

Externes Captive Portal im Cisco Business Dashboard

Ziel

In diesem Artikel werden die Schritte zum Konfigurieren der externen Captive Portal-Funktion in Cisco Business Dashboard (CBD) Version 2.5.1 und höher beschrieben.

Unterstützte Geräte | Software-Version

Cisco Business Dashboard | 2.5.1 ([Aktuelle Version herunterladen](#))

Serie CBW140 | 10.8.1.0 ([Aktuelle Version herunterladen](#))

Serie CBW150 | 10.3.2.0 ([Aktuelle Version herunterladen](#))

Einleitung

Die CBD-Version 2.5.1 hat eine externe Captive Portal-Seite für Netzwerke der Serien CBW140 und CBW150 implementiert. Diese Seite kann als Authentifizierungsseite für das Gastnetzwerk verwendet werden und bietet gegenüber lokalen Captive Portal-Seiten mehrere Vorteile.

Anstatt den Client an die lokale Captive Portal-Seite unter 192.0.2.1 umzuleiten, wird er mithilfe des FQDN- und SSL-Zertifikats des CBD an CBD umgeleitet. Dadurch wird vermieden, dass die von modernen Browsern implementierte HTTP Strict Transport Security (HSTS) aktiviert wird.

Die externe Captive Portal-Seite bietet eine vereinfachte Bereitstellung, die das Management mehrerer Standorte mit Gastnetzwerken vereinfacht.

Alle Einstellungen für die Seite und die Authentifizierungsrichtlinien werden im CBD konfiguriert.

Wenn Sie das Gastnetzwerk einrichten, unterstützt es die Web-Zustimmung, die E-Mail-Adresse und die Anmeldung bei CBD-Konten oder die Weiterleitung an einen anderen RADIUS-Server.

Inhalt

- [Anforderungen an das Gastnetzwerk](#)
- [Gastauthentifizierung konfigurieren](#)
- [Konfigurieren des Wireless LAN](#)
- [Einstellungen für CBW-Gastnetzwerk](#)
- [Captive Portal-Seite](#)

Anforderungen an das Gastnetzwerk

Um die neue Seite "Guest Network Authentication" zu verwenden, müssen Sie

CBD-Version 2.5.1

Firmware der Serie CBW140 10.8.1.0 (oder höher)

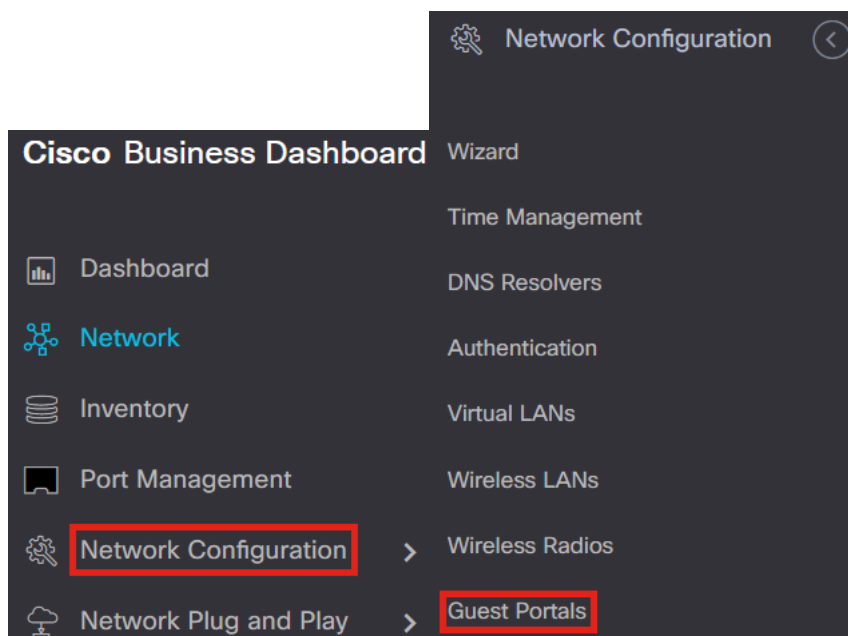
Firmware der Serie CBW150 10.3.2.0 (oder höher)

Gastauthentifizierung konfigurieren

So konfigurieren Sie die Captive Portal-Webseite:

Schritt 1

Melden Sie sich bei Ihrem CBD an, und navigieren Sie zu **Network Configuration > Guest Portals**.



