-G, and wireless-N devices.
- B-Only — The network consists of only wireless-B devices.
- G-Only — The network consists of only wireless-G devices.
- N-Only — The network consists of only wireless-N devices.
- B/G-Mixed — The network consists of a mix of wireless-B and wireless-G devices.
- G/N Mixed — The network consists of a mix of wireless-G and wireless-N devices.

Step 5. If the network mode consists of wireless-N devices, click the radio button that corresponds to the desired bandwidth of the wireless signal in the Wireless Band Selection field. The higher bandwidth indicates the greater amount of data the signal can carry.

- 20 MHz — The standard frequency for a wireless signal.
- 20/40 MHz — Automatically uses a 20 MHz and 40 MHz signal. A 40 MHz signal provides more bandwidth but is susceptible to more interference. This option is only used if the connected wireless devices are compatible with 40 MHz frequency.

Step 6. From the Wireless Channel drop-down list choose a wireless channel for the radio. Choose a channel that is not currently in use by neighbor networks. If multiple radios use the same channel, interference could occur.

Step 7. From the AP Management VLAN drop-down list, choose the management VLAN. The management VLAN is the VLAN used for the management of devices from a remote location.

Step 8. (Optional) To enable Unscheduled Automatic Power Save Delivery (U-APSD), check **Enable** in the U-APSD field. U-APSD is a feature that allows the radio to conserve power. However U-APSD may reduce throughput performance of the radio.

Step 9. Click **Save**.

Edit Wireless Table

Step 1. Check the check box of the network you want to edit in the Wireless Table.

Step 2. Click **Edit** to edit the specified network.

Step 3. Check the **Enable SSID** check box to enable the network. Service Set Identifier (SSID) is the name of the wireless network.

Step 4. In the SSID Name field, enter the name of the network. All devices on the network use this SSID to communicate with each other.

Step 5. Check the **SSID Broadcast** check box to enable wireless broadcast. When SSID broadcast is enabled, the availability of the CVR100W VPN router is advertised to nearby wireless devices.

Step 6. (Optional) To edit the security mode, refer to Edit Security Mode.

Step 7. (Optional) To edit the MAC filter, refer to Edit MAC Filtering.

Step 8. (Optional) To enable the Cisco Simple Connect (CSC), check the **CSC** check box. CSC enables easy setup of a wireless network and allows easy connection of wireless devices to the network. The wireless device uses CSC to obtain the SSID and password of the network, which allows for automatic connection to the network. To edit the CSC, refer to Edit CSC.

Note: The Cisco Simple Connect's VLAN cannot be the same as the current or other SSID's VLAN.

Step 9. From the VLAN drop-down list choose the VLAN that is associated with the network.

Step 10. Check **SSID Isolation** check box to prevent devices on the specified network from communicating with each other.

Step 11. Check **WMM** to enable Wi-Fi Multimedia (WMM) on the network. WMM is used to enhance the streaming of multimedia over wireless devices. Higher priority is given to multimedia traffic that is sent over a wireless connection when WMM is enabled.

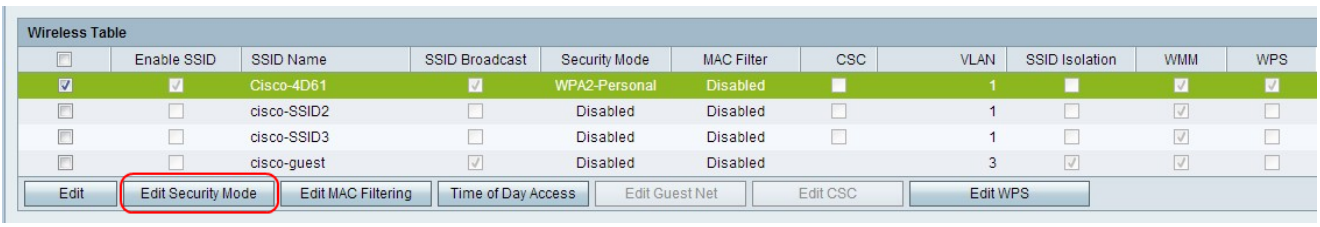
Step 12. Check **WPS** to assign the specified network as a Wi-Fi Protected Setup (WPS) network. WPS is a feature that allows for easy and secure network configuration. This feature allows devices to easily connect to the network.

Note: To configure WPS on the CVR100W VPN router, refer to the article *WiFi Protected Setup (WPS) on the CVR100W VPN Router*.

