

Wireless-Authentifizierung mit Cisco Business Dashboard

Ziel

In diesem Artikel wird die Wireless-Authentifizierungsfunktion mit Cisco Business Dashboard (CBD) Version 2.5.0 behandelt.

Unterstützte Geräte | Software-Version

- Cisco Business Dashboard | 2.5.0 (Aktuelle Version herunterladen)
- CBW140AC | [Neueste Version herunterladen](#)
- CBW145AC | [Neueste Version herunterladen](#)
- CBW240AC | [Neueste Version herunterladen](#)
- CBW150AX | [Neueste Version herunterladen](#)

Einleitung

CBD bietet Tools zur Überwachung und Verwaltung der Geräte in Ihrem Cisco Business-Netzwerk. Es erkennt automatisch Ihr Netzwerk und ermöglicht Ihnen die Konfiguration und Überwachung aller unterstützten Geräte wie Switches, Router und Wireless Access Points.

CBD 2.5.0 fügt CBD Authentifizierungsservicefunktionen hinzu. Der neue Service wird sowohl von den Geräten der Serie CBW140/240 als auch von den CBW 150AX-Geräten unterstützt.

Es richtet eine FreeRADIUS-Instanz auf dem CBD-Manager ein, die für die RADIUS-Authentifizierung verwendet werden kann, sodass Ihr Unternehmen einen Server einfach bereitstellen kann, ohne dass Clients RADIUS kennen oder verstehen müssen.

Wenn Sie bereit sind, starten Sie mit uns.

Inhalt

- [Authentifizierungsprofil konfigurieren](#)
- [Wireless-Netzwerke konfigurieren](#)
- [Verifizierung](#)
- [Tests](#)

Authentifizierungsprofil konfigurieren


Zunächst müssen Sie das Authentifizierungsprofil für Ihre Organisation konfigurieren.

In vielen Fällen können Sie einfach das Standardprofil verwenden.

Schritt 1

Melden Sie sich bei CBD an.

English ▾



Cisco Business Dashboard

User Name* 1

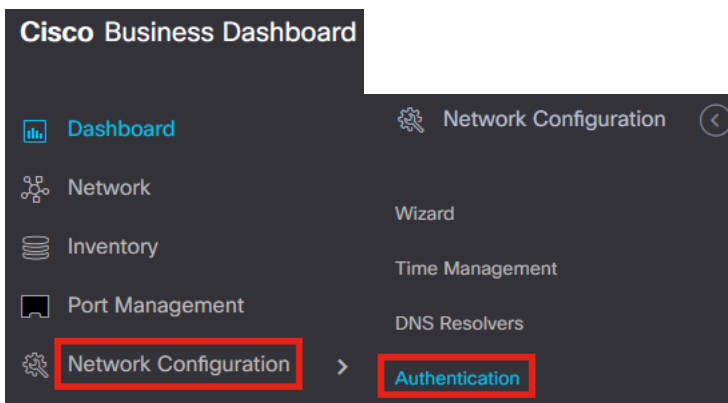
This field is required

Password* 2

Login 3

Schritt 2

Navigieren Sie zu **Netzwerkconfiguration > Authentifizierung**.







Schritt 3


Sie können das vorhandene *Standardprofil* bearbeiten oder ein anderes Profil hinzufügen. In diesem Beispiel ist das **Standard**-Profil ausgewählt. Klicken Sie auf **Bearbeiten**.

☰ Cisco Business Dashboard

Authentication 2

+    

1 Profile Name

 > Default

⏪ < 1 > ⏩ 10 ▾ Per Page

Schritt 4

Für CBD 2.5.0 gibt es eine neue Option zur Auswahl von *Cisco Business Dashboard Authentication Service verwenden*. Dies ist standardmäßig aktiviert. Nehmen Sie die gewünschten Änderungen vor, und klicken Sie auf **Aktualisieren**.