Schritt 2

Auf der Seite *Guest Portals* (Gastportale) wird die Webseite jeder CBD-Organisation angezeigt. Um eine Seite zu bearbeiten, wählen Sie das Profil aus, und drücken Sie die Schaltfläche Bearbeiten.

Guest Portals

	Profile Name	Organization
2		
1	Default guest portal	Default

Wenn Sie über zwei oder mehr Netzwerke verfügen, für die individuelle Captive Portal-Seiten erforderlich sind, müssen Sie separate CBD-Organisationen einrichten, und jedes

Netzwerk muss der separaten Organisation beitreten.

Schritt 3

Die Konfigurationsoptionen umfassen:

- *Profilname*: Hierbei handelt es sich um eine eindeutige Kennung innerhalb von CBD, sodass Sie leicht verfolgen können, welche Seite zu den einzelnen Organisationen gehört.
- *Organisation* - Zeigt an, mit welcher Organisation das Captive Portal verbunden ist.
- *Header Text (Kopfzeilentext)*: Zeigt die Kopfzeile an, die vom Webbrowser angezeigt wird.
- *Hintergrundbild* und *Logo-Bild* zeigen, wo Sie die Grafiken ziehen und ablegen können, um sie auf Ihrer Captive Portal-Seite anzuzeigen.
- Die Felder *Vordergrund*, *Hintergrund*, *Trennzeichen*, *Inhaltsvordergrund*, *Inhaltshintergrund* und *Kontentipps Hintergrundfarbe* ermöglichen Ihnen, die Farbe der jeweiligen Aspekte Ihres Bildschirms zu ändern.
- Im Menü *Schriftarten* können Sie die Schriftart auswählen, die auf der Captive Portal-Seite verwendet wird.
- In den anderen Feldern können Sie den auf der Seite angezeigten Text bearbeiten.

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), Foreground Color, Background Color.
- Appearance and Content:** Separator Color, Content Foreground Color, Content Background Color, Account Tips Background Color, 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, No Acceptance Warning, Work In Progress Message, Invalid Credentials Message, Connection Succeeded Message, Welcome Message.

Schritt 4

Klicken Sie auf eine der folgenden Registerkarten, um die Textoptionen für die Authentifizierung zu konfigurieren.

- Benutzername/Kennwort
- Web-Zustimmung
- Email-Adresse

Klicken Sie auf die Schaltfläche **Vorschau**, um zu sehen, wie die einzelnen Menüoptionen angezeigt werden.

Username/Password Web Consent Email Address

Preview

Schritt 5

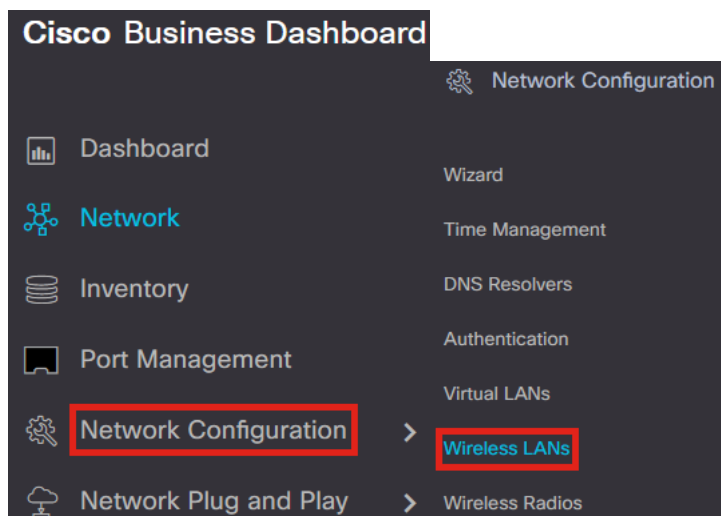
Nachdem Sie die Webseite angepasst haben, klicken Sie auf **Aktualisieren** oder **Abbrechen**.

