

WAP351、WAP131 および WAP371 の VAP の設定

目標

バーチャルアクセス アクセス・ポイント (VAPs) はイーサネット VLAN のワイヤレス等量である複数のブロードキャスト ドメインに Wireless LAN をセグメント化します。VAPs は 1 つの物理的な WAP デバイスの複数のアクセス ポイントを模倣します。4 つまで VAPs Cisco WAP131 でサポートされ、8 つまで VAPs Cisco WAP351 および WAP371 でサポートされます。

この資料の目標は WAP351、WAP131 および WAP371 アクセス ポイントの VAP を設定する方法を示すことです。

適当なデバイス

- WAP351
- WAP131
- WAP371

[Software Version]

- V1.0.0.39 (WAP351)
- V1.0.0.39 (WAP131)
- V1.2.0.2 (WAP371)

VAP を追加し、設定して下さい

注: 各 VAP はユーザ設定 サービス セット ID (SSID) によって識別されます。多重 VAPs は同じ SSID 名前がある場合がありません。

注: 機能する無線ネットワークのために設定された VAP が関連付けられること無線は有効になり、正しく設定する必要がありますと。 [WAP131 および WAP351 の基本的な電波設定](#)を詳細については [行うこと](#)または [WAP371 の基本的な電波設定を行うこと](#)を参照して下さい

ステップ 1. Web コンフィギュレーションユーティリティへのログインおよびワイヤレス > ネットワークへの移動。 ネットワーク ページは提示されます:

Networks

Select the radio interface first, and then enter the configuration parameters.

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

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>		

Add Edit Delete

Save

呼び出します。Radio フィールドで、VAPs を設定することを望むワイヤレス無線に Radio ボタンを選択して下さい。

Select the radio interface first, and then enter the configuration parameters.

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

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>		

Add Edit Delete

ステップ 3 新しい VAP を追加するために、『Add』をクリックして下さい。新しい VAP は表に現われます。

Select the radio interface first, and then enter the configuration parameters.

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

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>		

Add Edit Delete

注: WAP131 は WAP371 および WAP351 は 8 つまで VAPs サポートするが、4 つまで VAPs サポートします。

ステップ 4 VAP を編集し始めるためにテーブルエントリの左端のチェックボックスをクリックし、次に『Edit』をクリックして下さい。これは選択した VAP の選択不可能にされたフィールドを修正することを可能にします。

Select the radio interface first, and then enter the configuration parameters.

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

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>		
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1		<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>		

Add Edit Delete

ステップ 5 Enable チェックボックスがチェックされるように VAP の使用状況を有効にするために、して下さい。

Select the radio interface first, and then enter the configuration parameters.

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

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID Add New VLAN	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>		
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1		<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>		

Add Edit Delete

ステップ 6 VLAN ID フィールドでは、VAP と関連付けることを望む VLAN ID を規定して下さい。WAP131 が WAP371 を使用している場合、VLAN ID で入力して下さい。入力することができる最大値は 4094 です。

Select the radio interface first, and then enter the configuration parameters.

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

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID Add New VLAN	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>		
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1		<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>		

Add Edit Delete

注: 入る VLAN ID はネットワークにあり、正しく設定する必要があります。詳細については [WAP351 アクセスポイントの VLAN 構成を、タグ付けされる管理および ID WAP131 のタグなし VLAN](#)、または [タグ付けされる管理および ID WAP371 のタグなし VLAN](#) 参照して下さい。

ステップ 7. SSID Name フィールドで無線ネットワークの名前を入力して下さい。各 VAP はユニークな SSID 名前がなければなりません。

Select the radio interface first, and then enter the configuration parameters.

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

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID Add New VLAN	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>		
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>		

Add Edit Delete

ステップ 8 SSID 名前のようにブロードキャスト クライアントへ SSID ブロードキャスト チェックボックスをチェックして下さい。これは利用可能なネットワークのリストのクライアントに SSID 名前を表記します。

Select the radio interface first, and then enter the configuration parameters.

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

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID Add New VLAN	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>		
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>		

Add Edit Delete

セキュリティ設定の設定

ステップ 1.セキュリティ ドロップダウン リストからの VAP に接続するために必要となる認証方式を選択して下さい。 **どれも**以外のどのオプションでも選択されない場合、追加フィールドは現われません。

利用可能なオプションは次の通りです:

- なし
- スタティック WEP
- ダイナミック WEP
- 個人的な WPA
- WPA エンタープライズ

注: 個人的な、WPA エンタープライズ WPA は最大セキュリティ用の好まれた認証種別です。スタティック WEP およびダイナミック WEP はレガシー 機器としか使用する必要があり、無線が使用されるべき 802.11a か 802.11b/g にモード 設定 されることを必要とします。[WAP131 および WAP351 の基本的な電波 設定](#)を詳細については [行うこと](#)または [WAP371 の基本的な電波 設定を行うこと](#)を参照して下さい。

