Configure Work Group Bridge on WAP121 and WAP321 Access Points

Objective

The work group bridge feature enables the Wireless Access Point (WAP) to bridge traffic between a remote client and the wireless LAN that is connected with the work group bridge mode. The WAP device associated with the remote interface is known as an access point interface, and the one associated with the wireless LAN is called an infrastructure interface. This feature is recommended to be used when the WDS feature is not possible to use since the WDS feature is a preferred bridge solution for the WAP121 and WAP321. When the work group bridge feature is enabled, the WDS bridge feature does not work. To see how WDS Bridge is configured, refer to the article *Wireless Distribution System (WDS) Bridge Configuration on WAP121 and WAP321 Access Points* .

This article explains how to configure the work group bridge on WAP121 and WAP321 access points.

Applicable Devices

- WAP121
- WAP321

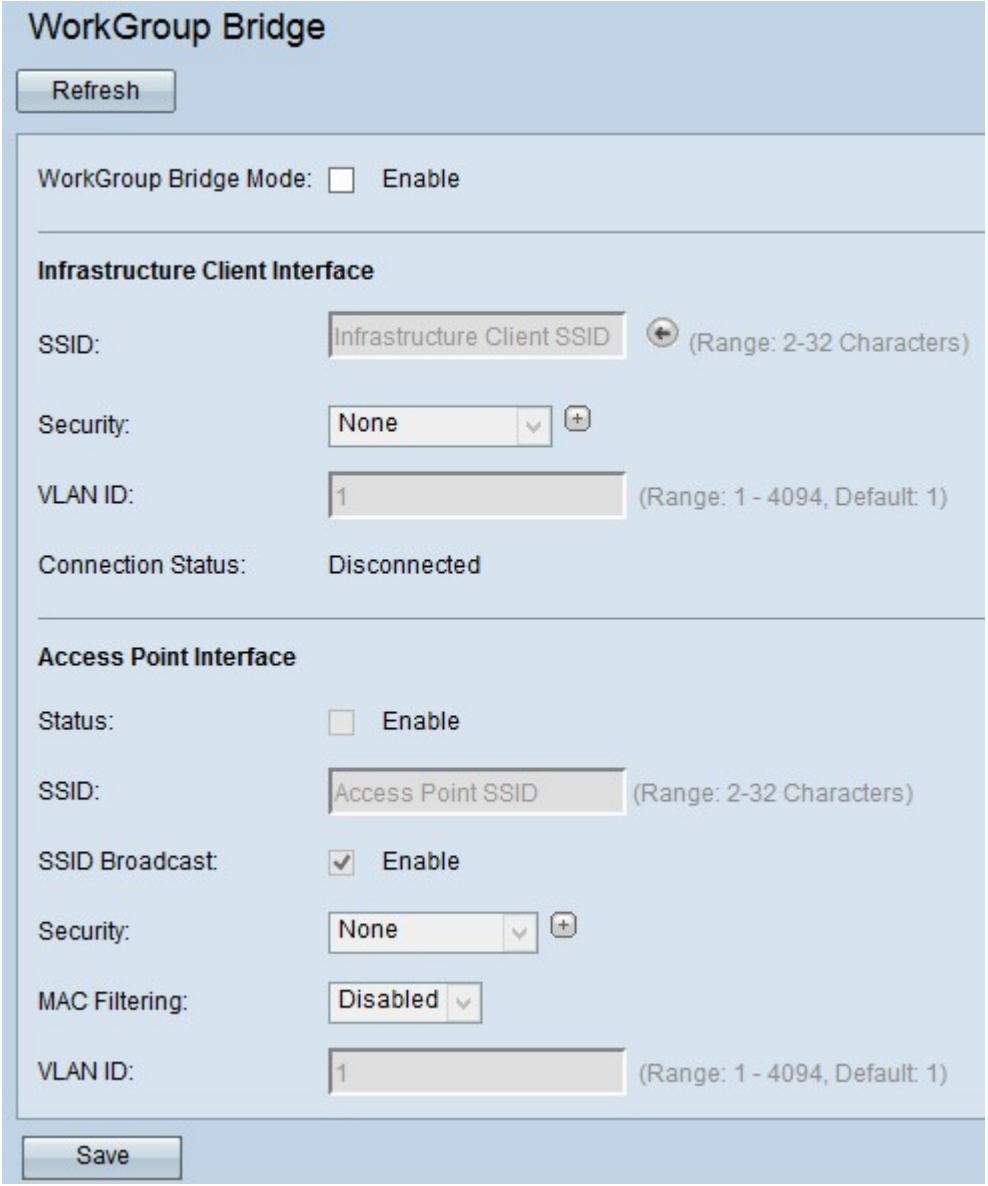
Software Version

- 1.0.3.4

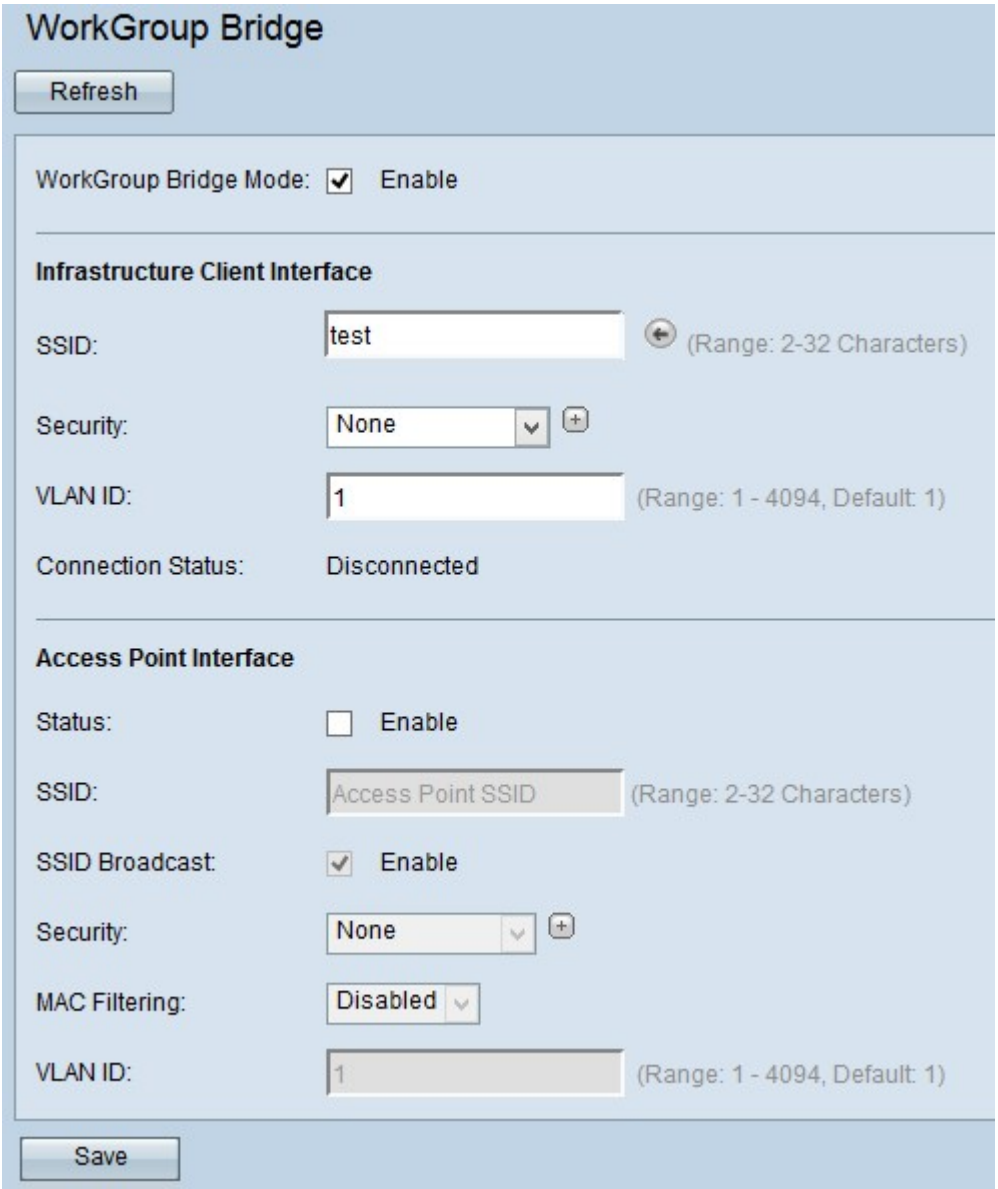
Configure Work Group Bridge

Note: To be able to enable work group bridge, clustering must be enabled in the WAP. If it is disabled, you need to Disable Single Point Setup which in turn enables clustering. All WAP devices that take part in the Workgroup bridge must have common settings for radio, IEEE 802.11 mode, Channel Bandwidth, and Channel (audio not recommended). To ensure these settings in all devices are the same, look up the radio settings. To configure these settings, refer to the article *Configuration of Basic Wireless Radio Settings on the WAP121 and the WAP321 Access Points* .

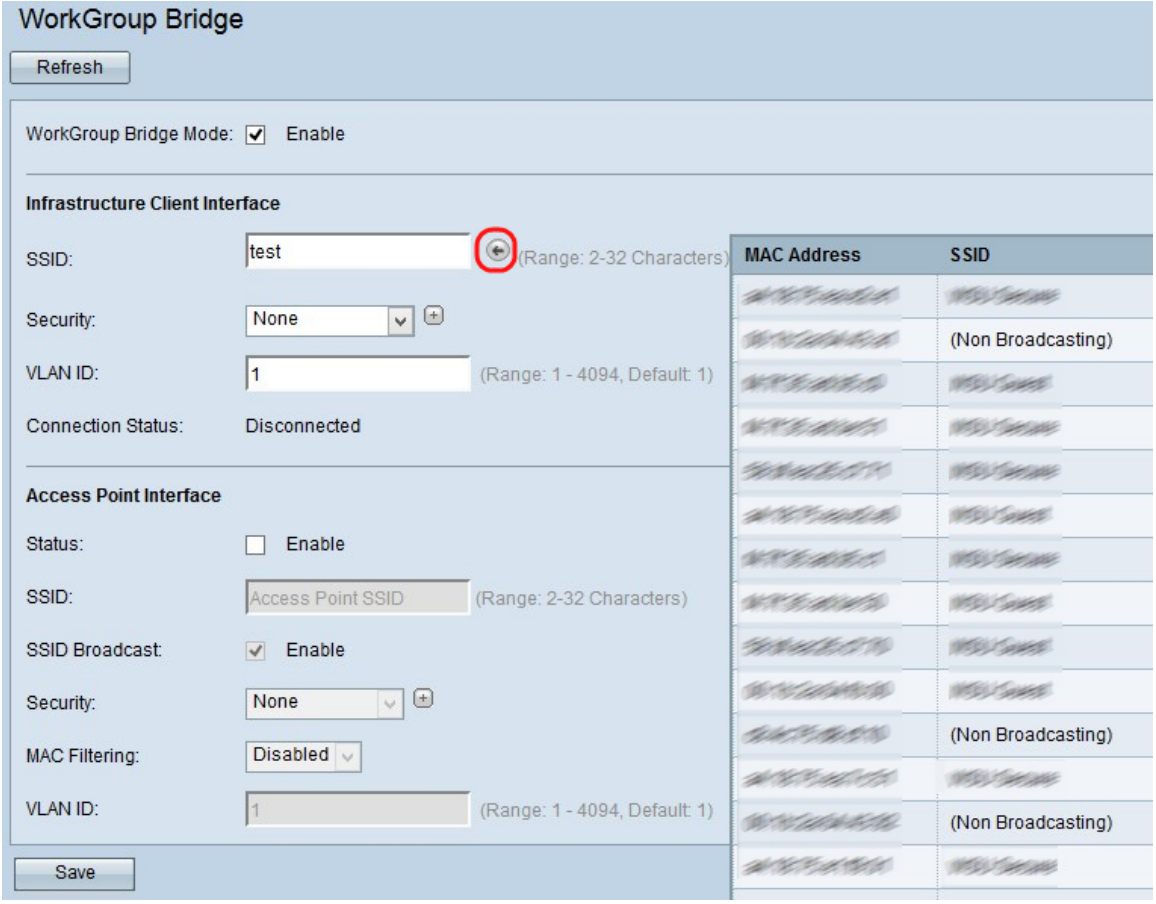
Step 1. Log in to the Access Point Configuration Utility and choose **Wireless > Work Group Bridge**. The *WorkGroup Bridge* page opens up:



Step 2. Check **Enable** in the *WorkGroup Bridge Mode* field to enable the work group bridge feature.

