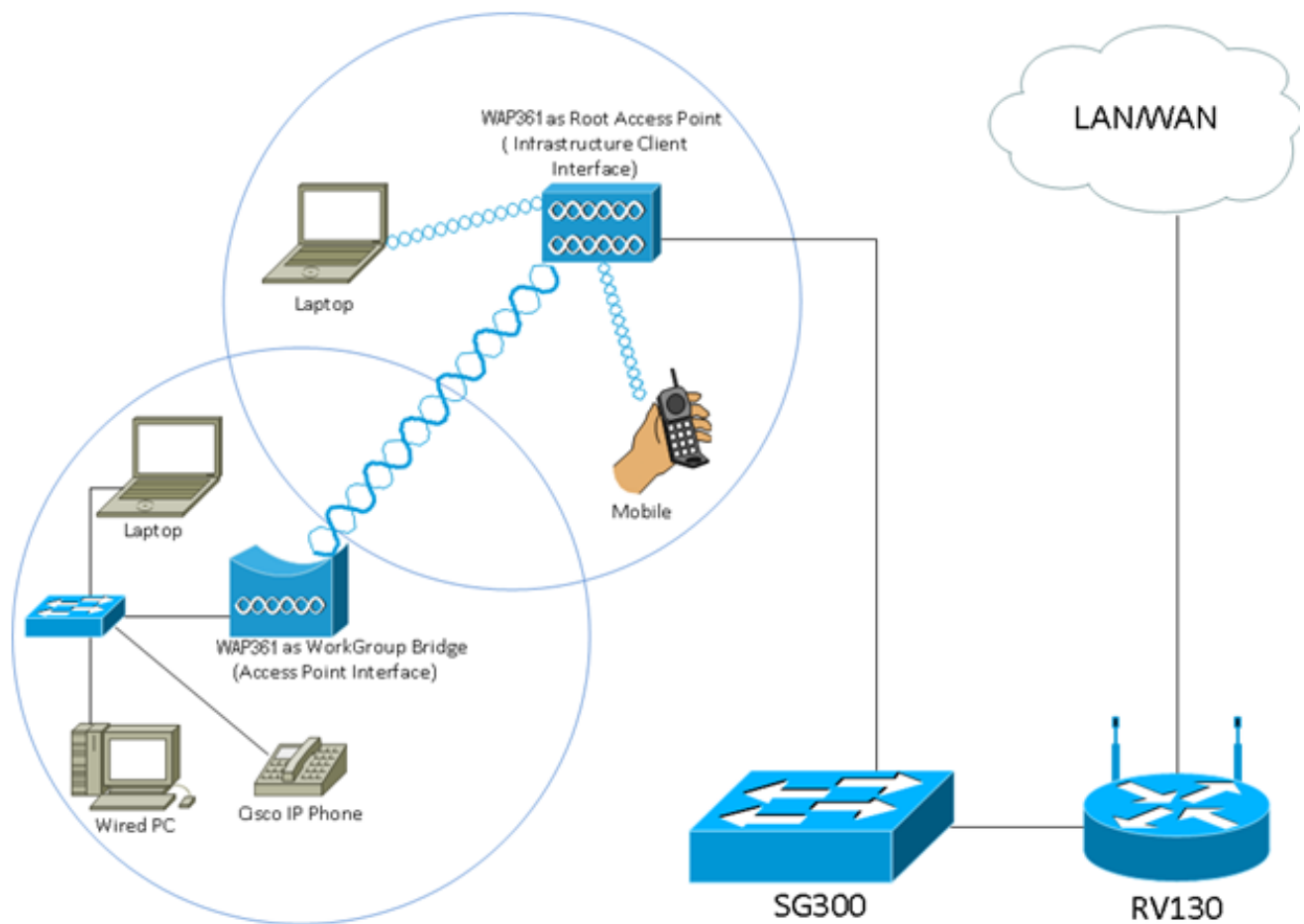


# Configure Workgroup Bridge on a Wireless Access Point (WAP)

## Objective

The WorkGroup Bridge feature enables the Wireless Access Point (WAP) to bridge traffic between a remote client and the wireless Local Area Network (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. WorkGroup Bridge Mode is recommended as an alternative when the Wireless Distribution System (WDS) feature is unavailable.