スタティック WEP

スタティック WEP は最少セキュア認証方式です。それは静的なキーに基づいて無線ネットワークのデータを暗号化します。それはこの静的なキーを不法に得やすくなりました従って必要な場合 WEP 認証はレガシー デバイスによってしか必要がありません使用する。

注: スタティック WEP をセキュリティ 方式として選択するとき、プロンプトはセキュリティ 方式選択が非常に不確かであることを現われ、告げます。

ステップ 1: *Transfer* 鍵インデックス ドロップダウン リストで、デバイスがデータを暗号化するのに使用しているその下でキーのリストから WEPキーのインデックスを選択して下さい。

Transfer Key Index: 1
 2
 3 bits
 4 bits

Key Length: 64 bits
 128 bits

Key Type: ASCII
 Hex

WEP Keys: (Required: 26)
1:
2:
3:
4:

Show Key as Clear Text

802.1X Authentication: Open System Shared Key

ステップ 2. キーが 64 ビットまたは 128 ビット長であるかどうか規定 するために 変調長さ フィールドから Radio ボタンを選択して下さい。

Transfer Key Index: 1 ▾

Key Length: 64 bits
 128 bits

Key Type: ASCII
 Hex

WEP Keys: (Required: 26)
1:
2:
3:
4:

Show Key as Clear Text

802.1X Authentication: Open System Shared Key

ステップ 3 キー Type フィールドで、ASCII か 16 進法フォーマットでキーを入力することを望むかどうか選択して下さい。ASCII はすべての文字が、数含まれ、16 進法が数だけ使用する A-F に文字を入れる間、シンボルはキーボードで示します。

Transfer Key Index: 1 ▾

Key Length: 64 bits
 128 bits

Key Type: ASCII
 Hex

WEP Keys: (Required: 26)

1:

2:

3:

4:

Show Key as Clear Text

802.1X Authentication: Open System Shared Key

ステップ 4 WEPキー フィールドでは、デバイスのための 4 つまでの異なる WEPキーを入力して下さい。このネットワークに接続する各クライアントはデバイスによって規定される同じスロットの同じ WEPキーの 1 つがなければなりません。

Transfer Key Index: 1 ▾

Key Length: 64 bits
 128 bits

Key Type: ASCII
 Hex

WEP Keys: (Required: 26)

1:

2:

3:

4:

Show Key as Clear Text

802.1X Authentication: Open System Shared Key

キーの文字列を明らかにする場合、ステップ 5. (オプションの) はクリアテキスト フィールドとして提示キーのチェックボックスをクリックします。

ができません。

- 公開システムおよび共有鍵—両方の認証アルゴリズムを選択したら、共有鍵 モードで WEP を使用するために設定されるクライアント ステーションは WAP デバイスによって関連付けるために有効な WEPキーがなければなりません。また、公開システム (有効にならない 共有鍵 モード) として WEP を使用するために設定されるクライアント ステーションは WAP デバイスによって正しい WEPキーを持たなくても関連付けることができます。

ステップ 7. 『SAVE』 をクリックして下さい。

ダイナミック WEP

ダイナミック WEP は 802.1X テクノロジーおよび Extensible Authentication Protocol (EAP) の組み合わせを示します。このモードは外部 RADIUSサーバの使用がユーザを認証するように要求します。WAP デバイスは EAP をサポートする Microsoft Internet Authentication Server のような RADIUSサーバを必要とします。Microsoft Windows クライアントとはたらくために、認証サーバは Protected EAP (PEAP) および MSCHAP v2 をサポートする必要があります。IEEE 802.1X モードが、証明書を含んで、Kerberos、および公開キー認証使用できますが、サポートする WAP デバイスが使用する同じ認証方式を使用するためにクライアント ステーションを設定して下さいのいろいろな認証方式。

ステップ 1.デフォルトで使用 グローバル な RADIUSサーバ設定はチェックされます。RADIUSサーバの異なるセットを使用するために VAP を設定したいと思う場合チェックボックスのチェックを外して下さい。さもなければステップ 8.にスキップして下さい。

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)

Server IP Address-2: (xxx.xxx.xxx.xxx)

Server IP Address-3: (xxx.xxx.xxx.xxx)

Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

呼び出します。サーバのIPアドレス Type フィールドで、サーバのIPアドレス タイプを WAP デバイス使用選択して下さい。オプションは IPv4 または IPv6 です。ドット付き 10進表記で表される IPv4 使用 32ビット 2進数。IPv6 は 128ビット 2進数を表すのに 16進数およびコロンを使用します。WAP デバイスはこのフィールドで選択したアドレスタ

