

Portal cautivo externo en Cisco Business Dashboard

Objetivo

El objetivo de este artículo es revisar los pasos para configurar la función de portal cautivo externo en Cisco Business Dashboard (CBD) versión 2.5.1 y posteriores.

Dispositivos aplicables | Versión de software

Panel empresarial de Cisco | 2.5.1 ([Descargar la última versión](#))

Serie CBW140 | 10.8.1.0 ([Descargar la última versión](#))

Serie CBW150 | 10.3.2.0 ([Descargar la última versión](#))

Introducción

La versión 2.5.1 de CBD ha implementado una página externa de portal cautivo para las redes de las series CBW140 y CBW150. Esto se puede utilizar como una página de autenticación de red de invitado y ofrece varias ventajas sobre las páginas del portal cautivo local.

En lugar de redirigir al cliente a la página local del portal cautivo en 192.0.2.1, dirige al CBD mediante el certificado FQDN y SSL del CBD. Esto evita activar la seguridad de transporte estricta HTTP (HSTS) mejorada que han implementado los navegadores modernos.

La página del portal cautivo externo cuenta con una implementación simplificada que facilita la administración de varios sitios con redes de invitados.

Todos los ajustes de la página y las políticas de autenticación se configuran en CBD.

Al configurar la red para invitados, admite el consentimiento web, la dirección de correo electrónico y el inicio de sesión en cuentas CBD o la conexión a otro servidor RADIUS.

Table Of Contents

- [Requisitos de red para invitados](#)
- [Configurar autenticación de invitado](#)
- [Configuración de LAN inalámbrica](#)
- [Configuración de red de invitado CBW](#)
- [Página Portal cautivo](#)

Requisitos de red para invitados

Para utilizar la nueva página Autenticación de red de invitado, debe tener

CBD versión 2.5.1

Firmware 10.8.1.0 (o posterior) de la serie CBW140

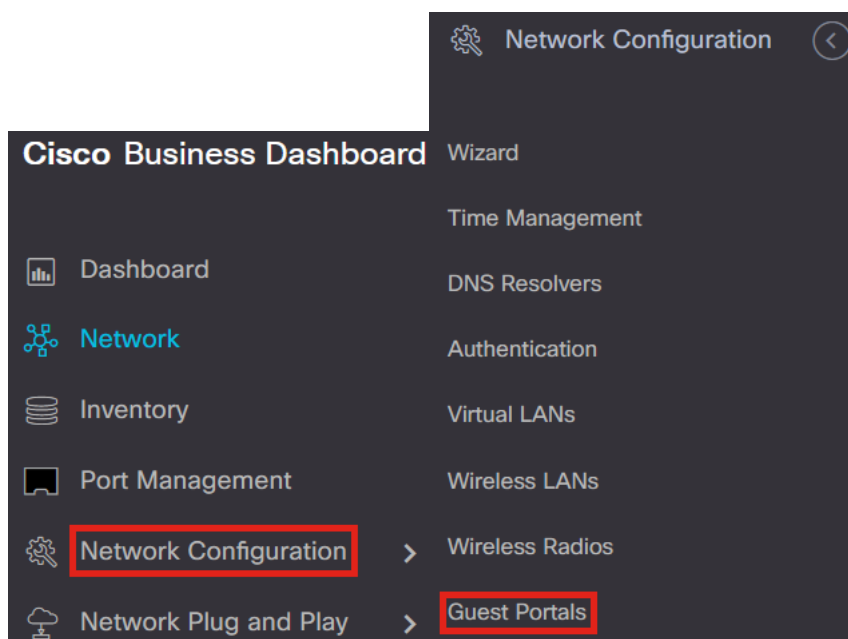
Firmware 10.3.2.0 (o posterior) de la serie CBW150

Configurar autenticación de invitado

Para configurar la página web del portal cautivo:

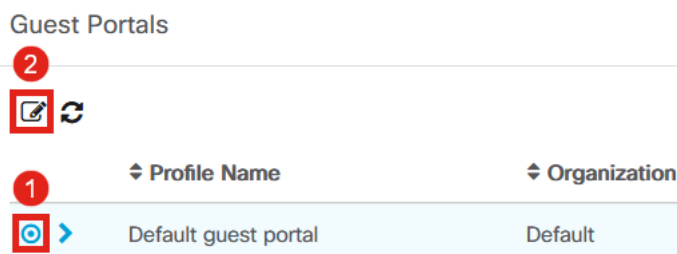
Paso 1

Inicie sesión en el CBD y navegue hasta **Network Configuration > Guest Portals**.