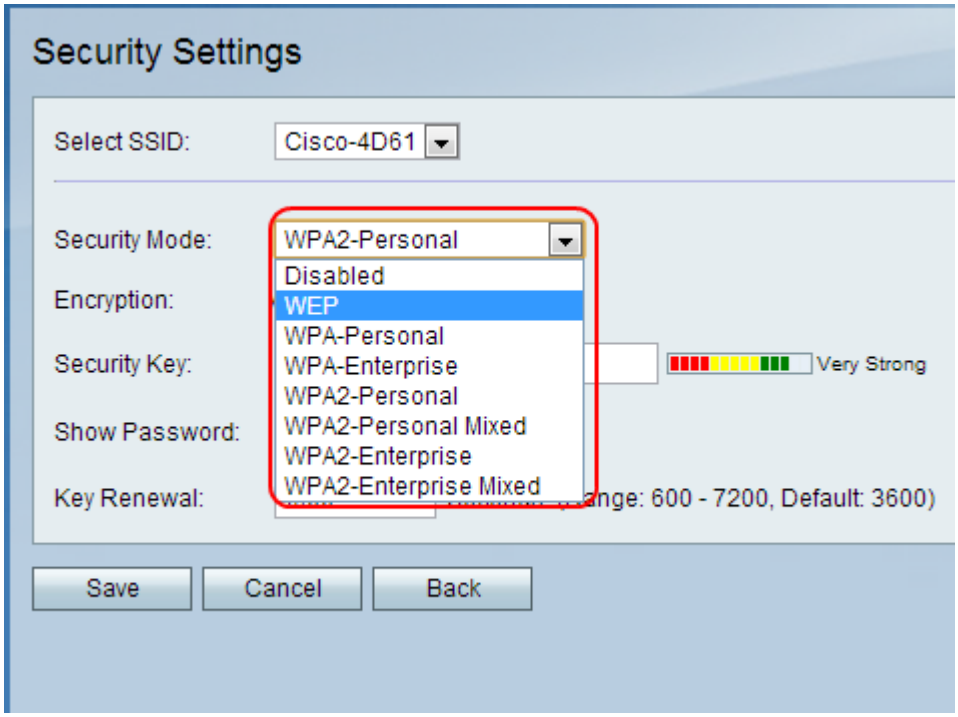
Step 13. Click **Save**.

Edit Security Mode

Step 1. Check the check box of the network you want to edit in the Wireless Table.



Step 2. Click **Edit Security Mode** to edit the security of the specified network. The *Security Settings* page opens.



Step 3. (Optional) To change the SSID that you want to configure the security for, choose the desired SSID from the Select SSID drop-down list.

Step 4. From the Security Mode drop-down list choose the security mode to configure.

- Disable Security - This option disables security on the CVR100W VPN router.

- WEP Security — Wired Equivalent Privacy (WEP) is an algorithm used to secure a wireless network. WEP is used to provide a basic encryption method which is less secure than WPA. WEP is used when connected network devices do not support WPA.

- WPA-Personal Security — Wi-Fi Protected Access (WPA) is a security standard for wireless networks. WPA-Personal is a version of WPA that is used for networks consisting of a few users. WPA-Personal provides a shared key that each user uses to access the wireless network. WPA was introduced with the key encryption methods Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).

- WPA-Enterprise Security — WPA-Enterprise is a version of WPA that is recommended for a network consisting of numerous users. Authentication to gain access to the network is controlled by a RADIUS server. Each connected user is given a unique key to access the wireless network. WPA was introduced with the key encryption methods Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).

- WPA2-Personal Security —WPA2 is an enhancement of WPA and it provides more security than WPA. WPA2-Personal is a version of WPA2 that is used for networks with few users. WPA2-Personal is more secure than WPA2-Personal Mixed. WPA2-Personal provides a shared key that every user uses to access the wireless network.

- WPA2-Personal Mixed Security — WPA2-Personal Mixed is a version of WPA2 that is used for networks with few users. WPA2-Personal Mixed supports backward compatibility for older devices not capable of utilizing WPA2. WPA2-Personal Mixed is a less secure connection.

- WPA2-Enterprise Security — WPA2-Enterprise is a version of WPA2 that is used for networks with numerous users. WPA2-Enterprise is more secure than WPA2-Enterprise

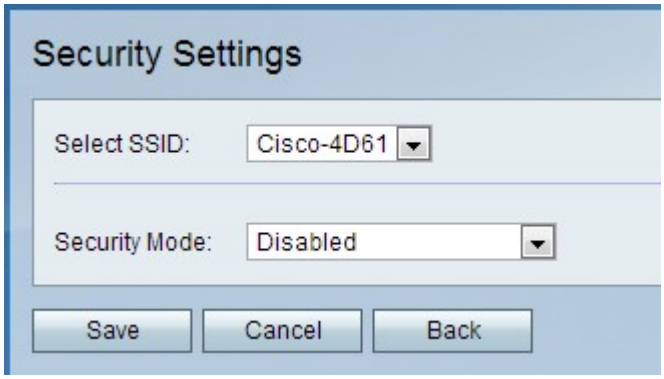
Mixed. Authentication used to gain access is controlled by a RADIUS server. This means that each connected user will be given a unique key to access the wireless network.