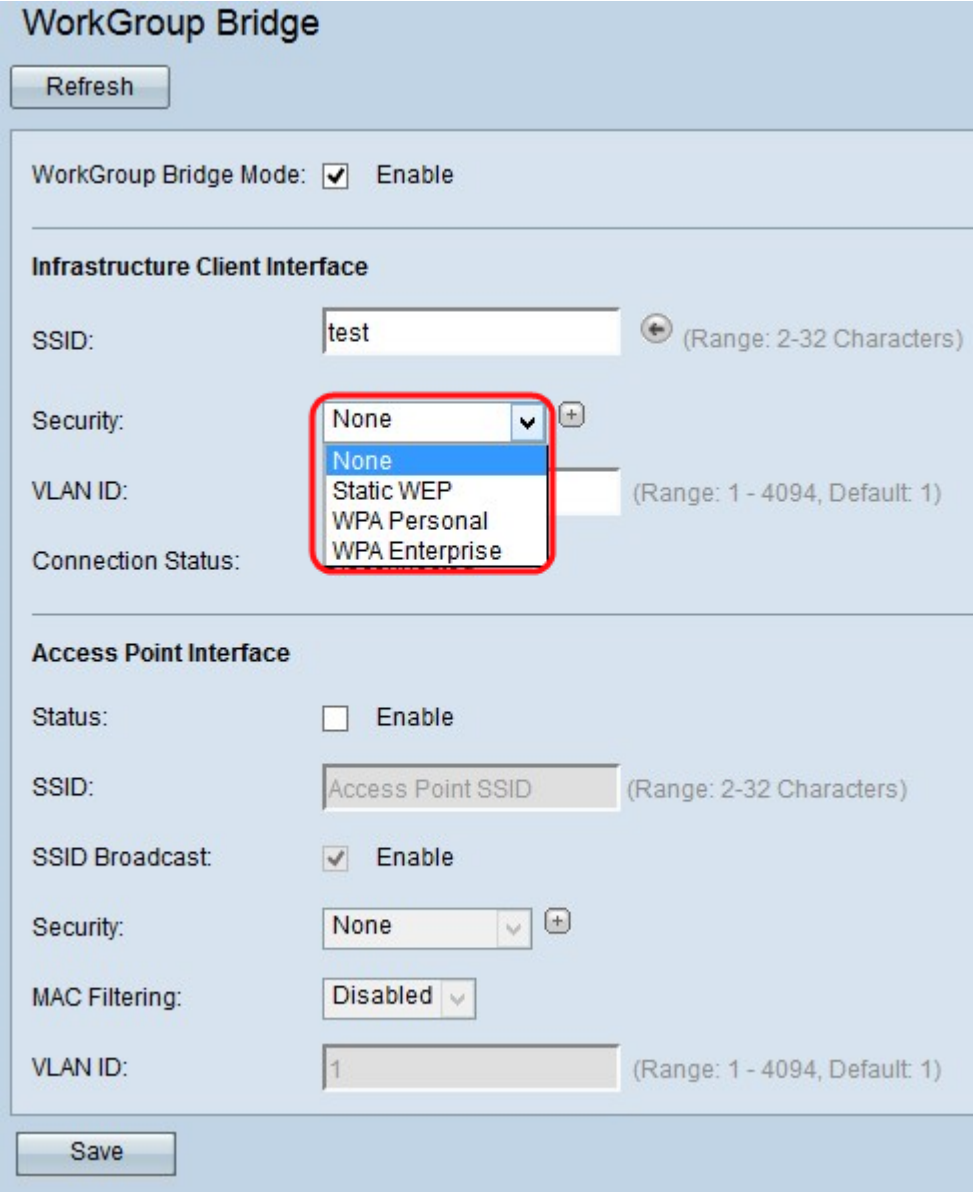


Step 3. Enter the Service Set Identifier (SSID) name in the *SSID* field for infrastructure client interface.



Tip: You can also click the **Arrow** icon beside the *SSID* field to scan for similar neighbor SSIDs. This is enabled only if AP Detection is enabled in Rogue AP Detection which is disabled by default. Refer to the article *Rogue AP Detection on the WAP121 and WAP321 Access Points* to enable Rogue AP detection.

Step 4. Choose the type of security to authenticate a client station on the upstream WAP device (Infrastructure Client Interface) from the *Security* drop-down list. The possible values are:



• None — Open or no security. This is the default value. If you choose this, skip to Step 5.

• Static WEP — Static WEP is the minimal security and can support up to 4 keys of length 64 to128 bits. The same key must be used in all nodes. For configuration for static WEP, go to Static WEP.

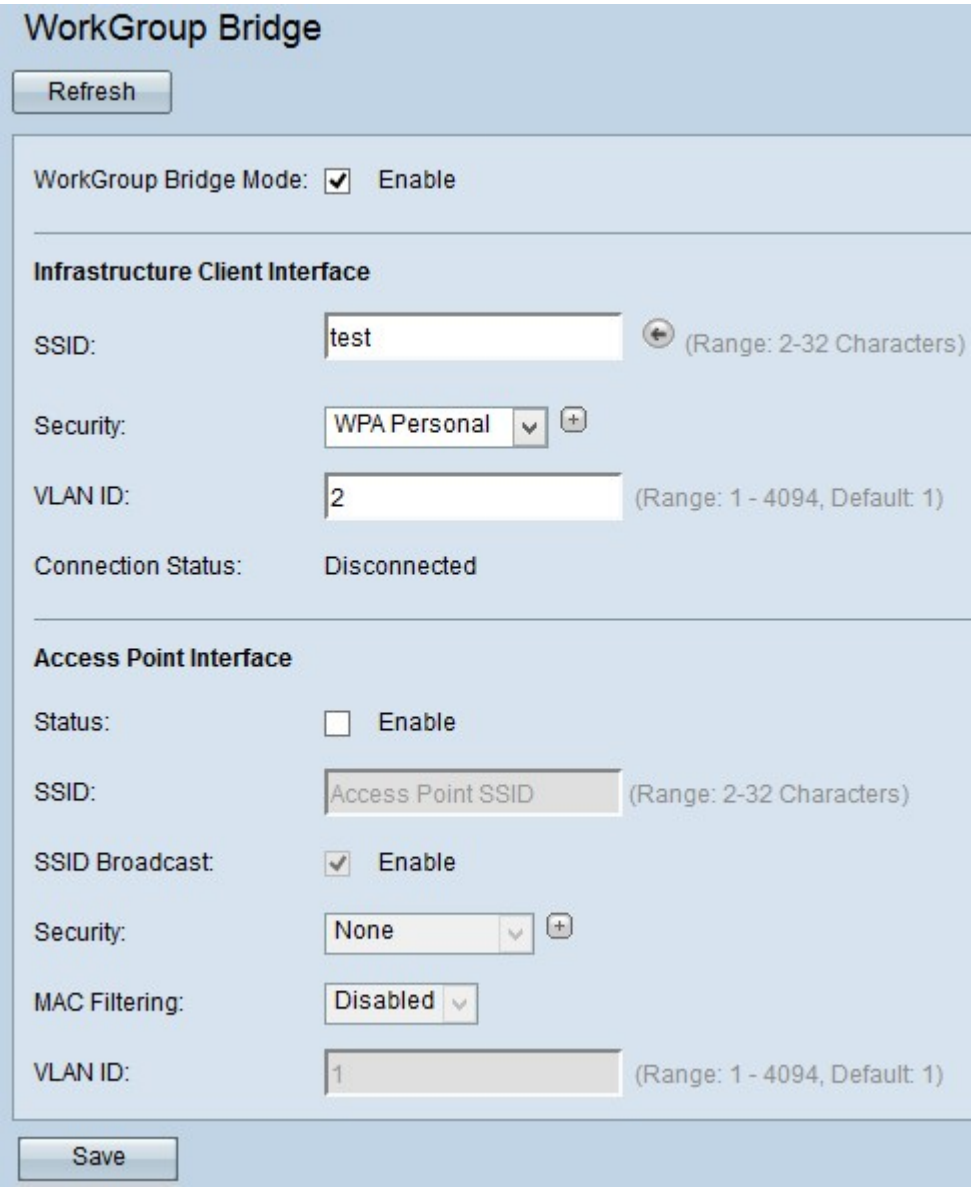
• WPA Personal — WPA Personal is more advanced compared to WEP and can support keys of length 8-63 characters. The encryption method is RC4 for WPA and Advanced Encryption Standard (AES) for WPA2. WPA2 is recommended as it has a more powerful encryption standard. For configuration of WPA personal, go to WPA Personal for Client Interface.

• WPA Enterprise — WPA Enterprise is the most advanced and recommended security. It uses Protected Extensible Authentication Protocol (PEAP) in which each and every wireless user under WAP is authorized with individual usernames and passwords that can even support AES encryption standards. It also uses Transport Layer Security (TLS) in addition to PEAP, in which each and every user also needs to provide an additional certificate to gain access. The encryption method is RC4 for WPA and Advanced Encryption Standard (AES) for WPA2. For configuration of the WPA enterprise, go to WPA Enterprise.

