Wireless Wizard on ISA550W and ISA570W Integrated Security Appliances

Objective

The Wireless Wizard on the ISA550W and ISA570W Integrated Security Appliances allows an administrator to configure wireless settings quickly. The administrator is able to configure wireless radio and SSID settings with the Wireless Wizard. This article explains how to configure wireless settings with the Wireless Wizard on the ISA550W and ISA570W Integrated Security Appliances.

Applicable Devices

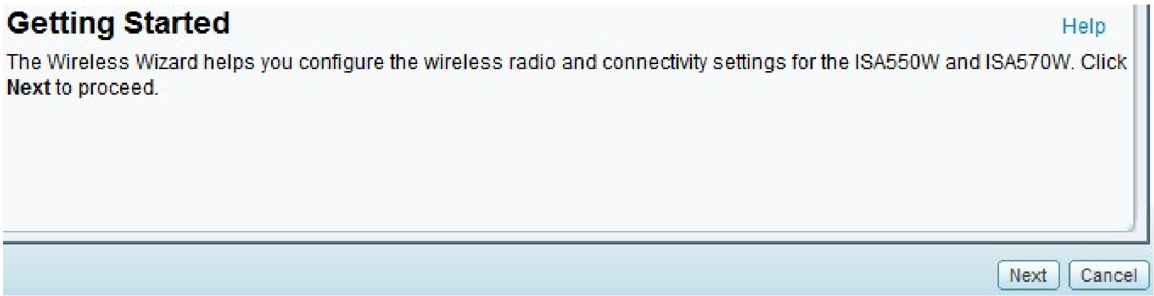
- ISA550W Integrated Security Appliance
- ISA570W Integrated Security Appliance

Software Version

- v1.1.14

Wireless Wizard

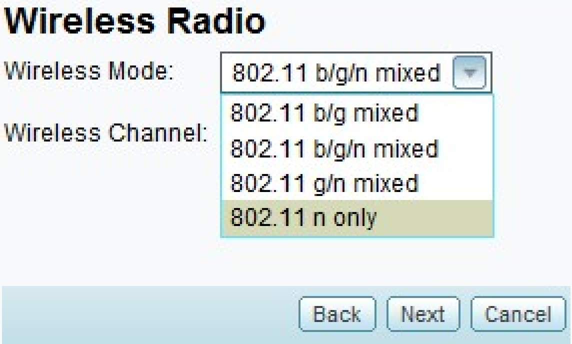
Step 1. Log in to the ISA500 Series Configuration Utility and choose **Configuration Wizards > Wireless Wizard**. The *Wireless Wizard* page opens:



Getting Started

The Wireless Wizard helps you configure the wireless radio and connectivity settings for the ISA550W and ISA570W. Click **Next** to proceed.

Step 2. Click **Next** to continue.



Wireless Radio

Wireless Mode: 802.11 b/g/n mixed

Wireless Channel:

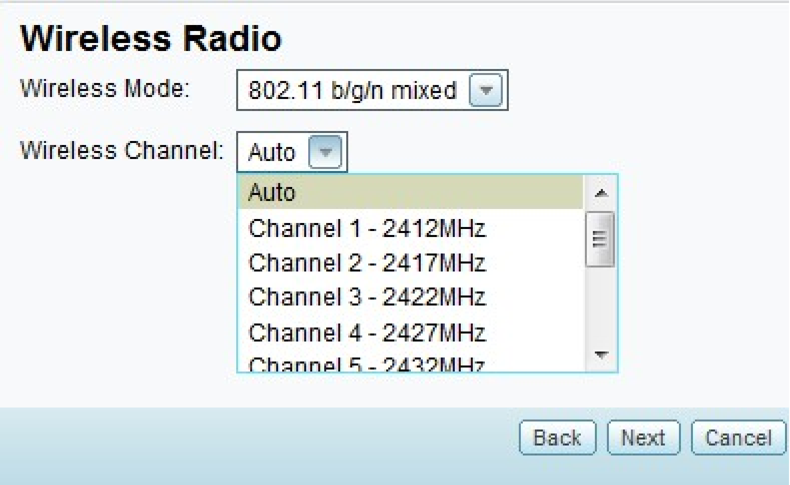
Step 3. From the Wireless Mode drop-down list, choose an option.

– 802.11 b/g mixed — This option only allows 802.11b and 802.11g devices to connect to the Integrated Security Appliance.

– 802.11 b/g/n mixed — This option allows 802.11b, 802.11g, and 802.11n devices to connect to the Integrated Security Appliance.

– 802.11 g/n mixed — This option only allows 802.11g and 802.11n devices to connect to the Integrated Security Appliance.

– 802.11 n only — This option only allows 802.11n devices to connect to the Integrated Security Appliance. They are faster than both 802.11 b and 802.11 g.



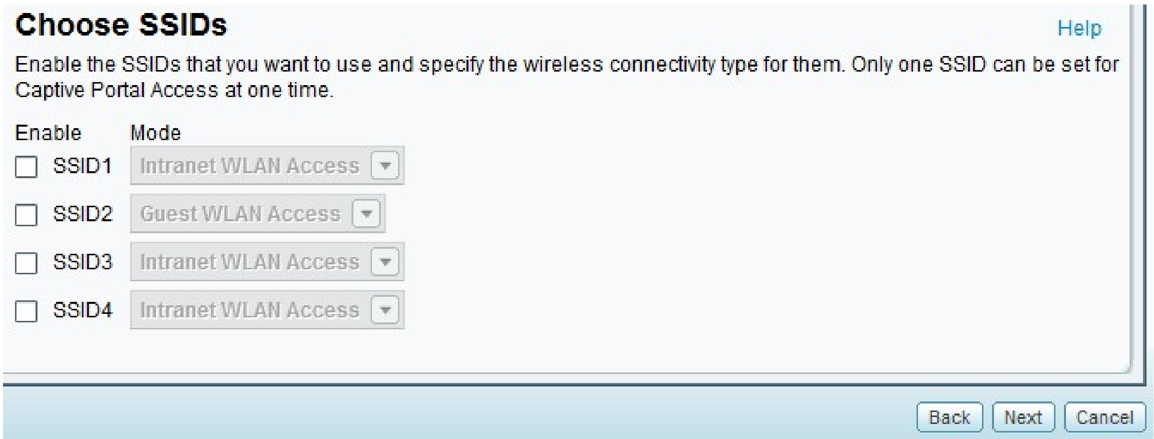
Wireless Radio

Wireless Mode: 802.11 b/g/n mixed

Wireless Channel: Auto

Step 4. From the Wireless Channel drop-down list, choose a channel for the frequency for the Integrated Security Appliance to use. Auto automatically chooses the optimal channel.

