

# Wireless Authentication using Cisco Business Dashboard

## Objective

The objective of this article is to go over wireless authentication feature using the Cisco Business Dashboard (CBD) version 2.5.0.

## Applicable Devices | Software Version

- Cisco Business Dashboard | 2.5.0 ([Download latest](#))
- CBW140AC | [Download latest](#)
- CBW145AC | [Download latest](#)
- CBW240AC | [Download latest](#)
- CBW150AX | [Download latest](#)

## Introduction

CBD provides tools that help you monitor and manage the devices in your Cisco Business network. It automatically discovers your network and allows you to configure and monitor all supported devices such as switches, routers, and wireless access points.

CBD 2.5.0 adds Authentication service functionality to CBD. The new service is supported on both CBW140/240 series and CBW 150AX devices.

It sets up a FreeRADIUS instance on the CBD manager to use for RADIUS authentication, giving your organization a simple way to deploy a server without clients having to know or understand RADIUS.

If you are ready to get started, let us dive in.

## Table of Contents

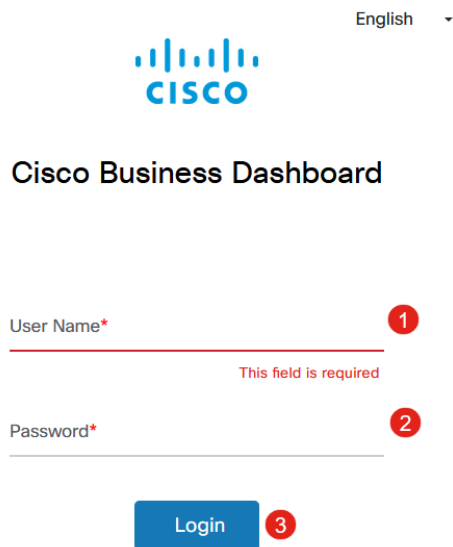
- [Configure Authentication Profile](#)
- [Configure Wireless Networks](#)
- [Verification](#)
- [Testing](#)

## Configure Authentication Profile

First, you must configure the authentication profile you will use for your organization. In many cases you can simply use the default profile.

## Step 1

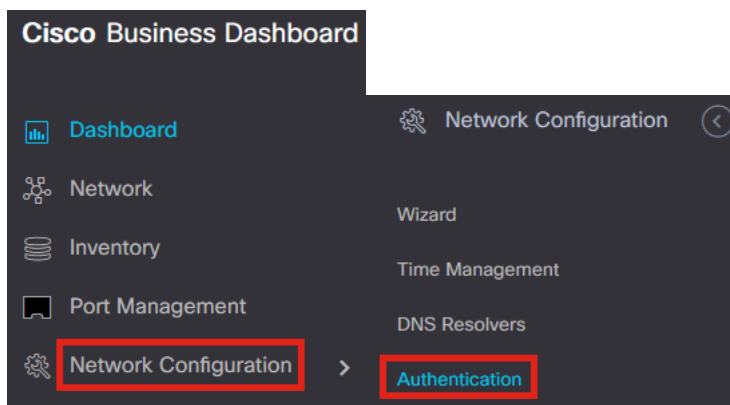
Login to CBD.



The image shows the Cisco Business Dashboard login page. At the top right, there is a language dropdown menu set to "English". Below it is the Cisco logo. The main heading is "Cisco Business Dashboard". There are two input fields: "User Name\*" and "Password\*", both marked with a red asterisk and a red circle containing the number 1 and 2 respectively. Below the "User Name" field is a red error message: "This field is required". Below the "Password" field is a red circle containing the number 2. At the bottom, there is a blue "Login" button with a red circle containing the number 3 next to it.

## Step 2

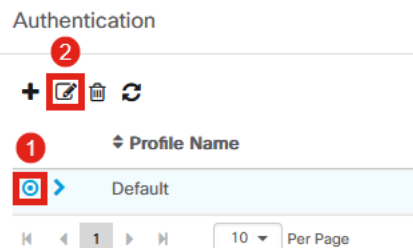
Navigate to **Network Configuration > Authentication**.



## Step 3

You can either edit the existing *Default* profile or add another profile. In this example, the **Default** profile is selected. Click **Edit**.