**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 acts as an access point interface, connects to the infrastructure interface.

This article aims to show you how to configure the WorkGroup Bridge between two WAPs.

## Applicable Devices

- WAP100 Series
- WAP300 Series
- WAP500 Series

# Software Version

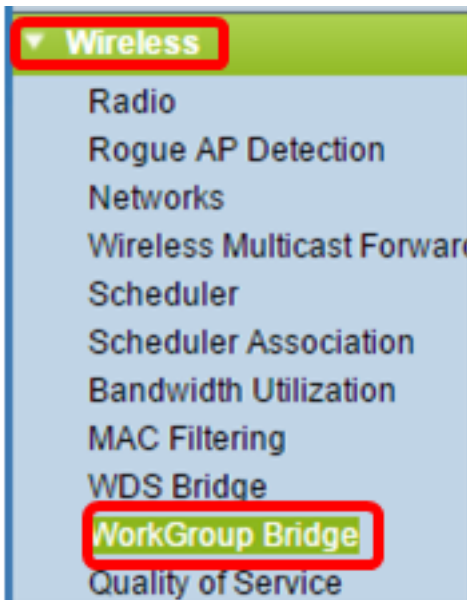
- 1.0.0.17 —WAP571, WAP571E
- 1.0.1.7 — WAP150, WAP361
- 1.0.2.5 — WAP131, WAP351
- 1.0.6.5 — WAP121, WAP321
- 1.2.1.3 — WAP551, WAP561
- 1.3.0.3 — WAP371

# Configure WorkGroup Bridge

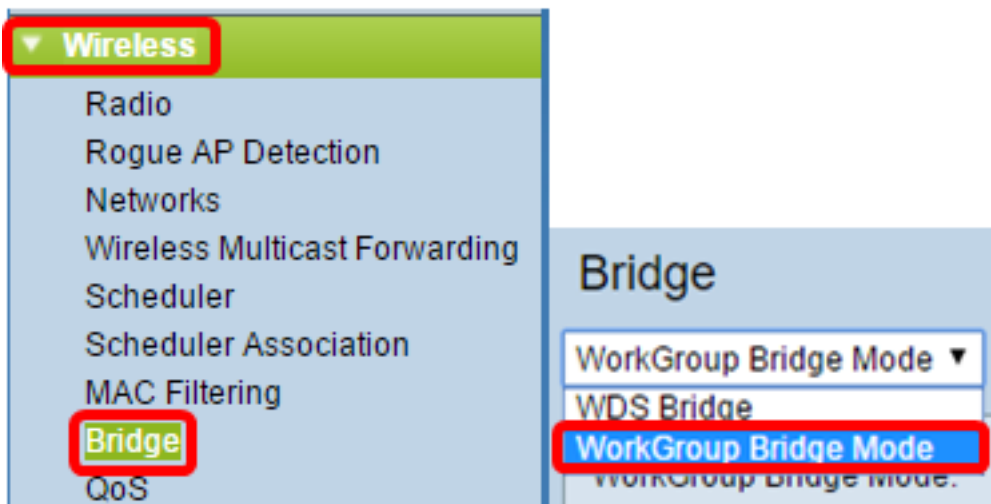
## Infrastructure Client Interface

Step 1. Log in to the web-based utility of the WAPand choose **Wireless > WorkGroup Bridge**.

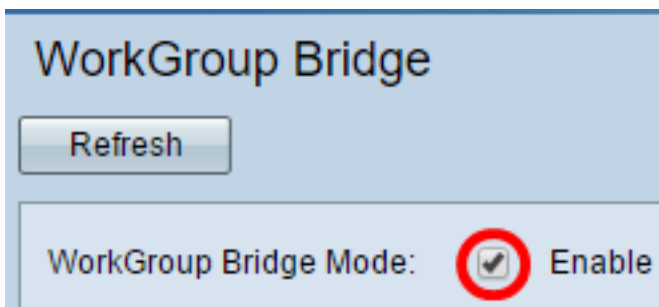
**Note:** The menu options may vary depending on the model of the device you are using. The images below are taken from the WAP361 unless stated otherwise.



