

Autenticación inalámbrica mediante Cisco Business Dashboard

Objetivo

El objetivo de este artículo es revisar la función de autenticación inalámbrica mediante Cisco Business Dashboard (CBD) versión 2.5.0.

Dispositivos aplicables | Versión de software

- Panel empresarial de Cisco | 2.5.0 ([Descargar la última versión](#))
- CBW140AC | [Descargar la última](#)
- CBW145AC | [Descargar la última](#)
- CBW240AC | [Descargar la última](#)
- CBW150AX | [Descargar la última](#)

Introducción

CBD proporciona herramientas que le ayudan a supervisar y gestionar los dispositivos de su red empresarial de Cisco. Detecta automáticamente la red y le permite configurar y supervisar todos los dispositivos compatibles, como switches, routers y puntos de acceso inalámbricos.

CBD 2.5.0 añade la funcionalidad del servicio de autenticación a CBD. El nuevo servicio es compatible con los dispositivos de las series CBW140/240 y CBW 150AX.

Configura una instancia de FreeRADIUS en el administrador CBD para utilizar la autenticación RADIUS, lo que brinda a su organización una manera simple de implementar un servidor sin que los clientes tengan que conocer o entender RADIUS.

Si está listo para comenzar, déjenos sumergirnos.

Table Of Contents

- [Configurar perfil de autenticación](#)
- [Configuración de redes inalámbricas](#)
- [Verificación](#)
- [Prueba](#)


Configurar perfil de autenticación

En primer lugar, debe configurar el perfil de autenticación que utilizará para su organización. En muchos casos, puede utilizar simplemente el perfil predeterminado.

Paso 1

Inicie sesión en CBD.

English ▾



Cisco Business Dashboard

User Name* 1

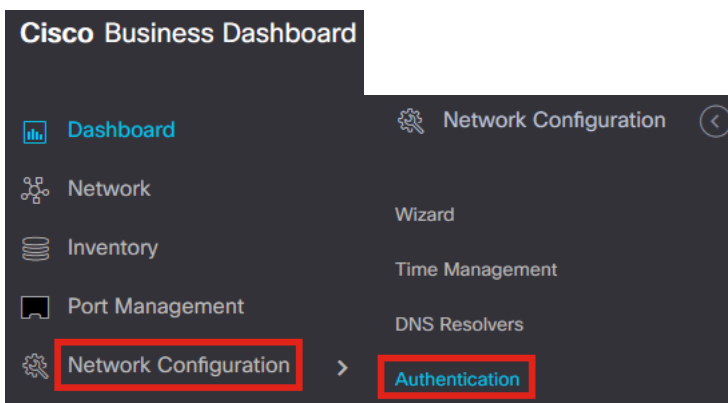
This field is required

Password* 2

Login 3

Paso 2

Vaya a **Network Configuration > Authentication**.







Paso 3

Puede editar el perfil *Default* existente o agregar otro perfil. En este ejemplo, se selecciona el perfil **Default**. Haga clic en **Editar**.


☰ Cisco Business Dashboard

Authentication

2

+    

1 Profile Name

 > Default

⏪ < 1 > ⏩ 10 Per Page

Paso 4

En CBD 2.5.0, hay una nueva opción para seleccionar *Use Cisco Business Dashboard Authentication Service*. Esta opción está activada de forma predeterminada. Realice

los cambios deseados y haga clic en **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.