Login Instructions	To start using this service, enter your credentials and click the connect button
Username Input Label	Username
Password Input Label	Password
Input Prompt	Enter your Username/Password
Enable Acceptable Use Policy	<input checked="" type="checkbox"/>
	Update Cancel

Konfigurieren des Wireless LAN

Schritt 1

Navigieren Sie zu **Network Configuration > Wireless LANs** (Netzwerkkonfiguration > WLANs).



Schritt 2

Sie können ein vorhandenes *WLAN*-Profil hinzufügen oder bearbeiten. In diesem Beispiel ist **add** ausgewählt.



Schritt 3

Geben Sie den *Profilnamen*, die *Organisation* und die *Gerätegruppen* innerhalb der Organisation an, auf die dies angewendet werden soll.

Wireless LANs->Add WLAN

Device Group Selection

Profile Name ✓ 1

Organization ✓ 2

Device Groups

Available Groups

Default

>

<

>>

<<

Selected Groups

3

Sie können einfach die *Standard-Organisation* und die *Standard-Gerätegruppe* auswählen.

Schritt 4

Fügen Sie ein Wireless LAN hinzu, indem Sie auf das **Plus**-Symbol klicken.

Wireless LANs



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

Schritt 5

Geben Sie den *SSID-Namen* und die *VLAN-ID* an. Wählen Sie im Dropdown-Menü *Security (Sicherheit)* die Option **Guest** aus.

Add Wireless LANs



Enable Enable

SSID Name ✓ 1

VLAN ID ✓ 2

Security 3

Schritt 6

Wählen Sie die Methode zur *Gastauthentifizierung* aus. Folgende Optionen sind verfügbar:

- Benutzername/Kennwort
- Web-Zustimmung
- Email-Adresse

Guest authentication

▼ Advanced Settings

Broadcast

Schritt 7

Unter *Erweiterte Einstellungen* können Sie auch angeben, ob die SSID die Einstellungen *Broadcast*, *Application Visibility (Anwendungstransparenz)*, *Local Profiling (Lokale Profilerstellung)* und *Radio (Funkübertragung)* aufweisen soll.

▼ Advanced Settings

Broadcast

 Enable

Application Visibility

 Enable

Local Profiling

 Enable

Radio

In den meisten Fällen behalten Sie die Standardeinstellung bei.

Schritt 8

Klicken Sie auf **Speichern**.

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

Schritt 9

Klicken Sie erneut auf **Speichern**.

Wireless LANs->Add WLAN

Device Group Selection

Profile Name

 ✓

Organization

 ✓

Device Groups

Available Groups: Default | Selected Groups

Einstellungen für CBW-Gastnetzwerk

Schritt 1

Melden Sie sich bei Ihrem Cisco Business Wireless Access Point (CBW) an.



Cisco Business Wireless Access Point

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

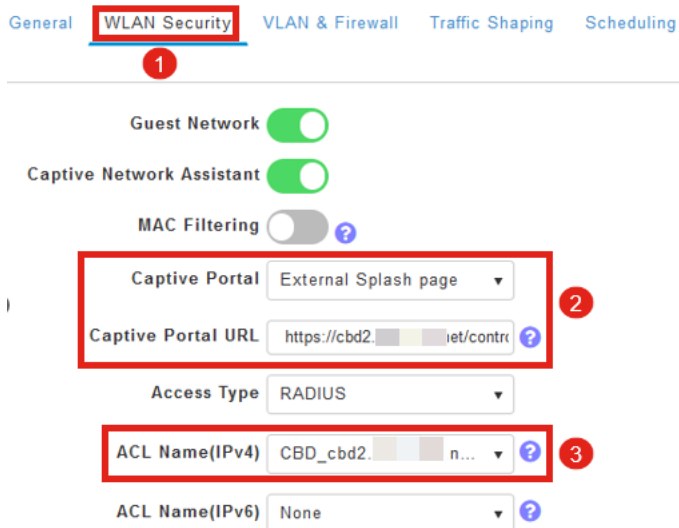


Schritt 2

Navigieren Sie zu **Wireless Settings > WLANs**.

