

NETGEAR®

ProSAFE

ワイヤレス LAN コントローラー

WC7520

管理マニュアル



350 East Plumeria Drive
San Jose, CA 95134
USA

February 1, 2016
202-10686-04 (英文参照文書)

NETGEAR 製品をお選びいただきありがとうございます。

NETGEAR 製品のインストール、設定、または仕様に関するご質問や問題については、下記の NETGEAR カスタマーサポートまでご連絡ください。

無償保証を受けるためには、本製品をご購入後 30 日以内にユーザー登録が必要になります。ユーザー登録方法につきましては、別紙[ユーザー登録のお知らせ]をご確認ください。

NETGEAR カスタマーサポート

電話:フリーコール 0120-921-080

(携帯・PHS など、フリーコールが使用できない場合:03-6670-3465)

受付時間:平日 9:00 - 20:00、土日祝 10:00 - 18:00(年中無休)

テクニカルサポートの最新情報は、NETGEAR のウェブサイトをご参照ください。

<http://www.netgear.jp/support/>

商標

NETGEAR、NETGEAR ロゴは米国およびその他の国における NETGEAR, Inc.の商標または登録商標です。

その他のブランドおよび製品名は、それぞれの所有者の商標または登録商標です。

記載内容は、予告なしに変更されることがあります。

© 2016 NETGEAR, Inc. All rights reserved.

適合性

本製品をお使いになる前に、適合性の情報をお読みください。

各種規格との適合に関する情報は、ネットギアのウェブサイト (<http://www.netgear.com/about/regulatory/>) をご覧ください(英語)。

| 製品型番 | ファームウェア |
|---------------|------------------|
| WC7520-100AUS | WC7520_V2.5.0.35 |

改版履歴

2016.2.2: 初版

目次

| | |
|--|----|
| 改版履歴..... | 3 |
| 1. はじめに..... | 13 |
| 主な機能..... | 13 |
| 同梱内容..... | 15 |
| ハードウェア機能..... | 15 |
| 前面パネルポートと LED..... | 15 |
| 背面パネル機能..... | 16 |
| 底面パネルと製品ラベル..... | 17 |
| WC7520 ワイヤレスコントローラーシステム要素..... | 17 |
| NETGEAR ProSAFE アクセスポイント..... | 17 |
| WC7520 ワイヤレスコントローラーでできること..... | 18 |
| ワイヤレスネットワークの計画..... | 18 |
| ネットワークでのアクセスポイントの発見および IP アドレスとファームウェアの提供..... | 18 |
| ネットワークの整理..... | 19 |
| ネットワークのワイヤレス設定を集中管理する..... | 19 |
| ネットワークのセキュリティを集中管理..... | 19 |
| 他のワイヤレスコントローラーの管理..... | 20 |
| ネットワークとその構成要素の監視..... | 20 |
| ライセンス..... | 20 |
| Web 管理インターフェースレイアウト..... | 20 |
| 初回接続と設定..... | 22 |
| ワイヤレスコントローラーを設定、設置する..... | 22 |
| 基本および拡張設定..... | 23 |
| プロファイルグループ..... | 24 |
| 基本(Basic)プロファイル..... | 24 |
| 拡張(Advanced)プロファイル..... | 25 |
| ワイヤレスコントローラーを設置する場所を選ぶ..... | 26 |
| ワイヤレスコントローラーの設置..... | 27 |
| ワイヤレスコントローラーを設置する..... | 27 |
| 2. システム計画と設置シナリオ..... | 28 |
| システム計画..... | 28 |
| 導入前計画..... | 28 |
| ワイヤレスコントローラーを設定する前に..... | 28 |
| VLAN..... | 28 |

| | |
|---|----|
| DHCP サーバー..... | 29 |
| クライアント認証とデータ暗号化..... | 29 |
| 基本プロファイルグループのシングルコントローラー構成..... | 30 |
| 基本プロファイルグループのシングルワイヤレスコントローラーシステムを設定する..... | 30 |
| 拡張プロファイルグループのシングルコントローラー構成..... | 31 |
| 拡張プロファイルグループのシングルワイヤレスコントローラーシステムを設定する..... | 31 |
| スタックコントローラー構成..... | 32 |
| スタックコントローラー構成を設定する..... | 32 |
| 管理 VLAN とデータ VLAN 計画..... | 32 |
| 導入シナリオ..... | 33 |
| シナリオ 1: 一つの VLAN の基本ネットワーク..... | 34 |
| ワイヤレスコントローラーのプロビジョニング..... | 35 |
| シナリオ 2: 複数の VLAN と SSID の拡張ネットワーク..... | 35 |
| 前提条件..... | 36 |
| ワイヤレスコントローラーのプロビジョニング..... | 37 |
| シナリオ 3: 冗長化の拡張ネットワーク..... | 38 |
| 前提条件..... | 39 |
| ワイヤレスコントローラーのプロビジョニング..... | 40 |
| 3. 電波計画..... | 41 |
| 電波計画の概要..... | 41 |
| 計画要件..... | 41 |
| ビルとフロアの定義と編集..... | 42 |
| ビルを定義する..... | 42 |
| ビルを編集する..... | 45 |
| ビルを削除する..... | 45 |
| アクセスポイントの要件を特定する..... | 45 |
| 無線 LAN の要件を特定するために、アクセスポイント数を推測し、推奨設置位置を確認する..... | 46 |
| ヒートマップを確認する..... | 48 |
| ヒートマップを表示し、アクセスポイントの設置場所を調整する..... | 48 |
| 4. アクセスポイントディスカバリーと管理..... | 51 |
| アクセスポイントディスカバリーとディスカバリーガイドライン..... | 51 |
| ローカルアクセスポイントのオートディスカバリー条件..... | 51 |
| 一般的なガイドライン..... | 51 |
| レイヤー3ネットワークを介してのオートディスカバリー手順のガイドライン..... | 51 |
| リモートアクセスポイントのオートディスカバリーの条件..... | 52 |

| | |
|---|----|
| リモートアクセスポイントのオートディスカバリー手順のガイドライン | 52 |
| ディスカバリー後の制限 | 53 |
| Discovery Wizard の実行 | 53 |
| Discovery Wizard を実行する | 54 |
| Discovery 結果 | 56 |
| アクセスポイントリスト (Access Point List) の管理 | 56 |
| Discovery 後アクセスポイントを Managed List に追加する | 56 |
| サイト指定を選択し、発見したアクセスポイントを管理リストに追加する | 56 |
| アクセスポイント情報の編集と削除 | 59 |
| Managed AP List でアクセスポイントを編集する | 59 |
| Managed AP List からアクセスポイントを削除する | 62 |
| 5. ネットワーク設定 | 63 |
| 一般設定 (General Settings) | 63 |
| 一般設定をする | 63 |
| 時間管理 | 64 |
| 時間設定をする | 64 |
| IP と VLAN 設定 | 65 |
| IP/VLAN 設定をする | 65 |
| 管理 VLAN | 66 |
| タグ無し VLAN | 66 |
| DHCP サーバーの管理 | 66 |
| DHCP サーバーを追加し設定をする | 67 |
| DHCP サーバーを編集する | 68 |
| DHCP サーバーを削除する | 68 |
| 証明書管理 | 69 |
| 証明書を追加する | 69 |
| Syslog とアラーム通知設定 | 69 |
| Syslog 設定をする | 70 |
| Syslog 設定をする | 70 |
| アラーム通知 (Alarm Notification) 設定 | 70 |
| アラームアクション (Alarm Actions) を設定する | 70 |
| メール通知サーバー設定 | 71 |
| メール設定をする | 71 |
| 6. セキュリティプロファイルとプロファイルグループ管理 | 73 |
| ワイヤレスセキュリティプロファイル管理 | 73 |

| | |
|--|----|
| 小さな無線 LAN ネットワーク..... | 73 |
| 大きな無線 LAN ネットワーク..... | 74 |
| プロファイル命名規則..... | 74 |
| プロファイルを設定する前に..... | 74 |
| 基本プロファイルグループのセキュリティプロファイル設定..... | 75 |
| 基本プロファイルグループにセキュリティプロファイルを追加する..... | 75 |
| 基本プロファイルグループでのプロファイルの編集・削除..... | 78 |
| 既存プロファイルの編集をする..... | 78 |
| 既存プロファイルを削除する..... | 78 |
| ネットワーク認証とデータ暗号化オプション..... | 78 |
| 拡張プロファイルグループのセキュリティプロファイル設定..... | 81 |
| プロファイルグループの追加、新しいプロファイルの設定、プロファイルの追加..... | 82 |
| Edit and Remove Profiles from an Advanced Profile Group..... | 84 |
| 拡張プロファイルグループのプロファイルを編集する..... | 84 |
| 拡張プロファイルグループからプロファイルを削除する..... | 84 |
| 拡張プロファイルグループの削除..... | 84 |
| 拡張プロファイルグループを削除する..... | 84 |
| 基本と拡張プロファイルグループの管理..... | 84 |
| アクセスポイントをプロファイルグループに割り当てる..... | 85 |
| 7. 無線と QoS 設定..... | 87 |
| 基本と拡張無線と QoS 設定..... | 87 |
| 電波設定..... | 87 |
| 基本電波設定..... | 88 |
| 電波をスケジュールする..... | 88 |
| プロファイルグループのための拡張電波設定..... | 88 |
| プロファイルグループの電波をスケジュールする..... | 89 |
| 無線設定..... | 89 |
| 基本無線設定..... | 89 |
| 基本無線設定をする..... | 89 |
| プロファイルグループの拡張無線設定..... | 93 |
| プロファイルグループの無線設定をする..... | 93 |
| チャンネル設定..... | 95 |
| チャンネル割り当てを変更する..... | 96 |
| 電波管理..... | 98 |
| 基本電波管理..... | 99 |

| | |
|--------------------------------------|-----|
| 基本電波管理を設定する..... | 99 |
| プロファイルグループの拡張電波監視..... | 101 |
| 拡張電波監視を設定する..... | 101 |
| プロファイルグループの QoS 設定..... | 102 |
| プロファイルグループの QoS を設定する..... | 103 |
| ロードバランス設定..... | 104 |
| ロードバランスを設定する..... | 105 |
| レートリミット設定..... | 106 |
| 基本レートリミット..... | 106 |
| 基本レートリミットを設定する..... | 106 |
| プロファイルグループの拡張レートリミット..... | 107 |
| 拡張レートリミットを設定する..... | 107 |
| 8. ネットワークアクセスとセキュリティ設定..... | 109 |
| 基本と拡張セキュリティ設定について..... | 109 |
| 不正アクセスポイント管理..... | 110 |
| 基本不正アクセスポイント検出設定..... | 110 |
| 不正アクセスポイント検出のためにサーバーを設定する..... | 110 |
| 拡張不正アクセスポイント検出設定..... | 112 |
| 拡張不正アクセスポイント検出を設定する..... | 112 |
| Known アクセスポイントのリストのファイルからのインポート..... | 113 |
| アクセスポイントをファイルからインポートする..... | 113 |
| MAC 認証と MAC 認証グループの管理..... | 114 |
| 外部 MAC 認証のガイドライン..... | 114 |
| 外部 ACL を使う..... | 114 |
| 基本ローカル MAC 認証設定..... | 115 |
| 基本 MAC 認証を設定する..... | 115 |
| ファイルから MAC リストをインポートする..... | 116 |
| ファイルから MAC リストをインポートする..... | 116 |
| ローカル MAC 認証グループ設定..... | 117 |
| MAC 認証グループを設定する..... | 117 |
| 認証サーバーと認証サーバーグループ管理..... | 118 |
| 基本認証サーバー設定..... | 119 |
| 基本認証サーバーを設定する..... | 119 |
| RADIUS 認証サーバーグループ設定..... | 120 |
| RADIUS 認証グループを設定する..... | 121 |

| | |
|--|-----|
| ゲストネットワーク管理..... | 121 |
| キャプティブポータル設定..... | 122 |
| キャプティブポータルを設定する..... | 123 |
| ユーザー、アカウント、パスワード管理..... | 124 |
| ユーザーまたはアカウントを追加する..... | 125 |
| ユーザーまたはアカウントを編集または削除する..... | 129 |
| ユーザーまたはアカウントのリストをエクスポートする..... | 129 |
| 9. コントローラーのメンテナンス..... | 130 |
| 設定ファイル管理..... | 130 |
| 設定ファイルのバックアップと復元..... | 130 |
| 設定ファイルをバックアップする..... | 130 |
| 設定ファイルを復元する..... | 131 |
| ファームウェアをアップグレードする..... | 131 |
| ファームウェアをアップグレードする..... | 131 |
| ワイヤレスコントローラーの再起動またはリセット..... | 134 |
| ワイヤレスコントローラーを再起動する..... | 134 |
| ワイヤレスコントローラーをリセットする..... | 134 |
| アクセスポイントの再起動..... | 135 |
| アクセスポイントを再起動する..... | 135 |
| 外部ストレージ管理..... | 135 |
| 外部ストレージデバイスをマウントしてデバイスの情報を見る..... | 136 |
| リモートアクセス管理..... | 136 |
| SNMP を有効にして設定をする..... | 136 |
| セッションタイムアウト設定..... | 138 |
| ワイヤレスコントローラーの HTTP セッションタイムアウトを設定する..... | 138 |
| ログの保存..... | 138 |
| アクセスポイントログを保存する..... | 138 |
| システムログを保存する..... | 139 |
| アラートとイベントを表示する..... | 139 |
| システムアラートを表示する..... | 140 |
| 電波イベント(RF events)を表示する..... | 140 |
| ロードバランスイベントを表示する..... | 141 |
| レートリミットイベントを表示する..... | 141 |
| 冗長化イベントを表示する..... | 142 |
| スタッキングイベントを表示する..... | 142 |

| | |
|--|-----|
| ライセンス管理..... | 142 |
| ライセンス情報..... | 143 |
| ライセンス情報を表示する..... | 143 |
| ライセンスサーバー設定..... | 144 |
| ライセンスサーバー設定をする..... | 144 |
| ライセンス登録..... | 145 |
| ライセンスを Retrieve Your Licenses..... | 146 |
| 10. スタックと冗長管理..... | 148 |
| スタック管理..... | 148 |
| スタック設定..... | 149 |
| スタックを設定する..... | 149 |
| コントローラー選択リスト..... | 151 |
| 冗長化管理 (Manage Redundancy)..... | 151 |
| シングルコントローラー冗長化..... | 151 |
| シングルコントローラー冗長化の要件と制限..... | 152 |
| シングルコントローラー冗長化の例..... | 152 |
| N:1 冗長..... | 154 |
| N:1 冗長の要件と制限..... | 154 |
| N:1 冗長構成の例..... | 155 |
| 冗長設定..... | 157 |
| 冗長を設定する..... | 157 |
| 冗長を設定後に冗長コントローラーを変更する..... | 159 |
| 冗長グループを削除する..... | 159 |
| 11. ワイヤレスネットワークと構成要素の監視..... | 160 |
| ネットワークを監視する..... | 160 |
| Network Summary 画面を表示する..... | 161 |
| ネットワーク使用量 (Network Usage) 表示..... | 163 |
| ワイヤレスコントローラー表示..... | 163 |
| アクセスポイント表示..... | 164 |
| クライアント表示..... | 168 |
| セキュリティプロファイル監視..... | 171 |
| ワイヤレスコントローラー監視..... | 172 |
| ワイヤレスコントローラーを監視する..... | 172 |
| Wireless Controller Summary 画面を表示する..... | 173 |
| ワイヤレスコントローラー使用量表示..... | 175 |

| | |
|--|-----|
| アクセスポイント表示 | 175 |
| クライアント表示 | 177 |
| 近隣クライアント表示 | 177 |
| 不正アクセスポイント表示 | 178 |
| セキュリティプロファイル表示 | 180 |
| DHCP リース表示 | 180 |
| キャプティブポータルゲストとユーザー | 181 |
| ゲストリストを表示する | 181 |
| キャプティブポータルユーザーリストを表示する | 182 |
| SSID 監視 | 183 |
| SSID を監視する To monitor the active SSIDs in the network: | 183 |
| クライアント監視 | 183 |
| クライアントを監視する | 183 |
| ローカルクライアント表示 | 184 |
| ブラックリストクライアント表示 | 184 |
| 12. トラブルシューティング | 186 |
| 基本機能のトラブルシューティング | 186 |
| Power LED が点灯しない | 186 |
| Test LED が消灯しない | 186 |
| LAN ポートの LED が点灯しない | 186 |
| Web 管理インターフェースのトラブルシューティング | 187 |
| イーサネットケーブル | 187 |
| IP アドレス設定 | 187 |
| インターネットブラウザ | 188 |
| Ping ユーティリティを使って TCP/IP ネットワークをトラブルシューティングする | 188 |
| ワイヤレスコントローラーへの LAN 接続を確認する | 188 |
| WindowsPC からワイヤレスコントローラーに Ping する | 189 |
| ファクトリーデフォルトボタンを使ってデフォルト設定を復元する | 190 |
| すべての情報を消去し、工場出荷設定を復元する | 190 |
| 日時の問題 | 190 |
| アクセスポイントの問題 | 191 |
| 発見 (Discovery) の問題 | 191 |
| すべてのアクセスポイントに対して | 191 |
| レイヤー3 ネットワークにインストールされているアクセスポイントに対して | 191 |
| リモートアクセスポイントに対して | 191 |

| | |
|----------------------------------|-----|
| 接続問題..... | 192 |
| ネットワークパフォーマンスと不正アクセスポイント検出 | 192 |
| ワイヤレスコントローラーで診断ツールを使う..... | 192 |
| アクセスポイントに Ping する..... | 192 |
| アクセスポイントにトレースルートする..... | 193 |
| 13. 工場出荷設定と技術仕様..... | 195 |
| 仕様..... | 195 |

1. はじめに

主な機能

ProSAFE ワイヤレス LAN コントローラーWC7520 は中規模の企業や学校、病院等での利用を想定したものです。スタック構成で必要なライセンスを利用すると、ワイヤレスコントローラーは 150 台のアクセスポイント、1500 以上のユーザーをサポートできます。ワイヤレスコントローラーは IEEE802.11a/b/g/n をサポートします。ワイヤレスコントローラーで、ワイヤレスネットワークの集中管理、集中的なセキュリティ機能の実行、レイヤー2、レイヤー3 ローミング、ゲストアクセスキャプティブポータル設定、ボイスオーバーWi-Fi (VoWi-Fi)を行うことができます。

ワイヤレスコントローラーは以下の機能を提供します。

- **スタッキングと冗長化によるスケーラブルアーキテクチャー**
 - 追加ライセンスなしに 1 台のワイヤレスコントローラーで 20 台のアクセスポイントをサポート。
 - ライセンス(WC7510L)の購入で 10 台単位のワイヤレスアクセスポイントの追加、1 台のワイヤレスコントローラーで 50 台まで管理可能。
 - 最大 3 台までのワイヤレスコントローラーのスタック構成で最大 150 アクセスポイントまで管理可能。
 - N:1 冗長化サポート。
 - 802.11a, 802.11b, 802.11g, 802.11n モード対応。
- **アクセスポイントの自動発見 (Autodiscovery)**
 - 同じレイヤー2 ドメインでの Autodiscovery。
 - レイヤー3 ドメインでの Autodiscovery。
 - VPN 接続経由のリモートアクセスポイントの Autodiscovery。
 - 発見されて、管理アクセスポイントリストに追加されたアクセスポイントに対するワイヤレスコントローラー用ファームウェアの自動ダウンロード。
- **集中管理**
 - 全ワイヤレスネットワークの一点集中管理。
 - ワイヤレスネットワークのライブカバレッジおよびヒートマップ。
 - すべての管理されたアクセスポイントに対して自動ファームウェアアップデート。
 - DHCP サーバー機能。
 - 設定・変更可能な管理 VLAN。
- **セキュリティ**
 - 外部 RADIUS または LDAP(Active Directory)サーバー、または内部認証サーバーでの認証。

- プロファイルグループ毎の 8 つのプロファイルおよび電波 (2.4GHz, 5GHz) 毎の 8 プロファイル (デュアルバンドアクセスポイントでは一つのプロファイルグループで計 16 プロファイルとなります。)
- 1 台のワイヤレスコントローラーで最大 128 のアクセスポイントプロファイル¹をサポートします (1 グループ 8 プロファイル、電波あたり 8 つのグループ)。各アクセスポイントプロファイルは SSID 設定、ネットワーク認証、データ暗号化、クライアント分離、VLAN, MAC ACL, ワイヤレス QoS をサポートします。
- ワイヤレスコントローラーは 8 つのアクセスポイントプロファイルグループ²をサポートします。
- 不正アクセスポイント検出、選別および鎮静機能。
- 課金および時間管理によるゲストアクセスとキャプティブポータルアクセス。
- ワイヤレスのオンオフスケジュール。
- **WMM(Wi-Fi Multimedia) QoS(Quality of Service)と拡張ワイヤレス機能**
 - WMM(Wi-Fi Multimedia)によるビデオ、オーディオ、Voice over Wi-Fi (VoWi-Fi)サポート。
 - WMM パワーセーブオプション。
 - 自動ワイヤレス LAN 修復機能によりワイヤレスユーザーのシームレスカバー。
 - レイヤー2、レイヤー3のシームレスローミング。
 - 高速処理のためのアクセスポイントレベルでのローカルレイヤー2トラフィックスイッチングとコントローラーレベルでのレイヤー3トラフィック処理。
- **電波計画と管理**
 - RF プラニングツールでビルディングのフロア毎のユーザー数と信号強度に基づきアクセスポイントの数と位置予測および予測カバー範囲の表示をします。
 - アクセスポイントの送信パワーと干渉を軽減するためのチャンネル割り当ての自動調整機能。
 - アクセスポイント間のクライアントの自動ロードバランシング。
 - プロファイル単位のレートリミット。
- **監視と報告**
 - リアルタイムな LAN 状態表示のためのワイヤレスバンドと信号強度によるアクセスポイントヒートマップ。
 - ネットワーク状態、ワイヤレスコントローラー、ワイヤレス LAN, クライアント、ネットワーク利用統計情報の監視。
 - アクセスポイントの詳細状態監視。
 - システムイベント、ロードバランスイベント、レートリミットイベント、冗長化フェールオーバーイベントのログとメール通知。

1. プロファイル数はワイヤレスコントローラーで使われるアクセスポイントのモデルに依存します。

2. プロファイルグループ数はワイヤレスコントローラーで使われるアクセスポイントのモデルに依存します。

同梱内容

ProSAFE ワイヤレス LAN コントローラーWC7520 製品パッケージには以下のものが同梱されています。

- ProSAFE ワイヤレス LAN コントローラーWC7520
- AC 電源ケーブル
- ラバーフット (4) と粘着シール
- ラックマウントキット
- カテゴリー5ストレートイーサネットケーブル
- インストールガイド
- リソース CD

ハードウェア機能

ワイヤレスコントローラーの前面パネルポートと LED、リアパネル、底面ラベルについて記します。

前面パネルポートと LED

以下の図にワイヤレスコントローラーの前面パネルポートとステータス LED を示します。



左から右に向かってワイヤレスコントローラーの前面パネルには以下のポートと LED があります。

- 電源 LED
- テスト LED
- 多くのフロアヒートマップや統計情報ヒストリーのための外部ストレージ用の USB ポート。
- 4ポート 10/100/1000Base-T RJ-45 イーサネットポート。すべてのイーサネットポート間はスイッチングされます。オートネゴシエーション、Auto MDI/MDIX。

メモ: 4ポートは一つのスイッチとして動作します。

LED の機能を以下に示します。

LED 機能

| LED | 状態 | 説明 |
|--------|----|---|
| 電源 LED | 点灯 | ワイヤレスコントローラーの電源が入っている時は 緑色 に点灯します。 |

| | | |
|------------------|----------|---|
| | 消灯 | ワイヤレスコントローラーの電源を入れてもこの LED が点灯しない場合は、電源の接続を確認します。 |
| テスト LED | 点灯 | ワイヤレスコントローラーが起動中です。約 2 分後ワイヤレスコントローラーのテスト機能が終了すると消灯します。テスト LED が点灯したままの時は、起動に失敗しています。 |
| | 消灯 | ワイヤレスコントローラーの起動が完了しました。通常の動作では消灯です。 |
| | 点滅 | ファームウェアアップデート中です。 |
| 各 LAN ポートの左側 LED | 消灯 | 物理リンクなし。機器が接続されていない。 |
| | 点灯(緑) | イーサネットデバイスが接続されています。 |
| | 点滅(緑) | ポートでデータ送受信中。 |
| 各 LAN ポートの右側 LED | 消灯 | ポート速度が 10Mbps で動作中。 |
| | 点灯(オレンジ) | ポート速度が 100Mbps で動作中。 |
| | 点灯(緑) | ポート速度が 1000Mbps で動作中。 |

背面パネル機能

以下の図にワイヤレスコントローラーの背面パネル構成要素を示します。



左から右に向かってワイヤレスコントローラーの背面パネルには以下の構成要素があります。

- **コンソールポート:** ネットギアテクニカルサポートの指導のもとに使うコンソールポートです。
- **ファクトリーデフォルトボタン:** 細い棒状のもので前面 LED が点滅するまで焼く 10 秒間押し続けます。ワイヤレスコントローラーは工場出荷状態に戻ります。

メモ: ワイヤレスコントローラーをリセットすると、すべての設定は消え、デフォルトパスワードに復帰します。

- **ケンジントンロック:** ケンジントンロックケーブルを接続しワイヤレスコントローラーの盗難等を防ぎます。
- **AC 電源ソケット:** 電源ケーブルを接続します。(本体に電源オンオフスイッチはありません)

底面パネルと製品ラベル

ワイヤレスコントローラーの底面にある製品ラベルには、デフォルト IP アドレス、デフォルトユーザー名、デフォルトパスワード、および標準規格、電源等の情報が記載されています。



WC7520 ワイヤレスコントローラーシステム要素

WC7520 ワイヤレスコントローラーシステムは一つまたは複数のワイヤレスコントローラーから構成され、ロケーションとネットワークアクセスにもとづいてグループ化されたアクセスポイントの集合です。

ワイヤレスコントローラーシステムは 1 台のワイヤレスコントローラー、あるいは 1 台のワイヤレスコントローラーと N:1 冗長化のための 1 台のバックアップワイヤレスコントローラー、3 台までのスタックされたワイヤレスコントローラーと N:1 冗長化のための 1 台のワイヤレスコントローラーを含みます。

WC7520 ワイヤレスコントローラーシステムは以下のアクセスポイントモデルをサポートします。(日本国内販売したもの)

- WNAP320
- WNDAP360

NETGEAR ProSAFE アクセスポイント

アクセスポイントをワイヤレスコントローラーにイーサネットケーブルで直接ルーターやスイッチ経由であるいは IP ネットワーク経由でリモート接続する事ができます。オートディスカバリー(自動発見)の後、アクセスポイントをワイヤレスコントローラーの管理アクセスポイントリストに追加すると、ワイヤレスコントローラーはアクセスポイントにファームウェアを送り込むことにより、通常のアクセスポ

イントを従属アクセスポイントに変換します。以降はアクセスポイントを集中管理、集中監視できるようになります。

WC7520 ワイヤレスコントローラーは以下のアクセスポイントをサポートします。(日本国外販売製品は含んでいません)

- **WNAP320 ProSAFE シングルバンド Wireless-N アクセスポイント**

- 802.11b, 802.11g, 802.11n 対応
- PoE(Power over Ethernet)対応
- オプションアンテナ
- ファームウェアバージョン WNAP320_2.0.7 以上

製品情報およびファームウェアについては以下のページを参照してください。

<http://www.netgear.jp/products/details/WNAP320.html>

- **WNDAP360 ProSAFE デュアルバンド Wireless-N アクセスポイント**

- 802.11a, 802.11b, 802.11g, 802.11n 対応
- PoE(Power over Ethernet)対応
- 2.4GHz、5GHz デュアルバンド同時動作
- オプションアンテナ
- ファームウェアバージョン WNDAP360_2.0.3 以上

製品情報およびファームウェアについては以下のページを参照してください。

<http://www.netgear.jp/products/details/WNDAP360.html>

WC7520 ワイヤレスコントローラーでできること

以下に WC7520 ワイヤレスコントローラーで行うことができるいくつかのタスクを示します。

ワイヤレスネットワークの計画

- **ワイヤレス LAN のデザイン:**ビルディングとフロア寸法によって効率のよいワイヤレス LAN をデザインできます。
- **必要なアクセスポイント数とおおよその位置の推定:**アクセスポイントが何台必要であり、最適なエリアとパフォーマンスのための位置を推定します。

ネットワークでのアクセスポイントの発見および IP アドレスとファームウェアの提供

- **ネットワークでアクセスポイントの発見:**アクセスポイントはファクトリーデフォルト状態あるいはスタンドアロンモードで動作している必要がありますが、ワイヤレスコントローラーが発見し管理

アクセスポイントリストに追加された後にアクセスポイントは従属した(管理された)アクセスポイントになります。

- **アクセスポイントに IP アドレスを提供:** 内部の DHCP サーバーを使ってネットワーク中の全てまたは一部のアクセスポイントに IP アドレスを割り当てることができます。
- **アクセスポイントファームウェアのアップグレード:** ネットワーク中のすべての管理されたアクセスポイントのファームウェアを最新にアップデートし同期します。

ネットワークの整理

- **アクセスポイントプロファイルの作成:** プロファイルを使って異なる SSID、クライアント認証、認証設定及びワイヤレス QoS 設定の異なるアクセスポイントを整理します。
- **アクセスポイントプロファイルグループの作成:** アクセスポイントプロファイルグループを使ってビル、フロア、業務、部署等の異なるアクセスポイントを整理します。簡単にアクセスポイントをプロファイルグループに割り当て、割り当てを変更することができます。

ネットワークのワイヤレス設定を集中管理する

- **電波スケジュール:** 全体のネットワークをオフラインにし、アクセスポイントプロファイルグループをオフラインにするようなスケジュールを立てる事ができます。
- **ワイヤレス設定とチャンネル割り当ての管理:** ワイヤレスモード、データレート、チャンネル帯域幅、等のワイヤレス設定をネットワーク全体、アクセスポイントプロファイルグループ管理、およびチャンネル割り当てをネットワーク全体に対して管理できます。
- **QoS 設定の管理:** データ、バックグラウンド、ビデオ、および音声トラフィックの QoS キュー設定をアクセスポイントプロファイルグループに対して管理します。
- **電波管理設定:** ネットワーク全体あるいはアクセスポイントプロファイルグループに対して、ワイヤレス LAN 修復およびワイヤレスカバレッジホール検出を設定します。

ネットワークのセキュリティを集中管理

- **ネットワークへのセキュアなアクセスとセキュアなデータ転送の管理:** クライアント認証、暗号化、ワイヤレスクライアントセキュリティ分離、MAC 認証をアクセスポイントプロファイルで管理します。
- **ネットワークの認証サーバーの管理:** ネットワーク全体あるいはネットワークの一部、アクセスポイントプロファイルグループのための内部または外部の認証サーバーを管理します。
- **MAC 認証の管理:** Trusted(信頼できる)、または Untrusted(信頼できない)MAC アドレスをネットワーク全体で指定します。
- **不正アクセスポイント管理:** 不正アクセスポイントとそれにつながるクライアントの管理。
- **ゲストアクセス管理:** ネットワークへのゲストアクセスとキャプティブポータルアクセスの管理。

他のワイヤレスコントローラーの管理

- **スタッキング管理:**スタック中のプライマリーとセカンダリーワイヤレスコントローラーを指定し、ワイヤレスコントローラー間で情報を同期します。
- **冗長化グループの管理:**冗長化グループのプライマリーとセカンダリーワイヤレスコントローラーを指定し、フェイルオーバープロテクションを有効にします。

ネットワークとその構成要素の監視

- **ヒートマップ表示:**設置したワイヤレス LAN のリアルタイムヒートマップを表示します。フロアでの無線電波の伝播状況を見てカバレッジホールと電波の弱い部分を特定します。
- **すべてのワイヤレスデバイスの状態の監視:**ワイヤレスコントローラー、アクセスポイント、クライアント、アクセスポイントプロファイル、およびネットワーク全体の状態を表示し、ネットワーク利用統計情報を表示します。
- **ネットワークの健康状態の監視:**どのアクセスポイントが健全でどのアクセスポイントがダウンや劣化しているかを表示します。

ライセンス

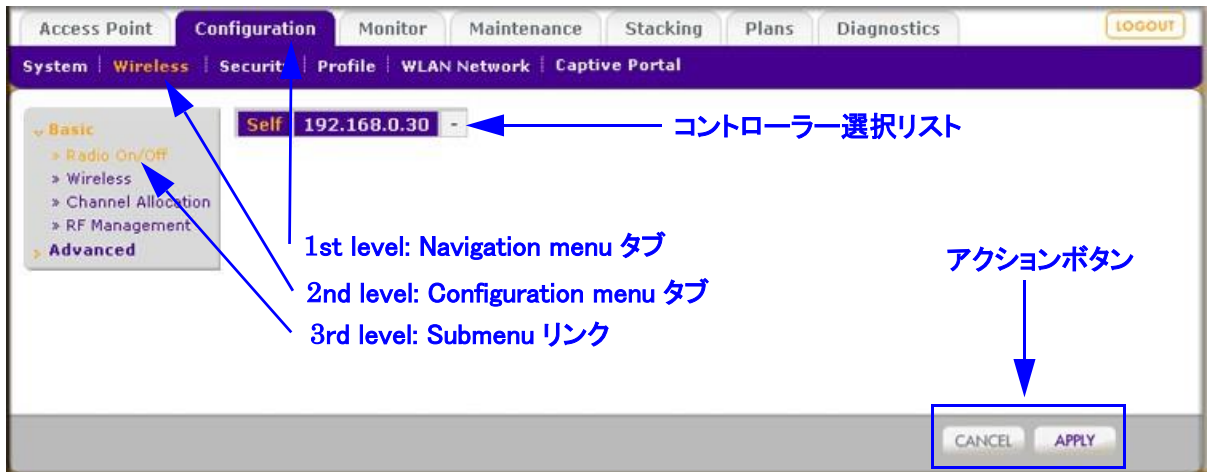
ワイヤレスコントローラーは 20 台までの 802.11a/b/g/n モードのアクセスポイントを管理できるライセンスを内蔵しています。追加ライセンスは 10 台のアクセスポイント単位(WC7510L)で購入ができ、1 台のワイヤレスコントローラーで 50 台のアクセスポイントまで管理可能です。50 台のアクセスポイントを管理するためには 3 つの WC7510L ライセンスを購入する必要があります。3 台のワイヤレスコントローラーをスタック構成で最大 150 台のアクセスポイントを管理するためには、9 つの WC7510L ライセンスを購入する必要があります。

冗長(リダンダント)ワイヤレスコントローラーにも冗長ワイヤレスコントローラーでサポートするアクセスポイント数に合わせたライセンスを購入する必要があります。

ライセンスはワイヤレスコントローラーのシリアル番号に関連付けられます。

Web 管理インターフェースレイアウト

以下の図はワイヤレスコントローラーの Web 管理インターフェース上部と左側のメニューを表示しています。(画面の表示内容は見やすくするために削除しています)



Web 管理インターフェース画面は以下の項目を含みます。

- **1st level: Main navigation menu タブ:** Web 管理インターフェースの一番上のライトグレーのバーにある Main navigation menu タブはワイヤレスコントローラーのすべての設定メニュータブへのアクセスを提供して、常時表示されています。Main navigation menu タブを選択すると、青い背景に白い文字の表示に変わります。
- **2nd level: Configuration menu タブ:** (Main navigation menu タブ直下の) 青いバーは選択した Main navigation menu タブの選択によって変わります。Configuration menu タブを選択すると、青い背景にオレンジの文字の表示に変わります。
- **3rd level: Submenu リンク:** 各 Configuration menu タブは画面左側のグレーのボックス内に一つまたは複数の Submenu リンクを持っています。Submenu リンクを選択すると、グレーの背景にオレンジの文字の表示に変わります。多くの画面で Submenu は Basic submenu と Advanced submenu にわかれます。
- **アクションボタン:** アクションボタンで設定を変更します。以下に最も共通なアクションボタンを記します。
 - **Apply:** 現在の画面のすべての設定変更を保存します。保存された設定はワイヤレスコントローラーの電源が切れても維持されます。保存されていない設定は失われます。
 - **Cancel:** 現在の画面で直前に適用 (Apply) または保存した設定にリセットします。
 - **Add:** 現在の画面で新しい項目を追加します。
 - **Edit:** 選択した項目の設定を編集します。
 - **Remove または Delete:** 選択した項目をテーブルまたは画面から削除します。
 - **Back:** 前の画面に戻ります。
 - **Next:** 次の画面に進みます。
- **Controller selection list:** スタック構成の場合に設定するワイヤレスコントローラーを選択します。

初回接続と設定

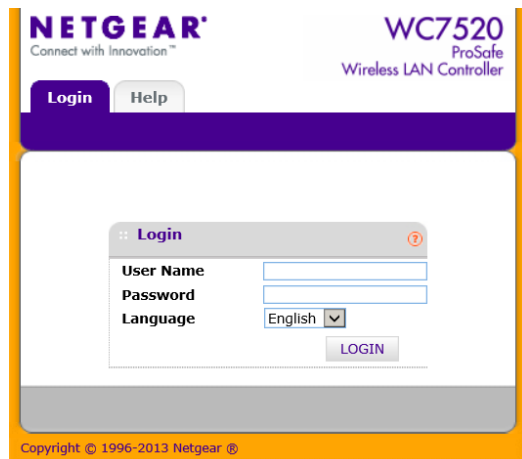
この手順に従ってワイヤレスコントローラーの設定をしてください。追加の情報として、WC7520 の製品ダウンロードページからインストールガイドをダウンロードして参照してください。

ワイヤレスコントローラーを設定、設置する

1. ワイヤレスコントローラーをコンピューターに接続する
 - a. コンピューターの IP アドレスを 192.168.0.210、サブネットマスクは 255.255.255.0 として固定 IP アドレスを設定します。
 - b. 接続はネットワーク経由(スイッチ等)またはイーサネットでワイヤレスコントローラーのイーサネットポートと直接接続します。
 - c. ワイヤレスコントローラーの電源ケーブルを AC コンセントに接続します。
 - d. ワイヤレスコントローラーの前面パネルの LED を確認します。
 - **Power:** 緑色の電源 LED が点灯します。電源 LED が点灯しない場合は電源ケーブルの接続を確認し、電源コンセントに電源が来ているか確認します。
 - **Test:** 電源を入れた時に点灯し、その後消灯します。
 - **LAN:** 機器が接続されているポートの LED が点灯します。
2. ワイヤレスコントローラーにログインする
 - a. ブラウザーのアドレスバーに <http://192.168.0.250> と入力します

メモ: Internet Explorer 5.1 以降あるいは Mozilla Firefox 1.x 以降で JavaScript、Cookie、SSL が有効であるものを使います。

ワイヤレスコントローラーのログイン画面が表示されます。



- b. User Name 欄に **admin**、Password 欄に **password** を入力します。どちらも小文字です。

- c. Login ボタンをクリックします。ワイヤレスコントローラーの Web 管理インターフェースが表示され、デフォルトのステータス画面が表示されます。

Monitor > Controller > Summary を選択しても表示できます。

The screenshot shows the 'Monitor' tab selected in the top navigation bar. The main content area is divided into several sections:

- Summary** (left sidebar): A list of navigation options including Usage, Access Point, Clients, Neighboring Clients, Rogue AP, Profiles, DHCP Lease, and Captive Portal Users.
- Network Status** (center): A table showing the status of devices.

| Device | Total | | Alarms | |
|---------------|-------|------|----------|-------|
| | Up | Down | Critical | Major |
| Access Points | 0 | 0 | 0 | 2 |
| Clients | 0 | NA | NA | NA |
- Wireless Clients** (center): A table showing the number of clients connected via different security protocols.

| Open | WEP | WPA | WPA2 |
|------|-----|-----|------|
| 0 | 0 | 0 | 0 |
- Rogue Access Points** (center): A table showing the current and 24-hour count of rogue access points.

| | |
|----------------------|---|
| Rogue AP current | 0 |
| Rogue AP count 24hrs | 0 |
- Network Info** (right): A list of system information including Firmware Version (2.1.0.21_Beta_2329), Controller Uptime (14 mins, 4 secs), Last Reboot (Wed Mar 23 03:29:17 2011), Last Configuration Change (Wed Mar 23 03:43:15 2011), Last Channel Allocation (Tue Mar 22 08:24:08 2011), and Last Admin Login (Wed Mar 23 03:29:42 2011).
- Redundancy Status** (right): A list of redundancy settings including Controller Mode (Primary), Redundancy State (Active), Secondary Status (Not Reachable), Sync Status (Not in Sync), Primary IP Address (192.168.0.250), Secondary IP Address (192.168.0.240), and Virtual IP (192.168.0.255).