IPv4に関してはRADIUSサーバがサーバだけ接続します。IPv6を選択する場合、ステップ4.にスキップして下さい。

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: 0.0.0.0 (xxx.xxx.xxx.xxx)

Server IP Address-2: (xxx.xxx.xxx.xxx)

Server IP Address-3: (xxx.xxx.xxx.xxx)

Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: Server IP Address-1

Broadcast Key Refresh Rate: 300 Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: 0 Sec (Range: 30-86400, 0 = Disable, Default: 0)

ステップ3ステップ2のIPv4を選択した場合、すべてのVAPsがデフォルトで使用するRADIUSサーバのIPアドレスを入力して下さい。それからステップ5.にスキップして下さい。

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: 192.168.10.23 (xxx.xxx.xxx.xxx)

Server IP Address-2: 192.168.11.1 (xxx.xxx.xxx.xxx)

Server IP Address-3: 192.168.12.2 (xxx.xxx.xxx.xxx)

Server IP Address-4: 192.168.13.3 (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: Server IP Address-1

Broadcast Key Refresh Rate: 300 Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: 0 Sec (Range: 30-86400, 0 = Disable, Default: 0)

注: 3までIPv4バックアップRADIUSサーバアドレスがあることができます。認証がプライマリサーバによって失敗した場合、各々の設定されたバックアップサーバは順に試みられます。

ステップ 4 ステップ 2 の IPv6 を選択する場合、プライマリ グローバル な RADIUSサーバの IPv6 アドレスを入力して下さい。

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IPv6 Address-1: 2001:DB8:1234:abcd:: (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

Server IPv6 Address-2: 2002:DB8:1234:abcd:: (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

Server IPv6 Address-3: 2003:DB8:1234:abcd:: (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

Server IPv6 Address-4: 2004:DB8:1234:abcd:: (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: Server IP Address-1

Broadcast Key Refresh Rate: 300 Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: 0 Sec (Range: 30-86400, 0 = Disable, Default: 0)

注: 3 まで IPv6 バックアップ RADIUSサーバ アドレスがあることができます。認証がプライマリ サーバーによって失敗した場合、各々の設定されたバックアップサーバは順に試みられます。

ステップ 5 Key-1 フィールドでは、WAP デバイスがプライマリ RADIUSサーバに認証するのに使用している共用秘密鍵で入力して下さい。

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: 192.168.10.23 (xxx.xxx.xxx.xxx)

Server IP Address-2: 192.168.11.1 (xxx.xxx.xxx.xxx)

Server IP Address-3: 192.168.12.2 (xxx.xxx.xxx.xxx)

Server IP Address-4: 192.168.13.3 (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: Server IP Address-1

Broadcast Key Refresh Rate: 300 Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: 0 Sec (Range: 30-86400, 0 = Disable, Default: 0)

ステップ 6 Key-4 フィールドへの Key-2 では、設定されたバックアップ RADIUSサーバと

の RADIUS 鍵準で入力して下さい。サーバIP Address-2 は Key-2 を、サーバのIPアドレス 3 使用します Key-3 を使用し、サーバのIPアドレス 4 は Key-4 を使用します。

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)

Server IP Address-2: (xxx.xxx.xxx.xxx)

Server IP Address-3: (xxx.xxx.xxx.xxx)

Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

トラッキングを有効にしたいと思い、リソースの測定が特定のユーザー消費したら場合有効 RADIUS 説明フィールドのステップ 7. (オプションの) は、チェックボックスをチェックします。RADIUS 説明を有効にすることは送受信されたデータのシステムの時刻および量をトラッキングします。情報は RADIUSサーバで保存されます。これはプライマリ RADIUSサーバおよびすべてのバックアップサーバのために有効になります。

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)

Server IP Address-2: (xxx.xxx.xxx.xxx)

Server IP Address-3: (xxx.xxx.xxx.xxx)

Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

注: 説明する有効 RADIUS がある場合プライマリ RADIUSサーバおよびすべてのバックアップサーバのために有効になります

ステップ 8.最初のサーバを選択して下さいアクティブなサーバフィールドでアクティブで

ある。これは有効にしまアクティブである各設定されたサーバを順に接続し、最初のサーバを選択する WAP デバイス試みを持っていますよりもむしろアクティブな RADIUSサーバの手動選択を。

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: 192.168.10.23 (xxx.xxx.xxx.xxx)

Server IP Address-2: 192.168.11.1 (xxx.xxx.xxx.xxx)

Server IP Address-3: 192.168.12.2 (xxx.xxx.xxx.xxx)

Server IP Address-4: 192.168.13.3 (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: **Server IP Address-1**

Broadcast Key Refresh Rate: **Server IP Address-1** Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: 0 Sec (Range: 30-86400, 0 = Disable, Default: 0)