Paso 2

La página *Portales de Invitados* muestra la página web de cada organización CBD. Para editar una página, seleccione el perfil y pulse el botón de edición.



Si tiene dos o más redes que necesitan páginas de portal cautivas únicas, tendrá que configurar organizaciones CBD independientes y hacer que cada red se una a la organización independiente.

Paso 3

Las opciones de configuración incluyen

- *Profile Name* - Es un identificador único dentro del CBD para que pueda fácilmente hacer un seguimiento de qué página va con cada organización.
- *Organización*: muestra a qué organización está conectado el portal cautivo.
- *Texto de encabezado*: muestra el encabezado que mostrará el explorador web.
- *La imagen de fondo y la imagen de logotipo* muestran dónde puede arrastrar y soltar los gráficos para mostrarlos en la página del portal cautivo.
- Los campos de color de primer plano, fondo, separador, contenido de primer plano, contenido de fondo y sugerencias de cuenta permiten cambiar el color de los aspectos respectivos de la visualización.
- El menú *Fuentes* le permite elegir la fuente utilizada en la página del portal cautivo.
- Los demás campos permiten editar el texto que se muestra en la página.

The image shows a configuration interface for a captive portal. It is organized into several sections:

- Device Group Selection:** Profile Name (text input: "Default guest portal"), Organization (dropdown: "Default").
- Web Portal Customization:** Header Text (text input: "Web Portal Guest Access"), Background Image (file upload area with "background.png"), Logo Image (file upload area with "loginlogo.png").
- Color and Font Settings:** Separator Color (color picker: grey), Content Foreground Color (color picker: black), Content Background Color (color picker: white), Account Tips Background Color (color picker: light blue), Fonts (dropdown: "Arial"), Button Label (text input: "Connect"), Browser Header Text (text input: "Captive Portal").
- Text and Policy Settings:** Portal Title (text input: "Welcome to the Wireless Network"), Acceptable Use Policy (text input: "Acceptance Use Policy").
- Acceptance Prompt:** A large text area for the main policy text, with a "Check here to indicate that you have read and accepted the Acceptance Use Policy" checkbox.
- Message Templates:** Several message boxes for different states: "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!), and "Welcome Message" (You are now authorized and...).

Paso 4

Haga clic en una de las fichas siguientes para configurar las opciones de texto para la autenticación.

- Nombre de usuario/Contraseña
- Consentimiento web
- Dirección de correo

Haga clic en el botón **Preview** para ver cómo se mostrarán las opciones de menú.

Preview

Paso 5

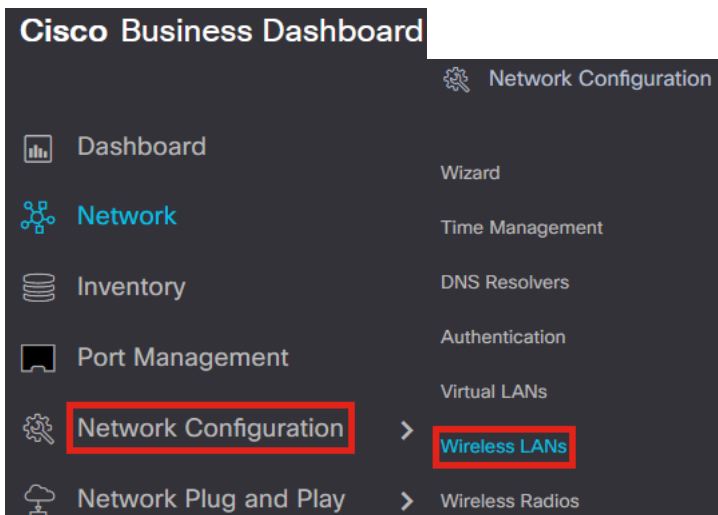
Una vez que haya personalizado la página web, haga clic en **Update** o *Cancel*.