• WPA2-Enterprise Mixed Security — WPA2-Enterprise Mixed is versions of WPA2 that is used for networks with numerous users. WPA2-Enterprise Mixed supports backward compatibility for older devices not capable of utilizing WPA2. WPA2-Enterprise Mixed provides a less secure connection than WPA2-Enterprise. Authentication used to gain access is controlled by a RADIUS server. This means that each connected user will be given a unique key to access the wireless network.

Disable Security

Wireless security may be disabled on the CVR100W VPN router for ease of use when setting up test networks.

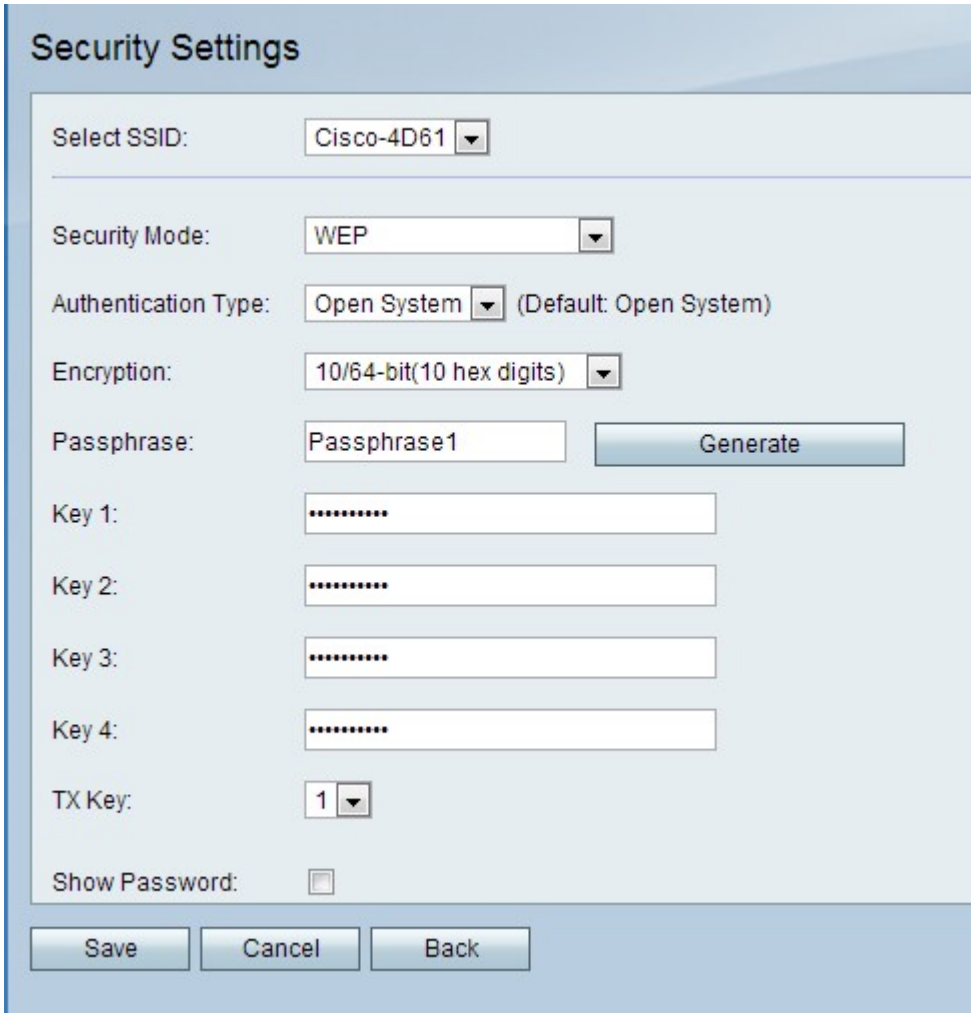
Note: Disabling security is not recommended.



Step 1. From the Security Mode drop-down list choose **Disabled**. The security is disabled for the wireless network.

Step 2. Click **Save**.

Configure WEP Security



Step 1. From the Security Mode drop-down list choose **WEP**.

Step 2. From the Authentication Type drop-down list choose an authentication type for the wireless network.

- Open System — Any network device can associate with the access point, but the WEP key is needed to pass traffic through the access point.
- Shared Key — A WEP key is needed to associate with the access point. It is also used to pass traffic through the access point.

Step 3. From the Encryption drop-down list choose an encryption method for the WEP key.

- 10/64-bit(10 hex digits) — Provides a 40-bit key.
- 26/128-bit(26 hex digits) — Provides a 104-bit key. This option is more secure.

Step 4. In the Passphrase field, enter a passphrase that is greater than eight characters. A passphrase is useful to make network security settings easier to remember.

Step 5. Click **Generate** to create keys in the Key 1, Key 2, Key 3, and Key 4 fields.

Note: You can also manually enter keys in the Key 1, Key 2, Key 3, and Key 4 fields.

