

Portail externe captif dans le tableau de bord Cisco Business

Objectif

L'objectif de cet article est de passer en revue les étapes de configuration de la fonctionnalité externe Captive Portal dans Cisco Business Dashboard (CBD) version 2.5.1 et ultérieure.

Périphériques pertinents | Version du logiciel

Tableau de bord Cisco Business | 2.5.1 ([Télécharger la dernière version](#))

Gamme CBW140 | 10.8.1.0 ([Télécharger la dernière version](#))

Gamme CBW150 | 10.3.2.0 ([Télécharger la dernière version](#))

Introduction

La version 2.5.1 de CBD a mis en oeuvre une page Captive Portal externe pour les réseaux des gammes CBW140 et CBW150. Cette page peut être utilisée comme page d'authentification de réseau invité et offre plusieurs avantages par rapport aux pages du portail captif local.

Au lieu de rediriger le client vers la page locale Captive Portal à l'adresse 192.0.2.1, il redirige vers CBD à l'aide du nom de domaine complet (FQDN) et du certificat SSL de CBD. Cela évite de déclencher le HTTP Strict Transport Security (HSTS) amélioré que les navigateurs modernes ont mis en oeuvre.

La page externe Captive Portal est dotée d'un déploiement simplifié qui facilite la gestion de plusieurs sites avec des réseaux invités.

Tous les paramètres de la page et les stratégies d'authentification sont configurés dans CBD.

Lorsque vous configurez le réseau invité, il prend en charge le consentement Web, l'adresse e-mail et la connexion aux comptes CBD ou l'accès à un autre serveur RADIUS.

Table des matières

- [Configuration réseau requise pour les invités](#)
- [Configurer l'authentification invité](#)
- [Configuration du LAN sans fil](#)
- [Paramètres du réseau invité CBW](#)
- [Page Captive Portal](#)

Configuration réseau requise pour les invités

Pour utiliser la nouvelle page Authentification du réseau invité, vous devez avoir

CDB version 2.5.1

Microprogramme de la gamme CBW140 10.8.1.0 (ou version ultérieure)

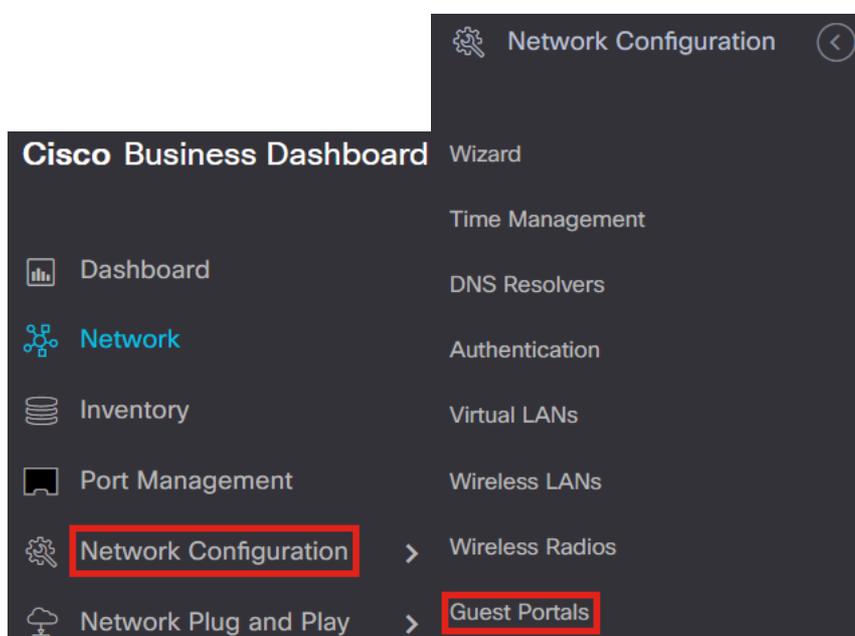
Microprogramme de la gamme CBW150 10.3.2.0 (ou version ultérieure)

Configurer l'authentification invité

Pour configurer la page Web du portail captif :

Étape 1

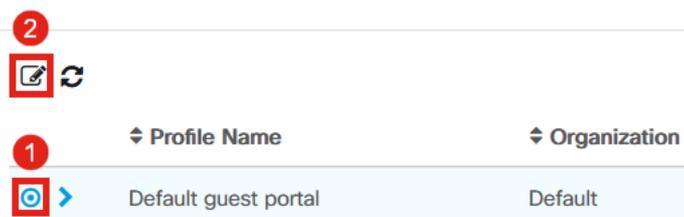
Connectez-vous à votre CBD et accédez à **Network Configuration > Guest Portals**.



Étape 2

La page *Guest Portals* affiche la page Web de chaque organisation CBD. Pour modifier une page, sélectionnez le profil et appuyez sur le bouton Modifier.

