

External Captive Portal in Cisco Business Dashboard

Obiettivo

L'obiettivo di questo articolo è esaminare i passaggi per configurare la funzionalità del portale captive esterno in Cisco Business Dashboard (CBD) versione 2.5.1 e successive.

Dispositivi interessati | Versione software

Cisco Business Dashboard | 2.5.1 ([scarica la versione più recente](#))

Serie CBW140 | 10.8.1.0 ([scarica la versione più recente](#))

Serie CBW150 | 10.3.2.0 ([scarica la versione più recente](#))

Introduzione

CBD versione 2.5.1 ha implementato una pagina esterna Captive Portal per le reti CBW140 e CBW150. Può essere utilizzata come pagina di autenticazione di rete guest e offre diversi vantaggi rispetto alle pagine di Captive Portal locali.

Anziché reindirizzare il client alla pagina locale del portale vincolato alla versione 192.0.2.1, esegue il reindirizzamento a CBD utilizzando il certificato FQDN e SSL del CBD. In questo modo si evita l'attivazione del protocollo HTTP Strict Transport Security (HSTS) migliorato implementato dai browser moderni.

La pagina Portale Captive esterno presenta una distribuzione semplificata che semplifica la gestione di più siti con reti guest.

Tutte le impostazioni per la pagina e i criteri di autenticazione vengono configurate in CBD.

Quando si configura la rete guest, sono supportati il consenso Web, l'indirizzo di posta elettronica e l'accesso agli account CBD o l'accesso a un altro server RADIUS.

Sommario

- [Requisiti di rete guest](#)
- [Configura autenticazione Guest](#)
- [Configurazione LAN wireless](#)
- [Impostazioni rete guest CBW](#)
- [Pagina Portale vincolato](#)

Requisiti di rete guest

Per utilizzare la nuova pagina Autenticazione di rete guest, è necessario disporre di

CBD versione 2.5.1

Firmware serie CBW140 10.8.1.0 (o versioni successive)

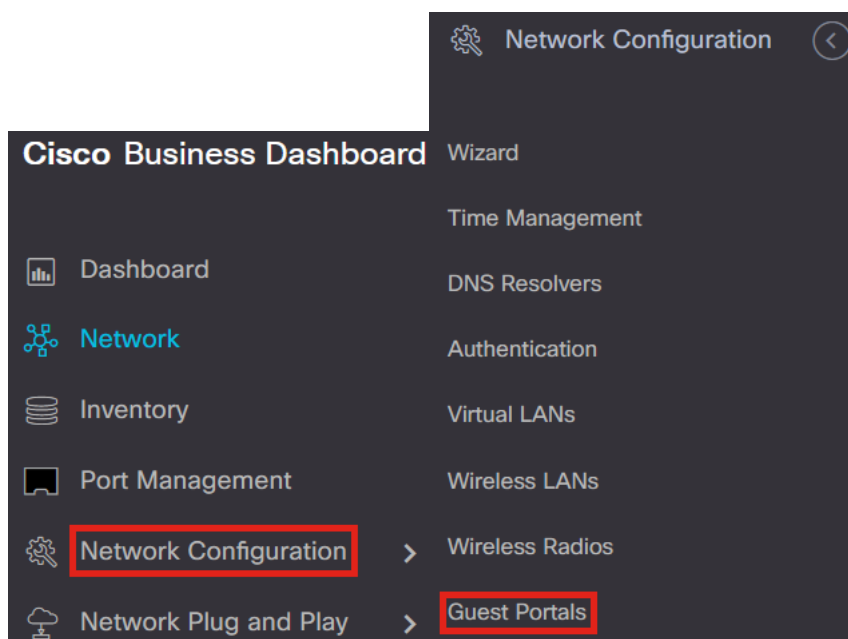
Firmware serie CBW150 10.3.2.0 (o versioni successive)

Configura autenticazione Guest

Per configurare la pagina Web di Captive Portal:

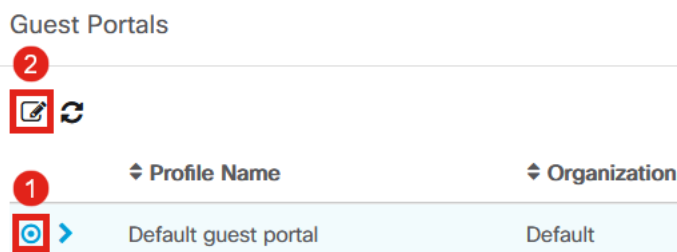
Passaggio 1

Accedere al CBD e selezionare **Configurazione di rete > Portali guest**.



