

# Draadloze verificatie met Cisco Business Dashboard

## Doel

Het doel van dit artikel is om over draadloze authenticatie functie met behulp van Cisco Business Dashboard (CBD) versie 2.5.0.

## Toepasselijke apparaten | Softwareversie

- Cisco Business Dashboard | 2.5.0 (Download nieuwste release)
- CBW140AC | [Laatste download](#)
- CBW145AC | [Laatste download](#)
- CBW240AC | [Laatste download](#)
- CBW150AXE | [Laatste download](#)

## Inleiding

CBD biedt tools die u helpen om de apparaten in uw Cisco Business-netwerk te bewaken en te beheren. Hiermee wordt uw netwerk automatisch herkend en kunt u alle ondersteunde apparaten configureren en controleren, zoals switches, routers en draadloze access points.

CBD 2.5.0 voegt de functionaliteit van de verificatieservice toe aan CBD. De nieuwe service wordt ondersteund op zowel CBW140/240-serie als CBW 150AX-apparaten.

Het stelt een FreeRADIUS-instantie in op de CBD-manager om te gebruiken voor RADIUS-verificatie, waardoor uw organisatie een eenvoudige manier heeft om een server te implementeren zonder dat klanten RADIUS moeten kennen of begrijpen.

Als je klaar bent om te beginnen, laten we dan binnenduiken.

## Inhoud

- [Verificatieprofiel configureren](#)
- [Draadloze netwerken configureren](#)
- [Verificatie](#)
- [Testen](#)

## Verificatieprofiel configureren

Eerst moet u het verificatieprofiel voor uw organisatie configureren. In veel gevallen kunt u eenvoudig het standaardprofiel gebruiken.

## Stap 1

Meld u aan bij CBD.



## Cisco Business Dashboard

User Name\*

1

This field is required

Password\*

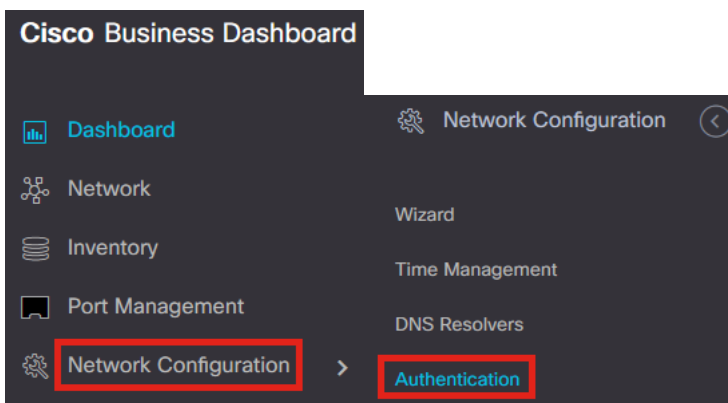
2

Login

3

## Stap 2

Ga naar **Netwerkconfiguratie > Verificatie**.



## Stap 3

U kunt het bestaande *standaardprofiel* bewerken of een ander profiel toevoegen. In dit voorbeeld wordt het **standaardprofiel** geselecteerd. Klik op **Edit** (Bewerken).

## Cisco Business Dashboard

Authentication



Profile Name

Default

10 Per Page

## Stap 4

In CBD 2.5.0 is er een nieuwe optie om *Cisco Business Dashboard Authenticatieservice* te selecteren. Dit wordt standaard gecontroleerd. Breng de

gewenste wijzigingen aan en klik op **Bijwerken**.

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.

