

External Captive Portal in Cisco Business Dashboard

Objective

The objective of this article is to go over the steps to configure the external Captive Portal feature in Cisco Business Dashboard (CBD) version 2.5.1 and later.

Applicable Devices | Software Version

Cisco Business Dashboard | 2.5.1 ([Download latest](#))

CBW140 Series | 10.8.1.0 ([Download latest](#))

CBW150 Series | 10.3.2.0 ([Download latest](#))

Introduction

CBD version 2.5.1 has implemented an external Captive Portal page for CBW140 and CBW150 series networks. This can be used as a guest network authentication page and offers several advantages over local captive portal pages.

Instead of redirecting the client to the local Captive Portal Page at 192.0.2.1, it redirects to CBD using the CBD's FQDN and SSL certificate. This avoids triggering the enhanced HTTP Strict Transport Security (HSTS) that modern browsers have implemented.

The external Captive Portal page has a simplified deployment that makes it easy to manage multiple sites with guest networks.

All the settings for the page and authentication policies are configured within CBD.

When you set up the guest network, it supports Web Consent, Email Address, and logging in CBD accounts or going to another RADIUS server.

Table of Contents

- [Guest Network Requirements](#)
- [Configure Guest Authentication](#)
- [Configure Wireless LAN](#)
- [CBW Guest Network Settings](#)
- [Captive Portal Page](#)

Guest Network Requirements

To use the new Guest Network Authentication page, you must have

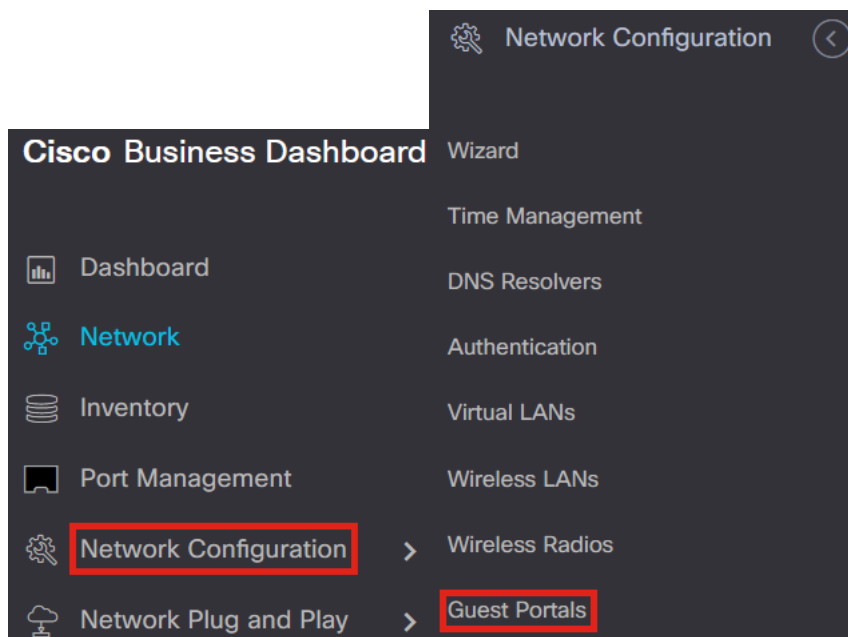
CBD version 2.5.1
CBW140 Series Firmware 10.8.1.0 (or later)
CBW150 Series Firmware 10.3.2.0 (or later)

Configure Guest Authentication

To configure the captive portal web page:

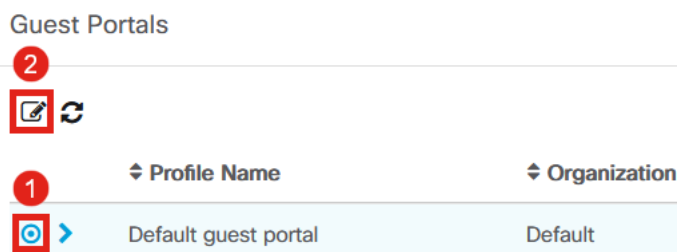
Step 1

Login to your CBD and navigate to **Network Configuration > Guest Portals**.



Step 2

The *Guest Portals* page shows each CBD Organization's web page. To edit a page, select the profile and press the edit button.



If you have two or more networks that need unique captive portal pages, you will need to set up separate CBD organizations and have each network join the separate organization.

Step 3

The configuration options include

- *Profile Name* - It is a unique identifier within CBD so you can easily keep track of what page goes with each organization.
- *Organization* - Shows what organization the captive portal is connected to.
- *Header Text* - Shows the header that will be displayed by the web browser.
- *Background Image* and *Logo Image* show where you can drag and drop in graphics to be displayed on your captive portal page.
- The foreground, background, separator, content foreground, content background, and account tips background color fields all allow you to change the color of the respective aspects of your display.
- The *Fonts* menu allows you to choose the font used on the captive portal page.
- The other fields allow you to edit the text that displays on the page.