メモ: スタック構成時のみ Monitor main navigation タブ選択時に Network Navigation menu タブが表示されます。

基本および拡張設定

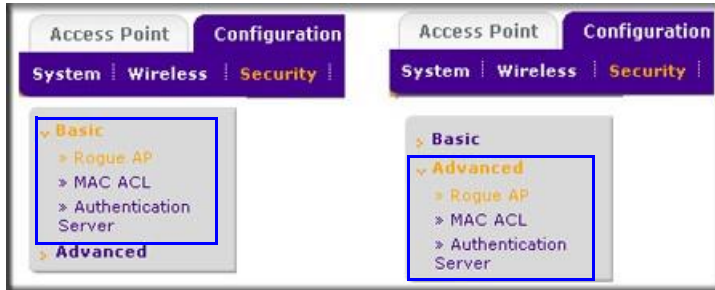
10 台から 20 台のアクセスポイントの小さなワイヤレスネットワークにコントローラーを設置することも、最大 150 台のアクセスポイントの大きなネットワークにコントローラーを設置することも可能です。小さなネットワークは基本的な設定で十分ですが、大きなネットワークは複雑になり、ワイヤレスコントローラーの拡張機能を設定する必要があります。

お使いのネットワーク設定によって基本設定または拡張設定を使ってアクセスポイントを管理します。

- **典型的なネットワークのための基本設定:** 基本設定は大部分のネットワーク設定で動作します。例えば、ワイヤレス LAN のすべてのアクセスポイントは同じ組織や企業向けであるため、同じポリシーに従い、少数のサービスセット (SSID またはネットワーク名) を使用します。
- **アクセスポイントプロファイルグループのための拡張設定:** 大きなワイヤレスネットワークを使用していたり、完全に独立したネットワークが一つのワイヤレス LAN を共有したりしている場合、拡張設定を使って複数のセキュリティプロファイル (SSID と関連するセキュリティ設定) で複数のアクセスポイントプロファイルグループを設定します。例えば、複数の企業が一つのワイヤレス LAN を今日するが、各企業がそれぞれのネットワークを持っている場合に、ショッピングモールは複数のアクセスポイントプロファイルグループを必要とするかもしれません。大きなネットワークはビルや部門単位で異なったポリシーを許可するために、複数のアクセスポイントプロファイルが必要とするでしょう。アクセスポイントはビル単位あるいは部門単位、例えばゲスト用、管理者用、セールス用のように異なるセキュリティプロファイルを持つかもしれません。

メモ: アクセスポイントプロファイルグループはプロファイルグループと呼ばれることもあります。
 プロファイル、セキュリティプロファイル、および SSID (SSID と関連するセキュリティ設定) は相互に交換可能な用語です。

すべてのタイプのネットワークに対応するために、Web 管理インターフェースのほとんどすべての設定メニューは **Basic** (基本) と **Advanced** (拡張) メニューに分けられています。以下の図は **Security > Wireless > Basic** メニュー (左) と **Security > Wireless > Advanced** メニュー (右) を示しています。



ワイヤレスコントローラーの設定を始める前に、基本設定を使うか拡張設定を使う必要があるかを決めます。決定をした後には、一貫して基本 (Basic) メニューあるいは拡張 (Advanced) メニューにしたがって設定をすれば容易にワイヤレスコントローラーの設定ができます。

プロファイルグループ

各アクセスポイントは最大 8 つのセキュリティプロファイル (デュアルバンドアクセスポイントでは 16 個) をサポートでき、それぞれ SSID、セキュリティ設定、MAC ACL、レートリミット設定、WMM 設定等を持ちます。

ワイヤレスコントローラーは同じアーキテクチャーに従います。ワイヤレスコントローラーの一つのプロファイルグループは個々のアクセスポイントに設定できる最大 8 個のプロファイル (デュアルバンドアクセスポイントでは 16 個) すべての機能 (SSID、セキュリティ設定、MAC ACL、レートリミット設定、WMM 設定等) を含みます。

基本 (Basic) プロファイル

基本プロファイルは 8 つのセキュリティプロファイル (デュアルバンドアクセスポイントでは 16 個) の設定ができます。

自動発見プロセスの後、ワイヤレスコントローラーの管理 AP リストに追加すると、アクセスポイントはデフォルトで基本 (Basic) プロファイルグループに割り当てられます。

もしもお使いのネットワークでワイヤレスコントローラーが異なる設定の複数のアクセスポイントを管理する必要があるなら、拡張 (Advanced) プロファイルを使います。

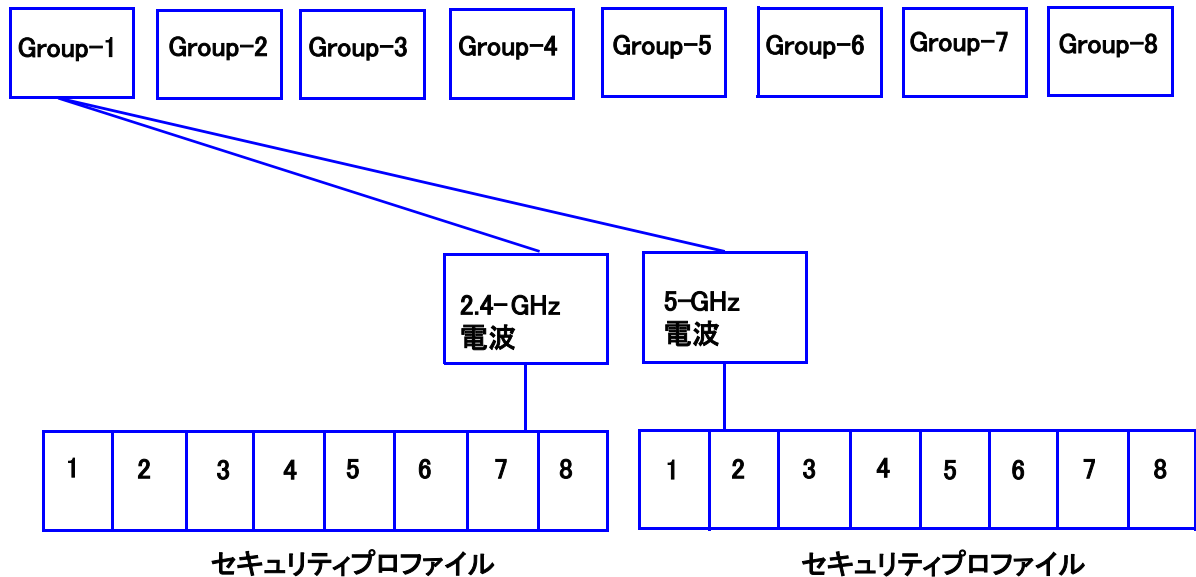
拡張(Advanced)プロファイル

拡張プロファイルでは 8 つのアクセスプロファイルグループを設定できます。各グループは 8 つのセキュリティプロファイル(デュアルバンドアクセスポイントでは 16 個)を設定できます。

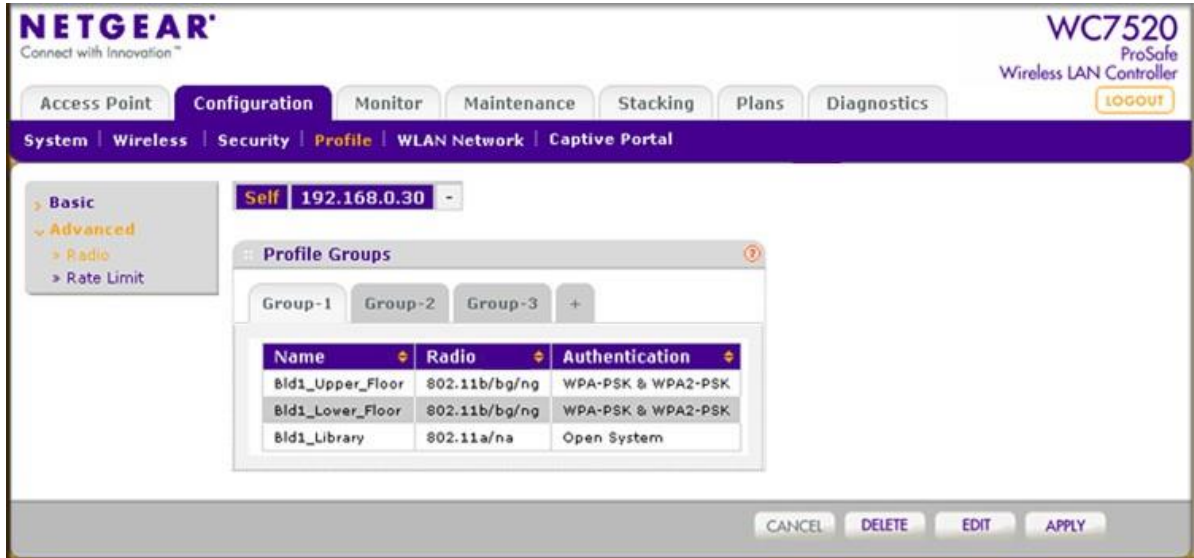
例えば、完全に異なるネットワークを持つ 4 つの会社がある場合、単純に 4 つのプロファイルグループを作成します。次に一つのビル内のすべてのアクセスポイントを一つのプロファイルグループに割り当て、他のビルのすべてのアクセスポイントを 2 つ目のプロファイルグループに割り当てていきます。

それぞれのプロファイルグループでは独立した電波のオンオフスケジュール、電波管理設定、MAC ACL、認証、認証サーバーを作成することができます。一つのプロファイルグループ中の各電波(2.4GHz と 5GHz)では、それぞれ独立した無線設定、WMM、レートリミット設定ができます。

以下の図では拡張(Advanced)プロファイルグループアーキテクチャーを示しています。グループ 1 の下の構造が他のグループ(グループ 2~8)の下にも同様に存在します。



次の図は1つめのプロファイルグループ(Group-1)が3つのセキュリティプロファイルを持つ3つのアクセスポイントプロファイルグループの例です。このプロファイルグループの各プロファイルでは、プロファイル名、ラジオモード、および認証設定が表示されています。(Group-1 が拡張プロファイルグループ設定のデフォルトグループです。他のプロファイルグループは作成する必要がありま



す。)

ワイヤレスコントローラーを設置する場所を選ぶ

ワイヤレスコントローラーはゴム足を使ってオフィス環境で使うのにも適しているし、19インチラックにマウントすることもできます。マウンティングキットがワイヤレスコントローラーに同梱されています。

ワイヤレスコントローラーを設置するには以下の点を考慮してください。

- ワイヤレスコントローラーに容易にアクセスケーブルを接続できること。
- 配線は電気的なノイズ源から離れていること。エレベーター、電子レンジ、空調機器等がノイズ源となります。
- 水分や湿気が機器内に侵入しないこと。
- 機器の周りのエアフローと機器の両側の通気口が塞がれないこと。最低 25mm はあけてください。
- 空気中にホコリがないこと。
- 温度上限を超えることがないこと。空調の効いた場所に設置すること。

ワイヤレスコントローラーの設置

ワイヤレスコントローラーを設置する

1. ワイヤレスコントローラーのコンピューターへの接続を外します。必要ならば設定のために変更したコンピューターの TCP/IP 設定を元に戻します。
2. ワイヤレスコントローラーとネットワークの LAN ポートをイーサネットケーブルでつなぎます。
3. 電源ケーブルをワイヤレスコントローラーにとりつけ、電源コンセントにつなぎます。電源、テストおよびイーサネット LED が点灯するはずです。

2. システム計画と設置シナリオ

システム計画

導入前計画

ワイヤレスコントローラーをインストールする前に以下の点を決定してください。

- シームレスにエリアをカバーするために必要なアクセスポイント数。
- 必要なワイヤレスコントローラー数。
- 最適な Wi-Fi 利用のために 802.11 周波数バンドとチャンネル。サイトサーベイを実施することをおすすめします。
- 現在の電波状況確認と 802.11 および 802.11 以外のノイズ検知のためにサイト(設置場所)でのチャンネルのスペクトル解析の実施。
- アクセスポイントとクライアントの接続性試験を行い、クライアントで達成可能な最大スループットを確認する。
- 電波妨害の可能性と干渉源の特定。
- 利用密度が高い部分での設置密度を高くする部分の特定。

サーベイ完了後、収集したデータを使って電波プラン(RF プラン)を作成します。

ワイヤレスコントローラーを設定する前に

以降のセクションはネットワークに最低一台のワイヤレスコントローラーを設置し、ワイヤレスコントローラーの設定ができる状態であることを前提とします。WC7520 ワイヤレスコントローラーを設置するには、**ワイヤレスコントローラーインストールガイド**を参照してください。

ほとんどの設定では、デフォルトワイヤレス設定を使うことができます。IP アドレス、VLAN、DHCP サーバー、クライアント認証、データ暗号化はお使いの環境により異なります。以下にこれらの設定に関して簡単に記します。

VLAN

管理 VLAN はワイヤレスコントローラーにアクセスするための専用の VLAN です。HTTP,HTTPS,SNMP,SSHトラフィックを含むワイヤレスコントローラーに向かうすべてのトラフィックは管理 VLAN で運ばれます。

管理 VLAN がタグ付き VLAN として設定されている時、ワイヤレスコントローラーから送受信されるパケットは割り当てられた VLAN 番号の 802.1QVLAN ヘッダーを持ちます。管理 VLAN がタグ無しに設定されている時、ワイヤレスコントローラーから送信されるパケットは 802.1Q ヘッダーを持た

ず、ワイヤレスコントローラーに送信されるすべてのタグ無しパケットは管理 VLAN トラフィックとして扱われます。

メモ: お使いの LAN のスイッチやハブが 802.1Q をサポートしている時のみタグ付き VLAN あるいはタグ VLAN ID を変更してください。802.1Q をサポートしていない場合やスイッチやハブと同じ VLAN ID を設定しない場合、IP 接続性が失われることがあります。

ワイヤレスコントローラーは管理 VLAN を介してアクセスポイントと IP 接続性が必要です。もしもワイヤレスコントローラーとアクセスポイントが異なる管理 VLAN 上に存在する場合、ワイヤレスコントローラーとアクセスポイントの IP 接続性を確保するために VLAN ルーティングが必要となります。

クライアント VLAN

認証されたそれぞれのワイヤレスユーザーはユーザーの DHCP サーバー、IP アドレス、レイヤー2 接続を決定する VLAN に割り当てられます。すべての認証されたワイヤレスユーザーを基本セキュリティプロファイルに定義された一つの VLAN に割り当てることも可能ですが、ワイヤレスコントローラーはネットワーク資源へのアクセスを区別するための SSID に基づいた異なる VLAN にワイヤレスユーザーをグループ化すること可能にします。例えば、認証された社員ユーザーを一つの VLAN に割り当て、契約社員やお客様のような一時的なユーザーを別の VLAN に割り当てます。異なる VLAN を使うためには、異なるセキュリティプロファイルを作成する必要があります。

DHCP サーバー

ワイヤレスコントローラーは DHCP として動作することができ、ワイヤレスと優先のどちらに接続されているデバイスに対して IP アドレスを割り当てることができます。異なる VLAN に対して最大 64 の DHCP サーバープールを追加することができます。

クライアント認証とデータ暗号化

ワイヤレス LAN 資源にアクセスするためにはユーザーはワイヤレス LAN に認証される必要があります。ワイヤレスコントローラーは外部の RADIUS や LDAP 認証サーバーを必要とするようなものを含む様々なセキュリティ方式のタイプをサポートしています。

選択できる暗号化オプションは選択した認証方式に依存します。以下に利用可能な認証方式とそれに対応する暗号化オプションを記します。

認証と暗号化オプション

| 認証方式 | 暗号化オプション | 認証サーバー |
|-------------|------------------------------|--------|
| Open system | 64-bit, 128-bit, 152-bit WEP | 無し |

| | | |
|----------------------|------------------------------|--|
| 共有キー | 64-bit, 128-bit, 152-bit WEP | 無し |
| WPA-PSK | TKIP または TKIP+AES | 無し |
| WPA2-PSK | AES または TKIP+AES | 無し |
| WPA-PSK および WPA2-PSK | TKIP+AES | 無し |
| WPA | TKIP または TKIP+AES | 以下の認証サーバーの中の一つ <ul style="list-style-type: none"> 外部 RADIUS サーバー 内部の認証サーバー 外部の LDAP サーバー |
| WPA2 | AES または TKIP+AES | 以下の認証サーバーの中の一つ <ul style="list-style-type: none"> 外部 RADIUS サーバー 内部の認証サーバー 外部の LDAP サーバー |
| WPA および WPA2 | TKIP+AES | 以下の認証サーバーの中の一つ <ul style="list-style-type: none"> 外部 RADIUS サーバー 内部の認証サーバー 外部の LDAP サーバー |

基本プロファイルグループのシングルコントローラー構成

基本設定は基本デフォルトグループで管理されるアクセスポイントを管理する一台のワイヤレスコントローラーからなります。

基本プロファイルグループのシングルワイヤレスコントローラーシステムを設定する

| ステップ | 設定 | Web 管理インターフェースパス |
|------|---|----------------------------------|
| 1. | オプション: 電波プラン作成 | Plans > Layout |
| 2. | (未完了の場合)ワイヤレスコントローラーのシステム設定 | |
| | 1.カントリーコード設定 | Configuration > System > General |
| | 2.ワイヤレスコントローラーの IP アドレス設定 3.VLAN 1 が管理 VLAN に設定されていて、タグ無し設定であることを確認(デフォルト設定) | Configuration > System > IP/VLAN |
| 3. | 最大 8 つのプロファイル設定。最低限以下を実施。 | |
| | 1.ワイヤレスアクセス用の SSID 設定。 | Configuration > Profile > Basic |

| | | |
|----|--|--|
| | 2.ネットワーク認証とデータ暗号化設定。 | |
| | 3.VLAN 割り当て。 | |
| | 必要ならば認証サーバー設定。 | Configuration > Security > Basic > Authentication Server |
| 4. | Discovery Wizard を実行してアクセスポイントを Managed Access Point List に追加する。 | Access Point > Discovery Wizard |

拡張プロファイルグループのシングルコントローラー構成

より複雑な設定は、アクセスポイントプロファイルグループで管理される 1 台のワイヤレスコントローラーからなり、各アクセスポイントプロファイルグループでいくつかのプロファイルを使うかもしれません。

拡張プロファイルグループのシングルワイヤレスコントローラーシステムを設定する

| ステップ | 設定 | Web 管理インターフェースパス |
|------|--|--|
| 1. | オプション: 電波プラン作成 | Plans > Layout |
| | (未完了の場合)ワイヤレスコントローラーのシステム設定 | |
| 2. | 1.カントリーコード設定 | Configuration > System > General |
| | 2.ワイヤレスコントローラーの IP アドレス設定 | Configuration > System > IP/VLAN |
| | 3.VLAN 1 が管理 VLAN に設定されていて、タグ無し設定であることを確認(デフォルト設定) | |
| | 最大 8 つのプロファイル設定。最低限以下を実施。 | |
| 3. | 1.ワイヤレスアクセス用の SSID 設定。 | Configuration > Profile > Basic |
| | 2.ネットワーク認証とデータ暗号化設定。 | |
| | 3.VLAN 割り当て。 | |
| | 必要ならば認証サーバー設定。 | Configuration > Security > Basic > Authentication Server |
| 4. | Discovery Wizard を実行してアクセスポイントを Managed Access Point List に追加する。 | Access Point > Discovery Wizard |

| | | |
|----|---|------------------------------|
| 5. | アクセスポイントをアクセスポイントプロファイルグループ(WLAN グループと呼ぶこともあります)へ割り当てます。A | Configuration > WLAN Network |
|----|---|------------------------------|

スタックコントローラー構成

スタックコントローラー構成は 3 台までのワイヤレスコントローラーで 150 台までのアクセスポイントを管理できます。

スタックコントローラー構成を設定する

| ステップ | 設定 | Web 管理インターフェースパス |
|------|--|---------------------|
| 1. | スタックメンバーにするそれぞれのワイヤレスコントローラーで前のセクションの手順に従い設定をします。 メモ: もしもスタックメンバーが別のフロアや別のビルに存在するのならば、各ビル、フロアに対してわかれたアクセスポイントプロファイルグループを設定します。 | 該当するセクション参照 |
| 2. | プライマリー (Primary) ワイヤレスコントローラーを設定しネットワークに設置します。 | |
| 3. | セカンダリー (Secondary) ワイヤレスコントローラーを設定しネットワークに設置します。 | |
| 4. | スタックにするコントローラー間を接続します。接続は有線接続ですが、コントローラー間にルーターやスイッチがあってもよく、直接接続する必要はありません。 | |
| 5. | プライマリー (Primary) コントローラーにするワイヤレスコントローラーでスタッキンググループを設定します。 | Stacking > Stacking |
| 6. | スタックメンバーのすべてのワイヤレスコントローラーを同期 (Synchronize) します。 | |

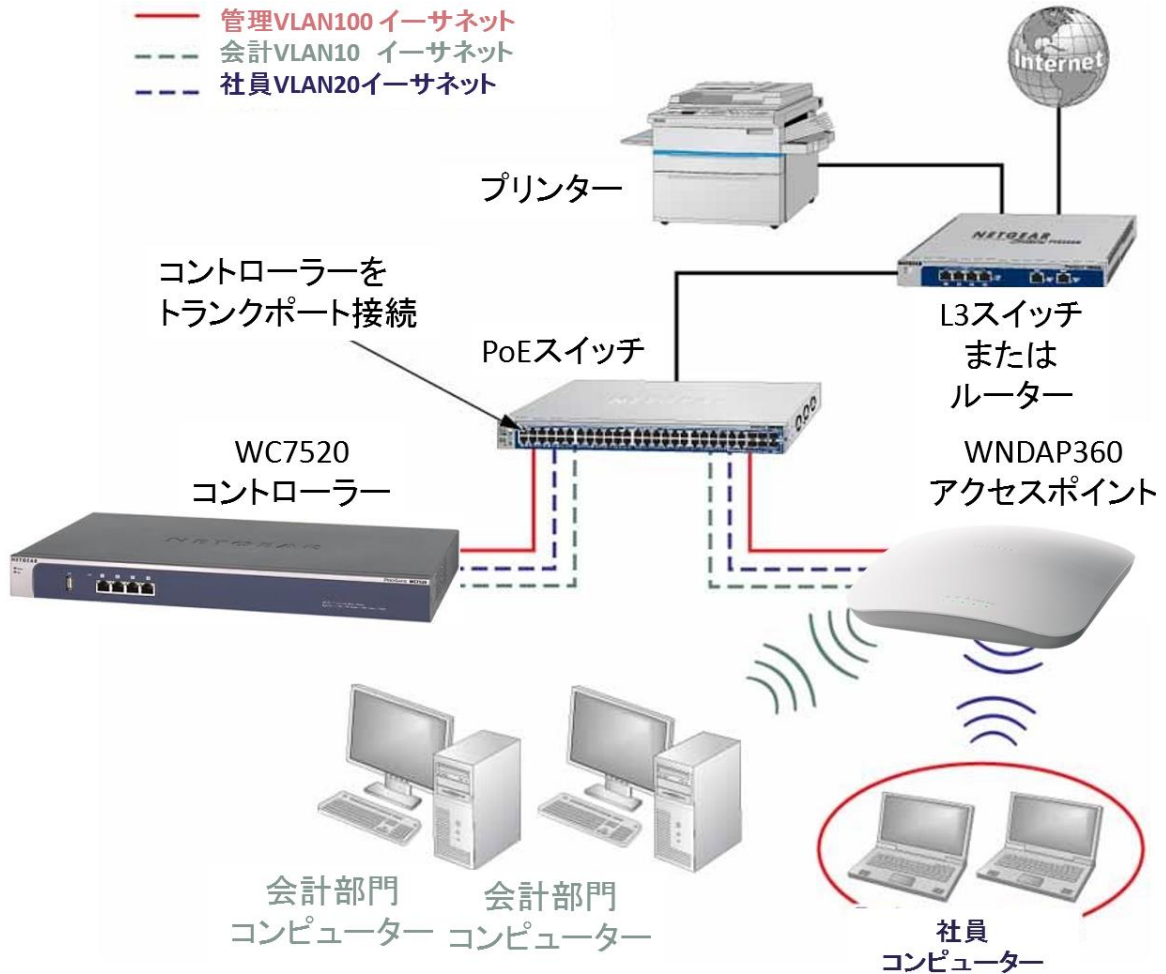
管理 VLAN とデータ VLAN 計画

もしもネットワークが 10 以上のアクセスポイントを含むのであれば、最低でも 2 つの VLAN グループ、管理 VLAN グループとデータ VLAN グループを設定することを推奨します。ネットワークが大きな場合は、複数の VLAN グループを作成すべきです。クライアント用にデータ VLAN を作ることによって、

- ユーザーの種類によってトラフィックを分類できます。

- ユーザーの種類に基づいたアクセスポリシーのような異なるポリシーをサクセスすることができます。

以下に VLAN を使ってユーザーの種類に応じてトラフィックを分類している図を示します。



ワイヤレスコントローラーは管理 VLAN を使ってアクセスポイントと継続的にパケットを交換しています。大きなネットワークですべてのトラフィックが一つの VLAN を使っていると、クライアントトラフィックがネットワークを溢れさせる可能性があります。こういう事態になり、コントローラーがアクセスポイントとパケットを交換できなくなると、ネットワークパフォーマンスが低下し、アクセスポイントはワイヤレスコントローラーと接続を失います。

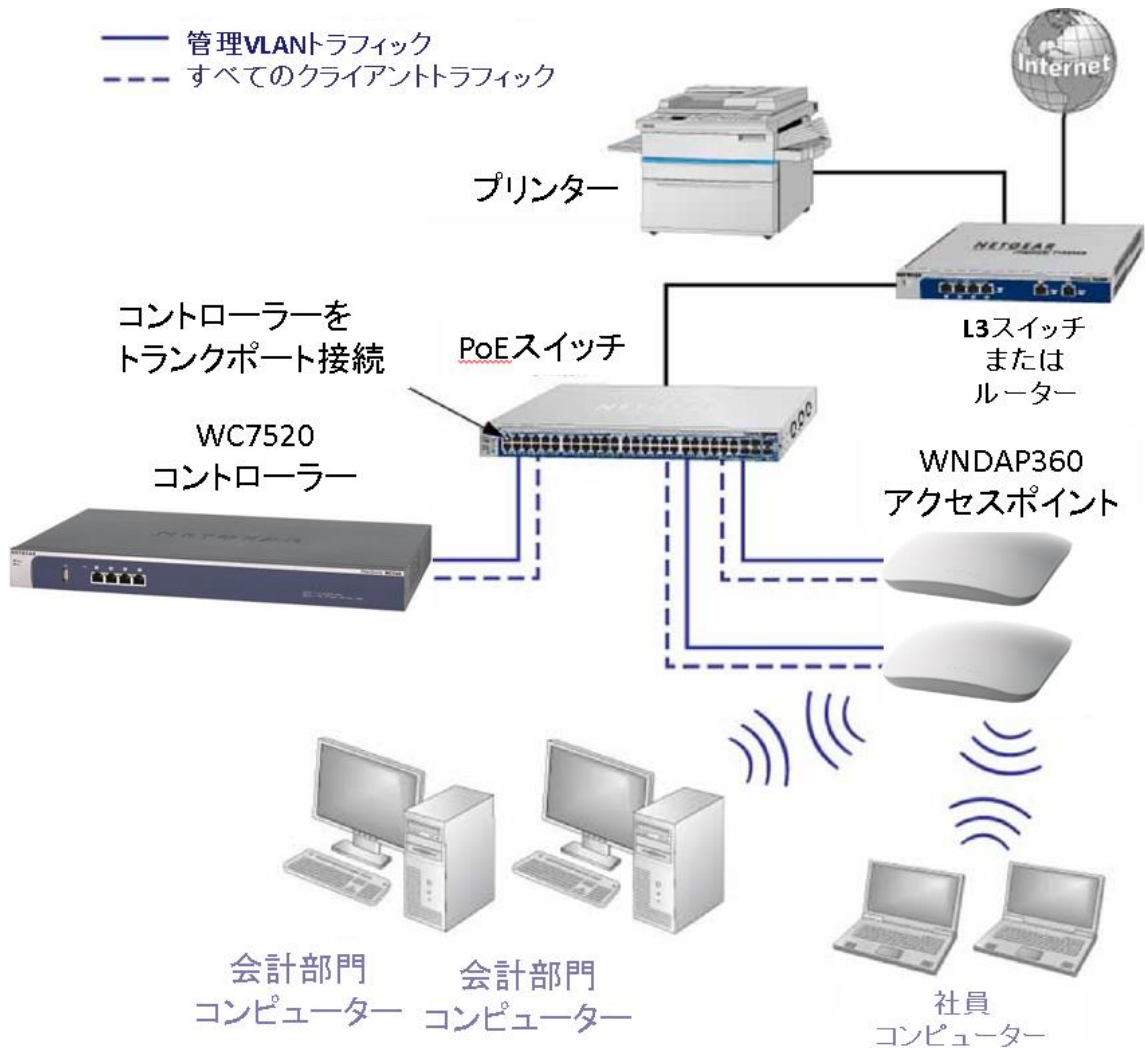
スイッチのトランクポートにワイヤレスコントローラーを接続すべきです。トランクポートはすべての VLAN にアクセスできるようにします。トランクのトラフィックを収容できるようにスイッチのできるだけ高速なポートを使います。

導入シナリオ

このセクションでは様々なネットワーク構成でワイヤレスコントローラーがどのように機能するかを示す 3 つの導入シナリオを提供します。

- シナリオ 1: 一つの VLAN の基本ネットワーク
- シナリオ 2: 複数の VLAN と SSID の拡張ネットワーク
- シナリオ 3: 冗長化の拡張ネットワーク

シナリオ 1: 一つの VLAN の基本ネットワーク



以下のシナリオはワイヤレスコントローラー、PoE スイッチ、L3 スイッチまたはルーターとアクセスポイントのシンプルなネットワーク例です。

アクセスポイントとワイヤレスコントローラーは同じサブネットで接続され、サブネットに割り当てられた同じ IP アドレス範囲を使います。ワイヤレスコントローラーとアクセスポイントの間にはルーターは存在しません。アクセスポイントは PoE スイッチに接続され、PoE スイッチはワイヤレスコントローラーに接続されています。PoE スイッチの上位にはインターネットアクセスを提供する L3 スイッチあるいはルーターが接続されています。

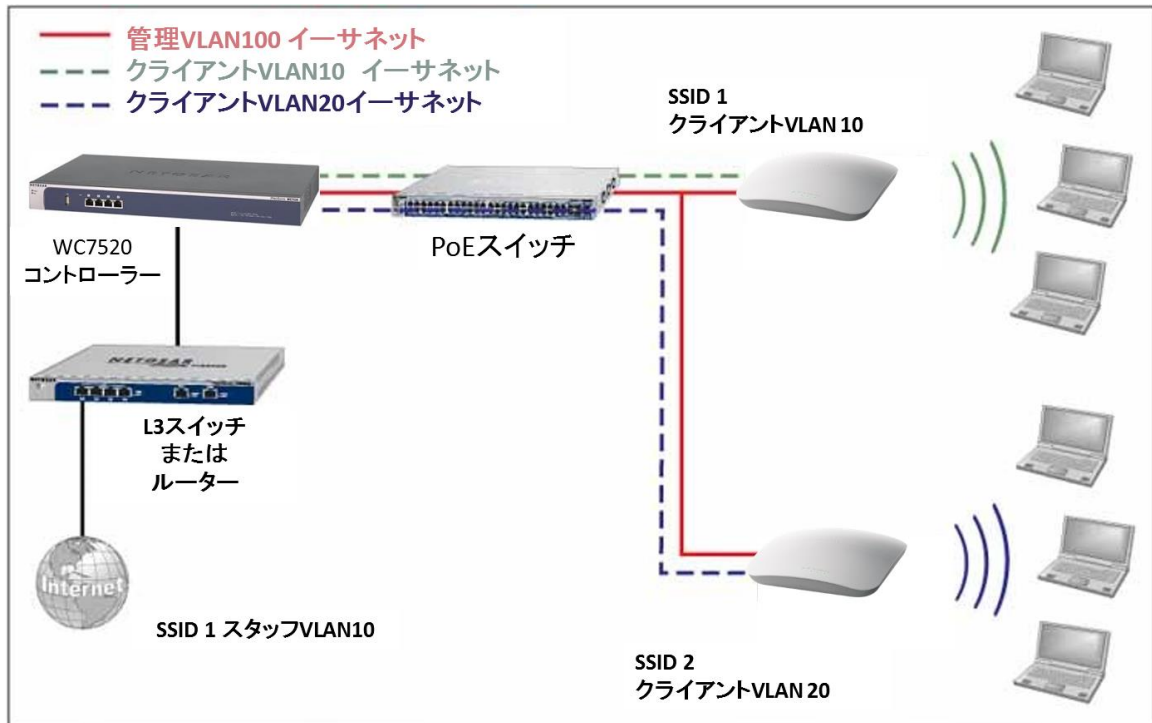
ワイヤレスコントローラーのプロビジョニング

| ステップ | 設定 | Web 管理インターフェースパス |
|------|---|----------------------------------|
| 1. | 基本システム設定をします。 | |
| | 1.カントリーコード設定をします。 | Configuration > System > General |
| | 2.ワイヤレスコントローラーの IP アドレス設定をします。 3.VLAN 1 が管理 VLAN に設定されていて、タグ無し設定であることを確認します(デフォルト設定)。 | Configuration > System > IP/VLAN |
| 2. | 基本ワイヤレスとセキュリティを設定します。 | |
| | 1.ワイヤレスアクセス用の SSID を設定します。 | Configuration > Profile > Basic |
| | 2.ネットワーク認証とデータ暗号化を設定します。 3.暗号化を設定します。 | |
| 3. | ワイヤレスコントローラーのイーサネットポートの一つを PoE スイッチのポートに接続します。 | |
| 4. | アクセスポイントを設置し、PoE スイッチに接続します。 | |
| 5. | Discovery Wizard を実行し、ネットワークレイアウトを選択し、ワイヤレスコントローラーで管理したいアクセスポイントを選択します。 メモ: デフォルトではすべてのアクセスポイントは基本グループに追加され、基本グループの基本設定(プロファイル定義、クライアント認証、認証設定とワイヤレス QoS)がアクセスポイントに適用されません。 | Access Point > Discovery Wizard |

シナリオ 2: 複数の VLAN と SSID の拡張ネットワーク

以下のシナリオはワイヤレスコントローラー、PoE スイッチ、L3 スイッチまたはルーターとアクセスポイント、複数の VLAN と SSID の拡張ネットワーク例です。以下の VLAN がワイヤレスコントローラーシステムに定義されています。

- VLAN 1: ワイヤレスコントローラーにアクセスするデフォルト、タグ無し VLAN
- VLAN 10: タグ付きのクライアント VLAN
- VLAN 20: 他のタグ付きクライアント VLAN
- VLAN 100: タグ付き管理 VLAN



アクセスポイントとワイヤレスコントローラーは同じサブネットと同じ VLAN で接続され、サブネットに割り当てられた同じ IP アドレス範囲を使います。ワイヤレスコントローラーとアクセスポイントの間にはルーターは存在しません。アクセスポイントは PoE スイッチに接続され、PoE スイッチはワイヤレスコントローラーに接続されています。PoE スイッチの上位にはインターネットアクセスを提供する L3 スイッチあるいはルーターが接続されています。

前提条件

このネットワーク構成は以下の前提条件があります。

- VLAN 10,20,100 はタグ付き VLAN でワイヤレスコントローラーと PoE スイッチに設定してあります。
- ワイヤレスコントローラーは PoE スイッチにデフォルト VLAN 1 に接続されています。コンピューターから PoE スイッチを通して VLAN 1 経由でワイヤレスコントローラーを管理します。
- ワイヤレスコントローラーの DHCP サーバーは管理 VLAN100で設定され、アクセスポイントは VLAN100 経由で IP アドレスを取得します。
- ワイヤレスコントローラーが接続されている PoE スイッチのポートはタグ付きポートとして設定され、VLAN100 からのタグ付きトラフィックを受信します。

ワイヤレスコントローラーのプロビジョニング

| ステップ | 設定 | Web 管理インターフェースパス |
|------|--|--------------------------------------|
| 1. | 初回のアクセスポイントの発見と設定のために、一時的に管理 VLAN100 をワイヤレスコントローラーと PoE スイッチでタグ無し管理 VLAN として設定します。 | Configuration > System > IP/VLAN |
| 2. | 基本システム設定をします。 | |
| | 1.カントリーコード設定をします。 | Configuration > System > General |
| | 2.ワイヤレスコントローラーの IP アドレス設定をします。 | Configuration > System > IP/VLAN |
| | 3.管理 VLAN を VLAN100 として設定します。 | |
| | 4. Untagged Vlan チェックボックスの選択を外します。この変更で VLAN1 がタグ付き VLAN となります。 | |
| 3. | VLAN100 に DHCP サーバーを追加します。 | |
| | 1.VLAN100 の IP アドレスレンジを設定します。 | Configuration > System > DHCP Server |
| | 2.DHCP サーバー設定の他の部分(ゲートウェイ、DNS サーバー等)を設定します。 | |
| 4. | 以下のプロファイルについてネットワーク認証、データ暗号化を設定します。 | |
| | 1.SSID 1 と VLAN 10 のプロファイル。 | Configuration > Profile > Basic |
| | 2. SSID 2 と VLAN 20 のプロファイル。 | |
| 5. | ワイヤレスコントローラーを PoE スイッチに接続します。 | |
| 6. | アクセスポイントを PoE スイッチに接続する前に、接続するスイッチのポートが管理 VLAN 100 に接続できるポートであることを確認します。 | |
| 7. | アクセスポイントを設置し、PoE スイッチのポートに接続します。 | |

| | | |
|-----|--|---------------------------------|
| 8. | <p>アクセスポイントが起動するのを待って、Discovery Wizard を Same L2 network ラジオボタンを選択して実行し、ワイヤレスアクセスポイントで管理したいアクセスポイントを選択します。</p> <p>メモ:アクセスポイントを Managed List に追加することによって、管理 VLAN100 経由で DHCP サーバーから IP アドレスを受信できるようになります。</p> | Access Point > Discovery Wizard |
| 9. | <p>Managed List 中のそれぞれのアクセスポイントについて、Untagged Vlan チェックボックスをはずし、VLAN 100 を管理 VLAN に設定します。この設定によってアクセスポイントはコントローラーとの接続を失います。</p> | |
| 10. | <p>アクセスポイントが接続されている PoE スイッチのポートをタグ付きのポートに変更することによってワイヤレスコントローラーとワイヤレスコントローラーの接続を回復します。(発見の過程でスイッチのポートは管理 VLAN 100 のアクセスポートになっていました。)</p> | |

シナリオ 3: 冗長化の拡張ネットワーク

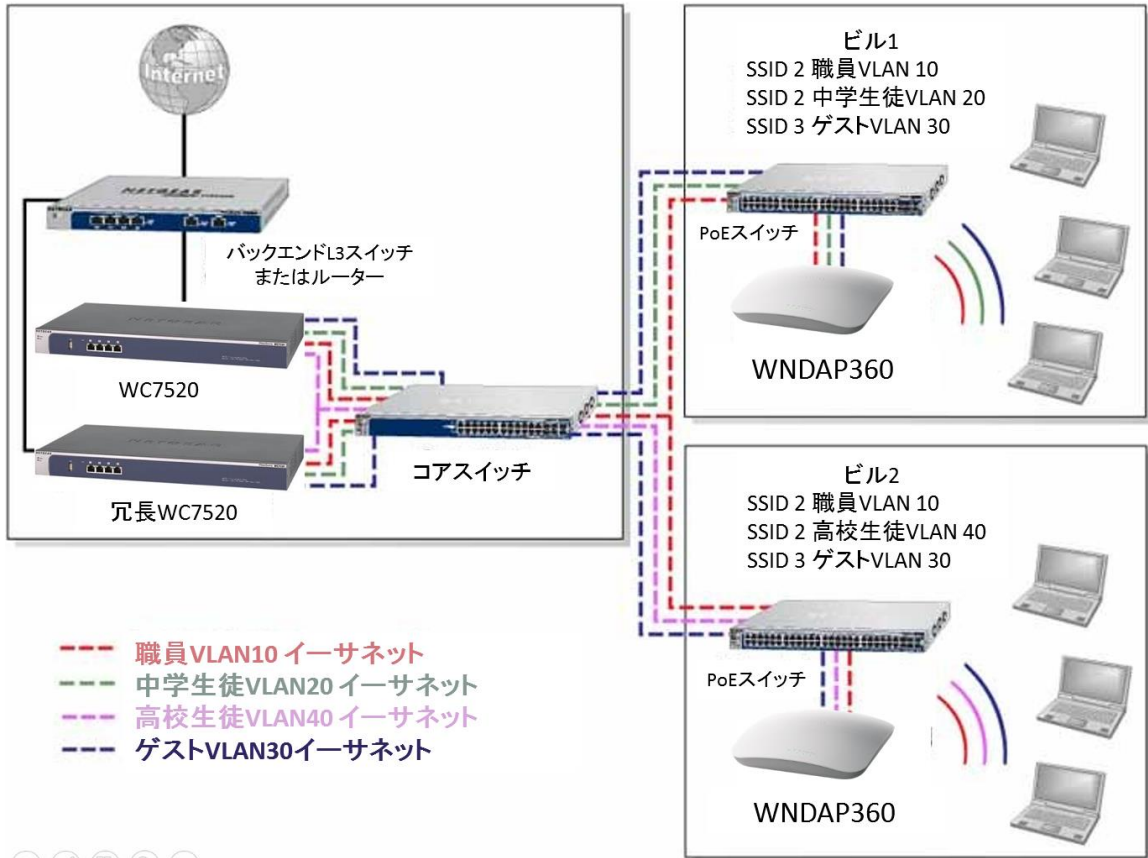
以下のシナリオは 1 台のワイヤレスコントローラー、1 台の冗長ワイヤレスコントローラー、1 台のコアスイッチ、異なるビルにある 2 台の PoE スイッチ、アクセスポイント、複数の VLAN と SSID の拡張ネットワーク例です。以下の要素がワイヤレスコントローラーシステムに定義されています。

- 1 台のワイヤレスコントローラー
- 50 台のアクセスポイント(管理 VLAN1 経由でワイヤレスコントローラーに管理されている)
- 1 台の冗長ワイヤレスコントローラー
- 4 つの VLAN: VLAN 10, VLAN 20, VLAN 30, VLAN 40
- 3 つの SSID: SSID 1, SSID 2, SSID 3

このシナリオでは、VLAN と SSID は学校の異なるユーザーグループを収容するために使われ、2 つのビルに分散されています。

- ビル 1:
 - 職員トラフィック用の VLAN 10 内の SSID 1
 - 中学生徒用の VLAN 20 内の SSID 2
 - ゲスト用の VLAN 30 内の SSID 3
- ビル 2:
 - 職員トラフィック用の VLAN 10 内の SSID 1
 - 高校生徒用の VLAN 40 内の SSID 2

- ゲスト用の VLAN 30 内の SSID 3



アクセスポイントとワイヤレスコントローラーは同じサブネットと同じ VLAN で接続され、サブネットに割り当てられた同じ IP アドレス範囲を使います。コアスイッチはワイヤレスコントローラーとアクセスポイントが接続されている PoE スイッチの間に接続されています。コアスイッチはインターネットアクセスを提供しています。

前提条件

このネットワーク構成には以下の前提条件があります。

- VLAN 1 はワイヤレスコントローラー、コアスイッチ、PoE スイッチに設定されています。この VLAN はタグ無しです。
- VLAN 10,20,30 はワイヤレスコントローラー、コアスイッチ、ビル1の PoE スイッチに設定されています。これらの VLAN はタグ付きです。
- VLAN 1,10,20,30,40 はワイヤレスコントローラー、コアスイッチ、PoE スイッチに設定されています。VLAN 1 以外はタグ付きです。

ワイヤレスコントローラーのプロビジョニング

| ステップ | 設定 | Web 管理インターフェースパス |
|------|---|------------------------------------|
| 1. | 基本システム設定をします。 | |
| | 1.カントリーコード設定をします。 | Configuration > System > General |
| | 2.ワイヤレスコントローラーの IP アドレス設定をします。 | Configuration > System > IP/VLAN |
| | 3.VLAN 1 が管理 VLAN に設定されていて、タグ無し設定であることを確認します(デフォルト設定)。 | |
| 2. | 以下のプロファイルについてネットワーク認証、データ暗号化を設定します。 | |
| | 1.SSID 1 と VLAN 10 のプロファイル。 | Configuration > Profile > Basic |
| | 2.SSID 2 と VLAN 20 のプロファイル。 | |
| | 3.SSID 2 と VLAN 40 のプロファイル | |
| | 4.SSID 3 と VLAN 30 のプロファイル | |
| | | |
| 3. | 以下のプロファイルグループを設定します。 | |
| | 1.Building 1 という名前のプロファイルグループに以下のプロファイルを追加します。 - SSID 1 と VLAN 10 のプロファイル - SSID 2 と VLAN 20 のプロファイル - SSID 3 と VLAN 30 のプロファイル | Configuration > Profile > Advanced |
| | 2. Building 2 という名前のプロファイルグループに以下のプロファイルを追加します。 - SSID 1 と VLAN 10 のプロファイル - SSID 2 と VLAN 40 のプロファイル - SSID 3 と VLAN 30 のプロファイル | |
| 4. | アクセスポイントを設置し PoE スイッチに接続します。 | |
| 5. | アクセスポイントが起動するのを待って、Discovery Wizard を Same L2 network ラジオボタンを選択して実行し、ワイヤレスアクセスポイントで管理したいアクセスポイントを選択します。 | Access Point > Discovery Wizard |
| 7. | アクセスポイントをアクセスポイントプロファイルグループ(WLAN グループ)に割り当てます。 | Configuration > WLAN Network |

3. 電波計画

電波計画の概要

電波計画によって以下の事ができます。

- 無線 LAN カバレッジの定義。
- 信号品質とアクセスポイント 1 台あたりのクライアント数から必要なアクセスポイント数の推定。
- 最善のカバレッジのためのアクセスポイント設置場所の最適化。
- 設置計画のための無線 LAN カバレッジ、不正アクセスポイント、ブラックリストのユーザーの監視。
- カバレッジホールから電波の弱い場所やデッドスポットを特定し、症状を軽減するためにアクセスポイントを追加します。

電波計画はどのように Wi-Fi カバレッジが提供されるかを定義できるように、各フロアの展望を提供します。また、カバレッジマップやアクセスポイント設置場所を提供します。リアルタイムキャリブレーションは電波の弱い部分やデッドスポットを特定し、それらを軽減するためにアクセスポイントを最適な場所に追加ことを可能にします。

計画要件

計画をはかどらせるために、電波計画の前に以下の情報を収集します。

- ビルの寸法
- フロア数
- フロア間の距離
- 総ユーザー数と 1 台のアクセスポイントあたりのユーザー数
- 電波のタイプ
- アクセスポイントに必要なデータ速度
- カバーしたくないエリアの特定
- アクセスポイントを設置できないエリアの特定

以下のようなワークシートを使って情報を収集します。

ビル計画ワークシート

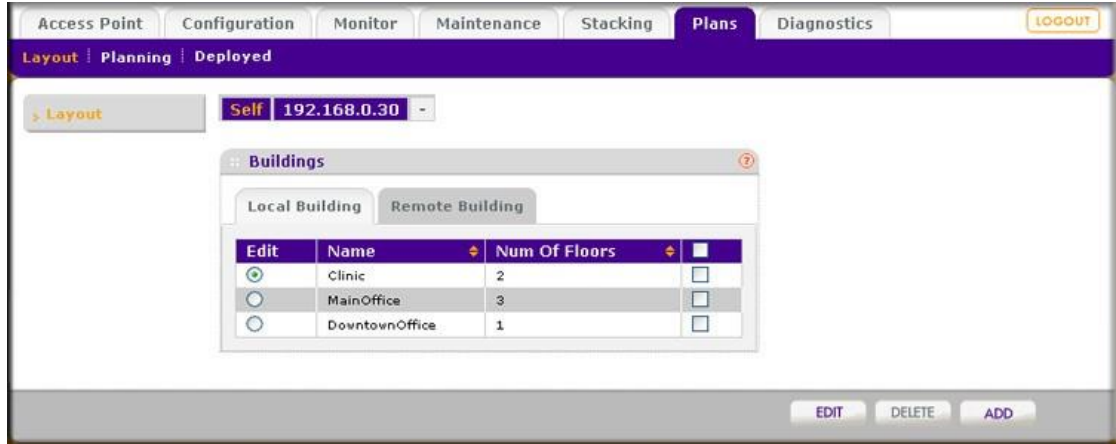
| ビル寸法 | |
|-------------------|--|
| 高さ | |
| 幅・奥行き | |
| フロア数 | |
| ユーザー情報 | |
| ユーザー数 | |
| アクセスポイントあたりのユーザー数 | |
| 電波タイプ | |
| アクセスポイントに必要な信号速度 | |
| 802.11b/bg/ng | |
| 802.11a/na | |
| 対応不要箇所 | |
| | |
| | |
| | |