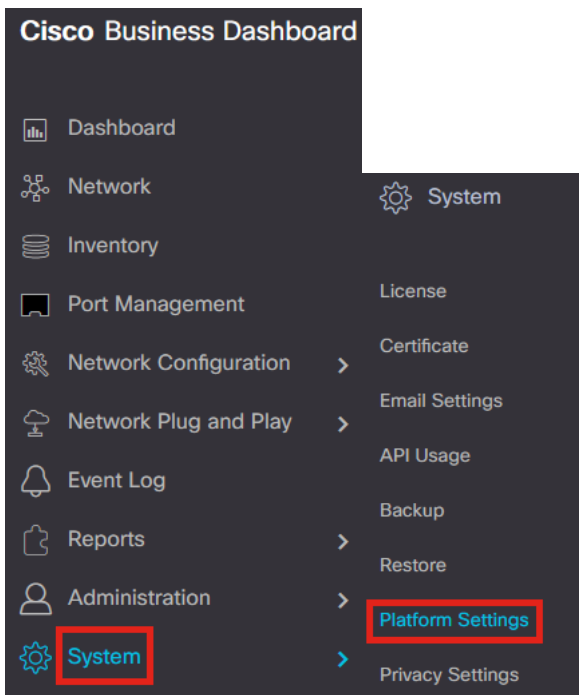
**+** Add custom authentication server

**2**

Controleer of *System > Platform Settings > System Variables* de juiste instellingen hebben om het Dashboard te kunnen bereiken op de netwerkapparaten.

## Stap 5

Navigeer naar **Systeem > Platform-instellingen** in het menu.



## Stap 6

Selecteer het tabblad **Systeemvariabelen**.

Platform Settings

Network Settings Web Server **System Variables**

## Stap 7

Controleer de instellingen om ervoor te zorgen dat het *externe Dashboard IP-adres* het openbare IP-adres van het CBD is en de *externe verificatieserverpoort* 1812 is. Dit is de standaardpoort. Klik op **Save** (Opslaan).

Platform Settings

Network Settings Web Server **System Variables**

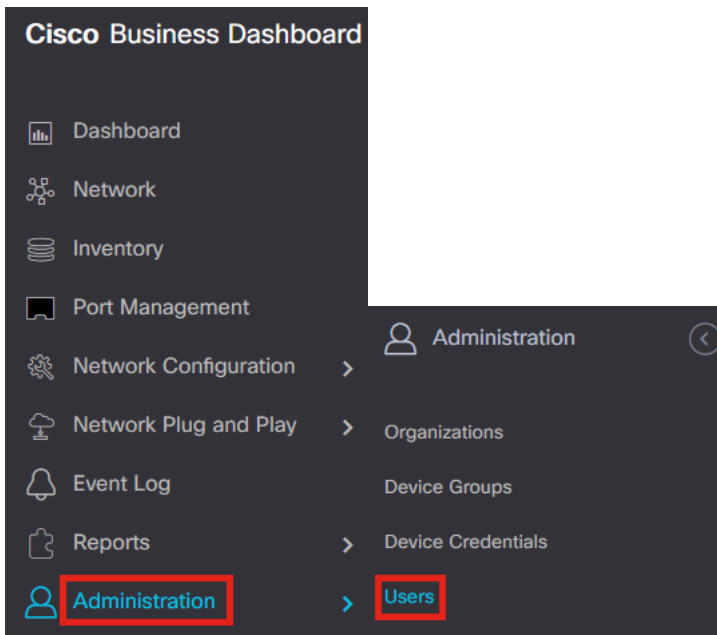
External System Settings

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

## Stap 8

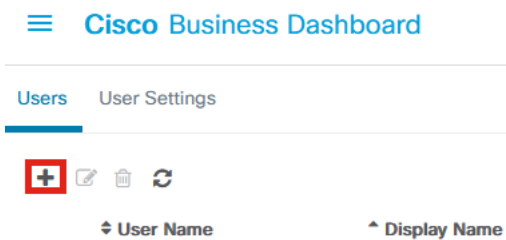
Als u gebruikers wilt maken die op het systeem zullen worden geverifieerd, gaat u naar

## Beheer > Gebruikers.



### Stap 9

Om gebruikers toe te voegen, klikt u op het **plus-pictogram**.



### Stap 10

Configureer het volgende:

- *Gebruikersnaam*
- *Display naam*
- *Email*
- *Dashboard Access* - selecteer in het uitrolmenu. In dit voorbeeld is **Geen toegang** geselecteerd.
- *Nieuw wachtwoord*
- *Nieuw wachtwoord opnieuw invoeren*

De andere velden zijn optioneel. Klik op **Save** (Opslaan).