Passaggio 2

La pagina *Guest Portals* mostra la pagina Web di ciascuna organizzazione CBD. Per modificare una pagina, selezionare il profilo e fare clic sul pulsante Modifica.



Se si dispone di due o più reti che richiedono pagine univoche del portale captive, sarà necessario impostare organizzazioni CBD separate e fare in modo che ogni rete si unisca all'organizzazione separata.

Passaggio 3

Le opzioni di configurazione includono

- *Nome profilo*: si tratta di un identificativo univoco all'interno di CBD che consente di tenere traccia facilmente della pagina associata a ciascuna organizzazione.
- *Organizzazione*: visualizza l'organizzazione a cui è connesso il portale vincolato.
- *Testo intestazione*: visualizza l'intestazione che verrà visualizzata dal browser Web.
- *Immagine di sfondo e immagine del logo* mostrano dove è possibile trascinare e rilasciare gli elementi grafici da visualizzare nella pagina del portale in cui è inserita l'immagine.
- I campi colore di primo piano, sfondo, separatore, primo piano del contenuto, sfondo del contenuto e sfondo dei suggerimenti per l'account consentono di modificare il colore dei rispettivi aspetti della visualizzazione.
- Il menu *Caratteri* consente di scegliere il carattere utilizzato nella pagina del portale captive.
- Gli altri campi consentono di modificare il testo visualizzato nella pagina.

The image shows a configuration interface 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).
- Color Selection**: Separator Color (grey), Content Foreground Color (black), Content Background Color (white), Account Tips Background Color (light blue), Foreground Color (white), Background Color (blue).
- Text and Font Settings**: Fonts (Arial), Button Label (Connect), Browser Header Text (Captive Portal), Portal Title (Welcome to the Wireless Network), Acceptable Use Policy (Acceptance Use Policy).
- Message Templates**: 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...).

Passaggio 4

Fare clic su una delle seguenti schede per configurare le opzioni di testo per l'autenticazione.

- Nome utente/Password
- Consenso Web
- Indirizzo email

Fare clic sul pulsante **Anteprima** per visualizzare la modalità di visualizzazione di ciascuna opzione di menu.

Preview

Passaggio 5

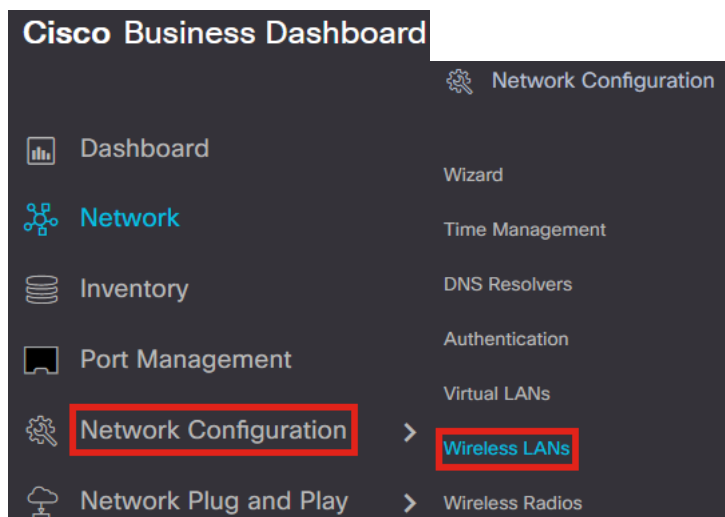
Una volta personalizzata la pagina Web, fare clic su **Aggiorna** o su *Annulla*.

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>

Configurazione LAN wireless

Passaggio 1

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



Passaggio 2

È possibile aggiungere o modificare un profilo *LAN wireless* esistente. Nell'esempio riportato di seguito, l'opzione **add** è selezionata.



Passaggio 3

Specificare il *nome del profilo*, l'*organizzazione* e i *gruppi di dispositivi* all'interno dell'organizzazione a cui si applica questa impostazione.

Wireless LANs->Add WLAN

Device Group Selection

Profile Name ✓ 1

Organization ✓ 2

Device Groups

Available Groups

Default

>

<

>>

<<

Selected Groups

3

È sufficiente scegliere l'organizzazione *predefinita* e il gruppo di dispositivi *predefinito*.

