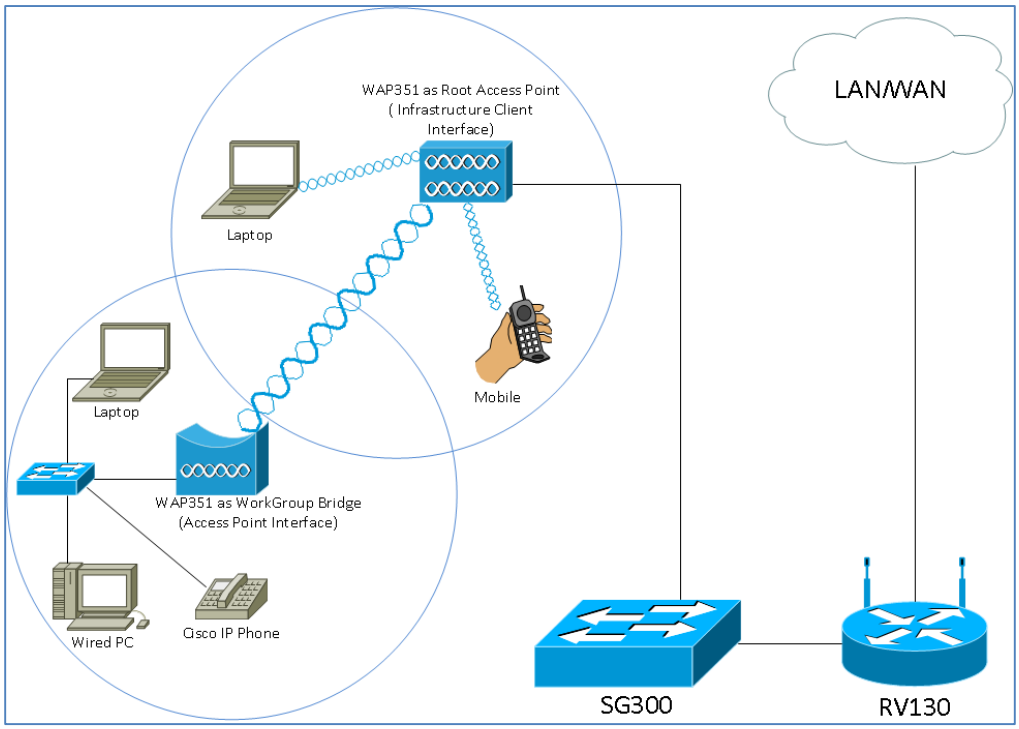
Article ID: 5047

Configure Workgroup Bridge on the WAP351

Objective

The Workgroup Bridge feature enables the Wireless Access Point (WAP) to bridge traffic between a remote client and the wireless LAN that is connected with the workgroup bridge mode. The WAP device associated with the remote interface is known as an access point interface, while the WAP device associated with the wireless LAN is known as an infrastructure interface. The Workgroup Bridge lets devices that only have wired connections connect to a wireless network. Although the Wireless Distribution System (WDS) is the preferred bridge solution for the WAP351, the Workgroup Bridge Mode is recommended when the WDS feature is unavailable. To see how WDS Bridge is configured, refer to the *article [Configuring Wireless Distribution System (WDS) Bridge on the WAP131 and WAP351 Access Point](#)*.



Note: The topology above illustrates a sample workgroup bridge model. Wired devices are tethered to a switch, which connects to the LAN interface of the WAP. The WAP, acting as an access point interface, connects to the infrastructure interface.

The objective of this document is to explain how to configure the Workgroup Bridge between two wireless access points. You will be configuring your WAP351 as an access point interface connecting to an existing infrastructure interface.

Applicable Devices

- WAP351

Software Version

- 1.0.0.39

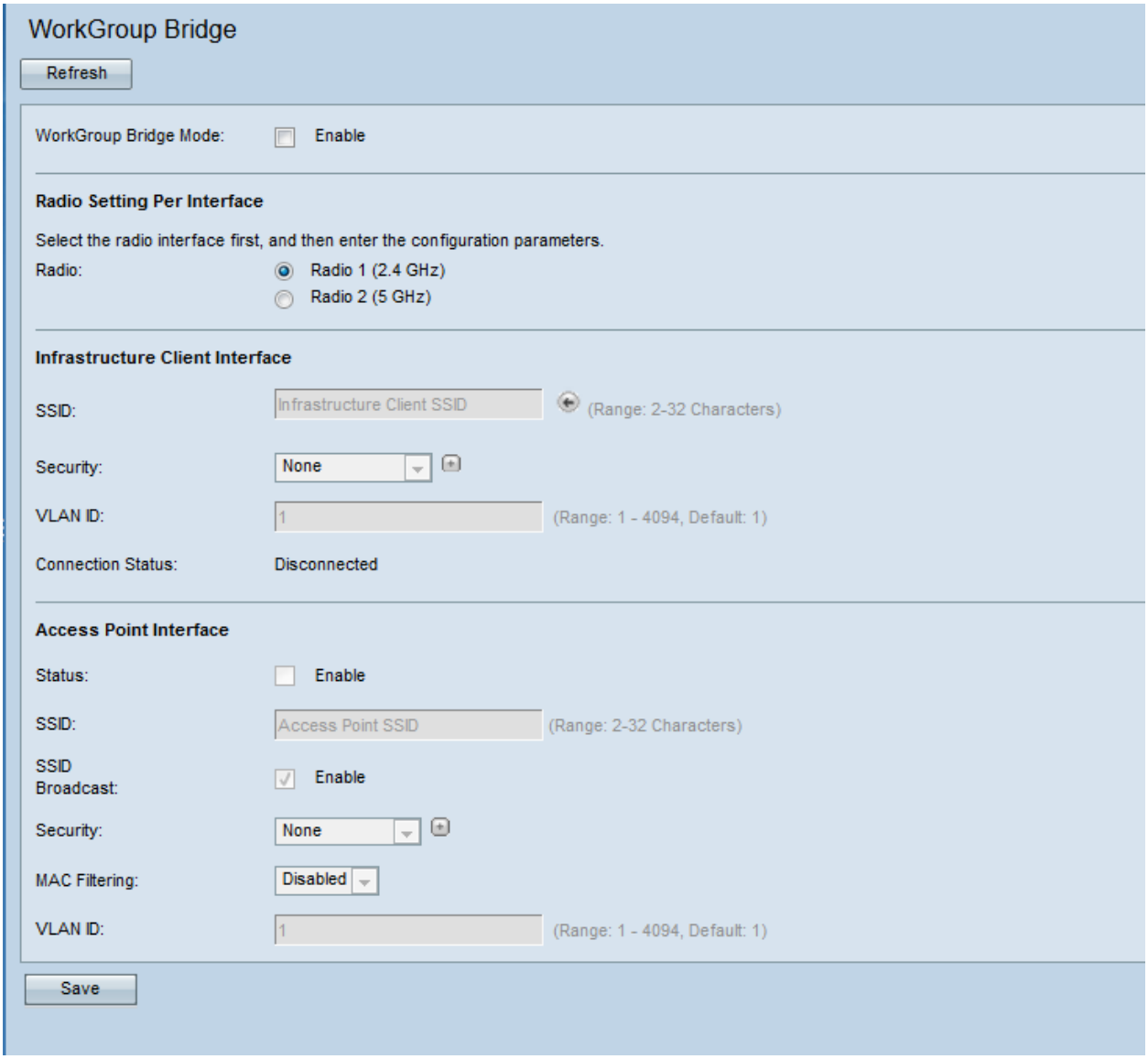
Configure Work Group Bridge

Note: In order to enable Workgroup Bridge, clustering must be disabled in the WAP. All WAP devices that take part in the Workgroup Bridge must have the following identical settings:

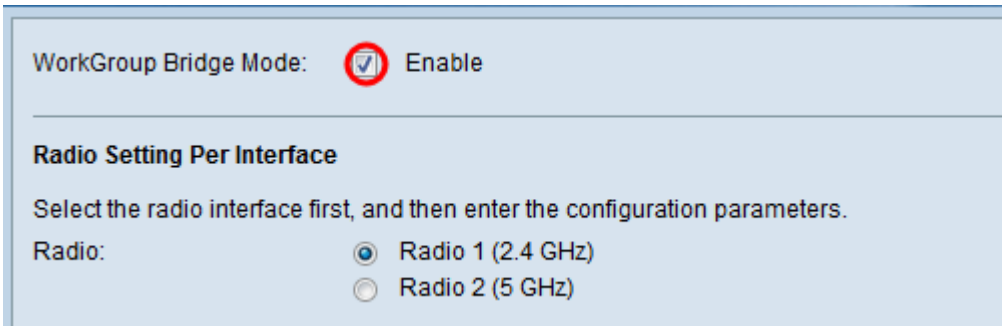
- Radio
- IEEE 802.11 mode
- Channel Bandwidth
- Channel (auto not recommended)

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 Radio Settings on the WAP131 and WAP351 Access Points.*

Step 1. Log in to the Web Configuration Utility of the WAP that you want to configure as an access point interface and choose **Wireless > WorkGroup Bridge**. The *WorkGroup Bridge* page opens:

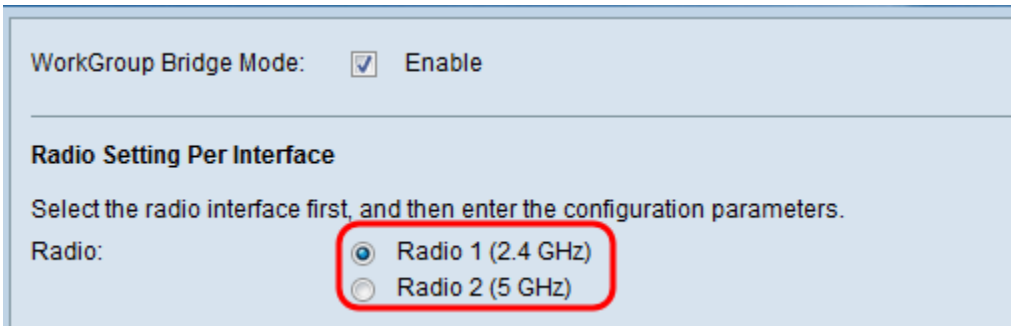


Step 2. Check the **Enable** checkbox in the *WorkGroup Bridge Mode* field to enable the workgroup bridge feature.