Login Instructions	<div style="border: 1px solid #ccc; padding: 5px;">To start using this service, enter your credentials and click the connect button</div>
Username Input Label	<input type="text" value="Username"/>
Password Input Label	<input type="password" value="Password"/>
Input Prompt	<input type="text" value="Enter your Username/Password"/>
Enable Acceptable Use Policy	<input checked="" type="checkbox"/>
	<div style="display: flex; gap: 10px;">Update Cancel</div>

Configuración de LAN inalámbrica

Paso 1

Vaya a **Network Configuration > Wireless LANs**.



Paso 2

Puede agregar o editar un perfil de *LAN inalámbricas* existente. En este ejemplo, se selecciona **add**.



Paso 3

Especifique el *nombre del perfil*, la *organización* y los *grupos de dispositivos* dentro de la organización a la que se aplicará.

Wireless LANs->Add WLAN

Device Group Selection

Profile Name ✓ 1

Organization ✓ 2

Device Groups

3

Available Groups		Selected Groups
Default	>	
	<	
	>>	
	<<	

Solo tiene que elegir la organización *Default* y el grupo de dispositivos *Default*.

Paso 4

Agregue una LAN inalámbrica haciendo clic en el icono **más**.

Wireless LANs



SSID Name	VLAN ID	Enable	Security	Action
-----------	---------	--------	----------	--------

Paso 5

Especifique el *nombre SSID* y el *ID de VLAN*. Elija **Invitado** en el menú desplegable *Seguridad*.

Add Wireless LANs



Enable Enable

SSID Name ✓ 1

VLAN ID ✓ 2

Security 3

Paso 6

Seleccione el método de *autenticación de invitado*. Las opciones son:

- Nombre de usuario/Contraseña

- Consentimiento web
- Dirección de correo

Guest authentication

▼ Advanced Settings

Broadcast

Paso 7

En *Advanced Settings*, también puede especificar si desea que el SSID se *transmita*, la configuración de *Application Visibility*, *Local Profiling* y *Radio*.

▼ Advanced Settings

Broadcast

 Enable

Application Visibility

 Enable

Local Profiling

 Enable

Radio

En la mayoría de los casos, los dejará con el parámetro predeterminado.

Paso 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

Save

Cancel

Paso 9

Haga clic en **Guardar** nuevamente.

Wireless LANs->Add WLAN

Device Group Selection

Profile Name

 ✓

Organization

 ✓

Device Groups

Available Groups		Selected Groups
Default	>	
	<	
	>>	

Configuración de red de invitado CBW

Paso 1

Inicie sesión en el punto de acceso Cisco Business Wireless (CBW).



Cisco Business Wireless Access Point

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

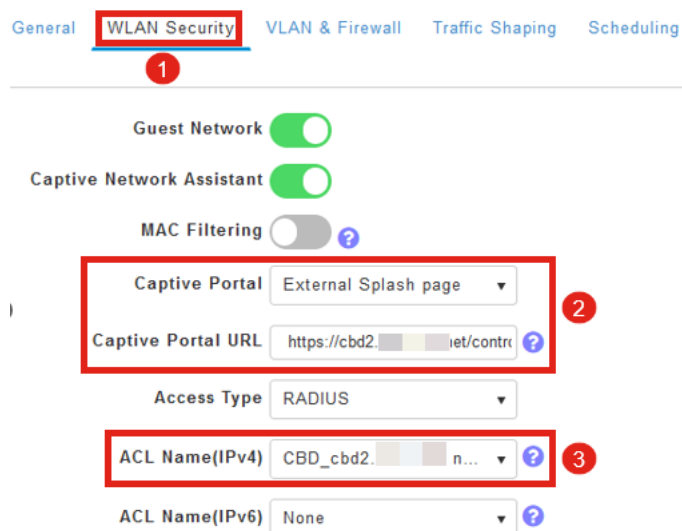


Paso 2

Vaya a **Wireless Settings > WLANs**.

Paso 3

Puede editar la WLAN e ir a la pestaña **WLAN Security**. El *portal cautivo* se configurará en la **página de bienvenida externa** con la *URL del portal cautivo* de su servidor CBD. El *nombre ACL* se configurará automáticamente.