For WAP571 and WAP571E, choose **Wireless > Bridge > WorkGroup Bridge Mode**.



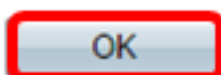
Step 2. Check the **Enable** WorkGroup Bridge Mode check box.



**Note:** If clustering is enabled on the WAP, a pop-up will notify you to disable clustering in order for the WorkGroup Bridge to work. Click **OK** to continue. To disable clustering, choose **Single Point Setup** from the navigation pane then choose **Access Points > Disable Single Point Setup**.

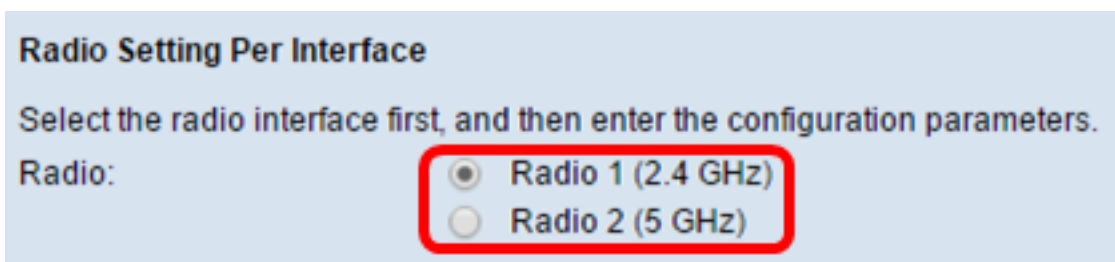


Workgroup Bridge cannot be enabled when clustering is enabled.



Step 3. Click the radio interface for the WorkGroup 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 WAP. The WAP is equipped to broadcast on two different radio interfaces. Configuring settings for one radio interface will not affect the other. Radio interface options may vary depending on the WAP model. Some WAPs show Radio 1 as 2.4 GHz while some have Radio 2 as 2.4 GHz.

**Note:** This step is only for the following WAPs with dual-band: WAP131, WAP150, WAP351, WAP361, WAP371, WAP561, WAP571, WAP571E. For this example, Radio 1 is chosen.



Step 4. Enter the Service Set Identifier (SSID) name in the *SSID* field or click the arrow button beside the field to scan for neighbors. This serves as the connection between the device and the remote client. You may enter 2 to 32 characters for the Infrastructure Client SSID.

**Note:** It is important to enable Rogue AP detection. To learn more about how to enable the said feature, click [here](#). For this example, the arrow button is clicked to choose WAP361\_L1 as the SSID of the Infrastructure Client Interface.

Infrastructure Client Interface

SSID:  (Range: 2-32 Characters)

Security:  (Range: 1 - 4094, Default: 1)

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

Connection Status: Disconnected

MAC Address	SSID
80:e8:6f:0a:5d:ee	WAP361_L1

Step 5. In the Infrastructure Client Interface area, choose the type of security to authenticate as a client station on the upstream WAP device from the Security drop-down list. The options are:

- None — Open or no Security. This is the default. If this is chosen, skip to [Step 18](#).
- WPA Personal — WPA Personal can support keys of length 8-63 characters. WPA2 is recommended as it has a more powerful encryption standard. Skip to [Step 6](#) to configure.
- 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). Skip to [Step 9](#) to configure. This type of security is often used in an office environment and needs a Remote Authentication Dial-In User Service (RADIUS) server configured. Click [here](#) to know more about RADIUS servers.