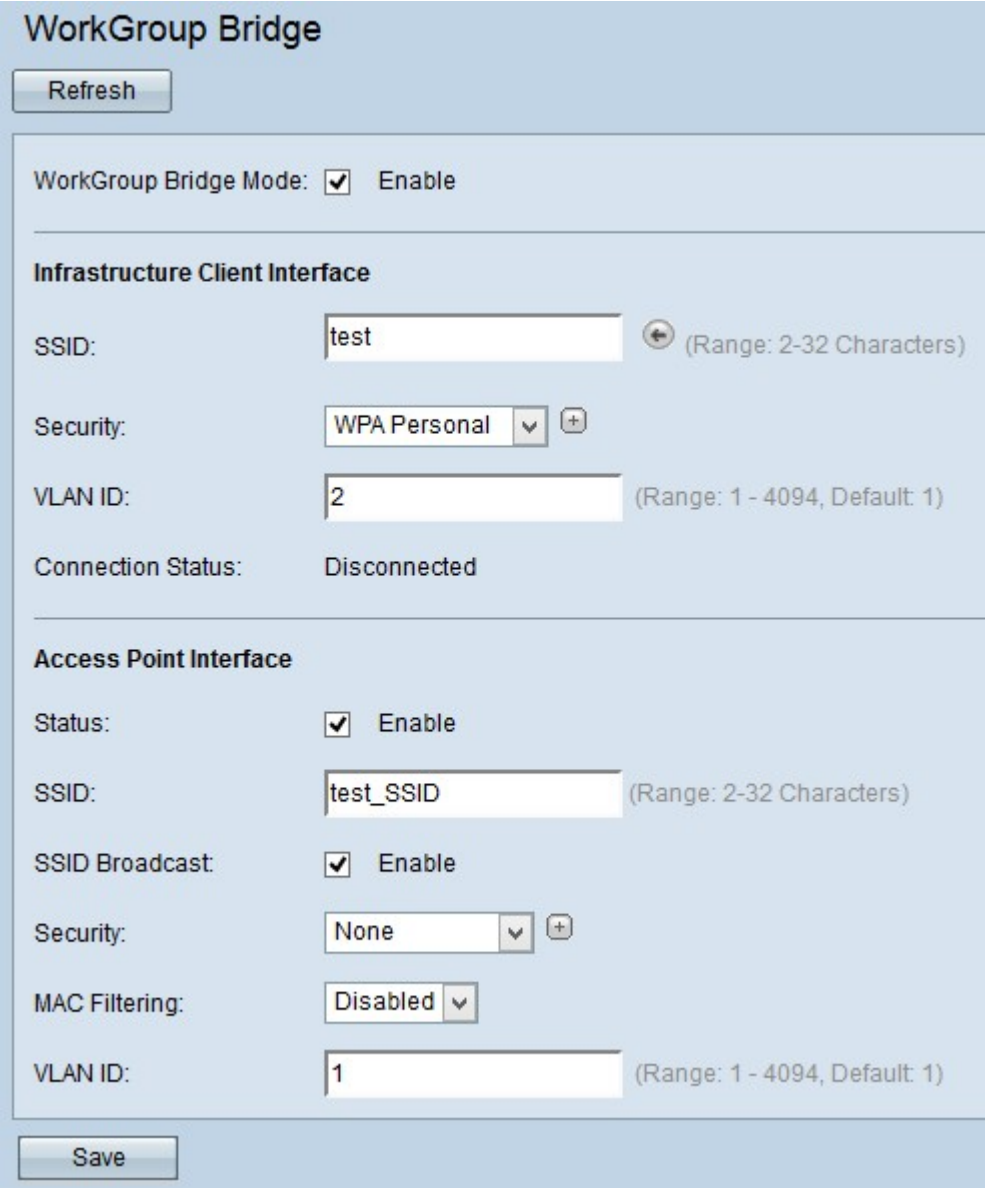
Note: Based on what IEEE 802.11 mode is chosen, the availability of the above options may

vary.

Step 5. Enter the VLAN ID in the *VLAN ID* field for the infrastructure client interface.



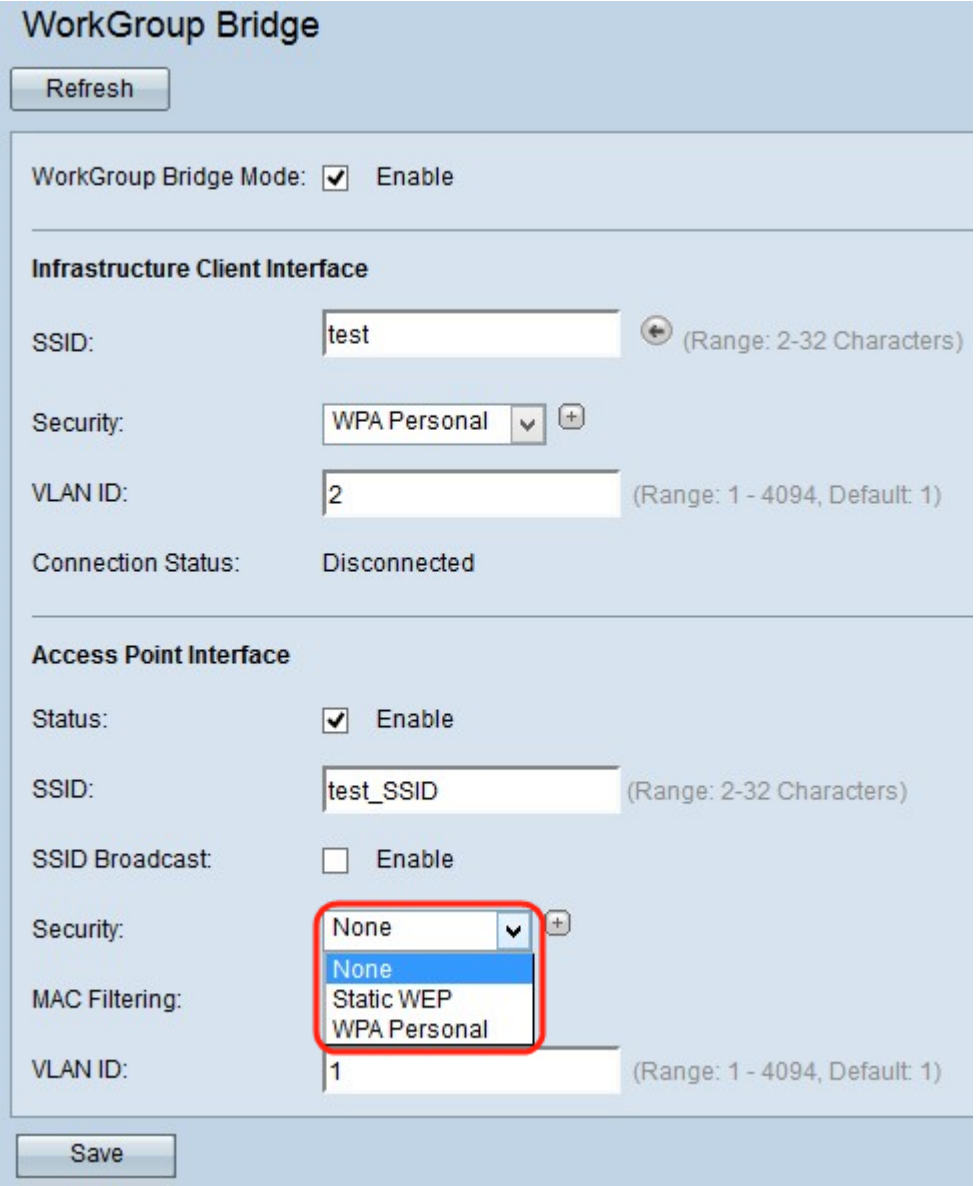
Step 6. Check **Enable** in the *Status* field to enable bridging on the access point interface.



Step 7. Enter the Service Set Identifier (SSID) in the *SSID* field name for the access point interface.

Step 8. (Optional) If you want to broadcast the downstream SSID, check **Enable** in the *SSID Broadcast* field to be broadcasted. It is enabled by default.