Radio Settings Per Interface

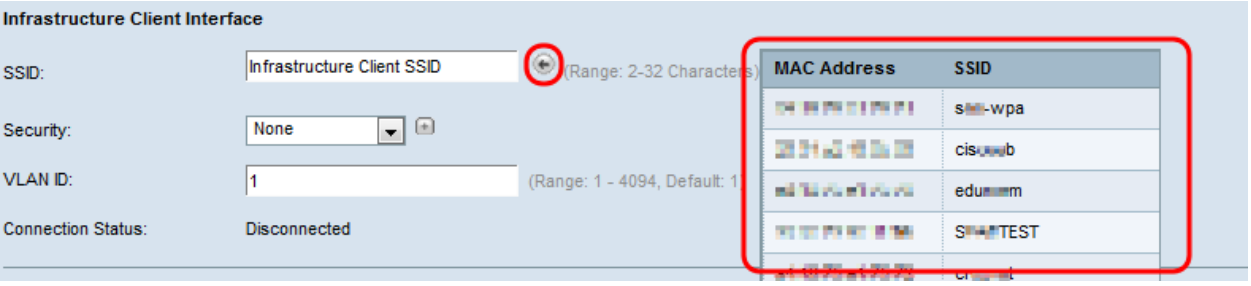
Step 1. Select the radio interface for the work group bridge. When you configure one radio as a workgroup bridge, the other radio remains operational. The radio interfaces correspond to the radio frequency bands of the WAP351. The WAP351 is equipped to broadcast on two different radio interfaces. Configuring settings for one radio interface will not affect the other.



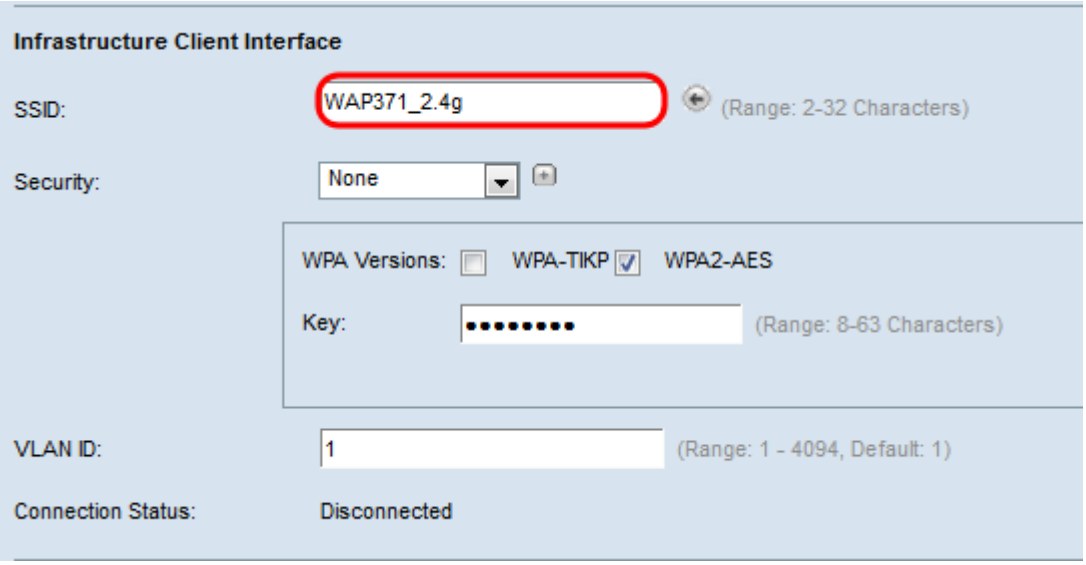
Infrastructure Client Interface

Step 1. Enter the Service Set Identifier (SSID) name in the *SSID* field. The SSID must be 2-32 characters long.

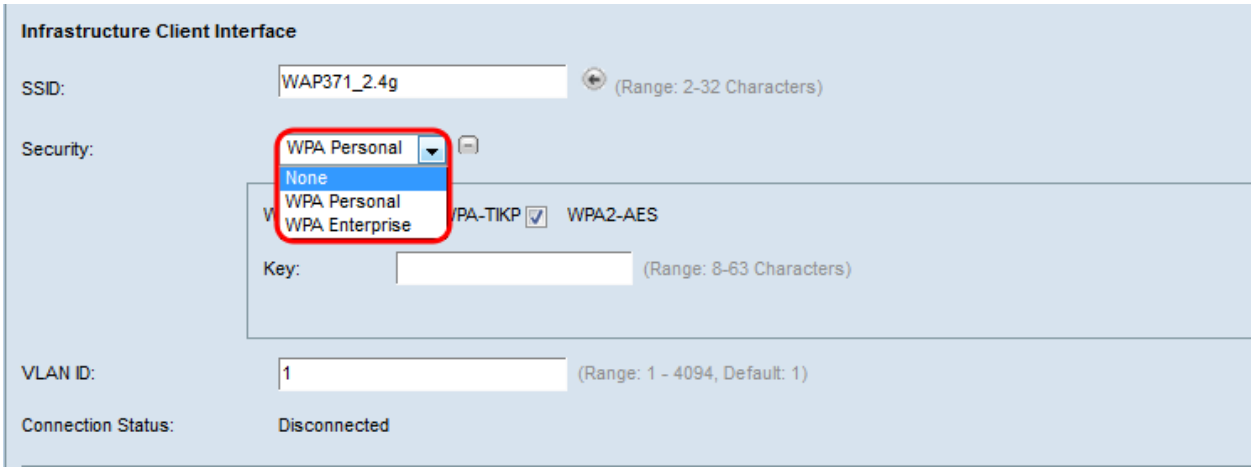
Step 2. (Optional) To select a specific Infrastructure Client Interface, click on the arrow next to the *SSID* field and select the desired interface. Rogue AP detection must be enabled if you want to scan for neighboring access points. For more information, refer to the article *Rogue AP Detection on the WAP351 Access Points* to enable Rogue AP detection.



The *SSID* field will automatically update to the desired interface.



Step 3. Choose the type of security to authenticate a client station on the upstream WAP device from the *Security* drop-down list.



The available options are defined as follows:

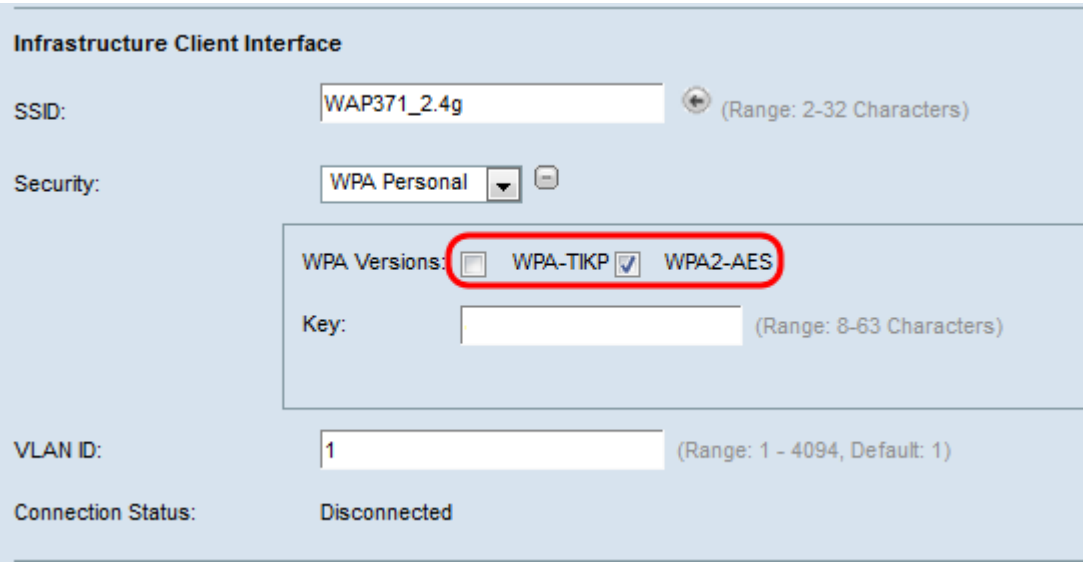
- None — Open or no security. This is the default value. If you choose this, skip to Step 16 of this section.

- WPA Personal — WPA Personal can support keys of length 8-63 characters. WPA2 is recommended as it has a more powerful encryption standard. For more information about WPA2 encryption methods, refer to Step 4 of the *WPA Personal* subsection. If you choose this option, go to Step 4.

