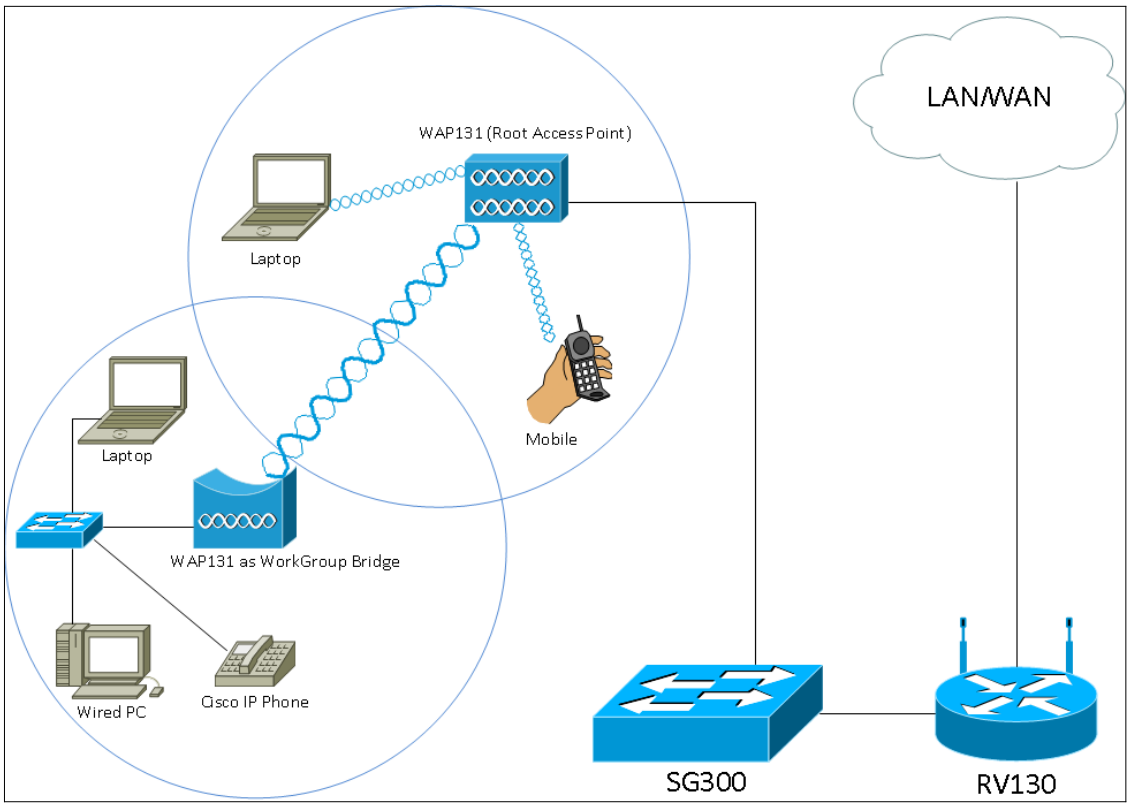
Configure WorkGroup Bridge on the WAP131 Access Point

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, and the one associated with the wireless LAN is called an infrastructure interface. Although the Wireless Distribution System (WDS) is the preferred bridge solution for the WAP131, the Workgroup Bridge Mode is recommended when the WDS feature is unavailable.



Note: When the Workgroup Bridge feature is enabled, the WDS bridge feature does not work. To see how WDS Bridge is configured, refer to the article *Configuring Wireless Distribution System (WDS) Bridge on the WAP131 and WAP351.*

The objective of this document is to explain how to configure the Workgroup Bridge on the WAP131 access point.

Applicable Devices

- WAP131

Software Version

- 1.0.3.4

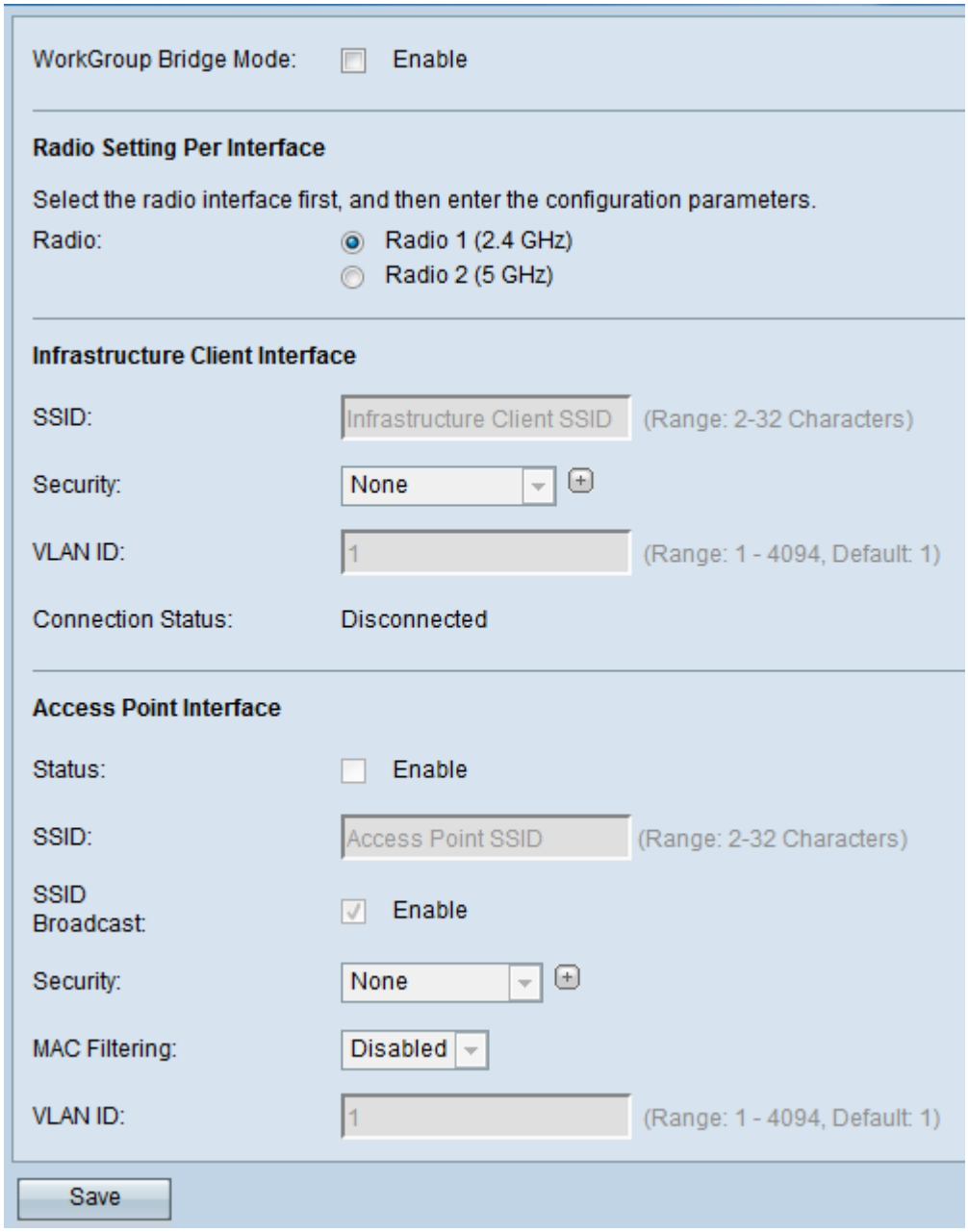
Configure Work Group Bridge

Note: In order to enable Workgroup Bridge, clustering must be enabled in the WAP. If clustering is disabled, you need to disable Single Point Setup to enable clustering. All WAP devices that take part in the Workgroup Bridge must have the following identical settings:

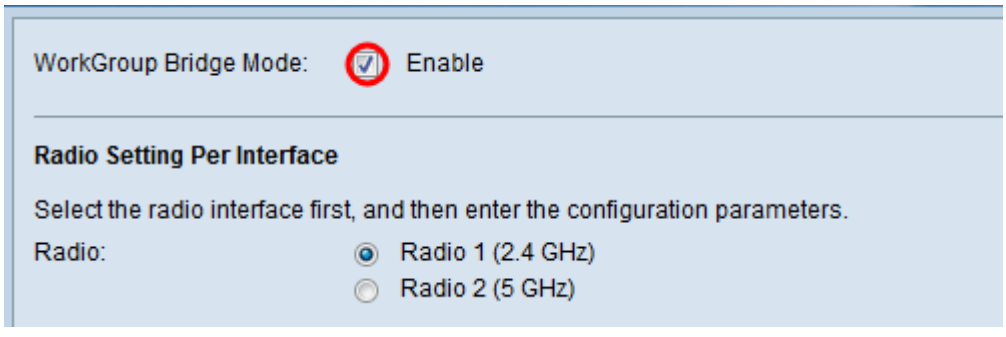
- Radio
- IEEE 802.11 mode
- Channel Bandwidth
- Channel (Auto not recommended)

To ensure these settings in all devices are the same, look up the radio settings. To configure these settings, refer to the article *Configuring Basic Wireless Radio Settings on the WAP131 and WAP351 Access Points*.

Step 1. Log in to the Web Configuration Utility and choose **Wireless > WorkGroup** Bridge. The *WorkGroup Bridge* page opens:

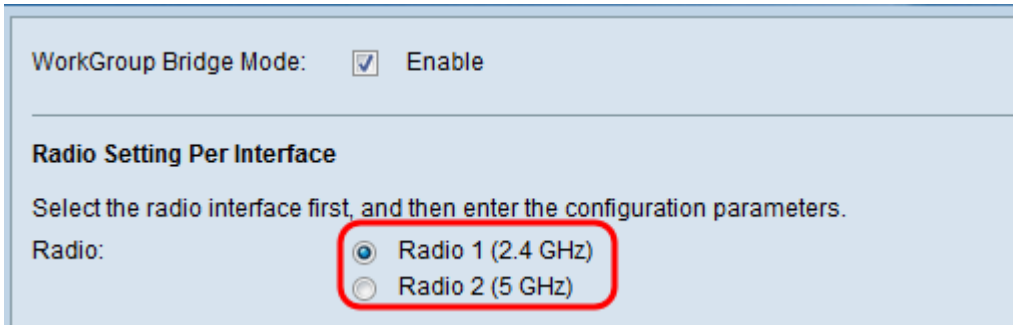


Step 2. Check the **Enable** checkbox in the *WorkGroup Bridge Mode* field to enable the workgroup bridge feature.