☰ Cisco Business Dashboard



## Step 4

In CBD 2.5.0, there is a new option to select *Use Cisco Business Dashboard Authentication Service*. This is checked by default. Make the desired changes and click

# Update.

## Authentication->Update Default

### Device Group Selection

Profile Name

Organization


Device Groups

Available Groups		Selected Groups
Branch 1	>	Default
	<	
	>>	
	<<	

### Authentication

#### Local User Authentication

 Existing local users on devices will be replaced by the users below if there is at least one user specific


 Add local user


#### Authentication Servers

 Existing authentications servers on devices will be replaced by the list below

Use Cisco Business Dashboard Authentication Service

Please ensure that the [System > Platform Settings > System Variables](#) contain the correct settings to allow the dashboard to be reached by the network devices.

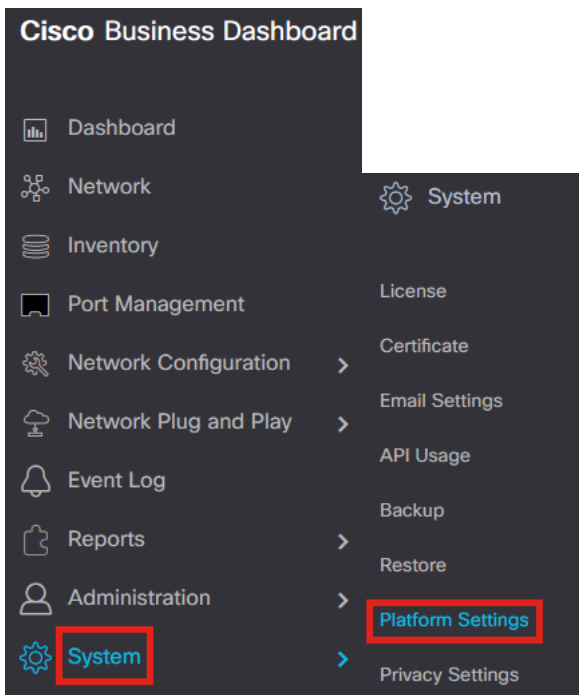
 Add custom authentication server



Make sure to see if *System > Platform Settings > System Variables* have the correct settings to allow the Dashboard to be reached by the network devices.

## Step 5

Navigate to **System > Platform Settings** in the menu.



## Step 6

Select the **System Variables** tab.

Platform Settings

Network Settings   Web Server   **System Variables**

## Step 7

Check the settings to ensure that the *External Dashboard IP Address* is the public IP address of the CBD and the *External Authentication Server Port* is 1812. This is the default port. Click **Save**.

Platform Settings

Network Settings   Web Server   **System Variables**

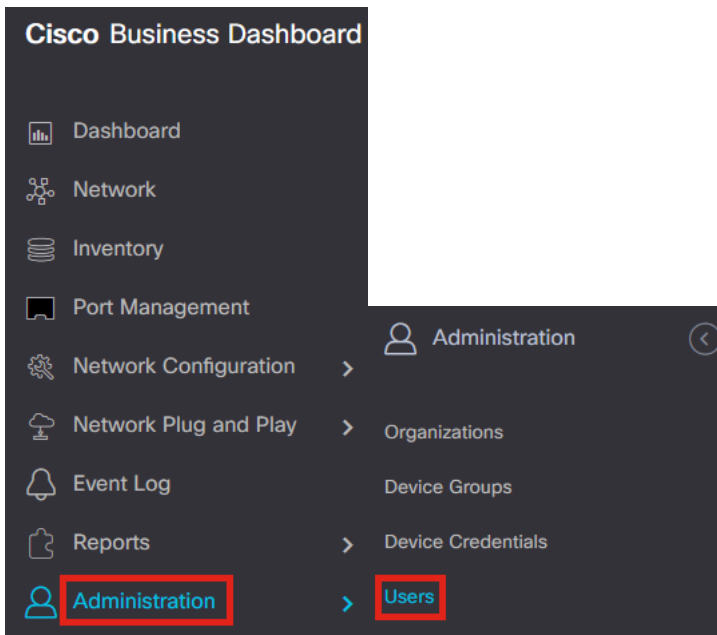
External System Settings

External Dashboard Hostname ?	<input type="text" value="cbd2.sbcenter.net"/>
External Dashboard IP Address ?	<input type="text" value="3. . 254"/> 1
External Dashboard IPv6 Address ?	<input type="text" value="fe80::854:18ff:fe36:9c00"/>
External Dashboard HTTP Port ?	<input type="text" value="80"/>
External Dashboard HTTPS Port ?	<input type="text" value="443"/>
External Authentication Server Port ?	<input type="text" value="1812"/> 2
	<input type="button" value="Save"/> 3

