

WAP125およびWAP581のワイヤレスセキュリティ設定

目的

ワイヤレスセキュリティを使用すると、ワイヤレスネットワークを不正アクセスから保護できます。WAP125およびWAP 581アクセスポイントは、Static Wired Equivalent Protection(WEP)、Wi-Fi Protected Access(WPA)Personal、およびWPA Enterpriseをサポートしています。これらの設定は、仮想アクセスポイント(VAP)ごとに設定できます。これらの設定を行うと、VAPごとにネットワークセキュリティが提供されます。通常、アクセスポイントが最初に導入されたとき、またはネットワークのワイヤレスセキュリティ設定が更新されたときに設定されます。

この記事では、WAP125またはWAP581アクセスポイントでワイヤレスセキュリティを設定する方法について説明します。

該当するデバイス

- WAP125
- WAP581

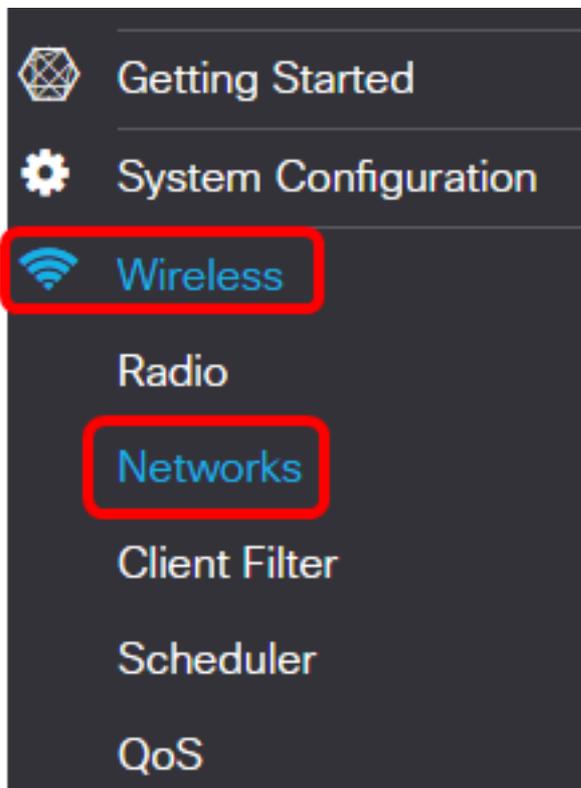
[Software Version]