☰ Cisco Business Dashboard

Authentication->Update Default


Device Group Selection

Profile Name	<input type="text" value="Default"/>															
Organization	<input type="text" value="Default"/>															
Device Groups	<table><thead><tr><th>Available Groups</th><th></th><th>Selected Groups</th></tr></thead><tbody><tr><td>Branch 1</td><td>></td><td>Default</td></tr><tr><td></td><td><</td><td></td></tr><tr><td></td><td>>></td><td></td></tr><tr><td></td><td><<</td><td></td></tr></tbody></table>	Available Groups		Selected Groups	Branch 1	>	Default		<			>>			<<	
Available Groups		Selected Groups														
Branch 1	>	Default														
	<															
	>>															
	<<															

Authentication

Local User Authentication

 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

 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**

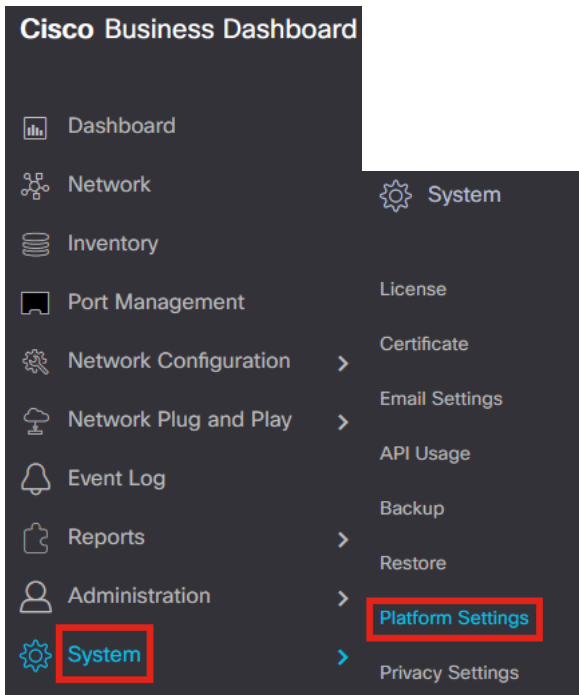
Update

Cancel

Vergewissern Sie sich, dass *System > Platform Settings > System Variables* über die richtigen Einstellungen verfügen, damit die Netzwerkgeräte das Dashboard erreichen können.

Schritt 5

Navigieren Sie im Menü zu **System > Platform Settings** (System > Plattformeinstellungen).



Schritt 6

Wählen Sie die Registerkarte **Systemvariablen** aus.

Platform Settings

Network Settings Web Server **System Variables**

Schritt 7

Überprüfen Sie die Einstellungen, um sicherzustellen, dass die *externe Dashboard-IP-Adresse* die öffentliche IP-Adresse des CBD und der *Port des externen Authentifizierungsservers* 1812 ist. Dies ist der Standardport. Klicken Sie auf **Speichern**

Platform Settings

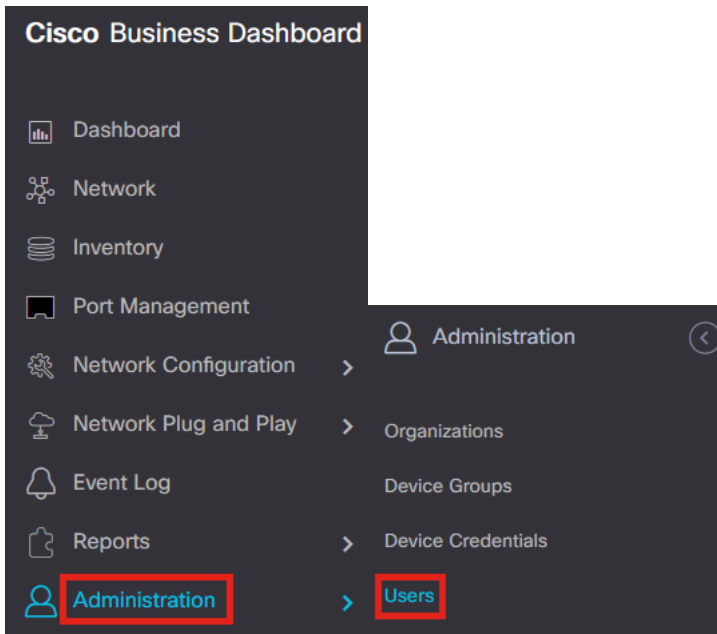
Network Settings Web Server **System Variables**