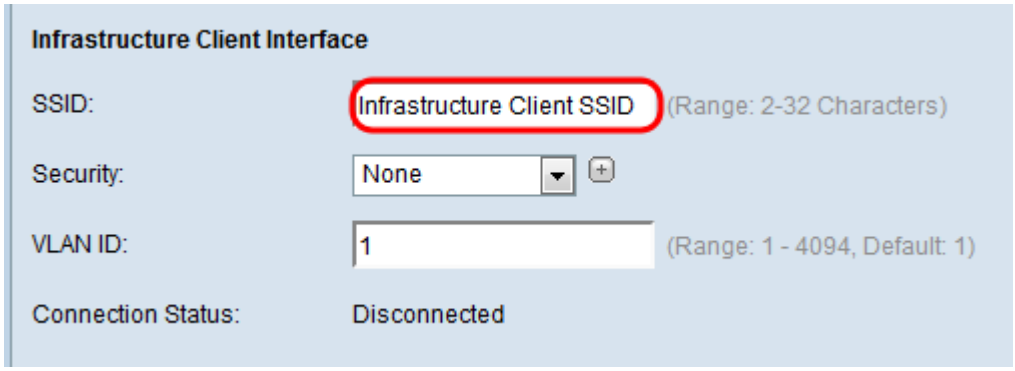
Radio Settings

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 WAP131. The WAP131 is equipped to broadcast on two different radio interfaces. Configuring settings for one radio interface will not affect the other.

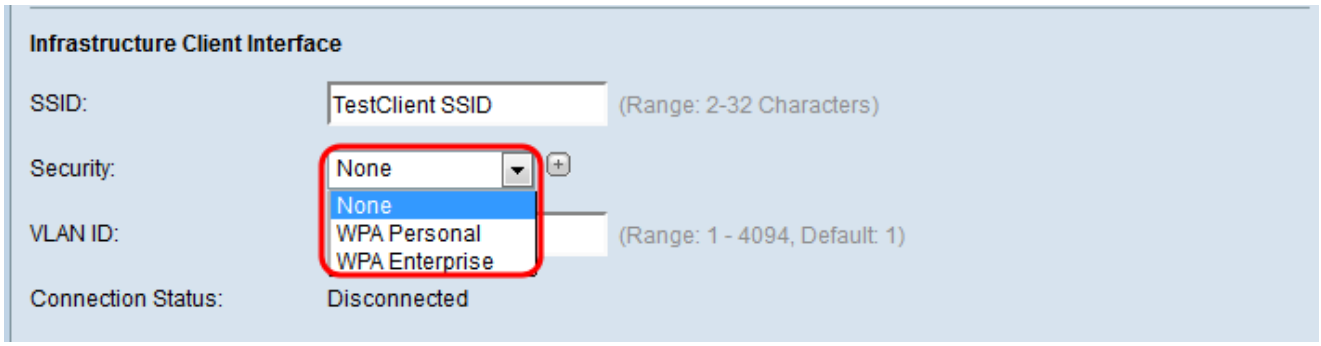


Infrastructure Client Interface

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



Step 2. Choose the type of security to authenticate a client station on the upstream WAP device from the *Security* drop-down list.



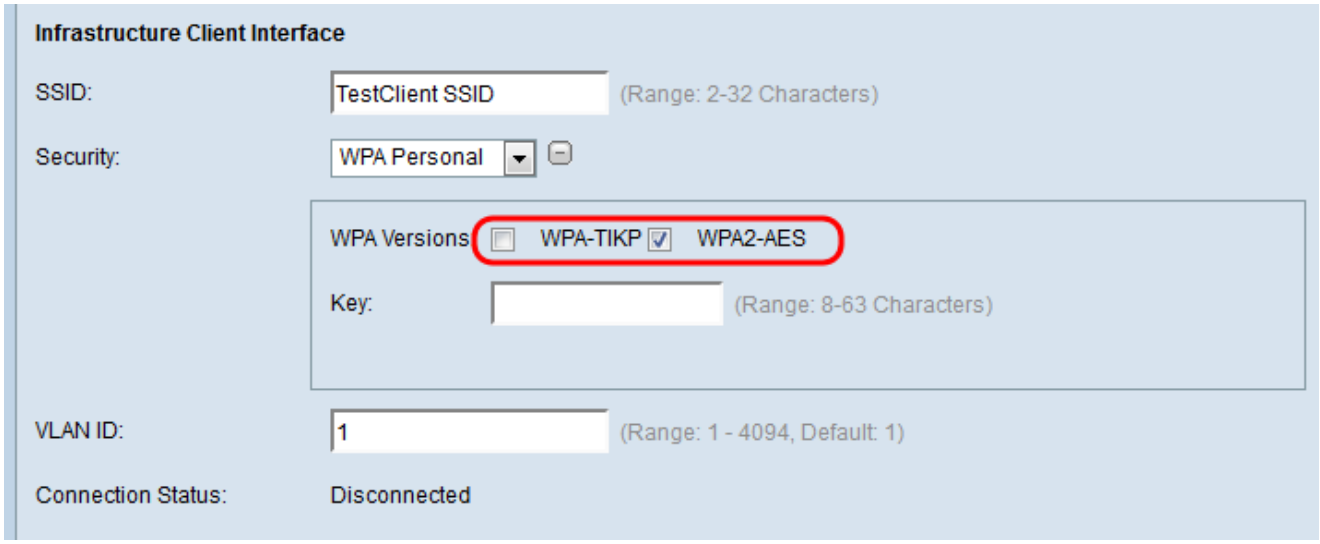
The available options are defined as follows:

- None — Open or no security. This is the default value. If you choose this, skip to Step 14.
- WPA Personal — WPA Personal 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. If you choose this, go to Step 3.
- 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, go to Step 5.

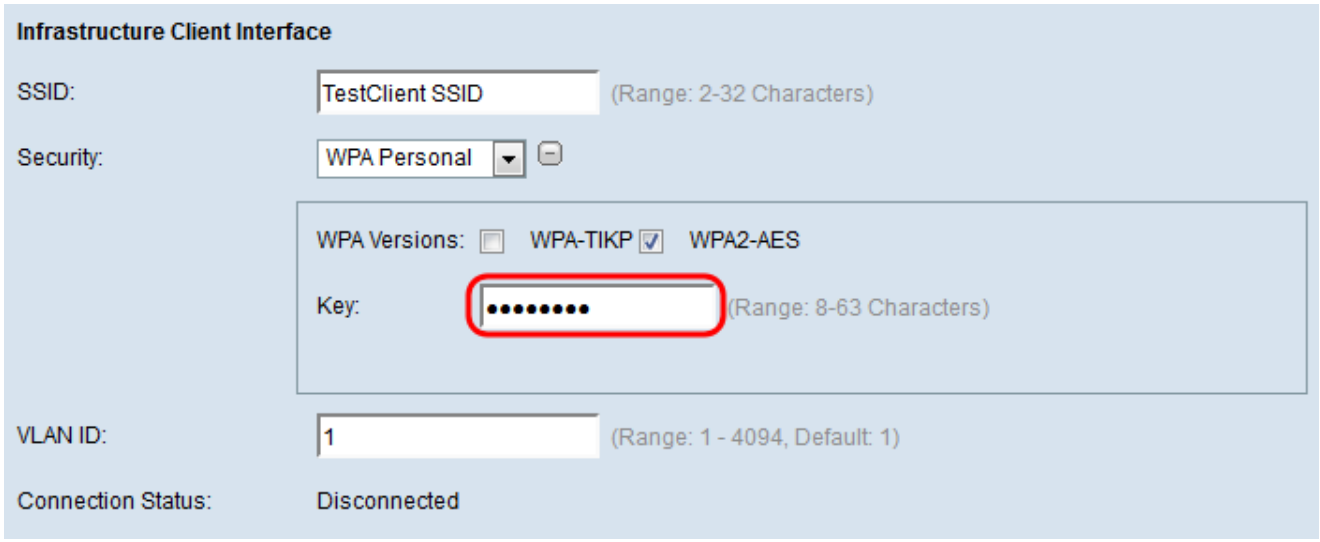
WPA Personal

Step 3. 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

supports WPA2, then set the infrastructure client security for WPA2-AES. If some of your wireless devices, like PDAs and other small wireless network devices, only connect with WPA-TKIP, then select WPA-TKIP.