The screenshot displays a configuration page for a captive portal. It is divided into several sections:

- Device Group Selection:** Profile Name (Default guest portal), Organization (Default).
- Web Portal Customization:** Header Text (Web Portal Guest Access), Background Image (background.png), Logo Image (loginlogo.png), Foreground Color, Background Color.
- Color and Font Settings:** Separator Color, Content Foreground Color, Content Background Color, Account Tips Background Color, Fonts (Arial), Button Label (Connect), Browser Header Text (Captive Portal).
- Authentication Messages:** Portal Title (Welcome to the Wireless Network), Acceptable Use Policy (Acceptance Use Policy).
- Message Previews:** A series of preview boxes on the right showing how messages will appear:
 - Acceptance Prompt: "Check here to indicate that you have read and accepted the Acceptance Use Policy"
 - No Acceptance Warning: "Error: You must acknowledge the Acceptance Use Policy before connecting!"
 - Work In Progress Message: "Connecting, please be patient..."
 - Invalid Credentials Message: "Error: Invalid Credentials, please try again!"
 - Connection Succeeded Message: "Congratulations!"
 - Welcome Message: "You are now authorized and"

Step 4

Click on one of the following tabs to configure the text options for authentication.

- Username/Password
- Web Consent
- Email Address

Click the **Preview** button to see how each of the menu options will be displayed.

The screenshot shows the configuration interface with three tabs: **Username/Password**, **Web Consent**, and **Email Address**. The **Preview** button is highlighted with a red border.

Step 5

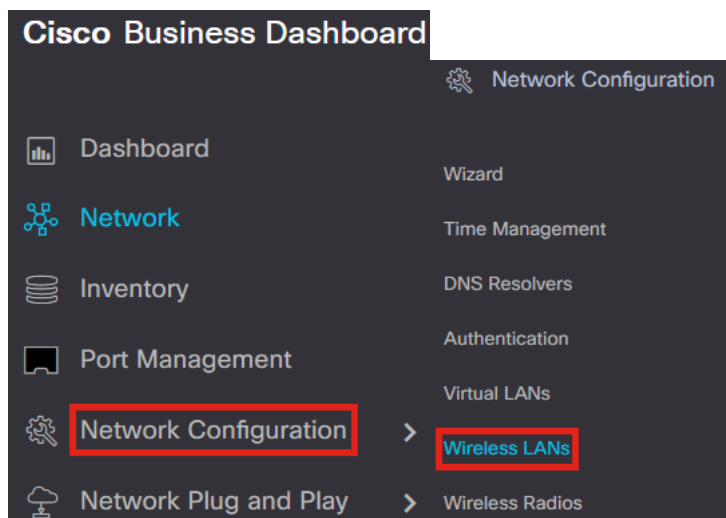
Once you have customized the web page, click on **Update** or *Cancel*.

The screenshot shows the 'Login Instructions' section with a preview box containing the text: "To start using this service, enter your credentials and click the connect button".

Configure Wireless LAN

Step 1

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



Step 2

You can either add or edit an existing *Wireless LANs* Profile. In this example, **add** is selected.

Wireless LANs

Wireless LANs



Step 3

Specify the *Profile Name*, *Organization*, and *Device Groups* within the organization that this will apply to.

Wireless LANs->Add WLAN

Device Group Selection

Profile Name

Training Test ✓ 1

Organization

Default ✓ 2

Device Groups

3

Available Groups		Selected Groups
Default	>	
	<	
	>>	
	<<	

You may simply choose the *Default* organization and the *Default* Device Group.

Step 4

Add a Wireless LAN by clicking the **plus** icon.

Wireless LANs



SSID Name

VLAN ID

Enable

Security

Action

Step 5

Specify *SSID Name* and *VLAN ID*. Choose **Guest** from the *Security* drop-down menu.

Add Wireless LANs ×

Enable

SSID Name ✓ 1

VLAN ID ✓ 2

Security 3

Step 6

Select the *Guest authentication* method. The options are:

- Username/Password
- Web Consent
- Email Address

Guest authentication

▼ Advanced Settings

Broadcast

Username/Password

Username/Password

Web Consent

Email Address

Step 7

Under *Advanced Settings*, you can also specify if you want the SSID to *Broadcast*, the *Application Visibility*, *Local Profiling*, and *Radio* settings.

▼ Advanced Settings

Broadcast

Application Visibility

Local Profiling

Radio

In most cases, you will leave these at the default setting.

Step 8

Click **Save**.

Add Wireless LANs ✕

Enable Enable

SSID Name ✓

VLAN ID ✓

Security

Guest authentication

▼ Advanced Settings

Broadcast Enable

Application Visibility Enable

Local Profiling Enable

Radio

Step 9

Click **Save** once again.

Wireless LANs->Add WLAN

Device Group Selection

Profile Name ✓

Organization ✓

Device Groups

Available Groups

Default

Selected Groups

Wireless LANs

+

SSID Name	VLAN ID	Enable	Security	Action
Guest Test	1	Yes	Guest (Username/Password)	

CBW Guest Network Settings

Step 1

Login to your Cisco Business Wireless (CBW) access point.