Schritt 3

Sie können das WLAN bearbeiten und zur Registerkarte **WLAN-Sicherheit** wechseln. Für *Captive Portal* wird die **externe Splash-Seite** mit der *Captive Portal-URL* Ihres CBD-Servers festgelegt. Der *ACL-Name* wird automatisch konfiguriert.



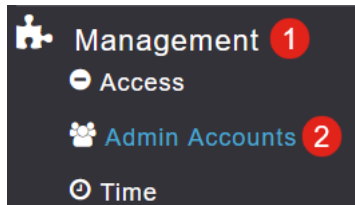
Schritt 4

Der RADIUS-Server wird automatisch konfiguriert. Wechseln Sie zur **Expertenansicht**, indem Sie oben auf der Seite auf den bidirektionalen Pfeil klicken.



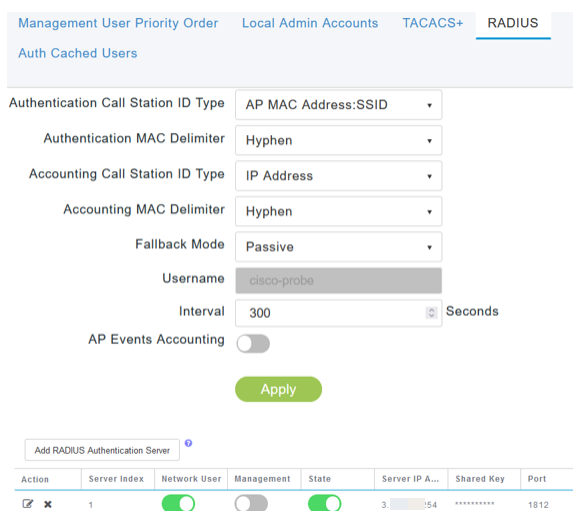
Schritt 5

Navigieren Sie zu **Management > Admin Accounts**.



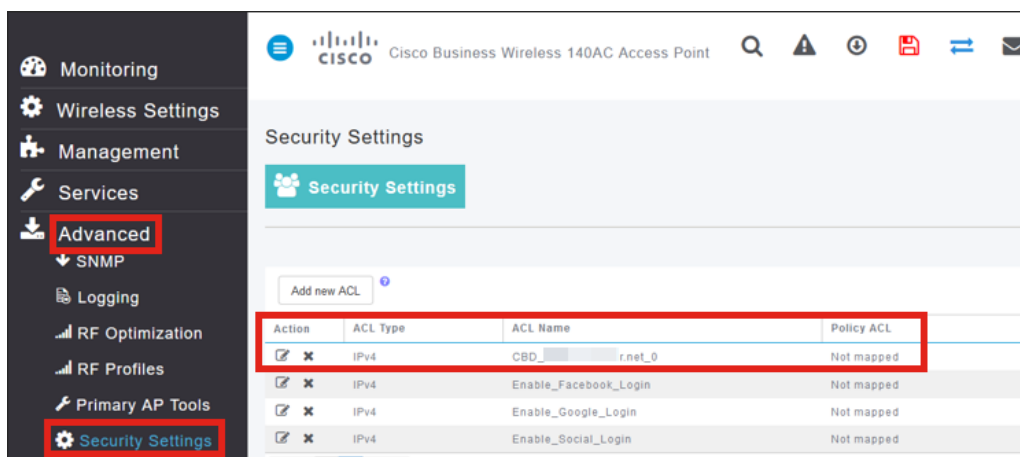
Schritt 6

Klicken Sie auf die Registerkarte **RADIUS**.