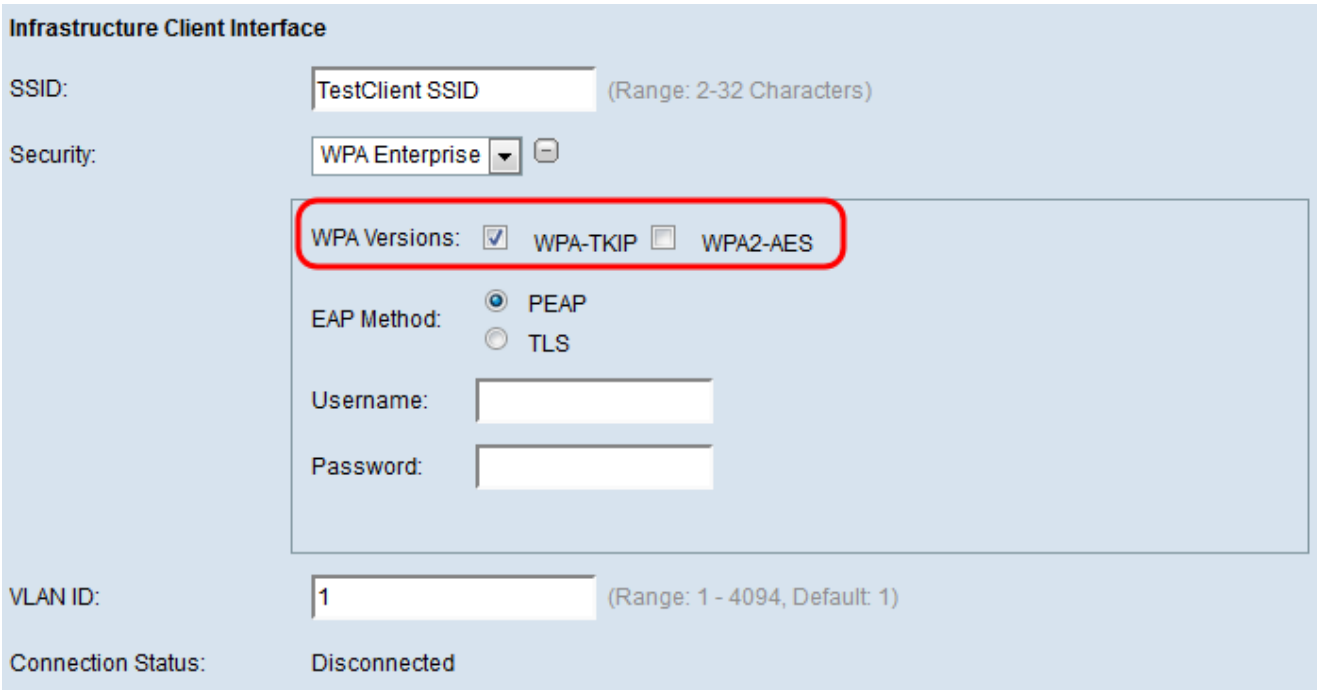


Step 4. Enter in the WPA encryption key in the *Key* field. The key must be 8-63 characters long. Skip to Step 14.

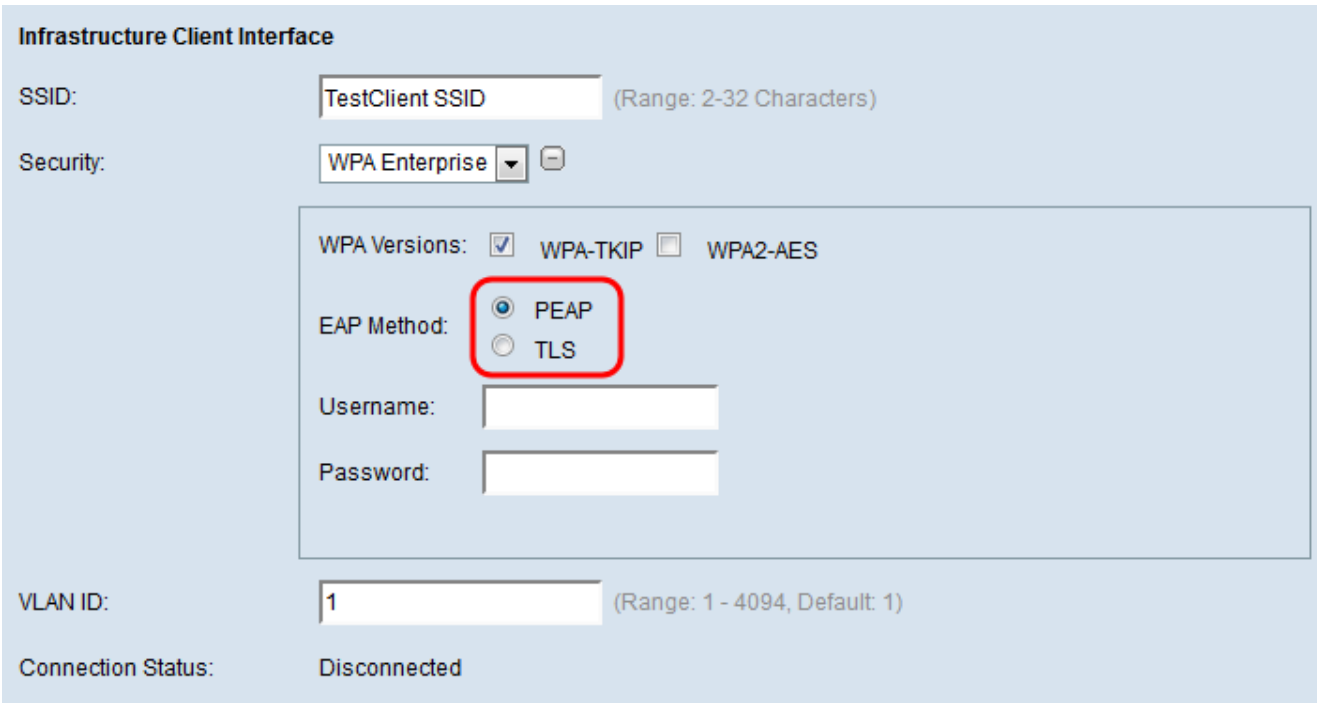


WPA Enterprise

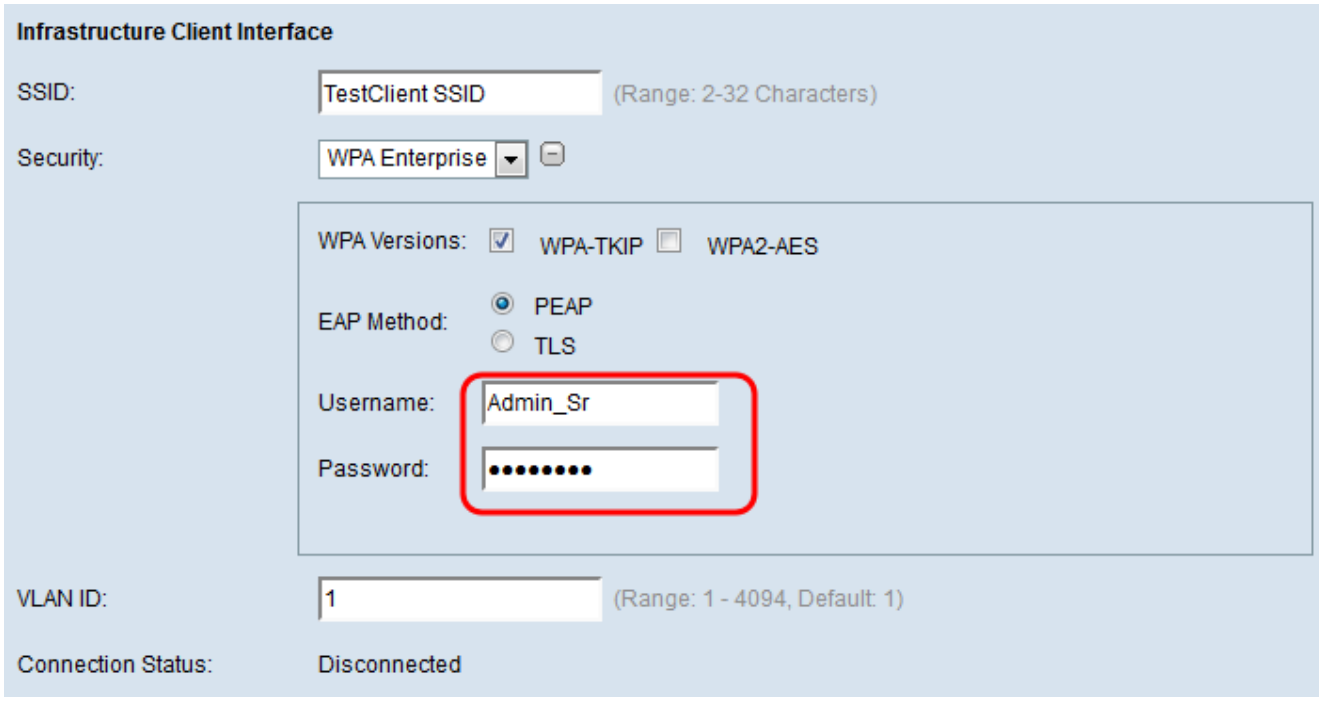
Step 5. Select the **WPA-TKIP** or **WPA2-AES** checkbox to determine which kind of WPA encryption the infrastructure client interface will use. If all of your wireless equipment support WPA2, then set the infrastructure client security for WPA2-AES. If some of your wireless devices can only connect with WPA-TKIP, then check both the **WPA-TKIP** and **WPA2-AES** checkboxes. In this configuration, your WPA2 devices will connect to WPA2, and your WPA devices will connect to WPA.



