

Autenticação sem fio usando o Cisco Business Dashboard

Objetivo

O objetivo deste artigo é passar pelo recurso de autenticação sem fio usando o Cisco Business Dashboard (CBD) versão 2.5.0.

Dispositivos aplicáveis | Versão do software

- Painel de negócios da Cisco | 2.5.0 (Baixe o mais recente)
- CBW140AC | [Download mais recente](#)
- CBW145AC | [Download mais recente](#)
- CBW240AC | [Download mais recente](#)
- CBW150AX | [Download mais recente](#)

Introduction

O CBD fornece ferramentas que ajudam você a monitorar e gerenciar os dispositivos na sua rede Cisco Business. Ele descobre automaticamente sua rede e permite que você configure e monitore todos os dispositivos suportados, como switches, roteadores e pontos de acesso sem fio.

O CBD 2.5.0 adiciona a funcionalidade do serviço de autenticação ao CBD. O novo serviço é suportado nos dispositivos CBW140/240 Series e CBW 150AX.

Ele configura uma instância FreeRADIUS no gerenciador CBD para usar na autenticação RADIUS, oferecendo à sua organização uma maneira simples de implantar um servidor sem que os clientes precisem conhecer ou entender o RADIUS.

Se estiver pronto para começar, vamos nos aprofundar.

Table Of Contents

- [Configurar perfil de autenticação](#)
- [Configurar redes sem fio](#)
- [Verificação](#)
- [Testando](#)


Configurar perfil de autenticação

Primeiro, você deve configurar o perfil de autenticação que usará para sua organização. Em muitos casos, você pode simplesmente usar o perfil padrão.

Passo 1

Faça login no CBD.

English ▾



Cisco Business Dashboard

User Name* 1

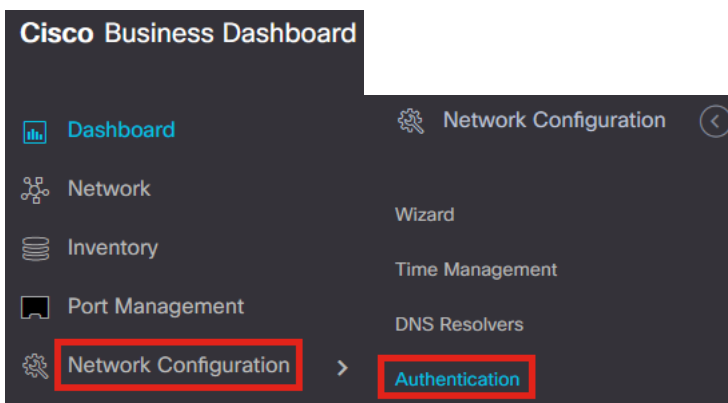
This field is required

Password* 2

Login 3

Passo 2

Navegue até **Network Configuration > Authentication**.






Etapa 3

Você pode editar o perfil *Padrão* existente ou adicionar outro perfil. Neste exemplo, o perfil **Default** está selecionado. Clique em **Editar**.


☰ Cisco Business Dashboard

Authentication

2

+   

1 Profile Name

 > Default

⏪ < 1 > ⏩ 10 Per Page

Passo 4

No CBD 2.5.0, há uma nova opção para selecionar *Use Cisco Business Dashboard Authentication Service*. Essa opção é marcada por padrão. Faça as alterações

desejadas e clique em **Update**.

Authentication->Update Default

Device Group Selection

Profile Name

Organization


Device Groups

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.

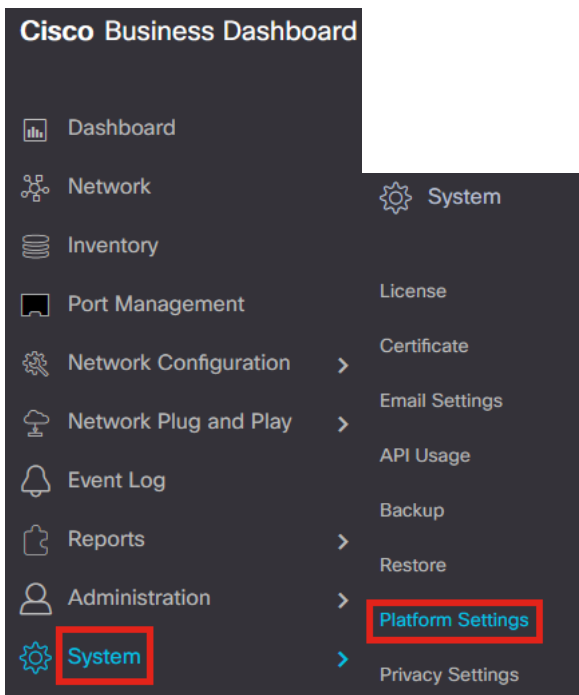
 Add custom authentication server



Verifique se *System > Platform Settings > System Variables* tem as configurações corretas para permitir que o Painel seja acessado pelos dispositivos de rede.