## Step 8

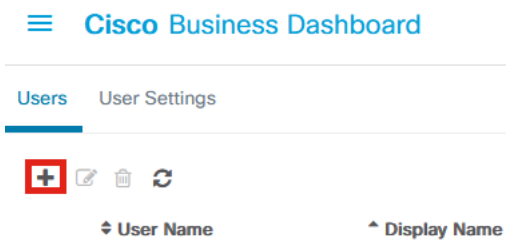
To create users that are going to be authenticating to the system, go to

## Administration > Users.



### Step 9

To add users, click on the **plus icon**.



### Step 10

Configure the following:

- *User Name*
- *Display Name*
- *Email*
- *Dashboard Access* – select from the dropdown menu. In this example, **No Access** is selected.
- *New Password*
- *Retype New Password*

The other fields are optional. Click **Save**.

User Name	<input type="text" value="user1"/>
Display Name	<input type="text" value="User 1"/>
Email	<input type="text" value="user1@sbcenter.net"/>
Dashboard Access	<input type="text" value="No Access"/>
Network Access	<input checked="" type="checkbox"/>
New Password	<input type="password" value="••••••"/>
Retype New Password	<input type="password" value="••••••"/>
Password Strength	<span style="display: inline-block; width: 10px; height: 10px; background-color: orange; border: 1px solid orange;"></span> <span style="display: inline-block; width: 10px; height: 10px; background-color: orange; border: 1px solid orange;"></span> <span style="display: inline-block; width: 10px; height: 10px; background-color: gray; border: 1px solid gray;"></span> <span style="display: inline-block; width: 10px; height: 10px; background-color: gray; border: 1px solid gray;"></span> Normal
Address	<input type="text"/>
City	<input type="text"/>
Country/region	<input type="text" value="United States"/>
ZIP or Postal Code	<input type="text"/>
Phone	<input type="text" value="+1"/>
	<input type="button" value="Save"/> <input type="button" value="Cancel"/>

## Step 11

Click on the **Organizations** tab.

### Cisco Business Dashboard

User Name	<input type="text" value="user1"/>
	<a href="#">Reset password</a>
Display Name	<input type="text" value="User 1"/>
Email	<input type="text" value="user1@sbcenter.net"/>
Dashboard Access	<input type="text" value="No Access"/>
Network Access	<input checked="" type="checkbox"/>
User Type	Local
	<a href="#">Show account settings</a>
Create Time	Jul 5 2022 09:31
Last Password Changed Time	Jul 5 2022 09:31
Last Login	Never
	<input type="button" value="Save"/> <input type="button" value="Cancel"/>

Access Key **Organizations**

## Step 12

Here, you need to associate the user you just created with your CBD organization. Click the **plus icon** and choose the option from the dropdown menu. In this example, **Default** is selected.

Access Key **Organizations**

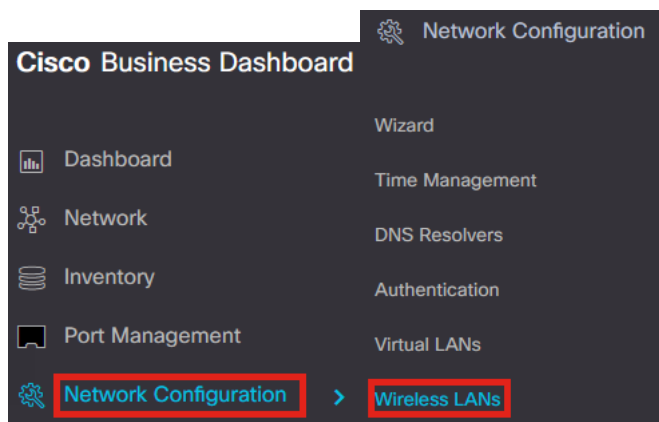
<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	▼ Org Name
<input type="checkbox"/>	Default

This user will now be able to login to the Default organization configured for wireless authentication.