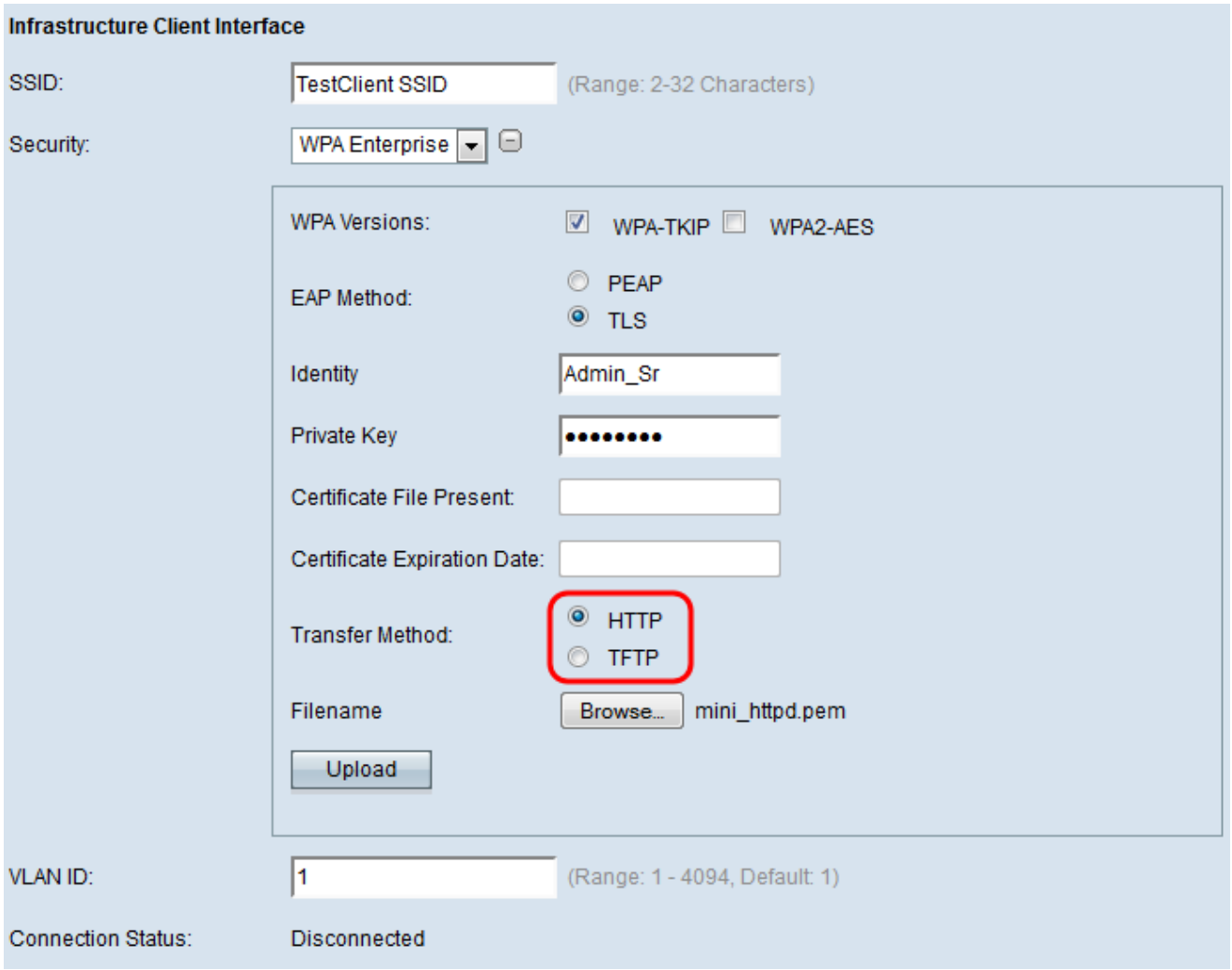
Step 6. In the *EAP Method* field, select either the **PEAP** or **TLS** radio button. The Protected Extensible Authentication Protocol (PEAP) gives each wireless user under the WAP individual usernames and passwords that support AES encryption standards. Transport Layer Security (TLS) requires each user to have an additional certificate to be granted access. If you select PEAP, skip to Step 14.



Step 7. Enter the username and password in the *Username* and *Password* field.



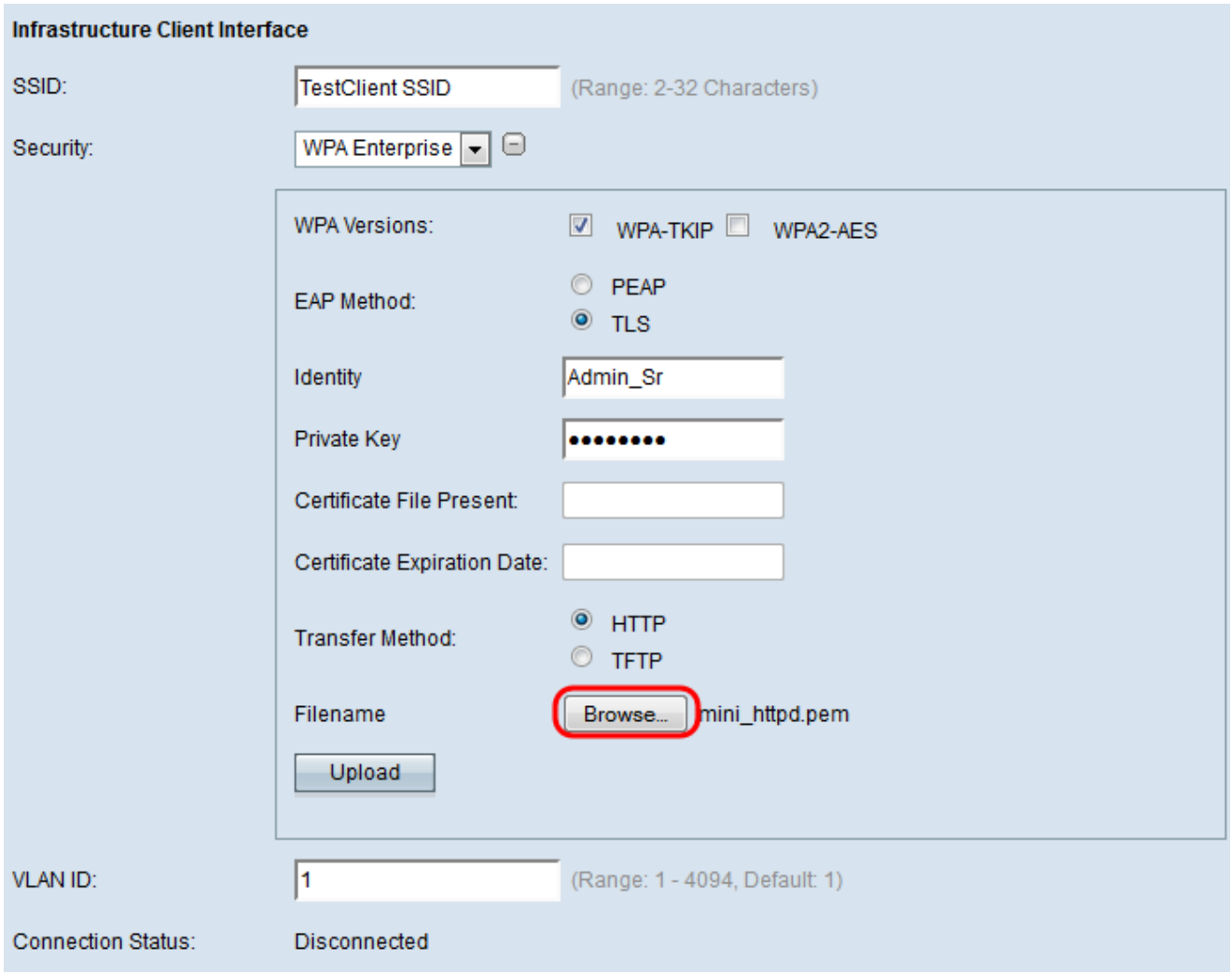
Step 8. Select either the **HTTP** or **TFTP** radio buttons in the *Transfer Method* field. Trivial File Transfer Protocol (TFTP) is a simplified unsecure version of File Transfer Protocol (FTP). It is mainly used to distribute software or authenticate devices among corporate networks. Hypertext Transfer 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 11.



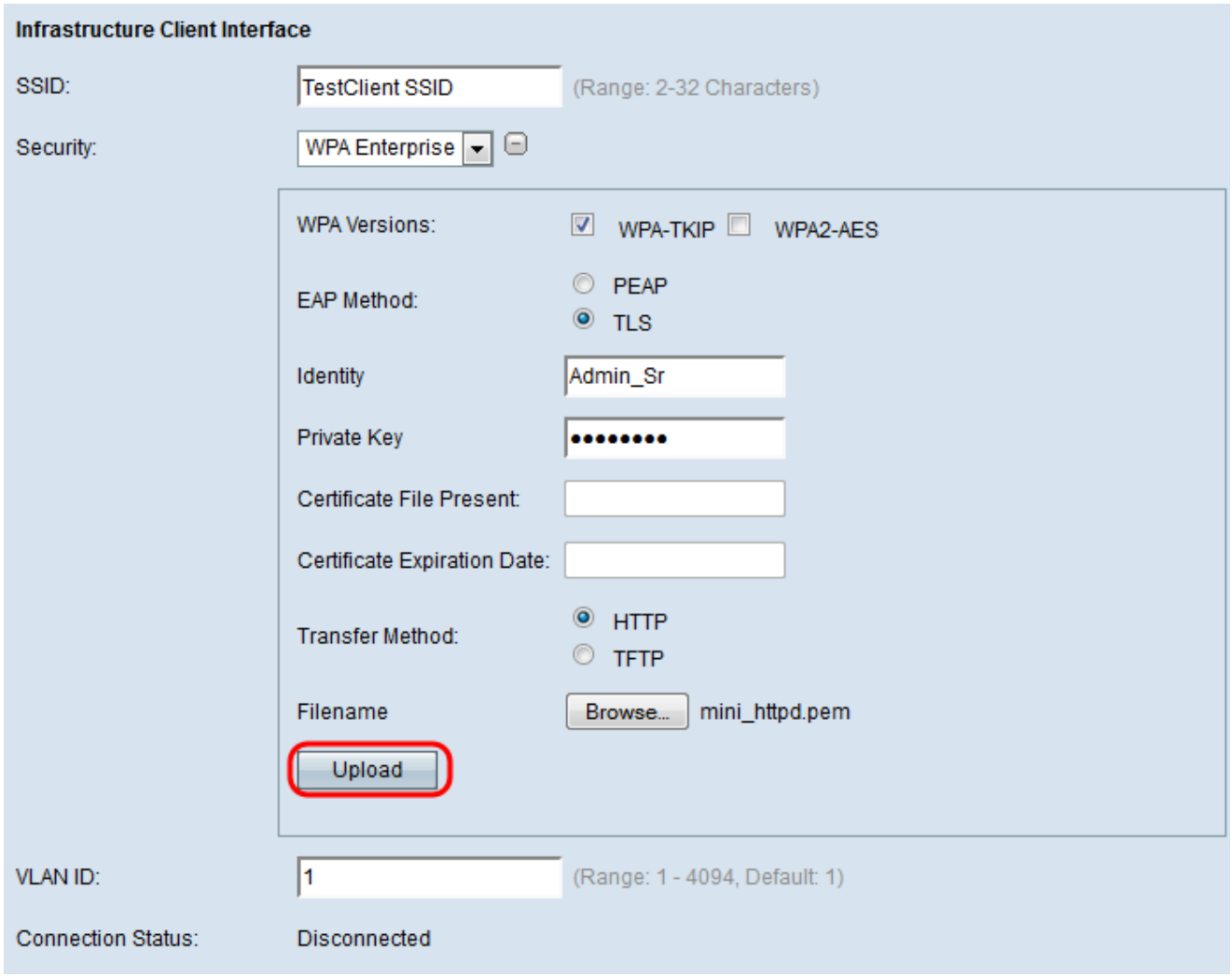
Note: If a certificate file is already present on the WAP, then the *Certificate File Present* and *Certificate Expiration Date* field will already be filled in with the relevant information. Otherwise, they will be blank.