- WAP125 - 1.0.0.3
- WAP581 - 1.0.0.4

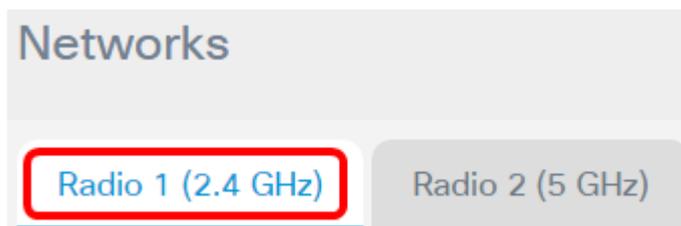
ワイヤレスセキュリティの設定

WPAパーソナルセキュリティの設定

ステップ1:WAPのWebベースのユーティリティにログインし、[Wireless] > [Networks]を選択します。

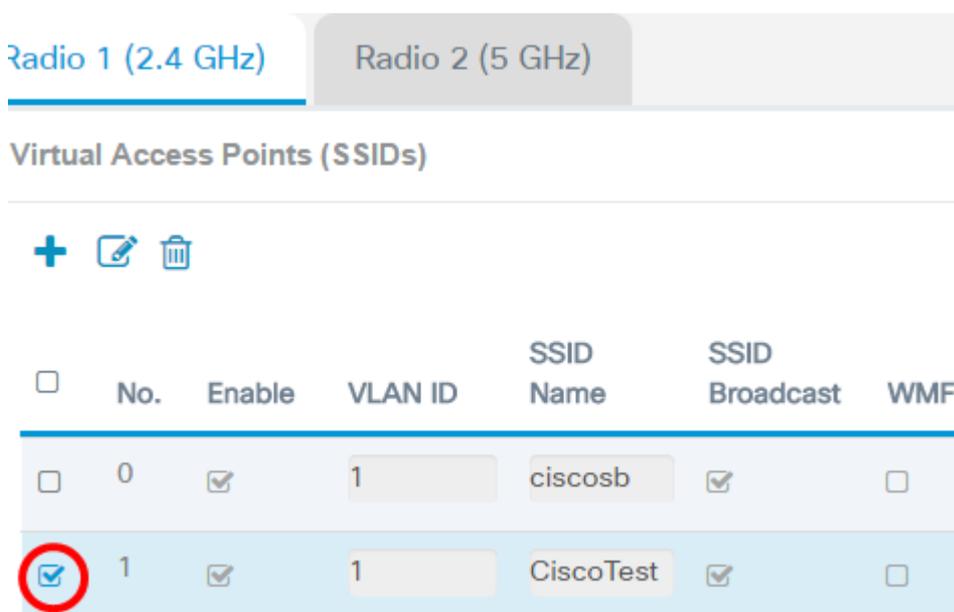


ステップ2：ワイヤレスセキュリティ設定を設定する必要がある無線を選択します。



注：この例では、無線1(2.4 GHz)が選択されています。

ステップ3：ワイヤレスセキュリティの設定が必要なVAPのチェックボックスをオンにします。



注：この例では、VAP 1が選択されています。

ステップ4:[Edit]をクリックします。

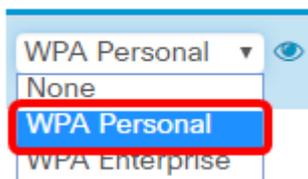


<input type="checkbox"/>	No.	Enable	VLAN ID	SSID Name	SSID Broadcast	WMF
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	ciscosb	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1	CiscoTest	<input checked="" type="checkbox"/>	<input type="checkbox"/>

ステップ5:[Security]ドロップダウンリストからセキュリティモードを選択します。次のオプションがあります。

- [なし(None)] : このオプションは、選択したVAPのワイヤレスセキュリティ設定を非アクティブにします。セキュリティモードを無効にすると、ワイヤレスネットワークが開き、ワイヤレスデバイスを持つユーザがネットワークとそのリソースに接続できるようになります。このモードは推奨されませんが、リモートロケーションのネットワークでは便利です。
- [WPA Personal] : このオプションは、ワイヤレスネットワークにWPAセキュリティを実装します。Temporal Key Integrity Protocol(TKIP)アルゴリズムまたはAdvanced Encryption Standard(AES)アルゴリズムを使用できます。混在させると、AESアルゴリズムをサポートしていないデバイスがネットワークに接続できるようになります。WPA Personalでは、64文字までの英数字パスワードを使用できます。WPA Personalは通常、Remote Authentication Dial-In User Service(RADIUS)サーバが使用されていないオフィスで使用されます。
- [WPA Enterprise] : このオプションを使用すると、WPAが提供するセキュリティ機能を組み合わせながら、RADIUSサーバも使用できます。これは通常、RADIUSサーバが使用される環境で使用されます。このオプションを選択した場合は、[ここをクリックします](#)。

Security



WPA Personal ▼ 

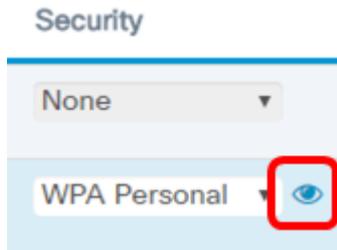
None

WPA Personal

WPA Enterprise

注 : この例では、[WPA Personal]が選択されています。

ステップ6:[View]ボタンをクリックして、WPA Personalパラメータを設定します。



ステップ7:[WPA Versions]領域でWPAバージョンを選択します。次のオプションがあります。

- WPA-TKIP：このオプションは、ワイヤレスネットワークに混合セキュリティを実装します。無線クライアントが混在するネットワークに最適です。このオプションはデフォルトで無効になっています。
- WPA2-AES：このオプションは、ネットワークにWPA2-AESセキュリティを実装します。これは、WPA2セキュリティをサポートするクライアントを備えたワイヤレスネットワークに最適です。

Security Setting

WPA Versions: WPA-TKIP WPA2-AES

Key: [?](#)

Show Key as Clear Text

Key Strength Meter: Below Minimum

Broadcast Key Refresh Rate [?](#)

注：この例では、WPA-TKIPがチェックされています。

ステップ8:[Key]フィールドにネットワークパスワードを入力します。キーには、8 ~ 63文字の文字と数字を組み合わせることができます。

Security Setting

WPA Versions: WPA-TKIP WPA2-AES

Key: [?](#)

Show Key as Clear Text

Key Strength Meter: Below Minimum

Broadcast Key Refresh Rate [?](#)