Etapa 5

Navegue até **System > Platform Settings** no menu.



Etapa 6

Selecione a guia **Variáveis de Sistema**.

Platform Settings

Network Settings Web Server **System Variables**

Etapa 7

Verifique as configurações para garantir que o *Endereço IP do painel externo* seja o endereço IP público do CBD e a *Porta do servidor de autenticação externo* seja 1812. Esta é a porta padrão. Click **Save**.

Platform Settings

Network Settings Web Server **System Variables**

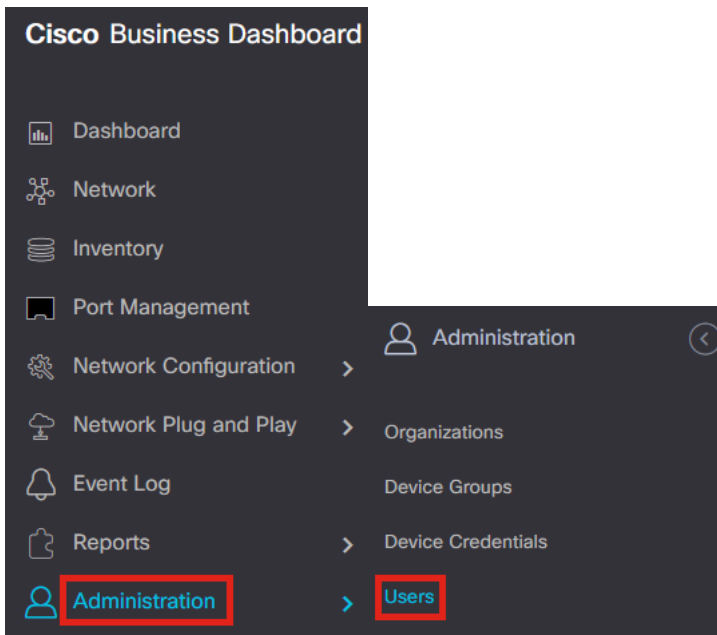
External System Settings

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

Passo 8

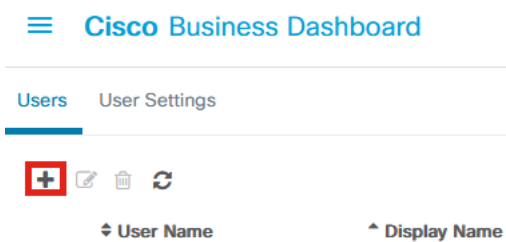
Para criar usuários que serão autenticados no sistema, vá para **Administração >**

Usuários.



Passo 9

Para adicionar usuários, clique no ícone de adição.



Passo 10

Configure o seguinte:

- *User Name*
- *Nome de exibição*
- *E-mail*
- *Acesso ao painel* - selecione no menu suspenso. Neste exemplo, **No Access** está selecionado.
- *Nova senha*
- *Digite a nova senha novamente*

Os outros campos são opcionais. Click **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: 20px; height: 10px; background-color: orange;"></div><div style="width: 20px; height: 10px; background-color: orange;"></div><div style="width: 20px; height: 10px; background-color: gray;"></div><div style="width: 20px; height: 10px; background-color: gray;"></div> Normal</div>
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"/>

Passo 11

Clique na guia **Organizations**.

☰ Cisco Business Dashboard

Users > user1

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**

Etapa 12

Aqui, você precisa associar o usuário que acabou de criar à sua organização de CBD. Clique no **ícone de adição** e escolha a opção no menu suspenso. Neste exemplo, **Default** está selecionado.

Access Key **Organizations**

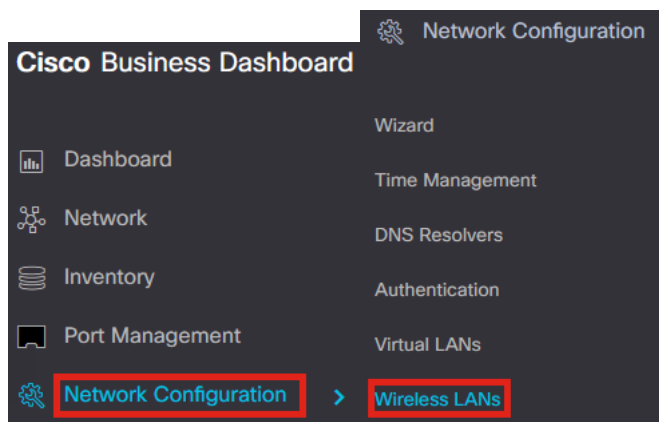
<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	▼ Org Name
<input type="checkbox"/>	Default

Este usuário poderá fazer login na organização padrão configurada para autenticação sem fio.