HTTP

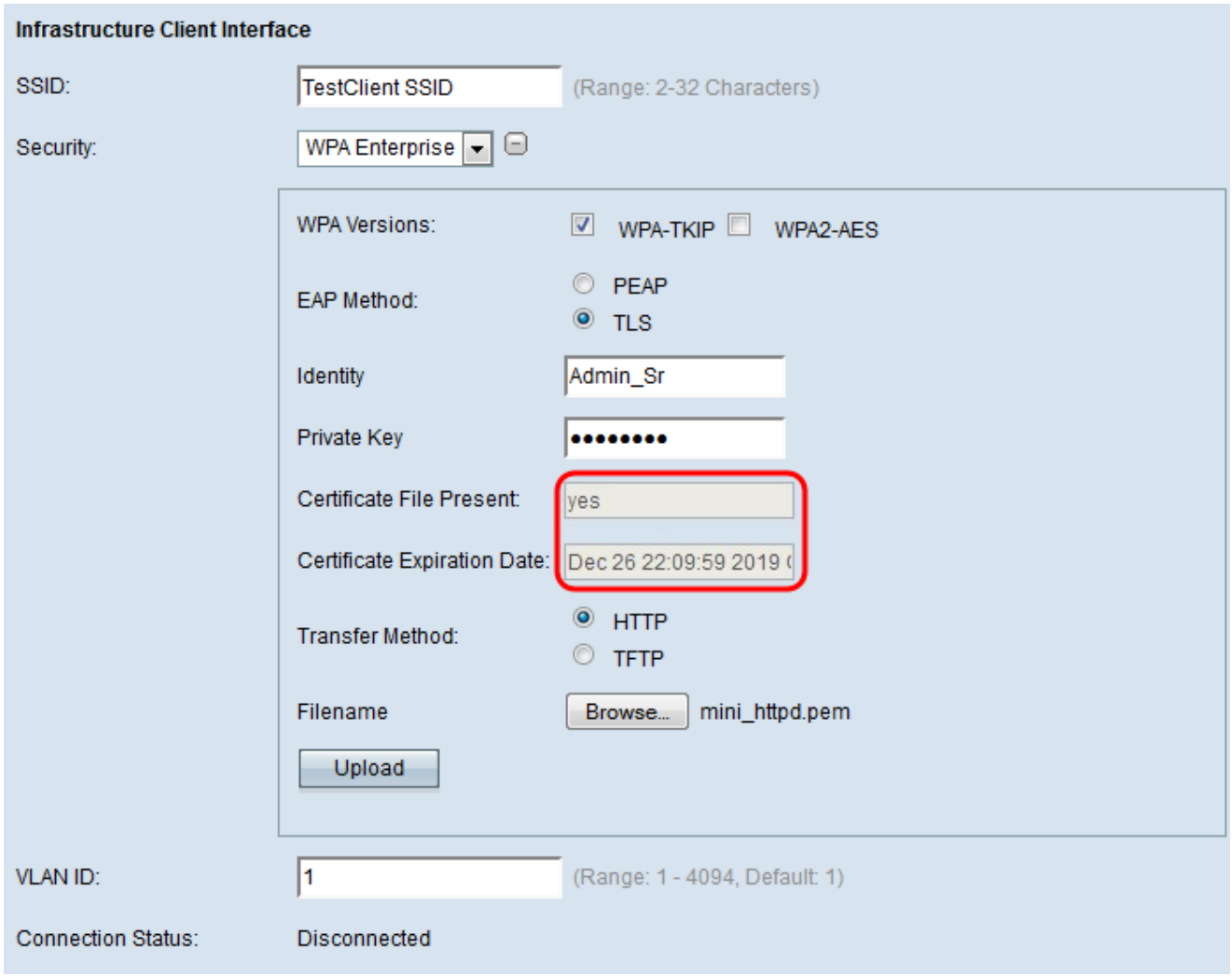
Step 9. Click the **Browse** button to find and select a certificate file. The file must have the proper certificate file extension (such as .pem or .pfx), otherwise the file will not be accepted.



Step 10. Click **Upload** to upload the selected certificate file. Skip to Step 14.

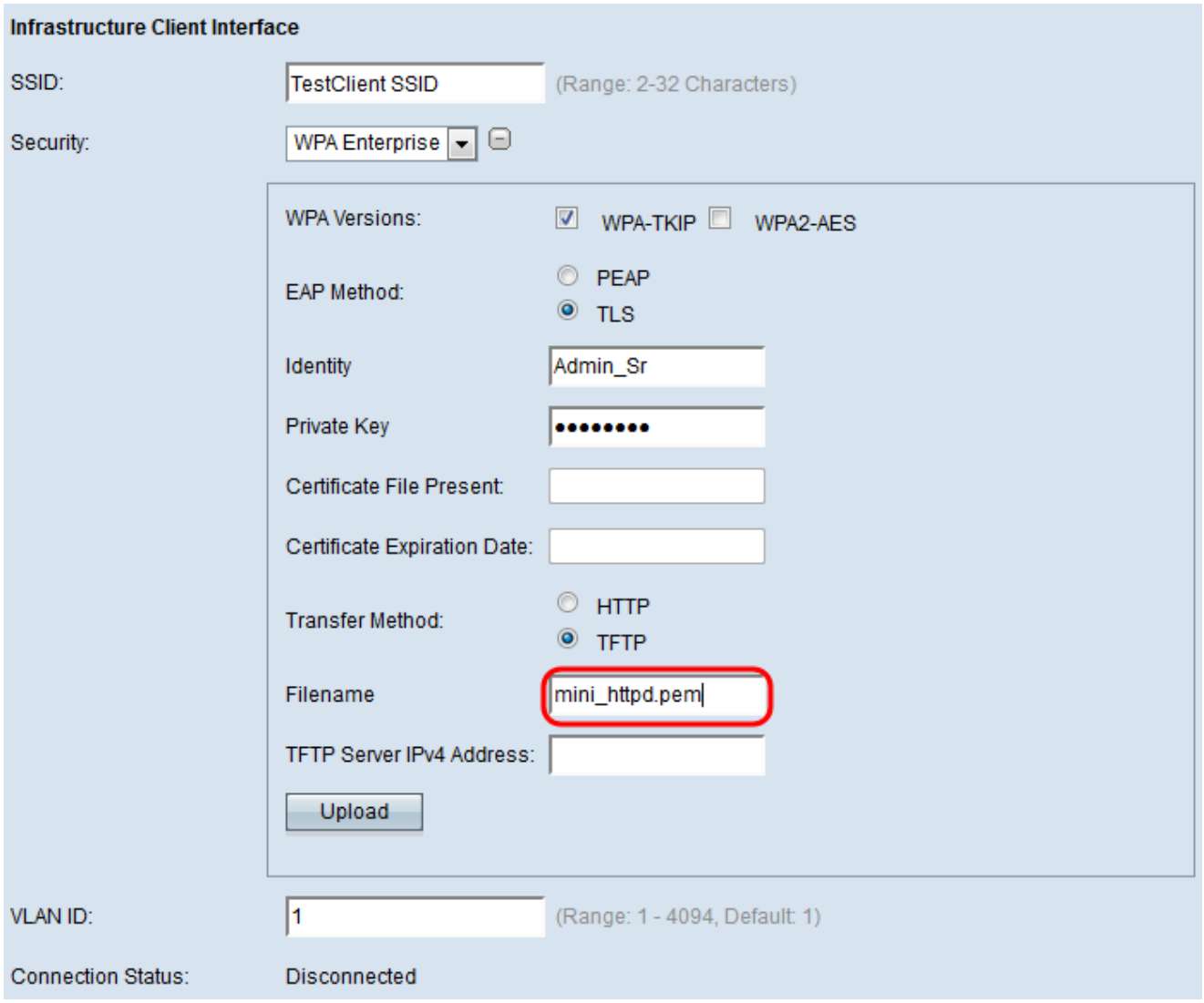


The *Certificate File Present* and *Certificate Expiration Date* field will be updated automatically.