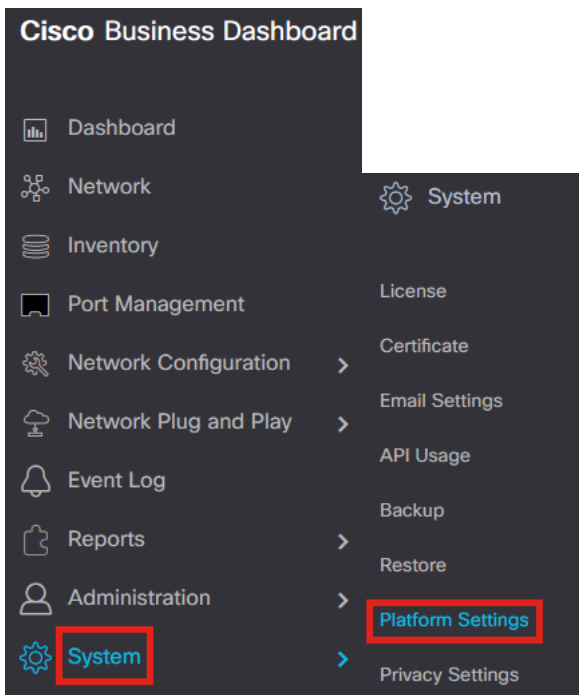
 Add custom authentication server



Asegúrese de ver si *System > Platform Settings > System Variables* tiene la configuración correcta para permitir que los dispositivos de red alcancen el Panel.

Paso 5

Vaya a **System > Platform Settings** en el menú.



Paso 6

Seleccione la pestaña **Variables del sistema**.

Platform Settings

Network Settings Web Server **System Variables**

Paso 7

Verifique la configuración para asegurarse de que la *dirección IP del tablero externo* es la dirección IP pública del CBD y el *puerto del servidor de autenticación externo* es 1812. Este es el puerto predeterminado. Click **Save**.

Platform Settings

Network Settings Web Server **System Variables**

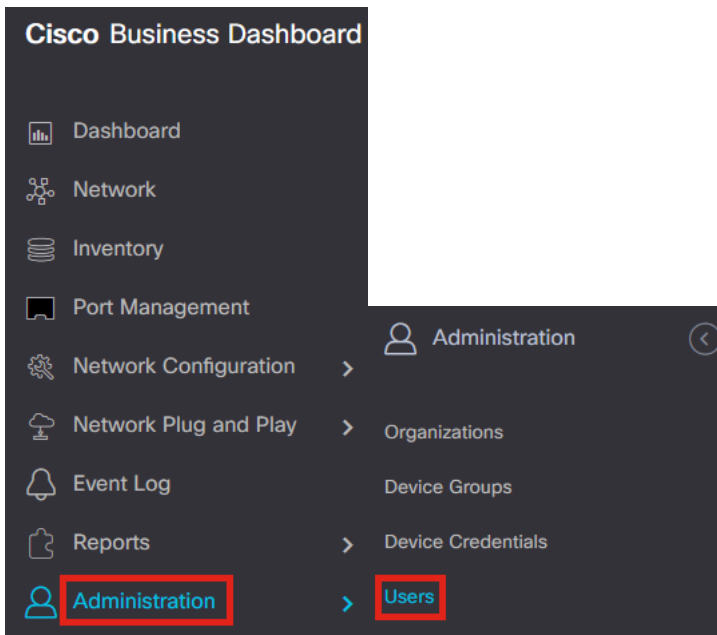
External System Settings

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

Paso 8

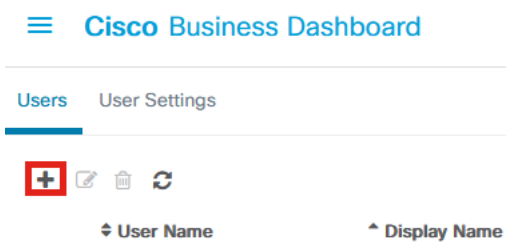
Para crear usuarios que vayan a autenticarse en el sistema, vaya a **Administration >**

Users.



Paso 9

Para agregar usuarios, haga clic en el **icono más**.



Paso 10

Configure lo siguiente:

- *User Name*
- *Mostrar nombre:*
- *Correo electrónico*
- *Acceso al panel:* selecciónelo en el menú desplegable. En este ejemplo, se selecciona **Sin acceso**.
- *Nueva contraseña*
- *Volver a escribir nueva contraseña*

Los demás campos son opcionales. 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	●●●● 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 checked="" type="button" value="Save"/> <input type="button" value="Cancel"/>

Paso 11

Haga clic en la ficha **Organizaciones**.