注：この例では、Cisco!@#\$\$%^&*()が入力されています。

ステップ9: (オプション) キーをテキスト形式で表示するには、「キーをクリアテキストとして表示」チェックボックスをオンにします。

Security Setting

WPA Versions: WPA-TKIP WPA2-AES

Key: [?](#)

Show Key as Clear Text

Key Strength Meter: Below Minimum

Broadcast Key Refresh Rate [?](#)

注：この例では、[Show Key as Clear Text]がオンになっています。

ステップ10:[Broadcast Key Refresh Rate]フィールドに、セキュリティキーを新しく生成したキーに置き換えるまでの秒数を入力します。デフォルト値は 86400 です。

Security Setting

WPA Versions: WPA-TKIP WPA2-AES

Key: [?](#)

Cisco!@#\$\$%^&*()

Show Key as Clear Text

Key Strength Meter:



Below Minimum

Broadcast Key Refresh Rate [?](#)

86400

OK

cancel

手順 11 : [OK] をクリックします。

Security Setting

WPA Versions: WPA-TKIP WPA2-AES

Key: [?](#)

Cisco!@#\$\$%^&*()

Show Key as Clear Text

Key Strength Meter:



Below Minimum

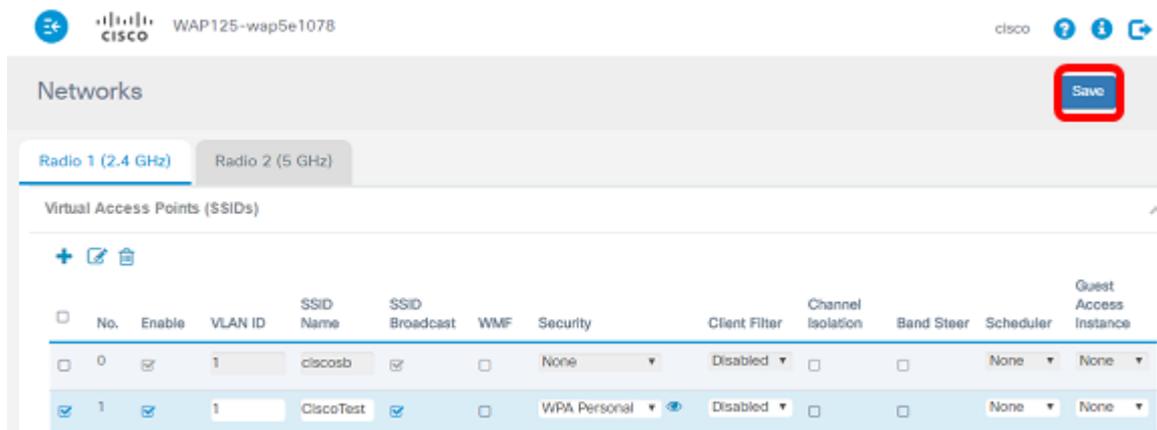
Broadcast Key Refresh Rate [?](#)

