

Authentification sans fil via Cisco Business Dashboard

Objectif

L'objectif de cet article est de passer en revue la fonctionnalité d'authentification sans fil à l'aide de Cisco Business Dashboard (CBD) version 2.5.0.

Périphériques pertinents | Version du logiciel

- Tableau de bord Cisco Business | 2.5.0 ([Télécharger la dernière version](#))
- CBW140AC | [Télécharger la dernière](#)
- CBW145AC | [Télécharger la dernière](#)
- CBW240AC | [Télécharger la dernière](#)
- CBW150AX | [Télécharger la dernière](#)

Introduction

CBD fournit des outils qui vous aident à surveiller et à gérer les périphériques de votre réseau d'entreprise Cisco. Il détecte automatiquement votre réseau et vous permet de configurer et de surveiller tous les périphériques pris en charge, tels que les commutateurs, les routeurs et les points d'accès sans fil.

CBD 2.5.0 ajoute la fonctionnalité de service d'authentification à CBD. Le nouveau service est pris en charge sur les périphériques CBW140/240 et CBW 150AX.

Il configure une instance FreeRADIUS sur le gestionnaire CBD à utiliser pour l'authentification RADIUS, donnant à votre organisation un moyen simple de déployer un serveur sans que les clients aient à connaître ou comprendre RADIUS.

Si vous êtes prêt à commencer, laissez-nous plonger.

Table des matières

- [Configurer le profil d'authentification](#)
- [Configuration des réseaux sans fil](#)
- [Vérification](#)
- [Test](#)

Configurer le profil d'authentification


Vous devez d'abord configurer le profil d'authentification que vous utiliserez pour votre organisation. Dans de nombreux cas, vous pouvez simplement utiliser le profil par

défaut.

Étape 1

Connectez-vous à CBD.

English ▾



Cisco Business Dashboard

User Name* 1

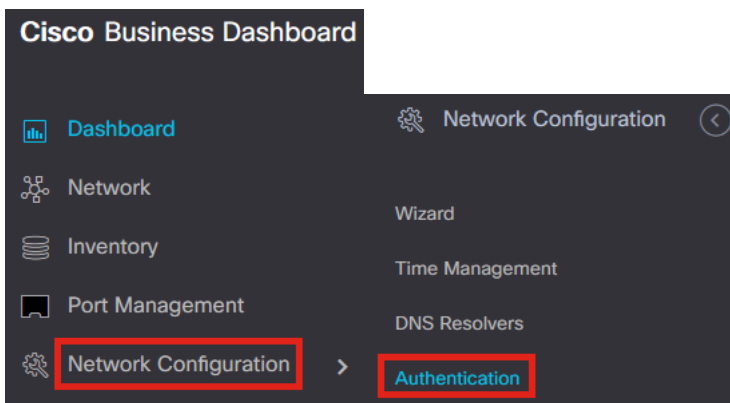
This field is required

Password* 2

Login 3

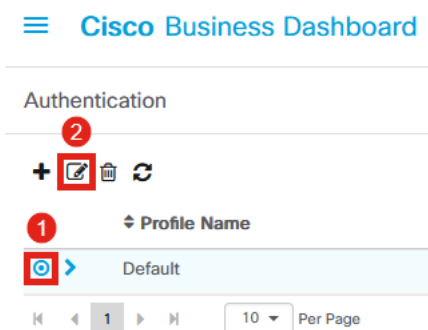
Étape 2

Accédez à **Network Configuration > Authentication**.



Étape 3

Vous pouvez modifier le profil *par défaut* existant ou en ajouter un autre. Dans cet exemple, le profil **par défaut** est sélectionné. Cliquez sur **Edit**.



Étape 4

Dans CBD 2.5.0, il y a une nouvelle option pour sélectionner *Use Cisco Business Dashboard Authentication Service*. Cette option est activée par défaut. Effectuez les modifications souhaitées et cliquez sur **Update**.

☰ Cisco Business Dashboard

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.

