

Autenticazione wireless con Cisco Business Dashboard

Obiettivo

L'obiettivo di questo articolo è quello di esaminare le funzionalità di autenticazione wireless utilizzando Cisco Business Dashboard (CBD) versione 2.5.0.

Dispositivi interessati | Versione software

- Cisco Business Dashboard | 2.5.0 (scarica la versione più recente)
- CBW140AC | [Scarica la versione più recente](#)
- CBW145AC | [Scarica la versione più recente](#)
- CBW240AC | [Scarica la versione più recente](#)
- CBW150AX | [Scarica la versione più recente](#)

Introduzione

CBD fornisce strumenti che consentono di monitorare e gestire i dispositivi nella rete aziendale Cisco. Individua automaticamente la rete e consente di configurare e monitorare tutti i dispositivi supportati, quali switch, router e punti di accesso wireless.

CBD 2.5.0 aggiunge la funzionalità del servizio di autenticazione a CBD. Il nuovo servizio è supportato sui dispositivi della serie CBW140/240 e CBW 150AX.

Consente di configurare un'istanza di FreeRADIUS in Gestione CBD da utilizzare per l'autenticazione RADIUS, offrendo all'organizzazione un modo semplice per distribuire un server senza che i client debbano conoscere o comprendere RADIUS.

Se siete pronti per iniziare, lasciateci entrare.

Sommario

- [Configura profilo di autenticazione](#)
- [Configurazione di reti wireless](#)
- [Verifica](#)
- [Test](#)


Configura profilo di autenticazione

È innanzitutto necessario configurare il profilo di autenticazione che verrà utilizzato per l'organizzazione. In molti casi è sufficiente utilizzare il profilo predefinito.

Passaggio 1

Accedere a CBD.

English ▾



Cisco Business Dashboard

User Name* 1

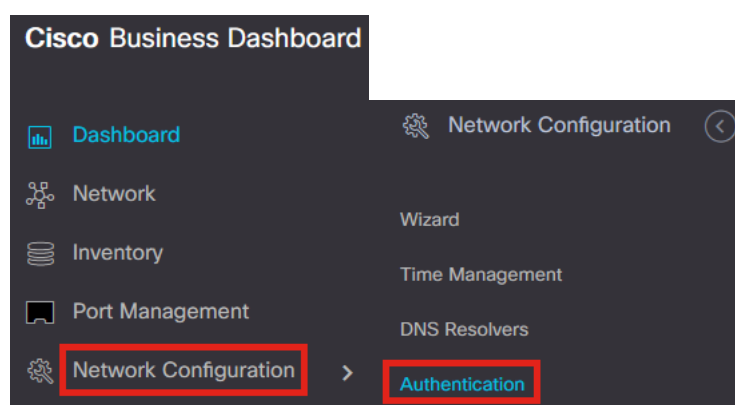
This field is required

Password* 2

Login 3

Passaggio 2

Selezionare **Configurazione di rete > Autenticazione**.






Passaggio 3

È possibile modificare il profilo *predefinito* esistente o aggiungere un altro profilo. In questo esempio, viene selezionato il profilo **predefinito**. Fare clic su **Modifica**.


☰ Cisco Business Dashboard

Authentication

2

+   

1 Profile Name

 > Default

⏪ < 1 > ⏩ 10 Per Page

Passaggio 4

In CBD 2.5.0 è disponibile una nuova opzione per selezionare *Utilizza Cisco Business Dashboard Authentication Service*. Questa opzione è selezionata per default.

Apportare le modifiche desiderate e fare clic su **Aggiorna**.

Authentication->Update Default

Device Group Selection

Profile Name

Organization

Device Groups

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

Authentication

Local User Authentication

i 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

1 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.