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	<span style="display: inline-block; width: 10px; height: 10px; background-color: orange; border: 1px solid orange;"></span> <span style="display: inline-block; width: 10px; height: 10px; background-color: orange; border: 1px solid orange;"></span> <span style="display: inline-block; width: 10px; height: 10px; background-color: gray; border: 1px solid gray;"></span> <span style="display: inline-block; width: 10px; height: 10px; background-color: gray; border: 1px solid gray;"></span> 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"/>

## Stap 11

Klik op het tabblad **Organisaties**.

### ☰ Cisco Business Dashboard

User Name	<input type="text" value="user1"/>
	<a href="#">Reset password</a>
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
	<a href="#">Show account settings</a>
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**

## Stap 12

Hier moet je de gebruiker die je net hebt gemaakt, associëren met je CBD organisatie. Klik op het **plus-pictogram** en kies de optie in het vervolgkeuzemenu. In dit voorbeeld is **Default** geselecteerd.

Access Key **Organizations**

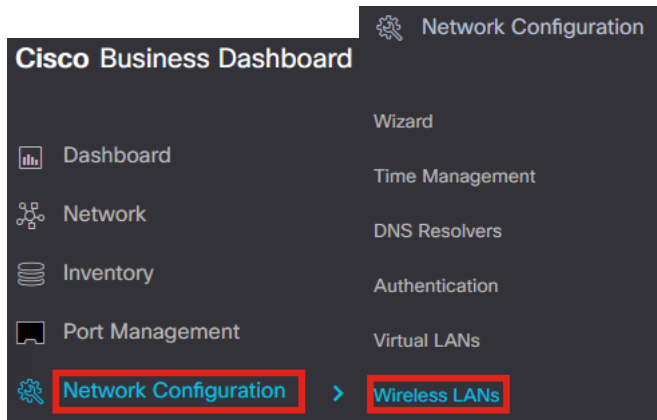
<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	▼ Org Name
<input type="checkbox"/>	Default

Deze gebruiker kan nu inloggen op de standaardorganisatie die is geconfigureerd voor draadloze verificatie.

# Draadloze netwerken configureren

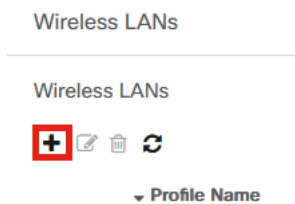
## Stap 1

Ga naar **Netwerkconfiguratie > Draadloze LAN's** menu.



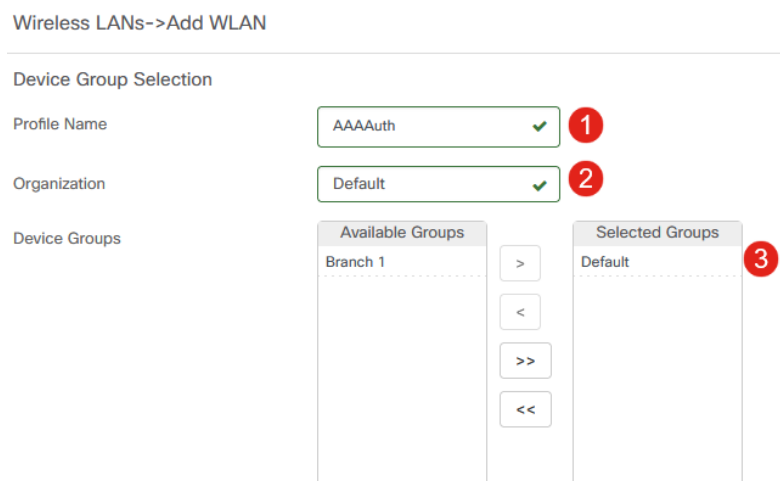
## Stap 2

Klik op het **pluspictogram** onder *Draadloze LAN's* om een nieuw profiel te maken.