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

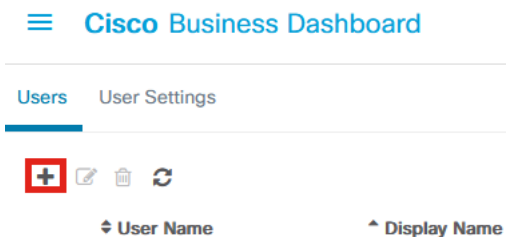
Schritt 8

Um Benutzer zu erstellen, die sich beim System authentifizieren, gehen Sie zu **Administration > Users**.



Schritt 9

Um Benutzer hinzuzufügen, klicken Sie auf das **Pluszeichen**.



Schritt 10

Konfigurieren Sie Folgendes:

- *Benutzername*
- *Anzeigename*
- *E-Mail*
- *Dashboard-Zugriff* - Wählen Sie diese Option aus dem Dropdown-Menü aus. In diesem Beispiel ist **Kein Zugriff** ausgewählt.
- *Neues Kennwort*
- *Neues Kennwort erneut eingeben*

Die anderen Felder sind optional. Klicken Sie auf **Speichern**.

Users > Add User

User Name ✓

Display Name ✓

Email ✓

Dashboard Access 1

Network Access

New Password ✓

Retype New Password ✓

Password Strength Normal

Address

City

Country/region

ZIP or Postal Code

Phone

2

Schritt 11

Klicken Sie auf die Registerkarte **Organisationen**.

☰ Cisco Business Dashboard

Users > user1

User Name
[Reset password](#)

Display Name

Email

Dashboard Access

Network Access

User Type
[Show account settings](#)

Create Time Jul 5 2022 09:31

Last Password Changed Time Jul 5 2022 09:31

Last Login Never

Access Key Organizations

Schritt 12

Hier müssen Sie den gerade erstellten Benutzer Ihrer CBD-Organisation zuordnen. Klicken Sie auf das **Pluszeichen**, und wählen Sie im Dropdown-Menü die gewünschte Option aus. In diesem Beispiel ist **Standard** ausgewählt.

Access Key Organizations

▼ Org Name

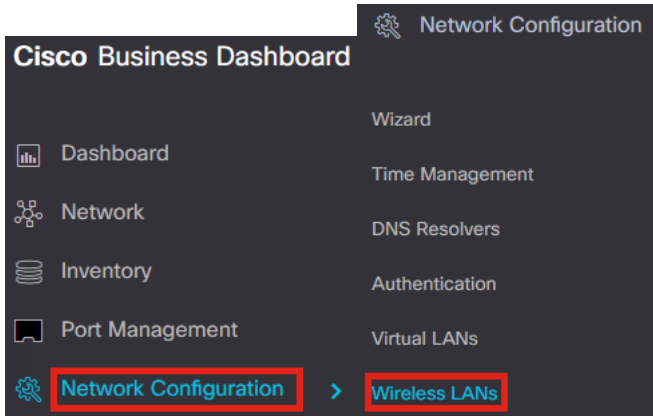
Default

Dieser Benutzer kann sich nun bei der Standardorganisation anmelden, die für die Wireless-Authentifizierung konfiguriert ist.