Passaggio 4

Aggiungere una LAN wireless facendo clic sull'icona **più**.

Wireless LANs



SSID Name

VLAN ID

Enable

Security

Action

Passaggio 5

Specificare il *nome SSID* e l'*ID VLAN*. Scegliere **Guest** dal menu a discesa *Security*.

Add Wireless LANs



Enable Enable

SSID Name ✓ 1

VLAN ID ✓ 2

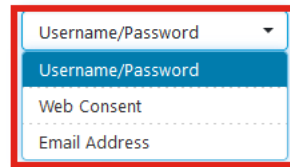
Security 3

Passaggio 6

Selezionare il metodo di *autenticazione Guest*. Le opzioni sono:

- Nome utente/Password
- Consenso Web
- Indirizzo email

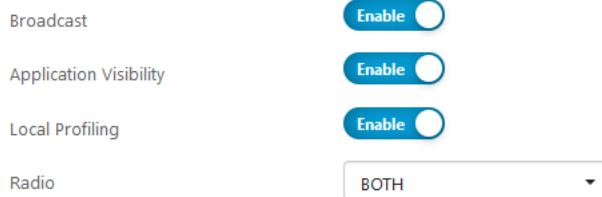
Guest authentication
▼ Advanced Settings
Broadcast



Passaggio 7

In *Impostazioni avanzate* è inoltre possibile specificare se si desidera che il SSID venga *trasmesso*, le impostazioni *Visibilità applicazione*, *Profilatura locale* e *Radio*.

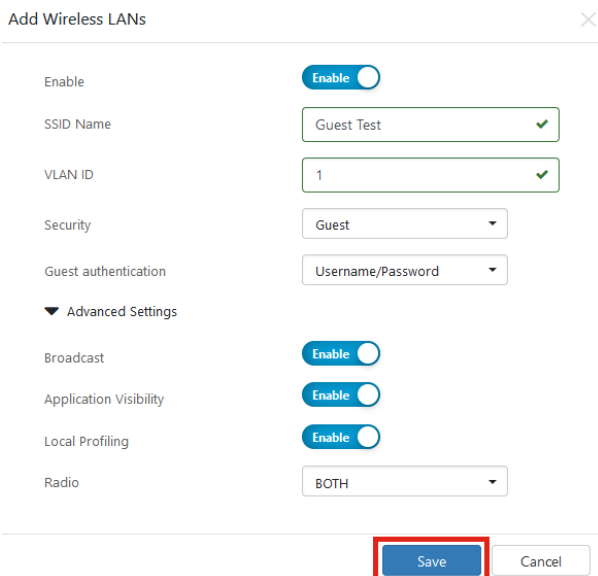
▼ Advanced Settings



Nella maggior parte dei casi, queste impostazioni vengono mantenute come predefinite.

Passaggio 8

Fare clic su **Salva**.



Add Wireless LANs

Enable

SSID Name

VLAN ID

Security

Guest authentication

▼ Advanced Settings

Broadcast

Application Visibility

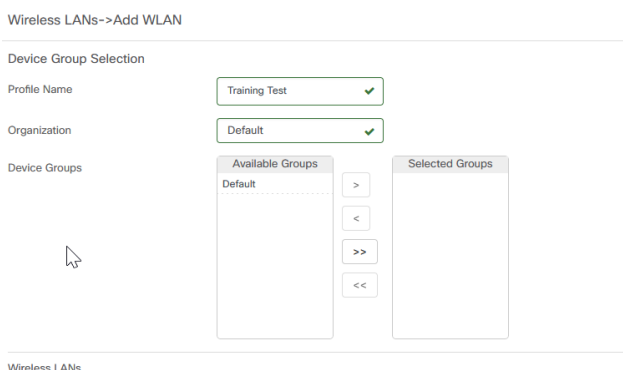
Local Profiling

Radio

Save Cancel

Passaggio 9

Fare di nuovo clic su **Salva**.



Wireless LANs->Add WLAN

Device Group Selection

Profile Name

Organization

Device Groups

Available Groups: Default

Selected Groups

> < >> <<

Wireless LANs

Impostazioni rete guest CBW

Passaggio 1

Accedere al punto di accesso Cisco Business Wireless (CBW).