ビルとフロアの定義と編集

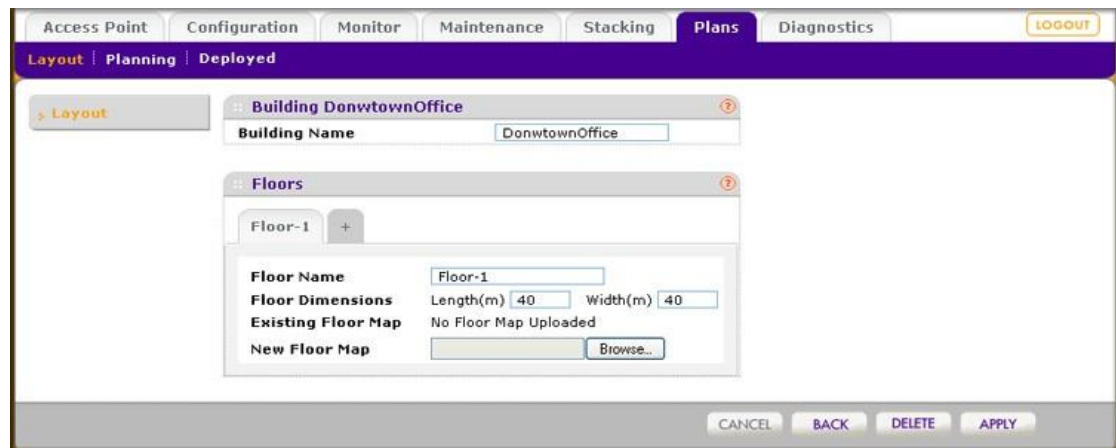
このセクションではどのようにしてビルとフロアを定義し、定義したあとの変更する方法について説明します。ローカルに3つのビル、リモートに3つ、合計で6つのビルを追加できます。

ビルを定義する

1. **Plans > Layout** を選択します。Local Building タブの Buildings レイアウト画面が表示されます。リモートビルを定義するには Remote Building タブをクリックします。



- Buildings テーブルは以前定義したビルの名前とそれらのフロア数を表示します。
- Building を追加するには、Add ボタンをクリックします。Add Building ポップアップ画面が表示されます。
- Building Name 欄に名前を記入し Add ボタンをクリックします。Building テーブルに新しいビルの名前が追加されます。名前は英数 64 文字まで、スペースを入れることはできません。
- ビルのフロアを定義するには、定義するビルのラジオボタンを選択し、Edit ボタンをクリックします。Floors レイアウト画面が表示されます。



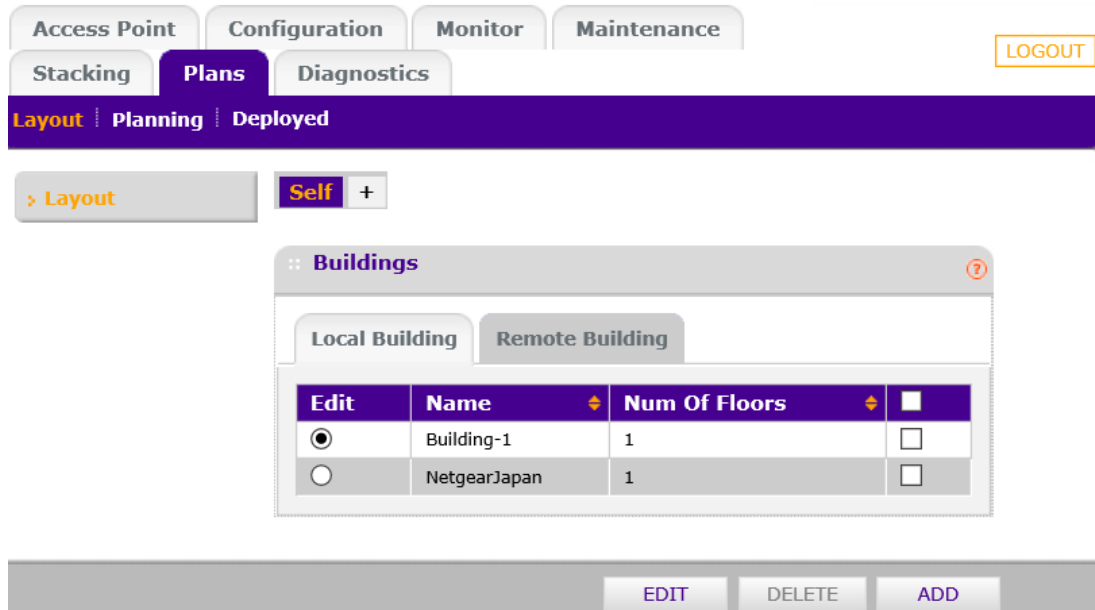
- 以下の表の説明にしたがってフロアを定義します。
ビル名とフロア

| 設定 | 説明 |
|--------------------|---|
| Building | |
| Building Name | 以前定義したビルの名前を変更できます。英数 64 文字まで、スペースを含むことはできません。 |
| Floors | |
| Floor Names | フロアの名前を定義します。英数 64 文字までです。 |
| Floor Dimensions | フロアの寸法を記入します。長さ (Length) と幅 (Width) をメートル単位で記入します。デフォルト値はそれぞれ 40m です。 |
| Existing Floor Map | フロアマップ画像をインポートすると、フロアマップの小さなイメージが表示されます。 Preview ボタンをクリックしてマップを拡大します。(フロアマップをインポートしていない場合、Preview ボタンは表示されません。) |
| New Floor Map | <p>フロアマップファイルをお持ちの場合は、参照 (Browse) ボタンをクリックして RF プランニングツールにマップをインポートすることができます。ブラウザーの指示にしたがってマップをインポートします。</p> <p>メモ: インポートする画像は JPGE 形式で 2048x2048 ピクセル以内ファイルサイズは 1MB 以内である必要があります。</p> <p>メモ: 画像は表示領域に合わせて調整されます。表示領域の比率は Floor Dimensions の比率によって決定されます。</p> <p>メモ: ワイヤレスコントローラーの内部フラッシュメモリーは 3 枚のフロアマップを保存可能です。追加のフロアを定義する場合は、外部 USB ストレージを使用します。</p> <p>メモ: フロアマップ画像はビルを定義する XML ファイルに埋め込まれるため、JPEG ファイルサイズを圧縮して使うことをおすすめします。</p> |

7. フロアを追加するには、フロアタブの横の + ボタンをクリックします。一つのビルで 6 つのフロアまで追加できますが、4 フロア以上を追加するには外部 USB ストレージが必要です。
8. **Apply** ボタンをクリックして設定を保存します。
9. **Back** ボタンをクリックして Layout Buildings 画面に戻ります。

ビルを編集する

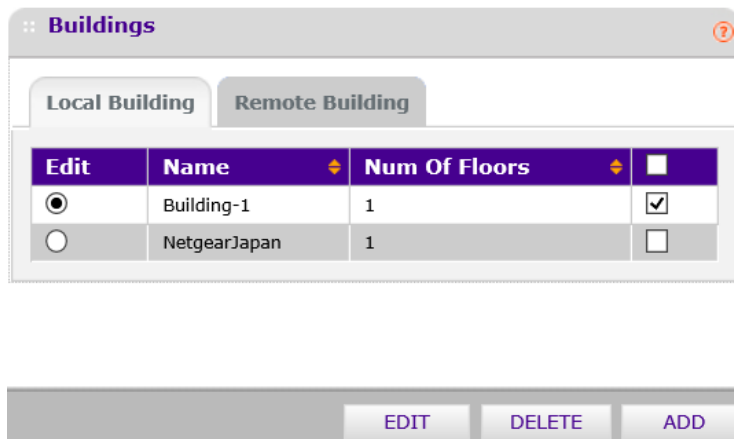
1. 編集をするビルの Edit 欄のラジオボタンを選択します。



2. Edit ボタンをクリックします。

ビルを削除する

1. 削除するビルのチェックボックスを選択するか、表の一番上のチェックボックスをクリックしてすべてのビルを選択します。



2. Delete ボタンをクリックします。

アクセスポイントの要件を特定する

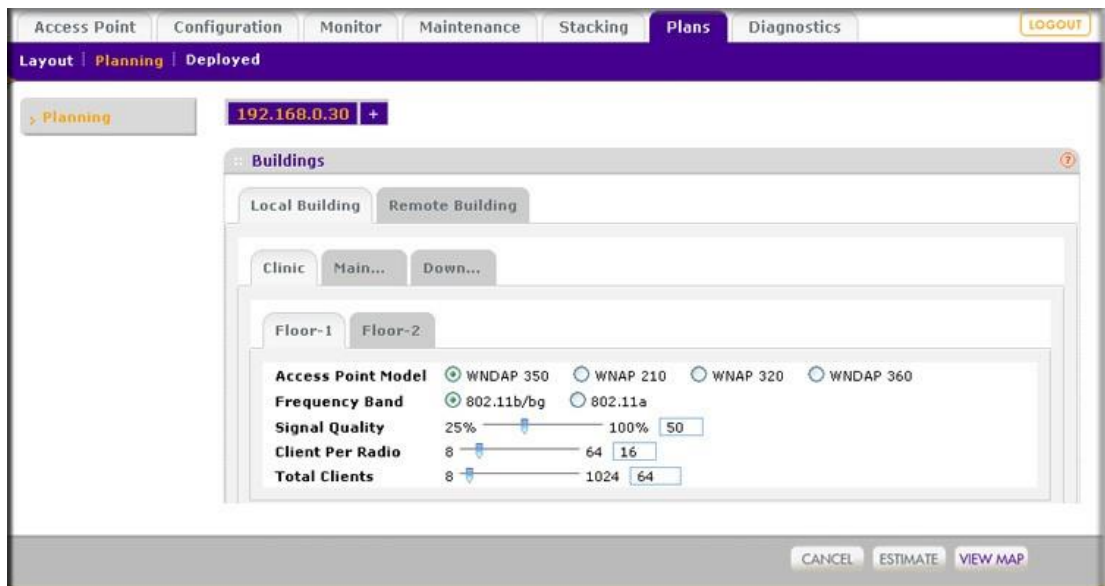
ビルとフロアを定義した後、各フロアおよび各アクセスポイント(WNAP320 と WNDAP360)において以下の RF 要件を特定する必要があります。

- **周波数バンド**: 使う周波数帯 (802.11b/bg/ng あるいは 802.11a/na)
- **信号品質**: 無線 LAN に期待する信号強度。この設定がアクセスポイントの自動チャンネル選択および自動送信出力設定を決定します。
- **アクセスポイントあたりのクライアント数**: 各アクセスポイントでサポートする総クライアント数。
- **フロアの総クライアント数**: 各フロアでサポートする総クライアント数。

フロア寸法とともにこれらの設定が想定アクセスポイント数を決定します。画面で最適なカバレッジのためのアクセスポイントの設置場所をビジュアル的に最適化します。

無線 LAN の要件を特定するために、アクセスポイント数を推測し、推奨設置位置を確認する

1. **Plans > Planning** を選択して Local Building タブとその設定画面を表示します。リモートビル情報は設定するには、**Remote Building** タブをクリックします。



Planning Buildings 画面は既に定義したビルのタブを表示します。各ビルはそれぞれのフロアを表示します。

2. 設定するビルとフロアのタブをクリックして選択します。
3. フロアの無線 LAN 要件を以下の表にしたがって定義します。

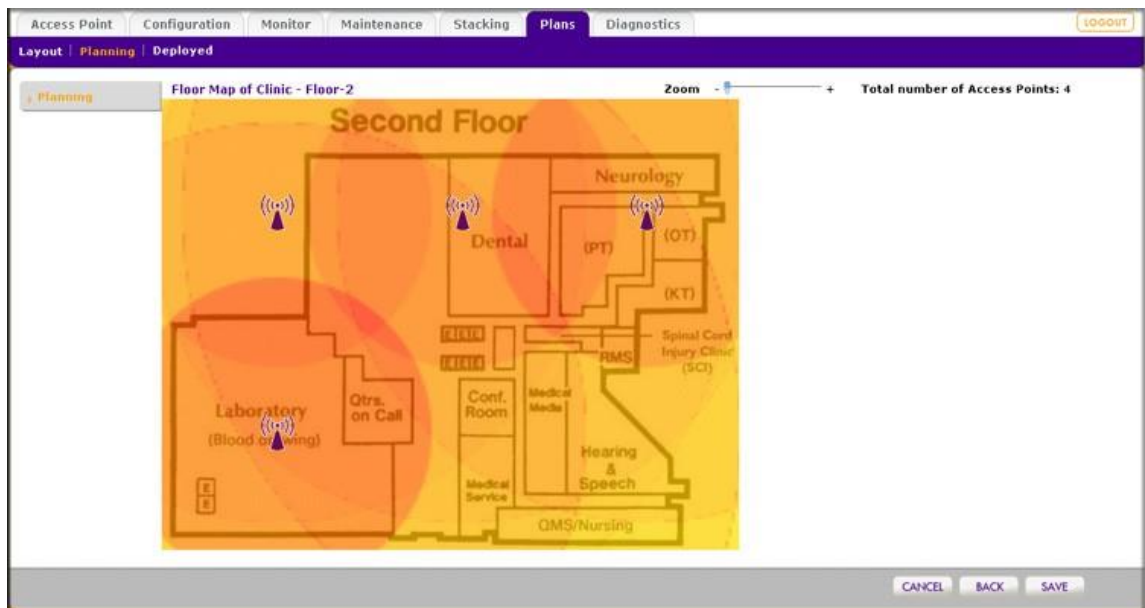
フロア無線 LAN 要件

| 設定 | 説明 |
|--------------------|---|
| Access Point Model | フロアで使用するアクセスポイントのモデル(WNAP320 または WNDAP360)を選択します。(WNAP210 と WNDAP350 は国内では販売していません) |
| Frequency Band | 以下のラジオボタンでアクセスポイントが動作する周波数帯を選択します。 <ul style="list-style-type: none"> • 802.11b/bg/ng • 802.11a/na |
| Signal Quality | スライダーを動かすかパーセント値を入力することによって信号品質要件を指定します。最小は 25%、最大は 100%です。 |
| Client Per Radio | スライダーを動かすか数値を入力することによって周波数帯で何台のアクセスポイントをサポートするかを指定します。最大は 64 です。 |
| Total Clients | スライダーを動かすか数値を入力することによってフロアでの最大クライアント数を指定します。1フロア最大 1024 台です。 |

4. **Estimate** ボタンをクリックして必要なアクセスポイント数を確認します。必要なアクセスポイント数はポップアップウィンドウに表示されます。Sentry Mode (見張りモード) に設定するアクセスポイント数は含まれません。

ポップアップウィンドウを閉じた後に Planning Building 画面に Estimated Access Points 行が追加されて表示されます。

5. **View Map** ボタンをクリックしてアクセスポイントの最適な設置場所を確認します。



プランニングツールはデフォルトの設置位置とそのカバレッジエリアを表示するのみであることに注意してください。

6. 必要なエリアにカバレッジを最適化し、不必要なエリアを避けるようにフロアプランをベースにアクセスポイントを移動します。

アクセスポイントの周りの円形の部分は、各アクセスポイントのおおよそのカバー範囲を示します。円形の色は信号強度を示し、重なった濃い色は近くのアクセスポイントとの信号の重なりを示します。

メモ: 赤い色は-50dBm RSSI 以上の最強の範囲を示します。オレンジは-60 dBm 以上、黄色は-70 dBm 以上をそれぞれ示します。

シームレスローミングのために適度な重なりが必要です。重なりがないと切断やデッドスポットにつながります。

アクセスポイントアイコンをクリックして移動することができます。**Cancel** ボタンをクリックしてアクセスポイントの移動をキャンセルします。

Zoom スライダーを使って画面の解像度を変更します。

7. **Save** ボタンをクリックしてマップを保存します。**Back** ボタンをクリックして変更を保存せずに Panning Buildings 画面に戻ります。

メモ: 各フロアで一つのロケーションマップのみ保存できます。ロケーションマップを変更や保存すると、以前に保存したロケーションマップは上書きされます。

ヒートマップを確認する

ヒートマップでビルフロアでの無線周波数帯、信号強度とワイヤレスカバレッジについてリアルタイムで表示することができます。ヒートマップは近隣のアクセスポイントから検知する実際の信号強度を表示します。

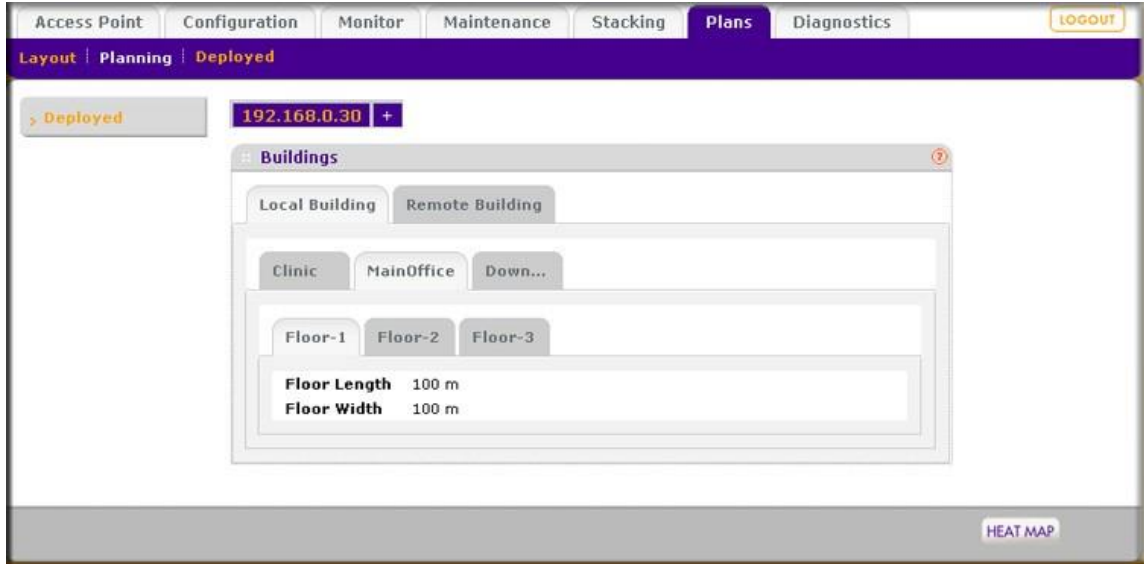
メモ: ヒートマップが正しく動作するために、フロアプランのアクセスポイントの設置位置と実際のアクセスポイントの設置位置はできるだけ一致する必要があります。

ヒートマップは以下の情報を表示します。

- カバレッジホールを含む信号強度と無線カバレッジ
- コントローラーが管理している既知のアクセスポイント
- 不正アクセスポイントの位置
- アクセスポイントに接続しているクライアントの位置
- ブラックリストのクライアントの位置

ヒートマップを表示し、アクセスポイントの設置場所を調整する

1. **Plans > Planning** を選択して Local Building タブとその設定画面を表示します。リモートビルドの情報を設定するには、**Remote Building** タブをクリックします。



Deployed Buildings 画面は設定をしたビルのタブを表示します。

各ビルにおいて定義したフロアを表示します。

2. 表示したいビルとフロアのタブを選択してヒートマップを表示します。

3. **Heat Map** をクリックすると選択したフロアのヒートマップが表示されます。



4. 最初にヒートマップを表示させた時、アクセスポイントの位置を実際の位置に合わせて移動する必要があります。

5. **Apply** ボタンをクリックしてアクセスポイントの位置を保存します。この操作によってフロアの完全なヒートマップを再構成します。

画面上部のスペクトルバーは色と信号強度と無線カバレッジの関係を示します。

ヒートマップ上でアクセスポイントあるいはクライアントの情報を表示するには、ポインターをアイコンの上に移動します。以下の情報が表示されます。

- IP アドレス
- MAC アドレス
- 名前
- モデル
- 状態
- チャンネルごとの電力
- 設定および動作しているチャンネル帯域

他の無線周波数帯を選択するには、Frequency Band ドロップダウンリストで周波数帯を選択します。

Zoom スライダーを使って画像サイズを変更します。

6. アクセスポイントの位置を変更して、無線信号強度とカバレッジをリアルタイムに変更します。
再度 **Apply** ボタンをクリックするまでヒートマップの色は表示されません。新しい位置を適用 (Apply) すると、新しい位置とアクセスポイントから入手する新しい電波情報をもとにヒートマップが更新されます。
7. **Apply** ボタンをクリックして変更のヒートマップへの影響を確認します。無線 LAN のサイズによりヒートマップが更新されるまで数分かかることもあります。変更を適用したくない場合は、**Close** ボタンをクリックして Deployed Building 画面に戻ります。

4. アクセスポイントディスカバリーと管理

アクセスポイントディスカバリーとディスカバリーガイドライン

ワイヤレスコントローラーで Discovery Wizard を実行して LAN または WAN にあるサポートしている NETGEAR アクセスポイントを発見する必要があります。ワイヤレスコントローラーはファクトリーデフォルト状態にあるアクセスポイントや既に設置されて動作しているものを発見することができます。アクセスポイントが発見された後、それらを Managed AP List に追加することができます。ワイヤレスコントローラーは管理されたアクセスポイント(Managed Access Point)を設定、管理、監視することができます。

ローカルアクセスポイントのオートディスカバリー条件

アクセスポイントがまだファクトリーデフォルト設定を持っているならば、オートディスカバリーは問題なく動作するはずですが、アクセスポイントの設定を変更した場合は、設定が以下の一般的なガイドラインに一致しているかを確認してください。

一般的なガイドライン

- すべてのスタンドアロンアクセスポイントは SNMP と SSH が有効である必要があります。
- UDP ポート番号 7890 がファイヤーウォールでブロックされていないこと。
- それぞれのアクセスポイントは IP アドレスを持っていること。同じモデルのすべてのアクセスポイントは同じデフォルト IP アドレスを持っています。複数のアクセスポイントが同じ IP アドレスを持っている場合、その中の1台のみがディスカバリーで発見されます。アクセスポイントを管理アクセスポイントリストに追加し、IP アドレスを変更し、ディスカバリーを再度実行し、同じ IP アドレスの次のアクセスポイントを発見します。
- アクセスポイントは初期出荷ファームウェアまたはそれよりも新しいバージョンのファームウェアで動作している必要があります。アクセスポイントがワイヤレスコントローラーと動作する追加の要件は他にありません。

レイヤー3ネットワークを介してのオートディスカバリー手順のガイドライン

前の一般的なガイドラインに加えて、レイヤー3ネットワークを介してオートディスカバリー手順が動作するために、以下のオプションの一つを有効にしてください。

- ワイヤレスコントローラーとアクセスポイントの間で IP アドレス 254.0.100.250 のマルチキャストルーティング。

- DHCP サーバーで DHCP オプション 43(ベンダー特有情報)。ワイヤレスコントローラーの IP アドレスを 16 進形式で指定し、アクセスポイントにワイヤレスコントローラーの IP アドレスの受信を許可させて、DHCP サーバーがワイヤレスアクセスポイントに IP アドレスを割り当てることができるようにします。16 進のアドレスの前にはベンダー特有の”0204”オクテットを付加します。

アドレス情報を作成するには、”02:04:”で始まって、4 オクテットの 16 進のアドレスを”:”で句切られた形で追加します。

例えば

192.168.33.27 は 16 進で”c0:a8:21:1b”です。ベンダー特有オクテットを追加して、アドレスは”02:04: c0:a8:21:1b”になります。

ワイヤレスコントローラーの DHCP サーバーは自動的に DHCP オプション 43 をワイヤレスコントローラーの IP アドレスで有効にします。

リモートアクセスポイントのオートディスカバリーの条件

ワイヤレスコントローラーはサイト間の VPN や VPN 接続無しのリモートの NAT ルーター介したリモートアクセスポイントをオートディスカバーすることができます。構成が以下の一般的なガイドラインに一致することを確認してください。

リモートアクセスポイントのオートディスカバリー手順のガイドライン

- すべてのスタンドアロンアクセスポイントは SNMP と SSH が有効である必要があります。
- リモートのアクセスポイントがワイヤレスコントローラーと通信できるように、以下のポートがワイヤレスコントローラーの設置されているサイトにおいてファイヤーウォールにブロックされていないこと。
 - TCP ポート 22:トンネルを介したソフトウェアイメージと大きな設定ファイルの転送のために SSH(Secure Shell)と SCP(Secure Copy)で使われます。
 - UDP ポート 69: スタンドアロンアクセスポイントでソフトウェアイメージアップデートのために TFTP で使われます。
 - UDP ポート 123: NTP(Network Time Protocol)で使われます。
 - UDP ポート 138: 名前解決のために NetBIOS で使われます。
 - UDP ポート 161: SNMP 発見プロセスで使われます。
 - ワイヤレスコントローラーとリモートアクセスポイントの間でコントロールチャンネルが使います。
 - UDP ポート 7890: マルチキャストディスカバリーで使われます。リモートアクセスポイントが NAT ルーター配下にある構成の場合にはアンブロックする必要はありません。

DHCP サーバーで DHCP オプション 43(ベンダー特有情報)を有効にします。ワイヤレスコントローラーの IP アドレスを 16 進形式で指定し、アクセスポイントにワイヤレスコントローラーの IP アドレスの受信を許可させて、DHCP サーバーがワイヤレスアクセスポイントに IP アドレスを割り当てることができるようにします。

ワイヤレスコントローラーの DHCP サーバーは自動的に DHCP オプション 43 をワイヤレスコントローラーの IP アドレスで有効にします。

- NAT ルーター配下のアクセスポイントはまず管理されたアクセスポイントに変更され、次に NAT ルーター配下でインストールされます。
- それぞれのアクセスポイントは IP アドレスを持っていること。同じモデルのすべてのアクセスポイントは同じデフォルト IP アドレスを持っています。複数のアクセスポイントが同じ IP アドレスを持っている場合、その中の1台のみがディスカバリーで発見されます。アクセスポイントを管理アクセスポイントリストに追加し、IP アドレスを変更し、ディスカバリーを再度実行し、同じ IP アドレスの次のアクセスポイントを発見します。
- アクセスポイントは初期出荷ファームウェアまたはそれよりも新しいバージョンのファームウェアで動作している必要があります。アクセスポイントがワイヤレスコントローラーと動作する追加の要件は他にありません。

ヒント: 管理と監視のために、一つのサイトのリモートアクセスポイントは同じロケーション名をつけ、意味のあるビルとフロア名を割り当てます。

ディスカバリー後の制限

リモートアクセスポイントが発見 (Discover) された後で以下の制限が適用されます。

- リモートアクセスポイントのクライアントに対してシームレスレイヤー2 ローミングはサポートされますが、リモートアクセスポイント間のシームレスレイヤー3 ローミングはサポートされません。リモートサイトでクライアントがある IP サブネットから別のサブネットに移動するとき、アクセスポイントから切断され、他のアクセスポイントに再接続する必要があります。
- もしもリモートアクセスポイントがワイヤレスコントローラーから切断された時、例えば VPN コネクションが切断された時、以下のことが発生します。
 - リモートアクセスポイントは直近の設定を使ってスタンドアロンアクセスポイントとして動作しながら、継続的にワイヤレスコントローラーと再接続を試みます。
 - アクセスポイントが WPA-PSK, WPA2-PSK, WPA-PSK & WPA2-PSK 認証を使っているならば新しいクライアントを受け付けることを継続します。アクセスポイントがワイヤレスコントローラーのローカルの RADIUS 認証を使っているならば、アクセスポイントは新しいクライアントを受け入れることはできません。
 - アクセスポイントが再起動すると、アクセスポイントは構成を失います。

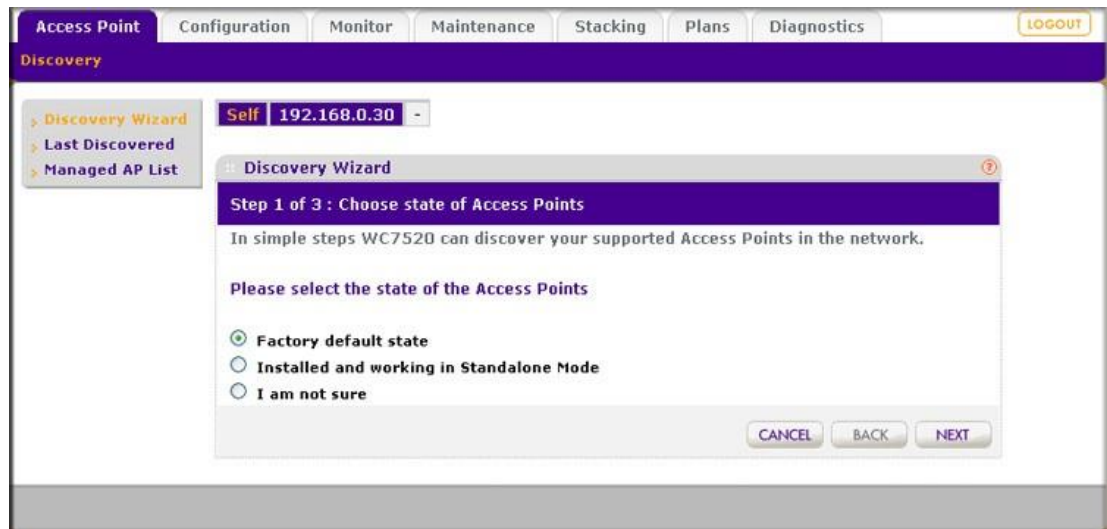
ワイヤレスアクセスポイントとの接続が再確立した後、リモートアクセスポイントは再度管理されたアクセスポイントとして機能します。

Discovery Wizard の実行

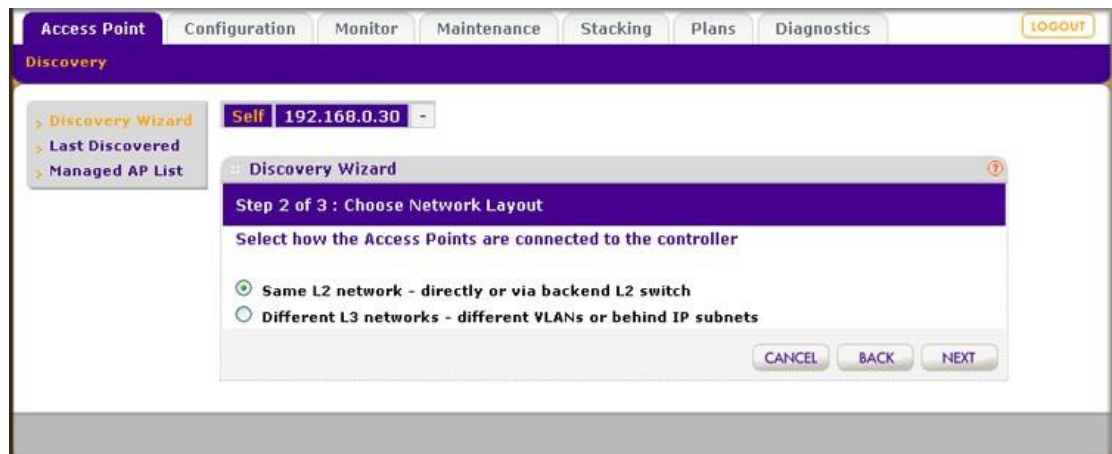
Discovery Wizard は Managed Access Point List に載っていないアクセスポイントを発見します。

Discovery Wizard を実行する

1. **Access Point > Discovery Wizard** を選択して Discovery Wizard 画面を表示します。S

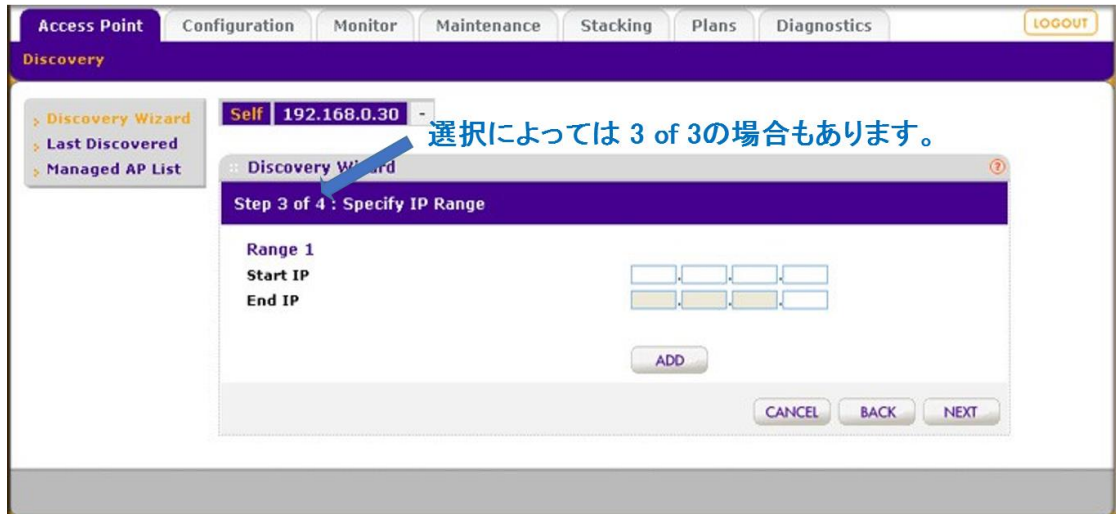


2. 発見したいアクセスポイントの状態をラジオボタンで選択します。
 - **Factory default state**: アクセスポイントの設定がされていない。
 - **Installed and working in Standalone Mode**: アクセスポイントは設定されているか設置されているが、Managed AP List には載っていない。
 - **I am not sure**: このラジオボタンを選択して資料を表示します。
3. **Next** ボタンをクリックします。次の Discovery Wizard 画面が表示されます。



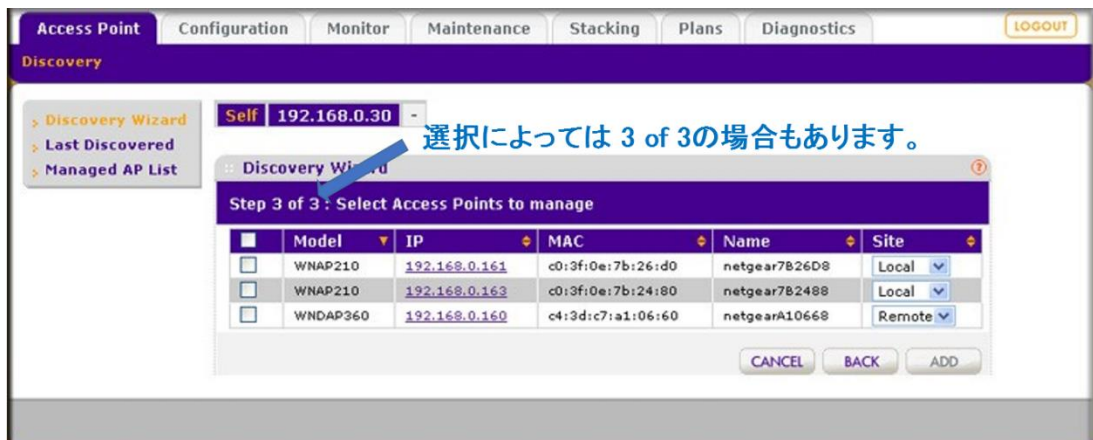
4. アクセスポイントのネットワーク状態をラジオボタンで選択し、**Next** ボタンをクリックします。
 - **Same L2 network - directly or via backend L2 switch**: 同じ IP サブネットにあり、直接またはバックエンドレイヤー2 スイッチを介してワイヤレスコントローラーに接続されているすべてのアクセスポイントを発見します。

- **Different L3 networks – different VLANs or behind IP subnets:**異なる IP サブネットにあり、ワイヤレスコントローラーとルーターを介して接続されているアクセスポイントを発見します。
5. 以下の図のように要求された場合には、ワイヤレスコントローラーがアクセスポイントを発見するための開始 IP アドレスと最後の IP アドレスの範囲を記入します。



6. (オプション) Add ボタンをクリックしてワイヤレスコントローラーが検索する追加の IP アドレスレンジを追加します。最大で 255 の IP アドレスを一度に検索できます。(複数のネットワークにアクセスポイントを設置している場合は繰り返し検索をします。)
7. Next ボタンをクリックして続きます。以下の動作が発生します。
- ワイヤレスコントローラーは MAC アドレスにもとづいて NETGEAR 製品を検索し、サポートしているアクセスポイントを識別します。
 - 発見が終了すると、発見されたアクセスポイントの表がモデルナンバー、IP アドレス、MAC アドレス、名前とともに表示されます。

Discovery Wizard は Select Access Points to Manage 画面を表示します。アクセスポイントが発見された画面を以下に示します。



8. すべてのアクセスポイントが表示されているかを確認します。

9. 以降のセクションを参考にしてサイト (Site) 設定を選択してアクセスポイントを追加します。

Discovery 結果

オートディスカバリーの効果はある程度 LAN のアクセスポイントがどのように設定されているかによります。各アクセスポイントが異なる IP アドレスが割り当てられ、最新のファームウェアで動作している場合、通常、発見は簡単です。

Discovery の結果が期待したものと異なる場合は以下を確認してください。

- 既にワイヤレスコントローラーで管理されているアクセスポイントは発見されたリストには表示されません。Managed AP List は **Access Point > Managed AP List** を選択して表示します。
- アクセスポイントは異なる IP サブネットに存在するかもしれません。ワイヤレスコントローラーの Ping ユーティリティを使ってアクセスポイントの IP アドレスに Ping できるか確認してください。
- アクセスポイントがファクトリーデフォルト状態でルーターを介して接続されている場合、アクセスポイントは検出されません。
- 複数のアクセスポイントが同じ IP アドレスを持っている場合、その中の1台のみがディスカバリーで発見されます。アクセスポイントを管理アクセスポイントリストに追加し、IP アドレスを変更し、ディスカバリーを再度実行し、同じ IP アドレスの次のアクセスポイントを発見します。
- DHCP サーバーがネットワークで動作しているか、ワイヤレスコントローラーの DHCP サーバーが動作していることを確認します。

メモ: 固定 IP でアクセスポイントを設定する場合でも、Discovery から Managed Access Point List に追加するまでは DHCP サーバーが動作している必要があります。

アクセスポイントリスト (Access Point List) の管理

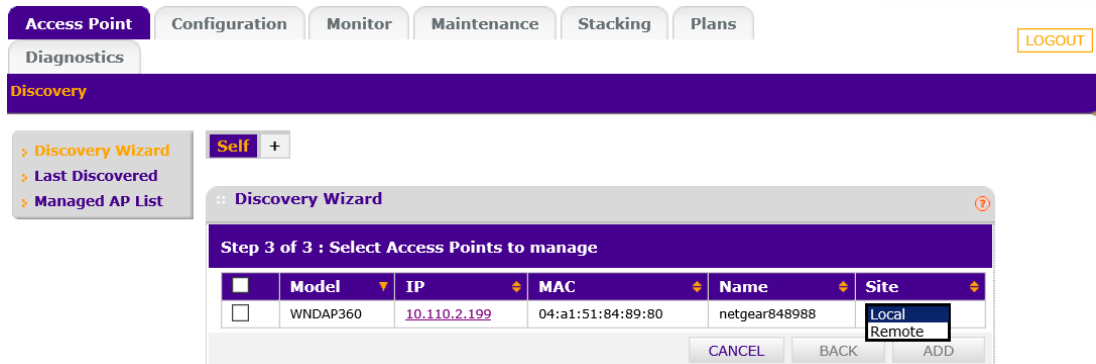
Discovery 後アクセスポイントを Managed List に追加する

ワイヤレスアクセスポイントがアクセスポイントをオートディスカバリー (Autodiscover) した後、ワイヤレスコントローラーが管理できるように、サイト指定を選択しアクセスポイントを管理リスト (Managed List) に追加します。

サイト指定を選択し、発見したアクセスポイントを管理リストに追加する

1. 発見したアクセスポイントのリストを表示する Discovery Wizard 画面でリモートアクセスポイントとして指定するアクセスポイントを選択します。

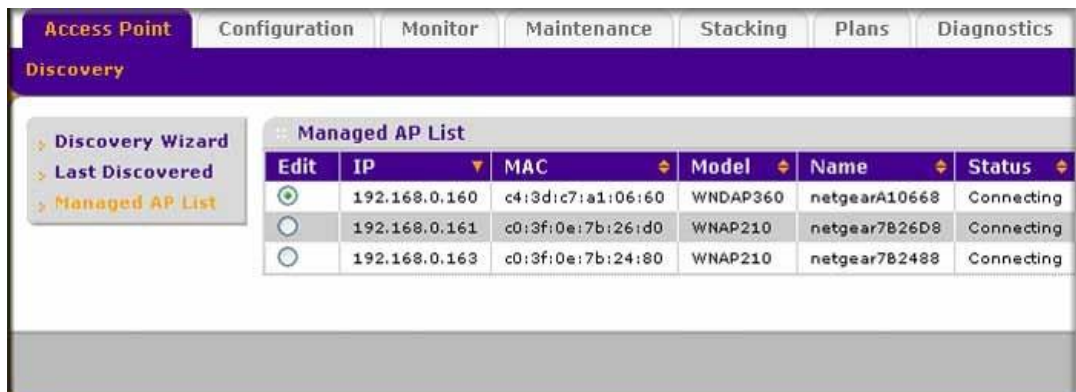
2. Site ドロップダウンリストで **Remote** を選択します。デフォルトは Local です。



3. ステップ 1,2 を繰り返してリモート(Remote)に設定したいアクセスポイントに設定します。
4. 各アクセスポイントのチェックボックスを選択するか、一番上のチェックボックスを選択してすべてのアクセスポイントを選択します。
5. **Add** ボタンをクリックします。発見されたアクセスポイントのタイプによってはログイン名とパスワードを入力する画面が表示されることがあります。

アクセスポイントは Managed AP List に追加され、ワイヤレスコントローラーはワイヤレスコントローラーに保存されている最新のファームウェアにアクセスポイントのファームウェアをアップグレードします。

- 後で発見したアクセスポイントを追加したい場合は、**Access Point > Last Discovered** を選択することで発見されたアクセスポイントを表示することができます。この画面からアクセスポイントを Managed AP List に追加することができます。
 - アクセスポイントを Managed AP List に追加すると、アクセスポイントはディスカバリー結果と Last Discovered 画面から削除されます。
6. **Access Point > Managed AP List** を選択して **Managed AP List** 画面を表示します。(横長画面なので 2 画面に分割して表示します)



| Site | Group Name | Capability | 2.4ghz Mode | 5ghz Mode | Sentry | |
|--------|------------|------------|-------------|-----------|--------|--------------------------|
| Remote | basic | ABGN | 802.11bg | 802.11a | No | <input type="checkbox"/> |
| Local | basic | BGN | 802.11bg | -NA- | No | <input type="checkbox"/> |
| Local | basic | BGN | 802.11bg | -NA- | No | <input type="checkbox"/> |

REMOVE EDIT REFRESH

Managed AP List はリストに追加した各アクセスポイントの以下の情報を表示します。

Managed AP List 情報

| 項目 | 説明 |
|------------|---|
| IP | アクセスポイントの IP アドレス。 |
| MAC | アクセスポイントの MAC アドレス。 |
| Model | アクセスポイントのモデル。 |
| Name | アクセスポイントの名前。 |
| Status | <p>以下の状態オプションの一つを表示します。</p> <ul style="list-style-type: none"> • Authentication in progress. (この状態は数分続きます。) • Applying configurations. • Firmware upgrade. • AP is rebooting. • Connecting. • Connected.: この状態が通常状態です。 • Not Connected: ワイヤレスコントローラーは設定された IP アドレスでアクセスポイントと通信できません。ワイヤレスコントローラーは管理されているアクセスポイントに 1 分おきにログインを試みます。エラーが一時的なものであれば、Status は自動的に Connected に変更されます。エラーが続く場合は、アクセスポイントの IP アドレスと接続性を確認してください。 <p>メモ: ネットワークで DHCP サーバーが有効になっていることを確認してください。でないと管理されたアクセスポイントは Connecting 状態のまま Connected 状態になりません。</p> |
| Site | <p>アクセスポイントがリモート(Remote)かローカル(Local)かを示します。</p> <ul style="list-style-type: none"> • Local: アクセスポイントはローカルサイトに設置されています。 • Remote: アクセスポイントはリモートサイトに設置されています。 |
| Group Name | デフォルトグループは Basic です。 |

| | |
|-------------|--|
| Capability | アクセスポイントがサポートしているワイヤレスモード。 |
| 2.4ghz Mode | 2.4GHz 帯でのアクセスポイントのワイヤレスモード。 |
| 5ghz Mode | 5GHz 帯でのアクセスポイントのワイヤレスモード。 |
| Sentry | Sentry(見張り)モードの有効・無効を表示します。 <ul style="list-style-type: none"> • No: Sentry モードが無効です。 • Yes: Sentry モードが有効です。 |

アクセスポイント情報の編集と削除

Managed AP List でアクセスポイントを編集する

1. **Access Point** > **Managed AP List** を選択して **Managed AP List** を表示します。
2. Managed AP List で編集をするアクセスポイントの Edit 欄のラジオボタンを選択します。
3. **Edit** ボタンをクリックします。Edit Access Point 画面が表示されます。

4. 以下の表にしたがって設定します。いくつかの欄はグレーアウトされて編集できませんが編集できる欄もあります。

Access point 設定

| 設定 | 説明 |
|----------------------------------|---|
| Access Point Info section | |
| Name | アクセスポイント名を記入します。デフォルトでは netgearxxxxxx(xxxxxx は MAC アドレスの下 6 桁)。わかりやすい名前をつけることをおすすめします。 |
| Model | アクセスポイントのモデル。編集不可。 |
| Group | アクセスポイントに割り当てられるグループ・アクセスポイントのディスカバリーの後、アクセスポイントは自動的に Basic グループに割り当てられます。プロファイルグループを設定していれば、ドロップダウンリストから選択してアクセスポイントを他のプロファイルグループに割り当てることができます。後に WLAN Group Assignment 画面でグループ割り当てを変更することもできます。 |

| | |
|---|---|
| IP Settings これらの欄はアクセスポイントの IP アドレスと他の IP 設定を表示します。デフォルトではこれらの欄はアクセスポイントディスカバリーの際に取得されます。 <ul style="list-style-type: none"> • Enable: デフォルト設定。アクセスポイントの DHCP クライアントは有効になります。 • Disable: DHCP クライアント機能を無効にします。アクセスポイントの IP アドレスを含む IP 設定をすることができます。 | |
| IP Address | アクセスポイントの IP アドレス。 |
| Subnet Mask | アクセスポイントのサブネットマスク。 |
| Default Gateway | アクセスポイントのデフォルトゲートウェイ。 |
| Primary DNS Server | アクセスポイントのプライマリDNS サーバー。 |
| Secondary DNS Server | アクセスポイントのセカンダリDNS サーバー。 |
| VLAN Settings section | |
| Untagged VLAN | VLAN ID を記入するかデフォルトの ID のままにします。デフォルトではタグ無しの VLAN は 1 で Untagged VLAN のチェックボックスが選択されています。ワイヤレスコントローラーが LAN(イーサネット)インターフェースにタグ無しの VLAN のフレームを送信すると、それらのフレームはタグが付きません。ワイヤレスコントローラーが LAN(イーサネット)インターフェースからタグ無しのトラフィックを受信すると、これらのフレームはタグ無しの VLAN に割り当てられます。 |
| Managed VLAN | VLAN ID を記入するかデフォルトの ID のままにします。デフォルトでは管理 VLAN は 1 です。 |
| Sentry Mode Settings section | |
| Sentry Mode | アクセスポイントを Sentry(見張りモード)として動作させるときにこのチェックボックスを選択します。Sentry モードではアクセスポイントは不正アクセスポイントの迅速な検知と対処のために、ワイヤレスネットワークをモニターしますが、ワイヤレスクライアントが接続することはできません。 メモ: WNAP210(国内未発売)は Sentry モードをサポートしていません。 |
| Wireless Settings section | |
| Antenna | アクセスポイントが内部アンテナか外部アンテナを使っているかをドロップダウンリストで選択できます。 <ul style="list-style-type: none"> • Internal: アクセスポイントは内部アンテナを使用します。 • External: アクセスポイントは外部アンテナを使用します。外部アンテナはアクセスポイントに付属していません。 |
| Plan Settings section | |

| | |
|----------|--------------------------------------|
| Site | サイト選択を表示します。 |
| Building | ドロップダウンリストでアクセスポイントを設置しているビルを選択します。 |
| Floor | ドロップダウンリストでアクセスポイントを設置しているフロアを選択します。 |
| Location | わかりやすい名前をつけます。 |

5. **Apply** ボタンをクリックして設定を保存します。
6. **Back** ボタンをクリックして Managed AP List に戻ります。

Managed AP List からアクセスポイントを削除する

1. Managed AP List で削除したいアクセスポイントのチェックボックスを選択します。
2. **Remove** ボタンをクリックします。

メモ: アクセスポイントのファームウェアを元のファームウェアに戻しスタンドアロンアクセスポイントとして使いたい時、アクセスポイントを Managed AP List から削除します。アクセスポイントの Web 管理画面にログインし、スタンドアロンファームウェアでアクセスポイントをアップグレードし、アクセスポイントを再起動します。

5. ネットワーク設定

一般設定 (General Settings)

メモ: 正しい国設定で使う必要があります。異なる国設定でアクセスポイントを使うことは違法になる可能性があります。

一般設定画面でワイヤレスコントローラーの基本設定をします。

一般設定をする

1. Configuration > System > General を選択して General Settings 画面を表示します。

2. 以下の表の内容に従い設定をします。

General settings

| 設定 | 説明 |
|----------------|---|
| Name | ワイヤレスコントローラー名を記入します。設定が終わったら名前を変更することをおすすめします。英数字とハイフン“-“が使用可能です。最大 31 文字です。 |
| Country/Region | ドロップダウンリストでワイヤレスコントローラーとアクセスポイントを動作させる国を選択します。この設定はワイヤレスコントローラーの最適なパフォーマンスのために肝要です。米国ではアクセスポイントの国設定は事前にされており、変更不可です。国や地域設定が正しく設定されていないと、ワイヤレスコントローラーはアクセスポイントに接続できない可能性があります。 |

| | |
|--------------------------|--|
| Controller Location Code | オプションとして、ワイヤレスコントローラーの物理的な位置を識別するコードを入力することができます。複数のワイヤレスコントローラーを使う場合に非常に役に立ちます。 |
|--------------------------|--|

3. **Apply** ボタンをクリックして設定を保存します。

時間管理

この画面でワイヤレスコントローラーとアクセスポイントの時間関連の設定をします。

時間設定をする

1. **Configuration > System > Time** を選択して Time Settings 画面を表示します。

The screenshot shows the 'Time Settings' configuration page. The 'Time Zone' is set to 'Japan'. The 'Current Time' is 'Mon Jan 4 22:25:04 JST 2016'. The 'NTP Client' is set to 'enable'. The 'Use Custom NTP Server' checkbox is checked. The 'Hostname/IP Address' is 'ntp.nict.jp'. There are 'CANCEL' and 'APPLY' buttons at the bottom right.