Step 9. Choose the type of security to authenticate downstream client stations to the WAP device (Access Point Interface) from the Security drop-down list. The possible values are:

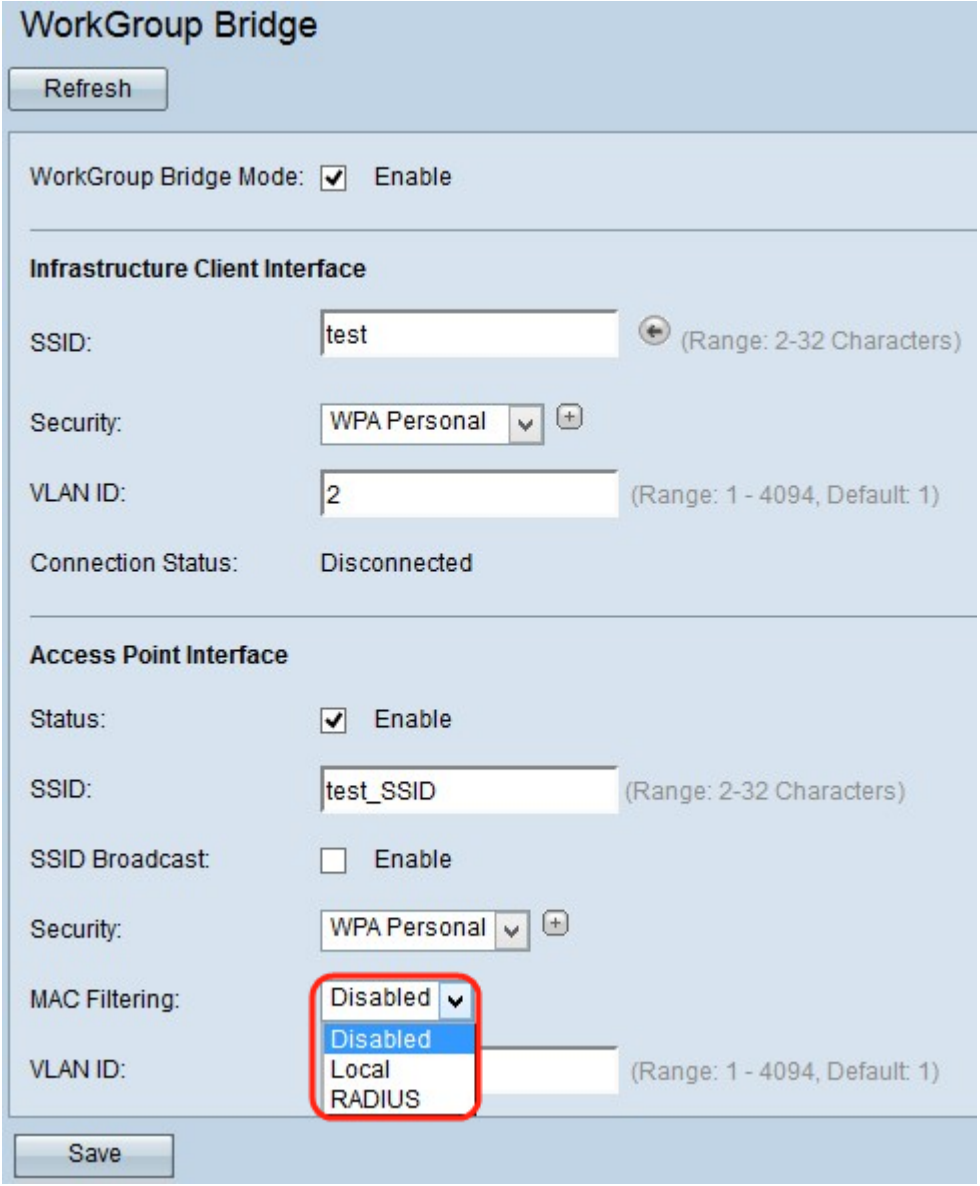


• None — Open or no security. This is the default value. Skip Step 10 if you choose this.

• Static WEP — Static WEP is the minimal security and can support up to 4 keys of length 64 to128 bits. For configuration for static WEP, go to Static WEP

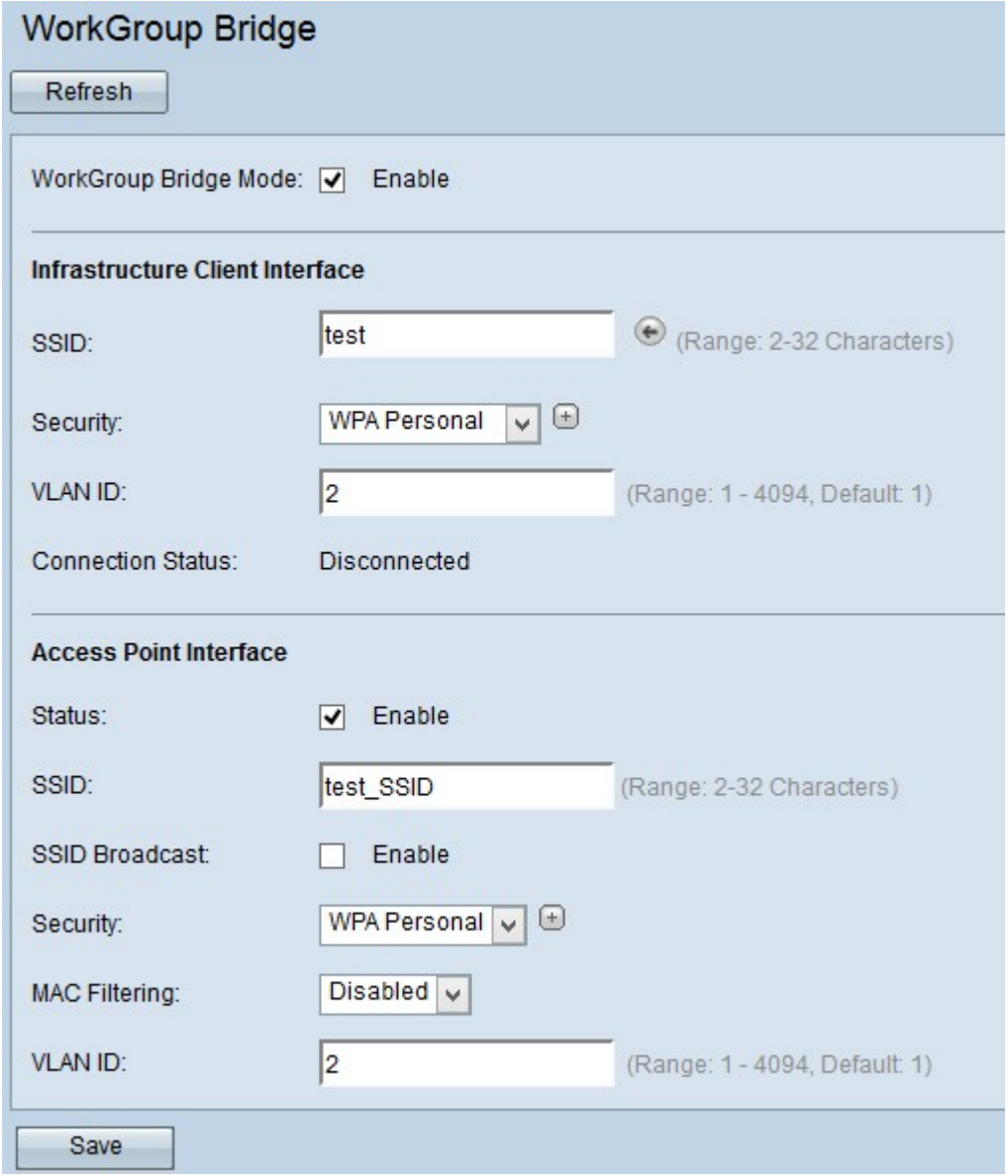
• WPA Personal — WPA Personal is more advanced compared to WEP and can support keys of length 8 to 63 characters. The encryption method is either Temporal Key Integrity Protocol (TKIP) or Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP). WPA2 with CCMP is recommended as it has a more powerful encryption standard, Advanced Encryption Standard (AES) compared to the TKIP that uses only a 64-bit RC4 standard. For configuration of WPA personal, go to WPA Personal for Access Point Interface.