Infrastructure Client Interface

SSID:

Security:  (Range: 1 - 4094, Default: 1)

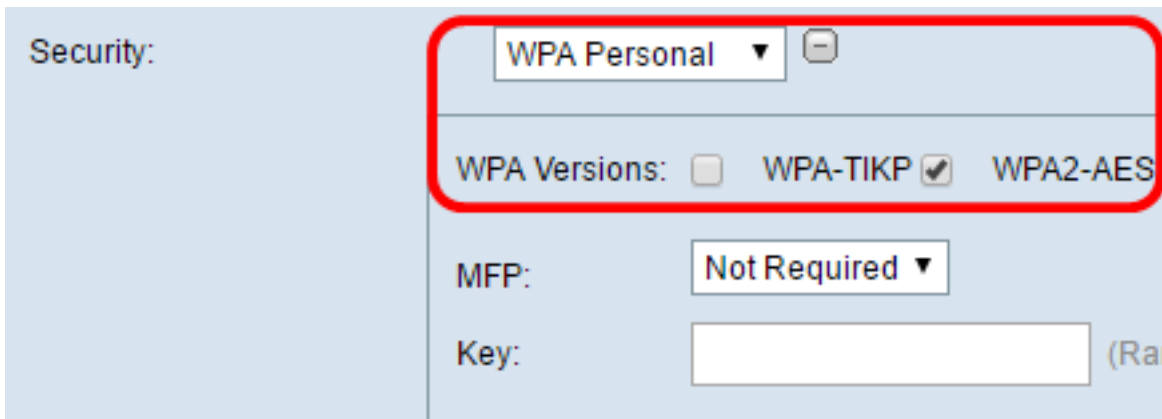
VLAN ID:  (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

**Note:** In this example, WPA Personal is chosen.

[Step 6](#). Click the + and check the WPA-TKIP or WPA2-AES check box to determine which kind of WPA encryption the infrastructure client interface will use.

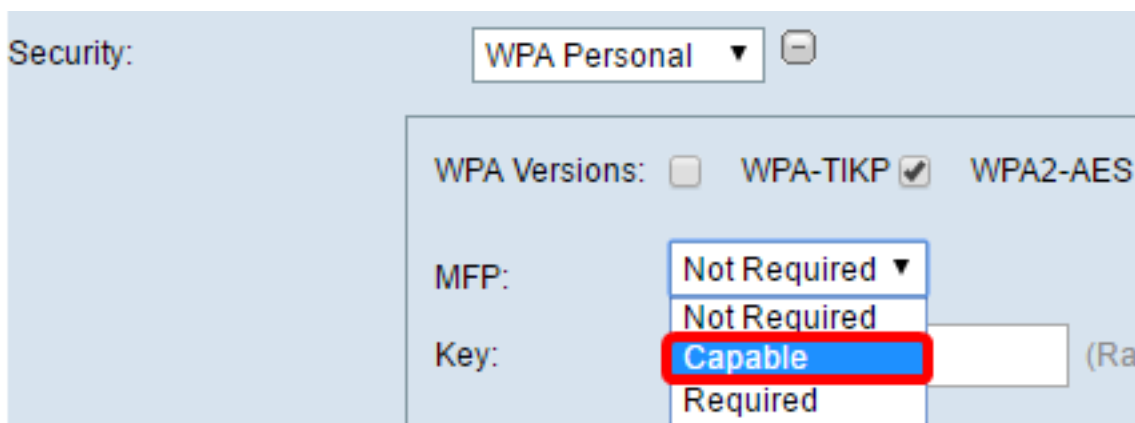
**Note:** If all of your wireless equipment support WPA2, set the infrastructure client security to WPA2-AES. The encryption method is RC4 for WPA and Advanced Encryption Standard (AES) for WPA2. WPA2 is recommended as it has a more powerful encryption standard. For this example, WPA2-AES is used.