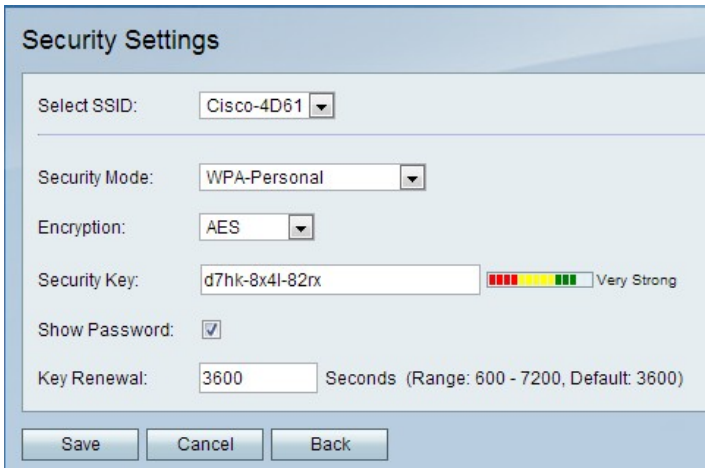
Step 6. From the TX Key drop-down list choose the Key that users must enter to access the wireless network.

Step 7. (Optional) Check the **Show Password** check box to reveal the character strings of

the keys.

Step 8. Click **Save**.

Configure WPA-Personal Security



Step 1. From the Security Mode drop-down list choose **WPA-Personal**.

Step 2. From the Encryption drop-down list choose an encryption method for the WPA key.

- TKIP/AES — This option is chosen when devices connected to the wireless network do not all support AES.
- AES — This option is preferable if all devices connected to the wireless network support AES.

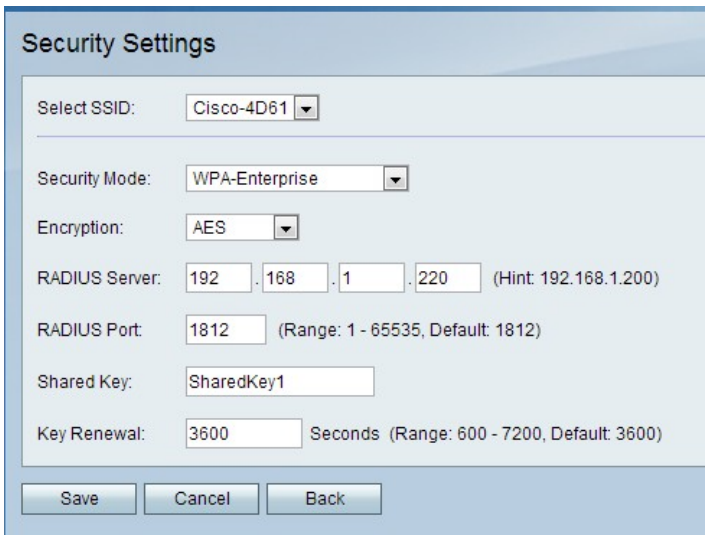
Step 3. Enter a security key in the Security Key field. The security key is a passphrase that consists of letters and digits. Devices use the security key to connect to the network.

Step 4. (Optional) To reveal the character string of the key, check the **Show Password** check box.

Step 5. In the Key Renewal field, enter the time in seconds the CVR100W VPN router uses the key before it generates a new one.

Step 6. Click **Save**.

Configure WPA-Enterprise Security



Step 1. From the Security Mode drop-down list choose **WPA-Enterprise**.

Step 2. From the Encryption drop-down list choose an encryption method for the WPA key.

- TKIP/AES — This option is chosen when devices connected to the wireless network do not all support AES.
- AES — This option is preferable if all devices connected to the wireless network support AES.

Step 3. In the RADIUS Server field, enter the IP address of the RADIUS server.

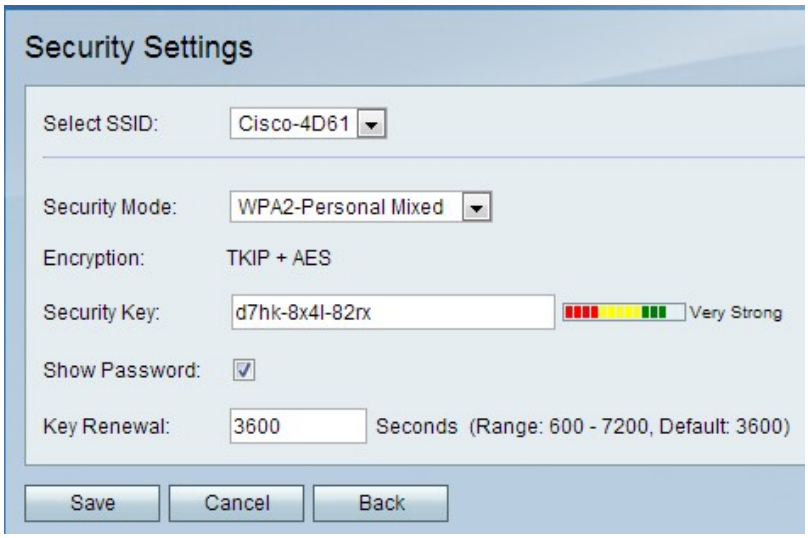
Step 4. In the RADIUS Port field, enter the port number used to access the RADIUS server.