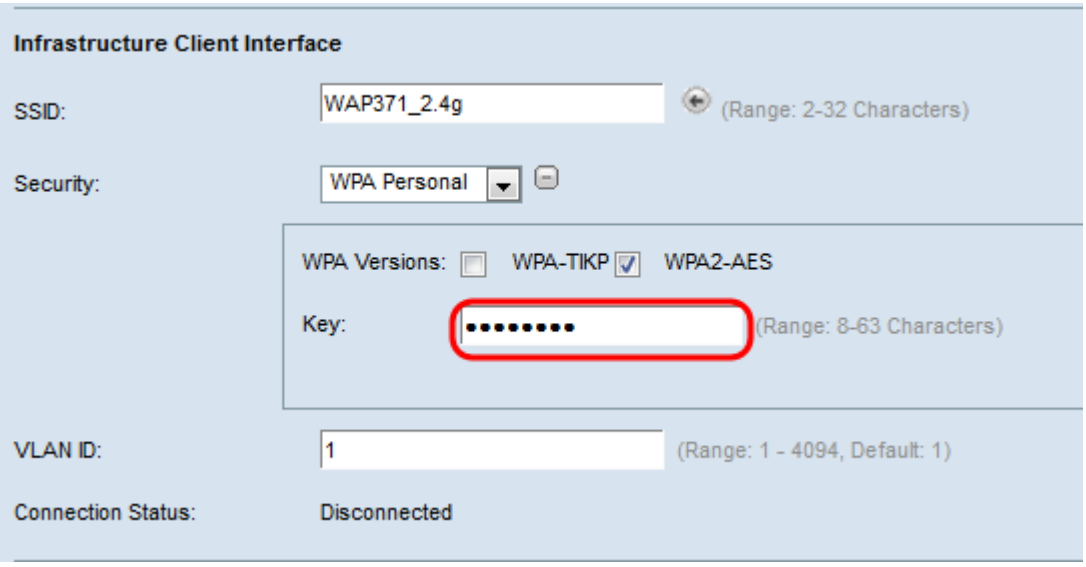
- WPA Enterprise — WPA Enterprise is more advanced than WPA Personal and is the recommended security for authentication. It uses Protected Extensible Authentication Protocol (PEAP) and Transport Layer Security (TLS). If you choose this, skip to Step 6.

WPA Personal

Step 4. Select the **WPA-TKIP** or **WPA2-AES,** checkbox to determine which kind of WPA encryption the infrastructure client interface will use. If all of your wireless equipment support WPA2, then set the infrastructure client security for WPA2-AES. . 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. If some of your wireless devices, like personal digital assistants, and other small wireless network devices, only connect with WPA-TKIP, then select WPA-TKIP.

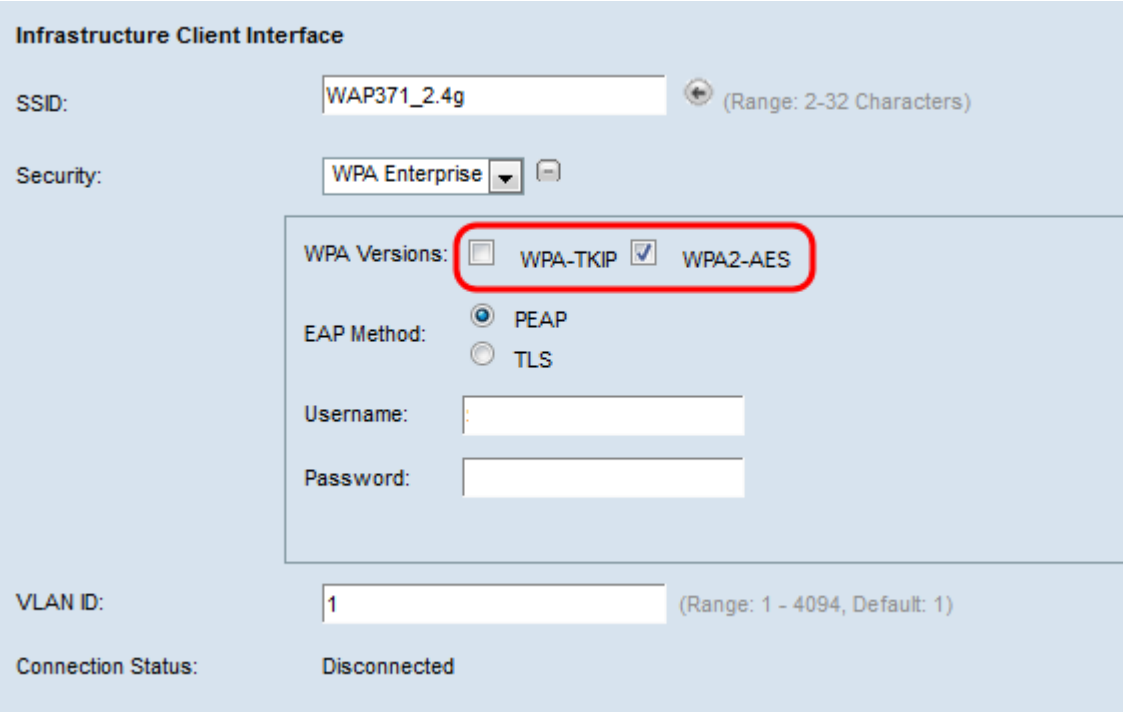


Step 5. Enter in the WPA encryption key in the *Key* field. The key must be 8-63 characters long. Skip to Step 16.