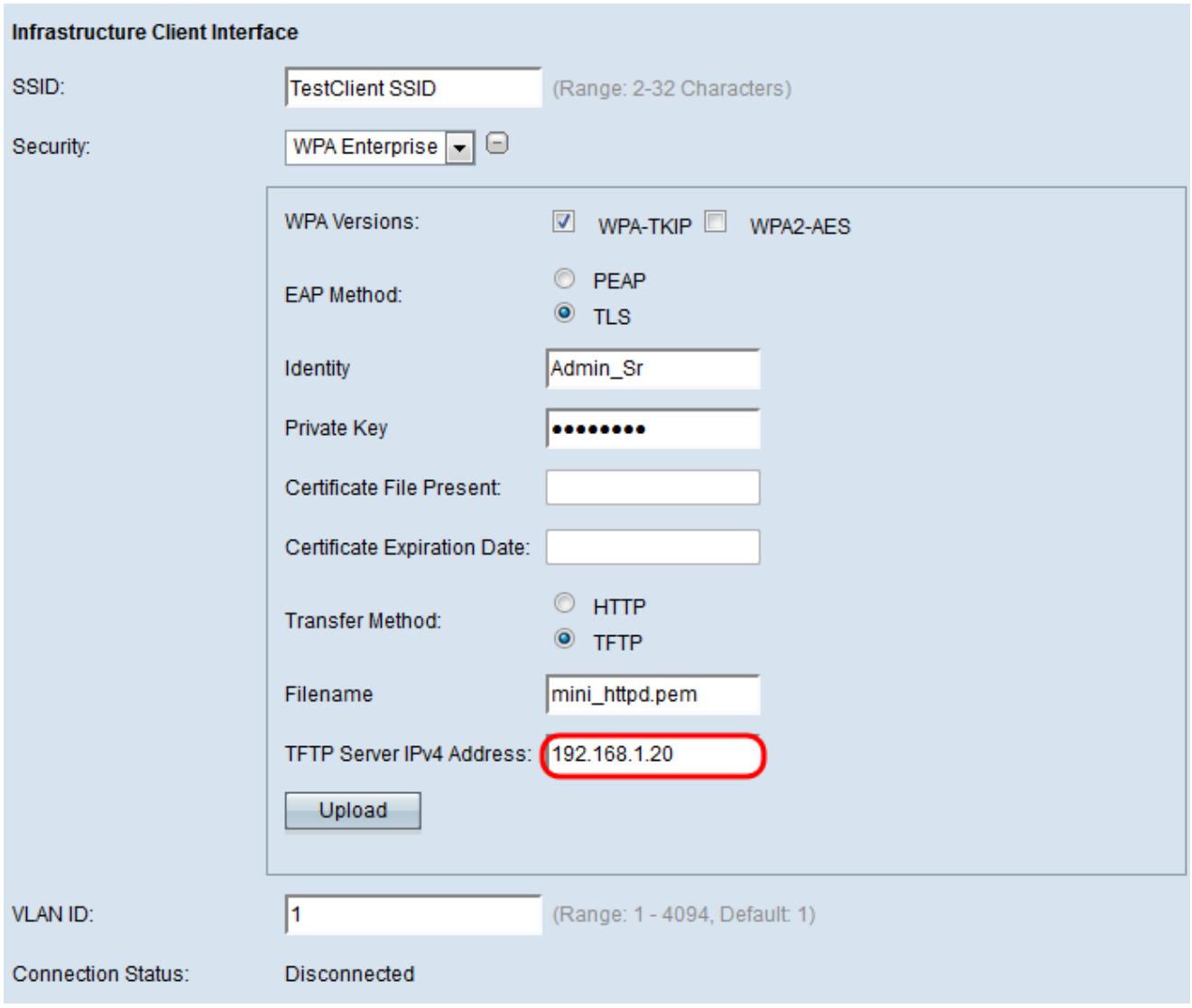


TFTP

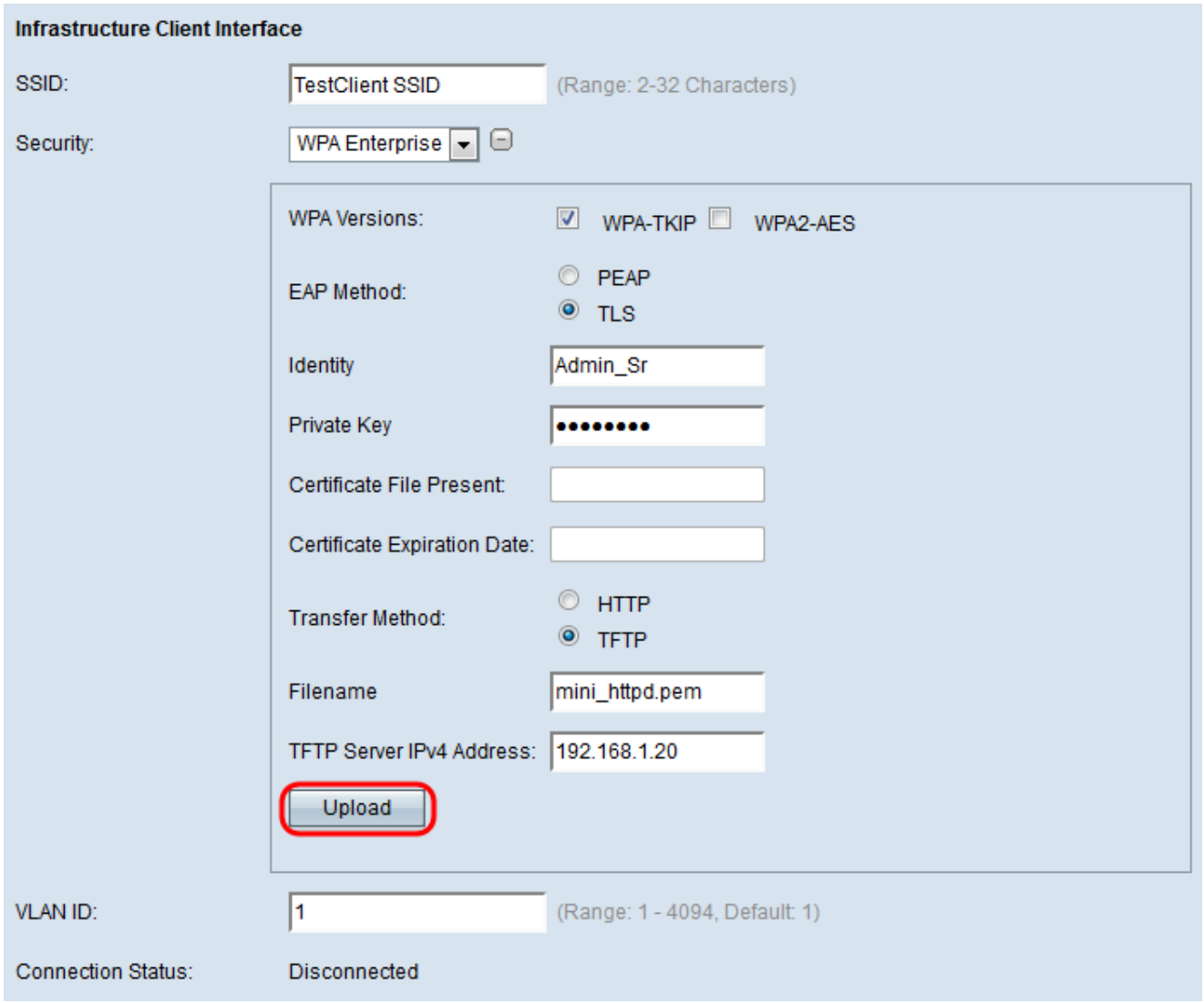
Step 11. Enter the filename of the certificate file in the *Filename* field.



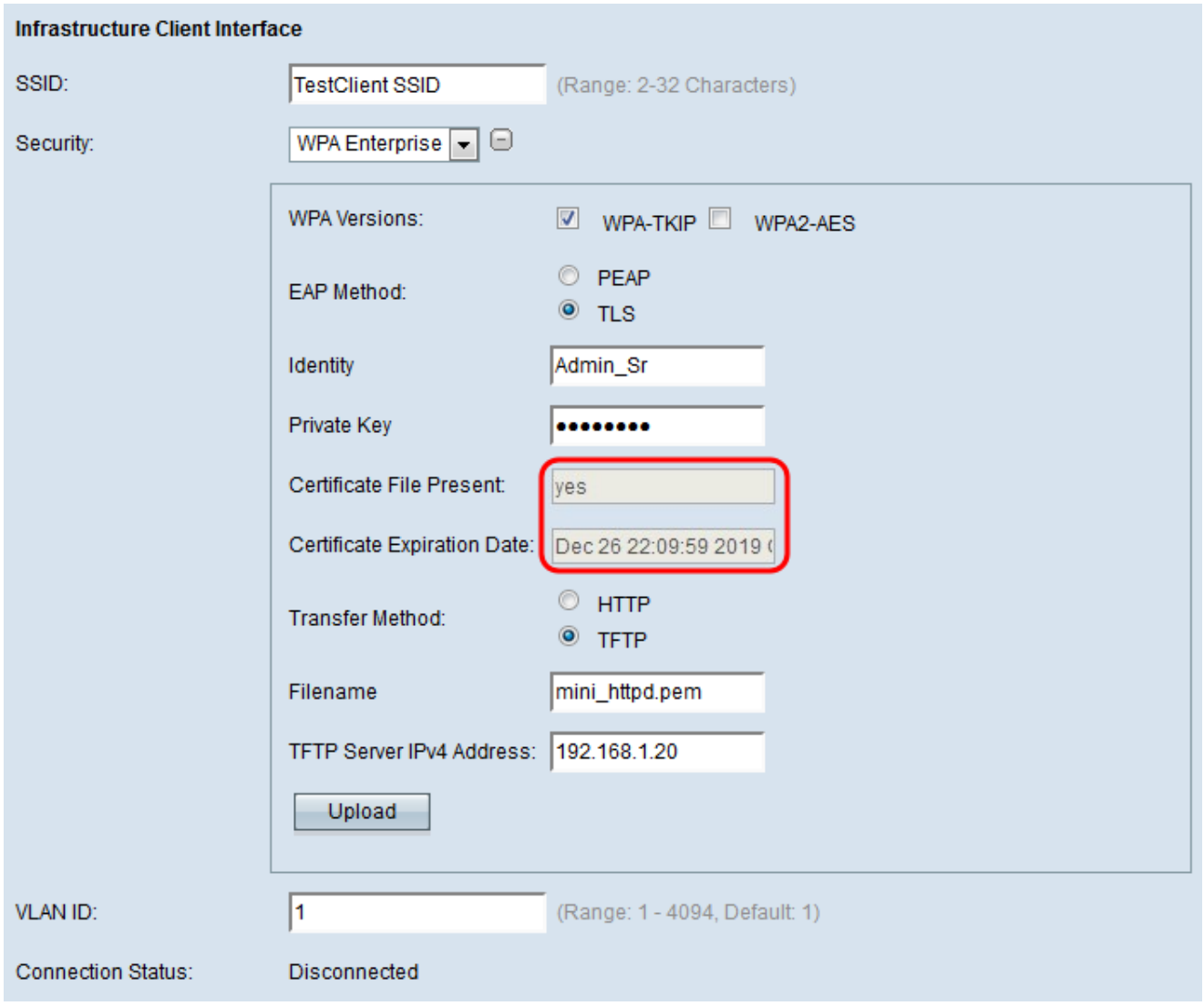
Step 12. Enter the TFTP Server address in the *TFTP Server IPv4 Address* field.