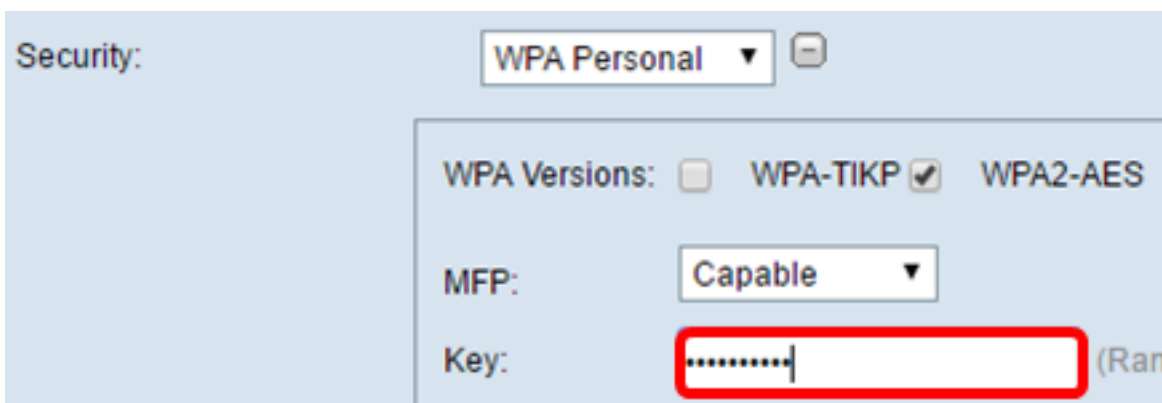
Step 7. (Optional) If you checked WPA2-AES in Step 6, choose an option from the Management Frame Protection (MFP) drop-down list whether you want the WAP to require to have protected frames or not. To learn more about MFP, click [here](#). The options are:

- Not Required — Disables the client support for MFP.
- Capable — Allows both MFP-capable and clients that do not support MFP to join the network. This is the default MFP setting on the WAP.
- Required — Clients are allowed to associate only if MFP is negotiated. If the devices do not support MFP, they are not allowed to join the network.

**Note:** For this example, Capable is chosen.



Step 8. Enter the WPA encryption key in the *Key* field. The key must be 8-63 characters long. This is a combination of letters, numbers, and special characters. It is the password that is used when connecting to the wireless network for the first time. Then, skip to [Step 18](#).



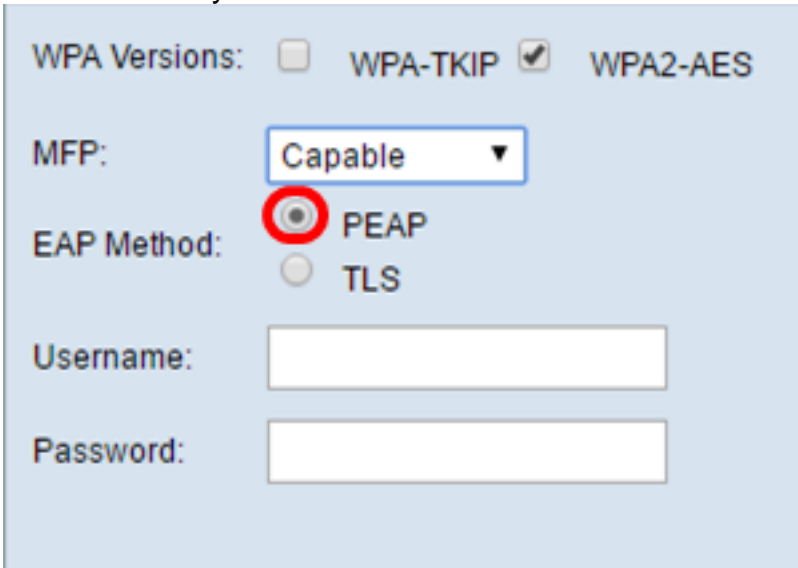
[Step 9](#). If you chose WPA Enterprise in Step 5, click a radio button for the EAP Method.

The available options are defined as follows:

- PEAP —This protocol 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 Wi-Fi security is based on the device credentials of the client. PEAP can pose a potentially serious security risk if you have weak passwords or unsecured clients. It relies on TLS but avoids the installation of digital certificates on every client. Instead, it provides authentication through a username and password.

- TLS — 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.