# Configure Wireless Networks

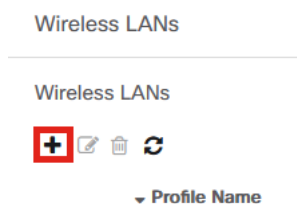
## Step 1

Navigate to **Network Configuration > Wireless LANs** menu.



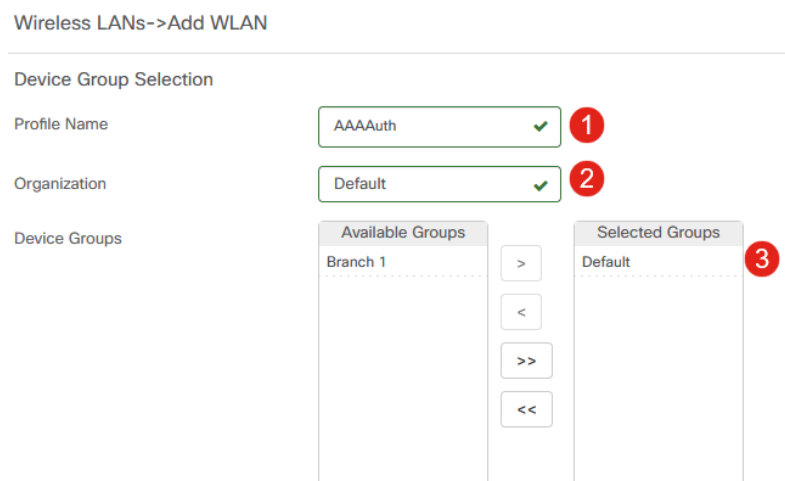
## Step 2

To create a new profile, click on the **plus icon** under *Wireless LANs*.



## Step 3

Enter the *Profile Name*, *Organization* and configure *Device Groups* to apply the settings to the wireless devices in the group.



## Step 4

To create an SSID, click the **plus icon**.



SSID Name

## Step 5

Enter the *SSID Name*, *VLAN ID* and select *Security* from the dropdown menu. In this example, **WPA2-Enterprise** is selected. Click **Save**.

Add Wireless LANs ×

Enable

SSID Name  ✓ **1**

VLAN ID  ✓ **2**

Security  **3**

An authentication server is required for enterprise authentication to work. Authentication servers may be set in [Network Configuration > Authentication](#). If you do not configure an authentication server, the Dashboard authentication service will be used.

▼ Advanced Settings

Broadcast

Application Visibility

Local Profiling

Radio

**4**

Cisco Business Dashboard Authentication Server will be used if you do not have an authentication server configured.

## Step 6

Click **Save** again to apply the wireless network and Radius settings to all the clients.

Wireless LANs-->Add WLAN

Device Group Selection

Profile Name  ✓

Organization  ✓

Device Groups

Available Groups  
Branch 1

Selected Groups  
Default

Wireless LANs

SSID Name	VLAN ID	Enable	Security	Action
AAATest	1	Yes	WPA2-Enterprise	



# Verification

To check if the settings have been applied,

## Step 1

Login to your CBW AP.



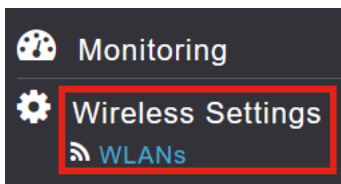
## Cisco Business Wireless Access Point

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



## Step 2

Go to **Wireless Settings > WLANs**.



## Step 3

The SSID that you created will be listed. In this example, it is **AAATest**.

WLANs

Active WLANs 2

Add new WLAN/RLAN

Action	Active	Type	Name	SSID	Security Policy	Radio Policy
<input checked="" type="checkbox"/> ✕	Enabled	WLAN	CBWireless	CBWireless	Personal(WPA2)	ALL
<input checked="" type="checkbox"/> ✕	Enabled	WLAN	AAATest	AAATest	WPA2Enterprise	ALL

## Step 4

Select the SSID and click **edit** to view the settings.