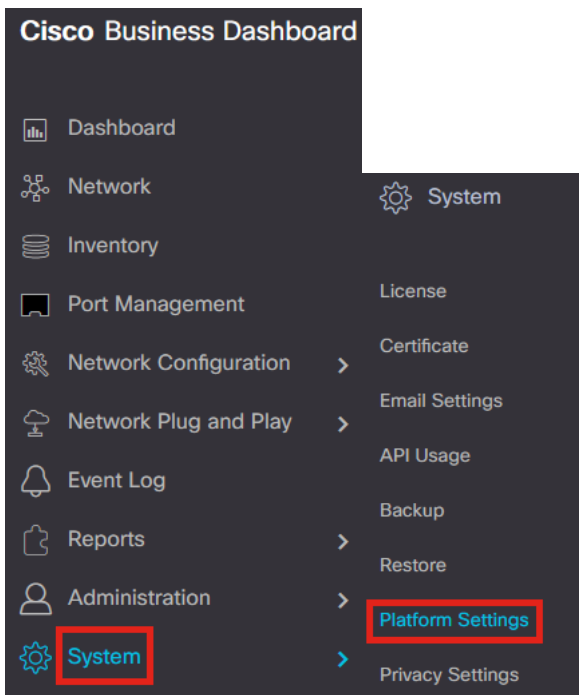
+ Add custom authentication server

2

Assurez-vous de voir si *System > Platform Settings > System Variables* ont les paramètres corrects pour permettre au tableau de bord d'être atteint par les périphériques réseau.

Étape 5

Accédez à **Système > Paramètres de la plate-forme** dans le menu.



Étape 6

Sélectionnez l'onglet **Variables système**.

Platform Settings

Network Settings Web Server **System Variables**

Étape 7

Vérifiez les paramètres pour vous assurer que l'adresse IP du tableau de bord externe est l'adresse IP publique du CBD et que le port du serveur d'authentification externe est 1812. Il s'agit du port par défaut. Cliquez **Save**.

Platform Settings

Network Settings Web Server **System Variables**

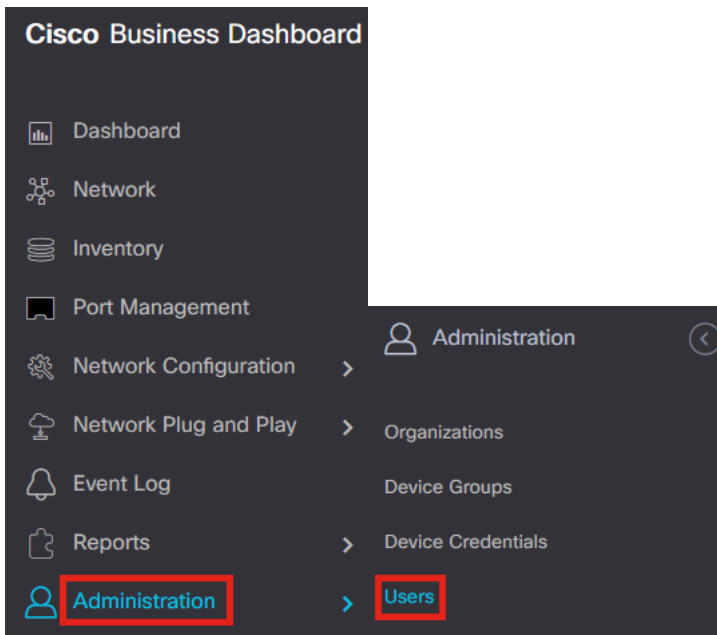
External System Settings

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

Étape 8

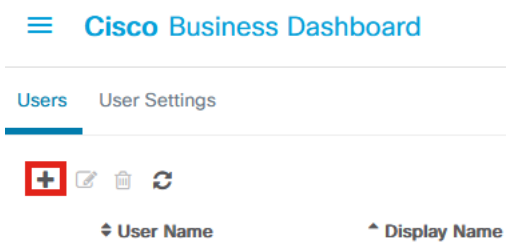
Pour créer des utilisateurs qui vont s'authentifier sur le système, accédez à

Administration > Users.



Étape 9

Pour ajouter des utilisateurs, cliquez sur l'icône plus.