WPA Versions:  WPA-TKIP  WPA2-AES

MFP: Capable ▼

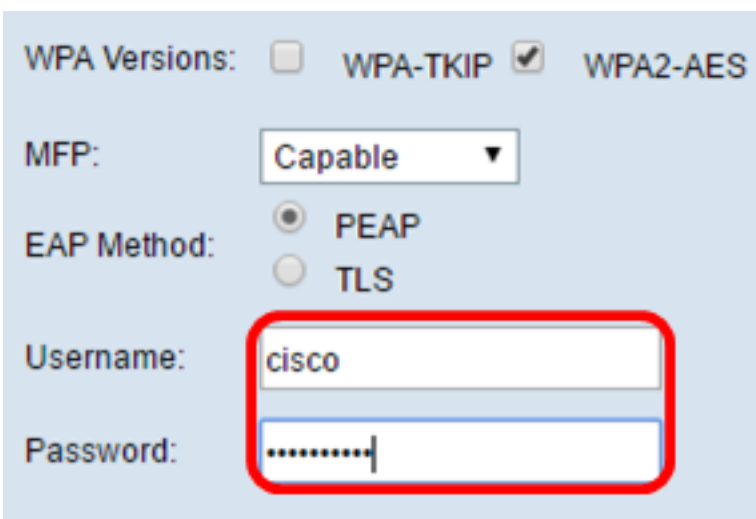
EAP Method:  PEAP  TLS

Username:

Password:

**Note:** For this example, PEAP is chosen.

Step 10. Enter the username and password for the infrastructure client in the *Username* and *Password* fields. 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. Then, skip to [Step 18](#).



WPA Versions:  WPA-TKIP  WPA2-AES

MFP: Capable ▼

EAP Method:  PEAP  TLS

Username: cisco

Password: .....

Step 11. If you clicked TLS in Step 9, enter the identity and private key of the infrastructure client in the *Identity* and *Private Key* fields.

WPA Versions:  WPA-TKIP  WPA2-AES

MFP:

EAP Method:  PEAP  TLS

Identity:

Private Key:

Certificate File Present:

Certificate Expiration Date:

Transfer Method:  HTTP  TFTP

Certificate File:  No file chosen

[Step 12.](#) In the transfer method area, click a radio button of the following options:

- TFTP — Trivial File Transfer Protocol (TFTP) is a simplified unsecured version of File Transfer Protocol (FTP). It is mainly used to distribute software or authenticate devices among corporate networks. If you clicked TFTP, skip to [Step 15](#).
- HTTP — Hypertext Transfer Protocol (HTTP) provides a simple challenge-response authentication framework that can be used by a client to provide authentication framework.

WPA Versions:  WPA-TKIP  WPA2-AES

MFP:

EAP Method:  PEAP  TLS

Identity:

Private Key:

Certificate File Present:

Certificate Expiration Date:

Transfer Method:  HTTP  TFTP

Certificate File:  No file chosen

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

## HTTP

Step 13. Click the **Choose File** 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.

**Note:** In this example, mini\_httpd(2).pfx is chosen.

Transfer Method:  HTTP  TFTP

Filename:  mini\_httpd (2).pfx

Step 14. Click **Upload** to upload the selected certificate file. Skip to [Step 18](#).



Transfer Method:  HTTP  TFTP

Filename  mini\_httpd (2).pfx

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

WPA Versions:  WPA-TKIP  WPA2-AES

MFP:

EAP Method:  PEAP  TLS

Identity

Private Key

Certificate File Present:

Certificate Expiration Date:

Transfer Method:  HTTP  TFTP

Certificate File:  No file chosen

## TFTP

[Step 15](#). If you clicked TFTP in [Step 12](#), enter the filename of the certificate file in the *Filename* field.

**Note:** In this example, mini\_httpd.pem is used.

Transfer Method:  HTTP  TFTP

Filename:

TFTP Server IPv4 Address:

Step 16. Enter the TFTP Server address in the *TFTP Server IPv4 Address* field.

**Note:** In this example, 192.168.1.20 is used as the TFTP Server address.

Transfer Method:  HTTP  TFTP

Filename:

TFTP Server IPv4 Address:

Step 17. Click the **Upload** button to upload the specified certificate file.

Transfer Method:  HTTP  TFTP

Filename:

TFTP Server IPv4 Address:

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

WPA Versions:  WPA-TKIP  WPA2-AES

EAP Method:  PEAP  TLS

Identity:

Private Key:

Certificate File Present:

Certificate Expiration Date:

Transfer Method:  HTTP  TFTP

Filename:

TFTP Server IPv4 Address:

[Step 18.](#) Enter the VLAN ID for the infrastructure client interface. The default is 1.