Step 5. Click **Next** to continue.



Choose SSIDs

Enable the SSIDs that you want to use and specify the wireless connectivity type for them. Only one SSID can be set for Captive Portal Access at one time.

Enable	Mode
□ SSID1	Intranet WLAN Access
□ SSID2	Guest WLAN Access
□ SSID3	Intranet WLAN Access
□ SSID4	Intranet WLAN Access

Step 6. Check the check box to the left of an SSID that you want to enable.

Step 7. From the Mode drop-down list, choose a mode for the enabled SSID. Only one SSID can be set to Captive Portal Access.

- Captive Portal Access — This option only lets authenticated users access the corporate network through the wireless network. The captive portal forces the user to look at a web page and accept the policy before the user gains access to the network.

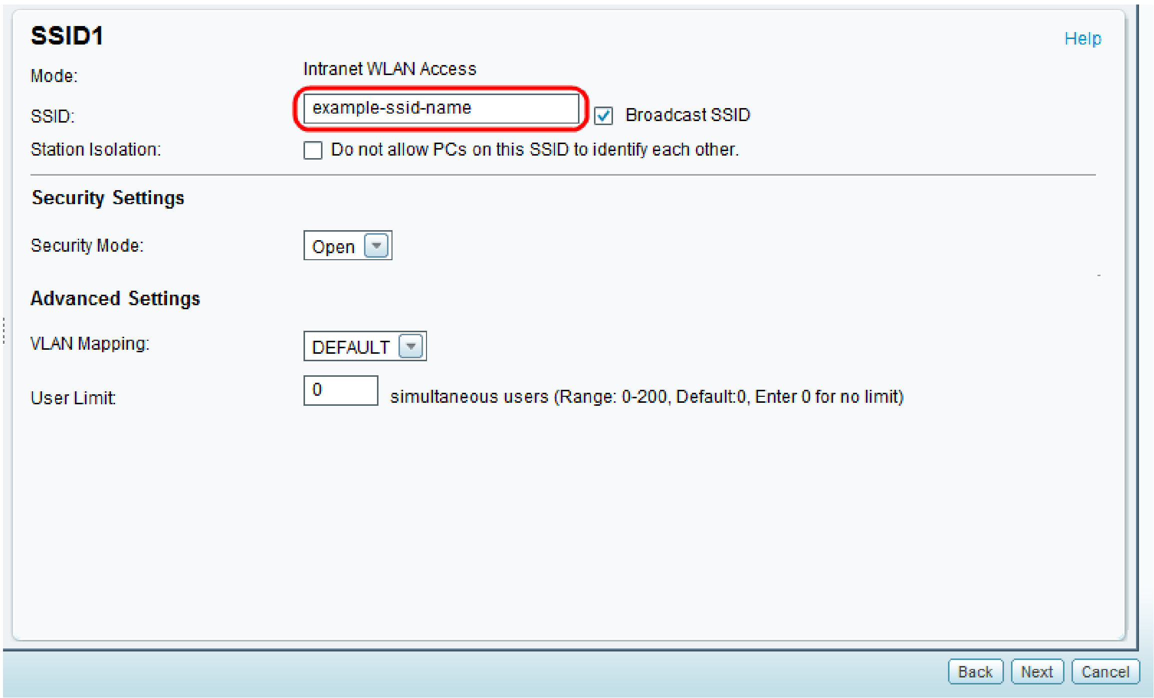
- Guest WLAN Access — This option allows the wireless users on the Guest SSID to access the wireless network and the users can't access the corporate network.

- Intranet WLAN Access — This option lets wireless users access the corporate network through the wireless network. The wireless network is formed by a collection of private computers within an organization.

Note: If you have chosen Captive portal in step 7, you can learn more about how to configure the Captive Portal Access in the article *Captive Portal Settings on ISA550W and ISA570W Series Integrated Security Appliances.*

Step 8. Repeat Steps 6 and 7 for each SSID that you want to enable.

Step 9. Click **Next** to continue.



SSID1

Mode: Intranet WLAN Access

SSID: example-ssid-name ☑ Broadcast SSID

Station Isolation: □ Do not allow PCs on this SSID to identify each other.

Security Settings

Security Mode: Open

Advanced Settings

VLAN Mapping: DEFAULT

User Limit: 0 simultaneous users (Range: 0-200, Default:0, Enter 0 for no limit)