Guest Portals



Si vous disposez d'au moins deux réseaux nécessitant des pages de portail captives

uniques, vous devrez configurer des organisations CBD distinctes et faire en sorte que chaque réseau rejoigne l'organisation distincte.

Étape 3

Les options de configuration incluent :

- *Nom du profil* - Il s'agit d'un identifiant unique au sein de CBD, ce qui vous permet de savoir facilement quelle page est associée à chaque organisation.
- *Organisation* : indique l'organisation à laquelle le portail captif est connecté.
- *Texte d'en-tête* - Affiche l'en-tête qui sera affiché par le navigateur Web.
- *Image d'arrière-plan* et *image de logo* montrent où vous pouvez faire glisser et déposer dans les graphiques à afficher sur votre page du portail captif.
- Les champs de couleur de premier plan, d'arrière-plan, de séparateur, de premier plan de contenu, d'arrière-plan de contenu et d'arrière-plan des conseils de compte vous permettent tous de modifier la couleur des aspects respectifs de votre affichage.
- Le menu *Polices* vous permet de choisir la police utilisée sur la page du portail captif.
- Les autres champs vous permettent de modifier le texte qui s'affiche sur la page.

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 (white), Background Color (blue).
- Separator Color:** A grey bar.
- Content Foreground Color:** A black bar.
- Content Background Color:** A white bar.
- Account Tips Background Color:** A light blue bar.
- Fonts:** Arial.
- Button Label:** Connect.
- Browser Header Text:** Captive Portal.
- Portal Title:** Welcome to the Wireless Network.
- Acceptable Use Policy:** Acceptance Use Policy.

On the right side, there are several message templates for authentication:

- 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

Étape 4

Cliquez sur l'un des onglets suivants pour configurer les options de texte pour l'authentification.

- Nom d'utilisateur/Mot de passe
- Consentement Web
- Adresse électronique

Cliquez sur le bouton **Preview** pour voir comment chacune des options de menu sera affichée.

Preview

Étape 5

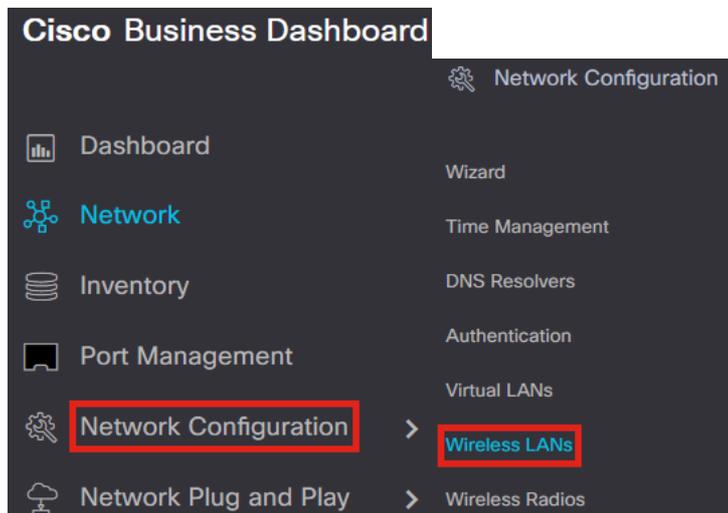
Après avoir personnalisé la page Web, cliquez sur **Update** ou sur *Cancel*.

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

Configuration du LAN sans fil

Étape 1

Accédez à **Network Configuration > Wireless LANs**.



Étape 2

Vous pouvez ajouter ou modifier un profil de *réseau local sans fil* existant. Dans cet exemple, **add** est sélectionné.



Étape 3

Spécifiez le *nom* du *profil*, l'*organisation* et les *groupes de périphériques* au sein de l'organisation à laquelle s'appliquera ce profil.

Wireless LANs->Add WLAN

Device Group Selection

Profile Name ✓ 1

Organization ✓ 2

Device Groups

Available Groups

Default

>

<

>>

<<

Selected Groups

3

Vous pouvez simplement choisir l'organisation *par défaut* et le groupe de périphériques *par défaut*.

Étape 4

Ajoutez un réseau local sans fil en cliquant sur l'icône **plus**.

Wireless LANs



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

Étape 5

Spécifiez le *nom SSID* et l'*ID VLAN*. Sélectionnez **Guest** dans le menu déroulant *Security*.

Add Wireless LANs



Enable

SSID Name ✓ 1

VLAN ID ✓ 2

Security 3

Étape 6

Sélectionnez la méthode *d'authentification Invité*. Les options sont les suivantes :

- Nom d'utilisateur/Mot de passe
- Consentement Web
- Adresse électronique

Guest authentication

▼ Advanced Settings

Broadcast

Étape 7

Sous *Advanced Settings*, vous pouvez également spécifier si vous voulez que le SSID diffuse, les paramètres *Application Visibility*, *Local Profiling* et *Radio*.