Cisco Business Wireless Access Point

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

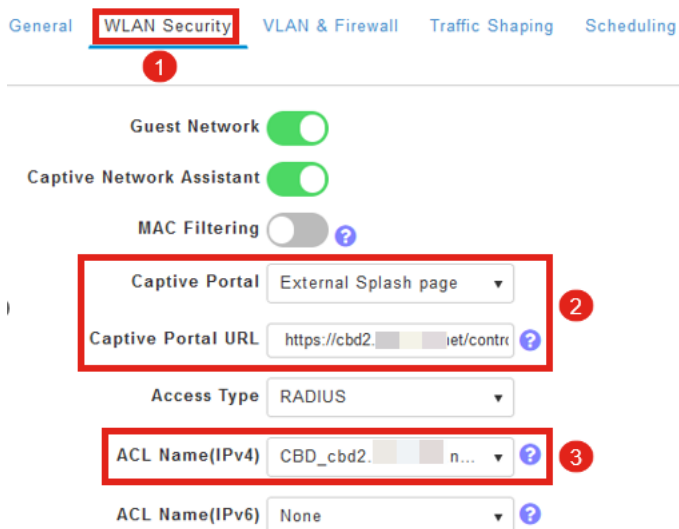


Passaggio 2

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

Passaggio 3

È possibile modificare la WLAN e andare alla scheda **Sicurezza WLAN**. Il *Captive Portal* verrà impostato sulla **pagina External Splash** con l'*URL Captive Portal* del server CBD. Il *nome ACL* verrà configurato automaticamente.



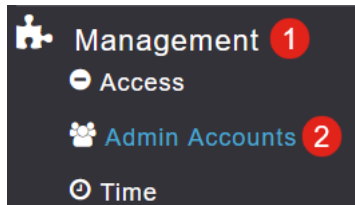
Passaggio 4

Il server RADIUS viene configurato automaticamente. Per visualizzarla, passare alla **visualizzazione Esperti** facendo clic sulla freccia bidirezionale nella parte superiore della pagina.



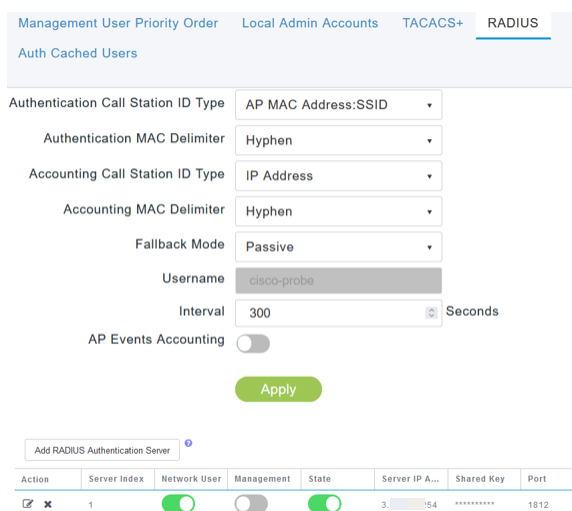
Passaggio 5

Passare a **Gestione > Account amministratore**.



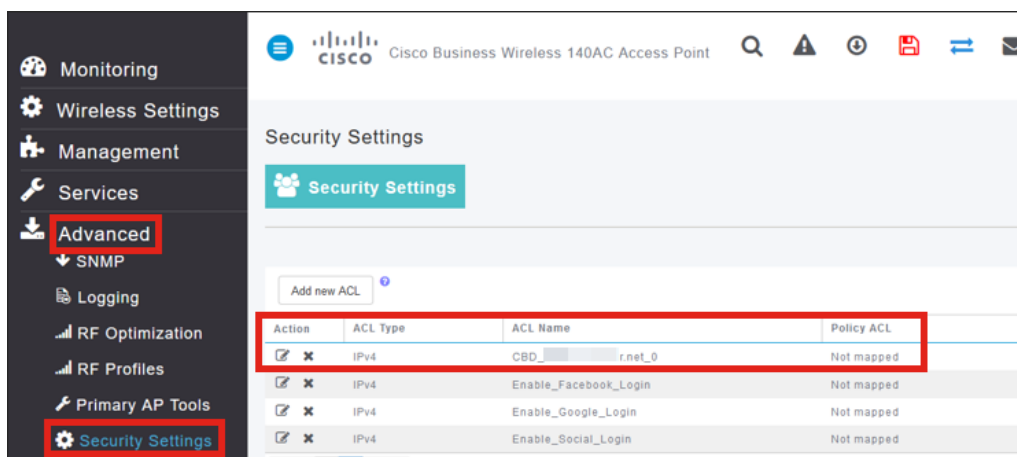
Passaggio 6

Fare clic sulla scheda **RADIUS**.