ステップ 9：ブロードキャストキーリフレッシュレートフィールドでは、ブロードキャスト（グループ）キーがこの VAP と関連付けられるクライアントのためにリフレッシュされる間隔を入力して下さい。デフォルトは 300 秒です。

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: 192.168.10.23 (xxx.xxx.xxx.xxx)

Server IP Address-2: 192.168.11.1 (xxx.xxx.xxx.xxx)

Server IP Address-3: 192.168.12.2 (xxx.xxx.xxx.xxx)

Server IP Address-4: 192.168.13.3 (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: Server IP Address-1

Broadcast Key Refresh Rate: **300** Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: 0 Sec (Range: 30-86400, 0 = Disable, Default: 0)

ステップ 10：セッションキーリフレッシュレートフィールドでは、WAP デバイスが VAP と関連付けられる各クライアントのためのセッション（ユニキャスト）キーをリフレッシュする間隔を入力して下さい。デフォルト値は 0 です。

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)

Server IP Address-2: (xxx.xxx.xxx.xxx)

Server IP Address-3: (xxx.xxx.xxx.xxx)

Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

個人的な WPA

個人的な WPA は AES-CCMP および TKIP 暗号化を含む Wi-Fi 同盟 IEEE 802.11i 規格です。WPA は IEEE 802.1X および EAP を使用するかわりにエンタープライズ WPA セキュリティモードで使用されるように事前共有キー (PSK) を使用します。PSK は資格情報だけがあるように最初のために確認します使用されます。WPA はまた WPA-PSK と言われます。このセキュリティモードはオリジナル WPA をサポートする無線クライアントのために逆方向互換性があります。

ステップ 1: WPA バージョンフィールドでは、WPA-TKIP を有効にしたいと思う場合 WPA-TKIP チェックボックスをチェックして下さい。WPA-TKIP および WPA2-AES を同時に有効にしてもらうことができます。WAP は WPA2-AES を常にサポートします従ってそれを設定できません。

WPA Versions: WPA-TKIP WPA2-AES

Key: (Range: 8-63 Characters)

Show Key as Clear Text

Key Strength Meter: Below Minimum

Broadcast Key Refresh Rate Sec (Range: 0-86400, 0 = Disable, Default: 300)

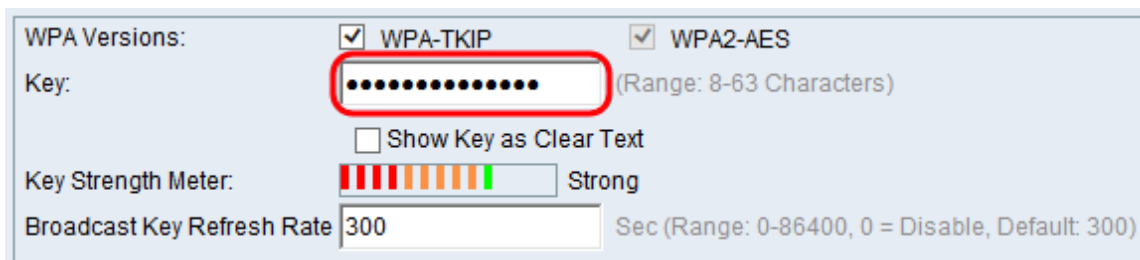
利用可能なオプションは次の通り定義されます:

- WPA-TKIP —ネットワークにオリジナル WPA および TKIP セキュリティプロトコルだけをサポートするいくつかのクライアントステーションがあります。最新の WiFi 同盟必要条件に従って、WPA-TKIP だけ選択することは推奨されません。
- WPA2-AES —ネットワークのすべてのクライアントステーションは WPA2 および AES-CCMP 暗号/セキュリティプロトコルをサポートします。この WPA バージョンは IEEE 802.11i 規格ごとの最もよいセキュリティを提供します。最新の WiFi 同盟要件に従って、AP はこのモードをいつもサポートしなければなりません。

• WPA-TKIP および WPA2-AES —ネットワークに何人かオリジナル WPA だけサポートする他および WPA2 をサポートするクライアントのミックスがある場合、チェックボックスの両方をチェックして下さい。この設定は WPA および WPA2 が両方クライアントステーションおよび認証する関連付けるようにしますが、それをサポートするクライアントのために非常に堅牢な WPA2 を使用します。この WPA 設定はセキュリティの代わりにより多くの相互運用性を割り当てます。

注: WPA クライアントは WAP デバイスによって関連付けられますこれらのキー (有効な TKIP キーが有効な AES CCMP 鍵) の 1 つがなければなりません。