Schritt 7

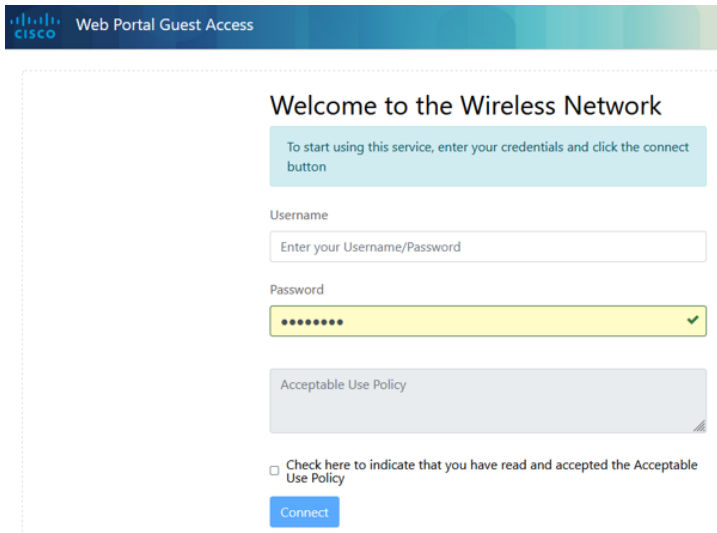
Außerdem wird dynamisch eine Sicherheits-ACL für CBD unter **Advanced > Security Settings (Erweitert > Sicherheitseinstellungen)** hinzugefügt.



Captive Portal-Seite

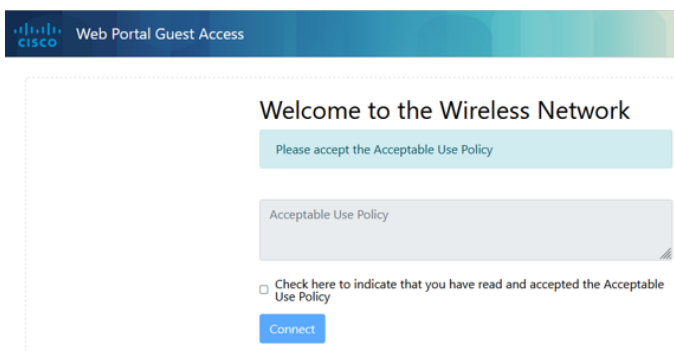
Je nachdem, wie Sie die Einstellungen konfiguriert haben, sieht die Captive Portal-Seite wie folgt aus:

Benutzername/Kennwort-Authentifizierung



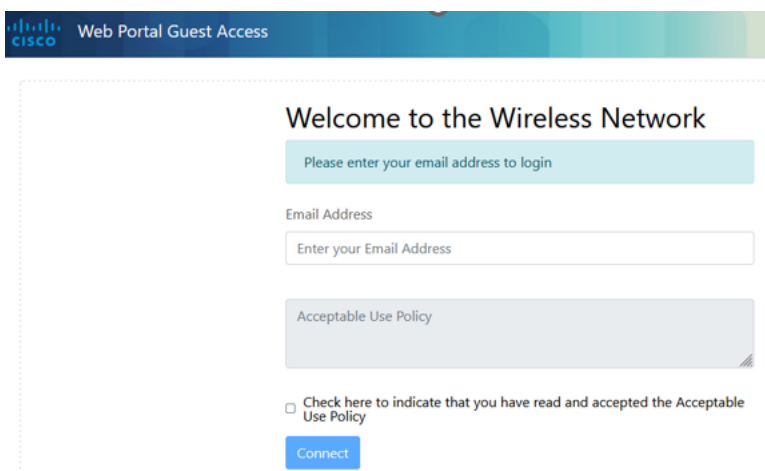
The screenshot shows the 'Web Portal Guest Access' interface. At the top, there is a header with the Cisco logo and the text 'Web Portal Guest Access'. Below the header, the main content area is titled 'Welcome to the Wireless Network'. A light blue box contains the instruction: 'To start using this 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.

Web-Zustimmung



The screenshot shows the '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.

E-Mail-Authentifizierung



The screenshot shows the '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.

Schlussfolgerung

Du hast es geschafft! Sie haben die externe Captive Portal-Seite erfolgreich mit CBD eingerichtet.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.