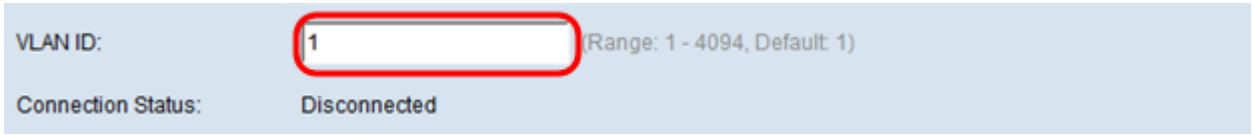
Step 13. Click the **Upload** button to upload the specified certificate file.



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

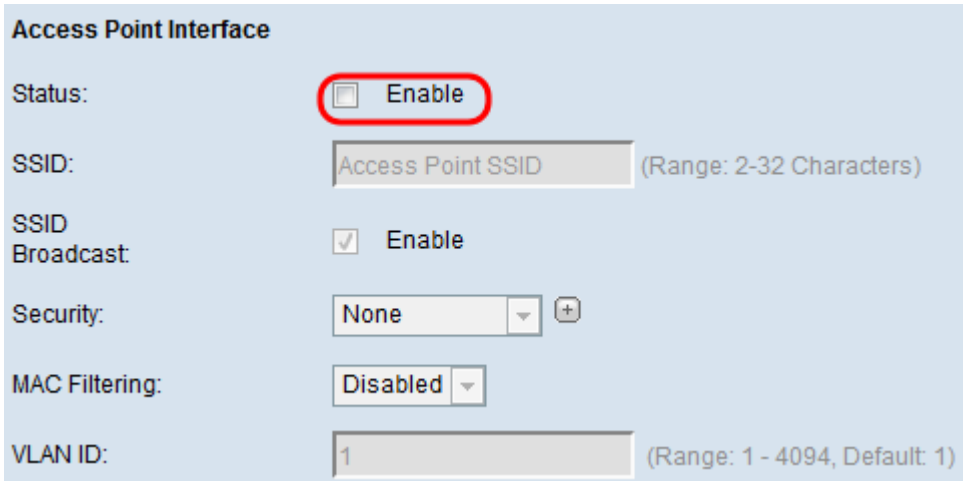


Step 14. Enter the VLAN ID for the infrastructure client interface.

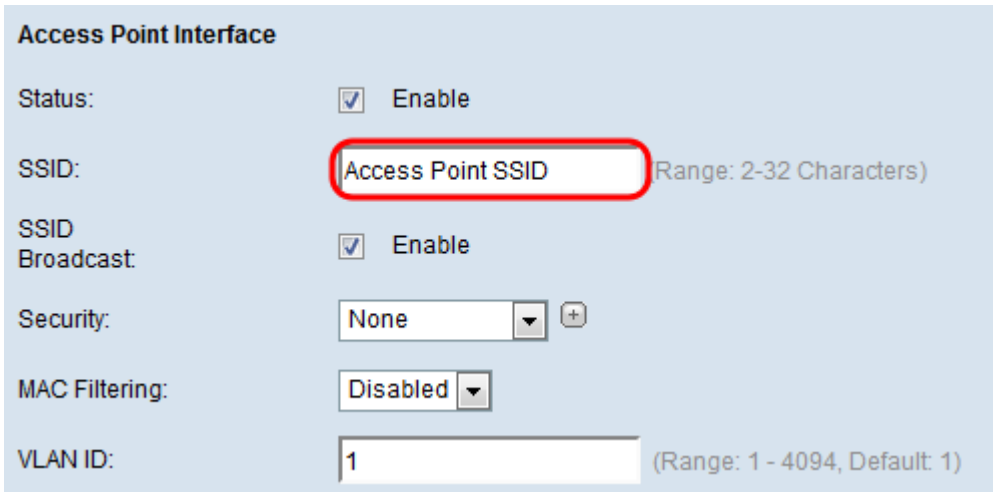


Access Point Interface

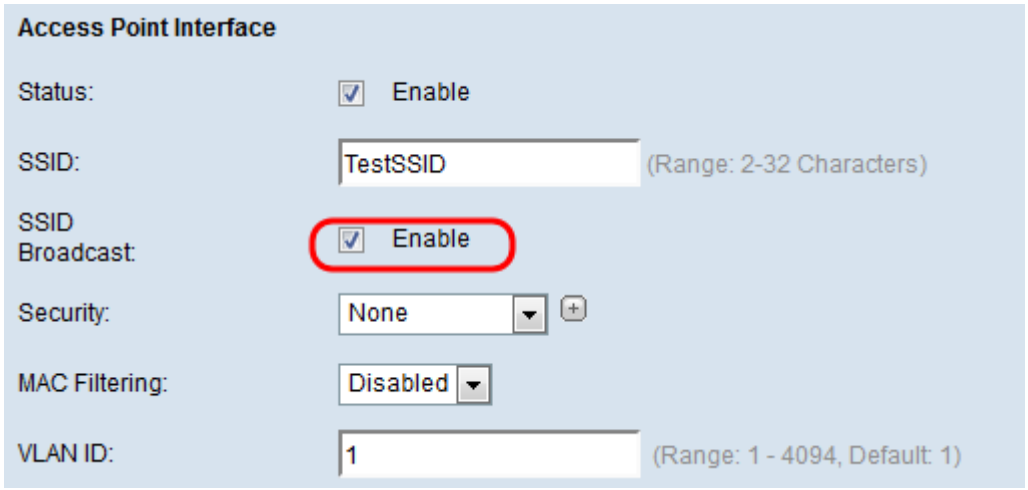
Step 1. Check the **Enable** checkbox in the *Status* field to enable bridging on the access point interface.



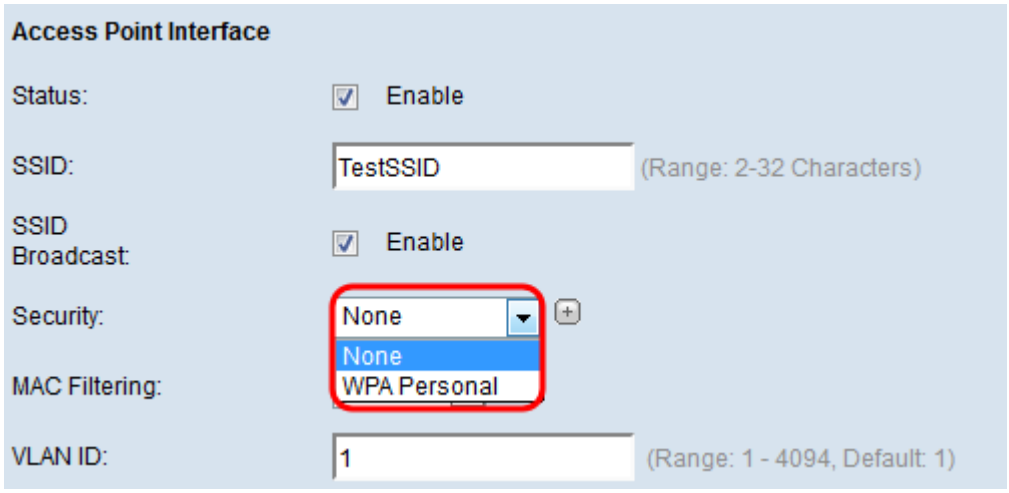
Step 2. Enter the Service Set Identifier (SSID) for the access point in the *SSID* field. The SSID length must be between 2 to 32 characters.



Step 3. (Optional) If you do not want to broadcast the downstream SSID, uncheck the **Enable** checkbox in the SSID Broadcast field. It is enabled by default.



