

# Personal Pre-Shared Key Feature in CBW Access Point

## Objective

This article will explain the personal pre-shared key (PSK) feature in Cisco Business Wireless (CBW) Access Point (AP) firmware version 10.6.1.0.

## Applicable Devices | Software Version

- Cisco Business Wireless 140AC Access Point | 10.6.1.0 ([Download latest](#))
- Cisco Business Wireless 145AC Access Point | 10.6.1.0 ([Download latest](#))
- Cisco Business Wireless 240AC Access Point | 10.6.1.0 ([Download latest](#))

## Introduction

If you have CBW gear in your network, you can now use the personal PSK feature in firmware version 10.6.1.0!

Personal PSK, also referred to as Individual PSK (iPSK), is a feature that allows an administrator to issue unique pre-shared keys to individual devices for the same Wi-Fi Protected Access II (WPA2) personal Wireless Local Area Network (WLAN). The unique PSK is tied to the MAC address of the device. This is not supported in WLANs where WPA3 policy is enabled.

This feature authenticates the client using a RADIUS Server. It is generally intended for use by IoT devices and company issued laptops and mobile devices.

## Table of Contents

- [Prerequisites](#)
- [Configure CBW RADIUS Settings](#)
- [Configure WLAN Settings](#)
- [Next Steps](#)

## Prerequisites

- Make sure you have upgraded the CBW AP firmware to 10.6.1.0. [Click if you would like step-by-step instructions on doing a firmware update.](#)
- You will require a RADIUS server where the personal PSK and the MAC address of the device need to be configured.
- This CBW feature is supported with three different RADIUS servers - FreeRADIUS, Microsoft's NPS, and Cisco's ISE. The configuration will vary depending on the RADIUS server used.

## Configure CBW RADIUS Settings

To configure the RADIUS settings on the CBW AP, follow the steps.

### Step 1

Login to the web user interface (UI) of the CBW AP.



## Cisco Business Wireless Access Point

Welcome! Please click the login button to enter your user name and password



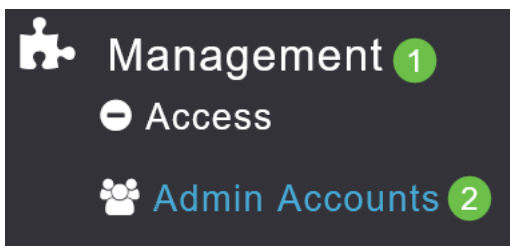
### Step 2

Click the **bi-directional arrow** symbol to switch to expert view.



### Step 3

Navigate to **Management > Admin Accounts**.



### Step 4

Select the **RADIUS** tab.

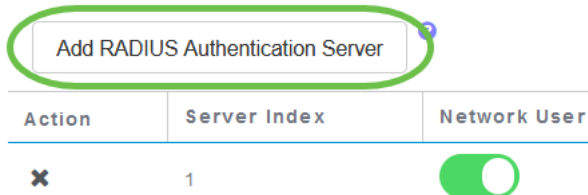
## Admin Accounts


 Users 8

Management User Priority Order Local Admin Accounts TACACS+ **RADIUS** Auth Cached Users

### Step 5

Click on **Add RADIUS Authentication Server**.



Action	Server Index	Network User
	1	<input checked="" type="checkbox"/>

### Step 6

Configure the following:

- *Server Index* - Select 1 through 6
- *Network User* - Enable the state. By default, this is Enabled
- *Management* - Enable the state. By default, this is Enabled
- *State* - Enable the state. By default, this is Enabled
- *CoA* – Make sure charge of authority (CoA) is enabled.
- *Server IP Address* - Enter the IPv4 address of the RADIUS server
- *Shared Secret* - Enter the shared secret key
- *Port Number* - Enter the port number being used for communicating with the RADIUS server.
- *Server Timeout* - Enter the server timeout

Click **Apply**.

## Add/Edit RADIUS Authentication Server.

Server Index

Network User

Management

State

CoA

Server IP Address

Shared Secret

Confirm Shared Secret

Show Password

Port Number

Server Timeout  Seconds

2

Apply

Cancel

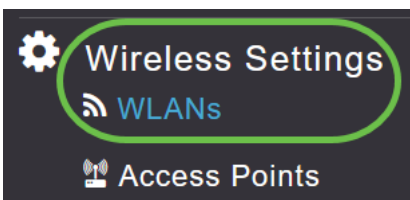
## Configure WLAN Settings

Create a WLAN as a standard WPA2 Personal Secured WLAN.