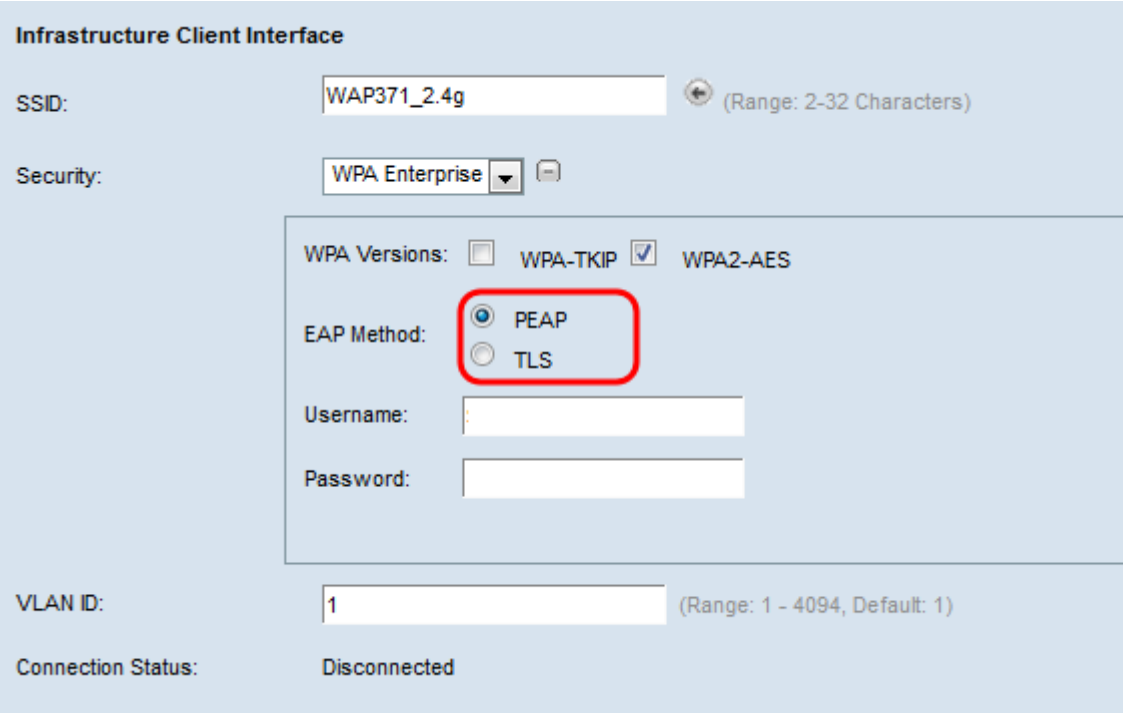


WPA Enterprise

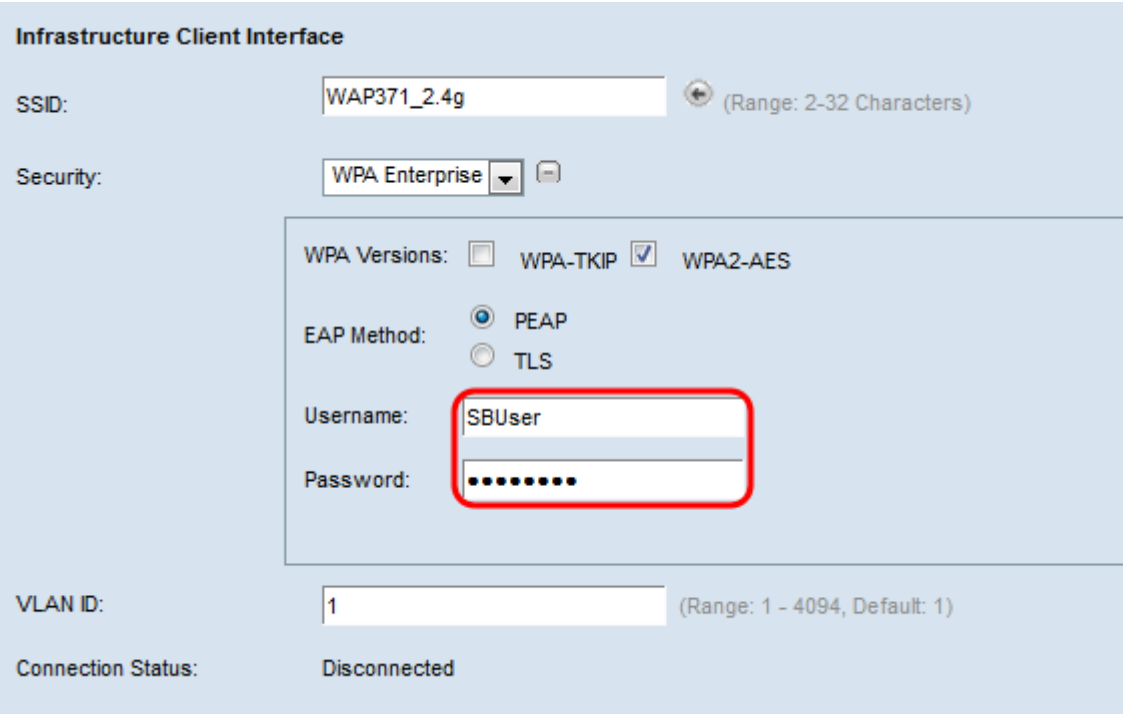
Step 6. Select the WPA-TKIP or WPA2-AES checkbox to determine which kind of WPA encryption the infrastructure client interface will use. WPA2 is a newer security system that represents the best long term, scalable solution to wireless LAN security. WPA2 was designed from the ground up, completely avoiding the security flaws of WEP and WPA. This is the new 802.11i standard, also known as WPA2 by the WiFi Alliance. If all of your wireless equipment supports WPA2, then set the infrastructure client security for WPA2-AES. If some of your wireless devices can only connect with WPA-TKIP, then check both the WPA-TKIP and WPA2-AES checkboxes. If both checkboxes are checked, your WPA2 devices will connect to WPA2, and your WPA devices will connect to WPA.



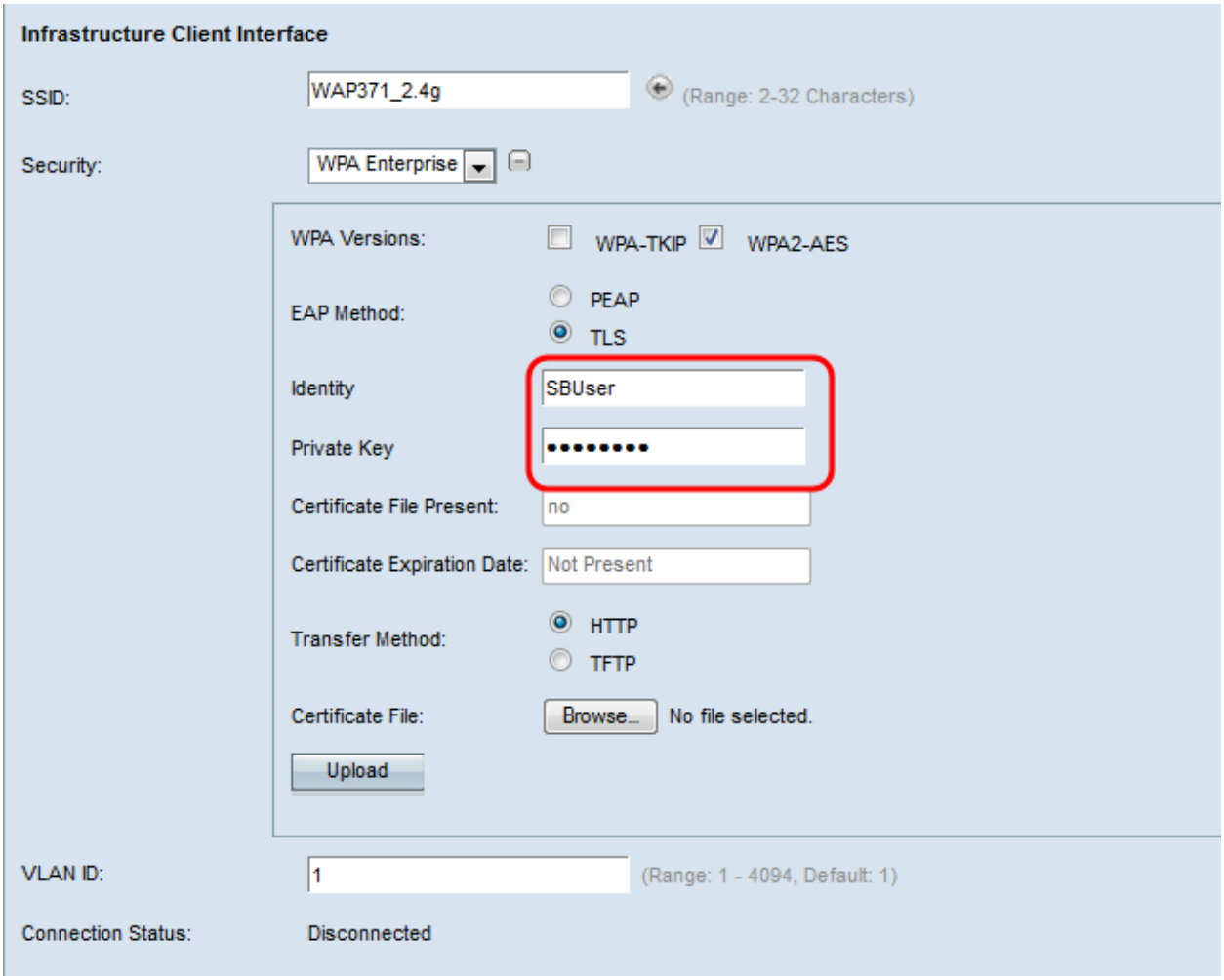
Step 7. In the *EAP Method* field, select either the **PEAP** or **TLS** radio button. The Protected Extensible Authentication Protocol (PEAP) gives each wireless user under the WAP individual usernames and passwords that support AES encryption standards. Since PEAP is a password based security method, your wifi security is based on your client's machine credentials. PEAP can potentially be a serious security risk if you have weak passwords or unsecured clients. Transport Layer Security (TLS) requires each user to have an additional certificate to be granted access. TLS is more secure if you have the additional servers and necessary infrastructure to authenticate users into your network. If you select TLS, skip to Step 9.



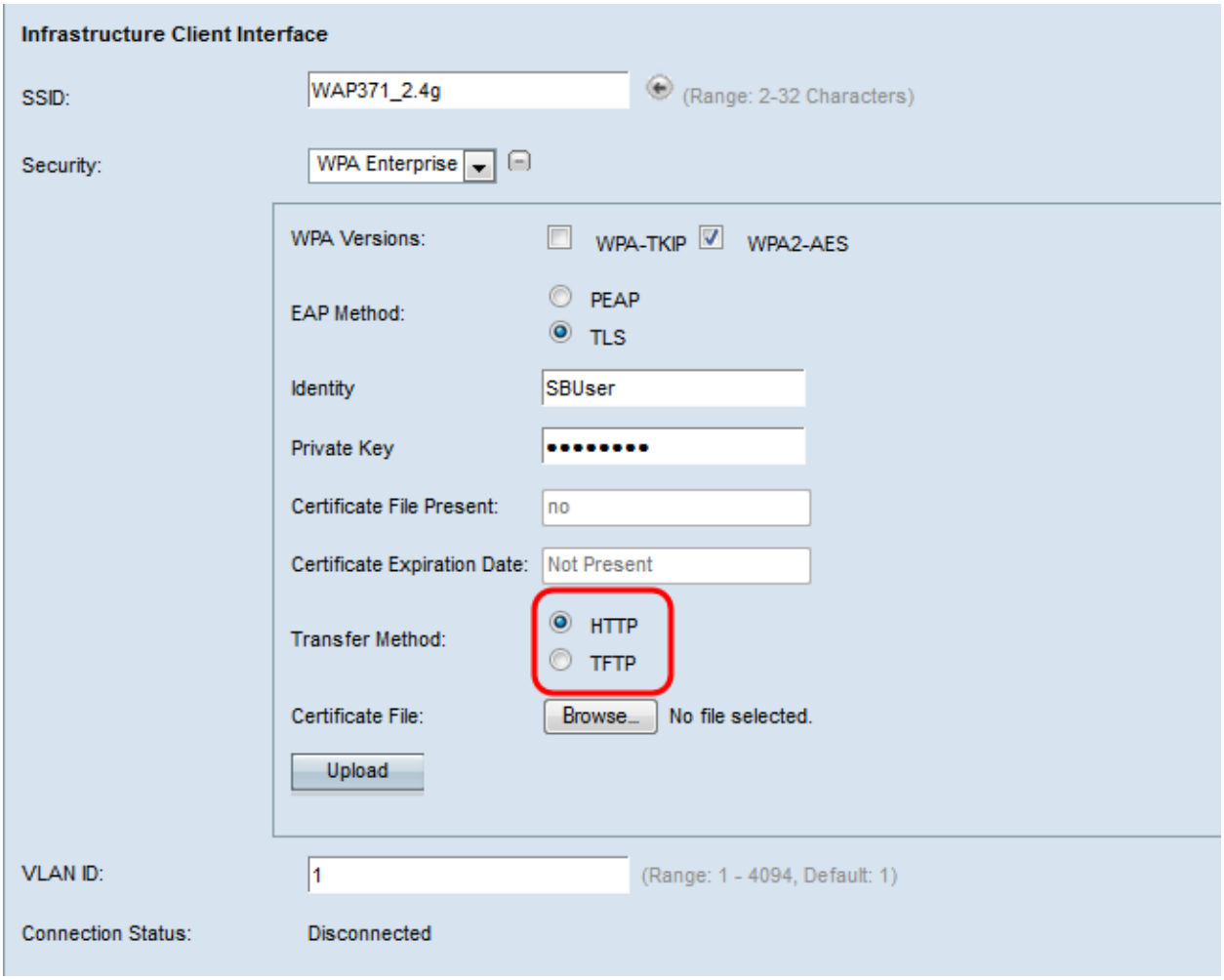
Step 8. Enter the username and password for the infrastructure client in the *Username* and *Password* field. This is the login information that is used to connect to the infrastructure client interface; refer to your infrastructure client interface to find this information. Skip to Step 16.