Étape 10

Configurez les éléments suivants :

- *nom de l'utilisateur*
- *Nom d'affichage*
- *Courriel*
- *Accès au tableau de bord* - sélectionnez dans le menu déroulant. Dans cet exemple, **No Access** est sélectionné.
- *Nouveau mot de passe*
- *Retapez le nouveau mot de passe*

Les autres champs sont facultatifs. Cliquez **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	<div><div style="width: 100%;"></div></div> 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"/>

Étape 11

Cliquez sur l'onglet **Organisations**.

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

Access Key **Organizations**

Étape 12

Ici, vous devez associer l'utilisateur que vous venez de créer à votre organisation CBD. Cliquez sur l'**icône plus** et choisissez l'option dans le menu déroulant. Dans cet exemple, **Default** est sélectionné.

Access Key **Organizations**

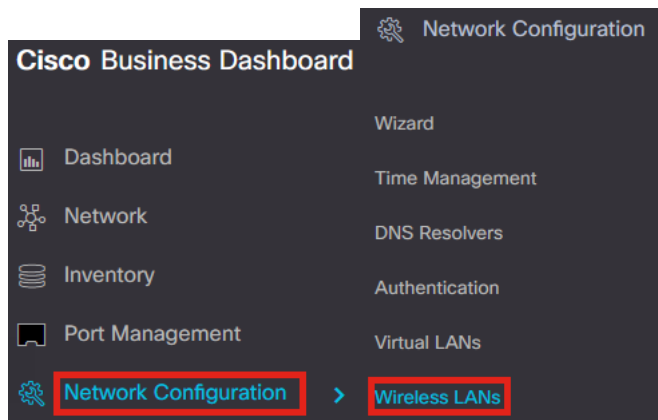
<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	▼ Org Name
<input type="checkbox"/>	Default

Cet utilisateur peut désormais se connecter à l'organisation par défaut configurée pour l'authentification sans fil.

Configuration des réseaux sans fil

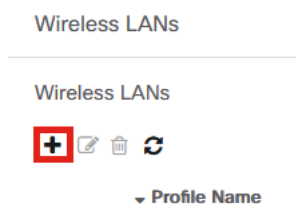
Étape 1

Accédez au menu **Network Configuration > Wireless LANs**.



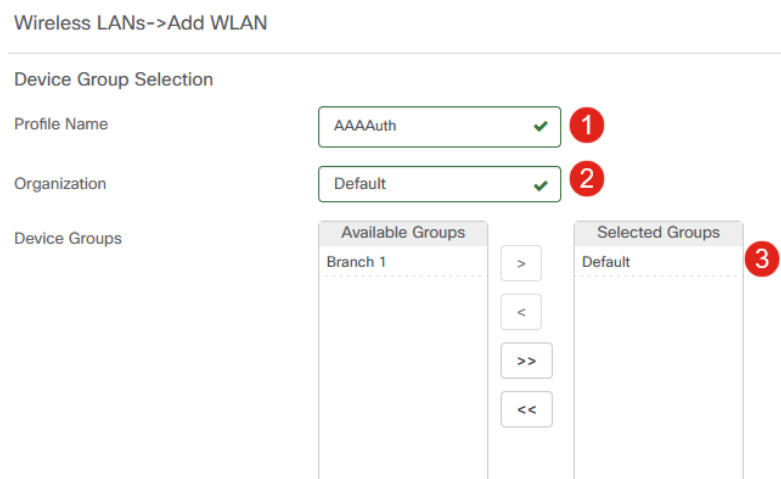
Étape 2

Pour créer un nouveau profil, cliquez sur l'**icône plus** sous *Réseaux locaux sans fil*.



Étape 3

Saisissez le *nom du profil*, l'*organisation* et configurez les *groupes de périphériques* pour appliquer les paramètres aux périphériques sans fil du groupe.



Étape 4

Pour créer un SSID, cliquez sur l'**icône plus**.



SSID Name

Étape 5

Entrez le *SSID Name*, *VLAN ID* et sélectionnez *Security* dans le menu déroulant. Dans cet exemple, **WPA2-Enterprise** est sélectionné. Cliquez **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

Cisco Business Dashboard Authentication Server sera utilisé si aucun serveur d'authentification n'est configuré.