Step 10. Choose the type of MAC filtering you wish to configure for the access point interface from the *MAC Filtering* drop-down list. When enabled, users are granted or denied access to the WAP based on the MAC address of the client they use. The possible values are:



- Disabled — All clients can access the upstream network. This is the default value.
- Local — The set of clients that can access the upstream network is restricted to the clients specified in a locally defined MAC address list.
- Radius — The set of clients that can access the upstream network is restricted to the clients specified in a MAC address list on a RADIUS server.

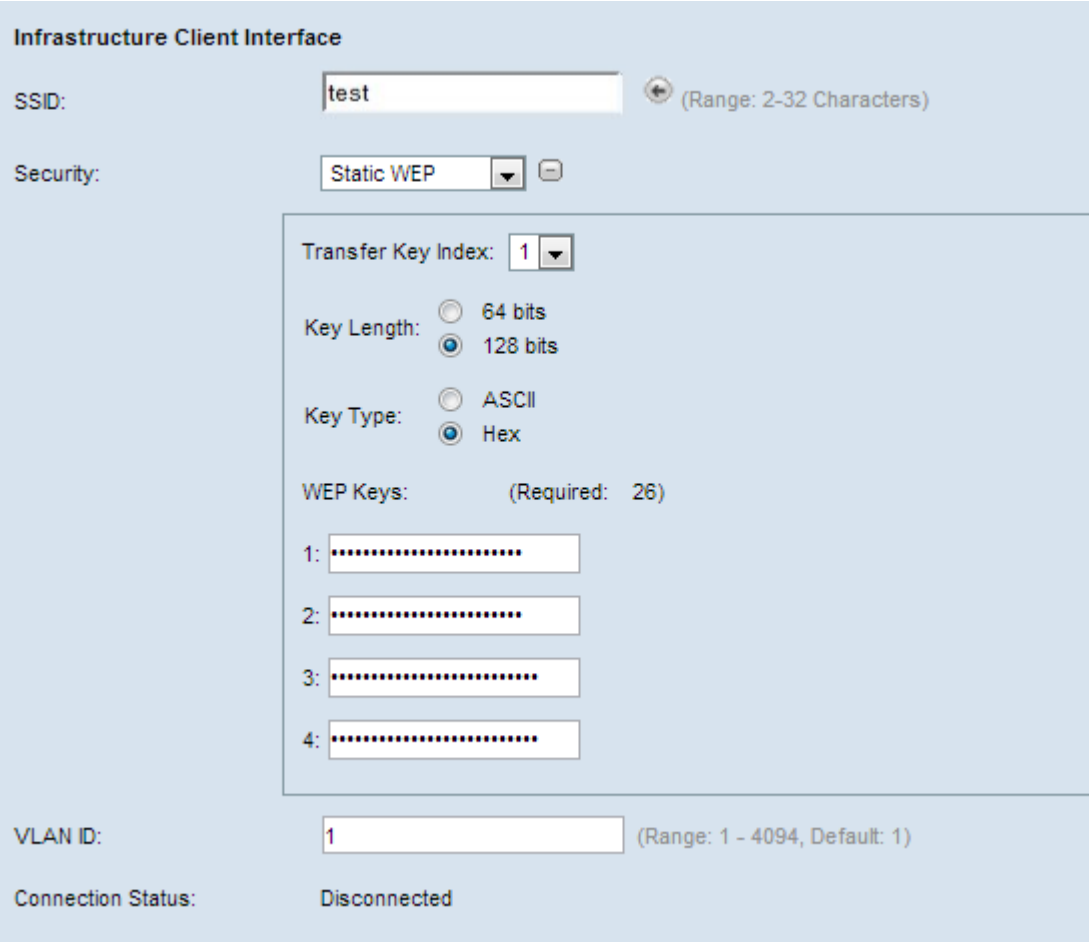
Step 11. Enter the VLAN ID in the VLAN ID field for the access point client interface.



Note: To allow the bridging of packets, the VLAN configuration for the access point interface and wired interface should match that of the infrastructure client interface.

Step 12. Click **Save** to save the settings.

Static WEP



Step 1. When you choose Static WEP some additional fields appear. From the drop-down list in the *Transfer Key Index* field, choose a key index. Available values are 1,2,3, and 4. The default value is 1. The key index is different for different WLAN. The devices connected to a pirticular WLAN must have the same key index. This key is used to encrypt data for communication.

Step 2. In the *Key Length* field, choose either the **64 bits** radio button or **128 bits** radio button. This specifies the length of the key used.

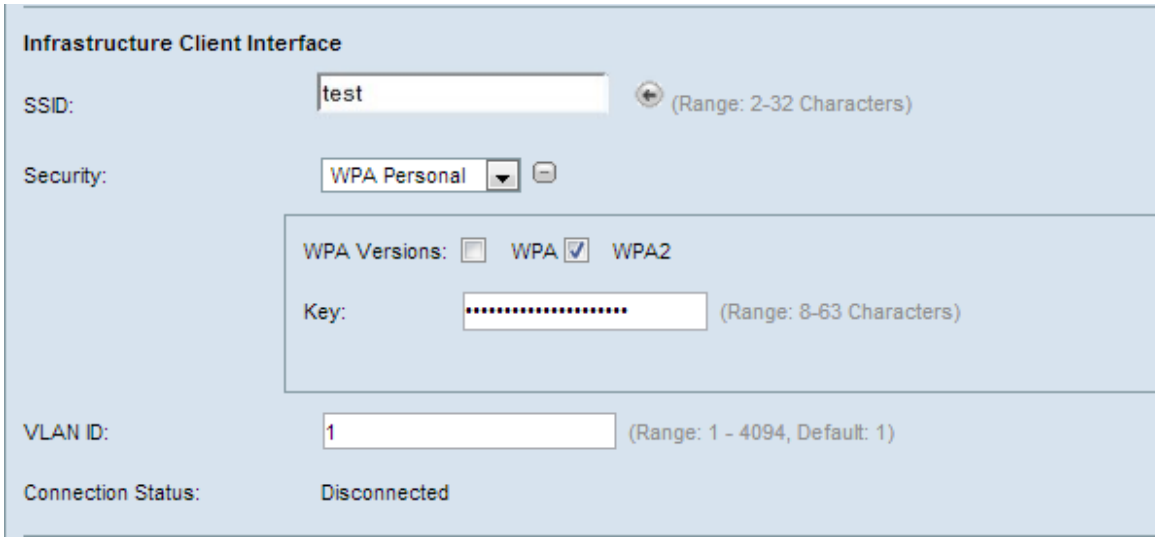
Step 3. Click the desired radio button in the *Key Type* field. WEP keys are usually in hex.

- ASCII — ASCII (American Standard Code for Information Interchange) is a character encoding scheme based on the English alphabet encoded into 128 specified characters.

- HEX — HEX (Hexadecimal) is a positional numeral system with base 16. It uses 16 distinct symbols 0-9 for 0 to 9 numbers and A,B,C,D,E,F to represent values from ten to fifteen. Each hexadecimal represents four binary digits.