▼ Advanced Settings

Broadcast

 Enable

Application Visibility

 Enable

Local Profiling

 Enable

Radio

Dans la plupart des cas, vous conservez ces paramètres par défaut.

Étape 8

Cliquez sur **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

Étape 9

Cliquez à nouveau sur **Save**.

Wireless LANs->Add WLAN

Device Group Selection

Profile Name

Organization

Device Groups

Available Groups		Selected Groups
Default	>	
	<	

Paramètres du réseau invité CBW

Étape 1

Connectez-vous à votre point d'accès Cisco Business Wireless (CBW).



Cisco Business Wireless Access Point

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

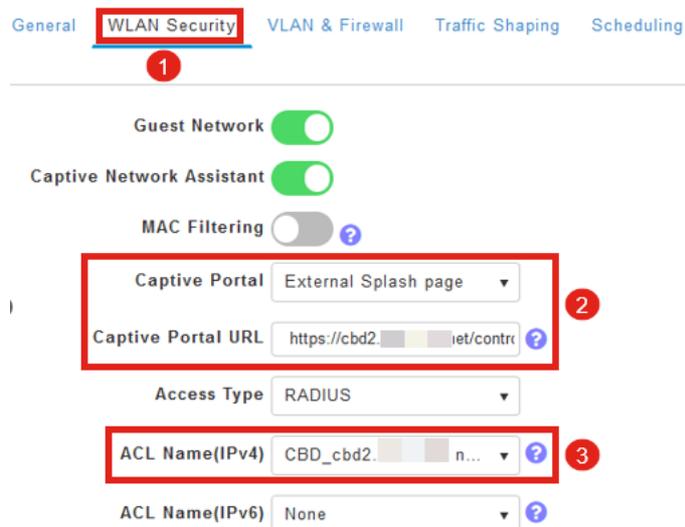


Étape 2

Accédez à **Wireless Settings > WLAN**.

Étape 3

Vous pouvez modifier le WLAN et aller à l'onglet **WLAN Security**. Le *portail captif* sera défini sur la **page External Splash** avec l'*URL du portail captif* de votre serveur CBD. Le *nom de la liste de contrôle d'accès* sera automatiquement configuré.



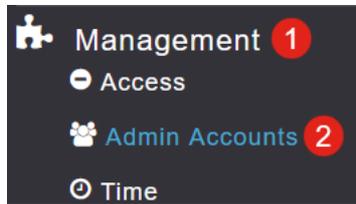
Étape 4

Le serveur RADIUS est automatiquement configuré. Pour l'afficher, passez à **Expert View** en cliquant sur la flèche bidirectionnelle en haut de la page.



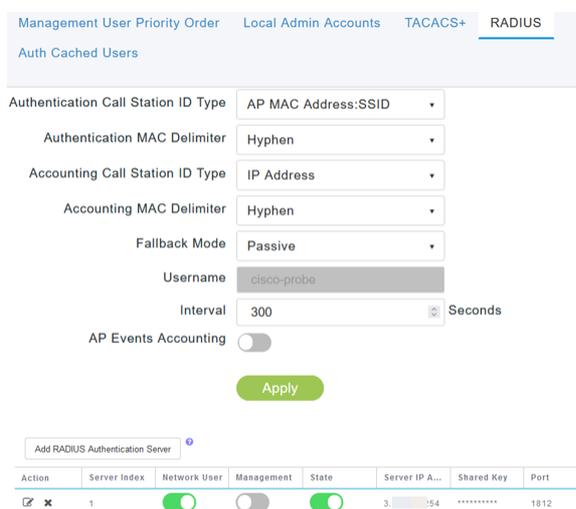
Étape 5

Accédez à **Management > Admin Accounts**.