Step 9. If you chose **TLS** in Step 7, enter the identity and private key of the infrastructure client in the *Identity* and *Private Key* fields.



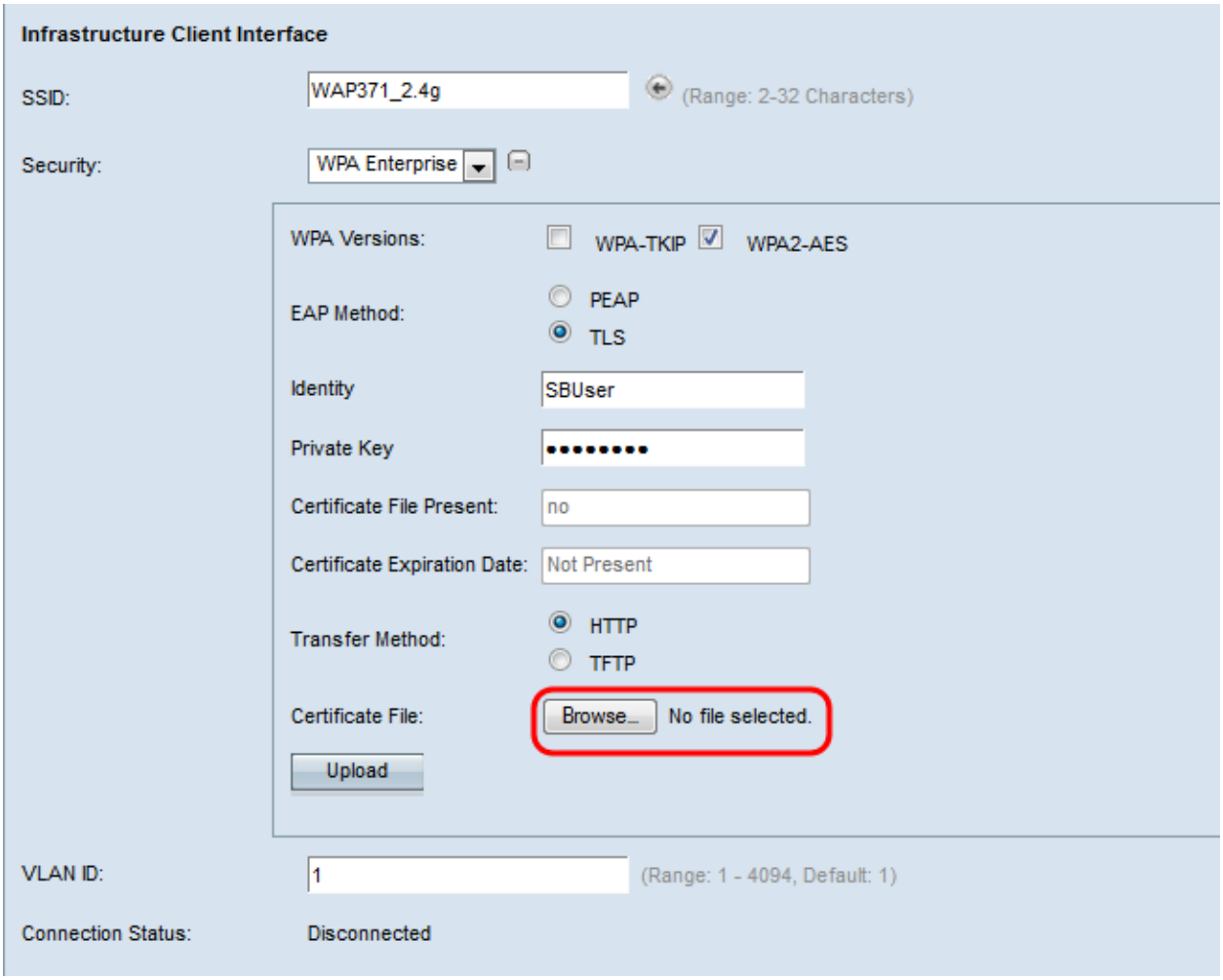
Step 10. Select either the **HTTP** or **TFTP** radio buttons in the *Transfer Method* field. Trivial File Transfer Protocol (TFTP) is a simplified unsecure version of File Transfer Protocol (FTP). It is mainly used to distribute software or authenticate devices among corporate networks. Hypertext Transfer Protocol (HTTP) provides a simple challenge-response authentication framework that can be used by a client to provide authentication framework**.** If you select **TFTP**, skip to Step 13.



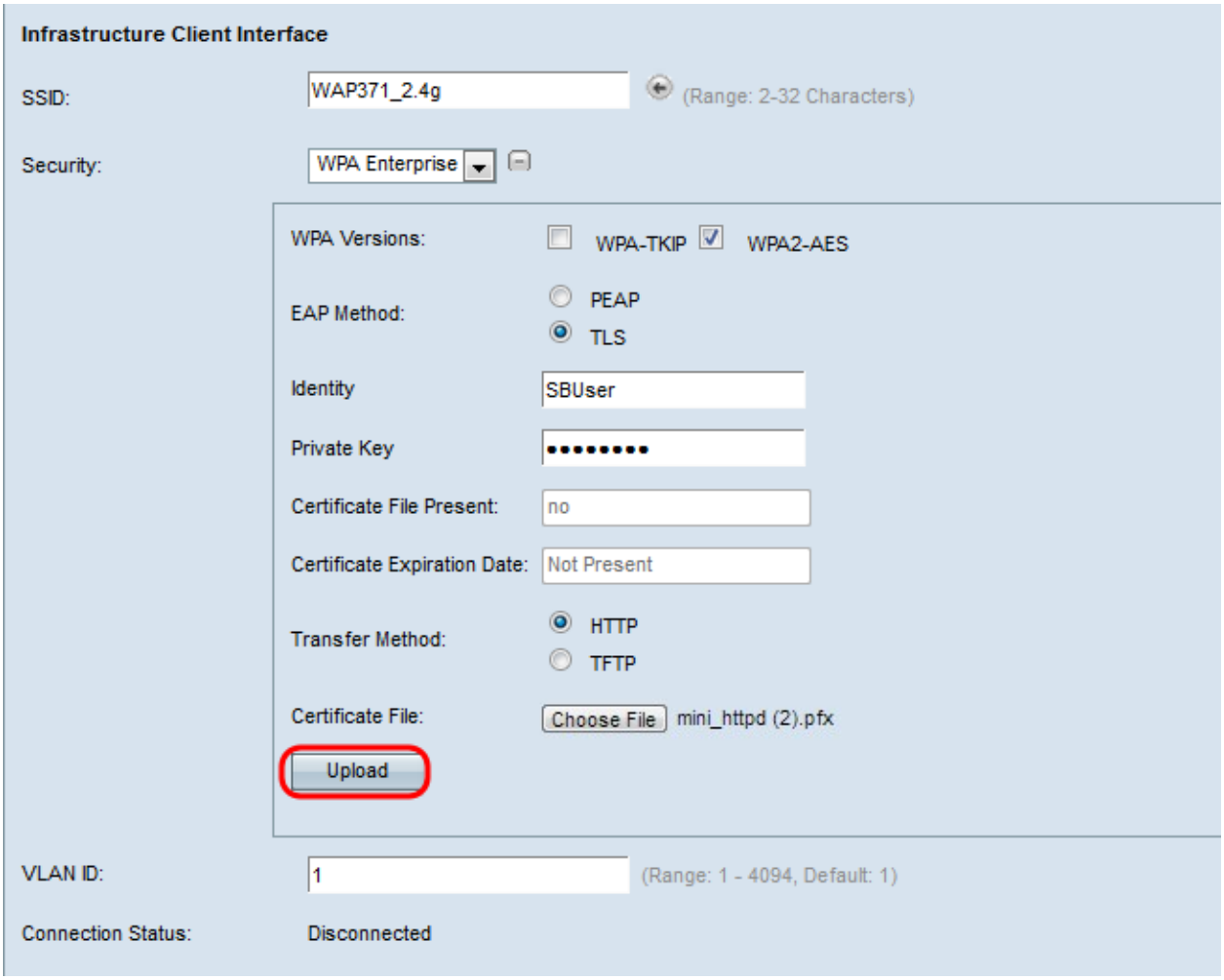
Note: If a certificate file is already present on the WAP, then the *Certificate File Present* and *Certificate Expiration Date* field will already be filled in with the relevant information. Otherwise, they will be blank.

