

CBW接入点中的个人预共享密钥功能

目标

本文将介绍思科企业无线(CBW)接入点(AP)固件版本10.6.1.0中的个人预共享密钥(PSK)功能。

适用设备 | 软件版本

- 思科企业无线140AC接入点 | 10.6.1.0(下载[最新版本](#))
- 思科企业无线145AC接入点 | 10.6.1.0(下载[最新版本](#))
- 思科企业无线240AC接入点 | 10.6.1.0(下载[最新版本](#))

简介

如果您的网络中有CBW设备，现在可以在固件版本10.6.1.0中使用个人PSK功能！

个人PSK（也称为个人PSK）是一种功能，它允许管理员为同一Wi-Fi保护访问II(WPA2)个人无线局域网(WLAN)向各个设备发出唯一的预共享密钥。唯一PSK与设备的MAC地址关联。在启用WPA3策略的WLAN中不支持此功能。

此功能使用RADIUS服务器对客户端进行身份验证。它通常用于IoT设备和公司发布的笔记本电脑和移动设备。

目录

- [先决条件](#)
- [配置CBW RADIUS设置](#)
- [配置WLAN设置](#)
- [后续步骤](#)

先决条件

- 确保已将CBW AP固件升级到10.6.1.0。 [单击是否要执行固件更新的分步说明](#)。
- 您需要配置个人PSK和设备MAC地址的RADIUS服务器。
- 此CBW功能受三个不同RADIUS服务器支持 — FreeRADIUS、Microsoft的NPS和思科的ISE。配置会因使用的RADIUS服务器而异。

配置CBW RADIUS设置

要在CBW AP上配置RADIUS设置，请执行以下步骤。

第 1 步

登录CBW AP的Web用户界面(UI)。

Cisco Business Wireless Access Point

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



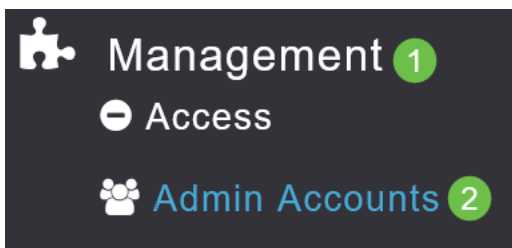
步骤 2

单击双向箭头符号切换到专家视图。



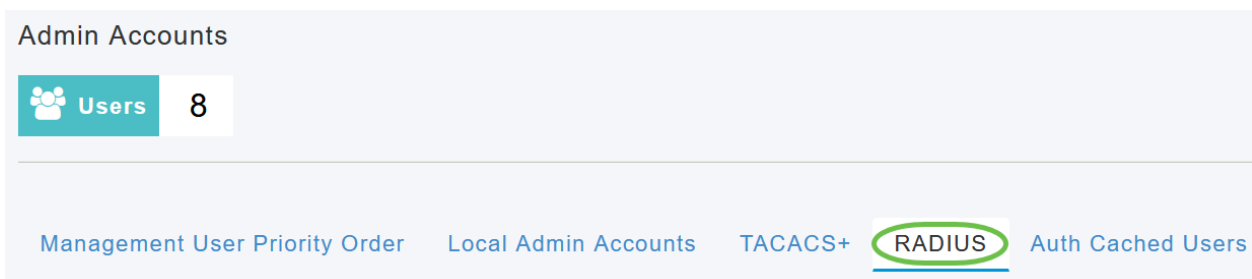
步骤 3

导航至Management > Admin Accounts。




步骤 4

选择“RADIUS”选项卡。



步骤 5

单击添加RADIUS身份验证服务器。

Action	Server Index	Network User
	1	<input checked="" type="checkbox"/>

步骤 6

配置以下内容：

- 服务器索引 — 选择1到6
- 网络用户 — 启用状态。默认情况下，此为Enabled
- 管理 — 启用状态。默认情况下，此为Enabled
- 状态 — 启用状态。默认情况下，此为Enabled
- CoA — 确保启用授权收费(CoA)。
- 服务器IP地址 — 输入RADIUS服务器的IPv4地址
- 共享密钥 — 输入共享密钥
- Port Number — 输入用于与RADIUS服务器通信的端口号。
- 服务器超时 — 输入服务器超时