## Stap 3

Voer de *profielnaam*, de *organisatie in* en configureer *apparaatgroepen* om de instellingen toe te passen op de draadloze apparaten in de groep.



## Stap 4

Klik op het **plus-pictogram** om een SSID te maken.



SSID Name

## Stap 5

Voer de *SSID-naam*, *VLAN-id* en selecteer *Beveiliging* in het vervolgkeuzemenu. In dit voorbeeld is **WPA2-Enterprise** geselecteerd. Klik op **Save (Opslaan)**.

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 Verification Server wordt gebruikt als u geen verificatieserver hebt geconfigureerd.

## Stap 6

Klik nogmaals op **Opslaan** om de instellingen voor het draadloze netwerk en de straal toe te passen op alle 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	



# Verificatie

Om te controleren of de instellingen zijn toegepast,

## Stap 1

Meld u aan bij uw CBW AP.



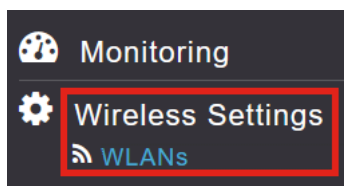
## Cisco Business Wireless Access Point

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



## Stap 2

Ga naar **Draadloze instellingen > WLAN's**.



## Stap 3

De SSID die u aanmaakt wordt weergegeven. In dit voorbeeld is het **AAATest**.

WLANs

Active WLANs 2

Add new WLAN/RLAN

Action	Active	Type	Name	SSID	Security Policy	Radio Policy
<input checked="" type="checkbox"/> ✕	Enabled	WLAN	CBWireless	CBWireless	Personal(WPA2)	ALL
<input checked="" type="checkbox"/> ✕	Enabled	WLAN	AAATest	AAATest	WPA2Enterprise	ALL

## Stap 4

Selecteer de SSID en klik op **bewerken** om de instellingen te bekijken.

WLANS

Active WLANS 2

Add new WLAN/RLAN

Action	Active	Type	Name
	Enabled	WLAN	CBWireless
	Enabled	WLAN	AAATest

## Stap 5

Navigeer naar het tabblad **WLAN-beveiliging**.

Edit WLAN

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

U ziet dat het *beveiligingstype* wordt aangeduid als **WPA2 Enterprise-** en *Verificatieserver* wordt de **Externe Straal**. Het *IP-adres* van de server is het adres dat u eerder hebt ingesteld.

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

## Stap 6

Switch naar **Expert weergave** door op de tweerichtingspijl bovenaan de gebruikersinterface te klikken.



## Stap 7

Ga naar **Beheer > Admin-accounts**.

Management 1

Access

Admin Accounts 2

Time

## Stap 8

Klik op het tabblad **RADIUS**.

Admin Accounts

**Users** 1

---

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

U ziet dat de RADIUS-verificatieserver is geconfigureerd voor *netwerkgebruiker*.

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

## Testen

Zo test u de instellingen:

### Stap 1

Ga naar **Geavanceerd > Primaire AP-tools**.

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

### Stap 2

Klik op het tabblad **Tools** voor probleemoplossing.

Primary AP Tools

**Tools**

---

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

### Stap 3

Voer in het gedeelte *Radius Response* de **gebruikersnaam** en het **wachtwoord** in en klik op **Start** om te zien of deze geverifieerd wordt op de Radius-server.

Radius Response ?

WLAN Profile AAATest ?

1 Username user1

2 Password .....

3 Start

Show Passphrase

Er verschijnt een *geslaagde verificatie*-melding nadat de test is voltooid.

Radius Response ?

WLAN Profile AAATest ?

Username user1

Password .....

Start Authentication success (3.1 254) ✓

Show Passphrase

Zorg ervoor dat je IP-verbinding hebt tussen de CBD Manager en het clientsysteem zodat dit goed werkt.

## Conclusie

Dat is alles! U hoeft zich geen zorgen meer te maken over het configureren van Radius op uw eigen. CBD doet al het werk en je kunt achterover leunen, ontspannen en genieten van de voordelen van draadloze authenticatie in je netwerk.

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.