Cisco Business Dashboard

User Name	<input type="text" value="user1"/>
	Reset password
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
	Show account settings
Create Time	Jul 5 2022 09:31
Last Password Changed Time	Jul 5 2022 09:31
Last Login	Never
	<input checked="" type="button" value="Save"/> <input type="button" value="Cancel"/>

Access Key **Organizations**

Paso 12

Aquí, debe asociar el usuario que acaba de crear con su organización CBD. Haga clic en el **icono más** y elija la opción en el menú desplegable. En este ejemplo, se selecciona **Default**.

Access Key **Organizations**

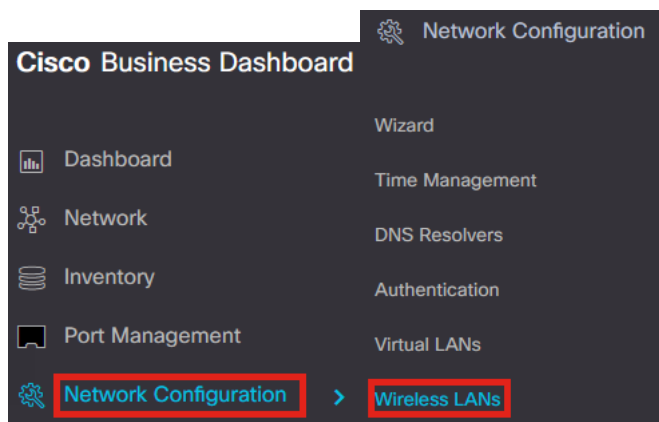
<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	▼ Org Name
<input type="checkbox"/>	Default

Este usuario podrá iniciar sesión en la organización predeterminada configurada para la autenticación inalámbrica.

Configuración de redes inalámbricas

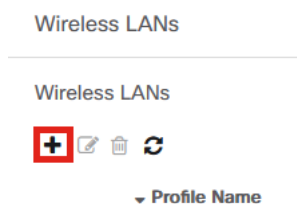
Paso 1

Vaya al menú **Network Configuration > Wireless LANs**.



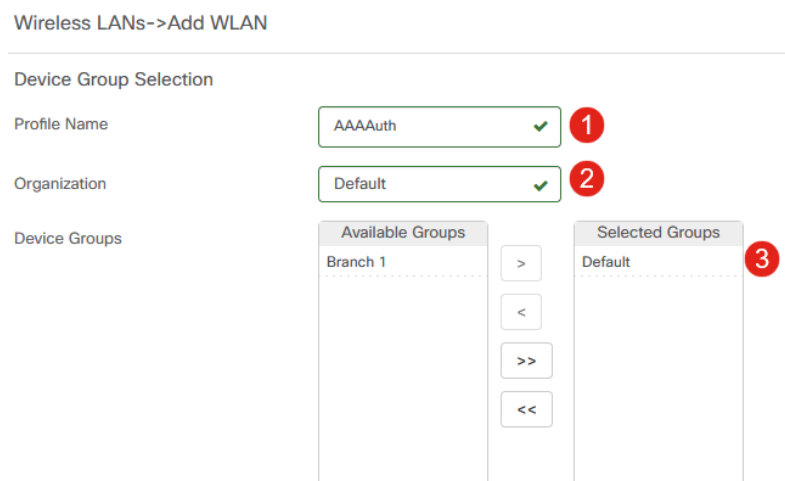
Paso 2

Para crear un nuevo perfil, haga clic en el **icono más** en *LAN inalámbricas*.



Paso 3

Ingrese *Profile Name*, *Organization* y configure *Device Groups* para aplicar las configuraciones a los dispositivos inalámbricos en el grupo.



Paso 4

Para crear un SSID, haga clic en el **icono más**.



SSID Name

Paso 5

Ingrese el *Nombre SSID*, *ID VLAN* y seleccione *Seguridad* en el menú desplegable. En este ejemplo, se selecciona **WPA2-Enterprise**. 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

Se utilizará el servidor de autenticación Cisco Business Dashboard si no tiene configurado un servidor de autenticación.