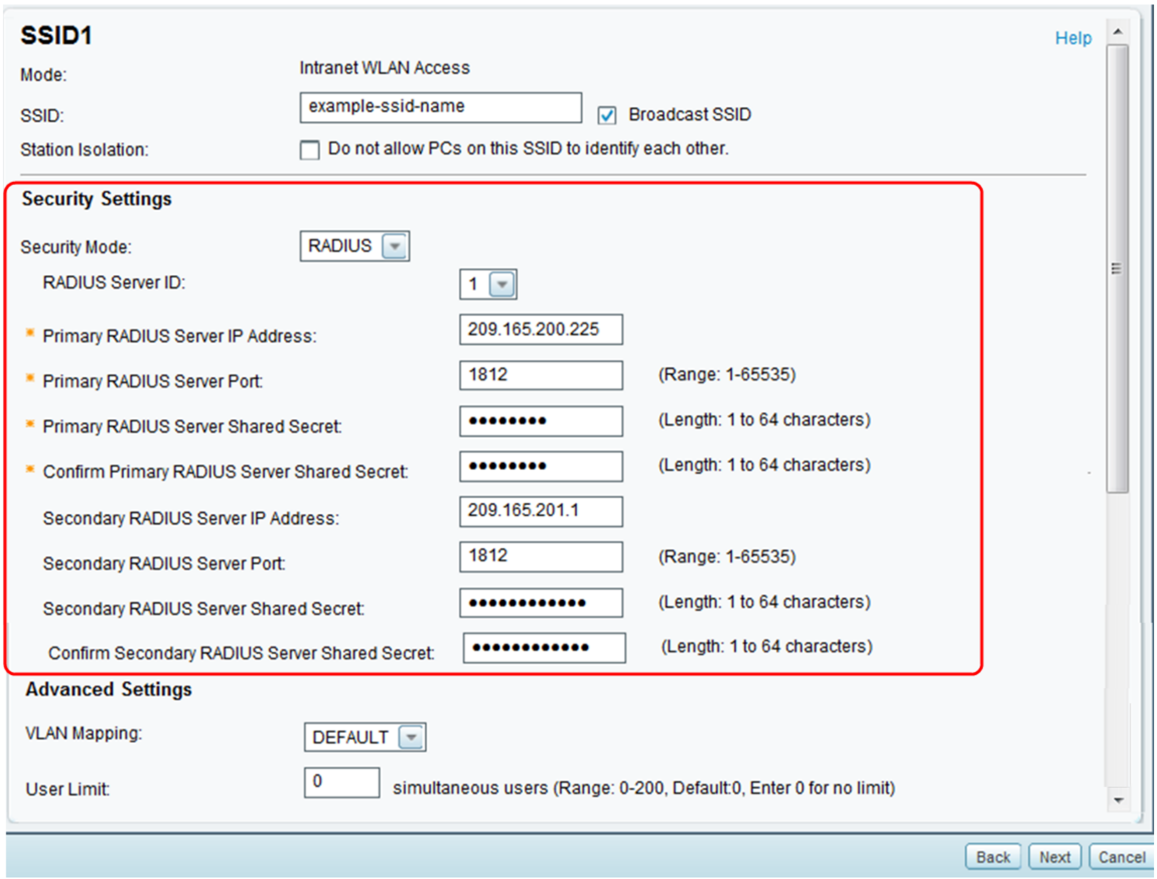
Step 10. In the SSID field, enter the name of the SSID.

Step 11. (Optional) Check the **Broadcast SSID** check box to broadcast the SSID to other devices.

Step 12. (Optional) Check the **Station Isolation** check box to hide devices on an SSID from one another.

Step 13. From the Security Mode drop-down list, choose a security protocol for the SSID.

- Open — This option allows all wireless devices to connect to the SSID.



SSID1

Mode: Intranet WLAN Access

SSID: example-ssid-name ☑ Broadcast SSID

Station Isolation: □ Do not allow PCs on this SSID to identify each other.

Security Settings

Security Mode: RADIUS

RADIUS Server ID: 1

* Primary RADIUS Server IP Address: 209.165.200.225

* Primary RADIUS Server Port: 1812 (Range: 1-65535)

* Primary RADIUS Server Shared Secret: •••••••• (Length: 1 to 64 characters)

* Confirm Primary RADIUS Server Shared Secret: •••••••• (Length: 1 to 64 characters)

Secondary RADIUS Server IP Address: 209.165.201.1

Secondary RADIUS Server Port: 1812 (Range: 1-65535)

Secondary RADIUS Server Shared Secret: ••••••••••••• (Length: 1 to 64 characters)

Confirm Secondary RADIUS Server Shared Secret: ••••••••••••• (Length: 1 to 64 characters)

Advanced Settings

VLAN Mapping: DEFAULT

User Limit: 0 simultaneous users (Range: 0-200, Default:0, Enter 0 for no limit)

• RADIUS — This option uses Remote Authentication Dial In User Service (RADIUS) servers and WEP for authentication.

– RADIUS Server ID — From this drop-down list, choose a RADIUS group to use for authentication.

– Primary RADIUS Server IP Address — Enter the IP address of the primary RADIUS server.

– Primary RADIUS Server Port — Enter the port number of the primary RADIUS server to which the user connects.

– Primary RADIUS Server Shared Secret — Enter the shared secret for the primary RADIUS server. The key which you enter must match it with the RADIUS Server key.

– Confirm Primary RADIUS Server Shared Secret — Enter the shared secret for the primary RADIUS server again.