HTTP

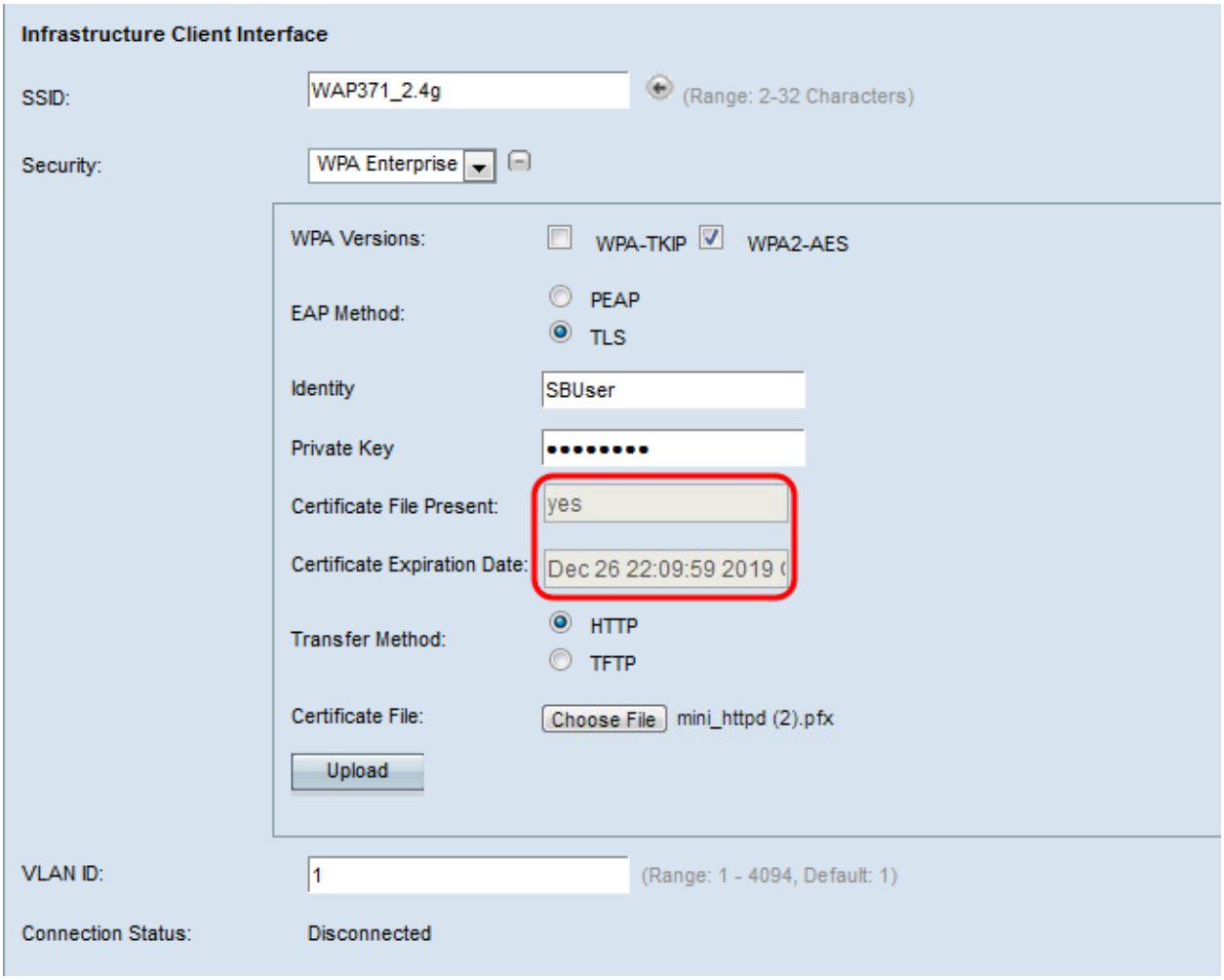
Step 11. Click the **Browse** button to find and select a certificate file. The file must have the proper certificate file extension (such as .pem or .pfx), otherwise the file will not be accepted.



Step 12. Click **Upload** to upload the selected certificate file. Skip to Step 16.



The *Certificate File Present* and *Certificate Expiration Date* field will be updated automatically.



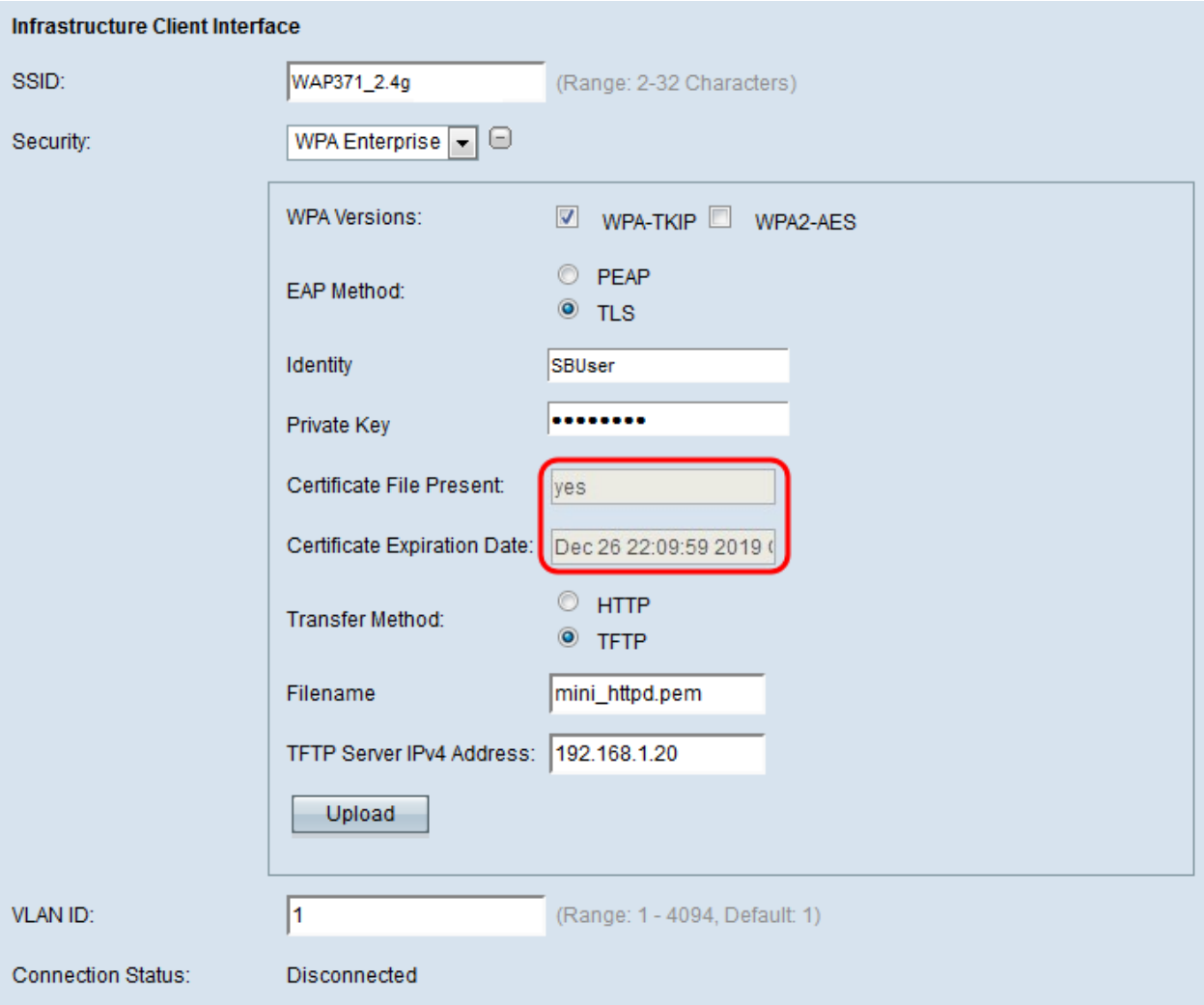
TFTP

Step 13. If you selected **TFTP** in Step 10, enter the filename of the certificate file in the *Filename* field.

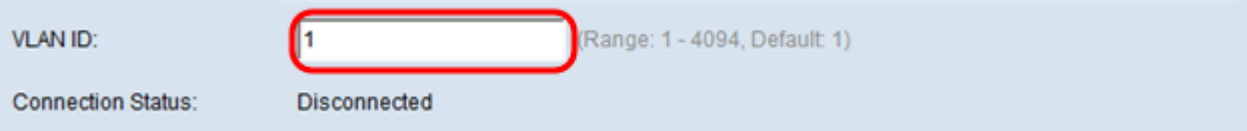
Step 14. Enter the TFTP Server address in the *TFTP Server IPv4 Address* field.

Step 15. Click the **Upload** button to upload the specified certificate file.

The *Certificate File Present* and *Certificate Expiration Date* field will be updated automatically.