2. 以下の表に従って設定をします。

時間設定

| 設定 | 説明 |
|-----------------------|--|
| Time Zone | ドロップダウンリストからお使いの国のタイムゾーンを選択します。 |
| Current Time | 現在のタイムゾーンでの時間を表示します。(変更不可) |
| NTP Client | Enable ラジオボタンを選択してワイヤレスコントローラーとアクセスポイントの時間をNTP(Network Time Protocol)サーバーを使って同期します。r Disable ラジオボタンを選択して NTP サーバーの使用を停止します。 |
| Use Custom NTP Server | NTP サーバーを指定したい時にチェックボックスを選択します。デフォルトではNETGEAR の NTP サーバーを使います。 |
| Hostname/IP Address | NTP サーバーのホスト名または IP アドレスを指定します。 |

3. **Apply** ボタンをクリックして設定を保存します。

IP と VLAN 設定

IP Settings 画面でワイヤレスコントローラーの管理 IP アドレス設定をします。

IP/VLAN 設定をする

1. **Configuration > System > IP/VLAN** を選択して IP Settings 画面を表示します。

The screenshot shows the configuration interface for the IP Settings and Management VLAN Settings. The IP Settings section includes fields for IP Address (192.168.0.251), IP Subnet Mask (255.255.255.0), Default Gateway (192.168.0.1), Primary DNS Server, Secondary DNS Server, and WINS Server. The Management VLAN Settings section includes a field for Management VLAN (1) and a checked checkbox for Untagged VLAN (1). Buttons for CANCEL and APPLY are visible at the bottom right.

2. 以下の表に従い設定をします。

IP と管理 VLAN 設定

| 設定 | 説明 |
|---|--|
| IP Settings section | |
| IP Address | ワイヤレスコントローラーの IP アドレスを指定します。デフォルトは 192.168.0.250 です。お使いの LAN で使われている IP アドレスの範囲の値を入力します。 |
| IP Subnet Mask | お使いの LAN のサブネットマスクを入力します。デフォルトは 255.255.255.0 です。 |
| Default Gateway | デフォルトゲートウェイの IP アドレスを指定します。 |
| Primary DNS Server | プライマリー-DNS サーバーの IP アドレスを指定します。 |
| Secondary DNS Server | セカンダリー-DNS サーバーの IP アドレスを指定します。 |
| WINS Server | WINS (Windows Internet Name Service) の IP アドレスを指定します。 |
| Management VLAN Settings section | |
| Management VLAN | 管理 VLAN ID を入力します。 |
| Untagged VLAN | 設定した管理 VLAN がタグ無しの場合チェックボックスを選択します。 |

3. **Apply** ボタンをクリックして設定を保存します。

管理 VLAN

管理 VLAN はワイヤレスコントローラーとアクセスポイントの間で送受信されるすべての SNMP と HTTP トラフィックに使われます。

大規模なネットワークでは、ワイヤレスコントローラーとアクセスポイントの通信を守るために独立した VLAN に所属させることを推奨します。

ワイヤレスコントローラーとアクセスポイントは同期を維持し、シームレスローミングを容易にするために設定とクライアントの情報を共有します。

タグ無し VLAN

Untagged VLAN チェックボックスが選択されると、一つの VLAN はタグ無しの VLAN として設定できます。

- ワイヤレスコントローラーがタグ無しの VLAN に関連付けられているフレームを LAN(イーサネット)インターフェースに送信すると、それらのフレームは 802.1QVLAN ヘッダーを持ちません。
- ワイヤレスコントローラーが LAN(イーサネット)インターフェースからタグ無しトラフィックを受信した時、これらのフレームはタグ無しの VLAN に割り当てられます。

Untagged VLAN チェックボックスの選択が外されると、ワイヤレスコントローラーはすべての送信する LAN(イーサネット)フレームにタグをつけ、設定されている VLAN ID のタグ付きのフレームのみを受信します。

メモ: お使いの LAN のスイッチやハブが VLAN(802.1Q)をサポートしている時のみ Untagged VLAN チェックボックスを外すことができます。同様にお使いの LAN のスイッチやハブが VLAN(802.1Q)をサポートしている時のみタグ無しの VLAN ID を変更することができます。

お使いのネットワークのハブやスイッチが関連する VLAN 設定をしないうちにいずれかの設定を変更すると、IP 接続を失います。

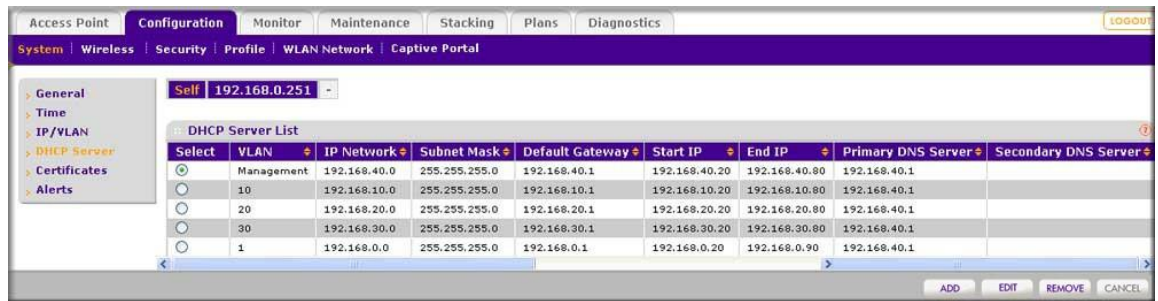
DHCP サーバーの管理

メモ: DHCP サーバーが動作していることを確認してください、でないと、Discovery Wizard は正しく動作しません。既にネットワークで DHCP サーバーが稼働している場合は、ワイヤレスコントローラーの DHCP サーバーを有効にしないでください。

ワイヤレスコントローラーは DHCP として動作することができます。異なる VLAN に対して複数の DHCP サーバールールを追加することが可能です。この画面では DHCP サーバーを有効にし設定することができます。DHCP サーバーを追加することもできます。

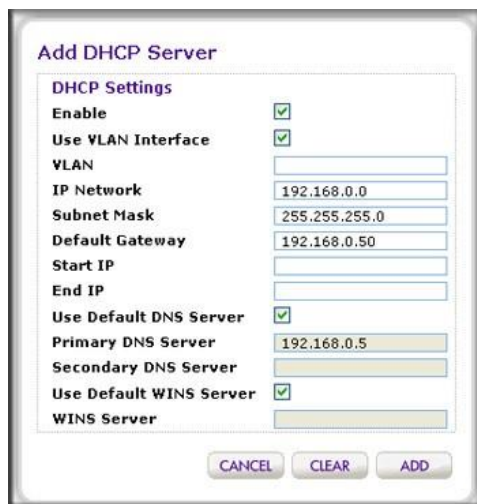
DHCP サーバーを追加し設定をする

1. **Configuration > System > DHCP** を選択して DHCP 設定画面を表示します。以下に DHCP 設定画面を示します。



DHCP Server List はワイヤレスコントローラーで設定されている DHCP サーバーを示します。

2. **Add** ボタンをクリックすると、Add DHCP Server ポップアップウィンドウが表示されます。



3. 以下の表の説明に従って設定をします。

DHCP 設定

| 設定 | 説明 |
|--------------------|--|
| Enable | チェックボックスを選択して DHCP サーバーを有効にします。選択を外して DHCP サーバーを無効にします。 |
| Use VLAN Interface | チェックボックスを選択して VLAN で DHCP サーバーを動作させます。 |
| VLAN | DHCP サーバーを動作させる VLAN ID を指定します。範囲は 1-4094 です。DHCP サーバーはこの VLAN で動作します。 |

| | |
|-------------------------|---|
| IP Network | 指定した VLAN でのワイヤレスコントローラーの IP アドレスを指定します。Use VLAN Interface チェックボックスを選択していない場合はワイヤレスコントローラーの管理 VLAN の IP アドレスが使われます。 |
| Subnet Mask | DHCP サーバーが割り当てるワイヤレスクライアントのサブネットマスクを指定します。 |
| Default Gateway | ローカルネットワーク外へ出て行くすべてのトラフィックのデフォルトゲートウェイの IP アドレスを指定します。 |
| Start IP | DHCP サーバーが割り当てる IP アドレス範囲の最初の IP アドレスを指定します。 |
| End IP | DHCP サーバーが割り当てる IP アドレス範囲の最後の IP アドレスを指定します。 |
| Use Default DNS Server | チェックボックスを選択して DHCP サーバーがワイヤレスコントローラーのデフォルト DNS サーバーを使うようにします。選択すると Primary DNS Server と Secondary DNS Server 欄はマスクされます。 |
| Primary DNS Server | プライマリーDNS サーバーの IP アドレスを指定します。 |
| Secondary DNS Server | セカンダリーDNS サーバーの IP アドレスを指定します。 |
| Use Default WINS Server | チェックボックスを選択して DHCP サーバーがワイヤレスコントローラーのデフォルト WINS サーバーを使うようにします。選択すると WINS Server 欄はマスクされます。 |
| WINS Server | WINS サーバーの IP アドレスを指定します。 |

4. **Add** ボタンをクリックして設定を保存し、新しい DHCP サーバーを DHCP Server List に追加します。

DHCP サーバーを編集する

1. DHCP Server List で編集する DHCP サーバーのラジオボタンを選択します。
2. **Edit** ボタンをクリックすると DHCP Server ポップアップウィンドウが表示されます。このウィンドウは Add DHCP Server ウィンドウと同じです。
3. 前の表を参考に設定を変更します。
4. **Apply** ボタンをクリックして設定を保存します。

DHCP サーバーを削除する

1. DHCP Server List で削除する DHCP サーバーのラジオボタンを選択します。
2. **Remove** ボタンをクリックします。

証明書管理

証明書を使った認証のための内部認証サーバーではワイヤレスコントローラーに証明書をインストールする必要があります。ワイヤレスコントローラーにはデフォルトの自己署名証明書がインストールされていますが、信頼された認証局 (CA) からサイトまたはドメインに対して発行された証明書で置き換えることを強く推奨します。

ワイヤレスコントローラー用の証明書を取得するには、CSR(Certificate Signing Request: 証明書署名要求)を生成して認証局 (CA) に提出します。CA 署名付きサーバー証明書を受け取ったら、このセクションに記載されている方法で証明書を PC からインストールします。証明書は X.509 PEM 形式である必要があります。

証明書を追加する

1. **Configuration > System > Certificates** を選択して **Add Certificates** 画面を表示します。

2. 以下の表にしたがって設定をします。

証明書設定

| 設定 | 説明 |
|------------------------|--------------------------------------|
| Password | ワイヤレスコントローラー証明書のパスワードを記入します。 |
| Controller Key | 参照ボタンをクリックしてコントローラーの Key ファイルを選択します。 |
| Controller Certificate | 参照ボタンをクリックしてコントローラーの証明書を選択します。 |
| CA Certificate | 参照ボタンをクリックして認証局証明書ファイルを選択します。 |

3. **Apply** ボタンをクリックして設定を保存します。

Syslog とアラーム通知設定

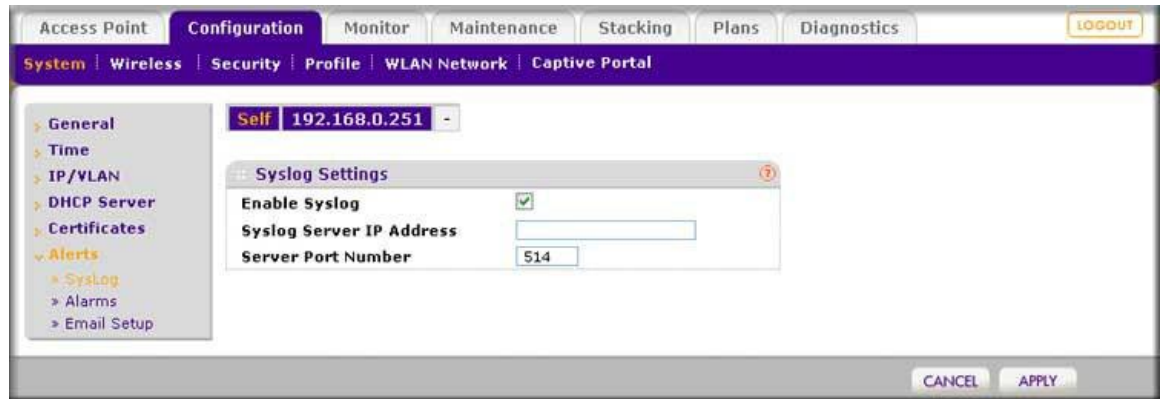
Alerts メニューから Syslog とアラーム (Alarm) を設定し、アラート (Alert) 送信元メールアドレスを設定できます。

Syslog 設定をする

この画面で Syslog サーバーがネットワークに存在する場合、Syslog サーバーへ接続する設定ができます。

Syslog 設定をする

1. **Configuration > System > Alerts > Syslog**を選択して **Syslog Settings** 画面を表示します。



2. 以下の表の説明に従って設定をします。

Syslog 設定

| 設定 | 説明 |
|--------------------------|---|
| Enable Syslog | チェックボックスを選択して Syslog 設定を有効にします。 |
| Syslog Server IP Address | Syslog の送信先(Syslog サーバー)の IP のアドレスを設定します。 |
| Server Port Number | Syslog サーバーのポート番号を指定します。 |

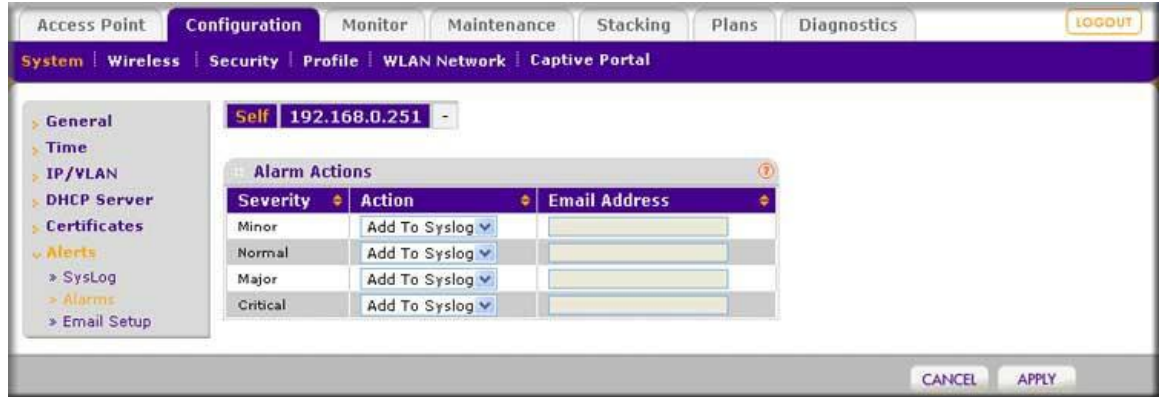
3. **Apply** ボタンをクリックして設定を保存します。

アラーム通知(Alarm Notification)設定

特定のイベントを critical, major, normal, または minor に分類することができます。いくつかのイベントは critical または major のみに分類できます。例えば、RF Management 画面では、カバレッジホールは critical あるいは major のみに設定できます。

アラームアクション(Alarm Actions)を設定する

1. **Configuration > System > Alerts > Alarms** を選択して **Alarm Actions** 画面を表示します。



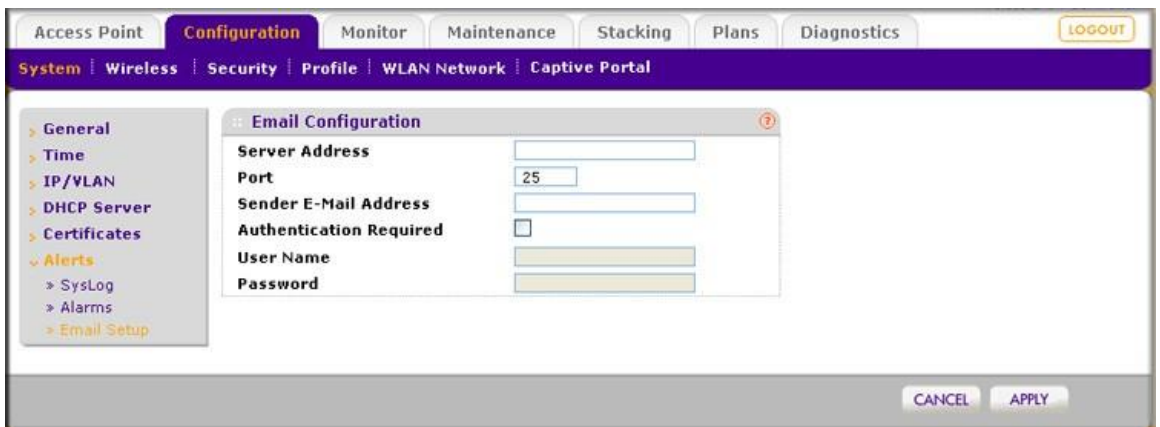
2. 各 Alarm Severity (Minor, Normal, Major, Critical) について希望する動作を Action ドロップダウンリストから選択します。
 - **No Action:** アラームが発生しても対応しません。
 - **Add To Syslog:** アラームが発生した時にワイヤレスコントローラーは Syslog にエントリーを追加します。
 - **Send Email:** アラームが発生した時に、ワイヤレスコントローラーをメールを送信します。
3. **Send Email** を選択した場合は、送信先メールアドレスを記入します。
4. **Apply** ボタンをクリックして設定を保存します。

メール通知サーバー設定

メール通知サーバーはメールアラートの送信元です。

メール設定をする

1. **Configuration > System > Alerts > Email** を選択して **Email Configuration** 画面を表示します。



2. 以下の表に従い設定をします。

メール設定

| 設定 | 説明 |
|----|----|
| | |

| | | |
|-------------------------|--|----------------------|
| Server Address | メール通知を送信するサーバーの IP アドレスを指定します。 | |
| Port | メール通知を送信するサーバーのポート番号を指定します。デフォルトは 25 です。 | |
| Sender Email Address | メール通知を送信するメールアドレスを指定します。 | |
| Authentication Required | メールサーバーが認証を必要とする場合、このチェックボックスを選択し、User Name と Password を設定します。 | |
| | User Name | メールサーバーのユーザー名を指定します。 |
| | Password | メールサーバーのパスワードを指定します。 |

3. **Apply** ボタンをクリックして設定を保存します。

6. セキュリティプロファイルとプロファイルグループ管理

メモ: この章と以降の章ではアクセスポイントプロファイルグループをプロファイルグループと表現します。
プロファイル、セキュリティプロファイル、SSID(すなわちセキュリティプロファイルと関連付けられている SSID)は交換可能な用語です。

ワイヤレスセキュリティプロファイル管理

プロファイルはアクセスポイントに適用できる設定の組み合わせです。設定には電波パラメーター、ロードバランスパラメーター、レートリミットパラメーターが含まれています。アクセスポイントのそれぞれの電波は 8 つのプロファイルをサポート可能です。デュアルバンドの WNDAP360 は合計で 16 のプロファイルをサポートできます。したがってワイヤレスコントローラーの一つのプロファイルグループは各電波(周波数帯域)で最大 8 つのプロファイル、すなわち 2.4GHz 帯で 8 つ、5GHz 帯で 8 つのセキュリティプロファイルを設定できます。

プロファイルの設定は無線 LAN ネットワークをオフラインで作ることを可能にします。次に無線 LAN ネットワークが起動し動作している時に管理されたアクセスポイントに設定を送り込むことが出来ます。ワイヤレスアクセスポイントの状態を考慮せずにプロファイルとプロファイルグループを設定することができます。アクセスポイントがコントローラーに接続された時に、プロファイル設定がアクセスポイントに適用されます。

メモ: アクセスポイントがビルから取り除かれた(だれかが家に持ち帰ったり、盗まれたりした)とき、アクセスポイントはコントローラーから受信した設定を保持しません。設定はアクセスポイントのメモリーには保存されていません。

お使いのネットワーク要件に応じて、基本プロファイルグループ(すなわち基本設定)あるいは拡張プロファイルグループ(すなわち拡張設定)を使うことが出来ます。基本プロファイルグループは小さな規模の無線 LAN ネットワークで良く動作し、拡張プロファイルは大規模な構成に役に立ちます。

小さな無線 LAN ネットワーク

小さな無線 LAN ネットワークでは、基本プロファイルグループの基本設定を使うことができます。すべてのアクセスポイントは同じグループに属し、同じ無線、セキュリティ、QoS 設定を使います。

基本プロファイルグループはデュアルバンドアクセスポイントでは最大 16、シングルバンドアクセスポイントでは最大 8 までのプロファイルを持つことができます。各プロファイルはそれぞれの SSID を持ち、それぞれのトンネルを確立するための VLAN を持ちます。プロファイルは同じ VLAN を共有することも可能です。

例えば、企業ネットワークにおいてすべてのアクセスポイントがワイヤレスコントローラーによって管理されて、同じ無線 LAN ネットワークを提供し、同じ設定を保つ場合、基本設定を使うことができます。

大きな無線 LAN ネットワーク

異なる設定の無線 LAN ネットワークからなる大きなネットワークでは、複数のプロファイルグループを作成するために拡張設定の利用を検討してください。同じプロファイルグループに属するアクセスポイントは同じ無線、セキュリティ、QoS 設定を使います。

ワイヤレスコントローラーは最大 8 つのプロファイルグループをサポートします。各プロファイルグループはそれぞれの無線、セキュリティ、QoS 設定を持つことができます。各プロファイルグループはデュアルバンドアクセスポイントでは最大 16 プロファイル、シングルアクセスポイントでは最大 8 つのプロファイルを持つことができます。デュアルバンドアクセスポイントを使うとワイヤレスコントローラーは合計 128 のプロファイルをサポートできます。各プロファイルはそれぞれの SSID を持ち、トンネルを確立するための VLAN を持ちます。プロファイルは同じ VLAN を共有することも可能です。

また大きなネットワークではゲストはビジネスネットワークではなくインターネットのみにアクセスし、ネットワーク上でピアツーピアアクセスをしないため、ゲストを別の VLAN に割り当てることも可能です。

プロファイル命名規則

Marketing のようなグループ名に基づいたプロファイル名や VLAN40 のような VLAN に基づいたプロファイル名、あるいは CompanyName15 のようなプロファイル名を作ることも可能です。

メモ: 拡張設定では、プロファイルグループ名を変更することはできません。しかし、MAC ACL や外部 RADIUS サーバーの名前を変更することは可能です。

プロファイルを設定する前に

基本プロファイルグループあるいは拡張プロファイルグループのためにプロファイルを作成し設定する前に以下の点を考慮してください。

- **認証サーバー:** 外部 LDAP あるいは RADIUS サーバーのどちらかあるいは両方を使うのならば最初に認証サーバー設定を作成してください。

- 基本 Authentication Server 画面で基本サーバー設定します。
- より複雑なネットワークのために、Advanced Authentication Server 画面で追加の RADIUS サーバーを設定します。

認証サーバー設定を行った後に基本プロファイルグループあるいは拡張プロファイルグループのセキュリティプロファイルに認証サーバーを割り当てることができます。

メモ:異なる認証サーバーで機能するプロファイルを設定することができます。たとえば、認証無しのゲストプロファイル、外部 RADIUS 認証を使うエンジニアリングプロファイル、外部 LDAP 認証を使うマーケティングプロファイルを作ることが可能です。他のプロファイルで追加の RADIUS サーバーを使うこともできます。

- **MAC アドレス認証:**ワイヤレスクライアントのアクセスを制御するために MAC ACL(Access Control List)を使うには最初に MAC ACL を作成してください。
 - Basic MAC Authentication 画面で Basic MAC ACL を設定します。
 - より複雑なネットワークのために、追加の MAC Authentication 画面で追加の MAC ACL を設定します。MAC ACL を設定した後に基本プロファイルグループあるいは拡張プロファイルグループ MAC ACL を割り当てることができます。
- **プロファイルの複製:**設定を速く行うために、プロファイルを複製(クローン: Clone)して名前を変更することが可能です。クローンは名前と SSID 以外の設定をすべて複製します。

基本プロファイルグループのセキュリティプロファイル設定

Edit Profile (Basic)画面でワイヤレス無線帯域ごとに最大 8 つのセキュリティプロファイル(デュアルバンドアクセスポイントでは 16、シングルバンドアクセスポイントでは 8)を設定できます。異なるプロファイルが 802.11b/bg/ng モードと 802.11a/na モードの無線に適用されます。

基本プロファイルグループにセキュリティプロファイルを追加する

1. **Configuration > Profile > Basic > Radio** を選択して Edit Profile (Basic)画面を表示します。
デフォルトでは NG_11g と NG_11a プロファイルが Basic Profile Group には表示されています。

Access Point Configuration Monitor Maintenance Stacking Plans Diagnostics

System | Wireless Security Profile | WLAN Network | Captive Portal

Basic > Radio > Load Balancing > Rate Limit > Advanced

Self +

802.11b/bg/ng 802.11a/na +をクリックしてプロファイルを追加する

WNDAP36024G +

Profile Definition

Name: WNDAP36024G
 Wireless Network Name (SSID): WNDAP36024G
 Broadcast Wireless Network Name (SSID): Yes No

Client Authentication

Network Authentication: WPA-PSK
 Data Encryption: TKIP
 WPA Passphrase (Network Key):
 Wireless Client Security Separation: Disable
 VLAN: 1

Authentication Settings

MAC ACL: Local External
 Local MAC ACL Group: basic
 Captive Portal:

Wireless QoS

Wi-Fi Multimedia (WMM): enable disable
 WMM Powersave: enable disable

CANCEL DELETE APPLY

2. 電波をタブで選択します。
3. +ボタンをクリックしてプロファイルを Basic Profile Group に追加します。ADD Profiles ポップアップウィンドウが表示されます。



4. Add ボタンをクリックするか、既存のプロファイルをクローンするには、Clone an existing Profile チェックボックスを選択し、Profiles ドロップダウンリストからプロファイルを選択し、Add ボタンをクリックします。新しく作成されたプロファイルが画面に表示され、新しいプロファイルを設定できるように新しいプロファイルのタブが自動的に選択されます。

メモ: Network Authentication 欄は認証サーバー設定によって変化します。

5. 以下の表に従って設定をします。

Basic security profile 設定

| 設定 | 説明 |
|---|---|
| Profile Definition section | |
| Name | プロファイルを識別できる名前を設定します。英数字 32 文字までです。デフォルト名ではなく意味のある名前に変更することをおすすめします。デフォルトプロファイル名は Profile1, Profile2, ~ Profile8 です。 |
| Wireless Network Name (SSID) | このプロファイルと関連付ける唯一のワイヤレスネットワーク名を指定します |
| Broadcast Wireless Network Name | Yes: SSID のブロードキャストを有効にします。これがデフォルト設定です。 No: SSID のブロードキャストを無効にし、正しい SSID 設定をしているデバイスのみがアクセスポイントに接続できます。 |
| Client Authentication section | |
| メモ: Network Authentication ドロップダウンリストの選択により表示されるオプションは異なります。 | |
| Network Authentication | 使用する認証タイプをドロップダウンリストから選択します。 |
| Data Encryption | 使用する暗号化タイプをドロップダウンリストから選択します。ネットワーク認証設定によりデータ暗号化のオプションは異なります。 |
| Wireless Client Security Separation | Disable: 接続しているワイヤレスクライアント間の直接通信を禁止します。 Enable: 接続しているワイヤレスクライアント間の直接通信を許可します。 Wireless client separation はホットスポットや公共でのアクセスの場合での利用を想定しています。 |
| VLAN | このセキュリティプロファイルに関連付ける VLAN ID を指定します。この VLAN ID は他のネットワークデバイスの設定に一致する必要があります。 |
| Authentication Settings section | |
| メモ: 画面に表示されるオプションは Network Authentication ドロップダウンリストの選択により異なります。 | |
| Open System, Shared Key, WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK | <p>ラジオボタンのどちらかを選択します。</p> <ul style="list-style-type: none"> • Local: ローカル MAC 認証を使います。Local MAC ACL Group ドロップダウンリストが表示され、グループを選択します。 • External: 外部 MAC 認証を使用します。External Radius Server ドロップダウンリストが表示され、サーバーを選択します。Basic-Auth RADIUS server または advanced authentication group の RADIUS server を使うことができます。外部 LDAP サーバーを使うことはできません。 <p>メモ: ネットワーク認証に外部 RADIUS サーバーを使うときには MAC ACL ラジオボタンは画面に表示されません。理由は外部 RADIUS サーバーで MAC 認証あるいは外部 RADIUS サーバーでネットワーク認証のいずれかの設定はできませんが、両方の設定はできないからです。すなわち、外部 RADIUS サーバーで WPA, WPA2, または WPA & WPA2 (あるいはレガシー802.1X)を設定すると、外部 MAC 認証を使うことはできず、MAC ACL ラジオボタンは表示されません。内部 MAC 認証をつかうことは可能です。</p> |

| | | |
|--|---|---|
| Open System, Shared Key, WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK (continued) | Captive Portal | <p>キャプティブポータル (Captive Portal) を使うときにチェックボックスを選択します。</p> <p>メモ: ネットワーク認証に外部 RADIUS サーバーを使うときにはキャプティブポータル認証は設定できません。すなわち、外部 RADIUS サーバーで WPA, WPA2, または WPA & WPA2 (あるいはレガシー-802.1X) を設定すると、Captive Portal チェックボックスは画面に表示されません。</p> |
| WPA with Radius, WPA2 with Radius, and WPA & WPA2 with Radius | Authentication Server | <p>どちらかのラジオボタンを選択します。</p> <ul style="list-style-type: none"> • Local: ローカル認証サーバーを使用します。 • External: 外部認証サーバーを使用します。Authentication Server ドロップダウンリストから外部認証サーバーを選択します。 |
| Wireless QoS section | | |
| Wi-Fi Multimedia (WMM) | <p>Enable: WMM を有効にします。(デフォルト設定)</p> <p>Disable: WMM を無効にします。</p> | |
| WMM Powersave | <p>Enable: WMM パワーセーブを有効にします。(デフォルト設定)</p> <p>Disable: WMM パワーセーブを無効にします。</p> | |

6. **Apply** ボタンをクリックして設定を保存します。

基本プロファイルグループでのプロファイルの編集・削除

既存プロファイルの編集をする

1. Basic Profile 画面でプロファイルのタブをクリックします。
2. タブをクリックして電波を選択します。
3. 設定を変更します。
4. **Apply** ボタンをクリックして設定を保存します。

既存プロファイルを削除する

1. Basic Profile 画面でプロファイルのタブをクリックします。
2. タブをクリックして電波を選択します。
3. **Delete** ボタンをクリックしてプロファイルの削除を確認します。

ネットワーク認証とデータ暗号化オプション

以下の表はネットワーク認証に基づくデータ暗号化のオプションであり、選択したネットワーク認証を実現するために必要な設定ステップです。

メモ: Edit Profile (Basic)あるいは Edit Profile (Group-X)画面で、RADIUS サーバーを必要とする Network Authentication ドロップダウンリストからのどの選択肢でも、認証は RADIUS サーバーには限定されず、内部認証サーバーや外部 LDAP サーバーを使用することも可能です。

メモ: 外部 RADIUS サーバーで MAC 認証あるいは外部 RADIUS サーバーでネットワーク認証のどちらかを設定することはできますが、両方を設定することはできません。すなわち、外部 MAC 認証をせっていると、外部 RADIUS サーバーで WPA, WPA2, または WPA & WPA2 を使うことはできません。

ネットワーク認証とデータ暗号化設定

| ネットワーク認証選択 | データ暗号化オプション | 設定ステップ |
|------------|--|--|
| Open | None WEP | Open System では暗号化無し、あるいは WEP 暗号化を使うことができます。 <ul style="list-style-type: none"> • No encryption: 暗号化をしません。デフォルト設定。追加のせっては不要です。 • WEP encryption: Open System で WEP 暗号化を設定するにはこの表の Shared Key と WEP の項目を参照してください。 |
| Shared Key | 64-bit WEP 128-bit WEP 152-bit WEP | WEP で Shared Key 認証を設定する <ol style="list-style-type: none"> 1. Data Encryption ドロップダウンリストで WEP 暗号化のレベルを選択します。 <ul style="list-style-type: none"> - 64-bit WEP: 40/64 ビット暗号化 - 128-bit WEP: 104/128 ビット暗号化 - 152-bit WEP: 独自モード。接続先がサポートしている場合のみ動作します。 2. Key ラジオボタン (Key1, Key2, Key3, Key4)を選択します。 3. Key を入力します。 <ul style="list-style-type: none"> - 64-bit WEP は 10 文字の Key が必要です。 - 128-bit WEP は 26 文字の Key が必要です。 - 152-bit WEP は 32 文字の Key が必要です。 |

| | | |
|------------------|--------------------|---|
| Legacy 802.1x | None | <p>レガシー802.1xを設定する</p> <ol style="list-style-type: none"> 1. 内部または外部 (RADIUS または LDAP) 認証サーバーを設定し有効にします。 2. Local または External ラジオボタンを選択します。 3. External ラジオボタンを選択した場合、ドロップダウンリストから認証サーバーを選択します。 |
| WPA with Radius | TKIP TKIP + AES | <p>RADIUS サーバーで WPA 認証を設定する</p> <ol style="list-style-type: none"> 1. 内部または外部 (RADIUS または LDAP) 認証サーバーを設定し有効にします。 2. Data Encryption ドロップダウンリストから暗号化タイプを選択します。 <ul style="list-style-type: none"> - TKIP: TKIP (Temporal Key Integrity Protocol) のみをサポートします。 - TKIP + AES: TKIP と AES (Advanced Encryption Standard) をサポートします。 3. Local または External ラジオボタンを選択します。 4. External ラジオボタンを選択した場合、ドロップダウンリストから認証サーバーを選択します。 |
| WPA2 with Radius | AES TKIP + AES | <p>RADIUS サーバーで WPA2 認証を設定する</p> <ol style="list-style-type: none"> 1. 内部または外部 (RADIUS または LDAP) 認証サーバーを設定し有効にします。 2. Data Encryption ドロップダウンリストから暗号化タイプを選択します。 <ul style="list-style-type: none"> - AES: AES のみをサポートします。 - TKIP + AES: TKIP と AES をサポートします。 3. Local または External ラジオボタンを選択します。 4. External ラジオボタンを選択した場合、ドロップダウンリストから認証サーバーを選択します。 |

| | | |
|--|--------------------|--|
| <p>WPA & WPA2 with Radius</p> <p>Note: Use this option if there are both WPA and WPA2 clients in the network.</p> | TKIP + AES | <p>RADIUS サーバーで WPA & WPA2 認証を設定する</p> <p>RADIUS サーバーで WPA2 認証を設定する</p> <p>内部または外部 (RADIUS または LDAP) 認証サーバーを設定し有効にします。</p> <ol style="list-style-type: none"> 内部または外部 (RADIUS または LDAP) 認証サーバーを設定し有効にします。 Local または External ラジオボタンを選択します。 External ラジオボタンを選択した場合、ドロップダウンリストから認証サーバーを選択します。 <p>メモ: Data Encryption ドロップダウンリストは TKIP + AES を表示し、これが唯一の利用可能なオプションです。TKIP と AES のどちらもサポートしています。</p> |
| WPA-PSK | TKIP TKIP + AES | <p>WPA-PSK 認証を設定する</p> <ol style="list-style-type: none"> Data Encryption ドロップダウンリストで暗号化タイプを選択します。: <ul style="list-style-type: none"> - TKIP: TKIP のみをサポートします。 - TKIP + AES: TKIP と AES の両方をサポートします。 WPA Passphrase (Network Key)欄に最低 8 文字のパスフレーズを設定します。 |
| WPA2-PSK | AES TKIP + AES | <p>WPA2-PSK 認証を設定する</p> <ol style="list-style-type: none"> Data Encryption ドロップダウンリストで暗号化タイプを選択します。: <ul style="list-style-type: none"> - AES: AES のみをサポートします。 - TKIP + AES: TKIP と AES の両方をサポートします。 WPA Passphrase (Network Key)欄に最低 8 文字のパスフレーズを設定します。 |
| <p>WPA-PSK & WPA2-PSK</p> <p>Note: Use this option if there are both WPA-PSK and WPA2-PSK clients in the network.</p> | AES TKIP + AES | <p>WPA-PSK & WPA2-PSK 認証を設定する</p> <p>WPA Passphrase (Network Key)欄に最低 8 文字のパスフレーズを設定します。</p> <p>メモ: Data Encryption ドロップダウンリストは TKIP + AES を表示し、これが唯一の利用可能なオプションです。TKIP と AES のどちらもサポートしています。</p> |

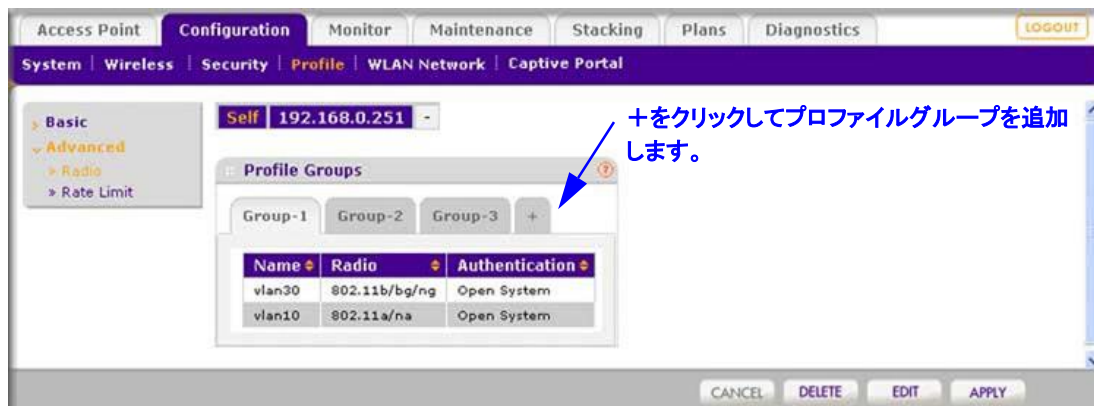
拡張プロファイルグループのセキュリティプロファイル設定

Advanced Profile Group 画面で 8 つのプロファイルグループを作成することができます。それぞれのプロファイルグループでワイヤレス無線帯域ごとに最大 8 つのセキュリティプロファイル (デュアルバンドアクセスポイントでは 16、シングルバンドアクセスポイントでは 8) を設定できます。異なるプロファイルが 802.11b/bg/ng モードと 802.11a/na モードの無線に適用されます。

デフォルトではすべてのアクセスポイントは基本プロファイルグループに割り当てられます。拡張プロファイルグループを作成後、WLAN Network 画面でアクセスポイントを拡張プロファイルグループに割り当てることができます。