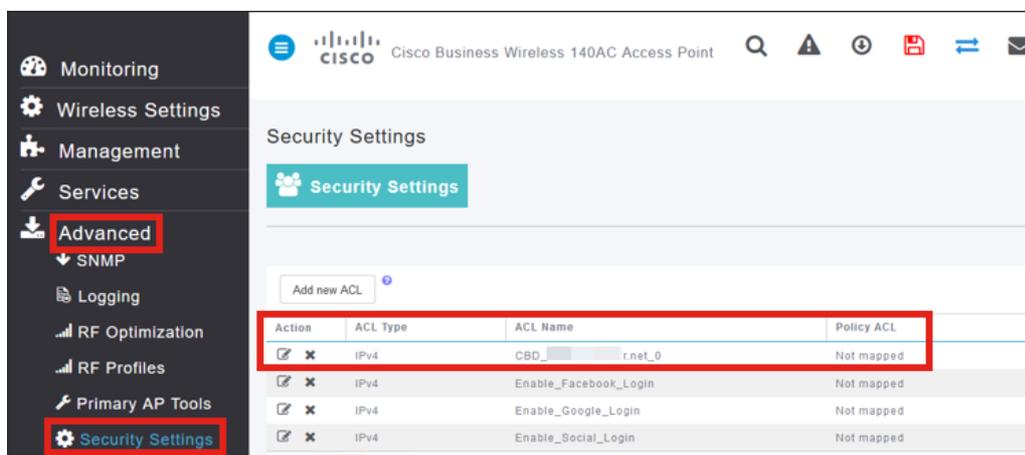
Étape 6

Cliquez sur l'onglet **RADIUS**.



Étape 7

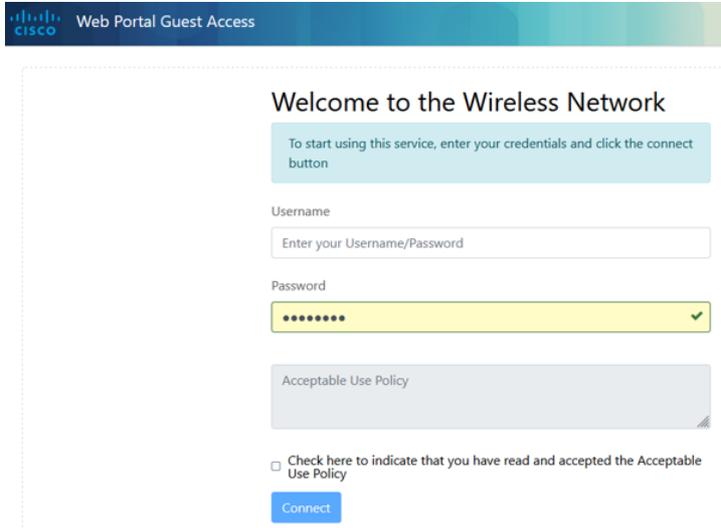
Il ajoutera également dynamiquement une ACL de sécurité pour CBD sous **Advanced > Security Settings**.



Page Captive Portal

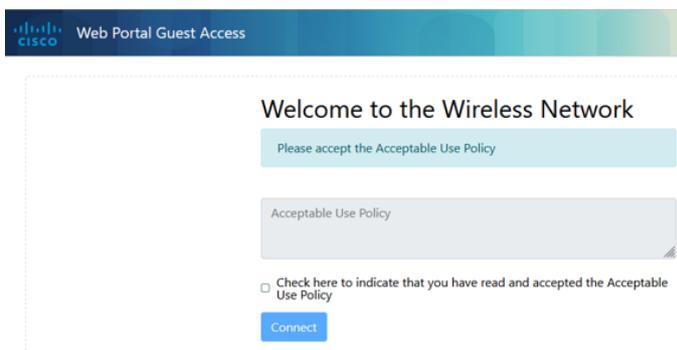
D'après la configuration des paramètres, la page du portail captif ressemblera à ce qui suit :

Authentification par nom d'utilisateur/mot de passe



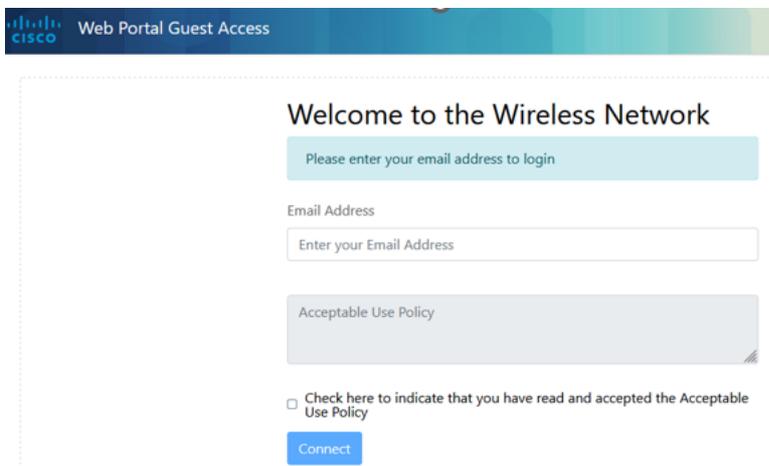
The screenshot shows the Cisco Web Portal Guest Access interface. At the top, there is a header with the Cisco logo and the text "Web Portal Guest Access". Below the header, the main content area is titled "Welcome to the Wireless Network". A light blue box contains the instruction: "To start using this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

Consentement 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.

Authentification du courrier électronique



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.

Conclusion

Tu l'as fait ! Vous avez correctement configuré la page Captive Portal externe à l'aide de CBD.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.