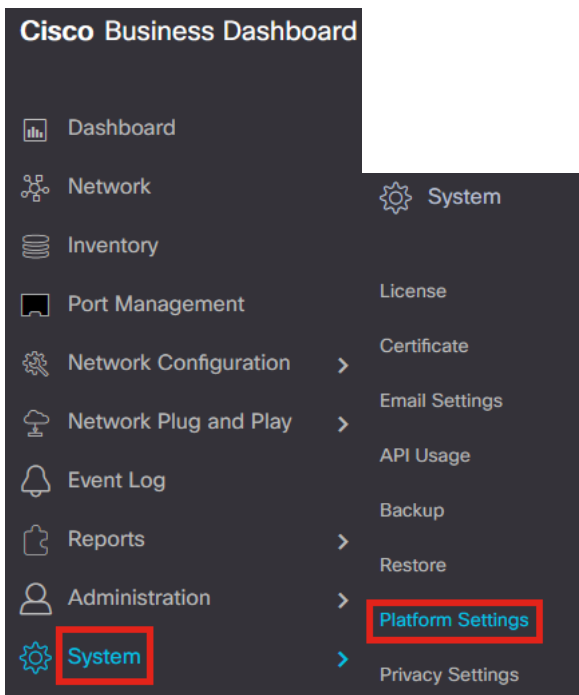
+ Add custom authentication server

2

Verificare che *Sistema > Impostazioni piattaforma > Variabili di sistema* disponga delle impostazioni corrette per consentire ai dispositivi di rete di raggiungere il dashboard.

Passaggio 5

Selezionare **Sistema > Impostazioni piattaforma** nel menu.



Passaggio 6

Selezionare la scheda **Variabili di sistema**.

Platform Settings

Network Settings Web Server **System Variables**

Passaggio 7

Verificare le impostazioni per assicurarsi che l'*indirizzo IP del dashboard esterno* sia l'indirizzo IP pubblico del CBD e che la *porta del server di autenticazione esterno* sia 1812. Questa è la porta predefinita. Fare clic su **Salva**.

Platform Settings

Network Settings Web Server **System Variables**

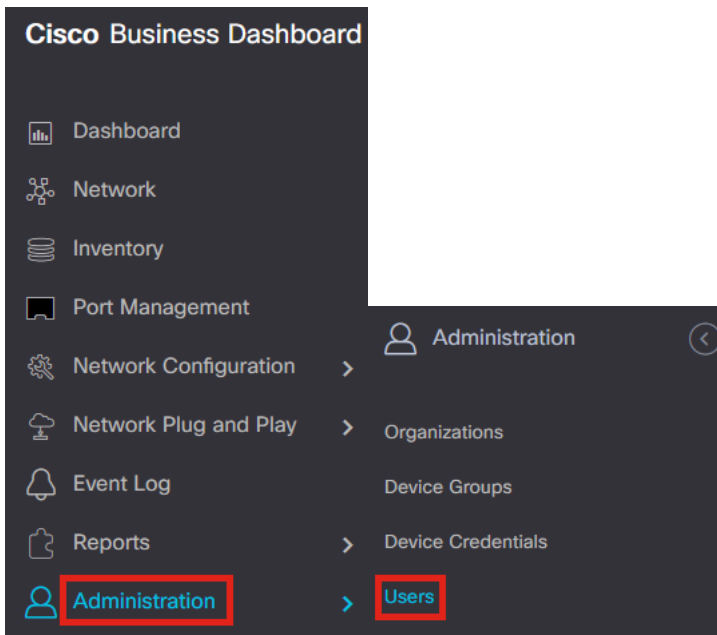
External System Settings

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

Passaggio 8

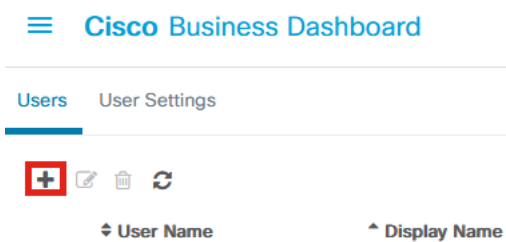
Per creare utenti che verranno autenticati nel sistema, passare ad **Amministrazione** >

Utenti.