86400

OK

cancel

ステップ12:[Save]をクリックします。

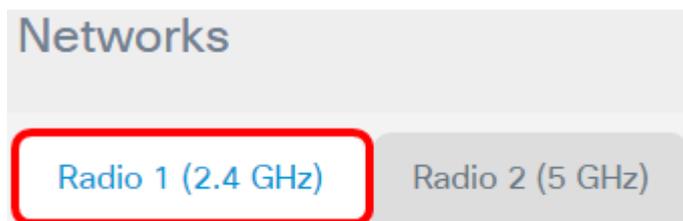


手順 13 : [OK] をクリックします。

WAP125でWPAパーソナルワイヤレスセキュリティ設定が設定されました。

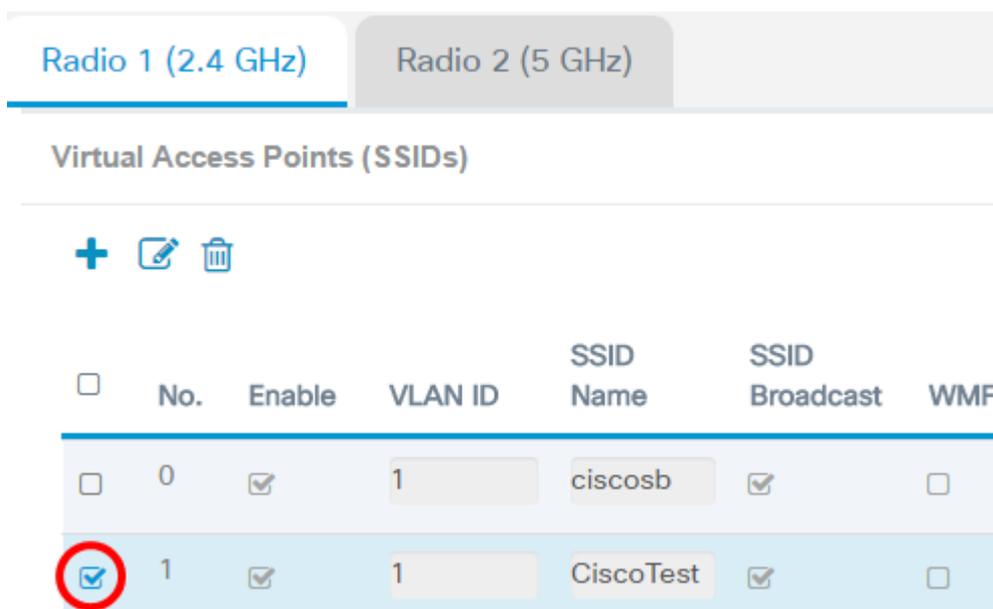
WPAエンタープライズセキュリティの設定

ステップ1 : ワイヤレスセキュリティ設定を設定する必要がある無線を選択します。



注 : この例では、無線1(2.4 GHz)が選択されています。

ステップ2 : ワイヤレスセキュリティ設定が必要なVAPのチェックボックスをオンにします。



注 : この例では、VAP 1が選択されています。

ステップ3:[Edit]をクリックします。

Radio 1 (2.4 GHz)

Radio 2 (5 GHz)

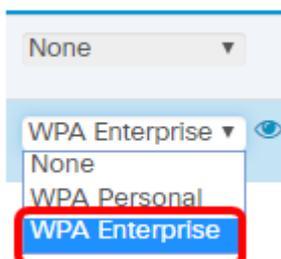
Virtual Access Points (SSIDs)



<input type="checkbox"/>	No.	Enable	VLAN ID	SSID Name	SSID Broadcast	WMF
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	ciscosb	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1	CiscoTest	<input checked="" type="checkbox"/>	<input type="checkbox"/>

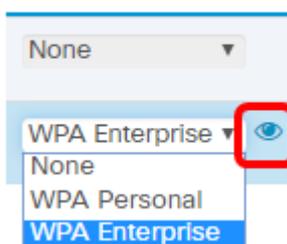
ステップ4:[Security]ドロップダウンリストから[WPA Enterprise]を選択します。

Security



ステップ5:[view]ボタンをクリックして、WPAエンタープライズパラメータを設定します。

Security



ステップ6:[WPA Versions]領域でWPAバージョンを選択します。次のオプションがあります。

- WPA-TKIP：このオプションは、ワイヤレスネットワークに混合セキュリティを実装します。無線クライアントが混在するネットワークに最適です。このオプションはデフォルトで無効になっています。
- WPA2-AES：このオプションは、ネットワークにWPA2-AESセキュリティを実装します。これは、WPA2セキュリティをサポートするクライアントを備えたワイヤレスネットワークに最適です。

Security Setting



注：この例では、WPA-TKIPがチェックされています。

ステップ7: (オプション) [Enable pre-authentication]チェックボックスをオンにして、機能をアクティブにします。オンにすると、ワイヤレスクライアントが現在ターゲットWAPに接続されているWAPから事前認証情報がリレーされます。この機能を有効にすると、複数のアクセスポイントに接続するローミングクライアントの認証を高速化できます。セキュリティモードを無効にすると、このオプションも無効になり、編集できなくなります。

Security Setting



ステップ8: (オプション) [Use global RADIUS server settings]チェックボックスをオフにして、別のRADIUSサーバセットを指定できるようにします。デフォルトでは、各VAPはWAPに定義されたグローバルRADIUS設定を使用します。

Security Setting

WPA Versions:

WPA-TKIP

WPA2-AES

Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type:

IPv4 IPv6

Server IP Address-1: [?](#)

192.168.1.1

Server IP Address-2: [?](#)

Key-1: [?](#)

.....