Step 4. Enter up to four WEP keys in the next four fields marked as 1,2,3, and 4 under the *WEP Key* field. This is a string entered as the key. The length of the key varies on the length and type of the key. The required length is indicated beside the WEP Key field. The WEP Key strings must match in all the WAP nodes (AP and Clients) and must be places in the same field. This means if string 1 is key 1 in one device, string 1 must also be key 1 in the other devices in the work group bridge.

WPA Personal for Client Interface

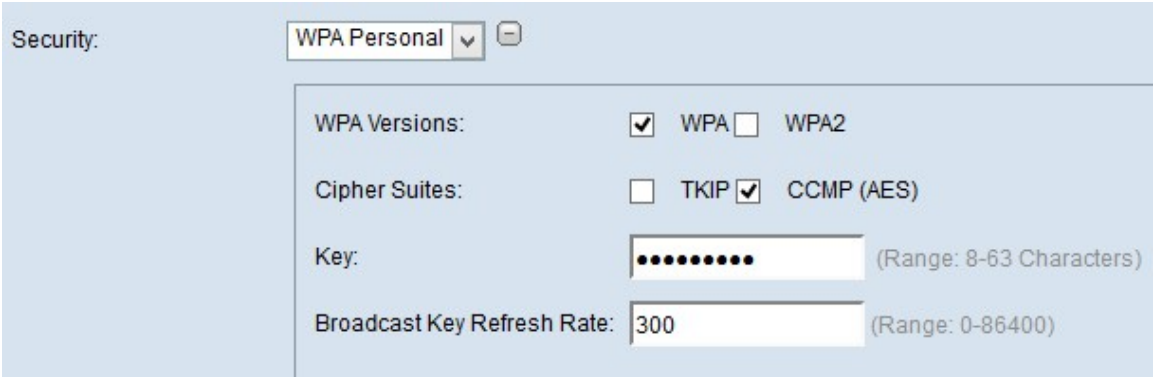


Step 1.Check the desired WPA versions from the *WPA Versions* field. Usually, WPA is chosen only if some of the WAPs in the bridge system do not support WPA2. WPA2 is the more advanced and recommended one.

- WPA — If the network has client stations that support the original version of WPA.
- WPA2 — If all client stations on the network support WPA2. This protocol version provides the best security per the IEEE 802.11i standard.

Step 2. Enter the shared WPA key in the *Key* field. The key may include alphanumeric characters, upper and lower case characters, and special characters.

WPA Personal for Access Point Interface



Step 1. Check the desired WPA versions from the *WPA Versions* field. Usually, WPA is chosen only if some of the WAPs involved do not support WPA2; otherwise, WPA2 is recommended.

- WPA — If the network has client stations that support the original version WPA.
- WPA2 — If all client stations on the network support WPA2. This protocol version provides the best security per the IEEE 802.11i standard.

Note: If the network is a mix of clients of WPA and WPA2, check both of the check boxes. This lets both WPA and WPA2 client stations associate and authenticate, but uses the more robust WPA2 for clients who support it.

Step 2. Choose the desired cipher suites from the *Cipher Suites* field.

• TKIP — Temporal Key Integrity Protocol (TKIP) uses only a 64-bit RC4 standard.

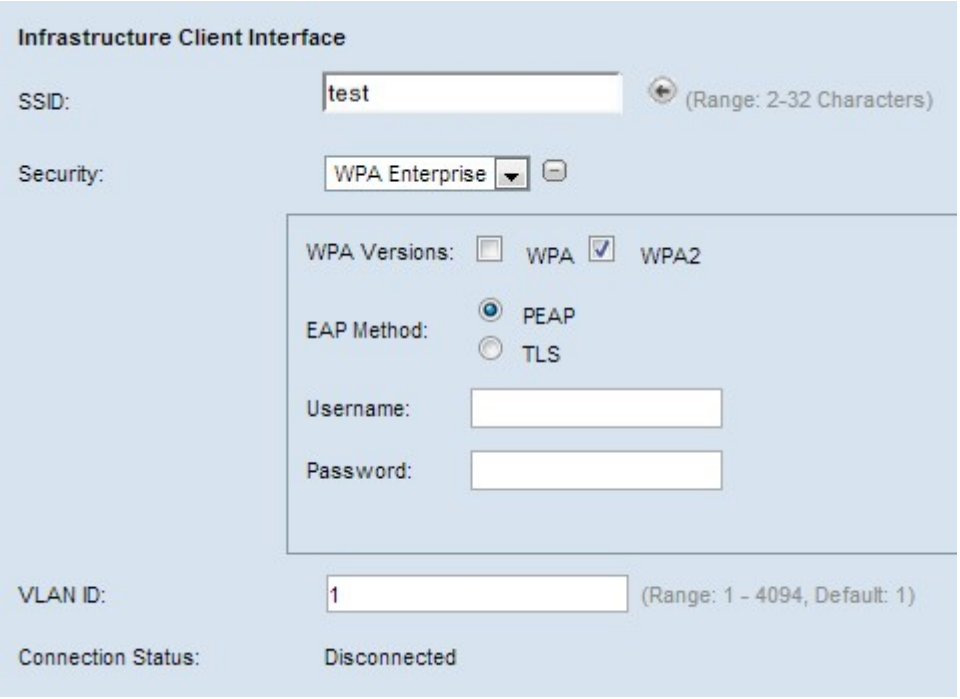
• CCMP (AES)— Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) is the security protocol used by AES (Advanced Encryption Standard). WPA2 with CCMP is recommended as it has a more powerful encryption standard.

Note: You can choose either or both. Both TKIP and AES clients can associate with the WAP device.

Step 3. Enter the shared WPA key in the *Key* field. The key may include alphanumeric characters, upper and lower case characters, and special characters.

Step 4. Enter the rate in the *Broadcast Key Refresh Rate* field.

WPA Enterprise



Step 1.Check the desired WPA versions in the *WPA Versions* field. Usually WPA is chosen only if some of the WAPs in the bridge system do not support WPA2. WPA2 is the more advanced and recommended one.

• WPA — If the network has client stations that support the original version WPA.

• WPA2 — If all client stations on the network support WPA2. This protocol version provides the best security per the IEEE 802.11i standard.

Note: If the network is a mix of clients of WPA and WPA2, then check the both of the check boxes. This lets both WPA and WPA2 client stations associate and authenticate, but uses the more robust WPA2 for clients who support it.

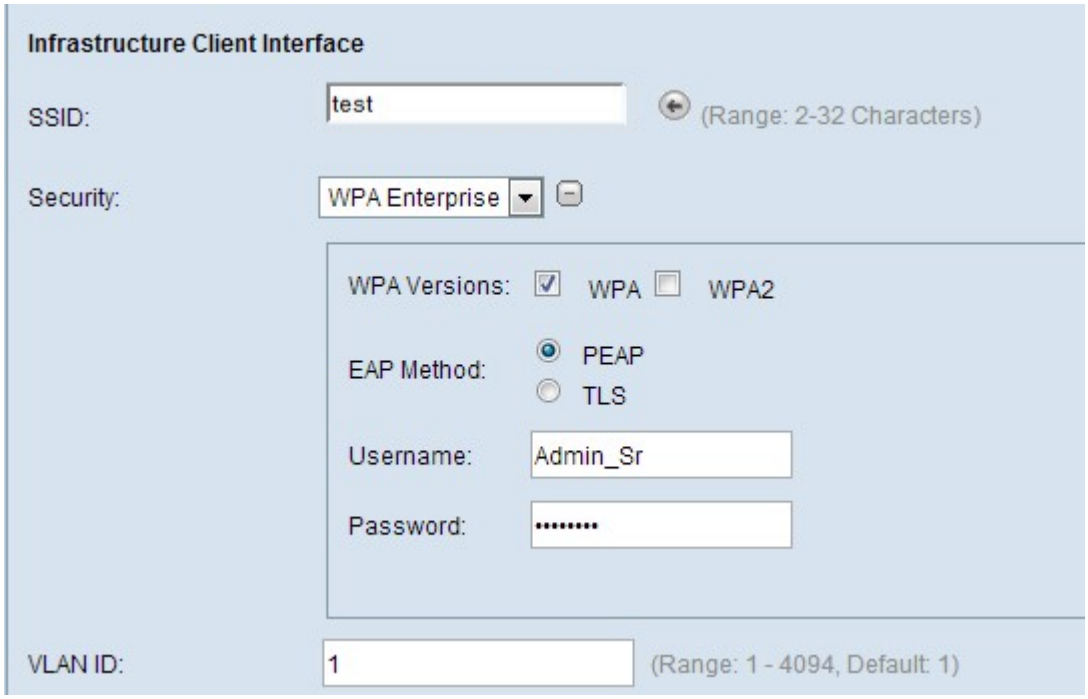
Step 2. Click the appropriate radio button to choose between the two EAP Methods.