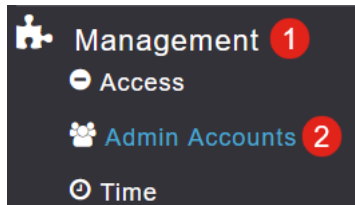
Paso 4

El servidor RADIUS se configura automáticamente. Para verla, cambie a la **vista Experto** haciendo clic en la flecha bidireccional de la parte superior de la página.



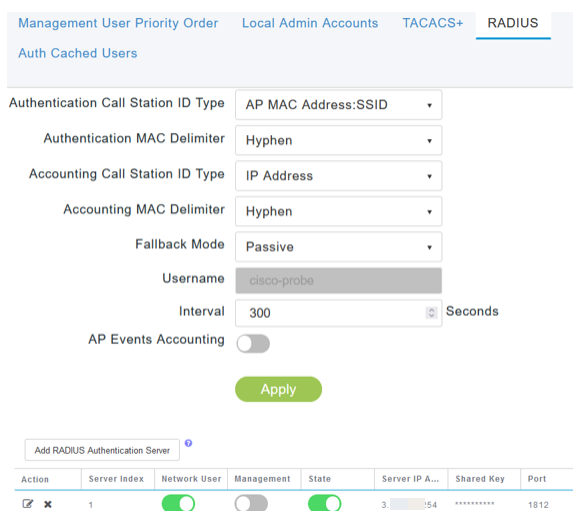
Paso 5

Vaya a **Administración > Cuentas de administrador.**



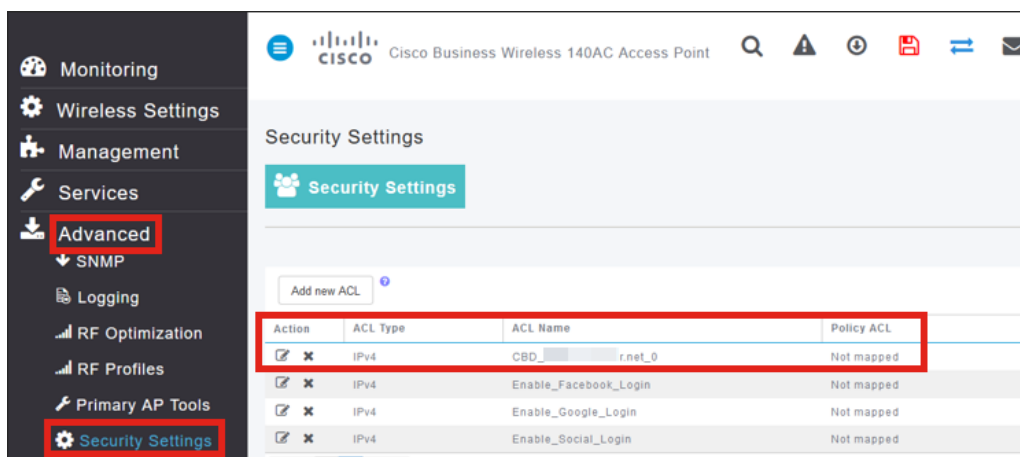
Paso 6

Haga clic en la pestaña **RADIUS.**



Paso 7

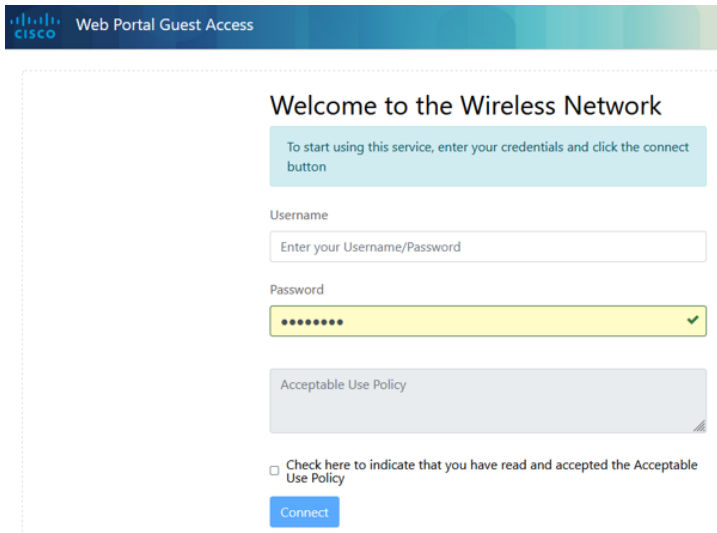
También agregará dinámicamente una ACL de seguridad para CBD en **Advanced > Security Settings.**