Passaggio 9

Per aggiungere utenti, fare clic sull'icona più.



Passaggio 10

Configurare quanto segue:

- *Nome utente*
- *Nome visualizzato*
- *Email*
- *Accesso al dashboard*: selezionare dal menu a discesa. Nell'esempio è selezionato **Nessun accesso**.
- *Nuova password*
- *Digita nuovamente la password*

Gli altri campi sono facoltativi. Fare clic su **Salva**.

Users > Add User

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 type="button" value="Save"/> <input type="button" value="Cancel"/>

Passaggio 11

Fare clic sulla scheda **Organizzazioni**.

☰ Cisco Business Dashboard

Users > user1

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 type="button" value="Save"/> <input type="button" value="Cancel"/>

Access Key **Organizations**

Passaggio 12

È necessario associare l'utente appena creato all'organizzazione CBD. Fare clic sul **segno più** e scegliere l'opzione dal menu a discesa. In questo esempio è selezionato **Default**.

Access Key **Organizations**

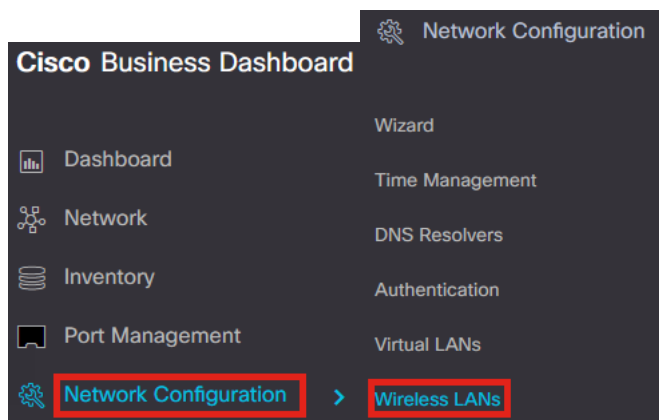
<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	▼ Org Name
<input type="checkbox"/>	Default

L'utente potrà accedere all'organizzazione predefinita configurata per l'autenticazione wireless.

Configurazione di reti wireless

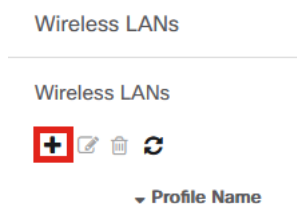
Passaggio 1

Selezionare **Configurazione rete** > Menu **LAN wireless**.



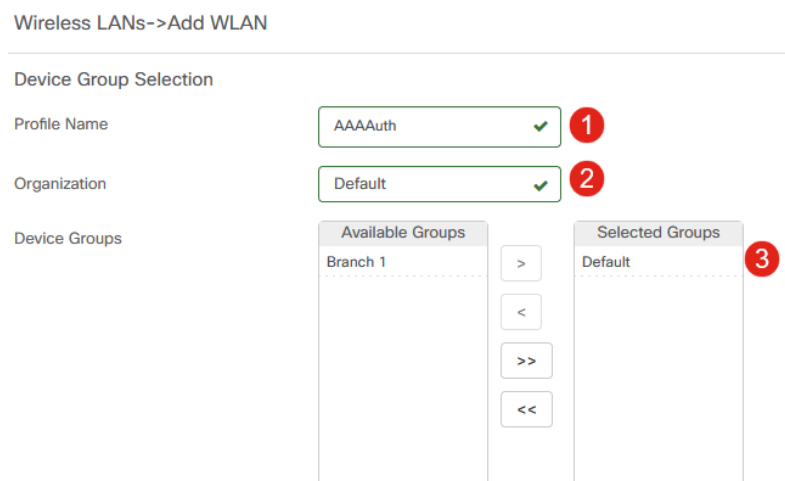
Passaggio 2

Per creare un nuovo profilo, fare clic sul **segno più** sotto *LAN wireless*.