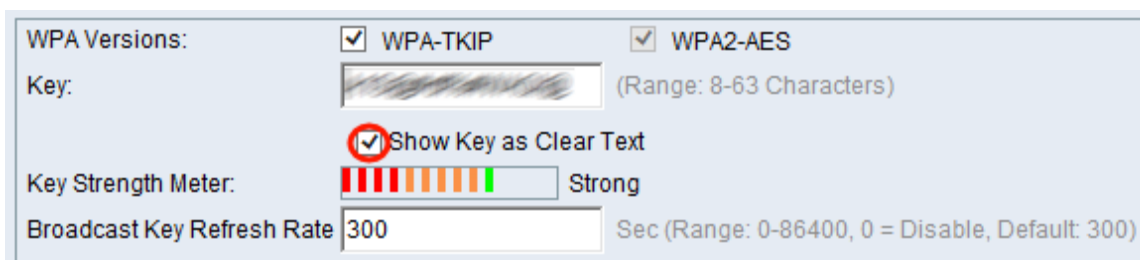
呼び出します。Key フィールドでは、WPA 個人的なセキュリティ用の共有秘密鍵で入力して下さい。63 文字を少なくとも 8 文字および最大入力して下さい。



WPA Versions: WPA-TKIP WPA2-AES
Key: [.....] (Range: 8-63 Characters)
 Show Key as Clear Text
Key Strength Meter: [.....] Strong
Broadcast Key Refresh Rate: [300] Sec (Range: 0-86400, 0 = Disable, Default: 300)

注: 受諾可能な文字は大文字および小文字アルファベット文字、含まれる数字および特別なシンボルが含まれています (か。!^@#%&*)。

テキストがほしいと思えばステップ 3. (オプションの) チェック クリアテキストチェックボックスとして提示キー目に見えるために入力します。チェックボックスはデフォルトでチェックを外されます。



WPA Versions: WPA-TKIP WPA2-AES
Key: [.....] (Range: 8-63 Characters)
 Show Key as Clear Text
Key Strength Meter: [.....] Strong
Broadcast Key Refresh Rate: [300] Sec (Range: 0-86400, 0 = Disable, Default: 300)

注: WAP351 の別のファームウェアを、WAP131、か WAP371 は、提示キー クリアテキストフィールドとして使用するとき抜けるかもしれません。

注: キーの強さメートル フィールドは文字の何異なる型使用される、そしてどの位キーがあるか WAP デバイスがのような複雑な状況基準に対してキーをチェックするところにです。WPA-PSK 複雑な状況チェック機能が有効になる場合、キーは最小条件を満たさなければ受け入れられません。WPA-PSK 複雑な状況に関する詳細については、[WAP131](#)、[WAP351](#) および [WAP371 のためのパスワードの複雑性の設定](#)を参照して下さい。



WPA Versions: WPA-TKIP WPA2-AES
Key: [.....] (Range: 8-63 Characters)
 Show Key as Clear Text
Key Strength Meter: [.....] Strong
Broadcast Key Refresh Rate: [300] Sec (Range: 0-86400, 0 = Disable, Default: 300)

ステップ 4 ブロードキャスト キー リフレッシュ レート フィールドでは、ブロードキャスト (グループ) キーがこの VAP と関連付けられるクライアントのためにリフレッシュされ

る間隔で入力して下さい。デフォルトは 300 秒です。

WPA Versions: WPA-TKIP WPA2-AES
Key: (Range: 8-63 Characters)
 Show Key as Clear Text
Key Strength Meter: Strong
Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

WPA エンタープライズ

RADIUS の WPA エンタープライズは CCMP (AES) が含まれている、および TKIP 暗号化です Wi-Fi 同盟 IEEE 802.11i 規格の実装。エンタープライズ モードは RADIUSサーバの使用がユーザを認証するように要求します。セキュリティモードはオリジナル WPA をサポートする無線クライアントと逆方向互換性があります。

注: ダイナミック VLAN モードはデフォルトで有効になります、RADIUS認証サーバがどの VLAN がステーションのために使用されるか決定するようにする。

ステップ 1: WPA バージョンフィールドでは、サポートされるべきクライアントステーションの種類があるようにチェックボックスを確認して下さい。それらはすべてデフォルトで有効になります。AP は WPA2-AES をいつもサポートする必要があります従ってそれを設定できません。

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication
 Use global RADIUS server settings
Server IP Address Type: IPv4 IPv6
Server IP Address-1: (xxx.xxx.xxx.xxx)
Server IP Address-2: (xxx.xxx.xxx.xxx)
Server IP Address-3: (xxx.xxx.xxx.xxx)
Server IP Address-4: (xxx.xxx.xxx.xxx)
Key-1: (Range: 1-64 Characters)
Key-2: (Range: 1-64 Characters)
Key-3: (Range: 1-64 Characters)
Key-4: (Range: 1-64 Characters)
 Enable RADIUS Accounting
Active Server:
Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)
Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

利用可能なオプションは次の通り定義されます:

- WPA-TKIP —ネットワークにオリジナル WPA および TKIP セキュリティプロトコルだけをサポートするいくつかのクライアントステーションがあります。アクセスポイントに WPA-TKIP だけ選択することが最新の WiFi 同盟要件によって許可されないことに注目し

て下さい。

- WPA2-AES —ネットワークのすべてのクライアントステーションは WPA2 バージョンおよび AES-CCMP 暗号セキュリティプロトコルをサポートします。この WPA バージョンは IEEE 802.11i 規格ごとの最もよいセキュリティを提供します。最新の Wi-Fi 同盟要件によって、WAP はこのモードをいつもサポートしなければなりません。

- 有効事前認証— WPA バージョンとして WPA2 だけまたは WPA および WPA2 両方選択する場合、WPA2 クライアントのための事前認証を有効にすることができます。WPA2 無線クライアントに事前認証パケットを送信してほしい場合このオプションをチェックして下さい。事前認証情報は WAP デバイスからクライアントがターゲット WAP に現在デバイスを使用していること中継されます。この機能を有効にすることは多重 WAPs に接続するローミングクライアントのための認証の高速化を助けることができます。このオプションはオリジナル WPA がこの機能をサポートしないので WPA バージョンのために『WPA』を選択した場合適用しません。

注: RADIUS と WPA を使用するために設定されるクライアントステーションはこれらのアドレスおよびキーの 1 つがなければなりません: 有効な TKIP RADIUS または有効な CCMP (AES) IP アドレスおよび RADIUS 鍵。

ステップ 2.デフォルトで使用 *グローバル* な RADIUSサーバ設定はチェックされます。RADIUSサーバの異なるセットを使用するために VAP を設定したいと思う場合チェックボックスのチェックを外して下さい。さもなければステップ 9.にスキップして下さい。

The screenshot shows a configuration window for WPA settings. At the top, 'WPA Versions:' has checkboxes for 'WPA-TKIP' and 'WPA2-AES', both of which are checked. Below that, 'Enable pre-authentication' is also checked. A section titled 'Use global RADIUS server settings' has an unchecked checkbox, which is circled in red. Underneath, 'Server IP Address Type:' has radio buttons for 'IPv4' (selected) and 'IPv6'. There are four input fields for 'Server IP Address-1' through 'Server IP Address-4', with the first containing '0.0.0.0'. Each field has a placeholder '(xxx.xxx.xxx.xxx)'. Below these are four 'Key' fields, each with a placeholder '(Range: 1-64 Characters)'. At the bottom, 'Enable RADIUS Accounting' is unchecked. There is a dropdown for 'Active Server:' set to 'Server IP Address-1'. Two more input fields are for 'Broadcast Key Refresh Rate:' (value 300) and 'Session Key Refresh Rate:' (value 0), both with ranges and default values.

ステップ 3 サーバのIPアドレス Type フィールドで、サーバのIPアドレスタイプを WAP デバイス使用選択して下さい。オプションは IPv4 または IPv6 です。ドット付き10進表記で表される IPv4 使用 32ビット 2進数。IPv6 は 128 ビット 2進数を表すのに 16 進数およびコロンを使用します。WAP デバイスはこのフィールドで選択したアドレスタイプに関しては RADIUSサーバかサーバだけ接続します。

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
 Server IP Address-2: (xxx.xxx.xxx.xxx)
 Server IP Address-3: (xxx.xxx.xxx.xxx)
 Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)
 Key-2: (Range: 1-64 Characters)
 Key-3: (Range: 1-64 Characters)
 Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▾

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)
 Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

ステップ 4 ステップ 2 の IPv4 を選択した場合、すべての VAPs がデフォルトで使用する RADIUSサーバの IP アドレスを入力して下さい。それからステップ 6.にスキップして下さい。

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
 Server IP Address-2: (xxx.xxx.xxx.xxx)
 Server IP Address-3: (xxx.xxx.xxx.xxx)
 Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)
 Key-2: (Range: 1-64 Characters)
 Key-3: (Range: 1-64 Characters)
 Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▾

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)
 Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

注: 3 まで IPv4 バックアップ RADIUSサーバ アドレスがあることができます。認証がプライマリー サーバーによって失敗した場合、各々の設定されたバックアップサーバは順に試み

られます。

ステップ 5 ステップ 2 の IPv6 を選択した場合、プライマリ グローバル な RADIUSサーバの IPv6 アドレスを入力して下さい。

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IPv6 Address-1: 2001:DB8:1234:abcd:: (XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX)

Server IPv6 Address-2: 2002:DB8:1234:abcd:: (XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX)

Server IPv6 Address-3: 2003:DB8:1234:abcd:: (XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX)

Server IPv6 Address-4: 2004:DB8:1234:abcd:: (XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: Server IP Address-1