Step 5. In the Shared Key field, enter the pre-shared key for the wireless users. A pre-shared key is a key used by all users. The pre-shared key feature is an added security feature.

Step 6. In the Key Renewal field, enter the time in seconds the CVR100W VPN router uses the key before it generates a new one.

Step 7. Click **Save**.

Configure WPA2-Personal/WPA2-Personal Mixed Security



Step 1. From the Security Mode drop-down list choose **WPA2-Personal** or **WPA2-Personal Mixed**.

Note: WPA2-Personal is used when all devices on the wireless network support AES. WPA2-Personal Mixed is used when devices on the network do not all support AES. The type of encryption used by the security method is displayed in the Encryption field.

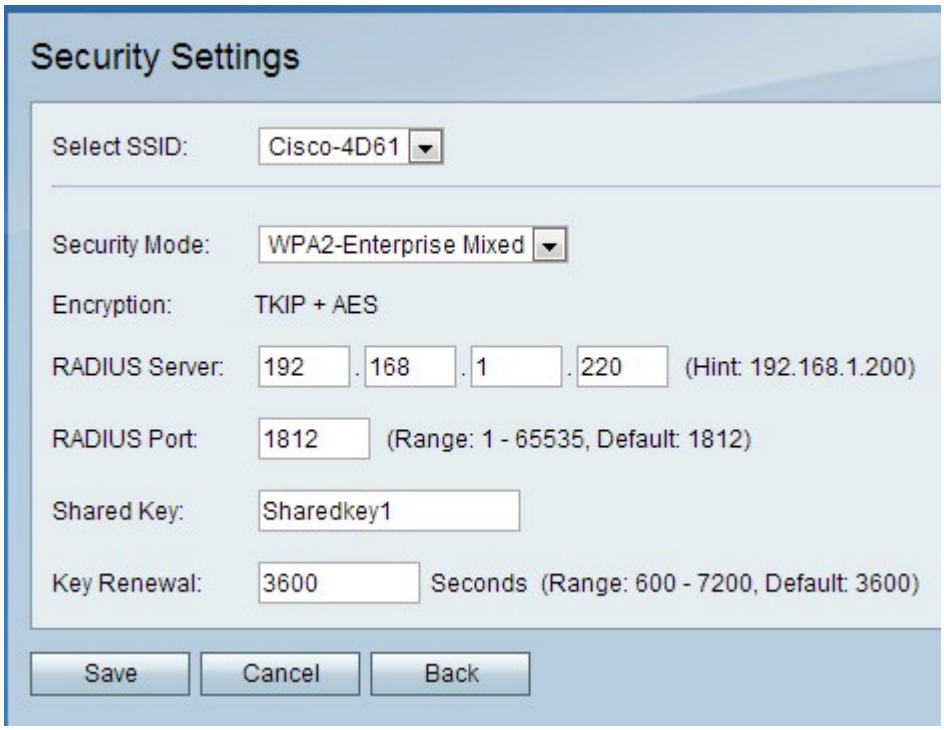
Step 2. In the Security Key field, enter a security key. The security key is a passphrase that consists of letters and digits. Devices use the security key to connect to the network.

Step 3. (Optional) To view the character strings of the key, check **Show Password** check box.

Step 4. In the Key Renewal field, enter the time in seconds for the time the CVR100W VPN router uses the key before it generates a new one.

Step 5. Click **Save**.

Configure WPA2-Enterprise/WPA2-Enterprise Mixed Security



Step 1. From the Security Mode drop-down list choose **WPA2-Enterprise** or **WPA2-Enterprise Mixed**.

Note: WPA2-Enterprise is used when all devices on the wireless network support AES. WPA2-Enterprise Mixed is used when devices on the network do not all support AES. The type of encryption used by the security method is displayed in the Encryption field.

Step 2. In the RADIUS Server field, enter the IP address of the RADIUS server.

Step 3. In the RADIUS Port field, enter the port number used to access the RADIUS server.