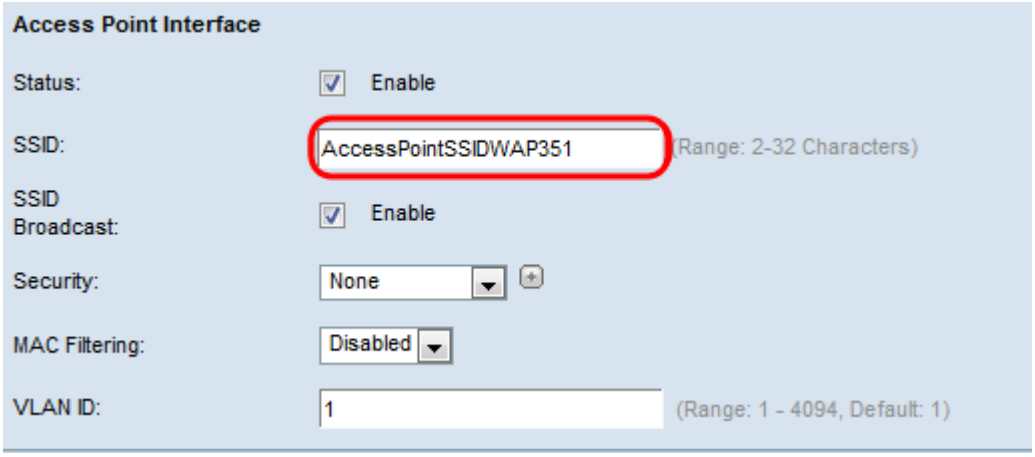
Step 16. Enter the VLAN ID for the infrastructure client interface.



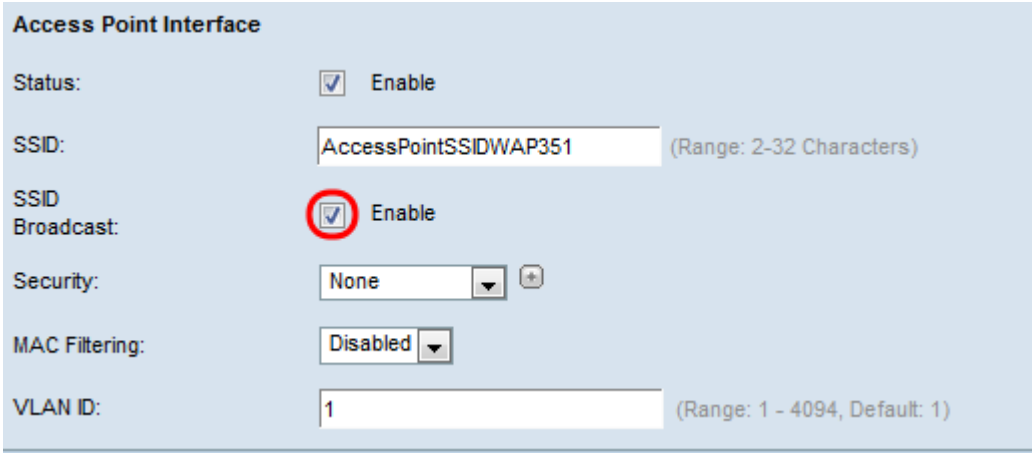
Access Point Interface

Step 1. Check the **Enable** checkbox in the *Status* field to enable bridging on the access point interface.

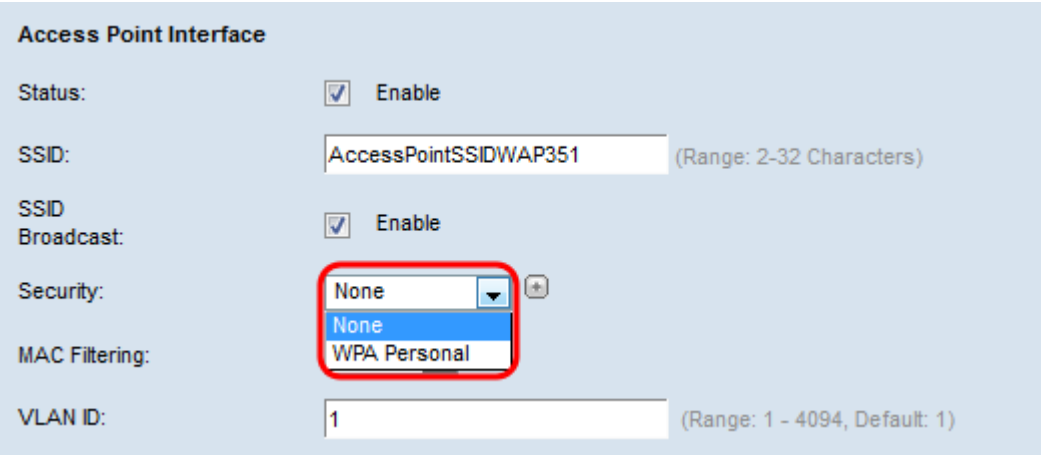
Step 2. Enter the Service Set Identifier (SSID) for the access point in the *SSID* field. The SSID length must be between 2 to 32 characters.



Step 3. (Optional) If you do not want to broadcast the SSID, uncheck the **Enable** checkbox in the *SSID Broadcast* field. Doing so will make the access point invisible to those searching for wireless access points; it can only be connected to by someone who already knows the SSID. It is enabled by default.



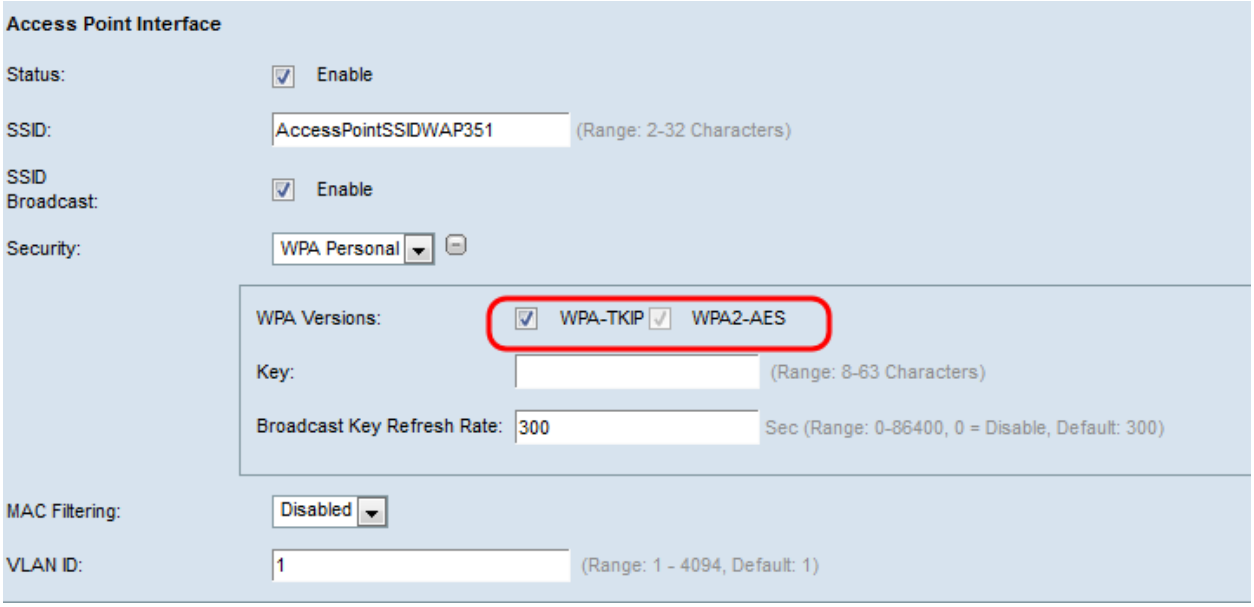
Step 4. Choose the type of security to authenticate downstream client stations to the WAP device from the *Security* drop-down list.



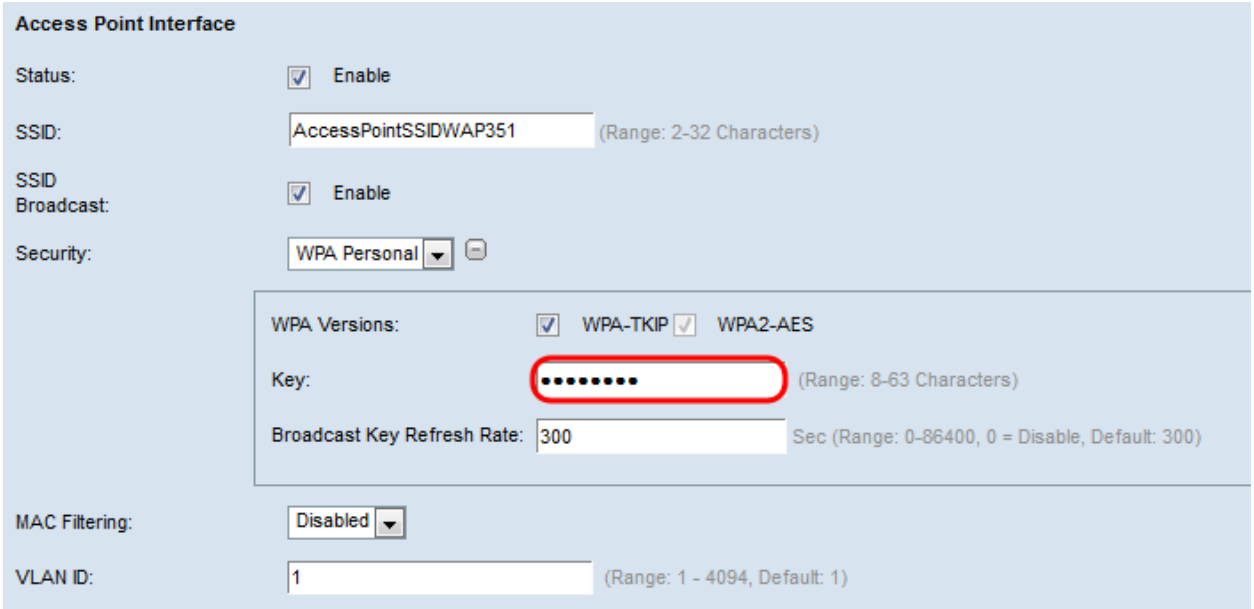
The available options are defined as follows:

- None — Open or no security. This is the default value. Skip to Step 10 if you choose this.
- WPA Personal — WPA Personal 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.