Key-2: [?](#)

Enable RADIUS Accounting

Active Server:

Server IP Address-1 ▼

Broadcast Key Refresh Rate: [?](#)

86400

Session Key Refresh Rate: [?](#)

0

OK

cancel

注：この例では、[Use global RADIUS server settings]はオンになっていません。これを確認した場合は、ステップ [17](#)に進んでください。

ステップ9: (オプション) サーバのIPアドレスタイプを選択します。次のオプションがあります。

- IPv4：このオプションを使用すると、WAPがIPv4 RADIUSサーバに接続できます。
- IPv6：このオプションを使用すると、WAPがIPv6 RADIUSサーバに接続できます。

Security Setting

WPA Versions: WPA-TKIP WPA2-AES

Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: Pv4 IPv6

Server IP Address-1:

Server IP Address-2:

Key-1:

Key-2:

Enable RADIUS Accounting

Active Server:

Broadcast Key Refresh Rate:

Session Key Refresh Rate:

OK

cancel

注：この例では、IPv4が選択されています。

ステップ10: (オプション) VAPのプライマリRADIUSサーバのIPアドレスを[Server IP Address -1]フィールドに入力します。

Server IP Address Type: IPv4 IPv6

Server IP Address-1:

Server IP Address-2:

Key-1:

Key-2:

注：この例では、192.168.1.1と入力します。

ステップ11: (オプション) VAPのバックアップRADIUSサーバのIPアドレスを[Server IP Address -2]フィールドに入力します。

Server IP Address Type: IPv4 IPv6

Server IP Address-1:

Server IP Address-2:

Key-1:

Key-2:

注：この例では、バックアップIPアドレスは入力されていません。

ステップ12: (オプション) [Key-1]フィールドにプライマリサーバアドレスのパスワードを入力します。

Server IP Address Type: IPv4 IPv6

Server IP Address-1:

Server IP Address-2:

Key-1:

Key-2:

ステップ13: (オプション) [Key-2]フィールドにバックアップサーバアドレスのパスワードを入力します。

Server IP Address Type: IPv4 IPv6

Server IP Address-1:

Server IP Address-2:

Key-1:

Key-2:

注：この例では、パスワードは入力されていません。

ステップ14: (オプション) [Enable RADIUS Accounting]チェックボックスをオンにします。このオプションは、システムの時刻や送受信データの量など、特定のユーザが消費したリソースを追跡および測定します。有効にすると、プライマリサーバとバックアップサーバで有効になります。

Enable RADIUS Accounting

Active Server:

Broadcast Key Refresh Rate:

Session Key Refresh Rate:

注：この例では、[Enable RADIUS Accounting]にチェックマークが付いています。

ステップ15: (オプション) [Active Server]ドロップダウンリストからアクティブサーバを選択します。

Server IP Address Type: IPv4 IPv6

Server IP Address-1:

Server IP Address-2:

Key-1:

Key-2:

Enable RADIUS Accounting

Active Server:

Broadcast Key Refresh Rate:

Session Key Refresh Rate:

注：この例では、[Server IP Address-1]が選択されています。

ステップ16: (オプション) [Broadcast Key Refresh Rate]フィールドに、セキュリティキーを新しく生成したキーに置き換えるまでの秒数を入力します。デフォルト値は 86400 です。

。

Active Server:

Broadcast Key Refresh Rate:

Session Key Refresh Rate:

注：この例では、[Broadcast Key Refresh Rate]はデフォルト値のままになっています。

[ステップ17](#):VAPに関連付けられている各クライアントのセッションキーをWAPが更新する間隔を入力します。30 ~ 86400秒の範囲で指定できます。

Active Server:

Broadcast Key Refresh Rate:

Session Key Refresh Rate:

手順 18 : [OK] をクリックします。

Active Server:

Broadcast Key Refresh Rate:

Session Key Refresh Rate:

ステップ19:[Save]をクリックします。

WAP125-wap5e1078

Networks

Radio 1 (2.4 GHz) Radio 2 (5 GHz)

Virtual Access Points (SSIDs)

No.	Enable	VLAN ID	SSID Name	SSID Broadcast	WMM	Security	Client Filter	Channel Isolation	Band Steer	Scheduler	Guest Access Instance
0	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	<input type="checkbox"/>	None	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	None	None
1	<input checked="" type="checkbox"/>	1	CiscoTest	<input checked="" type="checkbox"/>	<input type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	None	None

これで、ワイヤレスネットワークでWPAエンタープライズセキュリティが設定されました

。

この記事に関連するビデオを表示...

[シスコのその他のテクニカルトークを表示するには、ここをクリックしてください](#)