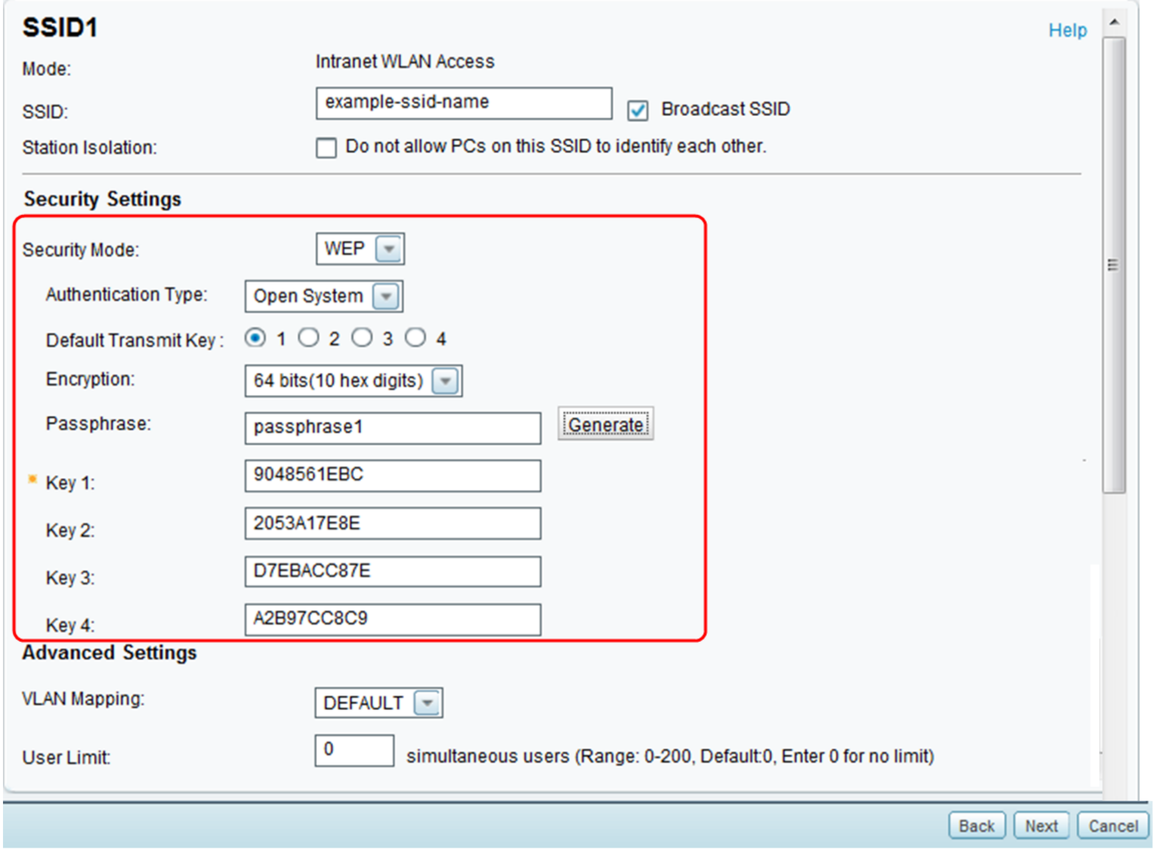
Note: Based on your needs, configure the Secondary RADIUS. The Secondary RADIUS Server is optional and it is used only for the back-up of the Primary RADIUS server.

– Secondary RADIUS Server IP Address — Enter the IP address of the secondary RADIUS server.

– Secondary RADIUS Server Port — Enter the port number of the secondary RADIUS server to which the user connects.

– Secondary RADIUS Server Shared Secret — Enter the shared secret for the secondary RADIUS server.

– Confirm Secondary RADIUS Server Shared Secret — Enter the shared secret for the secondary RADIUS server again.



SSID1

Mode: Intranet WLAN Access

SSID: example-ssid-name ☑ Broadcast SSID

Station Isolation: □ Do not allow PCs on this SSID to identify each other.

Security Settings

Security Mode: WEP

Authentication Type: Open System

Default Transmit Key : ● 1 ○ 2 ○ 3 ○ 4

Encryption: 64 bits(10 hex digits)

Passphrase: passphrase1

Key 1: 9048561EBC

Key 2: 2053A17E8E

Key 3: D7EBACC87E

Key 4: A2B97CC8C9

Advanced Settings

VLAN Mapping: DEFAULT

User Limit: 0 simultaneous users (Range: 0-200, Default:0, Enter 0 for no limit)

- WEP — Wired Equivalent Privacy (WEP) is an older encryption method and uses either a 64-bit or 128-bit shared key.

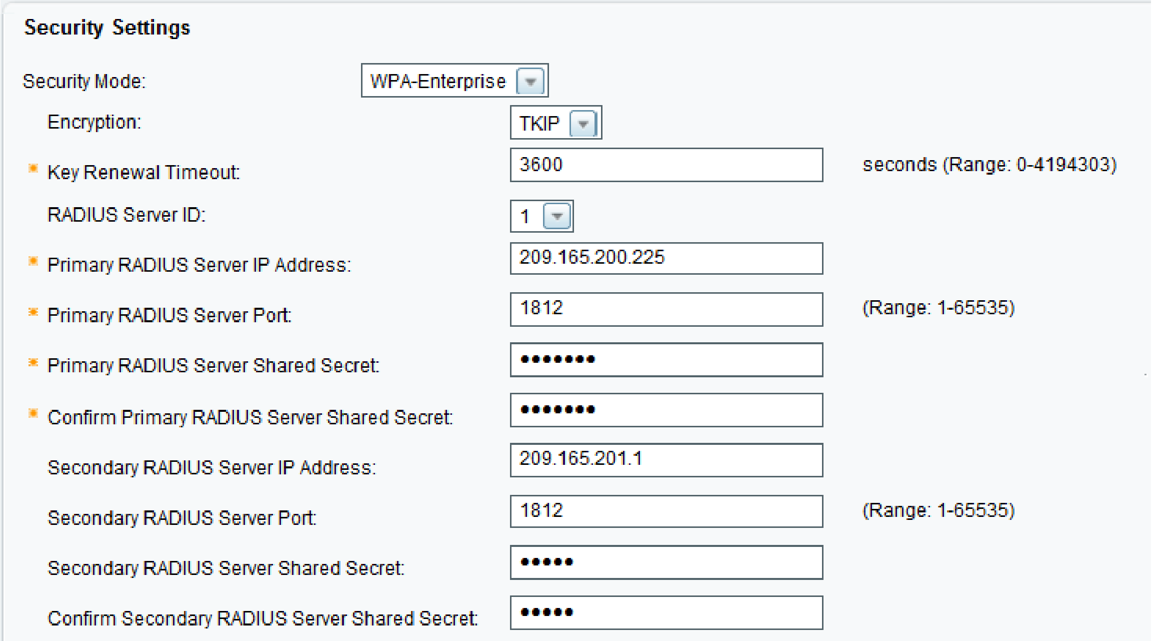
– Authentication Type — From this drop-down list, choose **Open System** or **Shared Key** , or choose **Auto** to use both. Open key system does not have an authentication mechanism and everyone can join this network if they know the SSID, whereas in the Shared key authentication both the ISA device and the wireless device must have the same key to authenticate.