Passaggio 3

Immettere il *Nome profilo*, *Organizzazione* e configurare *Gruppi di dispositivi* in modo da applicare le impostazioni alle periferiche wireless del gruppo.



Passaggio 4

Per creare un SSID, fare clic sull'icona con il segno più.



SSID Name

Passaggio 5

Immettere il *nome SSID*, l'*ID VLAN* e selezionare *Security* dal menu a discesa. Nell'esempio è selezionato **WPA2-Enterprise**. Fare clic su **Salva**.

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 non si dispone di un server di autenticazione configurato, verrà utilizzato Cisco Business Dashboard Authentication Server.

Passaggio 6

Fare di nuovo clic su **Salva** per applicare la rete wireless e le impostazioni Radius a tutti i client.

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	

Verifica

Per verificare se le impostazioni sono state applicate

Passaggio 1

Accedere all'access point CBW.



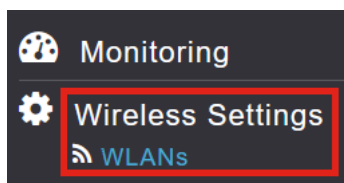
Cisco Business Wireless Access Point

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



Passaggio 2

Selezionare **Wireless Settings > WLAN** (Impostazioni wireless > WLAN).



Passaggio 3

Il SSID creato verrà elencato. Nell'esempio, questo valore è **AAATest**.

WLANs

Active WLANs 2

Add new WLAN/RLAN

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

Passaggio 4

Selezionare il SSID e fare clic su **Modifica** per visualizzare le impostazioni.

WLANS

Active WLANS 2

Add new WLAN/RLAN

Action	Active	Type	Name
	Enabled	WLAN	CBWireless
	Enabled	WLAN	AAATest

Passaggio 5

Passare alla scheda **Sicurezza WLAN**.

Edit WLAN

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

Il *Tipo di protezione* verrà elencato come **WPA2 Enterprise** e *Authentication Server* sarà il **Radius esterno**. L'*indirizzo IP* del server sarà quello configurato in precedenza.

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

Passaggio 6

Passare alla **visualizzazione Esperti** facendo clic sulla freccia bidirezionale nella parte superiore dell'interfaccia utente.



Passaggio 7


Passare a **Gestione > Account amministratore**.

- Management 1
- Access
- Admin Accounts 2
- Time

Passaggio 8


Fare clic sulla scheda **RADIUS**.






Admin Accounts

 **Users** 1

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

Il server di autenticazione Radius è stato configurato per l'*utente di rete*.

Add RADIUS Authentication Server 









Action	Server Index	Network User	Management	State	Server IP Address	Shared Key	Port
 	1				3.1.254	*****	1812

Test

Per verificare le impostazioni:

Passaggio 1


Passare a **Avanzate > Strumenti principali PA**.

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

Passaggio 2

Fare clic sulla scheda **Strumenti di risoluzione dei problemi**.

Primary AP Tools

 **Tools**

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

Passaggio 3

Nella sezione *Risposta Radius*, immettere **Nome utente** e **Password**, quindi fare clic su **Avvia** per verificare se viene eseguita l'autenticazione sul server Radius.

Radius Response ?

WLAN Profile AAATest ?

1 Username user1

2 Password

3 Start

Show Passphrase

Al termine del test verrà visualizzata una notifica di *autenticazione riuscita*.

Radius Response ?

WLAN Profile AAATest ?

Username user1

Password

Start

Authentication success (3.1 254) ✓

Show Passphrase

Assicurarsi di disporre di connettività IP tra CBD Manager e il sistema client per il corretto funzionamento di questa funzionalità.

Conclusioni

È tutto! Non dovete più preoccuparvi di configurare Radius da soli. Il CBD consente di eseguire tutte le operazioni necessarie e di rilassarsi e usufruire dei vantaggi dell'autenticazione wireless nella rete.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).