Cisco Business Wireless Access Point

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

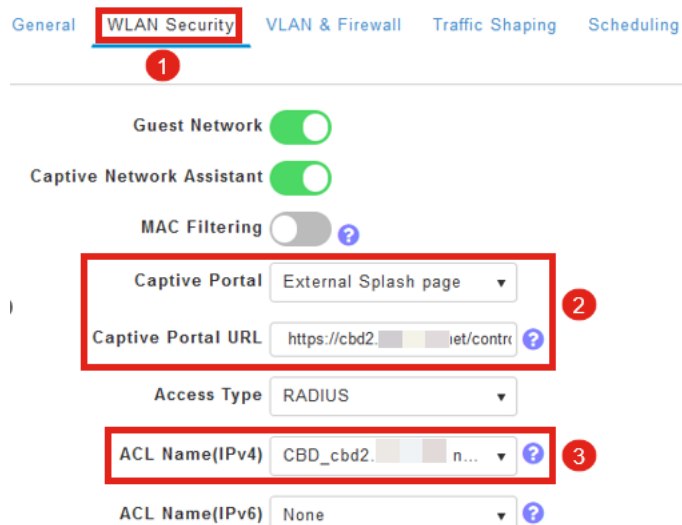


Step 2

Navigate to **Wireless Settings > WLANs**.

Step 3

You can edit the WLAN and go to the **WLAN Security** tab. The *Captive Portal* will be set to the **External Splash page** with the *Captive Portal URL* of your CBD server. The *ACL Name* will be automatically configured.



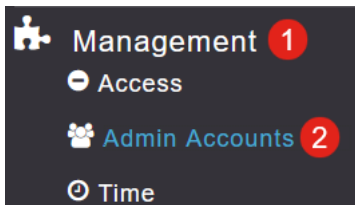
Step 4

The RADIUS server is automatically configured. To view it, switch to **Expert View** by clicking the bi-directional arrow at the top of the page.



Step 5

Navigate to **Management > Admin Accounts**.



Step 6

Click on the **RADIUS** tab.

Management User Priority Order Local Admin Accounts TACACS+ **RADIUS**

Auth Cached Users

Authentication Call Station ID Type AP MAC Address:SSID

Authentication MAC Delimiter Hyphen

Accounting Call Station ID Type IP Address

Accounting MAC Delimiter Hyphen

Fallback Mode Passive

Username cisco-probe

Interval 300 Seconds

AP Events Accounting

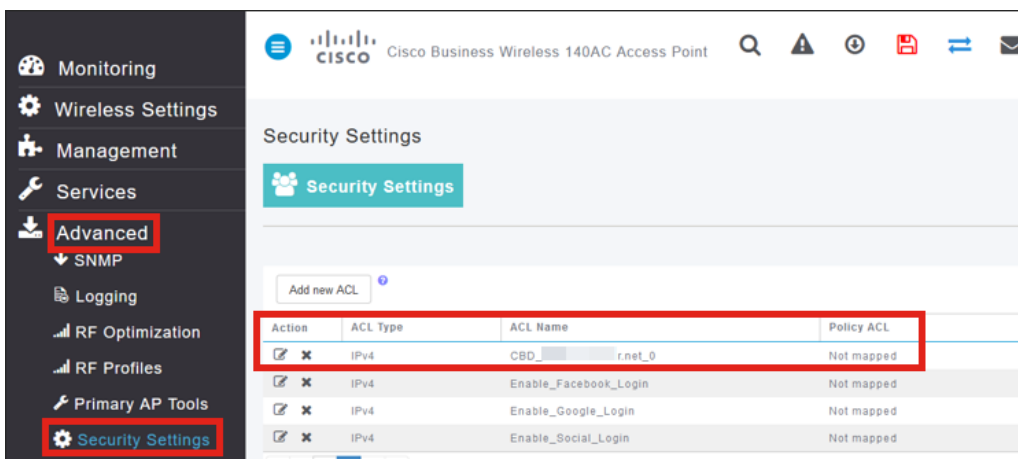
Apply

Add RADIUS Authentication Server

Action	Server Index	Network User	Management	State	Server IP A...	Shared Key	Port
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3	54	1812

Step 7


It will also dynamically add a security ACL for CBD under **Advanced > Security Settings**.



Captive Portal Page

Based on how you have configured the settings, the captive portal page will look like the following:

Username/Password Authentication

 Web Portal Guest Access

Welcome to the Wireless Network

To start using this service, enter your credentials and click the connect button

Username
Enter your Username/Password


Password
•••••••• ✓

Acceptable Use Policy

Check here to indicate that you have read and accepted the Acceptable Use Policy

Connect

Web Consent

 Web Portal Guest Access

Welcome to the Wireless Network


Please accept the Acceptable Use Policy

Acceptable Use Policy

Check here to indicate that you have read and accepted the Acceptable Use Policy

Connect

Email Authentication

 Web Portal Guest Access

Welcome to the Wireless Network

Please enter your email address to login

Email Address
Enter your Email Address

Acceptable Use Policy

Check here to indicate that you have read and accepted the Acceptable Use Policy

Connect

Conclusion

You did it! You have successfully set up the external Captive Portal page using CBD.