プロファイルグループの追加、新しいプロファイルの設定、プロファイルの追加

1. Configuration > Profile > Advanced > Radio を選択して Profile Groups 画面を表示します。



以下の表にプロファイルグループの各プロファイルの情報を示します。

プロファイルグループ設定

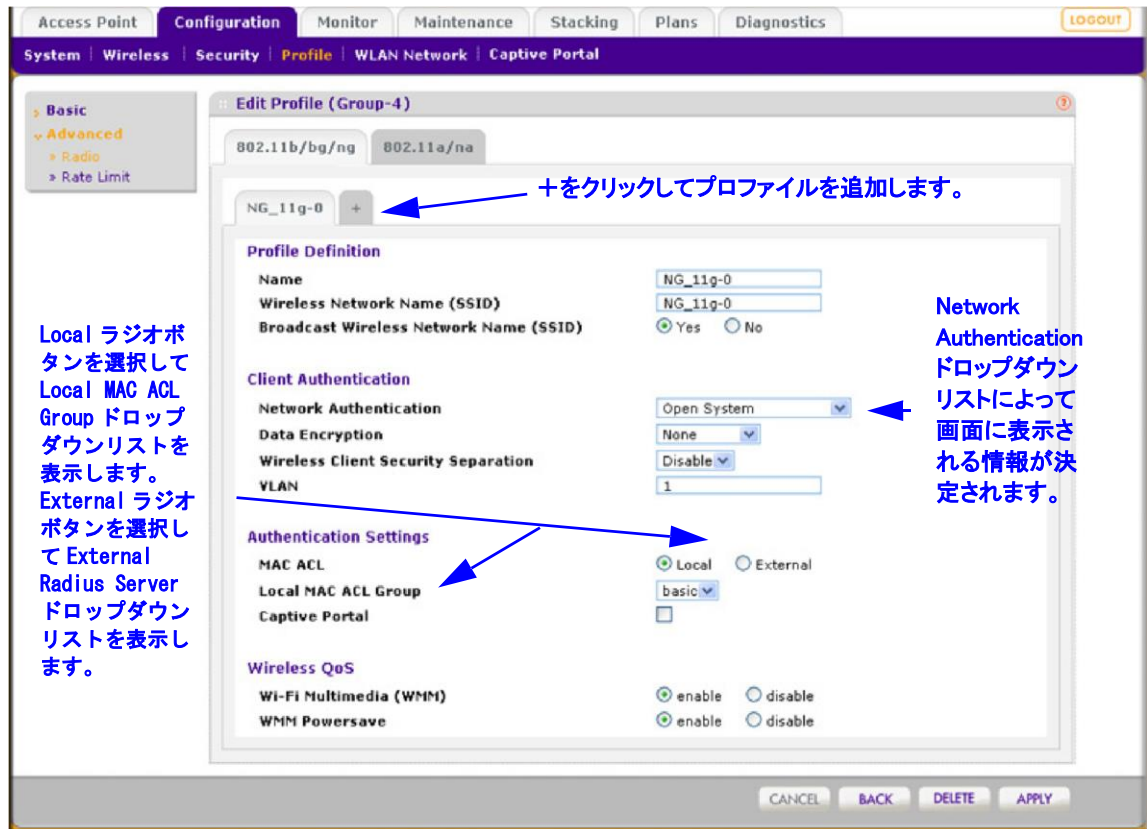
| 設定 | 説明 |
|----------------|-----------------------|
| Name | プロファイル名 |
| Radio | プロファイルの動作するワイヤレス電波モード |
| Authentication | プロファイルが動作している認証設定 |

2. +ボタンをクリックして追加のプロファイルグループを作成します。新しいプロファイルグループは advanced Profile Groups 画面に表示されます。デフォルトでは NG_11g-0 profile と NG_11a-0 プロファイルがプロファイルグループに設定されています。

メモ: デフォルトではプロファイルグループの名前は Group-1, Group-2, Group-3, ...となっています。プロファイルグループ名を変更することはできません。

3. Edit ボタンをクリックします。Advanced Edit Profile 画面が表示されます。

メモ: Network Authentication 欄の選択は Authentication Server 画面で指定した認証サーバー設定により異なります。Network Authentication 欄の選択が認証を必要とする場合、追加の欄が表示されます。



4. タブで電波を選択します。
5. 基本セキュリティプロファイル設定同様に設定をします。
6. **Apply** ボタンをクリックして設定を保存します。
7. 新しいプロファイルグループにプロファイルを追加します。
 - a. タブで電波を選択します。
 - b. + ボタンをクリックします。Add Profiles ポップアップウィンドウが表示されます。



- c. **Add** ボタンをクリックするか、既存のプロファイルをクローンするには、**Clone an existing Profile** チェックボックスを選択し、Profiles ドロップダウンリストからプロファイルを選択し、**Add** ボタンをクリックします。新しく作成されたプロファイルが画面に表示され、新しいプロファイルを設定できるように新しいプロファイルのタブが自動的に選択されます。
8. 基本セキュリティプロファイル設定同様に設定をします。
9. **Apply** ボタンをクリックして設定を保存します。

Edit and Remove Profiles from an Advanced Profile Group

拡張プロファイルグループのプロファイルを編集する

1. Profile Groups 画面でプロファイルグループのタブをクリックします。
2. **Edit** ボタンをクリックします。Edit Profile 画面が表示されます。
3. タブで電波を選択します。
4. タブでプロファイルを選択します。
5. 設定を変更します。
6. **Apply** ボタンをクリックして設定を保存します。

拡張プロファイルグループからプロファイルを削除する

1. Profile Groups 画面でプロファイルグループをクリックして選択します。
2. **Edit** ボタンをクリックします。Edit Profile 画面が表示されます。
3. タブで電波を選択します。
4. タブでプロファイルを選択します。
5. **Delete** ボタンをクリックし、削除を確認します。

拡張プロファイルグループの削除

拡張プロファイルグループを削除する

1. Profile Groups 画面でタブをクリックしてプロファイルグループを選択します。
2. **Delete** ボタンをクリックします。

メモ: プロファイルグループの編集はプロファイルの追加、削除、プロファイルの変更で行います。

基本と拡張プロファイルグループの管理

デフォルトではすべてのアクセスポイントは自動的に基本プロファイルグループに割り当てられます。この画面でアクセスポイントを他のプロファイルグループに割り当てることができます。

アクセスポイントをプロファイルグループに割り当てる

1. **Configuration > WLAN Network** を選択して WLAN Group Assignment 画面を表示します。



表示される設定は以下の表に示します。

WLAN Group Assignments

| 設定 | 説明 |
|----------|--|
| IP | アクセスポイントの IP アドレス |
| MAC | アクセスポイントの MAC アドレス |
| Model | アクセスポイントのモデル |
| Name | アクセスポイントの(設定した)名前 |
| Building | アクセスポイントが設置されているビル |
| Floor | アクセスポイントが設置されているフロア |
| Status | <p>アクセスポイントの接続状態</p> <ul style="list-style-type: none"> • Authentication in progress. (この状態が数分続くこともあります) • Applying configurations. • Firmware upgrade. • AP is rebooting. • Connecting. • Connected. (通常状態を示します) • Not Connected.: ワイヤレスコントローラーは設定された IP アドレスでアクセスポイントと通信できません。ワイヤレスコントローラーは毎分アクセスポイントにログインを試みます。エラーが一時的な場合は、状態は自動的に Connected に戻ります。エラーが長引く場合は、アクセスポイントの IP アドレスとネットワーク接続を確認してください。 <p>メモ: DHCP サーバーがネットワークで有効になっていることを確認してください。管理されたアクセスポイントは Connecting 状態のまま Connected 状態になりません。</p> |

| | |
|-----------|---|
| Remote AP | アクセスポイントのリモート、ローカルを示します。 <ul style="list-style-type: none">• Local: AP がローカルサイトに設置されています。• Remote: AP がリモートサイトに設置されています。 |
| Sentry | 見張りモード (Sentry mode) の状態を示します。 <ul style="list-style-type: none">• No: Sentry Mode が無効です。• Yes: Sentry Mode が有効です。 |

2. アクセスポイントをプロファイルグループに割り当てるには、Group Name ドロップダウンリストでプロファイルグループ名を選択します。追加やグループを指定するには前のセクションを参照してください。
3. **Apply** ボタンをクリックして設定を保存します。

7. 無線と QoS 設定

初期設定時に General Settings 画面で国や地域を設定します。位置と環境にもとづいてワイヤレスコントローラーはアクセスポイントの推奨無線設定を決定し、これらの設定をデフォルトとして管理されたアクセスポイントに送り込みます。アクセスポイントを設定する準備ができたなら、必要がなければデフォルト設定をそのまま使うことを推奨します。

基本と拡張無線と QoS 設定

どのようにしてネットワークを設定し、基本または拡張のどちらの設定モデルが最適であるかを決定することは重要です。どちらかに従えば、無線と QoS 設定のための同じ設定モデルを使うことは簡単です。

- **基本無線設定 (Basic wireless settings)** : 基本設定モデルを使うならば、以下の無線と QoS 設定が基本プロファイルグループのすべてのプロファイルに適用されます。
 - 基本電波オンオフスケジュール
 - 基本プロファイルのそれぞれの電波の基本無線設定
 - 基本電波管理
 - 基本プロファイルのそれぞれの電波のレートリミット(速度制限)
- **拡張無線設定 (Advanced wireless settings)** : 基本設定モデルを使うならば、作成したプロファイルグループごとに以下の無線と QoS 設定を別々に設定することができます。
 - 最大 8 つのプロファイルグループのための拡張電波オンオフスケジュール
 - 最大 8 つのプロファイルグループのための拡張電波設定
 - 最大 8 つのプロファイルグループのための拡張 QoS 設定
 - 最大 8 つのプロファイルグループのための拡張電波管理
 - 最大 8 つのプロファイルグループのそれぞれの電波のための拡張レートリミット(速度制限)
- **グローバル無線設定** : 以下の無線と QoS 設定は基本プロファイルおよび拡張プロファイルグループのすべてのプロファイルに適用されます。
 - 基本チャンネル割り当て
 - アクセスポイントの各モデルに対する基本ロードバランシング

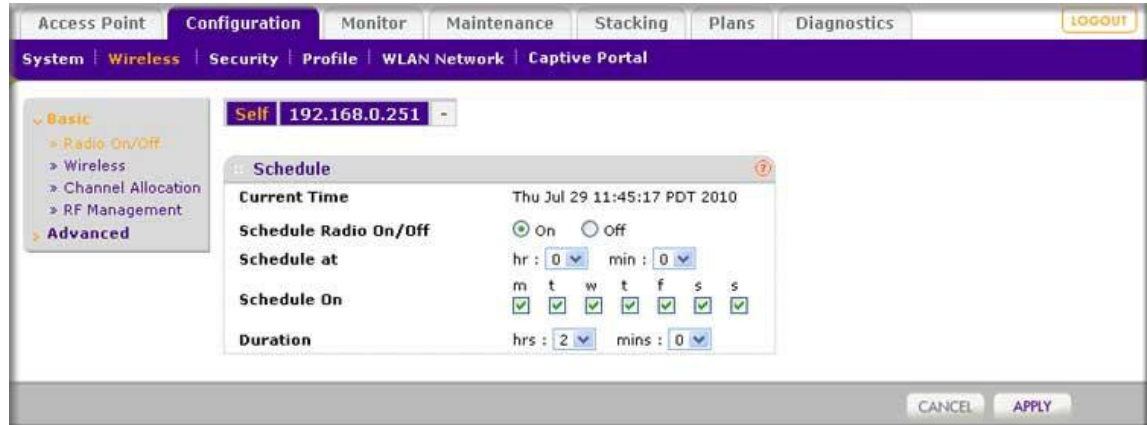
電波設定

電波オンオフは予定した休暇や工場閉鎖、夜や週末に使えるグリーン機能です。

基本電波設定

電波をスケジュールする

1. Configuration > Wireless > Basic > Radio On/Off を選択して Basic Schedule 画面を表示します。



2. 以下の表にしたがって設定をします。

電波オンオフスケジュール設定

| 設定 | 説明 |
|-----------------------|---|
| Current Time | ワイヤレスコントローラーの現在の時間を表示します。変更不可です。 |
| Schedule Radio On/Off | On: 指定した時間に電波をオンにします。 Off: 指定した時間に電波をオフにします。 |
| Schedule at | ドロップダウンリストで電波をオンまたはオフにする時間を設定します。 |
| Schedule On | スケジュール動作を行う曜日を選択します。 |
| Duration | オンまたはオフにする時間をドロップダウンリストで選択します。 |

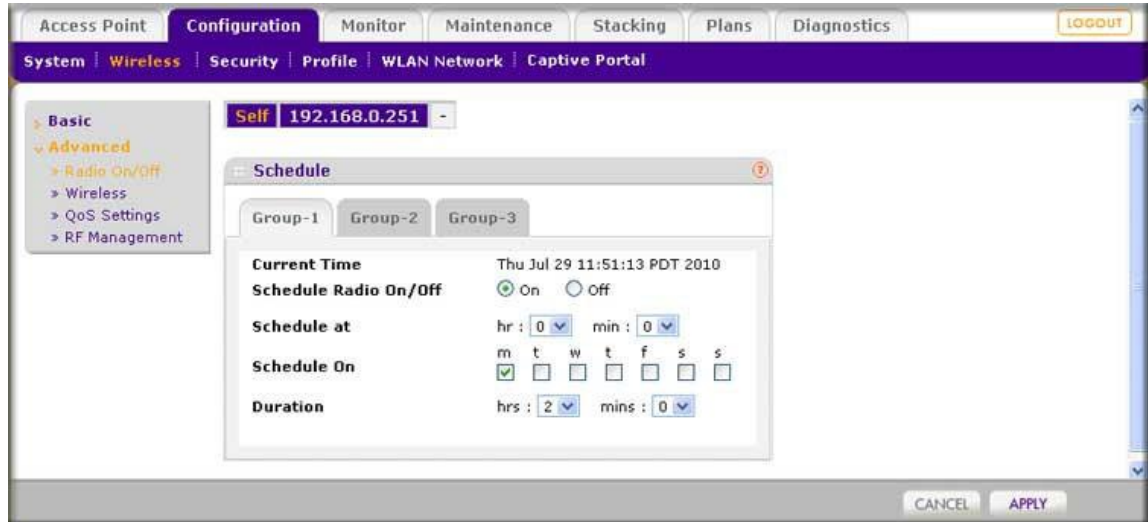
3. Apply ボタンをクリックして設定を保存します。

プロファイルグループのための拡張電波設定

プロファイルグループごとに電波スケジュールを設定することができます。

プロファイルグループの電波をスケジュールする

1. **Configuration > Wireless > Advanced > Radio On/Off** を選択して **Advanced Schedule** 画面を表示します。



2. タブでプロファイルグループを選択します。
3. 前の表に従い設定をします。
4. **Apply** ボタンをクリックして設定を保存します。

無線設定

一般的に、デフォルト無線設定を変更する必要はありません。無線電話機メーカーがデフォルトと異なる特定の設定を指定しているような特別な必要が有る場合は無線設定を変更します。基本プロファイルグループと拡張プロファイルグループの無線設定をすることができます。

基本無線設定

基本無線設定をする

1. **Configuration > Wireless > Basic > Wireless** を選択して **Basic Wireless Settings** 画面を表示します。

Access Point Configuration Monitor Maintenance Stacking Plans Diagnostics LOGOUT

System Wireless Security Profile WLAN Network Captive Portal

Self 10.110.2.92

Basic Wireless Settings

802.11b/bg/ng 802.11a/na

Turn Radio On

Wireless Mode 802.11ng

Data Rate Best

Channel Width 20/40 MHz Dynamic

Guard Interval 800 ns

RTS Threshold (0-2347) 2347

Fragmentation Length (256-2346) 2346

Beacon Interval (100-1000) 100

Aggregation Length (1024-65535) 65535

AMPSDU enable disable

RIFS Transmission enable disable

DTIM Interval (1-255) 3

Preamble Type Auto Long

High Density Bandwidth Auto High Low

| AP Name | Access Point Channel | Tx Power |
|---------------|----------------------|----------|
| netgearD44E88 | 10/2.457Ghz | Eighth |
| netgear9F3628 | 2/2.417Ghz | Half |
| netgearD448C8 | 1/2.412Ghz | Eighth |
| netgear848988 | 6/2.437Ghz | Eighth |

CANCEL APPLY

2. タブで電波を選択します。
3. Turn Radio On チェックボックスを選択して無線設定を有効にします。

メモ: Channel Allocation 画面で自動チャンネル設定が有効になっていると、Basic Wireless Settings 画面で無線設定をすることはできません。無線設定を変更するには自動チャンネル設定を無効にする必要があります。

メモ: アクセスポイントが 1 台もプロファイルグループに割り当てられていないと、無線設定をすることはできません。

4. 以下の表に従い設定をします。

無線設定

| 設定 | 説明 |
|--|---|
| Wireless Mode | <p>選択した電波モードによって選択肢は異なります。ド롭ダウンリストから無線モードを選択します。</p> <ul style="list-style-type: none"> • 802.11b/bg/ng モード <ul style="list-style-type: none"> - 11ng: デフォルト設定 - 11bg. - 11b. • 802.11a/na モード <ul style="list-style-type: none"> - 11na: デフォルト設定 - 11a <p>メモ: 802.11bg または 802.11b モードでは 802.11n および 802.11g 対応デバイスはアクセスポイントに接続できます。しかし、802.11ng モードを選択すると 802.11b 対応デバイスは接続できません。</p> |
| Data Rate | ド롭ダウンリストからワイヤレスネットワークの送信データレートを選択します。デフォルトは Best です。 |
| Channel Width (802.11n only) | ド롭ダウンリストからチャンネル帯域幅を選択します。広いチャンネル帯域幅はパフォーマンスを改善しますが、古いデバイスの中には 20MHz のみあるいは 40MHz のみで動作するものもあります。 |
| Guard Interval (802.11n only) | ド롭ダウンリストからガードインターバル値を選択します。短いガードインターバル値はパフォーマンスを改善しますが、古いデバイスの中には長いガードインターバルのみで動作するものもあります。 |
| RTS Threshold (0-2347) | RTS (Request To Send) スレッシュホールドパケットのサイズを指定します。RTS スレッシュホールドはパケットの送信メカニズム (CSMA/CA または CSMA/CD) と関連があります。もしもパケットサイズがこのスレッシュホールドと同じか小さいならば、データフレームは即時に送信されます。パケットサイズがそれよりも大きな場合は、実際のパケットデータを送信する前に送信端末は RTS スレッシュホールドパケットを受信端末に送信し、受信端末からの CTS (Clear To Send) パケットの受信するまで待ちます。 |
| Fragmentation Length (256-2346) | データパケットの最大フラグメンテーションパケット長を指定します。この辺りよりも大きなサイズのパケットは送信する前に小さなパケットに分割されます。フラグメンテーション長は 2 の倍数である必要があります。 |
| Beacon Interval (100-1000) | アクセスポイントがワイヤレスネットワークに同期するためのビーコン送信インターバルを指定します。 |
| Aggregation Length (1024-65535) (802.11n only) | AMPDU (Aggregated MAC Protocol Data Unit) パケットの最大長を指定します。大きな値はパフォーマンス向上につながります。アグリゲーションは高いスループットを達成するために使われるメカニズムです。 |

| | |
|----------------------------------|--|
| AMPDU (802.11n only) | On: 高いスループットを実現するために複数の MAC フレームを一つの大きなフレームにまとめます。 Off: 無効にします。 |
| RIFS Transmission (802.11n only) | On: RIFS(Reduced Interframe Space)を有効にします。 Off: RIFS(Reduced Interframe Space)を無効にします。 |
| DTIM Interval (1-255) | DTIM(Delivery Traffic Indication Message)インターバルを指定します。 |
| Preamble Type (802.11b/bg only) | プリアンブルタイプを選択します。 <ul style="list-style-type: none"> • Auto: 自動的に長短のプリアンブルを切り替えます。短い送信プリアンブルはパフォーマンスを向上します。Auto がデフォルト設定です。 • Long: 長い送信プリアンブルを有効にして、接続性の信頼性を上げ、範囲を少し大きくします。 |
| High Density Bandwidth | <ul style="list-style-type: none"> • High: RTS/CTS リトライを無効にします。 • Low: RTS/CTS リトライが有効になり、AP のセル範囲は向上します。 • Auto: 自動的に判断します。 |

5. チャンネルと送信出力を変更することもできます。

メモ: Basic RF Management 画面で Automatic Tx Power Control が有効にされていると、Basic Wireless 画面で送信出力を変更することはできません。変更するには Automatic Tx Power Control を無効にしてください。

Basic Wireless Settings 画面の表は基本プロファイルグループのプロファイルで管理されるアクセスポイントを示し、チャンネル割り当てと基本電波管理設定が適用されます。ドロップダウンリストでチャンネルと送信電力設定を変更します。

基本プロファイルグループチャンネルと送信電力設定

| 設定 | 説明 |
|----------------------|---|
| AP Name | アクセスポイント名 |
| Access Point Channel | <p>必要がある場合のみ変更してください。ドロップダウンリストでアクセスポイントが動作するチャンネルと周波数を選択してください。</p> <p>メモ: チャンネルを変更すると一時的にアクセスポイントのトラフィックに影響が出ることがあります。</p> <p>メモ: デフォルトではアクセスポイントのチャンネルと周波数は電波とプロファイルグループに有効にされているものに設定されます。次にチャンネルと周波数は最大のパフォーマンスを提供可能な値に変更されます。</p> |
| Tx Power | <p>ドロップダウンリストでアクセスポイントの送信電力を選択します。</p> <p>メモ: デフォルトではアクセスポイントの送信電力は Basic RF Management 画面で選択されたものに設定されます。</p> |

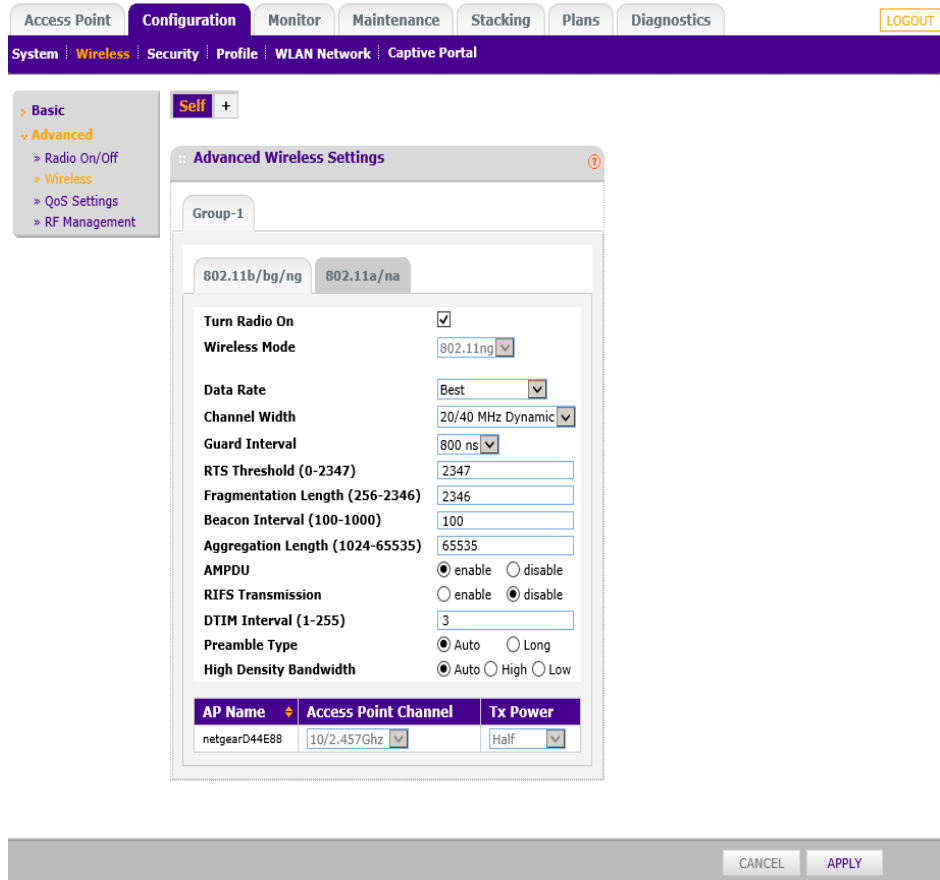
6. **Apply** ボタンをクリックして設定を保存します。

プロファイルグループの拡張無線設定

特別の理由がない限りデフォルト無線設定を使うことを推奨します。基本プロファイルグループと拡張プロファイルグループに対して無線設定をすることができます。

プロファイルグループの無線設定をする

1. **Configuration > Wireless > Advanced > Wireless** を選択して **Advanced Wireless Settings** 画面を表示します。



2. タブでプロファイルグループを選択します。
3. タブで電波を選択します。
4. **Turn Radio On** チェックボックスを選択して無線設定を有効にします。

メモ: Channel Allocation 画面で自動チャンネル設定が有効になっていると、Advanced Wireless Settings 画面で無線設定をすることはできません。無線設定を変更するには自動チャンネル設定を無効にする必要があります。

メモ: アクセスポイントが 1 台もプロファイルグループに割り当てられていないと、無線設定をすることはできません。

5. 基本無線設定を参照して設定をします。
6. チャンネルと送信出力を変更することもできます。

メモ: Advancec RF Management 画面で Automatic Tx Power Control が有効にされていると、Advanced Wireless Settings 画面で送信出力を変更することはできません。変更するには Automatic Tx Power Control を無効にしてください。

Advanced Wireless Settings 画面の表は選択されたプロファイルグループのプロファイルで管理されるアクセスポイントを示し、チャンネル割り当てと拡張電波管理設定が適用されます。ドロップダウンリストでチャンネルと送信電力設定を変更します。

拡張プロファイルグループ:チャンネルと送信出力設定

| 設定 | 説明 |
|----------------------|---|
| AP Name | アクセスポイント名 |
| Access Point Channel | <p>必要がある場合のみ変更してください。ドロップダウンリストでアクセスポイントが動作するチャンネルと周波数を選択してください。</p> <p>メモ: チャンネルを変更すると一時的にアクセスポイントのトラフィックに影響が出る場合があります。</p> <p>メモ: デフォルトではアクセスポイントのチャンネルと周波数は電波とプロファイルグループに有効にされているものに設定されます。次にチャンネルと周波数は最大のパフォーマンスを提供可能な値に変更されます。</p> |
| Tx Power | <p>ドロップダウンリストでアクセスポイントの送信電力を選択します。</p> <p>メモ: デフォルトではアクセスポイントの送信電力は Basic RF Management 画面で選択されたものに設定されます。</p> |

7. **Apply** ボタンをクリックして設定を保存します。

チャンネル設定



警告

デバッグやチャンネルに影響を与える深刻な事態以外ではチャンネル割り当て (Channel Allocation) を無効にしないでください。

自動チャンネル割り当て (Automatic channel allocation) は干渉を防ぐために管理されたアクセスポイント間でチャンネルを振り分けます。ワイヤレスコントローラーは設定されたセキュリティプロファイルに関係なく管理されたアクセスポイントにチャンネルを振り分けます。ワイヤレスコントローラーはアクセスポイントの最適なチャンネルを決定するために干渉、アクセスポイントのトラフィック量、近

隣のマップを検知します。コントローラーは過去 24 時間に収集されたこの情報を使ってアクセスポイントの最適なチャンネルを決定します。

チャンネル割り当てが動作するときに特定のチャンネルでチャンネル割り当てをするように設定できます。この機能によって管理ポリシーに従ったチャンネルのみをアクセスポイントが使うようにすることができます。

メモ: アクセスポイントの追加やネットワークを変更した時のように、ネットワークの管理状況が許すならば **Run Now** ボタンをクリックして直ちにチャンネルを割り当てることができます。チャンネル割り当てを実行するとネットワークの管理されたアクセスポイントのトラフィックに一時的に影響が出る場合があります。

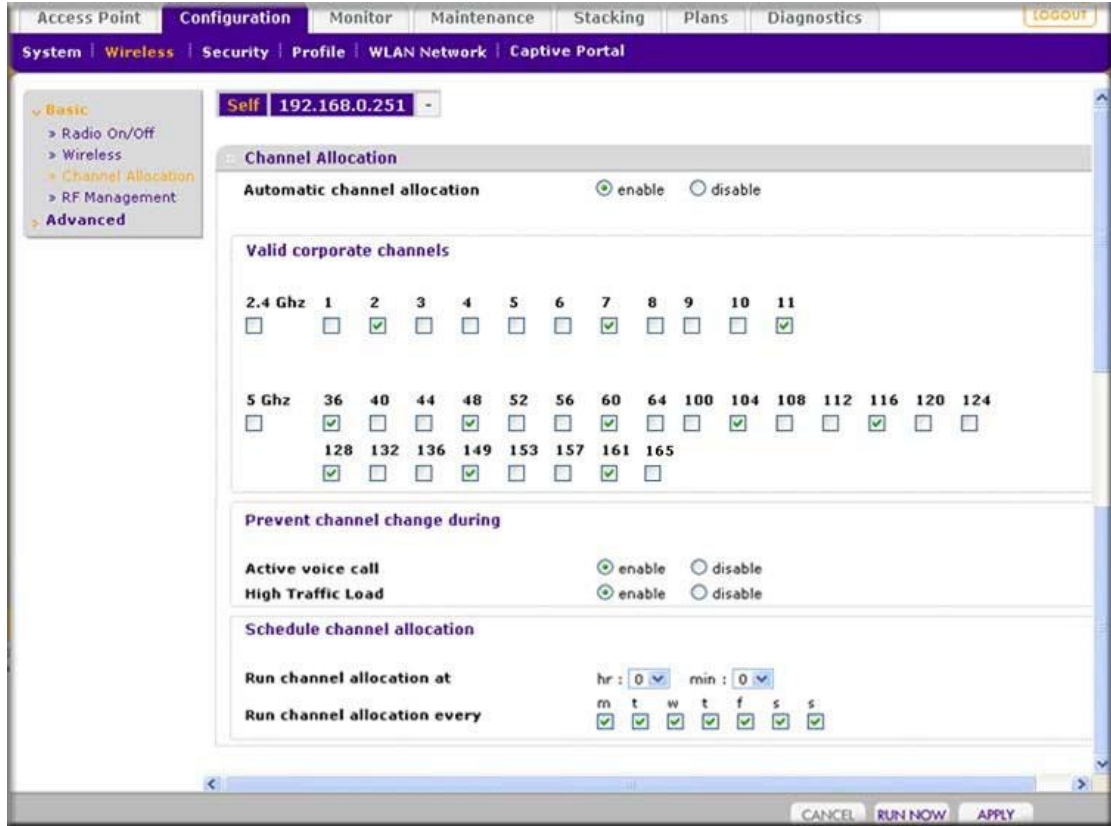
チャンネル割り当てを調整するときに最善の結果を得るために、以下を推奨します。

- チャンネルが重ならないように選択します。例えば、2.4GHz では 1,6,11 チャンネルを使います。
- 接続クライアント数が一番少ない時間にチャンネル割り当てをスケジュールします。これによって一日単位の有効な帯域管理を可能にします。

メモ: 割り当てられるチャンネルは基本プロファイルグループのプロファイルや拡張プロファイルのプロファイルにかかわらず、すべてのアクセスポイントに適用されます。

チャンネル割り当てを変更する

1. **Configuration > Wireless > Basic > Channel Allocation** を選択して **Channel Allocation** 画面を表示します。



- 以下の表に従い設定をします。
チャンネル割り当て設定

| 設定 | 説明 | |
|--|---|--|
| Automatic channel allocation | 通常は Enable ラジオボタンを選択してください。自動的に干渉を減少させるようにチャンネルを割り当てます。無効にするには Disable ラジオボタンを選択してください。 | |
| Valid corporate channels | 2.4 GHz または 5 GHz チェックボックスを選択して無線周波数帯を選択します。それぞれの周波数帯に対しては以下の通り。 <ul style="list-style-type: none"> • チェックボックスをクリアすることによって使用するチャンネルを除外することができます。医療環境で特定のチャンネルを使う機器との干渉を防ぐ良い方法です。 • 表示されていないチャンネルを追加することはできません。ワイヤレスコントローラーは設定された国・地域情報をもとに利用可能なチャンネルを決定しています。 | |
| Prevent channel change during メモ: 使用中で変更できなかった場合は次のチャンネル割り当ての際に再割り当てがされます。 | Active voice call | Enable: 音声通話中にチャンネル変更を防止します。 Disable: 音声通話中でもチャンネル変更をします。 |
| | High Traffic Load | Enable: トラフィック量が多いときにチャンネル変更を防止します。 Disable: トラフィック量が多いときでもチャンネル変更をします。 |
| Schedule channel allocation メモ: 一日一回接続クライアント数が最小になる時間帯にチャンネル割り当てを実行することを推奨します。 | Run channel allocation at | チャンネル割り当てを実行する時間をドロップダウンリストで選択します。 |
| | Run channel allocation every | チャンネル割り当てを実行する曜日をチェックボックスで選択します。 |

3. **Run Now** ボタンをクリックしてチャンネル割り当てを即時実行し、設定したチャンネルをアクセスポイントに適用することもできます。



警告

チャンネル割り当てを実行するとネットワークの管理されたアクセスポイントのトラフィックに一時的に影響が出ることがあります。

4. **Apply** ボタンをクリックして設定を保存します。

電波管理

Basic RF Management 画面で基本プロファイルグループに対して集中電波監理を設定することができます。拡張プロファイルグループを使っている場合は、Advanced RF Management 画面を使って各プロファイルグループに対して設定をすることができます。電波管理はクライアント、ユーザー

データトラフィック、アクセスポイントの近隣の電波環境に基づきアクセスポイントに対するチャンネル割り当てを最適化します。

ワイヤレスコントローラーは定期的に近隣の電波マップを確認し、近隣電波マップの変化やアクセスポイントのコントローラーへの接続断等を検知します。無線 LAN ヒーリング (WLAN healing) が使われる時、アクセスポイントがダウンしたり接続を失ったりすると、他のアクセスポイントがカバレッジホールを避けるために負担を分担します。そのために、他のアクセスポイントは送信出力を増加します。無線 LAN ヒーリングはセキュリティプロファイルグループ単位に設定され、セキュリティ設定を共通に持つアクセスポイント間で動作します。

ワイヤレスコントローラーは以下の機能を通して自動無線 LAN ヒーリング能力を持ちます。

- **自動チャンネル割り当て (Automatic channel allocation)** : フロアのアクセスポイント間で干渉を減少させるためにワイヤレスコントローラーがアクセスポイントのチャンネルを分散させます。自動チャンネル割り当てはアクセスポイントに最善のチャンネルを提供するために、フロアプラン、干渉、アクセスポイントのトラフィック量、近隣フロアマップやワイヤレスモードと帯域 (チャンネル幅) を考慮します。
- **自動送信出力調整** : 提供範囲要件にもとづきアクセスポイントの最適な送信出力を自動的に決定します。アクセスポイントは周辺をスキャンし、近隣のアクセスポイントの干渉、フロア間の漏洩、カバレッジホールを最小化するために電波環境を決定します。

無線 LAN ヒーリングを設定するときに、以下の点を推奨します。

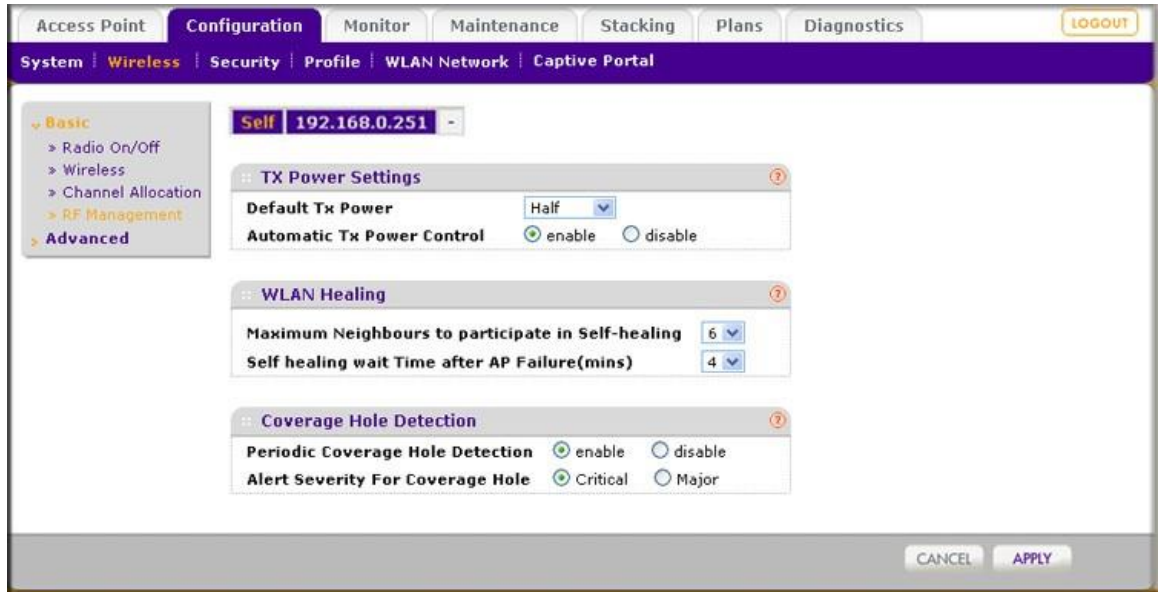
- 無線 LAN セルフヒーリング待機時間 (WLAN self-healing wait time) をアクセスポイント再起動時間、通常 1 分、よりも長くします。これによってアクセスポイントが再起動した時のゆらぎを許容します。
- 無線 LAN セルフヒーリングに参加する近隣 (AP) 数は大きくないもの (通常は 3, 4 台でほとんどの設置環境で十分です) にします。これによって 1 台の故障したアクセスポイントに対して多くのアクセスポイントが出力を増加することを防ぎます。

メモ: Basic Wireless Settings 画面で各アクセスポイントのデフォルト送信出力設定を変更することができます。

基本電波管理

基本電波管理を設定する

1. **Configuration > Wireless > Basic > RF Management** を選択して **RF Management** 画面を表示します。



2. 以下の表にしたがって設定をします。

RFManagement 設定

| 設定 | 説明 |
|--|---|
| TX Power Settings section | |
| Default Tx Power | ドロップダウンリストでアクセスポイントの送信 (Tx) 電力を選択します。Full, Half(1/2), Quarter(1/4), Eighth(8/1), Minimum. 自動送信電力制御を有効にすると、ドロップダウンリストの選択はアクセスポイントの初期設定となります。 |
| Automatic Tx Power Control | Enable: 自動送信出力制御を有効にします。 <ul style="list-style-type: none"> クライアントがアクセスポイントに低出力で接続しようとする時、アクセスポイントの送信出力は自動的にデフォルトレベルまで増加されます。 カバレッジエリアの重複(オーバーラップ)がある場合、アクセスポイントの送信出力はデフォルトレベルよりも低くなります。 Disable: 自動送信出力制御を無効にします。 |
| WLAN Healing section | |
| Maximum Neighbors to Participate in Self-healing | ドロップダウンリストで故障したアクセスポイントをカバーするために出力を増減する隣接のアクセスポイントの最大数を指定します。0 を選択すると、この機能を無効にします。近くのアクセスポイントを使い、すべてのアクセスポイントは使用しません。 |
| Self healing wait Time after AP Failure | ドロップダウンリストで故障したアクセスポイントが発生した時に故障を確認するまでの待機時間を選択します。アクセスポイントの再起動時間よりも長い時間、通常は 1 分、以上の値を設定します。この設定でアクセスポイントが再起動した時の電波のゆらぎを許容します。 |
| Coverage Hole Detection section | |
| Periodic Coverage Hole Detection | Enable: 定期的にバックグラウンドでのカバレッジホール検出を有効にします。 Disable: カバレッジホール検出を無効にします。 |

| | |
|----------------------------------|---|
| Alert Severity for Coverage Hole | Logs & Alerts 画面で Coverage-hole detection イベントのアラームレベルをラジオボタンで選択します。 ・ Critical ・ Major |
|----------------------------------|---|

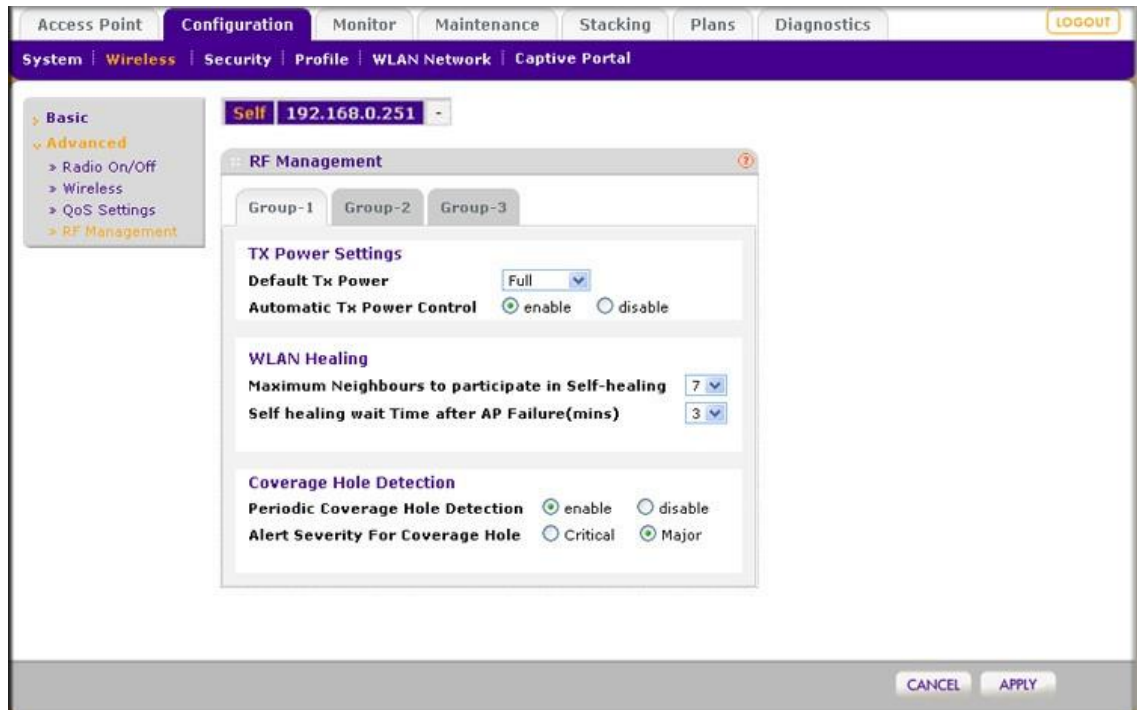
3. **Apply** を選択して設定を保存します。

プロファイルグループの拡張電波監理

Advanced RF Management 画面でプロファイルグループの集中電波管理の設定ができます。

拡張電波監理を設定する

1. **Configuration > Wireless > Advanced > RF Management** を選択して **Advanced RF Management** 画面を表示します。



2. タブをクリックしてプロファイルグループを選択します。
3. 以下の表にしたがって設定をします。

Advanced RFManagement 設定

| 設定 | 説明 |
|--|--|
| TX Power Settings section | |
| Default Tx Power | ドロップダウンリストでアクセスポイントの送信(Tx)電力を選択します。 Full, Half(1/2), Quarter(1/4), Eighth(8/1), Minimum. 自動送信電力制御を有効にすると、ドロップダウンリストの選択はアクセスポイントの初期設定となります。 |
| Automatic Tx Power Control | Enable: 自動送信出力制御を有効にします。 <ul style="list-style-type: none"> クライアントがアクセスポイントに低出力で接続しようとする、アクセスポイントの送信出力は自動的にデフォルトレベルまで増加されます。 カバレッジエリアの重複(オーバーラップ)がある場合、アクセスポイントの送信出力はデフォルトレベルよりも低くなります。 Disable: 自動送信出力制御を無効にします。 |
| WLAN Healing section | |
| Maximum Neighbors to Participate in Self-healing | ドロップダウンリストで故障したアクセスポイントをカバーするために出力を増減する隣接のアクセスポイントの最大数を指定します。0 を選択すると、この機能を無効にします。近くのアクセスポイントを使い、すべてのアクセスポイントは使用しません。 |
| Self healing wait Time after AP Failure | ドロップダウンリストで故障したアクセスポイントが発生した時に故障を確認するまでの待機時間を選択します。アクセスポイントの再起動時間よりも長い時間、通常は 1 分、以上の値を設定します。この設定でアクセスポイントが再起動した時の電波のゆらぎを許容します。 |
| Coverage Hole Detection section | |
| Periodic Coverage Hole Detection | Enable: 定期的にバックグラウンドでのカバレッジホール検出を有効にします。 Disable: カバレッジホール検出を無効にします。 |
| Alert Severity for Coverage Hole | Logs & Alerts 画面で Coverage-hole detection イベントのアラームレベルをラジオボタンで選択します。 <ul style="list-style-type: none"> • Critical • Major |

4. **Apply** ボタンをクリックして設定を保存します。

プロファイルグループの QoS 設定

QoS(Quality of Service)はデフォルトで動作しています。デバイスベンダー仕様が異なる設定を要求するような場合のときのみ、QoS 設定を変更します。

QoS WMM(Wi-Fi Multimedia)はより良いスループットとパフォーマンスを要求するアプリケーションに高い優先度(プライオリティ)の特別なキューを割り当てることを保証します。例えば、ビデオとオーディオアプリケーションは FTP のようなアプリケーションよりも高い優先度が与えられます。WMM は優先度の高い順に以下の 4 つのキューを定義しています。