The pre-shared key will not be used for the personal PSK devices. This would only be used for devices that are NOT authenticated on the RADIUS server. You would need to add the MAC addresses of ANY device that will be connecting to this WLAN to the allow-list of this device.

### Step 1

Navigate to **Wireless Settings > WLANs**.



### Step 2

Click on **Add new WLAN/RLAN**.

## WLANs



Active WLANs

5

Add new WLAN/RLAN

Action

Active

### Step 3

Under *General* tab, enter a *Profile Name* for the WLAN.

### Add new WLAN

1

General **WLAN Security** VLAN & Firewall Traffic Shaping Advanced Scheduling

WLAN ID 4

Type WLAN

Profile Name \* Personal 2

SSID \* Personal

WLANs with same SSID can be configured, unless layer-2 security settings are different.

Enable

Radio Policy ALL ?

Broadcast SSID

Local Profiling  ?

Apply Cancel

### Step 4

Navigate to **WLAN Security** tab and enable **MAC Filtering** by sliding the toggle.

**Guest Network**

**Captive Network Assistant**

**MAC Filtering**  ? 2

**Security Type** WPA2/WPA3 Personal ▼

**WPA2**  **WPA3**

**Passphrase Format** ASCII ▼

**Passphrase \***

**Confirm Passphrase \***

Show Passphrase

**Password Expiry**  ?

### Step 5

Click on **Add RADIUS Authentication Server** to add the RADIUS server that was configured in the previous section to provide authentication for this WLAN.

#### RADIUS Server

**Authentication Caching**

**Add RADIUS Authentication Server**

### Step 6

A pop-up window will appear. Enter the *Server IP Address*, *State*, and *Port Number*. Click **Apply**.

## Add RADIUS Authentication Server

Radius Server can be configured from 'Admin Accounts > RADIUS'(Expert view).

Server IP Address

State  1

Port Number

2

### Step 7

(Optional)

Enable *Authentication Caching*. When you enable this option, the following fields are displayed.

- *User Cache Timeout* - Specifies the time period at which the authenticated credential in the cache expires.
- *User Cache Reuse* - Use the credentials cache information before cache timeout. By default, this is disabled.

Authentication Caching

User Cache Timeout  minutes

User Cache Reuse

If this feature is enabled, a client who has already been authenticated to this server will not be required to pass data to the RADIUS server when they re-connect to this WLAN within the next 24 hours.

### Step 8

Navigate to the Advanced tab. Enable **Allow AAA Override** by sliding the toggle.

## Add new WLAN

General WLAN Security VLAN & Firewall Traffic Shaping **Advanced** Scheduling

Allow AAA Override



802.11r

Disabled (Default)

The *Advanced* tab will be visible only if you are in *Expert View*.

## Next Steps

Once you have configured the settings on your CBW AP and set up your RADIUS server, you should be able to connect your device. Enter the custom PSK configured for that MAC address, and it will join the network.

If you have configured authentication caching, you will be able to see the devices that have joined the WLAN by going to the *Auth Cached Users* tab under *Admin Accounts*. If needed, this can be deleted.

The screenshot shows the configuration interface for a Cisco Business Wireless 240AC Access Point. The left sidebar contains a navigation menu with the following items: Monitoring, Wireless Settings, Management, Access, Admin Accounts (circled in green with a '1'), Time, Software Update, Services, and Advanced. The main content area is titled 'Admin Accounts' and shows 'Users 2'. Below this, there are tabs for 'Management User Priority Order', 'Local Admin Accounts', 'TACACS+', and 'RADIUS'. The 'Auth Cached Users' tab is selected and circled in green with a '2'. Below the tabs, there is a search bar with the placeholder text 'MacAddress/Username/ssid' and a 'Delete Selected' button. A table displays the following data:

	Mac Address	Username	SSID	Timeout(Minutes)	RemainingTime(Minut...
<input checked="" type="checkbox"/>	98:c:5e	98:c:5e	Personal	1440	1425

## Conclusion

There you go! You can now enjoy the benefits of personal PSK feature on your CBW AP.