– Default Transmit Key — Click the radio button of one of the key indices. After the Passphrase is generated, the selected Key is used for authentication.

– Encryption — From this drop-down list, choose an encryption type. The options are a 64-bit and a 128-bit encryption type. The key strength of a 64-bit is less compared to a 128-bit.

– Passphrase — In this field, enter a passphrase to be used to make keys.

– Click **Generate**. Four keys are generated.



Security Settings

Security Mode:	WPA-Enterprise	
Encryption:	TKIP	
* Key Renewal Timeout:	3600	seconds (Range: 0-4194303)
RADIUS Server ID:	1	
* Primary RADIUS Server IP Address:	209.165.200.225	
* Primary RADIUS Server Port:	1812	(Range: 1-65535)
* Primary RADIUS Server Shared Secret:	•••••••	
* Confirm Primary RADIUS Server Shared Secret:	•••••••	
Secondary RADIUS Server IP Address:	209.165.201.1	
Secondary RADIUS Server Port:	1812	(Range: 1-65535)
Secondary RADIUS Server Shared Secret:	•••••	
Confirm Secondary RADIUS Server Shared Secret:	•••••	

- WPA-Enterprise — Wi-Fi Protected Access (WPA) uses dynamic key encryption and is meant to replace WEP. WPA-Enterprise uses both WPA and RADIUS servers and support both Temporal Key Integrity Protocol (TKIP) and Advanced Encryption System (AES) encryptions.

– Encryption — Choose either **TKIP** or **AES**. AES uses a strong encryption method as it uses 128 bits for encryption and provides better security, whereas TKIP also provides security but it uses only 64 bits for encryption, But AES requires more processing and computation resources to encrypt as it uses 128 bit.

– Key Renewal Timeout — Enter a length of time in seconds for how long the key waits before it is refreshed. A value of zero states that the key is never refreshed.

– RADIUS Server ID — Choose a RADIUS group to use for authentication.

– Primary RADIUS Server IP Address — Enter the IP address of the primary RADIUS server.

– Primary RADIUS Server Port — Enter the port number of the primary RADIUS server to which the user connects.

– Primary RADIUS Server Shared Secret — Enter the shared secret for the primary RADIUS server. The key which you enter must match it with the RADIUS Server key.

– Confirm Primary RADIUS Server Shared Secret — Enter the shared secret for the primary RADIUS server again.

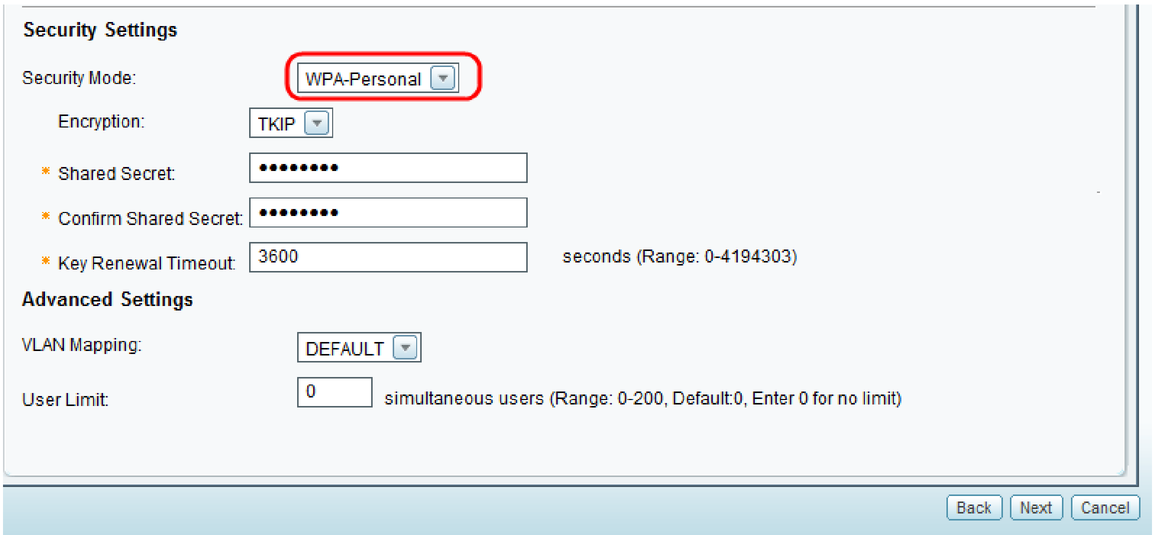
Note: Based on your needs, configure the Secondary RADIUS. The Secondary RADIUS Server is optional and it is used only for the back-up of the Primary RADIUS server.

– Secondary RADIUS Server IP Address — Enter the IP address of the secondary RADIUS server.

– Secondary RADIUS Server Port — Enter the port number of the secondary RADIUS server to which the user connects.

– Secondary RADIUS Server Shared Secret — Enter the shared secret for the secondary RADIUS server.

– Confirm Secondary RADIUS Server Shared Secret — Enter the shared secret for the secondary RADIUS server.