**Note:** For this example, the default VLAN ID is used.

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

Connection Status: Disconnected

## Access Point Interface

Step 1. Check the **Enable** Status check box to enable bridging on the access point interface.

**Access Point Interface**

Status:  Enable

SSID:  (Range: 2-32 Characters)

SSID Broadcast:  Enable

Security:

MAC Filtering:

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

Step 2. Enter the SSID for the access point in the *SSID* field. The SSID length must be between 2 to 32 characters. The default is Access Point SSID.

**Note:** For this example, the SSID used is bridge\_lobby.

**Access Point Interface**

Status:  Enable

SSID:  (Range: 2-32 Characters)

SSID Broadcast:  Enable

Security:  (+)

MAC Filtering:  ▾

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

Step 3. (Optional) If you do not want to broadcast the SSID, uncheck the **Enable SSID Broadcast** check box. 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. SSID Broadcast is enabled by default.

**Access Point Interface**

Status:  Enable

SSID:  (Range: 2-32 Characters)

SSID Broadcast:  Enable

Security:  (+)

MAC Filtering:  ▾

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

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

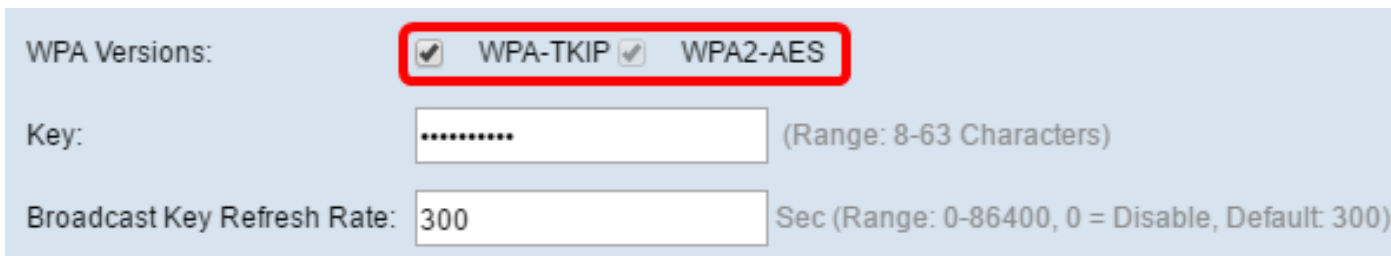
The available options are defined as follows:

- None — Open or no security. This is the default value. Skip to [Step 10](#) if you choose this.
- WPA Personal — Wi-Fi Protected Access (WPA) Personal can support keys of 8 to 63 characters long. The encryption method is either 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 Temporal Key Integrity Protocol (TKIP) that uses only a 64-bit RC4 standard.

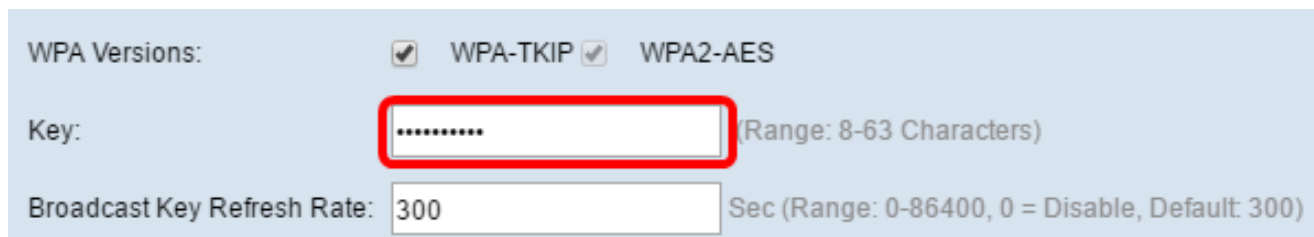


Step 5. Check the **WPA-TKIP** or **WPA2-AES** check box to determine which kind of WPA encryption the access point interface will use. These are enabled by default.