Étape 6

Cliquez à nouveau sur **Save** pour appliquer les paramètres du réseau sans fil et de Radius à tous les clients.

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	

Vérification

Pour vérifier si les paramètres ont été appliqués,

Étape 1

Connectez-vous à votre point d'accès CBW.



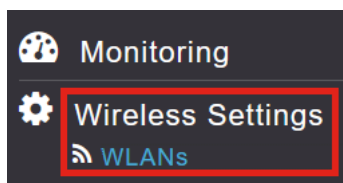
Cisco Business Wireless Access Point

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



Étape 2

Accédez à **Wireless Settings > WLANs**.



Étape 3

Le SSID que vous avez créé sera répertorié. Dans cet exemple, il s'agit de **AAATest**.

WLANs

Active WLANs 2

Add new WLAN/RLAN

Action	Active	Type	Name	SSID	Security Policy	Radio Policy
	Enabled	WLAN	CBWWireless	CBWWireless	Personal(WPA2)	ALL
	Enabled	WLAN	AAATest	AAATest	WPA2Enterprise	ALL

Étape 4

Sélectionnez le SSID et cliquez sur **edit** pour afficher les paramètres.

WLANS

Active WLANS 2

Add new WLAN/RLAN

Action	Active	Type	Name
	Enabled	WLAN	CBWireless
	Enabled	WLAN	AAATest

Étape 5

Accédez à l'onglet **WLAN Security**.

Edit WLAN

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

Vous verrez que le *type de sécurité* sera répertorié comme **WPA2 Enterprise** et que le *serveur d'authentification* sera le **Radius externe**. L'adresse IP du serveur sera celle que vous avez configurée précédemment.

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

Étape 6

Passez en **mode Expert** en cliquant sur la flèche bidirectionnelle située en haut de l'interface utilisateur.



Étape 7

Accédez à **Management > Admin Accounts**.

Management 1

Access


Admin Accounts 2

Time

Étape 8

Cliquez sur l'onglet **RADIUS**.



Admin Accounts

 **Users** 1

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

Vous verrez que le serveur d'authentification Radius a été configuré pour *Utilisateur réseau*.

[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

Test

Pour tester les paramètres :

Étape 1


Accédez à **Avancé > Outils AP principaux**.

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

Étape 2

Cliquez sur l'onglet **Outils de dépannage**.

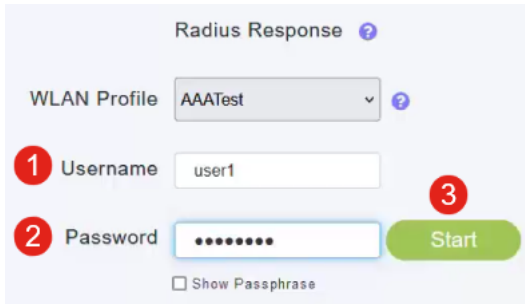
Primary AP Tools

 **Tools**

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

Étape 3

Sous la section *Radius Response*, entrez le **nom d'utilisateur** et le mot de **passé** et cliquez sur **Start** pour voir s'il s'authentifie auprès du serveur Radius.



The screenshot shows the 'Radius Response' configuration page. It includes a dropdown menu for 'WLAN Profile' set to 'AAATest'. Below it are input fields for 'Username' (containing 'user1') and 'Password' (masked with dots). A green 'Start' button is positioned to the right of the password field. Red numbered callouts (1, 2, 3) point to the Username, Password, and Start button respectively. A 'Show Passphrase' checkbox is located below the password field.

Une fois le test terminé, une notification de *réussite* d'authentification s'affiche.



This screenshot shows the same 'Radius Response' configuration page after the test. The 'Start' button is now highlighted in green. A blue notification bar with a green checkmark icon is displayed at the bottom right, containing the text 'Authentication success (3.1 254)'. A red rectangular box highlights this notification bar.

Assurez-vous que vous avez une connectivité IP entre le gestionnaire CBD et le système client pour que cela fonctionne correctement.

Conclusion

C'est tout ! Vous n'avez plus à vous soucier de configurer Radius vous-même. CBD fera tout le travail et vous pourrez vous asseoir, vous détendre et profiter des avantages de l'authentification sans fil dans votre réseau.

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.