Security Settings

Security Mode: WPA-Personal

Encryption: TKIP

* Shared Secret: ••••••••

* Confirm Shared Secret: ••••••••

* Key Renewal Timeout: 3600 seconds (Range: 0-4194303)

Advanced Settings

VLAN Mapping: DEFAULT

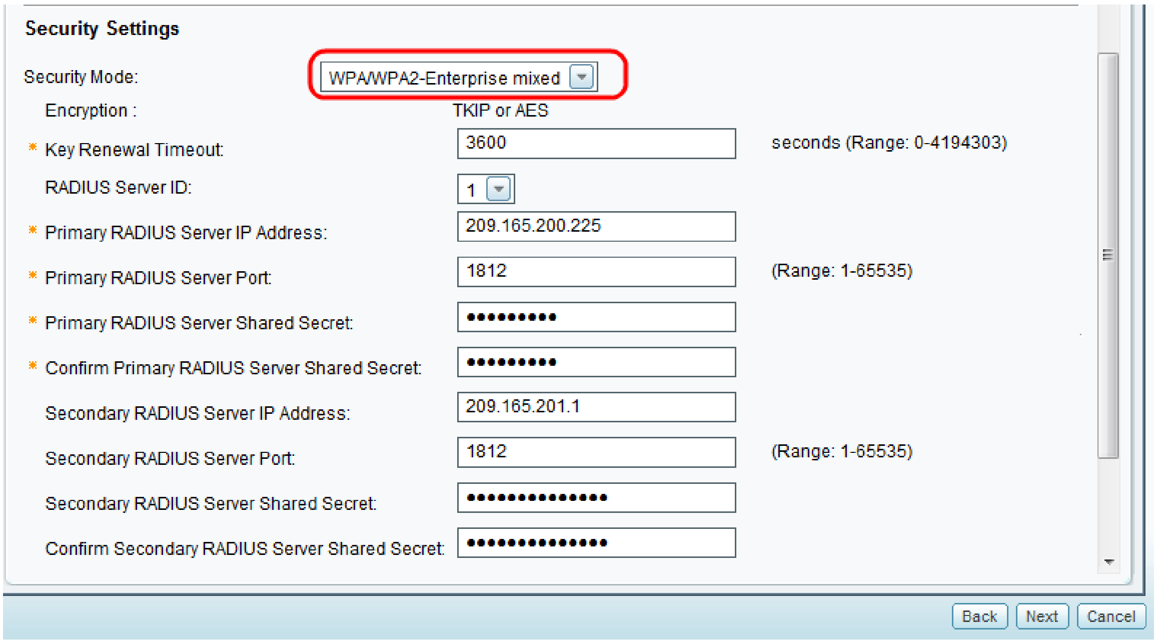
User Limit: 0 simultaneous users (Range: 0-200, Default:0, Enter 0 for no limit)

• WPA-Personal — This option uses WPA and supports TKIP and AES encryptions.

– Encryption — Choose either **TKIP** or **AES**. AES uses a strong encryption method as it uses 128 bits for encryption and provides better security, whereas TKIP also provides security but it uses only 64 bits for encryption. However, AES need more processing and computation resources to encrypt as it uses 128bit key.

– Shared Secret — Enter a pre-shared key.

– Key Renewal Timeout — Enter a length of time in seconds for how long the key waits before it is refreshed. A value of zero states that the key is never refreshed.



Security Settings

Security Mode: WPA/WPA2-Enterprise mixed

Encryption : TKIP or AES

* Key Renewal Timeout: 3600 seconds (Range: 0-4194303)

RADIUS Server ID: 1

* Primary RADIUS Server IP Address: 209.165.200.225

* Primary RADIUS Server Port: 1812 (Range: 1-65535)

* Primary RADIUS Server Shared Secret: •••••••••

* Confirm Primary RADIUS Server Shared Secret: •••••••••

Secondary RADIUS Server IP Address: 209.165.201.1

Secondary RADIUS Server Port: 1812 (Range: 1-65535)

Secondary RADIUS Server Shared Secret: ••••••••••••••

Confirm Secondary RADIUS Server Shared Secret: ••••••••••••••

• WPA/WPA2-Enterprise mixed — This option supports WPA-Enterprise and WPA2-Enterprise devices.

– Key Renewal Timeout — Enter a length of time in seconds for how long the key waits before it is refreshed. A value of zero states that the key is never refreshed.

– RADIUS Server ID — Choose a RADIUS group to use for authentication.

– Primary RADIUS Server IP Address — Enter the IP address of the primary RADIUS server.

– Primary RADIUS Server Port — Enter the port number of the primary RADIUS server to which the user connects.

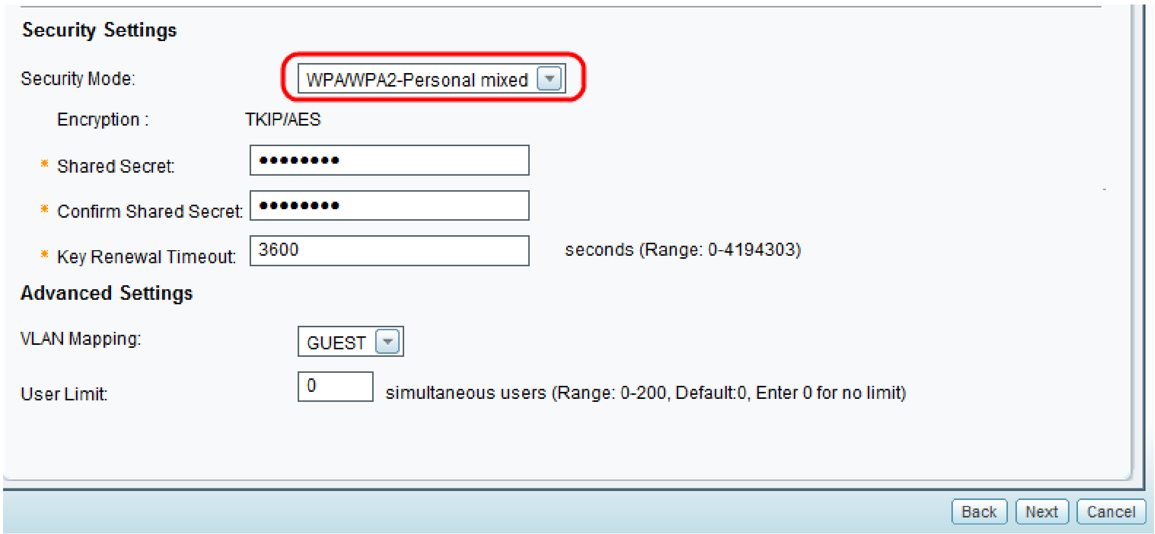
– Primary RADIUS Server Shared Secret — Enter the shared secret for the primary RADIUS server. The key which you enter must match it with the RADIUS Server key.