• PEAP — Protected EAP. It relies on TLS but avoids the installation of digital certificates on every client. Instead, it provides authentication through a username and password. If you choose this, go to PEAP (Protected Extensible Authentication Protocol).

• TLS — Authentication through exchange of digital certificates. If you choose this, go to

TLS (Transport Layer Security).

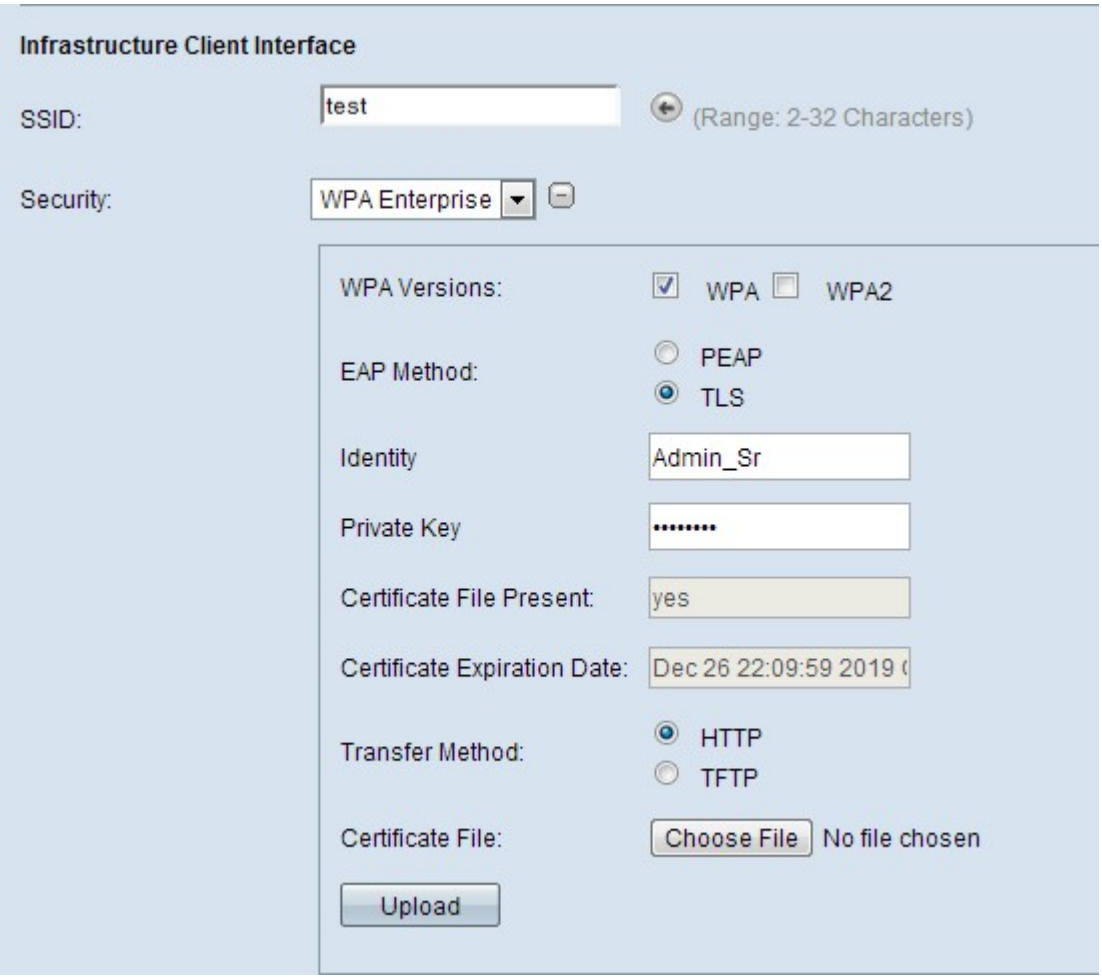
PEAP (Protected Extensible Authentication Protocol)



Step 1. Enter a username in the *Username* field.

Step 2. Enter a password in the *Password* field.

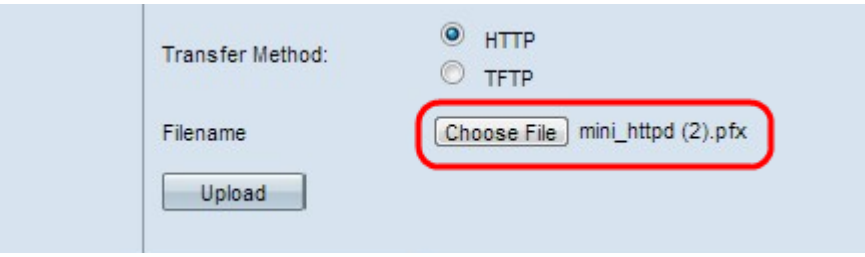
TLS (Transport Layer Security)



Step 1. Choose the transfer mode to download a Certificate File for TLS authentication.

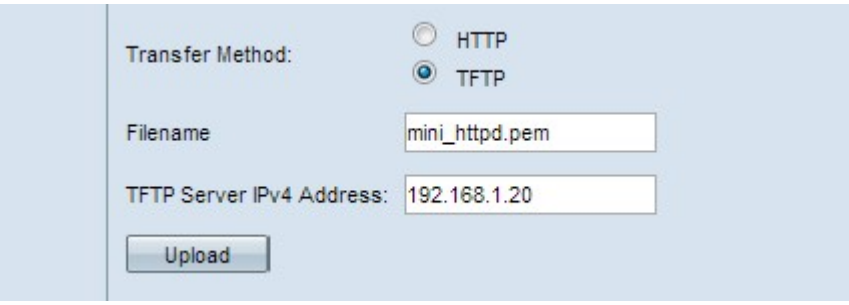
- HTTP — If you want download the certificate from a web server of PC. If you choose this, go to HTTP.
- TFTP — If you want download the certificate from a file server. If you choose this, go to TFTP.

HTTP



Step 1. Click **Choose file** to select a certificate file. It has to be a certificate type file with extension .pem, .pfx etc. Otherwise, file upload will be unsuccessful.

TFTP



Step 1. Enter the name of the certificate file in the *Filename* field.

Step 2. Enter the IP address of the TFTP server.

Note: The Certificate File Transfer field shows whether there is a certificate present in the WAP, and the Certificate Expiration Date field shows the expiration date of the present certificate.

Step 3. Click **Upload** to upload file to the device.