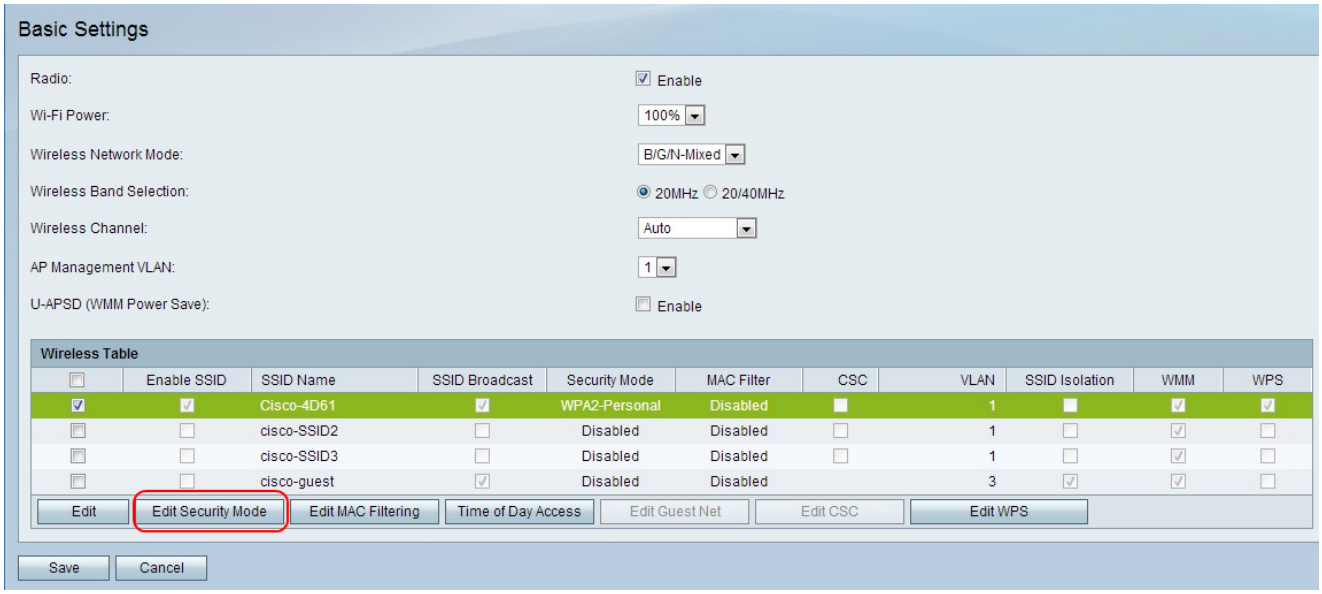
Step 4. In the Shared Key field, enter the pre-shared key for the wireless users. A pre-shared key is a key used by all users. The pre-shared key feature is an added security feature.

Step 5. In the Key Renewal field, enter the time in seconds the CVR100W VPN router uses the key before it generates a new one.

Step 6. Click **Save**.

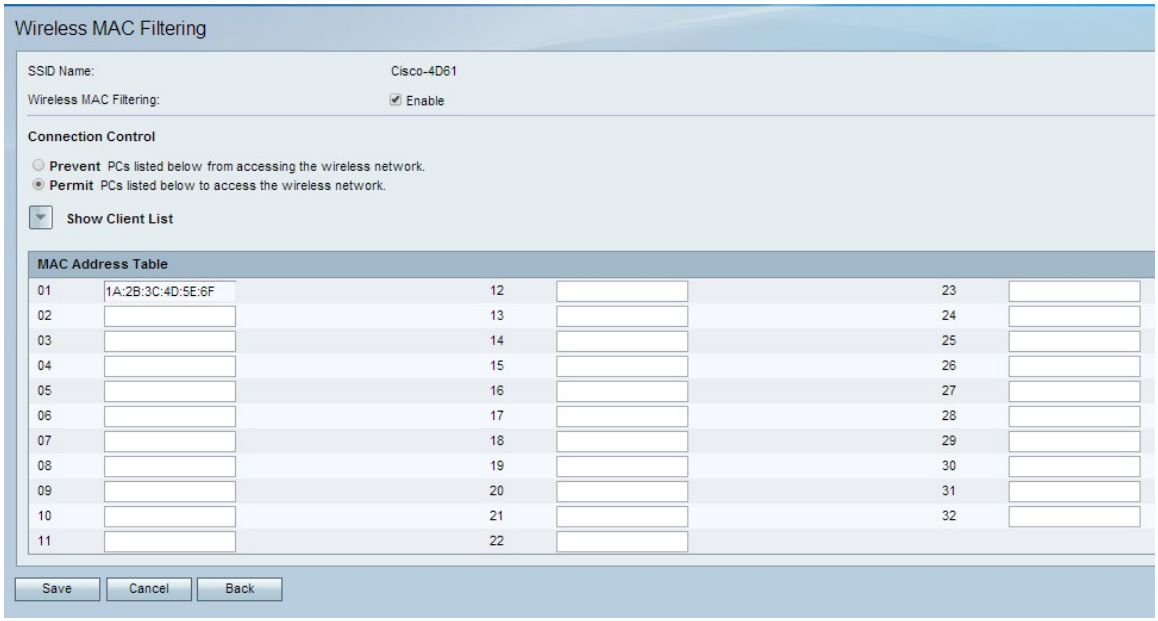
Edit MAC Filtering

MAC Filtering is used to permit or deny access to the wireless network based on the MAC address of the connecting device.