- **Voice:** 低遅延の最優先のキュー、VoIP やストリーミングメディアに最適です。

- **Video:** 2 番目の優先度の低遅延キュー、ビデオアプリケーションはこのキューに割り当てられます。
- **Best Effort:** 中程度の遅延のメディアムキュー。ほとんどの IP アプリケーションはこのキューを使います。The medium priority queue with medium delay is given to this queue. Most standard IP applications use this queue.
- **Background:** 高スループットの低優先度キュー、遅延の影響は受けにくいが高いスループットを要求する FTP のようなアプリケーションはこのキューを使います。

ワイヤレスメディアアクセスの QoS 優先と連携は有効です。アクセスポイントの QoS 設定はアクセスポイントからクライアント方向のダウンストリームトラフィックとクライアントからアクセスポイントへのアップストリームトラフィックを制御します。

プロファイルグループの QoS を設定する

1. **Configuration > Wireless > Advanced > QoS Settings** を選択して **Advanced QoS Settings** 画面を表示します。

The screenshot shows the 'Advanced QoS Settings' configuration page. The interface includes a navigation menu on the left with 'Basic' and 'Advanced' sections. The 'Advanced' section is expanded to show 'Radio On/Off', 'Wireless', 'QoS Settings', and 'RF Management'. The main content area is titled 'Advanced QoS Settings' and shows 'Group-1' configuration. There are two tabs: '802.11b/bg/ng' and '802.11a/na'. Below the tabs are two tables: 'AP EDCA parameters' and 'Station EDCA parameters'.

| Queue | AIFS | cwMin | cwMax | Max Burst |
|----------------------|------|-------|-------|-----------|
| Data 0 (Best Effort) | 3 | 15 | 63 | 0 |
| Data 1 (Background) | 7 | 15 | 1023 | 0 |
| Data 2 (Video) | 1 | 7 | 15 | 3008 |
| Data 3 (Voice) | 1 | 3 | 7 | 1504 |

| Queue | AIFS | cwMin | cwMax | TXOP Limit |
|----------------------|------|-------|-------|------------|
| Data 0 (Best Effort) | 3 | 15 | 1023 | 0 |
| Data 1 (Background) | 7 | 15 | 1023 | 0 |
| Data 2 (Video) | 2 | 7 | 15 | 3008 |
| Data 3 (Voice) | 2 | 3 | 7 | 1504 |

2. タブでプロファイルグループを選択します。
3. タブで電波を選択します。

この画面でプロファイルグループ毎の QoS 設定と電波単位のダウンストリームトラフィックとアップストリームトラフィックの QoS 設定を変更することができます。これらの設定はこれらの設定を実行可能な管理されたアクセスポイントのみに適用されます。

WMM を無効にすると、アップストリームトラフィックの Station EDCA パラメーターの QoS 制御が無効になります。(Station EDCA パラメーター設定を変更することはできますが、WMM を有

効にするまで変更は反映されません。)しかし、WMMが無効になっているときに、ダウンストリームトラフィックのいくつかのパラメーターを設定することはできますが、これらの設定はWMMが無効になった時に反映されます。

4. 以下の表にしたがって設定をします Configure the settings as explained in the following table:

QoS settings

| 設定 | 説明 |
|------------|---|
| AIFS | データフレームの待機時間(ms)を指定します。有効な範囲は 1-255 です。 |
| CwMin | 初期のランダムバックオフ待機時間の上限時間(ms)を選択します。選択可能な値は 1, 3, 7, 15, 31, 63, 127, 255, 511, 1024 です。CwMin(Minimum Contention Window)値は CwMax (Maximum Contention Window)値よりも小さい値である必要があります。 |
| CwMax | ランダムバックオフ待機時間の上限時間(ms)を選択します。選択可能な値は 1, 3, 7, 15, 31, 63, 127, 255, 511, 1024 です。CwMax (Maximum Contention Window)値は CwMin(Minimum Contention Window)値よりも大きい値である必要があります。 |
| Max Burst | ワイヤレスネットワークで許容する最大バースト長(ms)を指定します。パケットバーストはヘッダー情報なしに送信される複数のフレームの集まりです。有効な値は 0.0~999.9 です。Maximum Burst Length は AP EDCA パラメーターのみに適用されます。 |
| TXOP Limit | TXOP(Transmission Opportunity) Limit 値を設定します。TXOP limit は Station EDCA パラメーターのみに適用され、クライアントが送信を開始できる最大時間を指定します。 |

5. **Apply** ボタンをクリックして設定を保存します。

ロードバランス設定

ロードバランス(Load balancing)ではアクセスポイントがアクセスポイント間でアクセスポイントのクライアントを分散させることができます。アクセスポイントモデルタイプと電波単位にロードバランスを設定できます。クライアントの最大数と信号強度の2つの基準があります。

- **Maximum number of clients:** アクセスポイントに最大クライアント数を越えるクライアントが接続しようとする、他のアクセスポイントに回されます。
- **Signal strength:** 信号強度は速度を決定します。多くのクライアントが近くにあり、一つのクライアントが遠くにある場合、遠くのクライアントへの送信時間は長過ぎます。そのクライアントは受信をしている間に待つこととなります。信号強度に 50%というようなパーセント値でスレッシュホールド(閾値)を設定することができます。

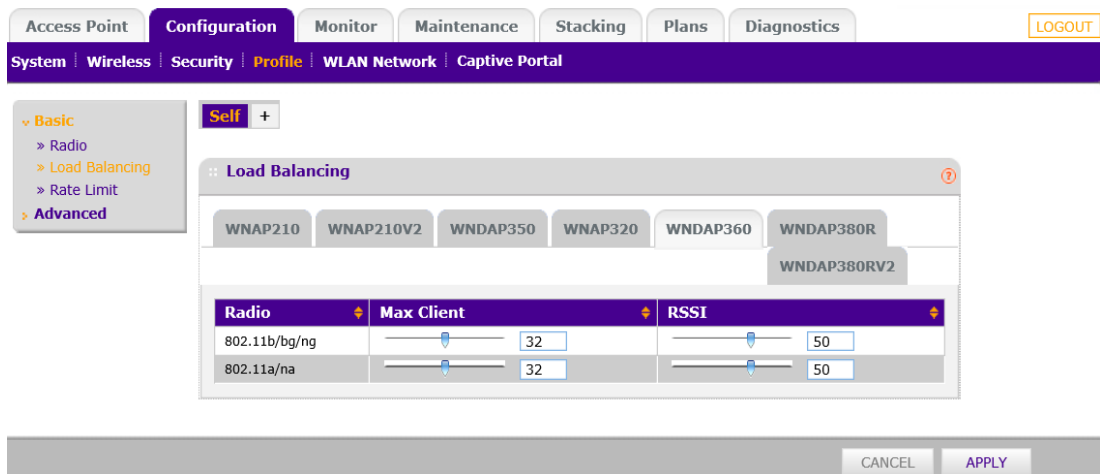
メモ: ロードバランス設定は基本プロファイルグループと拡張プロファイルグループのすべてのプロファイルに適用されます。

コントローラーは管理するアクセスポイントのロード(負荷)をバランスします。これはアクセスポイントに接続されるクライアント数とクライアントの信号品質にもとづきます。クライアントが(プローブ要求を使って)アクセスポイントを発見、あるいはアソシエーションフレームを送信した時、アクセスポイントは既に接続されているクライアント数とクライアントの信号品質にもとづいてクライアントを許可するかどうかを決定します。

- **クライアント数 (Number of clients)**: 複数のアクセスポイントが設置されていて、アクセスポイント間でクライアントを分散させたい時には、最大クライアント数を(オフィスやフロアの総クライアント数に比べて)低い値に設定します。
- **RSSI**: スループットへの期待が高く、アクセスポイントから近いクライアントをアクセスポイントに接続されたい時、RSSI(Received Signal Strength Indication)を高いパーセント値に設定します。クライアントがアクセスポイントから離れていて、クライアント数が少ない場合は、RSSI 値を低い値に設定します。

ロードバランスを設定する

1. **Configuration > Profile > Basic > Load Balancing** を選択して **Load Balancing** 画面を表示します。



2. タブで設定をするアクセスポイントのモデルを選択します。
3. 以下の表に従い設定をします。

Load-Balancing 設定

| 設定 | 説明 |
|------------|---|
| Max Client | 1 台のアクセスポイントの各電波に接続できる最大クライアント数をスライダーまたは数値を記入して設定します。最大 64 を設定可能です。 |
| RSSI | RSSI をスライダーまたは数値を記入して設定します。範囲は 0~100(%)です。0 はロードバランスの無効を意味します。 |

4. **Apply** ボタンをクリックして設定を保存します。

レートリミット設定

利用可能な帯域は送信中のエラーの数とパケットの送信キューでの滞在時間で決定されます。

プロファイルグループ内(基本プロファイルグループを含む)で各ワイヤレス電波(2.4GHz と 5GHz)のそれぞれにレートリミットを設定することができます。各プロファイルグループ内で合計 100%まで設定できます。

例えば、一つのプロファイルグループ内で 802.11b/bg/ng モードを使う 4 つのプロファイルと 802.11a/na モードを使う 2 つのプロファイルがある場合、802.11b/bg/ng モードを使う 4 つのプロファイルに一つのリートリミット設定、802.11a/na モードを使う 2 つのプロファイルにもう一つのリートリミット設定を作成することができます。802.11b/bg/ng モードを使う 4 つのプロファイルの合計パーセントと、同様に 802.11a/na モードを使う 2 つのプロファイルの合計パーセントはそれぞれ 100%を越えることはできません。

それぞれの管理されたアクセスポイント(または管理されたデュアルバンドアクセスポイントの各電波)で利用可能な帯域はプロファイルグループ内のプロファイル間で設定したパーセンテージで分散されます。一つのプロファイルに設定されたパーセンテージは接続されているすべてのクライアントで共有されます。

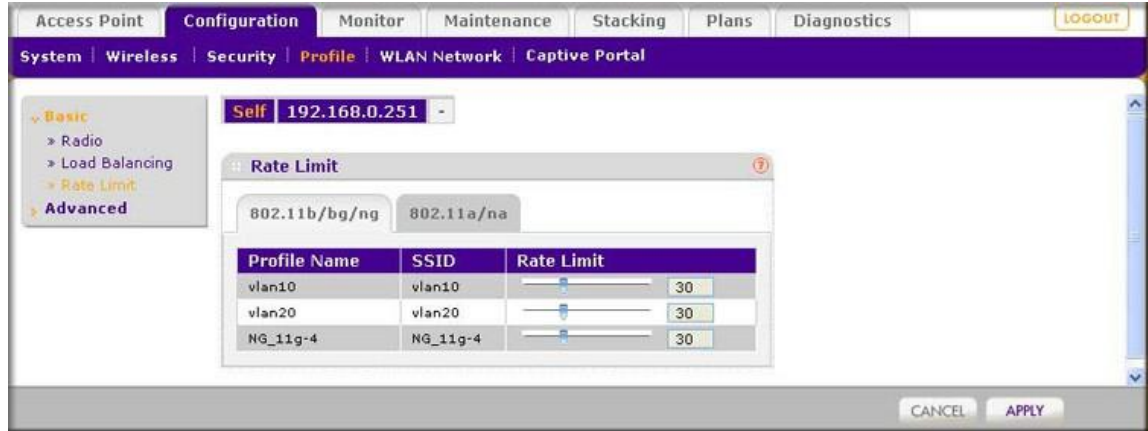
プロファイルにレートリミットを設定したくない場合は、設定を 0%にします。これでプロファイルのレートリミットを無効にします。0(%)設定はプロファイルが管理やテストのための場合は問題なく動作します。

基本レートリミット

基本プロファイルグループの各電波モード(802.11b/bg/ng モードと 802.11a/na モード)で、pro ファイルのレートリミットの合計は最大 100%まで設定可能です。各電波モードでタブがあります。

基本レートリミットを設定する

1. **Configuration > Profile > Basic > Rate Limit** を選択して **Basic Rate Limit** 画面を表示します。



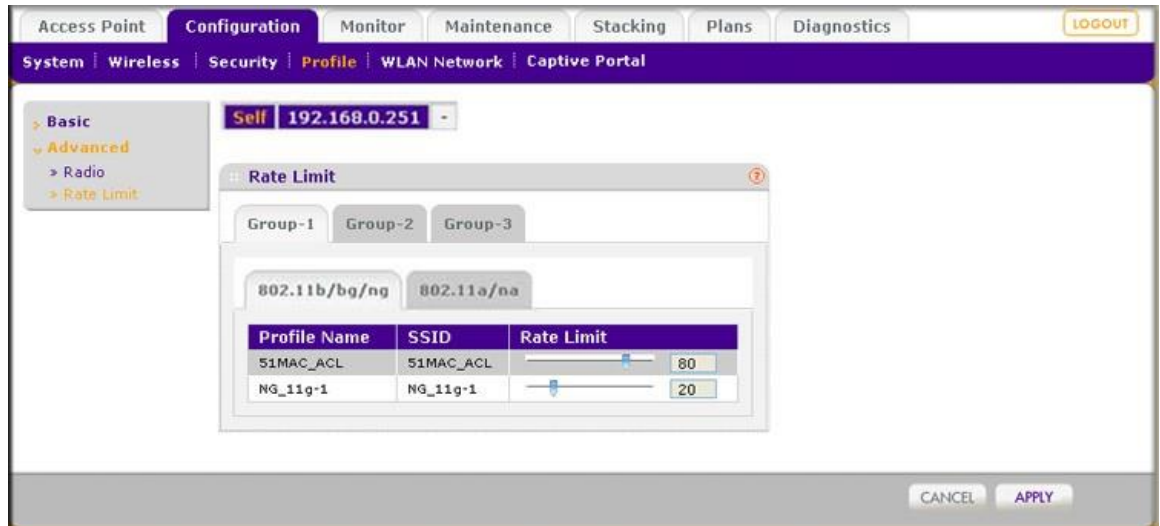
2. タブをクリックして電波を選択します。
3. 無線電波の各プロファイルでレートリミットをパーセンテージで設定します。スライダーまたは数値を入力して設定できます。
4. Apply ボタンをクリックして設定を保存します。

プロファイルグループの拡張レートリミット

各プロファイルグループおよび各電波モード(802.11b/bg/ng と 802.11a/na mode)で合計 100%までプロファイル単位のレートリミット設定可能です。各グループと各ワイヤレス電波モードにタブがあります。

拡張レートリミットを設定する

1. Configuration > Profile > Advanced > Rate Limit を選択して Advanced Rate Limit 画面を表示します。



2. タブでプロファイルグループを選択します。
3. タブで電波を選択します。

4. 選択したプロファイルグループの中の無線電波の各プロファイルグループでレートリミットを%で指定します。スライダーまたは値を記入して設定します。選択したプロファイルグループの一つの無線電波ですべてのプロファイルのパーセンテージの合計が 100%を超えないようにしてください。
5. **Apply** ボタンをクリックして設定を保存します。

8. ネットワークアクセスとセキュリティ設定



重要

ワイヤレスコントローラーでアクセスポイントに設定を送り込む前に、まずどのプロファイルとセキュリティが必要か？ 認証サーバーと MAC 認証を設定し、使う予定のあるプロファイルを設定します。



警告

もしもセキュリティが設定されていないまたは設定が不完全の場合にワイヤレスコントローラーがアクセスポイントに設定をプッシュすると、すべてのセキュリティを削除してすべてのネットワークがアクセス可能になることがあります。

基本と拡張セキュリティ設定について

基本セキュリティ設定モデル(Configuration > Security > Basic)は厳密には基本プロファイルグループに適用されるのではなく、拡張セキュリティ設定モデル(Configuration > Security > Advanced)は厳密には拡張プロファイルグループに適用されるのでもありません。理由は認証サーバーと MAC ACL をプロファイルグループではなく各プロファイルに適用するからです。

- **基本セキュリティ設定(Basic security settings)** : 次のセキュリティ設定を基本プロファイルグループと拡張プロファイルグループのどのプロファイルにも適用することができます。
 - 基本 MAC 認証(basic と呼ばれる MAC ACL グループ)
 - 基本認証サーバー(basic-Auth と呼ばれる RADIUS サーバーまたは basic-LDAP と呼ばれる LDAP サーバー)
- **拡張セキュリティ設定(Advanced security settings)** : 次のセキュリティ設定を基本プロファイルグループと拡張プロファイルグループのどのプロファイルにも適用することができます。
 - 拡張 MAC 認証(デフォルトで Acl-1, Acl-2, Acl-3... と呼ばれる MAC ACL であり、これらのデフォルト名を変更することは可能です)
 - 拡張認証サーバー(デフォルトで Autu-1, Auth-2, Auth-3... と呼ばれる RADIUS サーバー、デフォルト名を変更することは可能です)
- **グローバルセキュリティ設定(Global security settings)** : 次のセキュリティ設定は基本プロファイルグループと拡張プロファイルグループのどのプロファイルにも適用されます。
 - 基本不正 AP 検出(Basic rogue AP detection)
 - 拡張不正 AP 検出(Advanced rogue AP detection)

不正アクセスポイント管理

ワイヤレスコントローラーで不正アクセスポイント検出はデフォルトでは無効になっています。不正アクセスポイントを検出したいならば、不正アクセスポイント検出を有効にし、どのくらい積極的に不正アクセスポイントをスキャンするかを設定する必要があります。スキャンはアクセスポイントのサービス利用可能性に影響を与えます。不正アクセスポイント検出を aggressive に設定すると、アクセスポイントのスキャン頻度は高くなり、その間にはクライアントはアクセスポイントに接続することはできなくなります。

- アクセスポイントの BSSID(basic service set identifier)はどのアクセスポイントでも観測されません。
- 同じレイヤー2 のイーサネット側で送信しているアクセスポイントは管理されたアクセスポイントとして見えます。
- 最低一つのクライアントはアクセスポイントに接続されています。

上のすべての条件に一致しないどの管理されていないアクセスポイントはネイバー(neighbor)と分類されます。

アクセスポイントの電波がオフチャンネル(でスキャン中)の間、アクセスポイントはイーサネット上にフレームをブロードキャスト送信します。

メモ: 不正アクセスポイント検出の三角測量を動作させるためにアクセスポイントがフロアプラン通りに設置されていることを確認します。

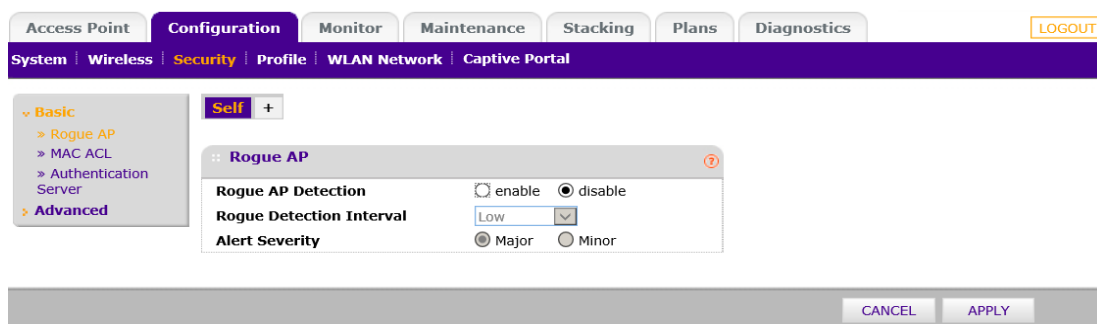
基本不正アクセスポイント検出設定

基本設定では一つの検出サーバーを設定し、拡張設定では複数の検出サーバーを設定します。

メモ: ネットワークでの長い遅延やクライアントがアクセスポイントから不意に切断されるようなときは不正アクセスポイント検出を無効にします。

不正アクセスポイント検出のためにサーバーを設定する

1. **Configuration > Security > Basic > Rogue AP** を選択して **Rogue AP** 画面を表示します。



ワイヤレスコントローラーは known(既知)と unknown(未知)を合わせて最大 512 台をリストでサポート可能です。

- 以下の表に従い設定をします。

基本不正 AP 検出設定

| 設定 | 設定 |
|--------------------------|--|
| Rogue AP Detection | <p>Enable ラジオボタンを選択して不正 AP 検出を有効にし、すべてのネイバーと不正アクセスポイントを表示可能にします。(ネイバーと不正を合わせて)最大 512 台のアクセスポイントをコントローラーで検出、維持できます。コントローラーはまた現在の不正アクセスポイント数と過去 24 時間に検出した不正アクセスポイント数を維持しています。</p> <p>外部ストレージが存在する場合は、不正アクセスポイント情報は 72 時間保存されません。</p> <p>不正 AP 検出を無効にするには Disable ラジオボタンを選択します。</p> |
| Rogue Detection Interval | <p>不正 AP 検出が有効になっている場合、検知周期をドロップダウンリストで選択します。</p> <ul style="list-style-type: none"> • Low: アクセスポイントが検出のためにオフチャンネルになる頻度は一番低くなっています。ほとんどの構成でうまく動作する Low 設定を推奨します。 • Medium. • High. • Aggressive: セキュリティに懸念がある場合は Aggressive を選択してスキャンの頻度を高めます。 |
| Alert Severity | <p>不正 AP 検出が有効で不正 AP を検出した時のアラームのレベルを設定します。Major または Minor をラジオボタンで選択します。</p> |

- Apply** ボタンをクリックして設定を保存します。

ネイバーと不正アクセスポイントはオフチャンネルスキャン時に検出されるので、ネイバーと不正アクセスポイントがリストに載るのには通常不正アクセスポイント検出を有効にしてから 10 分程度かかります。

メモ: 不正アクセスポイント検出が有効になるとアクセスポイントは断続的に短期間オフチャンネルになり、ネットワークパフォーマンスに影響を与えること

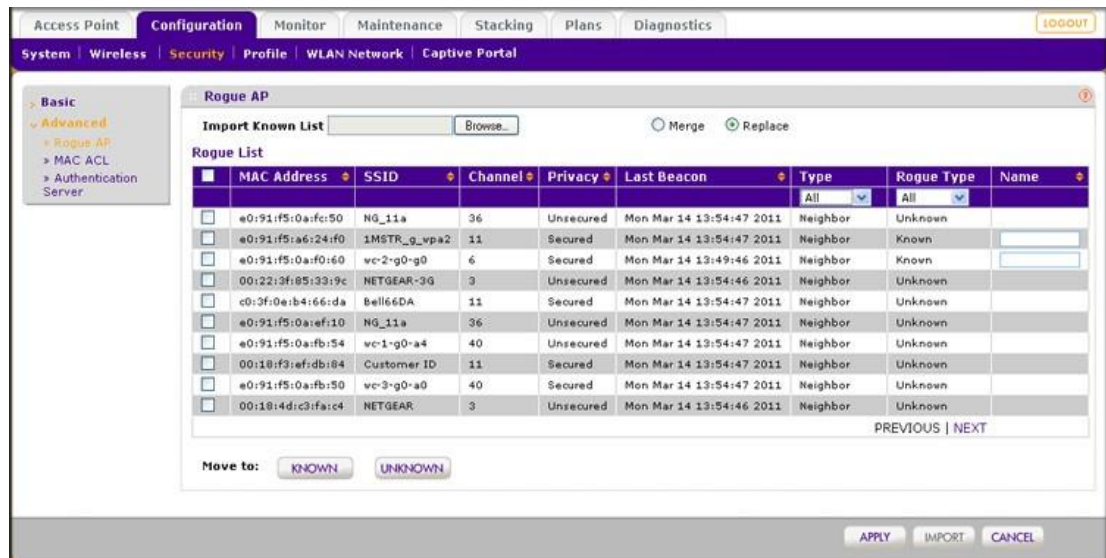
があります。セキュリティの懸念がネットワークパフォーマンスよりも重要であれば、High または Aggressive の不正アクセスポイント検出周期を一時的に選択できます。ネットワークパフォーマンスがセキュリティ懸念よりも需要ならば Low または Medium を選択します。通常的环境下では Low を推奨します。

拡張不正アクセスポイント検出設定

拡張不正 AP 画面は近隣のビジネスのアクセスポイントが既知かどうか判断することを可能にします。アクセスポイントを known あるいは unknown と識別して分類することによってワイヤレスコントローラーはそれらを発見、区分し続けることができなくなります。これによって管理すべきアクセスポイントと検出されるべき不正アクセスポイントを識別する助けになります。ネイバーは LAN 接続がなく、無線のみの接続があるアクセスポイントです。

拡張不正アクセスポイント検出を設定する

1. **Configuration > Security > Advanced > Rogue AP** を選択して **Advanced Rogue AP** 画面を表示します。



画面はすべての検出された不正アクセスポイントを直近のビーコンを含む重要な情報とともに Rogue List を表示しています。Rogue List をスクロールするには NEXT または PREVIOUS をクリックします。

ファイルからアクセスポイントのリストをインポートすることもできます。詳しくは次のセクションを参照してください。

2. **Rogue List** のアクセスポイントを分類します。
 - a. アクセスポイントのチェックボックスを選択します。
 - b. 次の 2 つのボタンのどちらかをクリックします。Rogue List の下にあります。

- **Known:** 選択したアクセスポイントを know list に移動します。Name 欄に名前を記入してアクセスポイントを識別しやすくすることができます。
- **Unknown:** 選択したアクセスポイントを unknown list に移動します。

3. **Apply** ボタンをクリックして設定を保存します。

Known アクセスポイントのリストのファイルからのインポート

保存したファイルから known アクセスポイントのリストをインポートすることができます。まず、各アクセスポイントの MAC アドレスを含むテキストファイルを作成します。このファイルは一行に 1 つの MAC アドレスが記述されているテキストファイルです。ワイヤレスコントローラーは known と unknown で合計 512 台のアクセスポイントをサポートすることができます。

アクセスポイントをファイルからインポートする

1. アクセスポイントの MAC アドレスのリストを含むテキストファイルを作成します。各 MAC アドレスはそれぞれ独立した行にあり、以下の例のように行間は強制改行されています。

```
00:00:11:11:22:29
00:00:11:11:22:28
00:00:11:11:22:27
00:00:11:11:22:26
00:00:11:11:22:25
```

2. **Configuration > Security > Advanced > Rogue AP** を選択して **Advanced Rogue AP** 画面を表示します。

The screenshot shows the 'Rogue AP' configuration page. The 'Import Known List' section is active, displaying a table of Rogue APs. The table has the following columns: MAC Address, SSID, Channel, Privacy, Last Beacon, Type, Rogue Type, and Name. The table contains 10 entries, all of which are currently unchecked. Below the table, there are buttons for 'Move to: KNOWN' and 'UNKNOWN', and 'APPLY', 'IMPORT', and 'CANCEL' buttons at the bottom right.

| | MAC Address | SSID | Channel | Privacy | Last Beacon | Type | Rogue Type | Name |
|--------------------------|-------------------|------------------|---------|-----------|--------------------------|-------------|------------|------|
| <input type="checkbox"/> | c0:8a:de:49:a6:8c | Wi2premium | 100 | Unsecured | Sat Jan 16 17:34:13 2016 | Neighbor AP | Unknown | |
| <input type="checkbox"/> | c0:8a:de:89:a6:8c | Wi2premium_club | 100 | Secured | Sat Jan 16 17:34:13 2016 | Neighbor AP | Unknown | |
| <input type="checkbox"/> | c0:8a:de:c9:a6:8c | au_Wi-Fi2 | 100 | Secured | Sat Jan 16 17:34:13 2016 | Neighbor AP | Unknown | |
| <input type="checkbox"/> | 04:a1:51:53:27:20 | BCWMNetgearJapan | 6 | Secured | Sat Jan 16 17:34:13 2016 | Neighbor AP | Unknown | |
| <input type="checkbox"/> | 04:a1:51:53:27:21 | BCWMFree | 6 | Secured | Sat Jan 16 17:34:13 2016 | Neighbor AP | Unknown | |
| <input type="checkbox"/> | 04:a1:51:53:27:22 | Vaucher1 | 6 | Secured | Sat Jan 16 17:34:13 2016 | Neighbor AP | Unknown | |
| <input type="checkbox"/> | 50:6a:03:ba:b6:ef | NETGEAR_EXT | 11 | Unsecured | Sat Jan 16 17:34:13 2016 | Neighbor AP | Unknown | |
| <input type="checkbox"/> | 00:1a:eb:3a:8a:11 | jnshare2 | 48 | Secured | Sat Jan 16 17:34:13 2016 | Neighbor AP | Unknown | |
| <input type="checkbox"/> | 04:a1:51:53:27:30 | BCWMNetgearJapan | 108 | Secured | Sat Jan 16 17:34:13 2016 | Neighbor AP | Unknown | |
| <input type="checkbox"/> | 04:a1:51:53:27:31 | BCWMFree | 108 | Secured | Sat Jan 16 17:34:13 2016 | Neighbor AP | Unknown | |

3. **参照**ボタンをクリックしてリストファイルを選択します。

4. **Import Known List** の右側のラジオボタンを選択します。

- **Merge:** 現在の Rogue List にマージします。
- **Replace:** Rogue List のリストをインポートするリストで置き換えます。

5. **Import** ボタンをクリックします。
6. **Apply** ボタンをクリックして設定を保存します。

MAC 認証と MAC 認証グループの管理

MAC 認証は外部または内部のクライアントの MAC アドレスの ACL(Access Control List)を設定して、ワイヤレスコントローラーが管理するアクセスポイントへのネットワークアクセス権限を許可したり拒否したりすることができます。設定は管理されたアクセスポイントのみに適用されます。

メモ: ワイヤレスコントローラーはローカル ACL では合計で 4096 の MAC アドレスをサポートできます。

外部 MAC 認証のガイドライン

外部 ACL を使う

1. 外部 RADIUS サーバーで ACL を設定します。
2. Edit Profile 画面の MAC ACL で **External** ラジオボタンを選択します。

The screenshot shows the configuration interface for a wireless LAN controller. The main menu includes 'Access Point', 'Configuration', 'Monitor', 'Maintenance', 'Stacking', 'Plans', 'Diagnostics', and 'LOGOUT'. The 'Configuration' menu is expanded to show 'System', 'Wireless', 'Security', 'Profile', 'WLAN Network', and 'Captive Portal'. The 'Profile' menu is further expanded to show 'Basic', 'Radio', 'Load Balancing', 'Rate Limit', and 'Advanced'. The 'Edit Profile(Basic)' window is open, showing the configuration for a profile named 'WNDAP36024G'. The 'Profile Definition' section includes fields for Name, Wireless Network Name (SSID), and Broadcast Wireless Network Name (SSID). The 'Client Authentication' section includes fields for Network Authentication (WPA-PSK), Data Encryption (TKIP), WPA Passphrase (Network Key), Wireless Client Security Separation (Disable), and VLAN (1). The 'Authentication Settings' section is highlighted with a red box, showing the 'MAC ACL' radio button selected as 'External'. The 'External RADIUS Server' field is set to 'basic-Auth'. The 'Wireless QoS' section includes fields for Wi-Fi Multimedia (WMM) and WMM Powersave, both set to 'enable'.

3. External Radius Server ドロップダウンリストで外部認証サーバーを選択します。

ワイヤレスコントローラーは最初のクライアント認証時に MAC ACL を問い合わせます。クライアントがローミングするときにはワイヤレスコントローラーはキャッシュした認証情報を使います。クライアントがアクセスポイントから切断された後に再接続を試みたとき、ワイヤレスコントローラーはサイド MAC ACL を問い合わせます。以下の RADIUS サーバーガイドラインに注意してください。

- 各 MAC 認証クライアントに対して RADIUS サーバーでポリシーを設定する必要があります。
- MAC 認証の最中にワイヤレスコントローラーは以下の情報を RADIUS サーバーに送ります。
 - xx:xx:xx:xx:xx:xx 形式の MAC アドレス
 - ユーザー名
 - calling station ID
- ワイヤレスコントローラーは RADIUS サーバーとの認証プロトコルとして CHAP を使います。
- 外部 RADIUS サーバーで MAC 認証または外部 RADIUS サーバーでネットワーク認証のどちらかを設定できますが、両方はできません。すなわち、外部 RADIUS サーバーで WPA, WPA2,あるいは WPA&WPA2 を設定すると、外部 MAC 認証を使うことはできません。内部 MAC 認証に限られます。

基本ローカル MAC 認証設定

小規模のネットワークで基本プロファイルグループのプロファイルで基本認証グループを使うことができます。しかし、基本プロファイルグループまたは拡張プロファイルグループのどのプロファイルにも基本 MAC 認証グループを割り当てることができます。

基本 MAC 認証を設定する

1. **Configuration > Security > Basic > MAC ACL** を選択して **MAC Authentication** 画面を表示します。

The screenshot shows the configuration interface for MAC Authentication. The breadcrumb navigation is Configuration > Security > Profile > WLAN Network > Captive Portal. The left sidebar shows the navigation tree with 'Basic' expanded to 'MAC ACL'. The main content area is titled 'MAC Authentication' and includes the following elements:

- Import MAC List from a file:** A text input field with a 'Merge' dropdown and a '参照...' button.
- Treat ACL as:** Radio buttons for 'Allow' and 'Deny' (selected).
- Selected Wireless Clients:** A table with columns for checkboxes and 'MAC Address'. It contains three entries: 00:00:11:11:22:29, 00:00:11:11:22:28, and 00:00:11:11:22:27. There are 'DELETE' and 'ADD' buttons above the table, and a 'MOVE' button between the two tables.
- Available Wireless Clients:** A table with columns for checkboxes and 'MAC Address', currently empty.
- Buttons:** 'CANCEL', 'APPLY', and 'IMPORT' buttons are located at the bottom right of the interface.

ファイルから MAC アドレスのリストをインポートすることもできます。以下のセクションを参照してください。

2. **Trust ACL as** 欄で以下のラジオボタンを選択します。
 - **Allow**: Selected Wireless Clients リストに MAC アドレスが載っているクライアントにネットワークアクセスが許可されます。
 - **Deny**: Selected Wireless Clients リストに MAC アドレスが載っているクライアントにネットワークアクセスは拒否されます。
3. 以下の方法の一つで Selected Wireless Clients リストにワイヤレスクライアントを追加します。
 - MAC Address 欄に MAC アドレスを入力し **Add** ボタンをクリックします。
 - Available Wireless Clients リストで MAC アドレスを選択して **Move** ボタンをクリックします。 Available Wireless Clients リストはアクセスポイント付近にあるワイヤレス端末を含むリストです。

Selected Wireless Clients リストから MAC アドレスを削除するには、削除する MAC アドレスのチェックボックスを選択して、**Delete** ボタンをクリックします。

メモ: ワイヤレスコントローラーは SSID あたり 256MAC アドレスをサポートしています。

4. **Apply** ボタンをクリックして設定を保存します。

ファイルから MAC リストをインポートする

保存したファイルから MAC アドレスをインポートできます。ファイルには 1 行に一つの MAC アドレスが記述されている必要があります。

ファイルから MAC リストをインポートする

1. MAC アドレスのリストを含むテキストファイルを作成します。各 MAC アドレスはそれぞれ独立した行にあり、以下の例のように行間は強制改行されています。

```
00:00:11:11:22:29
00:00:11:11:22:28
00:00:11:11:22:27
00:00:11:11:22:26
00:00:11:11:22:25
```

2. **Configuration > Security > Basic > MAC ACL** を選択して画面を表示します。

The screenshot shows the management interface for the ProSAFE Wireless LAN Controller. The navigation menu includes: Access Point, Configuration (selected), Monitor, Maintenance, Stacking, Plans, Diagnostics, and LOGOUT. The breadcrumb trail is: System | Wireless | Security | Profile | WLAN Network | Captive Portal. The left sidebar shows a tree view with Basic (selected), Rogue AP, MAC ACL (selected), Authentication Server, and Advanced. The main content area is titled 'Self + MAC Authentication'. It features an 'Import MAC List from a file' section with a 'Merge' dropdown and a '参照...' button. Below this is the 'Treat ACL as' section with radio buttons for 'Allow' and 'Deny' (selected). The 'Selected Wireless Clients' table has columns for checkboxes and 'MAC Address', with entries: 00:00:11:11:22:29, 00:00:11:11:22:28, and 00:00:11:11:22:27. A 'MOVE' button is positioned between the two tables. The 'Available Wireless Clients' table also has columns for checkboxes and 'MAC Address'.

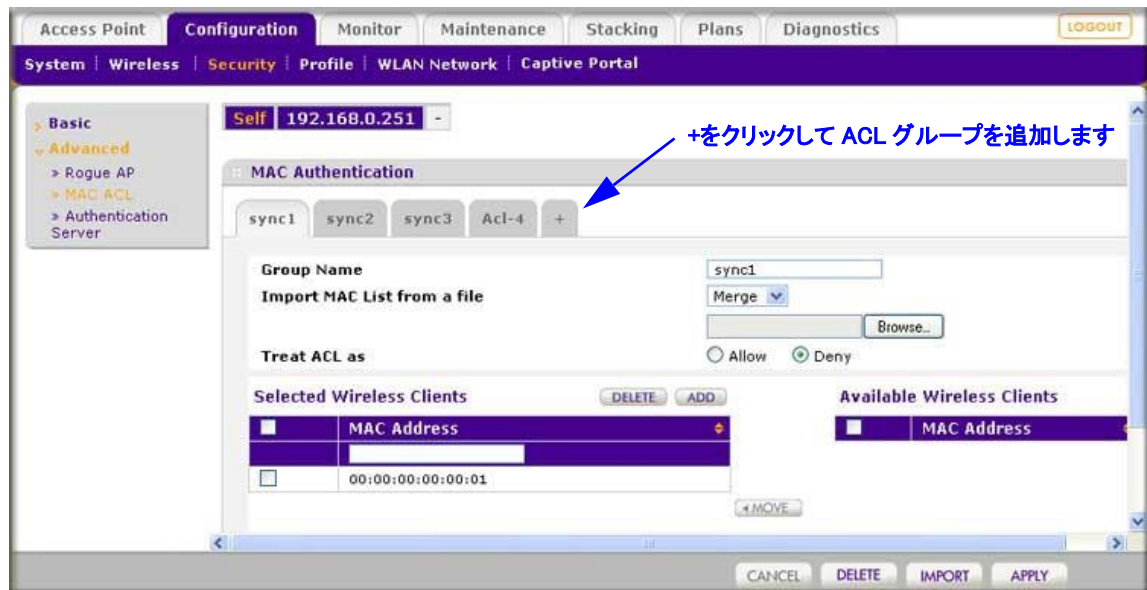
3. 参照ボタンをクリックして MAC アドレスを含むファイルを選択します。
4. Import MAC List のドロップダウンリストで選択します。
 - **Merge**: 現在の Selected Wireless Clients リストにマージします。
 - **Replace**: Selected Wireless Clients リストをインポートするリストで置き換えます。
5. **Import** ボタンをクリックします。
6. **Apply** ボタンをクリックして設定を保存します。

ローカル MAC 認証グループ設定

最大 8 つの MAC 認証グループ (MAC ACL) を作ってネットワークアクセスを許可、拒否することができます。どの MAC 認証グループ (基本 MAC 認証グループを含む) を基本プロファイルグループおよび拡張プロファイルグループに割り当てることができます。

MAC 認証グループを設定する

1. **Configuration > Security > Advanced > MAC Authentication** を選択して **Advanced MAC Authentication** 画面を表示します。



2. +ボタンをクリックして追加の ACL グループを作成します。新しい ACL グループが Advanced MAC Authentication 画面に表示され、新しい ACL のタブが自動的に選択されて新しいグループの設定ができます。

メモ: デフォルトでは ACL グループは Acl-1, Acl-2, Acl-3... となっています。ACL グループ名を変更することができます。

3. **Group Name** 欄に ACL グループ名を記入します。

4. Selected Wireless Clients リストを編集します。

メモ: ワイヤレスコントローラーは SSID1 つあたり最大 256MAC アドレスをサポートします。

5. Apply ボタンをクリックして設定を保存します。

ACL グループを削除するには、削除する ACL グループのタブを選択し、Delete ボタンをクリックします。

認証サーバーと認証サーバーグループ管理

3つのタイプの認証サーバーを指定することができます。内部、外部 RADIUS および外部 LDAP サーバーです。

- **内部認証サーバー (Internal authentication server)**: ワイヤレスコントローラーが認証を行います。この設定を選択すると、User Management 画面で Wi-Fi クライアントを設定します。
- **外部 RADIUS サーバー (External RADIUS server)**: 小規模のネットワークの基本プロファイルグループのプロファイルで使う基本外部 RADIUS サーバーを定義できます。Basic Authentication Server 画面(次のセクション参照)で設定をする必要があります。その結果プロファイルの設定をするときに認証オプションで選択することができます。拡張認証サーバー設定の一部として、通常多くのプロファイルを持つ多くの複雑なネットワークで使う複数の外部 RADIUS サーバーを定義することができます。次に異なる RADIUS サーバーを異なるプロファイルに割り当てます。

デフォルトでは、基本認証グループの外部 RADIUS サーバーは basic-Auth と呼ばれます。この名前を変更することはできません。デフォルトでは拡張認証サーバーの外部 RADIUS 認証サーバーは Auth1~auth8 と呼ばれ、これらの名前は変更することができます。Basic-Auth サーバーを拡張プロファイルグループに割り当てることができ、拡張認証グループの RADIUS サーバーを基本プロファイルグループに割り当てることができます。

- **外部 LDAP サーバー (External LDAP server)**: 1 台の外部 LDAP サーバー(通常 Active Directory サーバーと呼ばれます)を定義することができます。Basic Authentication Server 画面で設定をする必要があります。その結果プロファイル設定の際に認証オプションを選択することができます。

デフォルトでは基本認証グループの外部 LDAP サーバーは basic-LDAP と呼ばれます。この名前を変更することはできません。また、拡張認証グループで LDAP サーバーを設定することはできません。基本 LDAP サーバーを基本プロファイルグループと拡張プロファイルグループに割り当てることができます。

3つのすべてのサーバーがアクティブであることは可能で、設定するプロファイルは異なる認証サーバーと動作できます。例えば、ゲストプロファイルを認証無し、エンジニアリングプロファイルは外部 RADIUS 認証、マーケティングプロファイルは外部 LDAP 認証を使うことができます。

Authentication Server 画面の設定は Network Authenticaion ドロップダウンリストと Edit Profile 画面の Authentication Server 欄に影響を与えます。

基本認証サーバー設定

Basic Authentication Server 画面を使って内部認証サーバー、基本外部 RADIUS サーバー (Auth-basic と呼ばれる) と外部 LDAP サーバー (Auth-LDAP) を設定します。これらの認証サーバーの設定後、それらを基本プロファイルグループ、拡張プロファイルグループのどのプロファイルへも割り当てることができます。

基本認証サーバーを設定する

1. **Configuration > Security > Basic > Authentication Server** を選択して **Basic Authentication Server** 画面を表示します。
2. 設定する認証サーバーに対応するラジオボタンを選択します。
 - External RADIUS Server (外部 RADIUS サーバー)
 - Internal Authentication Server (内部認証サーバー)
 - External LDAP Server (外部 LDAP サーバー)
3. 選択した認証サーバーに対応する設定を以下の表に従って行います。

The screenshot shows the configuration page for the Basic Authentication Server. The 'External LDAP Server' radio button is selected. The configuration fields are as follows:

| Field | Value |
|-----------------------|----------------------|
| Server IP | 1.1.1.1 |
| Server Port | 389 |
| User Base DN | OU=idapusers,CN=var |
| Workgroup Name | varsalesdomain |
| Admin Domain | VAR SALES DOMAIN.LOC |
| Domain Admin User | admin |
| Domain Admin Password | ***** |

Authentication Server 設定

| 設定 | 説明 | |
|--------------------------------|-----------------------------------|---|
| External RADIUS Server | Primary Authentication Server | IP アドレス、ポート(デフォルトは 1812)と Shared Secret を指定します。 |
| | Secondary Authentication Server | IP アドレス、ポート(デフォルトは 1812)と Shared Secret を指定します。 |
| | Primary Accounting Server | IP アドレス、ポート(デフォルトは 1813)と Shared Secret を指定します。 |
| | Secondary Accounting Server | IP アドレス、ポート(デフォルトは 1813)と Shared Secret を指定します。 |
| | Reauthentication time (Seconds) | すべてのワイヤレスクライアントの再認証時間(秒)を指定します。 |
| | Update Global Key Every (Seconds) | チェックボックスを選択してグローバルキーの更新を有効にし、すべてのワイヤレスクライアントの再認証の時間(秒)を指定します。 |
| Internal Authentication Server | Reauthentication Time (seconds) | すべてのワイヤレスクライアントの再認証時間(秒)を指定します。 |
| | Update Global Key Every (seconds) | チェックボックスを選択してグローバルキーの更新を有効にし、すべてのワイヤレスクライアントの再認証の時間(秒)を指定します。 |
| External LDAP Server | Server IP | 外部 AD(Active Directory) サーバーの IP アドレスを指定します。 |
| | Server Port | 外部 AD(Active Directory) サーバーのポートを指定します。デフォルトは 389 です。 |
| | User Base DN | AD サーバーでのユーザーベース DN(Distinguished Name)を指定します。 |
| | Workgroup Name | AD サーバーでのワークグループ名を指定します。 |
| | Admin Domain | AD サーバーでの管理ドメイン(administrative domain)を指定します。 |
| | Domain Admin User | 管理ドメインでのユーザー名(user name)を指定します。 |
| | Domain Admin Password | 管理ドメインのパスワードを指定します。 |