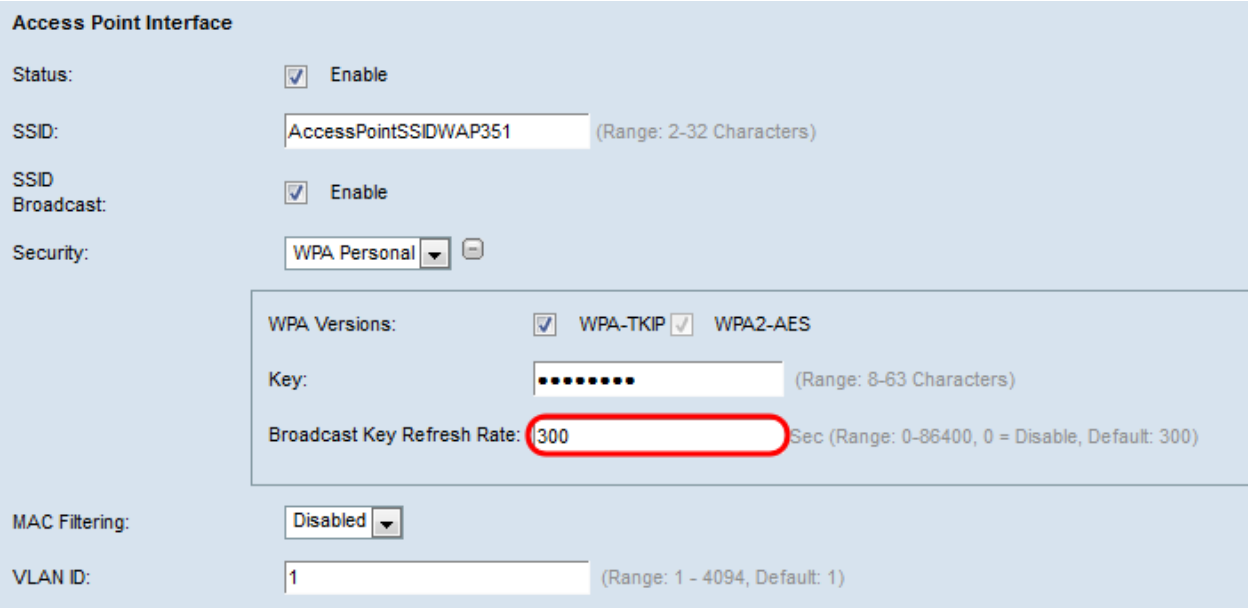
Step 5. Select the **WPA-TKIP** or **WPA2-AES** checkbox in the *WPA Versions* field to determine which kind of WPA encryption the infrastructure client interface will use. WPA2 is a newer security system that represents the best long term, scalable solution to wireless LAN security. WPA2 was designed from the ground up, completely avoiding the security flaws of WEP and WPA. This is the new 802.11i standard, also known as WPA2 by the WiFi Alliance. If all of your wireless equipment supports WPA2, then set the infrastructure client security for WPA2-AES, which is always enabled. If some of your wireless devices can only connect with WPA-TKIP, then check both the WPA-TKIP and WPA2-AES checkboxes. If both checkboxes are checked, your WPA2 devices will connect to WPA2, and your WPA devices will connect to WPA.



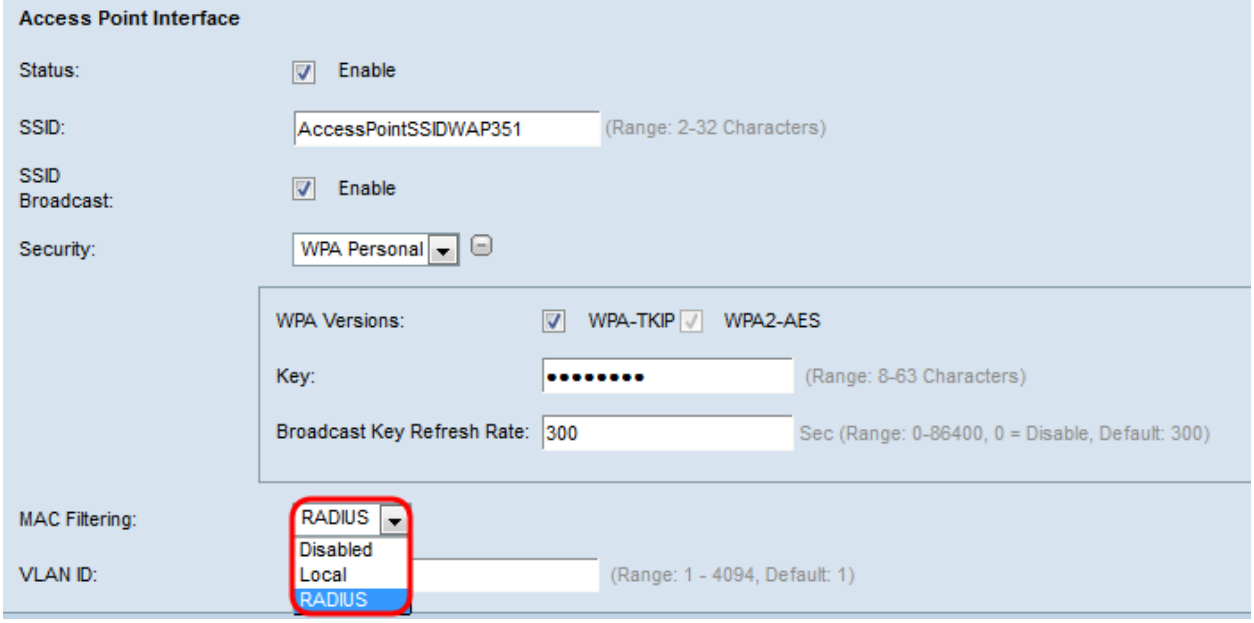
Step 6. Enter the shared WPA key in the *Key* field. The key must be 8-63 characters long, and can include alphanumeric characters, upper and lower case characters, and special characters.



Step 7. Enter the rate in the *Broadcast Key Refresh Rate*. The broadcast key refresh rate specifies the interval at which the security key is refreshed for clients associated to this access point. The rate must be between 0-86400, with a value of 0 disabling the feature. The default is 300.



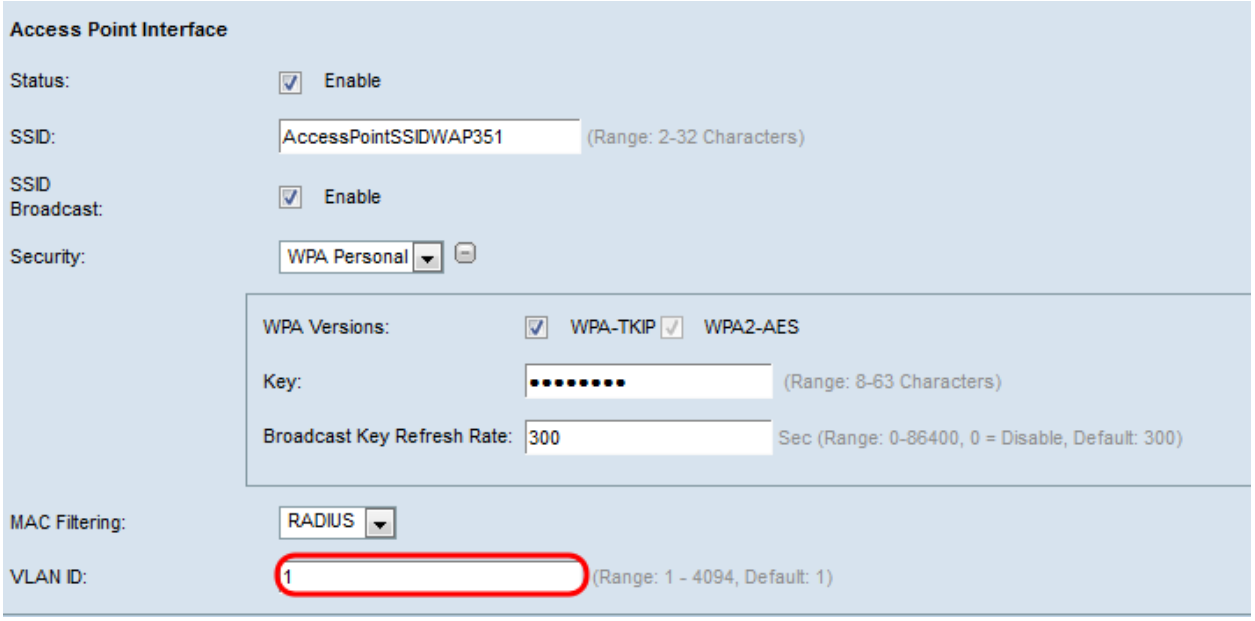
Step 8. Choose the type of MAC filtering you wish to configure for the access point interface from the *MAC Filtering* drop-down list. When enabled, users are granted or denied access to the WAP based on the MAC address of the client they use.



The available options are defined as follows:

- 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 9. 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 10. Click **Save** to save your changes.