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

Step 2. Click **Edit MAC Filtering** to create MAC access control list for the specified network. The *Wireless MAC Filter* page opens:



Step 3. Check **Enable** to enable MAC filtering on the network.

Step 4. Click the radio button that corresponds to the desired list type in the Connection Control field.

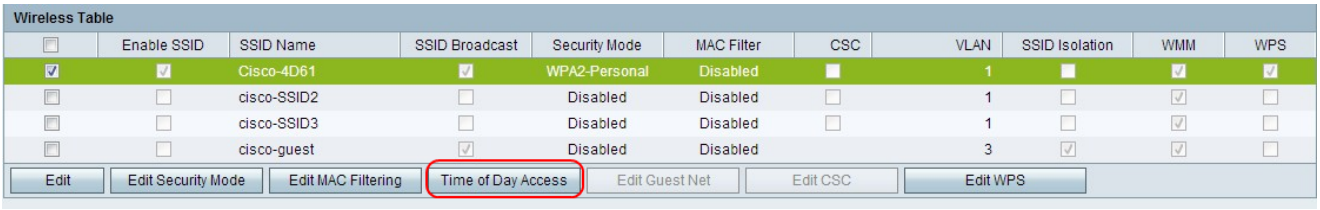
- Prevent PCs — Prevents PCs with the listed MAC addresses from entering the network.
- Permit PCs — Allows PCs with the listed MAC addresses to enter the network.

Step 5. In the MAC Address Table, enter the desired MAC addresses.

Step 6. Click **Save**.

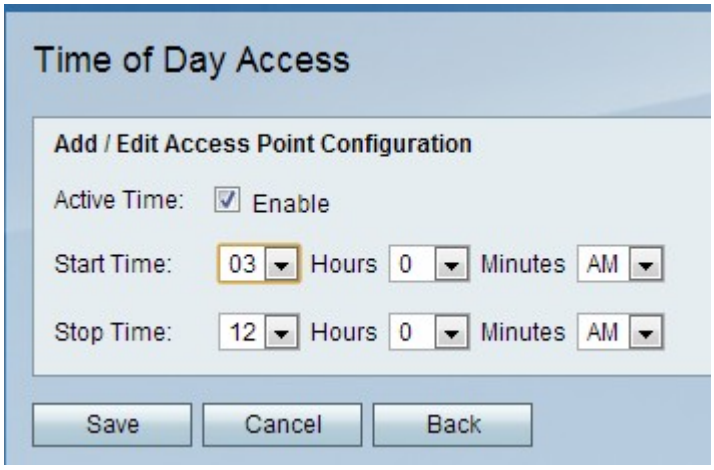
Time of Day Access

The Time of Day Access feature is used to allow access to users based on a configured schedule.



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

Step 2. Click **Time of Day Access** to configure when users can access the specified network. The *Time of Day Access* page opens:



Step 3. Check **Enable** in the Active Time field to enable time of day access for the network.

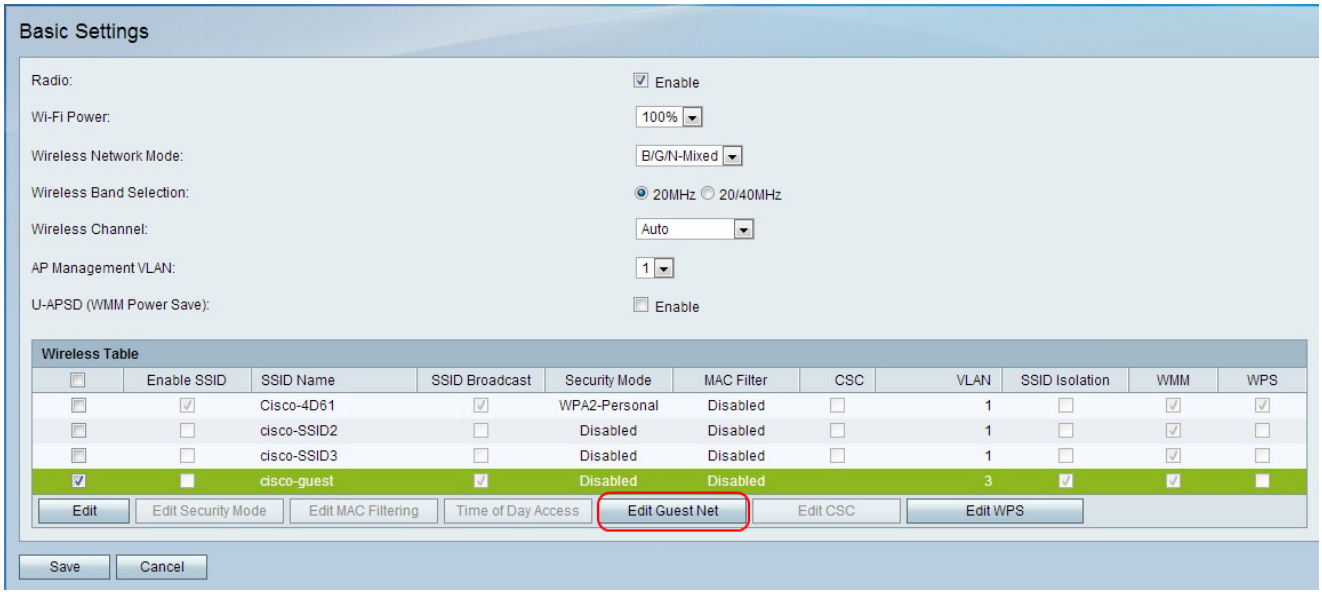
Step 4. In the Start Time field, enter the time when the access of the network begins.