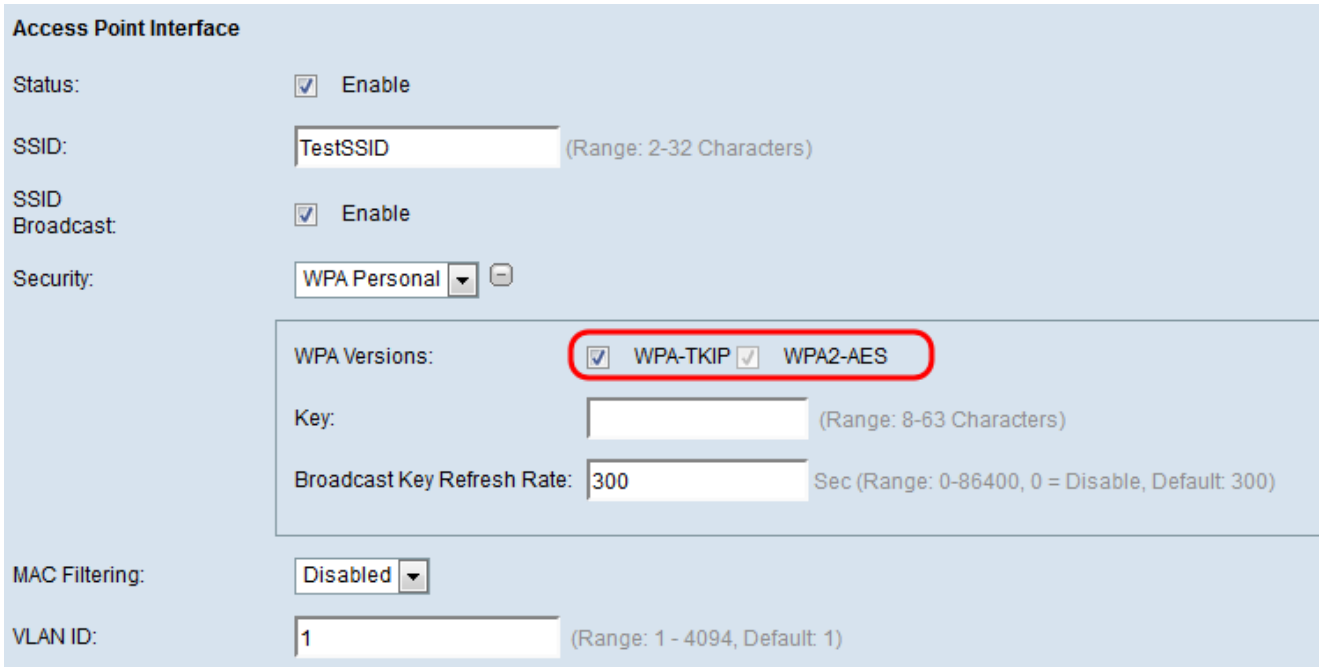
Step 4. Choose the type of security to authenticate downstream client stations to the WAP device from the *Security* drop-down list.



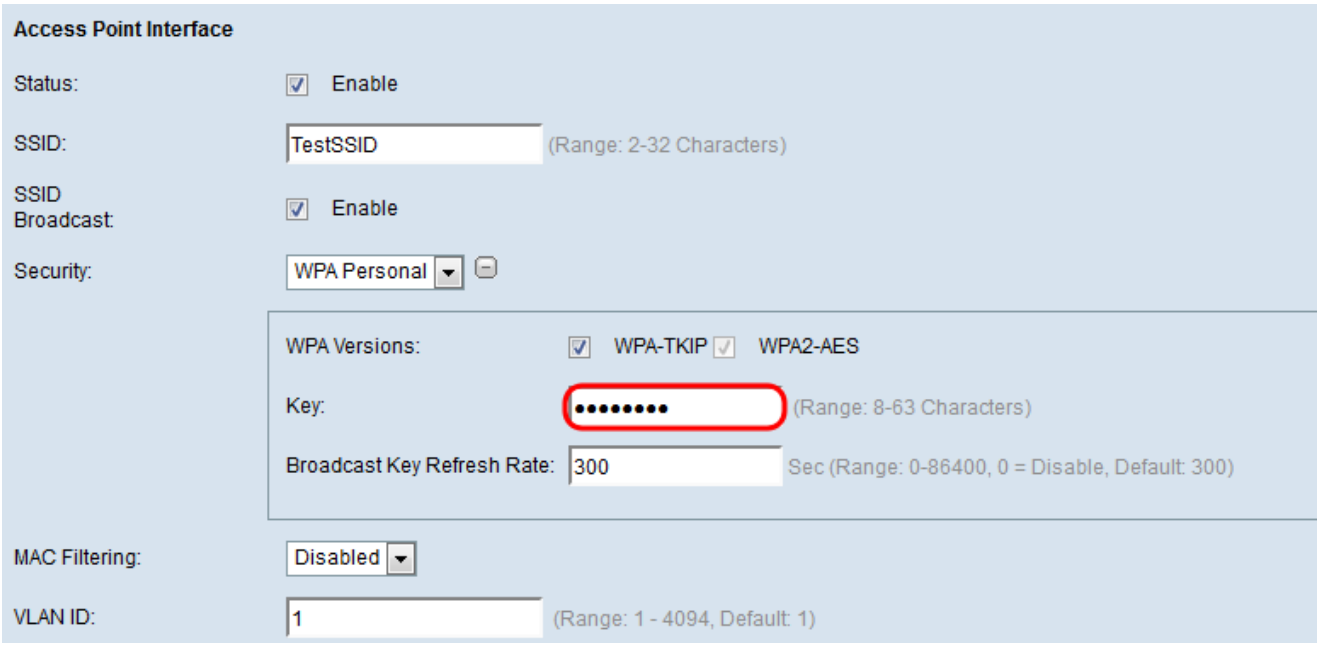
The available options are defined as follows:

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

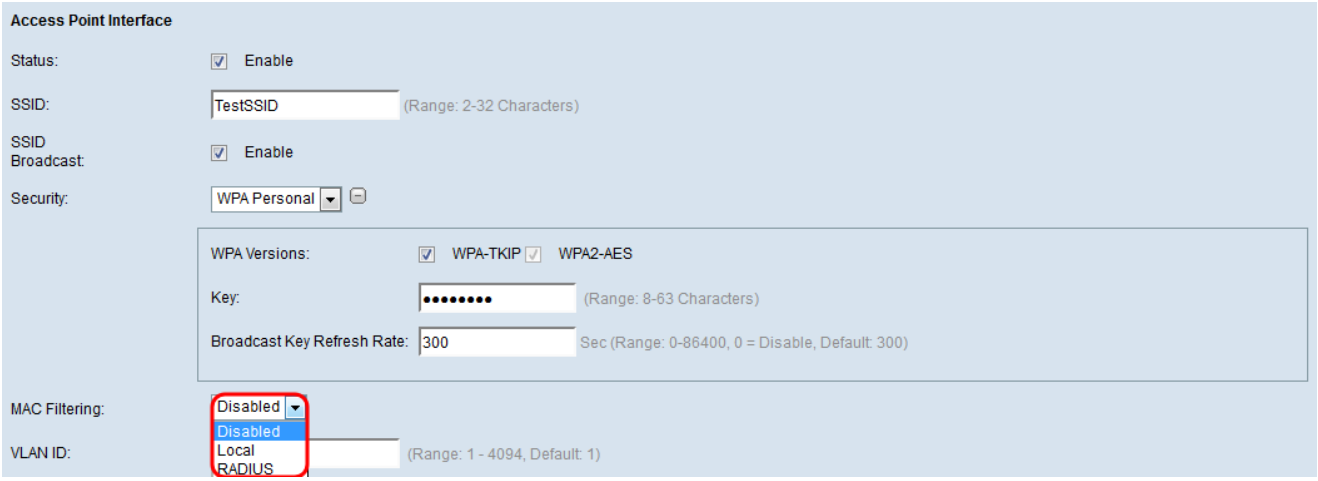


Step 6. Enter the shared WPA key in the *Key* field. The key must be 8-63 characters long, and can include alphanumeric characters, upper and lower case characters, and special characters.



Step 7. Enter the rate in the *Broadcast Key Refresh Rate*. The 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.



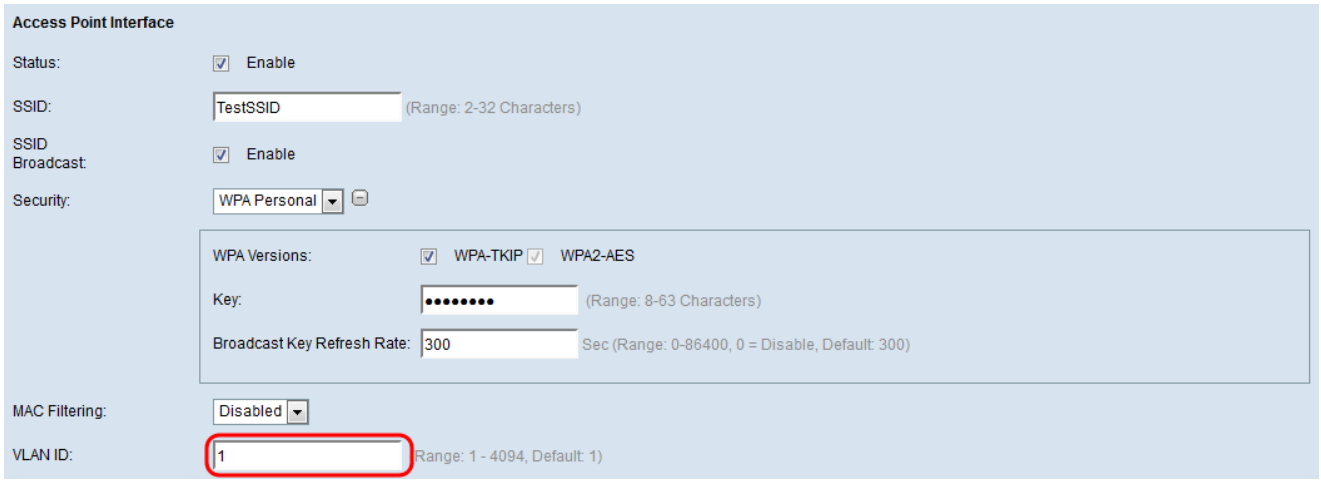
The available options are defined as follows:

- 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.

WorkGroup Bridge Mode: Enable

Radio Setting Per Interface

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (2.4 GHz)
Radio 2 (5 GHz)

Infrastructure Client Interface

SSID: TestClient SSID (Range: 2-32 Characters)

Security: WPA Personal

VLAN ID: 1 (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

Access Point Interface

Status: Enable

SSID: TestSSID (Range: 2-32 Characters)

SSID Broadcast: Enable

Security: WPA Personal

MAC Filtering: Disabled

VLAN ID: 1 (Range: 1 - 4094, Default: 1)

Save