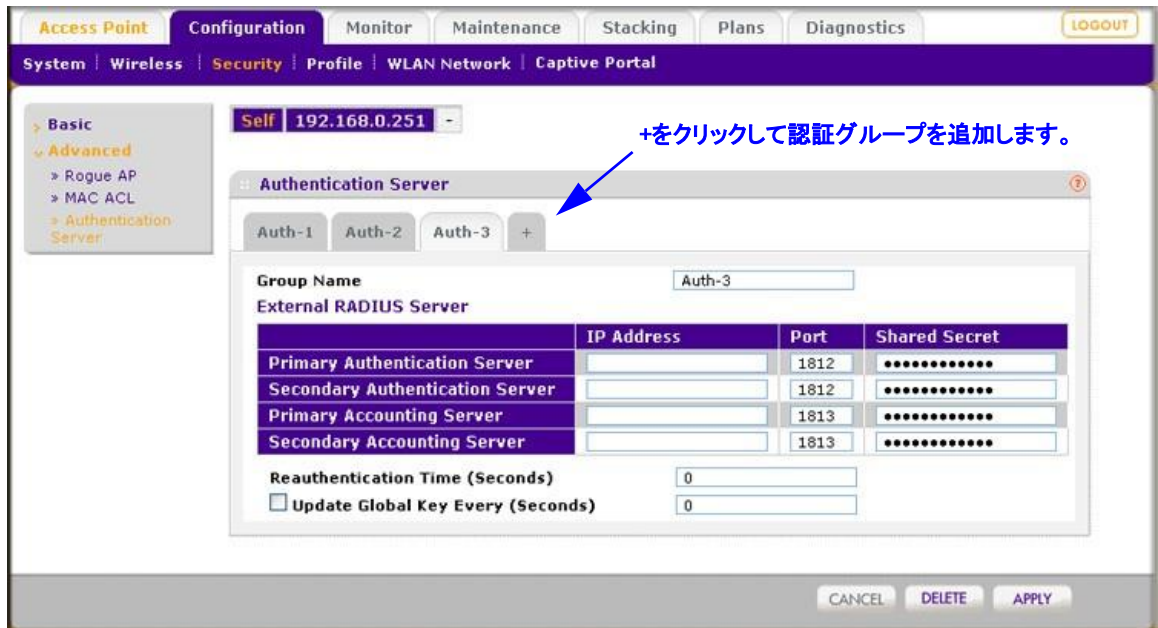
4. Apply ボタンをクリックして設定を保存します。

RADIUS 認証サーバーグループ設定

最大 8 つの外部 RADIUS サーバーを作成して異なるユーザーグループの認証をすることができます。これらの認証サーバーを設定した後、基本 RADIUS サーバーを含むどのサーバーでも基本プロファイルグループと拡張プロファイルグループのプロファイルに割り当てることができます。

RADIUS 認証グループを設定する

1. **Configuration > Security > Advanced > Authentication Server** を選択して **Advanced Authentication Server** 画面を表示します。



2. +ボタンをクリックして追加の認証グループを作成します。Advanced Authentication Server 画面に新しい認証グループが表示され、新しい認証グループのタブが自動的に選択されて新しいグループの設定ができます。

メモ: デフォルトでは認証グループの名前は Auth-1, Auth-2, Auth-3...となっています。認証グループ名を変更することができます。

3. Group Name 欄に認証グループ名を入力します。
4. 基本認証サーバー設定の外部 RADIUS サーバー設定部分の説明を参照して設定をします。
5. **Apply** ボタンをクリックして設定を保存します。

認証グループを削除するには、タブを選択してから **Delete** ボタンをクリックします。

ゲストネットワーク管理

管理者権限 (admin) を持つユーザー、例えば受付担当者やホテルの受付係、はゲストを提供することができます。ゲストはメールアドレス、あるいはメールアドレスとパスワードを提供する必要があります。後半のゲストはキャプティブポータルユーザーと呼ばれ、そのためにキャプティブポータルとキャプティブポータルユーザー資格を設定する必要があります。

キャプティブポータル設定

キャプティブポータル認証は通常ホットスポットユーザーとインターネットアクセスを購入する課金ユーザーのために使われます。ワイヤレスコントローラーでただ一つキャプティブポータルを設定することができます。

キャプティブポータルを設定するとき、ワイヤレスコントローラーをローアリア認証サーバーとして使うか、外部 RADIUS サーバーを認証のために設定することができます。2 つのタイプのポータル設定があります。

- **ゲストポータル (Guest portal)** : すべてのワイヤレスユーザーがメールアドレスを提供することによってネットワークにアクセス可能とする場合にこのポータルを使います。これらのユーザーにはユーザー名とパスワードを定義する必要はありません。
- **キャプティブポータル (Captive portal)** : ネットワークにアクセスする前にワイヤレスユーザーがログイン名とパスワードを提供する必要がある場合にこのポータルを使います。これらのユーザーのためにユーザー名とパスワードを定義する必要があります。

メモ: ネットワーク認証に外部 RADIUS サーバーを使っている場合、キャプティブポータルを設定することはできません。すなわち、WPA, WPA2, WPA&WPA2 で外部 RADIUS サーバーを設定すると、キャプティブポータル認証を設定できません。ネットワーク認証は Open System, Shared Key, WPA-PSK, WPA2-PSK, or WPA-PSK & WPA2-PSK となります。

外部 RADIUS サーバーを使ってキャプティブポータルユーザー認証と課金のための以下のガイドラインに注意してください。

- Basic-Auth RADIUS サーバーまたは拡張認証グループの RADIUS サーバーを使うことができます。外部 LDAP サーバーを使うことはできません。
- ワイヤレスコントローラーは CHAP または MS-CHAP を認証サーバーとの認証に使います。
- 以下の RADIUS 認証変数がワイヤレスコントローラーでサポートされています。
 - User-Name
 - User-Password
 - WISPr-Session-Terminate-Time
 - Session-Timeout

これらの変数をワイヤレスクライアントがアクセスポイントから切断する前に変更すると、新しい値はワイヤレスコントローラーでは更新されません。

- ワイヤレスコントローラーは管理されているアクセスポイントに対してプロキシ-RADIUS クライアントとして機能するので、管理されているアクセスポイントは外部 RADIUS サーバーに対して課金情報を送信することができます。以下の RADIUS 課金変数がワイヤレスコントローラーでサポートされています。

- Acct-Input-Octets
- Acct-Output-Octets
- Acct-Input-Gigawords
- Acct-Input-Gigawords

キャプティブポータルを設定する

1. Configuration > Captive Portal を選択して Portal Settings 画面を表示します。

The screenshot displays the 'Captive Portal' configuration page. At the top, there are navigation tabs: 'Access Point', 'Configuration' (selected), 'Monitor', 'Maintenance', 'Stacking', 'Plans', and 'Diagnostics'. Below these are sub-tabs: 'System', 'Wireless', 'Security', 'Profile', 'WLAN Network', and 'Captive Portal'. A 'LOGOUT' button is in the top right corner. The main content area shows a 'Basic' configuration pane with a 'Self +' button. The 'Portal Settings' window is open, showing:

- Portal Type:** Guest, Captive
- Radius Server:** Local, External, dropdown menu set to 'basic-Auth'
- Select Placement:** Three preview boxes showing the portal's appearance. Below them are radio buttons for Center, Bottom, and Top.
- Load Background Image (gif,jpg,bmp):** A text input field with a '参照...' (Browse) button.
- EULA:** A section with a checkbox for 'Eula Text Required' which is currently unchecked.

 At the bottom of the configuration area, there are three buttons: 'CANCEL', 'PREVIEW', and 'APPLY'.

2. 以下の表にしたがって設定をします。

Portal settings

| 設定 | 説明 |
|---|---|
| Portal Settings section | |
| Portal Type | 以下のラジオボタンから選択します。 <ul style="list-style-type: none"> • Guest: メールアドレス入力欄を持つゲストポータル。パスワードは不要でネットワークに非制限にアクセスできます。ゲストアカウントを設定する必要はありません。 • Captive: ログインユーザー名とパスワード欄を持つキャプティブポータル。このオプションを選択すると、RADIUS サーバーラジオボタンとドロップダウンリストが表示されます。 |
| Radius Server メモ : キャプティブポータル のみの設定です。 | 以下のラジオボタンから選択します。 <ul style="list-style-type: none"> • Local: ローカル認証サーバーを使います。 • External: ドロップダウンリストから外部認証サーバーを選択します。 |
| Select Placement | ログイン画面でのログインプロンプトの表示位置を設定します。 Center, Bottom, Top から選択します。 |
| Load Background Image | 参照 ボタンをクリックしてログイン画面の背景画像を選択することができます。Gif, jpg, bmp 形式を使うことができます。 |
| EULA section | |
| EULA Text Required | ライセンス表示をする場合にこのチェックボックスを選択し、ライセンス表示分を記入します。 |

3. **Apply** ボタンをクリックして設定を保存します。
4. **Preview** ボタンをクリックしてポータル設定を表示することができます。キャプティブポータルのデフォルト URL は http://192.168.0.250/guest_access/index.php です。コントローラーの IP アドレスを変更した場合は、192.168.0.250 のかわりにコントローラーの IP アドレスを使います。

ユーザー、アカウント、パスワード管理

ワイヤレスコントローラーは管理ユーザー、キャプティブポータルユーザー、Wi-Fi クライアントの 3 つのタイプのユーザーをサポートします。これらのすべてのユーザーはワイヤレスコントローラーの Web 管理インターフェース、またはワイヤレスネットワークにアクセスするためにワイヤレスコントローラーの内部認証サーバーに認証されるためにログイン名とパスワードを提供する必要があります。

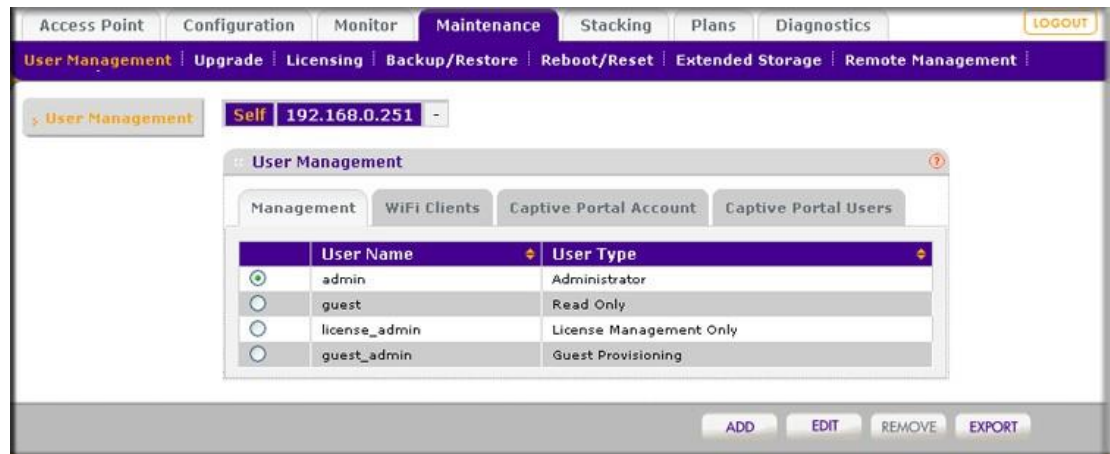
- **管理ユーザー (Management users)**: これらのユーザーはワイヤレスコントローラーの Web 管理インターフェースにアクセスします。これらには 4 つのグループがあります。
- **Administrators**: 読み書き権限のある管理ユーザー (admin)。ワイヤレスコントローラーの設定を変更することができます。
- **Read-only**: ワイヤレスコントローラーの Web 管理インターフェースにアクセスはできるが、Monitor と Help タブのみにアクセスができます。ワイヤレスコントローラーの設定を変更することはできません。

- **Guest provisioning:** キャプティブユーザーのみを作成可能、すなわち Maintenance タブ配下の User Management 設定タブのみにアクセス可能。
- **License management only:** ライセンスのみを設定可能、すなわち Maintenance タブ配下の Licence 設定タブのみアクセス可能。
- **Captive portal users:** キャプティブポータルにアクセス可能な権限を持つユーザー、一時的あるいは期限なしにアクセスできる。
- **Wi-Fi clients:** ワイヤレスネットワークにアクセス可能な権限を持つユーザー。これらのユーザーはワイヤレスネットワークにアクセスするためにキャプティブポータルやゲストポータルを使う必要はなく、アクセスの期限はありません。

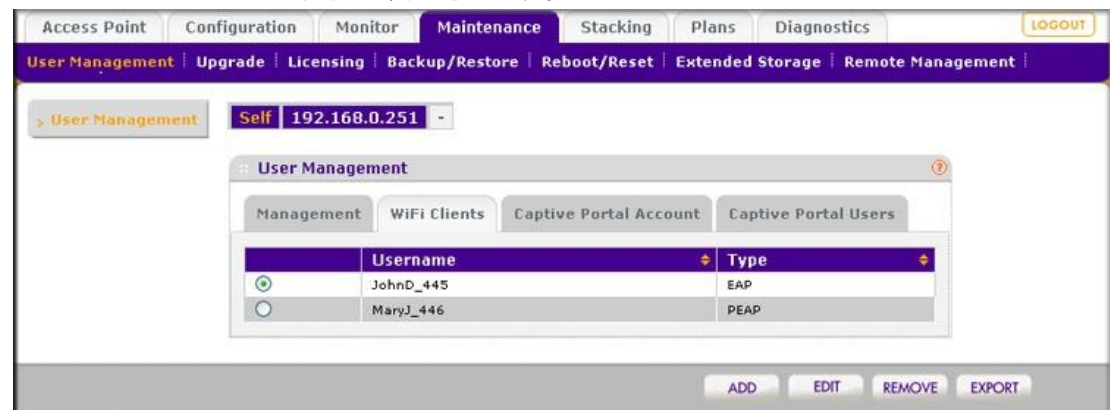
ユーザーに加えてキャプティブポータルユーザーとの組み合わせで使うキャプティブポータルアカウントを設定することができます。アカウントはワイヤレスアクセスが可能な時間を指定し、課金の金額を指定します。

ユーザーまたはアカウントを追加する

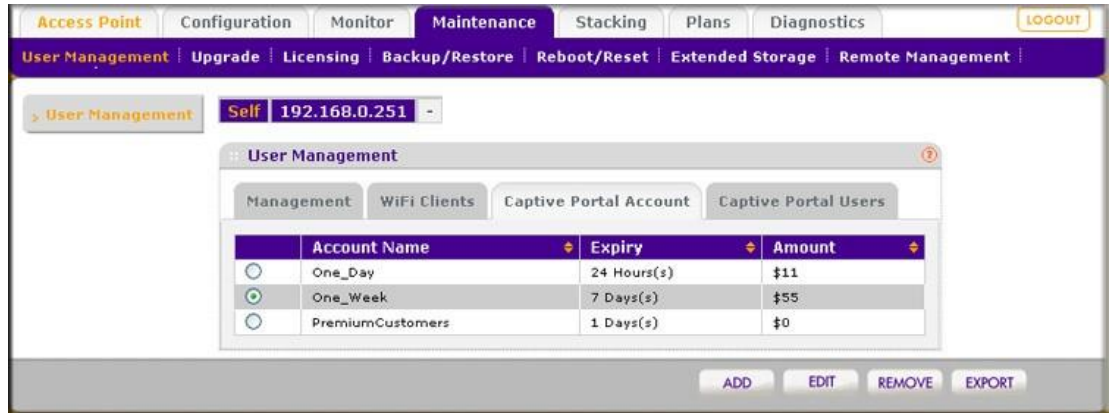
1. **Maintenance > User Management** を選択して **User Management** 画面を表示します。
2. **User Management** 配下の以下のタブを選択して還元する画面を表示します。
 - **Management:** Management 画面が表示されます。(Maintenance > User Management を選択した時のデフォルト画面です。)



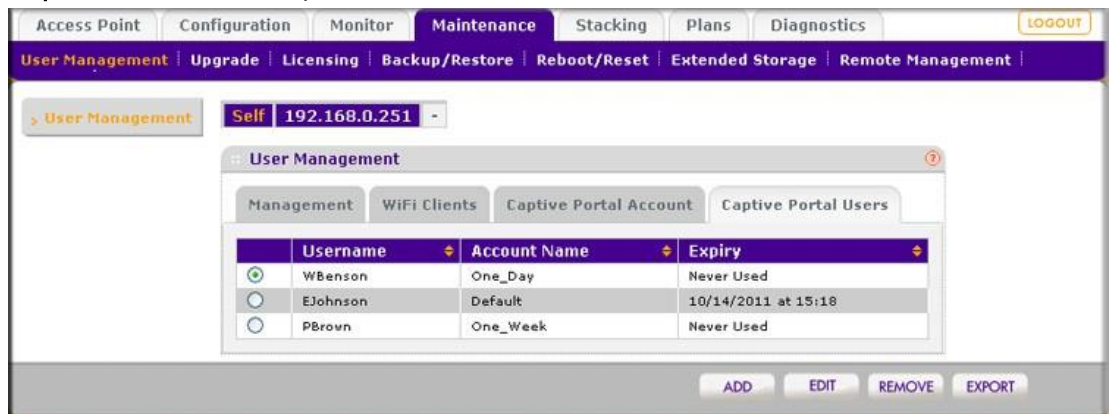
- **WiFi Clients:** WiFi Client 画面が表示されます。



- **Captive Portal Account:** Captive Portal Account 画面が表示されます。





- **Captive Portal Users:** Captive Portal Users 画面が表示されます。



3. **Add** ボタンをクリックして新しいユーザーやアカウントを追加します。ポップアップウィンドウが表示されます。ポップアップウィンドウを以下の表に示します。
4. 以下の表にしたがってユーザーやアカウントを設定します。

User and account settings

| 設定 | 説明 |
|------------|-------------------------------------|
| Management | |
| User Name | ユーザー名を指定します。英数字とアンダーバー () が利用可能です。 |

| | | |
|--|--|---|
| | <p>User Type</p> | <p>ドロップダウンリストからワイヤレスコントローラーの Web 管理インターフェースへのアクセスを決定するユーザーのタイプを選択します。</p> <ul style="list-style-type: none"> • Administrator: リードライトのフルアクセス。 • Read Only: Monitor と Help タブへのリードオンリーアクセス。 • Guest Provisioning: Maintenance タブの User Manmanagement 設定タブのみへのアクセス。 • License Management Only: Maintenance メニューの Licence タブのみへのアクセス。 |
| | <p>Password</p> | <p>Password 欄にパスワードを記入し、Confirm Password 欄に再度入力します。</p> |
| <p>WiFi Clients</p> |  | |
| | <p>User Name</p> | <p>ユーザー名を指定します。英数字とアンダーバー () が利用可能です。</p> |
| | <p>Password</p> | <p>Password 欄にパスワードを記入し、Confirm Password 欄に再度入力します。</p> |
| | <p>Authentication Type</p> | <p>ドロップダウンリストで以下のプロトコルから選択します。</p> <ul style="list-style-type: none"> • EAP. Extensible Authentication Protocol. • PEAP. Protected EAP. |
| <p>Captive Portal Accounts</p> <p>メモ: ポータル設定がキャプティブポータルではなくゲストポータルの場合はこの選択は無効になります。</p> | |  |

| | | |
|---|---|---|
| | Account Name | アカウント名を指定します。英数字とアンダーバー () が利用可能です。 |
| | Amount | 課金する金額を指定します。 |
| | Currency Sign | 課金の通過の単位を指定します。 |
| | Expiry | <p>ドロップダウンリストでアクセスの時間単位を指定し、その数字を指定します。</p> <ul style="list-style-type: none"> • Hour(s): 時間単位の設定をします。 • Day(s): 日単位の設定をします。 • Week(s): 週単位の設定をします。 • Month(s): 月単位の設定をします。 |
| | Print Message | キャプティブポータルユーザーに対するメッセージを記入できます。 |
| <p>Captive Portal Users</p> <p>メモ: ポータル設定がゲストポータルではなくキャプティブポータルの場合はこの選択は無効になります。</p> |  | |
| | User Name | ユーザー名を指定します。英数字とアンダーバー () が利用可能です。 |
| | Password | パスワードを Password 欄と Confirm Password 欄に記入します。 Generate ボタンをクリックしてパスワードを生成することもできます。 |

| | | |
|--|--------|--|
| | Expiry | <p>ワイヤレスアクセスの失効日時を設定します。</p> <ul style="list-style-type: none"> • Account: ドロップダウンリストでアカウントを選択します。ワイヤレスアクセスは選択したアカウントで選択した項目に従って失効します。 • No Expiry: ワイヤレスアクセスは失効しません。 • Expires in: ワイヤレスアカウントは 1 時間以内に失効します。ドロップダウンリストで失効するまでの分数を選択します。 • Expires at: 失効する日時を選択します。 |
|--|--------|--|

5. **Apply** ボタンをクリックして設定を保存します。
6. **Close** ボタンをクリックしてポップアップウィンドウを閉じます。

ユーザーまたはアカウントを編集または削除する

1. タブ(Management, WiFi Clients, Captive Portal Account, Captive Portal Users)をクリックします。
2. ユーザーまたはアカウントのラジオボタンを選択します。
3. 以下のボタンをクリックします。
 - **Edit:** ポップアップウィンドウが開き、設定を編集します。ユーザー名、ユーザータイプ、アカウント名を変更することはできません。
 - **Remove:** ユーザーの表からユーザーを削除します。

ユーザーまたはアカウントのリストをエクスポートする

1. タブ(Management, WiFi Clients, Captive Portal Account, Captive Portal Users)をクリックします。
2. **Export:** 選択したリストが CSV 形式のファイルで保存されます。
3. ブラウザーの指示に従ってファイルを保存します。

9. コントローラーのメンテナンス

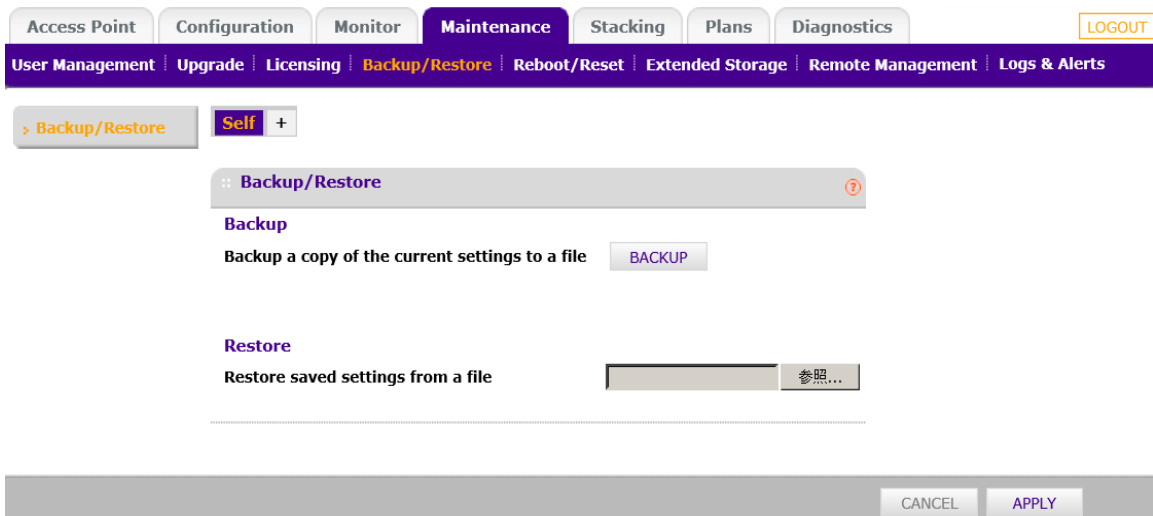
設定ファイル管理

ワイヤレスコントローラーの設定はワイヤレスコントローラーの設定ファイルに保存されています。このファイルはコンピューターに保存（バックアップ）、コンピューターからの復元、あるいは工場出荷状態に戻すことができます。

ワイヤレスコントローラーがインストールされて正しく動作したら、設定ファイルのバックアップをコンピューターに作成します。必要であれば、このファイルからワイヤレスコントローラーの設定を復元することができます。

設定ファイルのバックアップと復元

Maintenance > Backup/Restore を選択して Backup/Restore 画面を表示します。



Backup/Restore 画面では

- 現在の設定のコピーをバックアップして保存することができます。
- バックアップファイルから保存した設定を復元することができます。

設定ファイルをバックアップする

1. Backup/Restore 画面で Backup ボタンをクリックして現在の設定のコピーを保存します。ダイアログが表示され、バックアップファイルのファイル名が表示されます。通常、バックアップファイル名は backup.tgz です。
2. ブラウザーの指示に従い設定ファイルを保存します。

設定ファイルを復元する

1. **Backup/Restore** 画面で**参照**ボタンをクリックします。
2. 保存した設定ファイルを選択します。
3. **Apply** ボタンをクリックして設定ファイルをワイヤレスコントローラーにアップロードします。ワイヤレスコントローラーは再起動します。



警告！

設定ファイルを復元するときにはワイヤレスコントローラーが再起動し終わるまでブラウザの操作をしたり、ワイヤレスコントローラーの電源を切ったり、パソコンをシャットダウンしたり、ワイヤレスコントローラーに操作を加えるようなことはしないでください。Test LED が消灯してからさらに 2,3 秒待ってから操作をしてください。

メモ: 同じバージョンで保存したバックアップファイルで復元をしてください。

ファームウェアをアップグレードする

ワイヤレスコントローラーはファームウェアアップグレードする 2 つの方法を提供します。

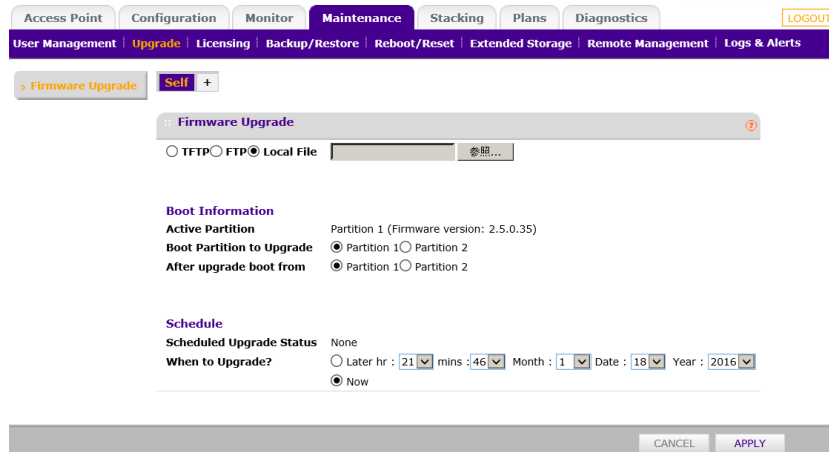
- スケジュールした自動アップデート
- マニュアルアップデート

ワイヤレスコントローラーは 2 つのブートパーティションを持ち、ファームウェアを切り替えることができます。

ファームウェアをアップグレードする

1. WC7520 の製品のダウンロードページからファームウェアを PC にダウンロードします。**Release Notes** をよく読んでからアップデートをしてください。

2. Maintenance > Upgrade を選択して Firmware Upgrade 画面を表示します。



3. 以下の表にしたがって設定をします。

Firmware Upgrade 設定

| 設定 | 説明 |
|--|--|
| TFTP, FTP, or Local File | <p>ファームウェアをアップグレードする方法を選択します。選択に従い画面が更新されます。</p> <ul style="list-style-type: none"> • TFTP: TFTP サーバーからアップグレードします。Server IP と File Name 欄が表示されます。 • FTP: FTP サーバーからアップグレードします。すべてのサーバーパラメーター欄が表示されます。 • Local File: ダウンロードしたローカルファイルでアップデートします。サーバーパラメーター欄は表示されず、参照ボタンとファイル設定欄が表示されます。ブラウザの指示に従いファームウェアアップデートファイルを選択します。 |
| Server Parameters section (TFTP と FTP のみ) | |
| Server IP | TFTP サーバーまたは FTP サーバーの IP アドレスを指定します。 |
| File Name | ファームウェアのファイル名を指定します。 |
| User Name (FTP only) | FTP サーバーにアクセスするためのユーザー名を指定します。 |
| Password (FTP only) | FTP サーバーにアクセスするためのパスワードを指定します。 |
| Boot Information section | |
| Active Partition | 現在の有効なパーティションとファームウェアバージョンを表示します。 |
| Boot Partition to Upgrade | 新しいファームウェアを保存するパーティションを選択します。 |

| | |
|-------------------------|---|
| After upgrade boot from | ファームウェアがアップグレードされた後に起動するパーティションを選択します。 |
| Schedule section | |
| Schedule Update Status | スケジュールされたファームウェアアップグレードの有無を表示します。スケジュールがない場合は None と表示されます。 |
| When to Upgrade? | ファームウェアアップグレードを実行するタイミングを設定します。 <ul style="list-style-type: none"> • Later: ドロップダウンリストアップグレードを実行する日時を指定します。 • Now: Apply ボタンをクリックするとすぐにアップグレードを開始します。 |

4. **Apply** ボタンをクリックして設定を保存します。**Now** を選択した時は、ワイヤレスコントローラーは再起動します。



警告！

ファームウェアアップグレードの最中、ワイヤレスコントローラーが再起動し終わるまでブラウザの操作をしたり、ワイヤレスコントローラーの電源を切ったり、パソコンをシャットダウンしたり、ワイヤレスコントローラーに操作を加えるようなことはしないでください。Test LED が消灯してからさらに 2,3 秒待ってから操作をしてください。

5. ワイヤレスコントローラーの動作しているファームウェアを確認するには、**Monitor > Network > Controller** を選択して **Controllers** 画面を表示し、**Version** 欄のファームウェアバージョンを確認します。

The screenshot shows the 'Monitor' tab selected in the navigation menu. Below it, the 'Controllers' table is displayed with the following data:

| Controller IP | Name | Location | Type | Version | Status | Config Status | Config Sync Time |
|---------------|----------|-------------------|--------|----------|--------|-------------------|--------------------------|
| 10.110.2.91 | WC7520 | JapanOfficeWC7520 | Master | 2.5.0.35 | Up | NA | NA |
| 10.110.2.92 | wc941254 | | Slave | 2.5.0.35 | Up | UPDATE SUCCESSFUL | Mon Jan 18 22:23:56 2016 |

A 'REFRESH' button is visible at the bottom right of the table area.

メモ: ファームウェアのアップグレード後に Web 管理インターフェースでブラウザが正しいファームウェアバージョンを表示しない場合、ブラウザのキャッシュをクリアし、画面を更新してみてください。

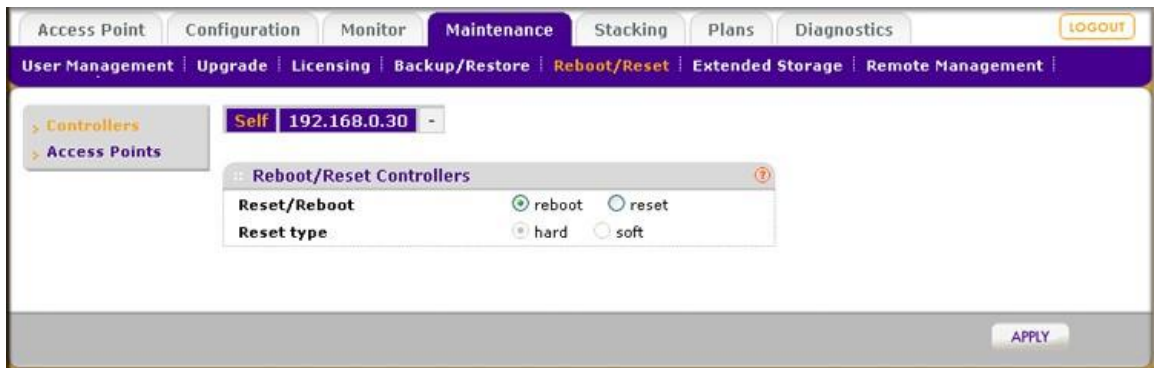
メモ: メジャーファームウェアアップグレードなどの際に、設定を削除してファームウェアアップグレードの後に再設定をする必要がある場合があります。Release Notes を確認してワイヤレスコントローラーのファームウェアをアップグレードしてください。

ワイヤレスコントローラーの再起動またはリセット

Reboot/Reset Controllers 画面でワイヤレスコントローラーを再起動やリセットすることができます。2つのタイプのリセットがあります。

- **Hard reset (ハードリセット)**: ワイヤレスコントローラーの設定は工場出荷状態に戻ります。この機能は本体のリアパネルの Factory Default ボタンと同じです。
- **Soft reset (ソフトリセット)**: IP アドレス、フロアプランと管理アクセスポイントリストは保持し、その他の設定をクリアします。

Maintenance > Reboot/Reset > Controllers を選択して Reboot/Reset Controllers 画面を表示します。



ワイヤレスコントローラーを再起動する

1. **Reboot** ラジオボタンを選択します。
2. **Apply** ボタンをクリックして設定を保存します。ワイヤレスコントローラーが再起動します。数分後フロントパネルの Test LED が消灯して再起動プロセスは終了します。

ワイヤレスコントローラーをリセットする

1. **Reset** ラジオボタンをクリックします。
2. ラジオボタンでハードリセットかソフトリセットを選択します。
 - **Hard**: 工場出荷設定に戻します。
 - **Soft**: IP アドレス、フロアプラン、管理アクセスポイントリスト以外の設定をクリアします。
3. **Apply** ボタンをクリックして設定を保存します。ハードリセットを選択した場合は、ワイヤレスコントローラーは再起動します。

メモ: ワイヤレスコントローラーを工場出荷状態に戻すと、ワイヤレスコントローラーの管理しているアクセスポイントの設定は失われます。

**警告！**

ハードリセットを実行するとき、ワイヤレスコントローラーが再起動し終わるまでブラウザの操作をしたり、ワイヤレスコントローラーの電源を切ったり、パソコンをシャットダウンしたり、ワイヤレスコントローラーに操作を加えるようなことはしないでください。Test LED が消灯してからさらに 2,3 秒待ってから操作をしてください。

アクセスポイントの再起動

通常はアクセスポイントを再起動する必要はありません。アクセスポイントに問題がある場合、アクセスポイントを再起動して問題が解消するかどうか確認することができます。

アクセスポイントを再起動する

1. **Maintenance > Reboot/Reset > Access Points** を選択して **Reboot Access Points** 画面を表示します。

The screenshot shows the 'Reboot Access Points' page. At the top, there are navigation tabs: 'Access Point', 'Configuration', 'Monitor', 'Maintenance' (selected), 'Stacking', 'Plans', and 'Diagnostics'. Below these are more navigation options: 'User Management', 'Upgrade', 'Licensing', 'Backup/Restore', 'Reboot/Reset' (selected), 'Extended Storage', 'Remote Management', and 'Logs & Alerts'. A 'LOGOUT' button is in the top right. On the left, there are expandable menus for 'Controllers' and 'Access Points'. The main area has a 'Self +' button and a 'Reboot Access Points' title. Below the title is a search bar labeled 'Search Access Point by IP/MAC/Name' with 'SEARCH' and 'CLEAR' buttons. A table titled 'List of Access Points' is shown below the search bar. At the bottom of the page, there are 'CANCEL' and 'REBOOT' buttons.

| | IP | MAC | Name | Building | Floor | Location |
|--------------------------|--------------|-------------------|---------------|------------|---------|----------|
| <input type="checkbox"/> | 10.110.2.209 | c0:ff:d4:d4:4e:80 | netgearD44E88 | Building-1 | Floor-1 | |
| <input type="checkbox"/> | 10.110.2.199 | 04:a1:51:84:89:80 | netgear848988 | Building-1 | Floor-1 | |

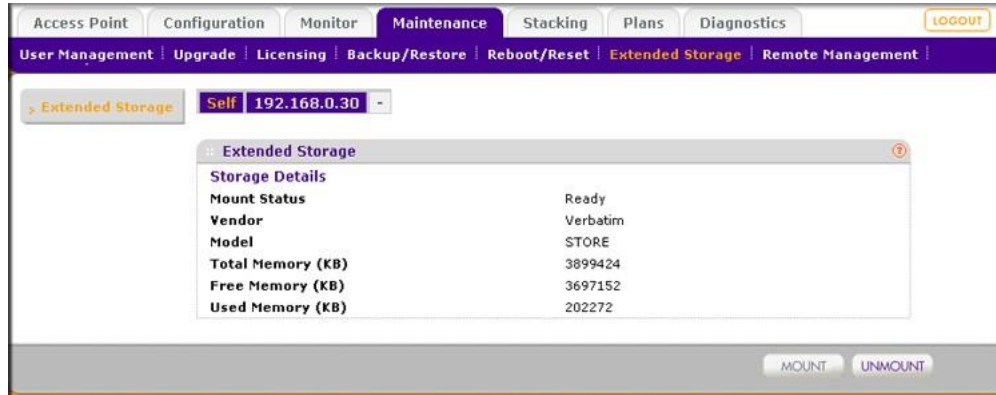
2. **Search Access Point by IP/MAC/Name** 欄に IP アドレス、MAC アドレス、名前を記入して **Search** ボタンをクリックしてアクセスポイントを検索することもできます。
3. **List of Access Points** で、IP アドレス、MAC アドレス、Name をクリックしてソートすることができます。Building, Floor, Location でフィルターすることができます。再起動するアクセスポイントのチェックボックスを選択します。
4. **Reboot** ボタンをクリックします。

外部ストレージ管理

Extended Storage 画面では接続された USB メモリーや USB ハードディスクの情報を表示し、ストレージデバイスをマウント、アンマウントすることができます。外部ストレージを使ってフロアヒートマップや統計情報を多く保存できます。

外部ストレージデバイスをマウントしてデバイスの情報を見る

1. **Maintenance > Extended Storage** を選択して **Extended Storage** 画面を表示します。下の図は接続した USB メモリーの例です。



2. ワイヤレスコントローラーのフロントパネルの USB ポートに外部ストレージデバイスを接続します。
3. **Mount** ボタンをクリックすると Storage Details 画面が表示されます。外部ストレージデバイスを取り外す時は **Unmount** ボタンをクリックします。

リモートアクセス管理

SNMP を有効にして SNMPv1 あるいは SNMPv2c プロトコルを使って SNMP 管理ソフトでワイヤレスコントローラーの監視をすることができます。

以下の機能の例外を除いて、SNMP を使ってワイヤレスコントローラーの設定をすることができます。

- ヒートマップ (Heat maps)
- ゲストアクセス管理
- 電波管理 (RF management)
- スタック管理

SNMP を有効にして設定をする

1. **Maintenance > Remote Management > SNMP** を選択して **SNMP** 画面を表示します。

Access Point Configuration Monitor **Maintenance** Stacking Plans Diagnostics LOGOUT

User Management Upgrade Licensing Backup/Restore Reboot/Reset Extended Storage Remote Management Logs & Alerts

> SNMP Self +

> Session Timeout

SNMP

SNMP

Read-Only Community Name

Read-Write Community Name

Trap Community Name

IP Address to Receive Traps

Trap Port

SNMP Manager IP

CANCEL APPLY

2. 以下の表に従い SNMP を有効にして設定をします。

SNMP settings

| 設定 | 説明 |
|-----------------------------|---|
| SNMP | チェックボックスを選択してワイヤレスコントローラーの SNMP を有効にします。 |
| Read-Only Community Name | ワイヤレスコントローラーのリードオンリー (Read Only) のコミュニティ名を設定します。デフォルトは "public" です。 |
| Read-Write Community Name | ワイヤレスコントローラーのリードライトオンリー (Read and Write) のコミュニティ名を設定します。デフォルトは "private" です。 |
| Trap Community Name | Trap を受信する IP アドレスと関連付けるコミュニティ名を設定します。デフォルトは "trap" です。 |
| IP Address to Receive Traps | ワイヤレスコントローラーが送信するトラップの送信先 SNMP マネージャーの IP アドレスを指定します。 |
| Trap Port | ワイヤレスコントローラーが送信するトラップの送信先 SNMP マネージャーのポート番号を指定します。デフォルトは 162 です。 |
| SNMP Manager IP | SNMP マネージャーの IP アドレスを指定します。 メモ: どの SNMP マネージャーでもワイヤレスコントローラーにアクセスできるようにするにはこの 255.255.255.255 を設定します。 |

3. **Apply** ボタンを押して設定を保存します。

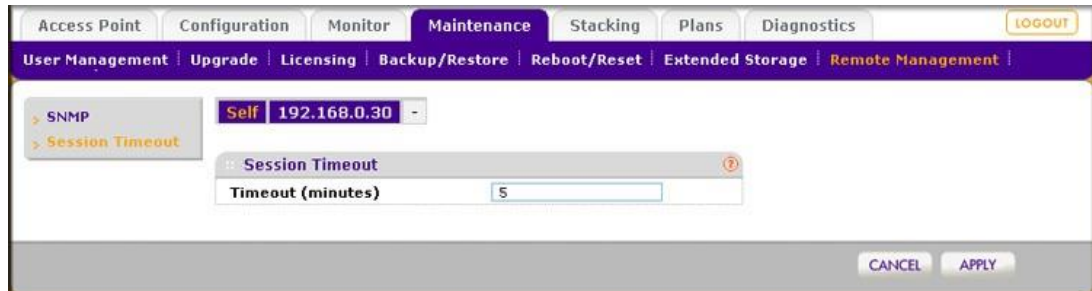
メモ: ワイヤレスコントローラーはコンソールポート経由で Telnet と SSH をサポートしていますがコンソールポートはネットギアテクニカルサポートの指導のもとにデバック目的のためのみに使われます。

セッションタイムアウト設定

HTTP セッションがタイムアウトすると、ユーザーはパスワード認証のためにログインウィンドウにリダイレクトされます。

ワイヤレスコントローラーの HTTP セッションタイムアウトを設定する

1. **Maintenance > Remote Management > Session Timeout** を選択して **Session Timeout** 画面を表示します。



2. In the **Timeout (minutes)**欄にアクティブな HTTP ログインセッションのタイムアウト値(分)を指定します。
3. **Apply** ボタンをクリックして設定を保存します、

アラートとイベント表示とログ保存

システムアラートを表示しワイヤレスコントローラーに収集されたシステムログを保存することができます。個々のアクセスポイントのログを保存することもできます。問題や障害発生時にバックアップした設定ファイルは原因を究明するために役に立つことがあります。

ログの保存

アクセスポイントログを保存する

1. **Maintenance > Logs & Alerts > Save Logs > AP Logs** を選択して **Access Points** 画面を表示します。

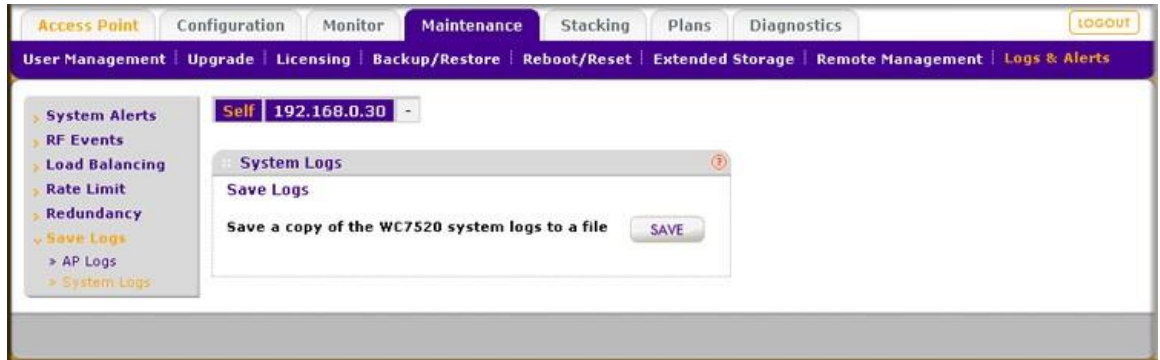


2. ドロップダウンリストでアクセスポイントを選択します。

3. **Save** ボタンをクリックしてブラウザの指示に従い選択したアクセスポイントのログを保存します。ログファイルは tgz 形式で ZIP されています。

システムログを保存する

1. **Maintenance > Logs & Alerts > Save Logs > System Logs** を選択して **System Logs** 画面を表示します。



2. **Save** ボタンをクリックしてブラウザの指示に従いログをコンピューターに保存します。ZIP されたログファイルのファイル名は wnc_logs.tgz です。

アラートとイベントを表示する

ワイヤレスコントローラーでは以下のアラートとイベントを表示することができます。

- **System Alerts:** アクセスポイントの起動、シャットダウン、ワイヤレスコントローラーの起動、シャットダウン、ファームウェアアップグレードのようなシステムアラート。
- **RF Events:** カバレッジホールの検出、チャンネル変更、管理アクセスポイントのダウンのような電波や周波数のイベント。
- **Load Balancing:** 悪い RSSI、ロードバランススレッショルド違反のようなロードバランシングイベント。
- **Rate Limit:** レートリミットスレッショルド超過のようなレートリミットイベント。
- **Redundancy:** 冗長化ワイヤレスコントローラーの起動やダウン、他のワイヤレスコントローラーへのフェイルオーバーのような冗長化イベント。
- **Stacking:** セカンダリーワイヤレスコントローラーの起動やダウン、2つのワイヤレスコントローラー間の同期のようなスタックイベント。

アラートやイベントを表示する画面は3つのカラムを含む表です。

- **Severity:** アラームの重要度レベル。All, Major, Minor, Critical。ドロップダウンリストで表示をフィルターできます。
- **Description:** アラートまたはイベントに説明
- **Raised Time:** アラートまたはイベントが報告された日時。Raised Time ドロップダウンリストで日時をフィルターできます。

追加のアラートやイベントを表示するには、**Next** ボタンをクリックし、前のアラートやイベントを表示するには **Previous** ボタンをクリックします。

最新の情報を表示するには **Refresh** ボタンをクリックします。画面とメモリーから情報をクリアするには、**Clear All** ボタンをクリックします。

システムアラートを表示する

Maintenance > Logs & Alerts > System Alerts を選択して **System Alerts** 画面を表示します。

The screenshot shows the 'System Alerts' page in a web management interface. The top navigation bar includes 'Access Point', 'Configuration', 'Monitor', 'Maintenance', 'Stacking', 'Plans', and 'Diagnostics'. Below this, a secondary bar contains 'User Management', 'Upgrade', 'Licensing', 'Backup/Restore', 'Reboot/Reset', 'Extended Storage', 'Remote Management', and 'Logs & Alerts'. A left sidebar lists various system settings like 'System Alerts', 'RF Events', 'Load Balancing', etc. The main content area is titled 'System Alerts' and contains a table with the following data:

| Severity | Description | Raised Time |
|----------|---|--------------------------|
| Major | Access Point [NAME: netgearB59D48, IP: 10.110.2.248, MAC: 04:a1:51:b5:9d:48, MODEL: WNAP320] UP | Sat Jan 23 10:03:28 2016 |
| Normal | Access Point [NAME: netgearB59D48, MAC: 04:a1:51:b5:9d:48, IP: 10.110.2.248, MODEL: WNAP320] Site:0 added to Managed List | Sat Jan 23 09:57:12 2016 |
| Major | Access Point [NAME: netgearD44E88, IP: 10.110.2.209, MAC: c0:ff:d4:d4:4e:80, MODEL: WNDAP360] DOWN | Fri Jan 22 16:28:45 2016 |
| Major | Access Point [NAME: netgearD44E88, IP: 10.110.2.209, MAC: c0:ff:d4:d4:4e:80, MODEL: WNDAP360] DOWN | Fri Jan 22 16:27:26 2016 |
| Normal | Access Point [NAME: netgearB48988, IP: 10.110.2.199, MAC: 04:a1:51:84:89:80, MODEL: WNDAP360] removed from Managed List | Tue Jan 19 13:39:26 2016 |
| Normal | Access Point [NAME: netgearD448CB, IP: 10.110.2.198, MAC: c0:ff:d4:d4:48:c0, MODEL: WNDAP360] removed from Managed List | Mon Jan 18 20:17:55 2016 |
| Normal | Assoc [Cleared client from blacklist] Event for Client bc:6e:64:77:15:47 [Timer Expiry, status 1] | Mon Jan 18 19:00:58 2016 |
| Normal | Assoc [Assoc Success] Event for Client bc:6e:64:77:15:47 | Mon Jan 18 19:00:48 2016 |
| Normal | Assoc [Cleared client from blacklist] Event for Client bc:6e:64:77:15:47 [Timer Expiry, status 1] | Mon Jan 18 18:45:10 2016 |
| Normal | Assoc [Assoc Success] Event for Client bc:6e:64:77:15:47 | Mon Jan 18 18:45:00 2016 |
| Normal | Assoc [Cleared client from blacklist] Event for Client bc:6e:64:77:15:47 [Timer Expiry, status 2] | Fri Jan 15 11:00:44 2016 |
| Normal | Assoc [Assoc Success] Event for Client bc:6e:64:77:15:47 | Fri Jan 15 11:00:34 2016 |
| Major | Assoc [Auth Failed] Event for Client bc:6e:64:77:15:47 from AP c0:ff:d4:d4:48:c0 | Fri Jan 15 10:54:58 2016 |
| Normal | Access Point [NAME: netgear9F3628, IP: 10.110.2.222, MAC: 28:c6:8e:9f:36:20, MODEL: WNDAP360] removed from Managed List | Tue Jan 13 13:31:39 2016 |
| Major | Access Point [NAME: netgear9F3628, IP: 10.110.2.222, MAC: 28:c6:8e:9f:36:20, MODEL: WNDAP360] UP | Wed Jan 13 13:29:55 2016 |
| Major | Access Point [NAME: netgear9F3628, IP: 10.110.2.222, MAC: 28:c6:8e:9f:36:20, MODEL: WNDAP360] DOWN | Wed Jan 13 13:28:33 2016 |

At the bottom of the table, there is a pagination control: '1-16 of 17 | Entry Per Page | Default | PREVIOUS | 1 of 2 | NEXT'. Below the table, there are three buttons: REFRESH, CLEAR ALL, and EXPORT.