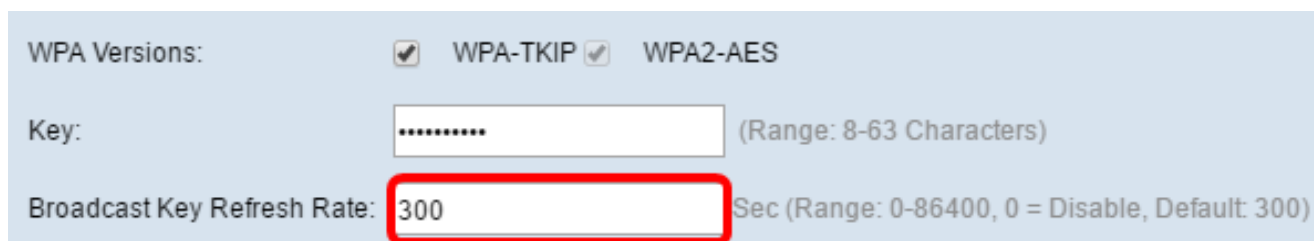
**Note:** If all of your wireless equipment support WPA2, then set the infrastructure client security to WPA2-AES. The encryption method is RC4 for WPA and Advanced Encryption Standard (AES) for WPA2. WPA2 is recommended as it has a more powerful encryption standard. For this example, WPA2-AES is used.



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* field. 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.

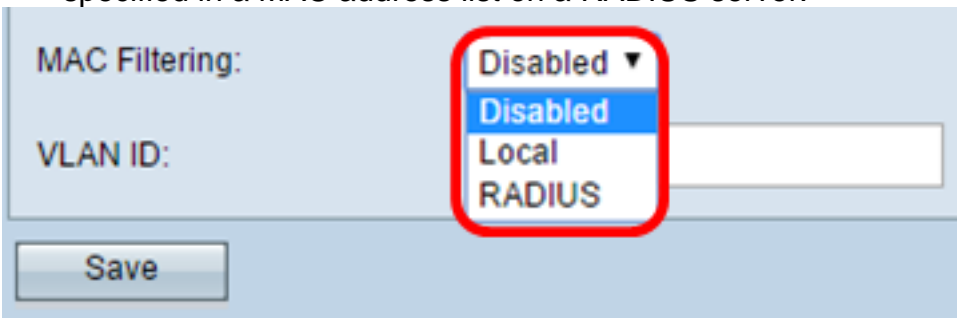


Step 8. Choose the type of MAC filtering you wish to configure for the access point interface from the MAC Filtering drop-down list. When enabled, users are granted or denied access to the WAP based on the MAC address of the client they use.

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.



MAC Filtering: Disabled ▾  
Disabled  
Local  
RADIUS

VLAN ID:

Save

**Note:** For this example, Disabled is chosen.

Step 9. Enter the VLAN ID in the *VLAN ID* field for the access point 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.

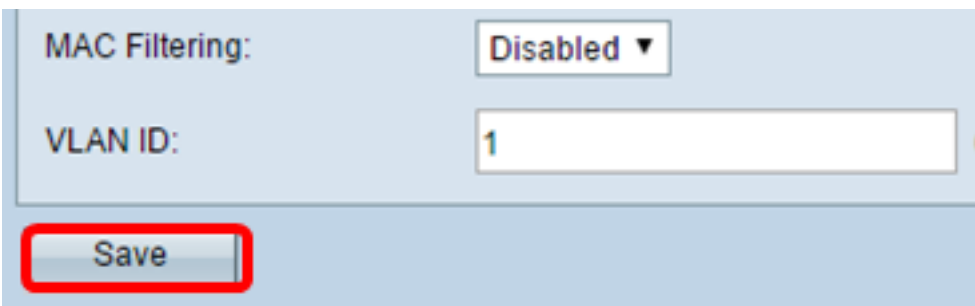


MAC Filtering: Disabled ▾

VLAN ID:

Save

[Step 10.](#) Click **Save** to save your changes.



MAC Filtering: Disabled ▾

VLAN ID:

Save

You should now have successfully configured a WorkGroup Bridge on a Wireless Access Point.