Broadcast Key Refresh Rate: 300 Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: 0 Sec (Range: 30-86400, 0 = Disable, Default: 0)

注: 3 まで IPv6 バックアップ RADIUSサーバ アドレスがあることができます。認証がプライマリ サーバーによって失敗した場合、各々の設定されたバックアップサーバは順に試みられます。

ステップ 6 Key-1 フィールドでは、WAP デバイスがプライマリ RADIUSサーバに認証するのに使用している共有秘密鍵で入力して下さい。

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
 Server IP Address-2: (xxx.xxx.xxx.xxx)
 Server IP Address-3: (xxx.xxx.xxx.xxx)
 Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)
 Key-2: (Range: 1-64 Characters)
 Key-3: (Range: 1-64 Characters)
 Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)
 Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

ステップ7 Key-4 フィールドへの Key-2 では、設定されたバックアップ RADIUSサーバとの RADIUS 鍵準で入力して下さい。サーバIP Address-2 は Key-2 を、サーバのIPアドレス3 使用します Key-3 を使用し、サーバのIPアドレス 4 は Key-4 を使用します。

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
 Server IP Address-2: (xxx.xxx.xxx.xxx)
 Server IP Address-3: (xxx.xxx.xxx.xxx)
 Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)
 Key-2: (Range: 1-64 Characters)
 Key-3: (Range: 1-64 Characters)
 Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)
 Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

トラッキングを有効にしたいと思い、リソースの測定が特定のユーザー消費したら場合有効 RADIUS 説明フィールドのステップ 8. (オプションの) は、チェックボックスをチェッ

クします。RADIUS 説明を有効にすることは送受信された特定のユーザーのデータのシステムの時刻および量をトラッキングすることを可能にします。

WPA Versions:	<input checked="" type="checkbox"/> WPA-TKIP	<input checked="" type="checkbox"/> WPA2-AES
	<input checked="" type="checkbox"/> Enable pre-authentication	
<input type="checkbox"/> Use global RADIUS server settings		
Server IP Address Type:	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6	
Server IP Address-1:	<input type="text" value="192.168.10.23"/>	(xxx.xxx.xxx.xxx)
Server IP Address-2:	<input type="text" value="192.168.10.24"/>	(xxx.xxx.xxx.xxx)
Server IP Address-3:	<input type="text" value="192.168.10.25"/>	(xxx.xxx.xxx.xxx)
Server IP Address-4:	<input type="text" value="192.168.10.26"/>	(xxx.xxx.xxx.xxx)
Key-1:	<input type="text" value="....."/>	(Range: 1-64 Characters)
Key-2:	<input type="text" value="....."/>	(Range: 1-64 Characters)
Key-3:	<input type="text" value="....."/>	(Range: 1-64 Characters)
Key-4:	<input type="text" value="....."/>	(Range: 1-64 Characters)
<input checked="" type="checkbox"/> Enable RADIUS Accounting		
Active Server:	<input type="text" value="Server IP Address-1"/> ▼	
Broadcast Key Refresh Rate:	<input type="text" value="300"/>	Sec (Range: 0-86400, 0 = Disable, Default: 300)
Session Key Refresh Rate:	<input type="text" value="0"/>	Sec (Range: 30-86400, 0 = Disable, Default: 0)

注: プライマリ RADIUSサーバおよびすべてのバックアップサーバのために説明するイネーブルになった RADIUS それ有効に なれば。

ステップ 9.最初のサーバを選択して下さいアクティブなサーバフィールドでアクティブである。これは有効に しま各設定されたサーバを順に接続する WAP デバイス試みを持って いますよりもむしろアクティブな RADIUSサーバの手動選択を。

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
 Server IP Address-2: (xxx.xxx.xxx.xxx)
 Server IP Address-3: (xxx.xxx.xxx.xxx)
 Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)
 Key-2: (Range: 1-64 Characters)
 Key-3: (Range: 1-64 Characters)
 Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: Server IP Address-1
Server IP Address-2
Server IP Address-3
Server IP Address-4

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)
 Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

ステップ 10: ブロードキャスト キーリフレッシュレートフィールドでは、ブロードキャスト (グループ) キーがこの VAP と関連付けられるクライアントのためにリフレッシュされる間隔で入力して下さい。デフォルトは 300 秒です。

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
 Server IP Address-2: (xxx.xxx.xxx.xxx)
 Server IP Address-3: (xxx.xxx.xxx.xxx)
 Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)
 Key-2: (Range: 1-64 Characters)
 Key-3: (Range: 1-64 Characters)
 Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: 300 Sec (Range: 0-86400, 0 = Disable, Default: 300)
 Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

ステップ 11: セッションキーリフレッシュレートフィールドでは、WAP デバイスが VAP と関連付けられる各クライアントのためのセッション (ユニキャスト) キーをリフレ