Paso 6

Vuelva a hacer clic en **Guardar** para aplicar la red inalámbrica y los parámetros de RADIUS a todos los clientes.

Wireless LANs->Add WLAN

Device Group Selection

Profile Name ✓

Organization ✓

Device Groups

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

Wireless LANs +

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

Verificación

Para comprobar si se han aplicado los parámetros,

Paso 1

Inicie sesión en el punto de acceso de CBW.



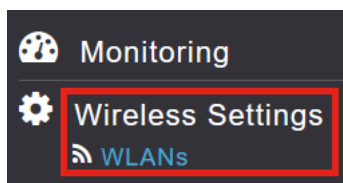
Cisco Business Wireless Access Point

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



Paso 2

Vaya a **Wireless Settings > WLANs**.



Paso 3

Se mostrará el SSID que ha creado. En este ejemplo, es **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

Paso 4

Seleccione el SSID y haga clic en **edit (editar)** para ver la configuración.

WLANS

Active WLANS 2

Add new WLAN/RLAN

Action	Active	Type	Name
	Enabled	WLAN	CBWireless
	Enabled	WLAN	AAATest

Paso 5

Vaya a la pestaña **Seguridad WLAN**.

Edit WLAN

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

Verá que el *Tipo de seguridad* aparecerá como **WPA2 Enterprise** y el *Servidor de autenticación* será el **Radio externo**. La *dirección IP del servidor* será la que configuró anteriormente.

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

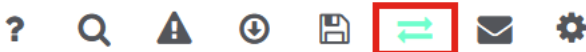
Authentication Caching

Add RADIUS Authentication Server

State	Server IP Address	Port
Enabled	3. 254	1812

Paso 6

Cambie a la **vista Experto** haciendo clic en la flecha bidireccional en la parte superior de la interfaz de usuario.



Paso 7

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

Management 1

Access

Admin Accounts 2

Time

Paso 8

Haga clic en la pestaña **RADIUS**.

Admin Accounts

Users 1

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

Verá que el servidor de autenticación Radius se ha configurado para *Usuario de red*.

Add RADIUS Authentication Server ⓘ

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

Prueba

Para probar la configuración:

Paso 1

Vaya a **Avanzado > Herramientas de AP Primario**.

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

Paso 2

Haga clic en la pestaña **Herramientas de solución de problemas**.

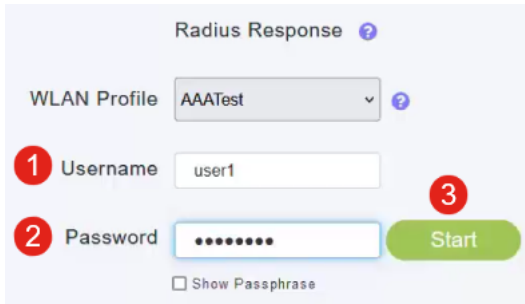
Primary AP Tools

Tools

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

Paso 3

En la sección *Radius Response*, ingrese el **Nombre de usuario** y la **Contraseña** y haga clic en **Start** para ver si se autentica contra el servidor Radius.



The screenshot shows the 'Radius Response' configuration page. At the top, there is a 'WLAN Profile' dropdown menu set to 'AAATest'. Below it, there 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 circles (1, 2, 3) are overlaid on the Username, Password, and Start button respectively. A 'Show Passphrase' checkbox is located below the password field.

Verá una notificación de *autenticación correcta* después de que se complete la prueba.



This screenshot shows the same 'Radius Response' configuration page after the 'Start' button has been clicked. A blue notification bar with a green checkmark icon is displayed at the bottom right, containing the text 'Authentication success (3.1 254)'. The 'Start' button is now highlighted in green. The 'Show Passphrase' checkbox remains unchecked.

Asegúrese de que tiene conectividad IP entre el administrador CBD y el sistema cliente para que esto funcione correctamente.

Conclusión

¡Eso es! Ya no tendrá que preocuparse por configurar Radius por sí mismo. CBD hará todo el trabajo y podrá sentarse, relajarse y disfrutar de las ventajas de la autenticación inalámbrica en su red.

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).