Passaggio 7

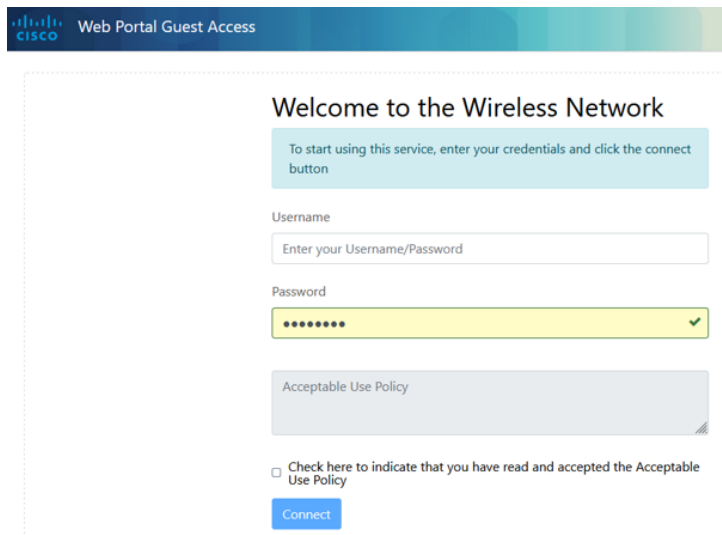
Inoltre, aggiungerà dinamicamente un ACL di sicurezza per il CBD in **Impostazioni avanzate > Impostazioni di sicurezza**.



Pagina Portale vincolato

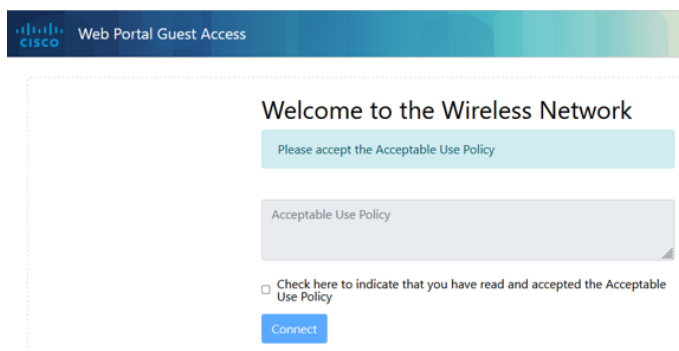
In base alla configurazione delle impostazioni, la pagina Portale vincolato avrà il seguente aspetto:

Autenticazione nome utente/password



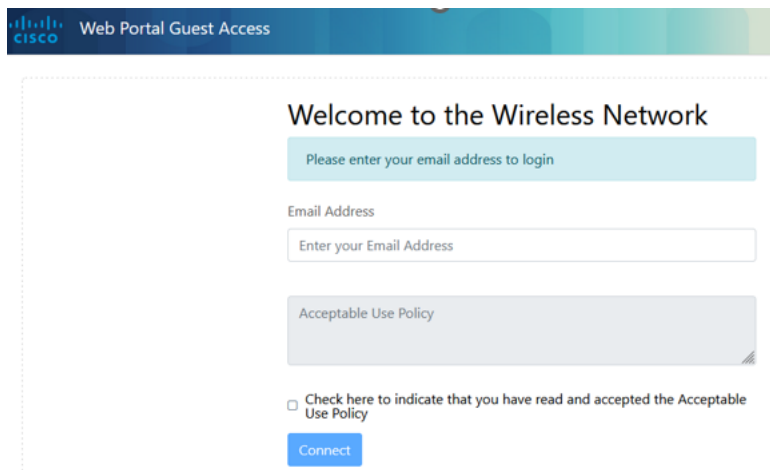
The screenshot shows the Cisco Web Portal Guest Access interface. At the top, there is a header with the Cisco logo and the text "Web Portal Guest Access". Below the header, the main content area is titled "Welcome to the Wireless Network". A light blue box contains the instruction: "To start using this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

Consenso 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 labeled "Check here to indicate that you have read and accepted the Acceptable Use Policy" and a blue "Connect" button.

Autenticazione e-mail



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 labeled "Check here to indicate that you have read and accepted the Acceptable Use Policy" and a blue "Connect" button.

Conclusioni

Ce l'hai fatta! La pagina del Portale Captive esterno è stata configurata correttamente utilizzando CBD.

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).