Note: Based on your needs, configure the Secondary RADIUS. The Secondary RADIUS Server is optional and it is used only for the back-up of the Primary RADIUS server.

– Secondary RADIUS Server IP Address — Enter the IP address of the secondary RADIUS server.

– Secondary RADIUS Server Port — Enter the port number of the secondary RADIUS server to which the user connects.

– Secondary RADIUS Server Shared Secret — Enter the shared secret for the secondary RADIUS server.



Security Settings

Security Mode: WPA/WPA2-Personal mixed

Encryption : TKIP/AES

* Shared Secret: ●●●●●●●●

* Confirm Shared Secret: ●●●●●●●●

* Key Renewal Timeout: 3600 seconds (Range: 0-4194303)

Advanced Settings

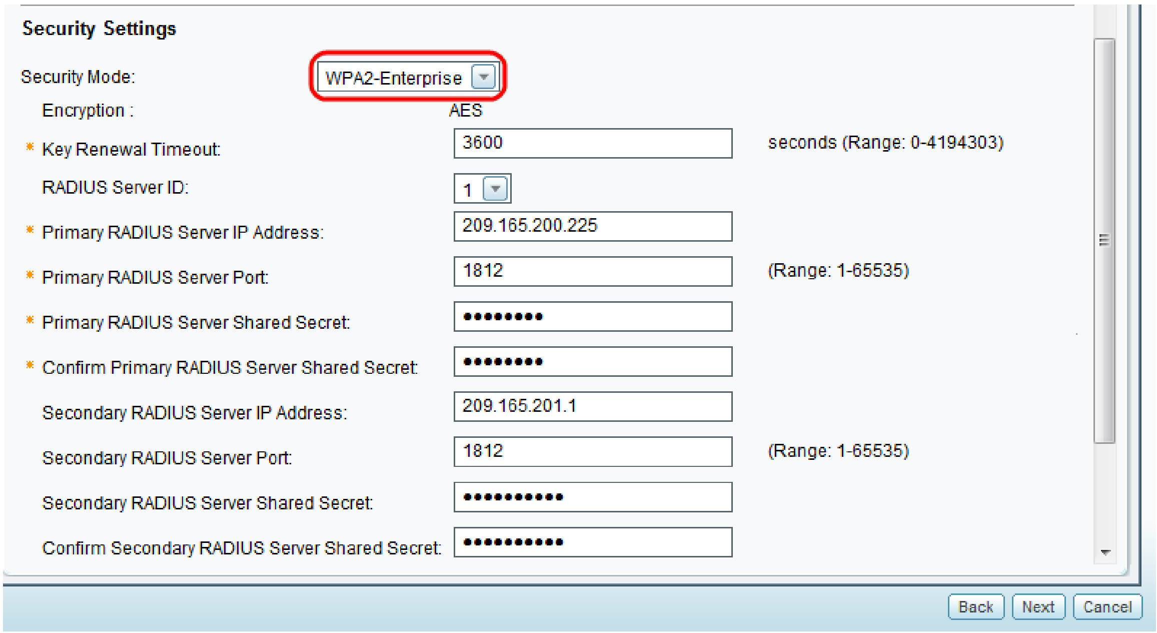
VLAN Mapping: GUEST

User Limit: 0 simultaneous users (Range: 0-200, Default:0, Enter 0 for no limit)

• WPA/WPA2-Personal mixed — This option supports WPA-Personal and WPA2-Personal devices.

– Shared Secret — Enter a pre-shared key.

– Key Renewal Timeout — Enter a length of time in seconds for how long the key waits before it is refreshed. A value of zero states that the key is never refreshed.



Security Settings

Security Mode:	WPA2-Enterprise	
Encryption :	AES	
* Key Renewal Timeout:	3600	seconds (Range: 0-4194303)
RADIUS Server ID:	1	
* Primary RADIUS Server IP Address:	209.165.200.225	
* Primary RADIUS Server Port:	1812	(Range: 1-65535)
* Primary RADIUS Server Shared Secret:	•••••••••	
* Confirm Primary RADIUS Server Shared Secret:	••••••••	
Secondary RADIUS Server IP Address:	209.165.201.1	
Secondary RADIUS Server Port:	1812	(Range: 1-65535)
Secondary RADIUS Server Shared Secret:	•••••••••••	
Confirm Secondary RADIUS Server Shared Secret:	•••••••••••	

• WPA2-Enterprise — WPA2 is the most secure option for wireless connections. WPA2-Enterprise uses WPA2 and RADIUS servers for authentication and supports AES encryption only.

– Key Renewal Timeout — Enter a length of time in seconds for how long the key waits before it is refreshed. A value of zero states that the key is never refreshed.

– RADIUS Server ID — Choose a RADIUS group to use for authentication.

– Primary RADIUS Server IP Address — Enter the IP address of the primary RADIUS server.

– Primary RADIUS Server Port — Enter the port number of the primary RADIUS server to which the user connects.