Página Portal cautivo

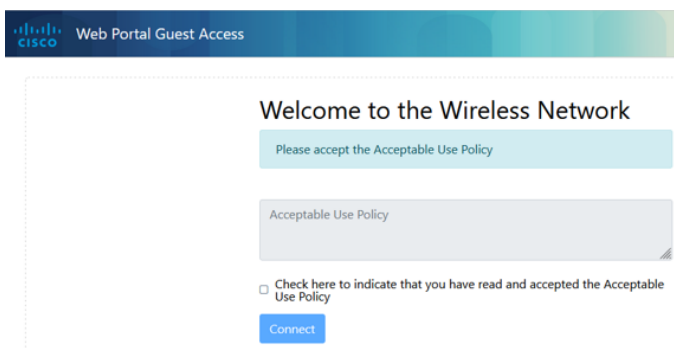
Según cómo haya configurado los parámetros, la página del portal cautivo tendrá el siguiente aspecto:

Autenticación de nombre de usuario/contraseña



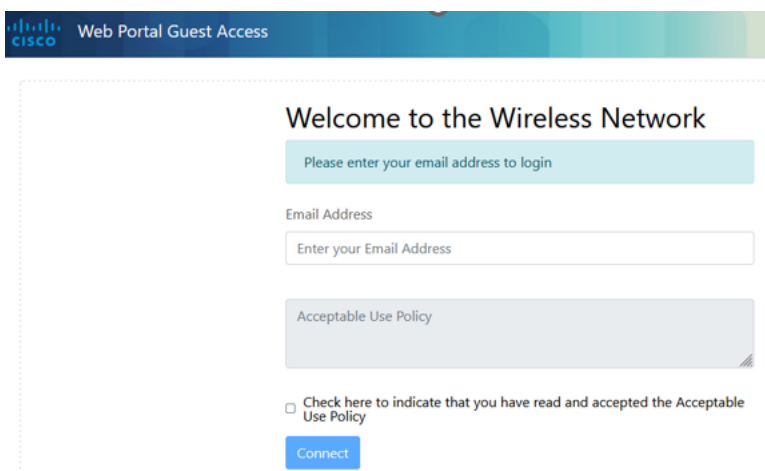
The screenshot shows the Cisco Web Portal Guest Access interface. At the top, there is a header with the Cisco logo and the text "Web Portal Guest Access". Below the header, the main content area is titled "Welcome to the Wireless Network". A light blue box contains the instruction: "To start using this service, enter your credentials and click the connect button". Below this, there are two input fields: "Username" with the placeholder text "Enter your Username/Password" and "Password" with a masked password "••••••••" and a green checkmark on the right. Below the password field is a grey box labeled "Acceptable Use Policy". At the bottom, there is a checkbox with the text "Check here to indicate that you have read and accepted the Acceptable Use Policy" and a blue "Connect" button.

Consentimiento web



The screenshot shows the Cisco Web Portal Guest Access interface. At the top, there is a header with the Cisco logo and the text "Web Portal Guest Access". Below the header, the main content area is titled "Welcome to the Wireless Network". A light blue box contains the instruction: "Please accept the Acceptable Use Policy". Below this, there is a grey box labeled "Acceptable Use Policy". At the bottom, there is a checkbox with the text "Check here to indicate that you have read and accepted the Acceptable Use Policy" and a blue "Connect" button.

Autenticación de correo electrónico



The screenshot shows the Cisco Web Portal Guest Access interface. At the top, there is a header with the Cisco logo and the text "Web Portal Guest Access". Below the header, the main content area is titled "Welcome to the Wireless Network". A light blue box contains the instruction: "Please enter your email address to login". Below this, there is an "Email Address" input field with the placeholder text "Enter your Email Address". Below the input field is a grey box labeled "Acceptable Use Policy". At the bottom, there is a checkbox with the text "Check here to indicate that you have read and accepted the Acceptable Use Policy" and a blue "Connect" button.

Conclusión

¡Lo lograste! Ha configurado correctamente la página de portal cautivo externo mediante CBD.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).