Wireless-Netzwerke konfigurieren

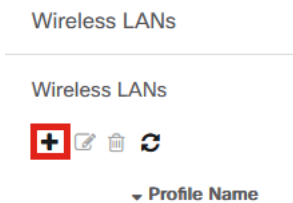
Schritt 1

Navigieren Sie zum Menü **Network Configuration > Wireless LANs** (Netzwerkconfiguration > WLANs).



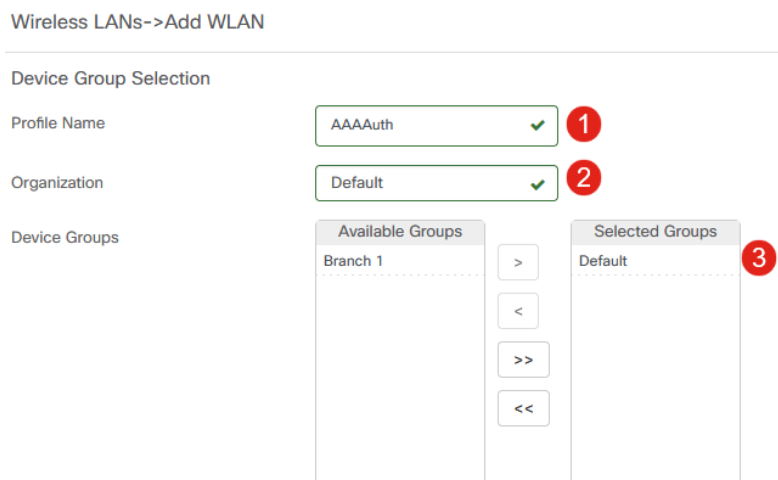
Schritt 2

Um ein neues Profil zu erstellen, klicken Sie auf das **Pluszeichen** unter *WLANs*.



Schritt 3

Geben Sie den *Profilnamen*, die *Organisation ein*, und konfigurieren Sie *Gerätegruppen*, um die Einstellungen auf die Wireless-Geräte in der Gruppe anzuwenden.



Schritt 4

Um eine SSID zu erstellen, klicken Sie auf das **Pluszeichen**.



SSID Name

Schritt 5

Geben Sie den *SSID-Namen* und die *VLAN-ID* ein, und wählen Sie im Dropdown-Menü die Option *Security (Sicherheit)* aus. In diesem Beispiel ist **WPA2-Enterprise** ausgewählt. Klicken Sie auf **Speichern**.

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**

4

Der Cisco Business Dashboard Authentication Server wird verwendet, wenn kein Authentifizierungsserver konfiguriert ist.

Schritt 6

Klicken Sie erneut auf **Speichern**, um die Einstellungen für das Wireless-Netzwerk und den Radius auf alle Clients anzuwenden.

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	

Verifizierung

Um zu überprüfen, ob die Einstellungen übernommen wurden,

Schritt 1

Melden Sie sich bei Ihrem CBW AP an.



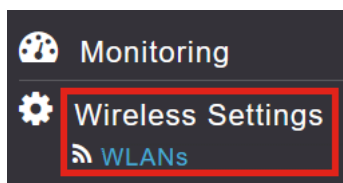
Cisco Business Wireless Access Point

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



Schritt 2

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



Schritt 3

Die von Ihnen erstellte SSID wird aufgelistet. In diesem Beispiel ist es **AAATest**.

WLANs

Active WLANs 2

Add new WLAN/RLAN

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

Schritt 4

Wählen Sie die SSID aus, und klicken Sie auf **Edit**, um die Einstellungen anzuzeigen.

WLANs

Active WLANs 2

Add new WLAN/RLAN

Action	Active	Type	Name
	Enabled	WLAN	CBWireless
	Enabled	WLAN	AAATest

Schritt 5

Navigieren Sie zur Registerkarte "WLAN Security".

Edit WLAN

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

Sie sehen, dass der *Sicherheitstyp* als **WPA2 Enterprise** aufgeführt wird und der *Authentifizierungsserver* als **externer RADIUS** festgelegt wird. Die *Server-IP-Adresse* ist die zuvor konfigurierte Adresse.