ツッシュする間隔を入力して下さい。デフォルト値は 0 です。

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication
 Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: 192.168.10.23 (xxx.xxx.xxx.xxx)
Server IP Address-2: 192.168.10.24 (xxx.xxx.xxx.xxx)
Server IP Address-3: 192.168.10.25 (xxx.xxx.xxx.xxx)
Server IP Address-4: 192.168.10.26 (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)
Key-2: (Range: 1-64 Characters)
Key-3: (Range: 1-64 Characters)
Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: Server IP Address-1

Broadcast Key Refresh Rate: 300 Sec (Range: 0-86400, 0 = Disable, Default: 300)
Session Key Refresh Rate: 0 Sec (Range: 30-86400, 0 = Disable, Default: 0)

MAC フィルタ

MAC フィルタはこの VAP にアクセスできるステーションが MAC アドレスの設定されたグローバル リストに制限されるかどうか規定します。

ステップ 1: MAC フィルタ ドロップダウン リストで、MAC フィルタリングの目的の型を選択して下さい。

Select the radio interface first, and then enter the configuration parameters.
Radio: Radio 1 (2.4 GHz) Radio 2 (5 GHz)

VAP No.	Enable	VLAN ID Add New VLAN	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation
0	<input checked="" type="checkbox"/>	1	CISCO00D	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>
1	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	None	Disabled Local RADIUS	<input type="checkbox"/>

Add Edit Delete

利用可能なオプションは次の通り定義されます:

- 無効— MAC フィルタリングを使用しません。
- ローカル— MAC フィルタリング セクションで設定する MAC 認証リストを、MAC フィルタリングについて詳細を学ぶのに使用したり [WAP351 および WAP131 の MAC フィルタリングを設定する方法](#)を参照します。
- radius —外部 RADIUSサーバの MAC 認証リストを使用します。

チャネル分離

チャネル分離が無効になるとき、無線クライアントは WAP デバイスを通してトラフィック

クの送信によって普通互いに通信できます。有効にされたとき、WAP デバイスは同じ VAP の無線クライアント間の通信をブロックします。WAP デバイスはまだネットワークの、WDS リンクを渡って、および異なる VAP と、ない無線クライアント間で関連付けられる他の無線クライアントの無線クライアントと配線されたデバイス間のデータトラフィックを可能にします。

ステップ 1: チャンネル分離フィールドでは、チャンネル分離を有効にしたいと思う場合チェックボックスをチェックして下さい。

Select the radio interface first, and then enter the configuration parameters.

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

VAP No.	Enable	VLAN ID Add New VLAN	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discoSB	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	None	Disabled	<input checked="" type="checkbox"/>

Add Edit Delete

ステップ 2. 『SAVE』 をクリックして下さい。

注: 新しい設定が保存された後、対応するプロセスは停止し、再起動するかもしれません。この条件が起こるとき、WAP デバイスは接続を失うかもしれません。接続の損失が最少影響無線クライアントとき WAP デバイス設定を変更することを推奨します。

帯域雄牛

帯域雄牛は WAP371 だけで利用できます。帯域雄牛は 2.4 ギガヘルツ帯域からの 5 ギガヘルツ帯域にステアリングデュアルバンドサポートされているクライアントによって効果的に利用します 5 ギガヘルツ帯域をあります。これはレガシーデバイスによって使用のための 2.4GHz 帯域を自由に使えるようにします二重無線サポートがない。

注: 帯域雄牛を使用するために 5 GHz および 2.4 GHz 無線は両方有効になる必要があります。無線を有効にすることに関する詳細については [WAP371 の基本的な電波設定を行う方法を参照](#)して下さい。

ステップ 1. 帯域雄牛は両方の無線で有効になる基礎および必要毎 VAP の a で設定されます。帯域雄牛を有効にしたいと思う場合帯域雄牛フィールドのチェックボックスをチェックして下さい。

Select the radio interface first, and then enter the configuration parameters.

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

VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discoSB	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	None	Disabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add Edit Delete

注: 帯域雄牛は時間に依存する音声またはビデオトラフィックの VAPs で励まされません。5 ギガヘルツ無線はより少ない帯域幅を使うために起こってもその無線にクライアントを操縦することを試みます。

ステップ 2. 『SAVE』 をクリックして下さい。

VAP の削除

ステップ 1: 削除したいと思う VAP のチェックボックスをチェックして下さい。

Select the radio interface first, and then enter the configuration parameters.

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

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>		
Show Details									
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>		
Show Details									

ステップ 2. VAP を削除するために『Delete』をクリックして下さい。

Select the radio interface first, and then enter the configuration parameters.

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

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>		
Show Details									
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>		
Show Details									

ステップ 3. 削除を永久に保存するために『SAVE』をクリックして下さい。

Select the radio interface first, and then enter the configuration parameters.

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

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>		