Configurar redes sem fio

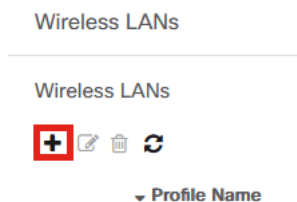
Passo 1

Navegue até o menu **Network Configuration > Wireless LANs**.



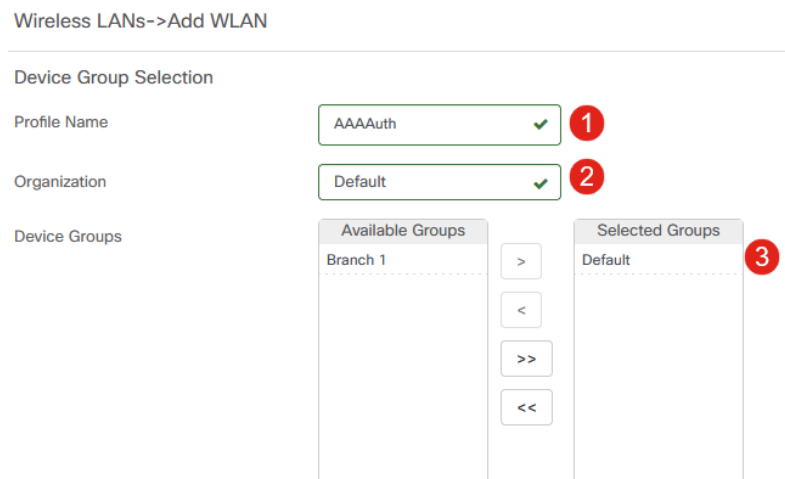
Passo 2

Para criar um novo perfil, clique no ícone de **adição** em *Wireless LANs*.



Etapa 3

Insira o *Nome do perfil*, *Organização* e configure *Grupos de dispositivos* para aplicar as configurações aos dispositivos sem fio do grupo.



Passo 4

Para criar um SSID, clique no ícone de **adição**.



SSID Name

Etapa 5

Insira o *SSID Name*, *VLAN ID* e selecione *Security* no menu suspenso. Neste exemplo, **WPA2-Enterprise** está selecionado. Click **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

O Cisco Business Dashboard Authentication Server será usado se você não tiver um servidor de autenticação configurado.

Etapa 6

Clique em **Save** novamente para aplicar a rede sem fio e as configurações Radius a todos os clientes.

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	

Verificação

Para verificar se as configurações foram aplicadas,

Passo 1

Faça login em seu AP CBW.



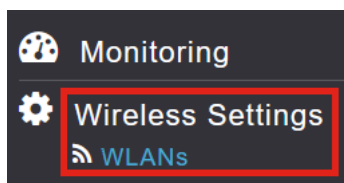
Cisco Business Wireless Access Point

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



Passo 2

Vá para **Wireless Settings > WLANs**.



Etapa 3

O SSID que você criou será listado. Neste exemplo, é **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

Passo 4

Selecione o SSID e clique em **editar** para exibir as configurações.

WLANS

Active WLANS 2

Add new WLAN/RLAN

Action	Active	Type	Name
	Enabled	WLAN	CBWireless
	Enabled	WLAN	AAATest

Etapa 5

Navegue até a guia **WLAN Security**.

Edit WLAN

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

Você verá que o *Tipo de segurança* será listado como **WPA2 Enterprise** e **Servidor de autenticação** será o **Radius externo**. O *endereço IP do servidor* será o que você configurou anteriormente.

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

Etapa 6

Altere para a **visualização Expert** clicando na seta bidirecional na parte superior da interface do usuário.



Etapa 7

Navegue até **Gerenciamento > Contas de administração**.

Management 1

Access

Admin Accounts 2

Time

Passo 8

Clique na guia **RADIUS**.

Admin Accounts

Users 1

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

Você verá que o servidor de autenticação Radius foi configurado para *Network User*.

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

Testando

Para testar as configurações:

Passo 1

Navegue até **Advanced > Primary AP Tools**.

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

Passo 2

Clique na guia **Ferramentas de solução de problemas**.

Primary AP Tools

Tools

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

Etapa 3

Na seção *Radius Response*, insira o **Username** e **Password** e clique em **Start** para ver se ele se autentica no servidor Radius.

Radius Response ?

WLAN Profile AAATest ?

1 Username user1

2 Password

3 Start

Show Passphrase

Você verá uma notificação *Authentication success* após a conclusão do teste.

Radius Response ?

WLAN Profile AAATest ?

Username user1

Password

Start Authentication success (3.1 254) ✓

Show Passphrase

Certifique-se de que haja conectividade IP entre o CBD Manager e o sistema cliente para que isso funcione corretamente.

Conclusão

É isso aí! Você não precisa mais se preocupar com a configuração do Radius por conta própria. O CBD fará todo o trabalho e você poderá relaxar e aproveitar os benefícios da autenticação sem fio em sua rede.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.