单击 **Apply**。

Add/Edit RADIUS Authentication Server. ✕

Server Index

Network User

Management

State

CoA

Server IP Address

Shared Secret

Confirm Shared Secret

Show Password

Port Number

Server Timeout Seconds

2 Apply
✕ Cancel

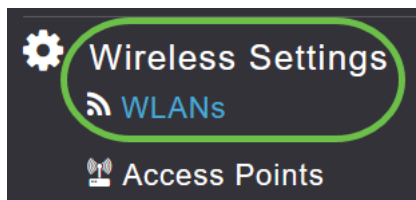
配置WLAN设置

创建WLAN作为标准WPA2个人安全WLAN。

预共享密钥不会用于个人PSK设备。这仅用于未在RADIUS服务器上身份验证的设备。您需要将要连接到此WLAN的任何设备的MAC地址添加到此设备的允许列表。

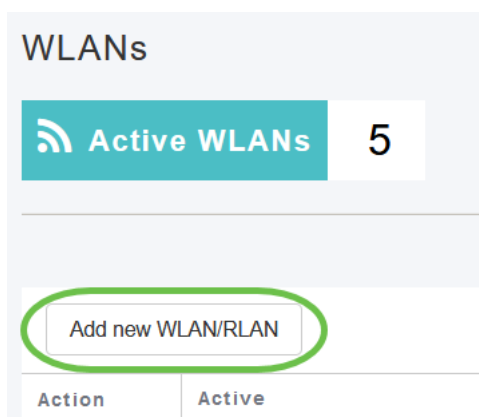
第 1 步

导航至Wireless Settings > WLANs。



步骤 2

单击“Add new WLAN/RLAN (添加新WLAN/RLAN)”。



步骤 3

在“常规”选项卡下，输入WLAN的配置文件名称。

Add new WLAN

1

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

WLAN ID 4

Type WLAN

Profile Name * Personal

SSID * Personal

WLANs with same SSID can be configured, unless layer-2 security settings are different.

Enable

Radio Policy ALL

Broadcast SSID

Local Profiling

Apply Cancel

步骤 4

导航至WLAN Security选项卡，并通过滑动切换启用MAC过滤。

1

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

Guest Network

Captive Network Assistant

MAC Filtering 2

Security Type WPA2/WPA3 Personal

WPA2 WPA3

Passphrase Format ASCII

Passphrase * *****

Confirm Passphrase * *****

Show Passphrase

Password Expiry

步骤 5

单击Add RADIUS Authentication Server以添加在上一节中配置的RADIUS服务器，为此WLAN提供身份验证。

Authentication Caching

步骤 6

系统将显示一个弹出窗口。输入服务器IP地址、状态和端口号。单击 **Apply**。

Add RADIUS Authentication Server ✕

Radius Server can be configured from 'Admin Accounts > RADIUS'(Expert view).

Server IP Address

State 1

Port Number

2

步骤 7

(可选)

启用身份验证缓存。启用此选项时，将显示以下字段。

- *User Cache Timeout* — 指定缓存中经过身份验证的凭据过期的时间段。
- *用户缓存重用* — 在缓存超时之前使用凭证缓存信息。默认情况下，已禁用。

Authentication Caching

User Cache Timeout minutes

User Cache Reuse

如果启用此功能，则已通过此服务器身份验证的客户端在24小时内重新连接到此WLAN时，无需将数据传递到RADIUS服务器。

步骤 8

转到高级选项卡。通过滑动切换启用允许AAA覆盖。

Add new WLAN

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

Allow AAA Override



802.11r Disabled (Default)

只有在“专家视图”中，“高级”选项卡才可见。

后续步骤

在CBW AP上配置设置并设置RADIUS服务器后，您应能连接设备。输入为该MAC地址配置的自定义PSK，它将加入网络。

如果已配置身份验证缓存，则通过转到Admin Accounts下的Auth Cached Users选项卡，您将能够看到已加入WLAN的设备。如果需要，可以删除。

Monitoring
Wireless Settings
Management
Access
Admin Accounts 1
Time
Software Update
Services
Advanced

Admin Accounts
Users 2

Management User Priority Order Local Admin Accounts TACACS+ RADIUS

Auth Cached Users 2

MacAddress/Username/ssid

Delete Selected

	Mac Address	Username	SSID	Timeout(Minutes)	RemainingTime(Minut...
<input checked="" type="checkbox"/>	98:c...5e	98...5e	Personal	1440	1425

结论

给你！您现在可以享受CBW AP上个人PSK功能的优势。