WLANs

Active WLANs 2

Add new WLAN/RLAN

Action	Active	Type	Name
	Enabled	WLAN	CBWireless
	Enabled	WLAN	AAATest

## Step 5

Navigate to **WLAN Security** tab.

Edit WLAN

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

You will see that the *Security Type* will be listed as **WPA2 Enterprise** and *Authentication Server* will be the **External Radius**. The *Server IP Address* will be the one you configured earlier.

Edit WLAN

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

Guest Network

Captive Network Assistant

MAC Filtering  ?

Security Type WPA2 Enterprise

Authentication Server External Radius ?

No Radius Server is configured for Accounting. Radius Server can be configured from 'Admin Accounts > RADIUS'(Expert view)

Radius Profiling  ?

BYOD

RADIUS Server

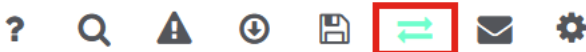
Authentication Caching

Add RADIUS Authentication Server

State	Server IP Address	Port
Enabled	3.254	1812

## Step 6

Switch to **Expert view** by clicking the bi-directional arrow at the top of the user interface.



## Step 7

Navigate to **Management > Admin Accounts**.

Management 1

Access


Admin Accounts 2

Time

## Step 8

Click on the **RADIUS** tab.

Admin Accounts



 **Users** 1

---

[Management User Priority Order](#) [Local Admin Accounts](#) [TACACS+](#) **[RADIUS](#)** [Auth Cached Users](#)

You will see that the Radius authentication server has been configured for *Network User*.

[Add RADIUS Authentication Server](#) <sup>?</sup>









Action	Server Index	Network User	Management	State	Server IP Address	Shared Key	Port
 	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3.1.254	*****	1812

## Testing

To test the settings:

### Step 1


Navigate to **Advanced > Primary AP Tools**.

-  **Advanced** <sup>1</sup>
-  SNMP
-  Logging
-  RF Optimization
-  RF Profiles
-  **Primary AP Tools** <sup>2</sup>
-  Security Settings
-  CBD Settings

### Step 2

Click on **Troubleshooting Tools** tab.

Primary AP Tools

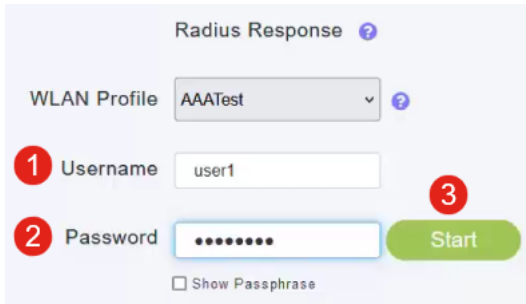
 **Tools**

---

[Restart Primary AP](#) [Configuration Management](#) [Troubleshooting Files](#) **[Troubleshooting Tools](#)** [Upload File](#)

### Step 3

Under the *Radius Response* section, enter the **Username** and **Password** and click **Start** to see if it authenticates against the Radius server.



The screenshot shows the 'Radius Response' configuration page. At the top, there is a 'WLAN Profile' dropdown menu set to 'AAATest'. Below it are two input fields: 'Username' with the value 'user1' and 'Password' with masked characters. A green 'Start' button is positioned to the right of the password field. Red numbered callouts (1, 2, and 3) point to the Username field, Password field, and Start button respectively. A 'Show Passphrase' checkbox is located at the bottom left of the form.

You will see an *Authentication success* notification after the test is completed.



This screenshot shows the same 'Radius Response' configuration page after the test. The 'Start' button is now highlighted with a green background. A blue notification bar with a green checkmark icon is displayed at the bottom right, containing the text 'Authentication success (3.1 254)'. A red rectangular box highlights the notification bar. The 'Show Passphrase' checkbox remains at the bottom left.

Make sure you have IP connectivity between the CBD Manager and client system for this to work properly.

## Conclusion

That's it! You do not have to worry anymore about configuring Radius on your own. CBD will do all the work and you can sit back, relax, and enjoy the benefits of wireless authentication in your network.