Step 5. In the Stop Time field, enter the time when the access of the network ends.

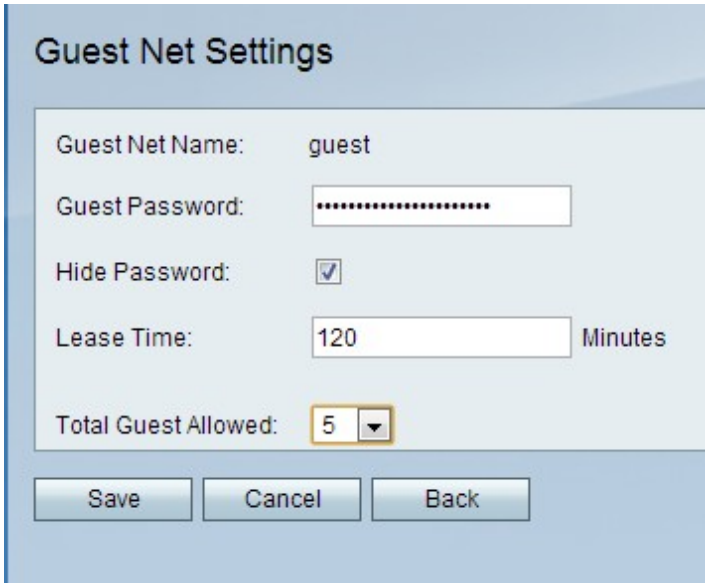
Step 6. Click **Save**.

Edit Guest Network

A guest network is a section of a network designed for temporary users. This is used to allow guests to access the network without the need to expose private Wi-Fi keys. A guest network can be configured to restrict the access time and bandwidth use of a user.



Step 1. Click **Edit Guest Network** to configure the guest network. The *Guest Net Settings* page opens:



Step 2. In the Guest Password field, enter a password that the users will use to enter the guest network.

Step 3. (Optional) To hide the password on the page, check the check box in the Hide Password field.

Step 4. In the Lease Time field, enter the time in minutes the users are allowed to stay connected to the guest network.

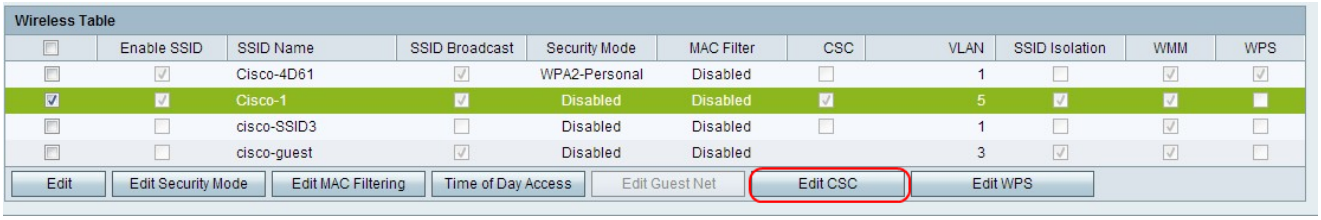
Step 5. From the Total Guest Allowed drop-down list, choose the total number of allowed guests.

Step 6. Click **Save**.

Edit CSC

CSC enables easy setup of a wireless network and allows easy connection of wireless devices to the network. The wireless device uses CSC to obtain the SSID and password of

the network, which allows for automatic connection to the network.



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

Step 2. Click **Edit CSC** to edit Cisco Simple Connect.

Step 3. Check the CSC check box.

Step 4. From the VLAN drop-down list choose the VLAN that is used for CSC.

Note: The Cisco Simple Connect VLAN cannot be the same as the current or other SSID VLAN. To create a new VLAN, refer to the article *VLAN Membership on the CVR100W Router*.

Note: CSC can only take effect of Wireless Distribution System (WDS) on SSID1. Refer to the article *Wireless Distribution System (WDS) on the CVR100W Router*.

Step 5. Click **Save**.