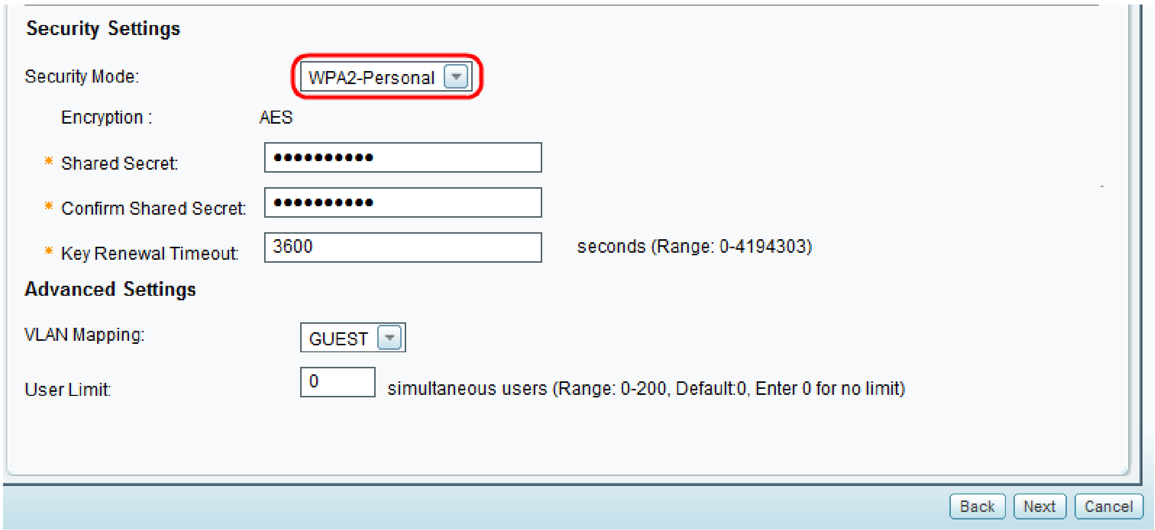
– Primary RADIUS Server Shared Secret — Enter the shared secret for the primary RADIUS server. The key which you enter must match it with the RADIUS Server key.

Note: Based on your needs, configure the Secondary RADIUS. The Secondary RADIUS Server is optional and it is used only for the back-up of the Primary RADIUS server.

– Secondary RADIUS Server IP Address — Enter the IP address of the secondary RADIUS server.

– Secondary RADIUS Server Port — Enter the port number of the secondary RADIUS server to which the user connects.

– Secondary RADIUS Server Shared Secret — Enter the shared secret for the secondary RADIUS server.



Security Settings

Security Mode: WPA2-Personal

Encryption : AES

* Shared Secret: ●●●●●●●●●●●

* Confirm Shared Secret: ●●●●●●●●●●●

* Key Renewal Timeout: 3600 seconds (Range: 0-4194303)

Advanced Settings

VLAN Mapping: GUEST

User Limit: 0 simultaneous users (Range: 0-200, Default:0, Enter 0 for no limit)

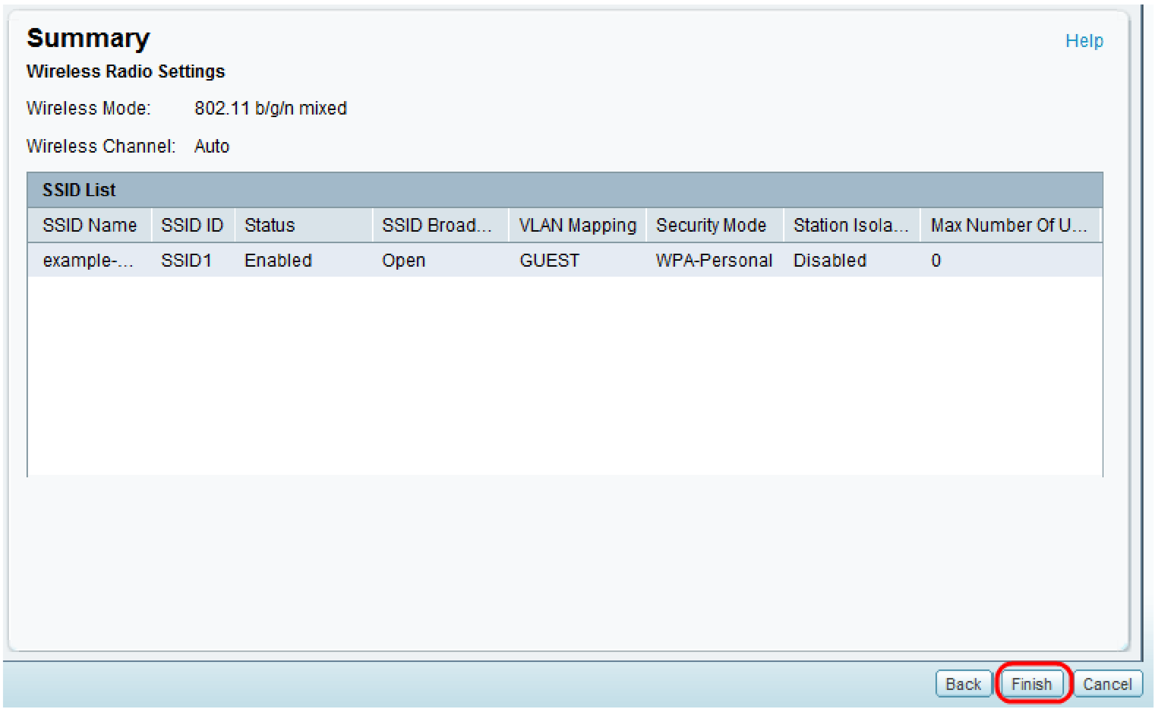
- WPA2-Personal — This option uses WPA2 for encryption and supports AES encryption only.

  – Shared Secret — Enter a pre-shared key.

  – Key Renewal Timeout — Enter a length of time in seconds for how long the key waits before it is refreshed. A value of zero states that the key is never refreshed.

Step 14. Repeat Steps 10 through 13 for each enabled SSID.

Step 15. Click **Next** to continue.



Summary

Wireless Radio Settings

Wireless Mode: 802.11 b/g/n mixed

Wireless Channel: Auto

SSID List

SSID Name	SSID ID	Status	SSID Broad...	VLAN Mapping	Security Mode	Station Isola...	Max Number Of U...
example-...	SSID1	Enabled	Open	GUEST	WPA-Personal	Disabled	0

Step 16. Click **Finish**.