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

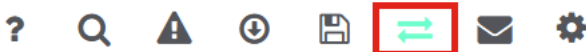
Authentication Caching

Add RADIUS Authentication Server

State	Server IP Address	Port
Enabled	3. 254	1812

Schritt 6

Wechseln Sie zur **Expertenansicht**, indem Sie oben auf der Benutzeroberfläche auf den bidirektionalen Pfeil klicken.



Schritt 7

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

Management 1

Access


Admin Accounts 2

Time

Schritt 8

Klicken Sie auf die Registerkarte **RADIUS**.



Admin Accounts

 **Users** 1

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

Sie sehen, dass der Radius-Authentifizierungsserver für *Netzwerkbenutzer* konfiguriert wurde.

[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

Tests

So testen Sie die Einstellungen:

Schritt 1


Navigieren Sie zu **Erweitert > Primäre AP-Tools**.

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

Schritt 2

Klicken Sie auf die Registerkarte **Tools** zur Fehlerbehebung.

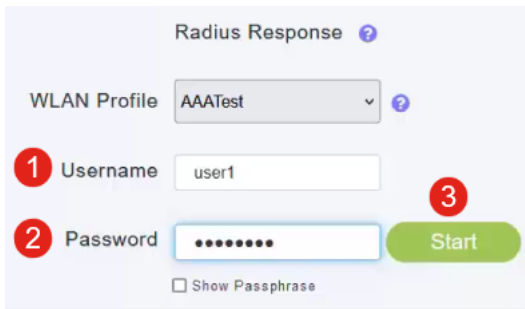
Primary AP Tools

 **Tools**

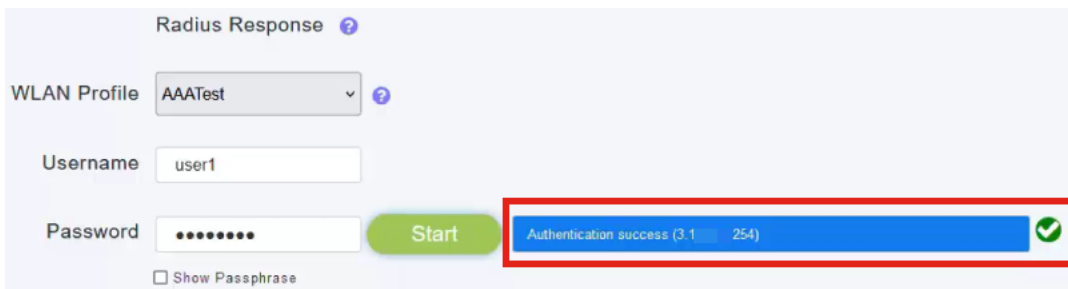
[Restart Primary AP](#) [Configuration Management](#) [Troubleshooting Files](#) **[Troubleshooting Tools](#)** [Upload File](#)

Schritt 3

Geben Sie im Abschnitt "*Radius Response*" den **Benutzernamen** und das **Kennwort ein**, und klicken Sie auf **Start**, um zu prüfen, ob die Authentifizierung beim Radius-Server erfolgt.



Nach Abschluss des Tests wird eine Benachrichtigung über die *erfolgreiche Authentifizierung* angezeigt.



Stellen Sie sicher, dass Sie über eine IP-Verbindung zwischen dem CBD-Manager und dem Client-System verfügen, damit dies ordnungsgemäß funktioniert.

Schlussfolgerung

Das ist alles! Sie müssen sich keine Gedanken mehr darüber machen, Radius selbst zu konfigurieren. CBD erledigt die gesamte Arbeit und Sie können sich zurücklehnen, entspannen und die Vorteile der drahtlosen Authentifizierung in Ihrem Netzwerk genießen.

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.