既存のログをクリアするには **Clear All** ボタンをクリックします。**Export** ボタンをクリックしてログを **csv** 形式でエクスポートすることができます。システムアラートをクリアする前に保存することを検討してください。

電波イベント(RF events)を表示する

Maintenance > Logs & Alerts > RF Events を選択して **RF Events** 画面を表示します。

Access Point Configuration Monitor **Maintenance** Stacking Plans Diagnostics LOGOUT

User Management Upgrade Licensing Backup/Restore Reboot/Reset Extended Storage Remote Management **Logs & Alerts**

Self 192.168.0.30 -

System Alerts
 RF Events
 Load Balancing
 Rate Limit
 Redundancy
 Stacking
 Save Logs

RF Events

| Severity | Description | Raised Time |
|----------|--|--------------------------|
| Major | Coverage Hole detected around AP netgear782488 in 2.4GHz frequency band in building Clinic on Floor Floor-1. | Fri Sep 17 00:02:37 2010 |
| Major | Coverage Hole detected around AP netgear782488 in 2.4GHz frequency band in building Clinic on Floor Floor-1. | Thu Sep 16 16:12:36 2010 |
| Major | Coverage Hole detected around AP netgear782488 in 2.4GHz frequency band in building Clinic on Floor Floor-1. | Thu Sep 16 16:07:36 2010 |
| Major | Coverage Hole detected around AP netgear7826D8 in 2.4GHz frequency band in building Clinic on Floor-1. | Wed Aug 11 20:10:05 2010 |
| Major | Coverage Hole detected around AP netgear782488 in 2.4GHz frequency band in building Clinic on Floor-1. | Wed Aug 11 20:10:05 2010 |
| Major | Coverage Hole detected around AP netgear7826D8 in 2.4GHz frequency band in building Clinic on Floor-1. | Wed Aug 11 20:05:05 2010 |
| Major | Coverage Hole detected around AP netgear782488 in 2.4GHz frequency band in building Clinic on Floor-1. | Wed Aug 11 20:05:05 2010 |
| Major | Coverage Hole detected around AP netgear7826D8 in 2.4GHz frequency band in building Clinic on Floor-1. | Wed Aug 11 20:00:05 2010 |
| Major | Coverage Hole detected around AP netgear782488 in 2.4GHz frequency band in building Clinic on Floor-1. | Wed Aug 11 20:00:05 2010 |
| Major | Coverage Hole detected around AP netgear7826D8 in 2.4GHz frequency band in building Clinic on Floor-1. | Wed Aug 11 19:55:05 2010 |

REFRESH CLEAR ALL

ロードバランスイベントを表示する

Maintenance > Logs & Alerts > Load Balancing を選択して Load Balancing 画面を表示します。

Access Point Configuration Monitor **Maintenance** Stacking Plans Diagnostics LOGOUT

User Management Upgrade Licensing Backup/Restore Reboot/Reset Extended Storage Remote Management **Logs & Alerts**

Self 192.168.0.30 -

System Alerts
 RF Events
 Load Balancing
 Rate Limit
 Redundancy
 Stacking
 Save Logs

Load Balancing

| Severity | Description | Raised Time |
|----------|---|--------------------------|
| Normal | Load Balancing[Bad RSSI] Event for Client 04:1e:64:81:ed:d1 | Fri Mar 11 16:42:06 2011 |
| Normal | Load Balancing[Bad RSSI] Event for Client 00:16:ea:ba:cf:be | Fri Mar 11 16:39:41 2011 |
| Normal | Load Balancing[Bad RSSI] Event for Client 90:27:e4:47:b2:22 | Fri Mar 11 16:36:50 2011 |
| Normal | Load Balancing[Bad RSSI] Event for Client 90:27:e4:47:b2:22 | Fri Mar 11 16:35:55 2011 |
| Normal | Load Balancing[Bad RSSI] Event for Client 90:27:e4:47:b2:22 | Fri Mar 11 16:35:34 2011 |
| Normal | Load Balancing[Bad RSSI] Event for Client 90:27:e4:47:b2:22 | Fri Mar 11 16:35:13 2011 |
| Normal | Load Balancing[Bad RSSI] Event for Client 90:27:e4:47:b2:22 | Fri Mar 11 16:35:12 2011 |
| Normal | Load Balancing[Bad RSSI] Event for Client 90:27:e4:47:b2:22 | Fri Mar 11 16:35:12 2011 |
| Normal | Load Balancing[Bad RSSI] Event for Client 90:27:e4:47:b2:22 | Fri Mar 11 16:33:18 2011 |
| Normal | Load Balancing[Bad RSSI] Event for Client 00:21:5c:03:39:0b | Fri Mar 11 16:25:18 2011 |
| Normal | Load Balancing[Bad RSSI] Event for Client 00:21:5c:03:39:0b | Fri Mar 11 16:25:18 2011 |
| Normal | Load Balancing[Bad RSSI] Event for Client 00:21:5c:03:39:0b | Fri Mar 11 16:25:01 2011 |

REFRESH CLEAR ALL

レートリミットイベントを表示する

Maintenance > Logs & Alerts > Rate Limit を選択して Rate Limit 画面を表示します。

Access Point Configuration Monitor **Maintenance** Stacking Plans Diagnostics LOGOUT

User Management Upgrade Licensing Backup/Restore Reboot/Reset Extended Storage Remote Management Logs & Alerts

Self 192.168.0.30 -

System Alerts
RF Events
Load Balancing
Rate Limit
Redundancy
Stacking
Save Logs

Rate Limit

| Description | Severity | Raised Time |
|-------------|----------|-------------|
| | All | All |

REFRESH CLEAR ALL

冗長化イベントを表示する

Maintenance > Logs & Alerts > Redundancy を選択して Redundancy 画面を表示します。

Access Point Configuration Monitor **Maintenance** Stacking Plans Diagnostics LOGOUT

User Management Upgrade Licensing Backup/Restore Reboot/Reset Extended Storage Remote Management Logs & Alerts

Self 192.168.0.30 -

System Alerts
RF Events
Load Balancing
Rate Limit
Redundancy
Stacking
Save Logs

Redundancy

| Severity | Description | Raised Time |
|----------|---------------------------|--------------------------|
| All | | All |
| Major | Switching to Active State | Mon Sep 20 17:32:16 2010 |

REFRESH CLEAR ALL

スタッキングイベントを表示する

Maintenance > Logs & Alerts > Stacking を選択して Stacking 画面を表示します。

Access Point Configuration Monitor **Maintenance** Stacking Plans Diagnostics LOGOUT

User Management Upgrade Licensing Backup/Restore Reboot/Reset Extended Storage Remote Management Logs & Alerts

Self 192.168.0.30 -

System Alerts
RF Events
Load Balancing
Rate Limit
Redundancy
Stacking
Save Logs

Stacking

| Severity | Description | Raised Time |
|----------|--------------------------|--------------------------|
| All | | All |
| Major | Peer 192.168.0.251 is UP | Tue Sep 21 15:25:24 2010 |

REFRESH CLEAR ALL

ライセンス管理

License 画面ではネットワークに必要なライセンスのインポート、登録(register)、表示をすることができます。

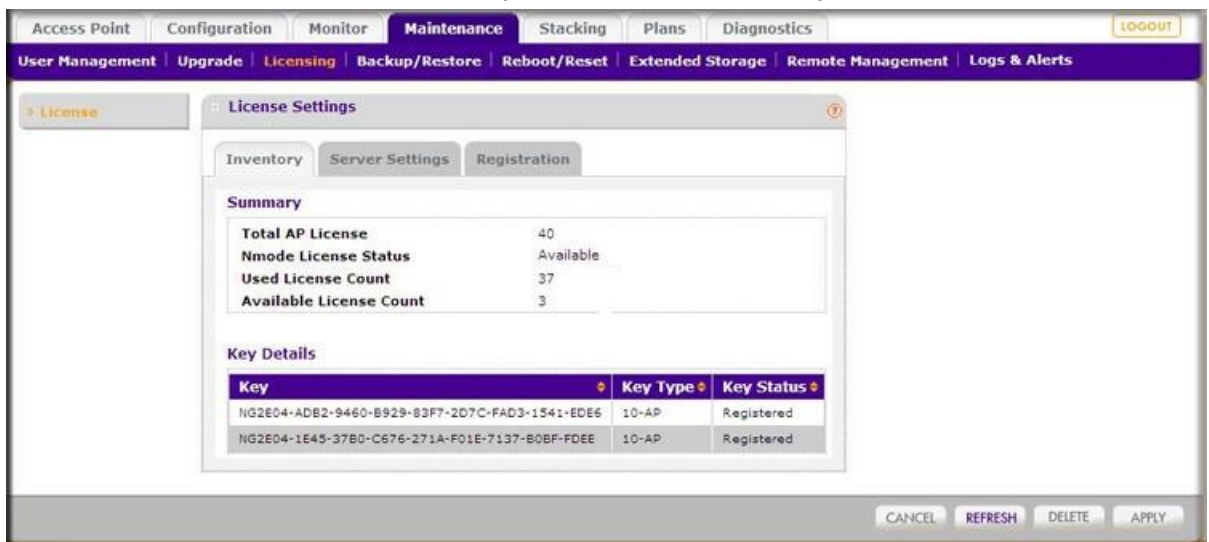
License 画面は 4 つの独立した画面からなります。

- **Inventory screen:** ライセンスの概要を表示します。
- **Server Settings screen:** ライセンスをインポートするためのサーバーを設定します。
- **Registration screen:** ライセンスを登録します。
- **Advanced screen:** ライセンスを復元します。この画面はネットギアから交換機器を受け取った場合に関連する情報を表示します。

ライセンス情報

ライセンス情報を表示する

Maintenance > License を選択し、Inventory タブをクリックし、Inventory 画面を表示します。



以下の表に説明を記します。

License inventory settings

| 設定 | 説明 |
|-------------------------|--|
| Summary section | |
| Total AP License | ライセンスがサポートする最大アクセスポイント数。 |
| Nmode License Status | 802.11n モードライセンスの有無。(デフォルトで有効で、Pre-installed または Available と表示されます。) |
| Used License Count | 使用したライセンス数。 |
| Available License Count | 利用可能なライセンス数。 |

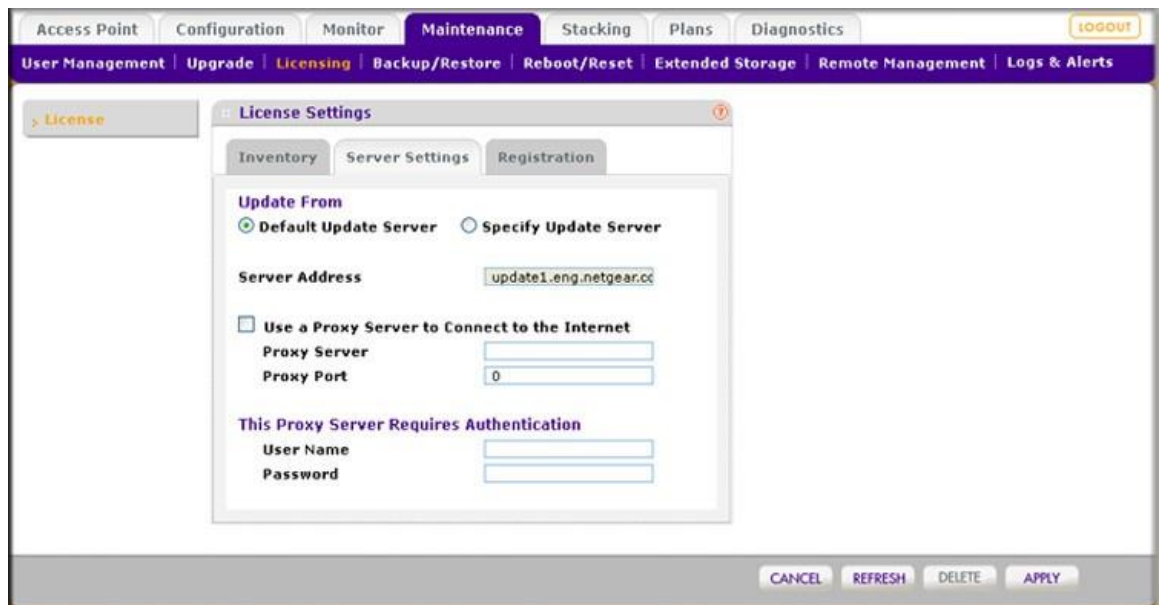
| Key Details section | |
|---------------------|---|
| Key | ライセンスを解除するライセンスキー。 |
| Key Type | ライセンスキーでサポートされるアクセスポイント数。 |
| Key Status | キーの状態 (Registering key with server または Registered). |

Refresh ボタンをクリックしてライセンス情報を更新します。

ライセンスサーバー設定

ライセンスサーバー設定をする

1. Maintenance > License を選択し Server Setting タブをクリックして Server Setting 画面を表示します。



2. 以下の表示にしたがって設定をします。

License server settings

| Setting | Description |
|-------------|--|
| Update From | <p>ライセンス更新サーバー(License update server)を選択します。</p> <ul style="list-style-type: none"> • Default Update Server: デフォルトを使います。 • Specify Update Server: ライセンス更新サーバーを Server Address 欄に指定します。 |

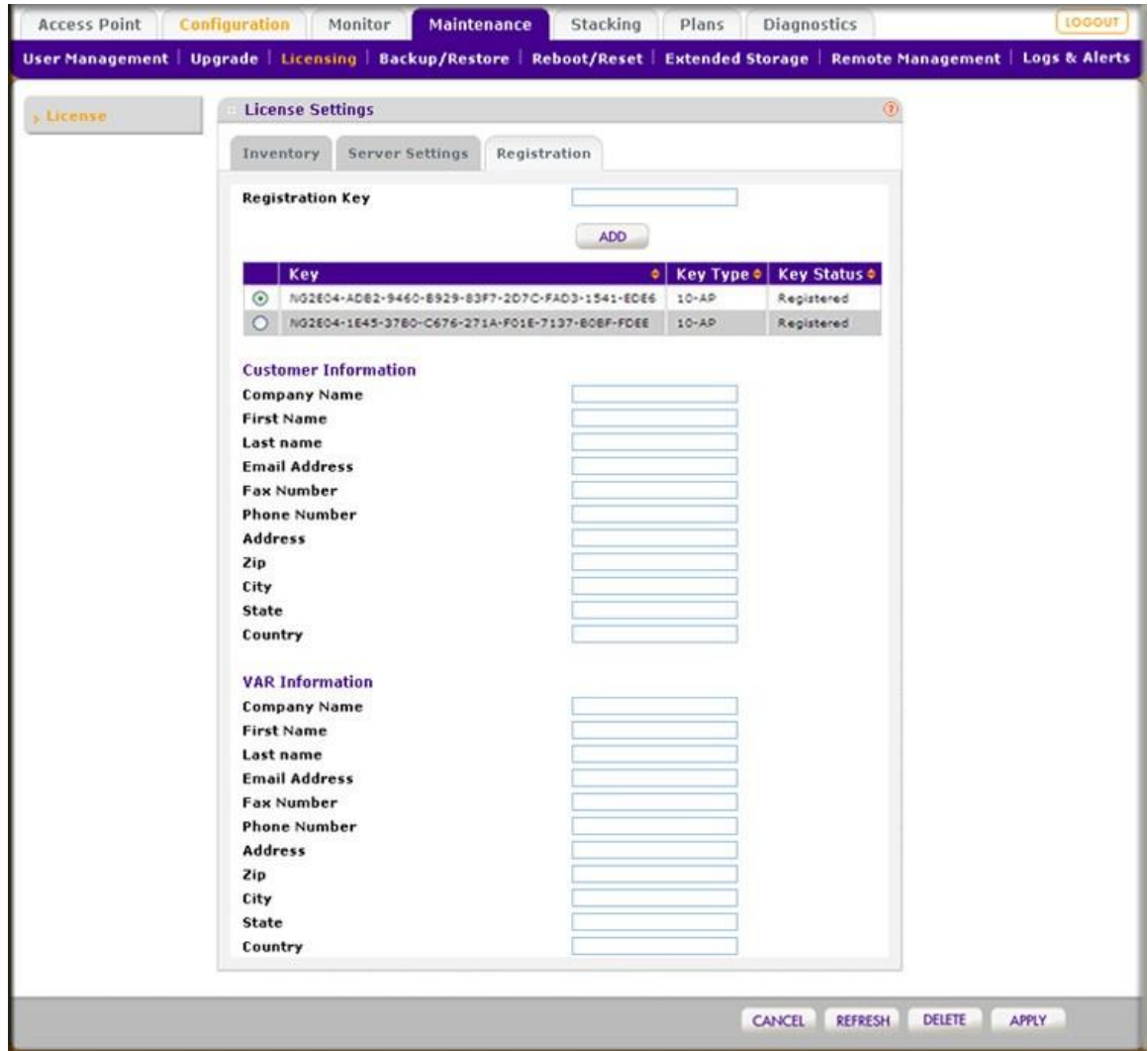
| | | |
|---|---------------------------------------|--|
| | Server Address | ライセンスをインポートするサーバーの IP アドレスまたは FQDN(Fully Qualified Domain Name)を指定します。 |
| Use a Proxy Server to Connect to the Internet | インターネットに接続するのに Proxy サーバーを使うときに選択します。 | |
| | Proxy Server | Proxy サーバーの IP アドレスまたは FQDN(Fully Qualified Domain Name)を指定します。 |
| | Proxy Port | Proxy サーバーのポートを指定します。 |
| This Proxy Server Requires Authentication | Proxy サーバーが認証を必要とする場合にチェックボックスを選択します。 | |
| | User Name | Proxy サーバーにアクセスするためのユーザー名を指定します。 |
| | Password | Proxy サーバーにアクセスするためのパスワードを指定します。 |

3. **Apply** ボタンをクリックして設定を保存します。

ライセンス登録

ライセンスを登録する

1. ワイヤレスコントローラーがインターネットの接続されていることを確認します。
2. **Maintenance > License** を選択し **Registration** タブをクリックして **Registration** 画面を表示します。



1. **Customer Information** 欄に記入します。
2. **VAR Information** 欄に記入します。
3. **Registration Key** 欄に登録する Registration Key を入力します。
4. **Add** ボタンをクリックして表にライセンスを追加します。
5. **Apply** ボタンをクリックしてライセンスを登録します。

表からライセンスを削除するには、ライセンスをラジオボタンで選択して **Delete** ボタンをクリックします。

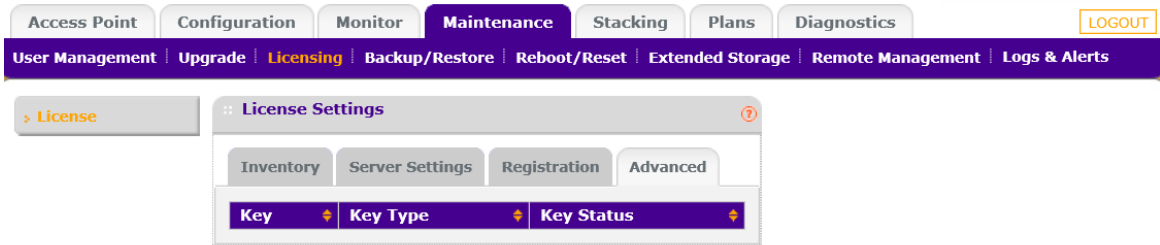
ライセンスを Retrieve Your Licenses

ワイヤレスコントローラーを交換した場合、ライセンスは Inventory と Registration 画面に表示されません。ライセンス更新サーバーからライセンスを復元する必要があります。

ワイヤレスコントローラーを交換した後にライセンスを復元する

1. ワイヤレスコントローラーがインターネットに接続されていることを確認します。

2. **Maintenance > License** を選択し **Advanced** タブをクリックして **Advanced** 画面を表示します。



3. **Replace** ボタンをクリックします。ワイヤレスコントローラーがライセンス更新サーバーに接続してライセンスを復元します。

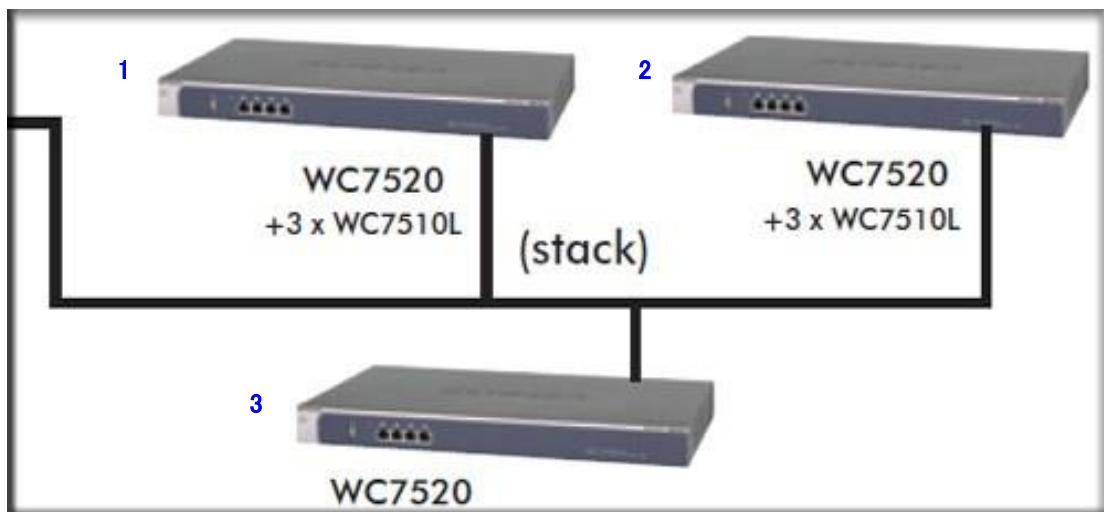
10. スタックと冗長管理

スタック管理

ワイヤレスコントローラーは最大 3 台までのスタック構成をサポートし、追加ライセンスを購入したうえで最大 150 台までのアクセスポイントを管理できます。1 台のワイヤレスコントローラーはプライマリーコントローラー（マスターとしても知られる）として機能し、他の 2 台のワイヤレスコントローラーはセカンダリーコントローラー（スレーブとしても知られる）として機能します。

以下の図は最大 120 台まで管理可能なライセンスを持つスタック構成を示します。

- 2 台のコントローラー(1 と 2)がそれぞれ 50 台のアクセスポイントをサポートします。
- 1 台のコントローラー(3)は 20 台のアクセスポイントをサポートします。



スタックのメンバーとしたいワイヤレスコントローラーは有線で接続されている必要があります。スタックを構成するワイヤレスコントローラー間にスイッチまたはルーターが存在することができます。

個別にプライマリーとセカンダリーコントローラーを設定し、すべてのコントローラーでスタックを有効にし、それらのアクセスポイント設定をプライマリーコントローラーと同期します。スタックを有効にすると、プライマリーコントローラーは管理ユーザー名とパスワード、ファームウェアイメージをセカンダリーコントローラーと同期します。

マスターコントローラーはすべての設定変更をセカンダリーコントローラーを介して個々のアクセスポイントにプッシュすることができます。管理を容易にするために、マスターコントローラーでロケーションベースのプロファイルを設定し、各セカンダリーコントローラーにロケーションを割り当てることができます。

スタック機能はワイヤレスクライアントが同じスタックグループのあるワイヤレスコントローラーに管理されているアクセスポイントから同じスタックグループの他のワイヤレスコントローラー配下のアクセスポイントへのローミングを可能にします。

以下にスタックのプライマリーとセカンダリーコントローラー能力をあげます。

Primary controller: 以下のことができます。

- セカンダリーコントローラーの管理
- セカンダリーコントローラーの電波計画の実行
- アクセスポイントディスカバリーとライセンス追加を含むネットワーク全体の設定
- 全体のネットワーク監視
- 新しいファームウェアイメージをセカンダリーコントローラーへのプッシュ

Secondary controller: 以下のことができます。

- プライマリーコントローラーへの Web 管理インターフェースへのアクセス(すべてのコントローラーで管理ユーザー名とパスワードは共通です)
- サブネットワークの設定
- サブネットワークの監視
- セカンダリーコントローラーのみのファームウェアイメージのアップグレード
- サブネットワークでのアクセスポイントディスカバリーの実行
- サブネットワークのライセンス追加

スタック設定

スタックを設定する

1. **Stacking > Stacking/Redundancy** を選択して画面を **Stacking/Redundancy** 表示します。

The screenshot shows the 'Stacking/Redundancy' configuration page. At the top, there are tabs for 'Access Point', 'Configuration', 'Monitor', 'Maintenance', 'Stacking', 'Plans', and 'Diagnostics'. The 'Stacking' tab is active. Below the tabs, there is a 'Logout' button. The main content area is titled 'Stacking/Redundancy' and contains a 'Stacking' section with a table and a 'Redundancy' section with a checkbox.

| Role | Controller IP | Local IP | Master IP | Status |
|--|---------------|-------------|-------------|--------|
| <input type="radio"/> Master | 10.110.2.91 | 10.110.2.94 | 10.110.2.91 | Up |
| <input checked="" type="radio"/> Slave | 10.110.2.92 | 10.110.2.95 | 10.110.2.91 | Up |

Buttons: ADD, EDIT, DELETE

Redundancy: Enable Redundancy

Buttons at the bottom: APPLY, REPLACE, SYNC, CANCEL

Stacking テーブルはスタック内のワイヤレスコントローラーをそれらの IP アドレスと役割(マスターまたはスレーブ)とともに表示します。

2. **Add** ボタンをクリックしてワイヤレスコントローラーをスタックに追加します。**ADD Settings** ポップアップウィンドウが表示されます。

3. 以下の表に従い設定をします。

Stacking settings

| 設定 | 説明 |
|---------------|---------------------------------------|
| Controller IP | コントローラーの IP アドレスを指定します。 |
| UserName | コントローラーの管理インターフェースのユーザー名。変更不可。”admin” |
| Password | ワイヤレスコントローラーにアクセスするためのパスワード。 |

4. **Add** ボタンをクリックします。ワイヤレスコントローラーが Stacking テーブルに追加され以下の情報が表示されます。

Stacking table fields

| 設定 | 説明 |
|------------|--|
| Role | スタック内でのワイヤレスコントローラーの役割。Master または Slave。 |
| Controller | ワイヤレスコントローラーの IP アドレス。 |
| Local IP | リダンダンシーグループの中のワイヤレスコントローラーのローカル IP アドレス。リダンダンシー(冗長化)を設定していない場合は、マスターコントローラーのローカル IP アドレスはコントローラーの IP アドレスと同じで、スレーブコントローラーにはローカル IP アドレスはありません。 |
| Master IP | スタック内のマスターの IP アドレス。 |
| Status | ワイヤレスコントローラーの状態。Up または Down。 |

5. スタック内のマスターコントローラーで **Sync** ボタンをクリックしてプロファイル、キャプティブポータル、ユーザー管理設定をスタック内のスレーブコントローラーに同期することができます。同期の後スレーブコントローラーは再起動します。

メモ: スタック内のスレーブコントローラーで、マスターコントローラーをスタックメンバーとして追加すると、スレーブコントローラーは新しいマスターコントローラーとなり、前のマスターコントローラーは新しいスレーブコントローラーになります。

コントローラー選択リスト

ワイヤレスコントローラーをスタックに追加した後、Web 管理インターフェースのほとんどの画面に設定したいワイヤレスコントローラーを選択可能にするコントローラー選択リストが表示されるようになります。

Self 192.168.0.251 192.168.0.252 -

Self をクリックして Web 管理インターフェースを通してアクセスしているワイヤレスコントローラー (192.168.0.251) を設定します。他の IP アドレスをクリックしてスタック内のコントローラー (192.168.0.252) を設定することができます。以下の図ではコントローラー選択リストの例を示します。



冗長化管理 (Manage Redundancy)

ワイヤレスコントローラーはフェイルオーバー可能な N:1 冗長化をサポートしています。冗長化 (Redundancy) は VRRP (Virtual Router Redundancy Protocol) を使うことによって実装されています。

シングルコントローラー冗長化

2 台のコントローラーを使って冗長化グループを構成することができます。冗長化グループの 1 台のコントローラーをプライマリーコントローラーとし、もう 1 台のワイヤレスコントローラーを冗長コントローラーに設定します。プライマリーコントローラーが故障あるいはネットワークから切断されると、冗長コントローラーへの自動フェイルオーバーが発生します。冗長コントローラーはプライマリーコントローラーのすべての機能を引き継ぎます。

メモ: 冗長フェイルオーバーが発生するとき、ワイヤレスクライアントは数秒のサービス中断を経験することがあります。

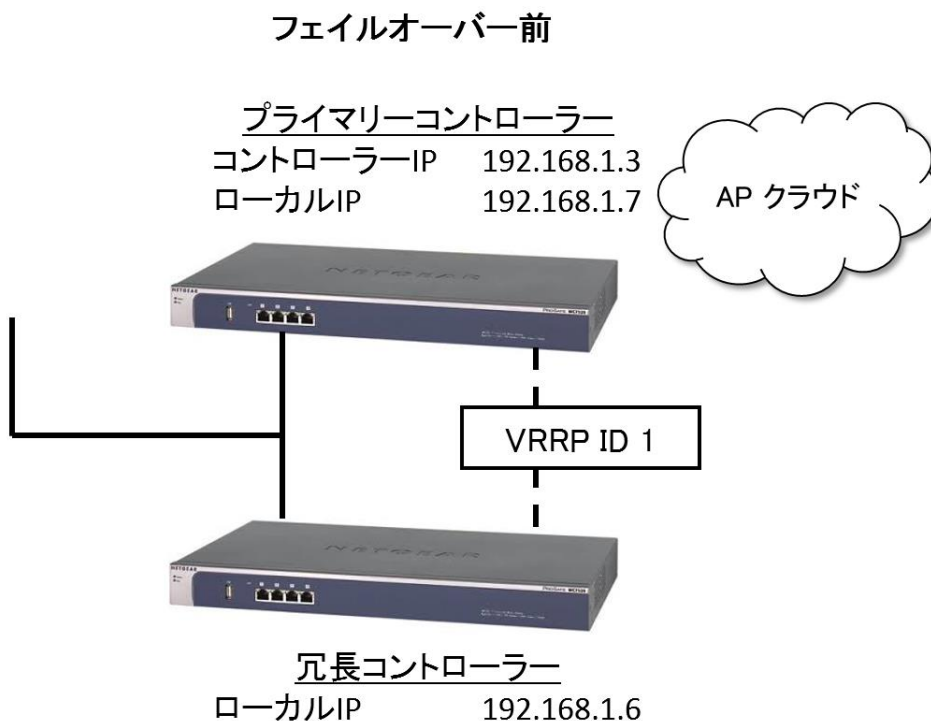
シングルコントローラー冗長化の要件と制限

以下にシングルコントローラー冗長化が正しく機能するための要件と制限を記します。

- プライマリーとセカンダリーコントローラーは同じ管理 VLAN と同じ IP サブネットに存在する必要があります。
- プライマリーコントローラーと冗長コントローラーの関係のための VRRP ID はネットワーク内の他の目的の VRRP ID に対しても一意である必要がある必要があります。
- プライマリーコントローラーと冗長コントローラーは同じファームウェアバージョンを実行している必要があります。ファームウェアバージョンが異なる場合、冗長機能は動作しません。
- 冗長コントローラーのライセンスはプライマリーコントローラーのライセンスに一致する必要があります。ライセンスが一致しない場合、冗長機能は動作しません。
- プライマリーコントローラーと冗長コントローラーはサービスを提供する同じコントローラー IP アドレスを持つ必要がありますが、それぞれのコントローラーはそれぞれのローカル IP アドレスを持ちます。

シングルコントローラー冗長化の例

以下の図はフェイルオーバーが発生する前のプライマリーコントローラーと冗長コントローラーを示しています。

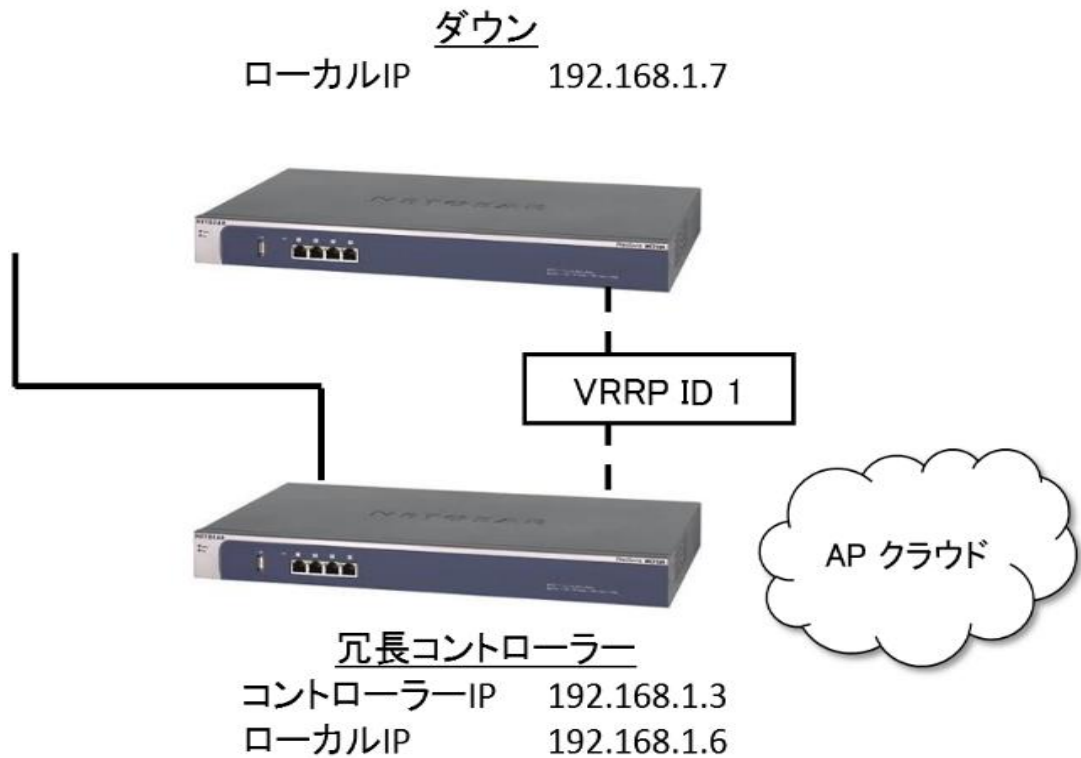


以下の図はフェイルオーバーが発生する前の Stacking/Redundancy 画面の設定を示します。



以下の図はフェイルオーバーが発生した後のプライマリーコントローラーと冗長コントローラーを示しています。

フェイルオーバー後



N:1 冗長

N:1 冗長化によって、最大 3 台のコントローラーに対して 1 台の冗長コントローラーを追加する k ことができます。すなわち 4 台のコントローラーの冗長グループで 1 台が冗長コントローラーとすることができます。

N:1 冗長グループの 3 台のプライマリコントローラーと 1 台の冗長コントローラーでは、冗長コントローラーで 3 つのバーチャルコントローラーを構成することができます。バーチャルコントローラーのそれぞれがプライマリコントローラーと冗長関係を持ちます。それぞれの冗長関係に VRRP ID が必要です。

冗長グループのそれぞれのコントローラーは一意のコントローラー IP アドレスと一意のローカル IP アドレスを持ちます。ローカルアドレスは不変なのでコントローラーはフェイルオーバーの前後でいつも識別可能です。プライマリコントローラーが故障あるいはネットワークから切断されると、冗長コントローラーへの自動フェイルオーバーが発生します。冗長コントローラーはプライマリコントローラーのコントローラー IP アドレスの所有権を持ち、プライマリコントローラーのすべての機能を引き継ぎます。

フェイルオーバー発生後には冗長グループの他のプライマリコントローラーには冗長性はありません。

故障あるいは切断されたプライマリコントローラーが復活し安定すると、自動的にスイッチバックが発生し、コントローラー IP アドレスの所有権は復帰したプライマリコントローラーに戻されます。冗長コントローラーは受動的な状態に戻り、冗長が冗長グループのすべてのプライマリコントローラーに対して再度有効になります。

メモ: 冗長フェイルオーバーが発生した時、ワイヤレスクライアントは 2,3 秒のサービス断を経験することがあります。

N:1 冗長の要件と制限

以下に N:1 冗長化が正しく機能するための要件と制限を記します。

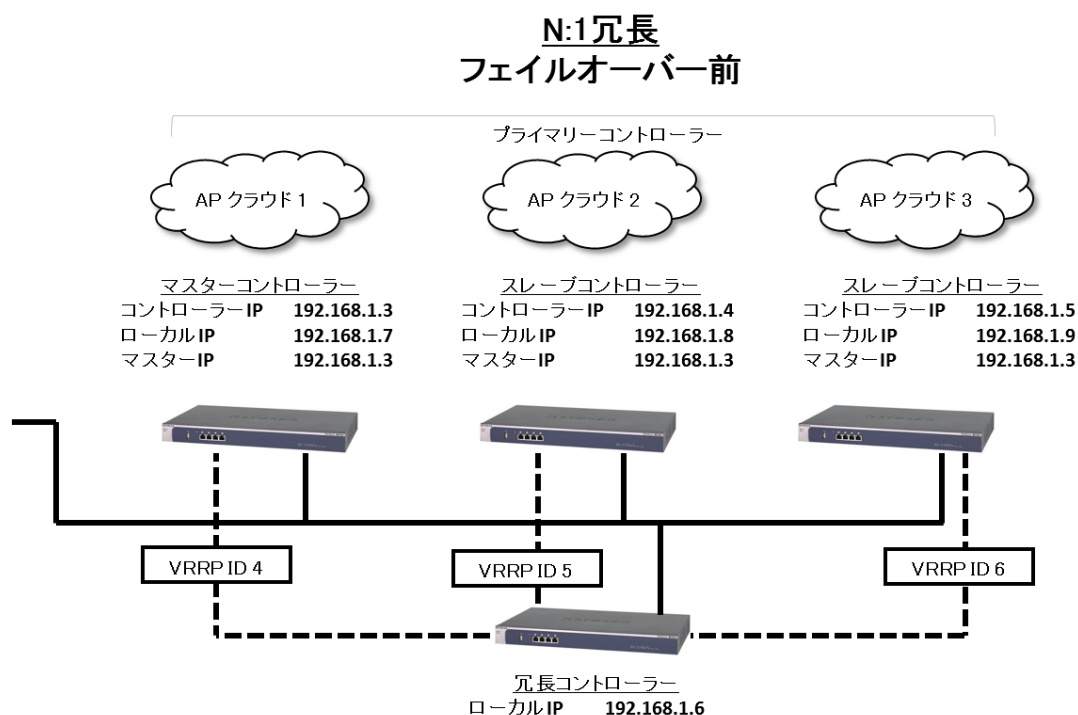
- 冗長グループのすべてのコントローラーは同じ管理 VLAN と同じ IP サブネットに存在する必要があります。
- プライマリコントローラーはスタックされている必要があります。
- 3 台または 4 台のコントローラーが同じ冗長グループに所属しているならば、1 台のコントローラーを冗長コントローラー、残りのコントローラーをプライマリコントローラーとして設定する必要があります。
- 冗長グループのすべてのコントローラーは同じファームウェアバージョンを実行する必要があります。ファームウェアバージョンが異なる場合、冗長機能は動作しません。
- 冗長コントローラーのライセンスはプライマリコントローラーの中の最大ライセンス数に一致する必要があります。例えば、2 台のプライマリコントローラーの冗長グループの場合、1 台

のプライマリコントローラーが 20 台のアクセスポイントのライセンスを持ち、もう 1 台のプライマリコントローラーが 20 台のアクセスポイントのライセンスを持つ場合、冗長コントローラーは 50 ライセンスを持つ必要があります。ライセンス数が一致しない場合、冗長機能は動作しません。

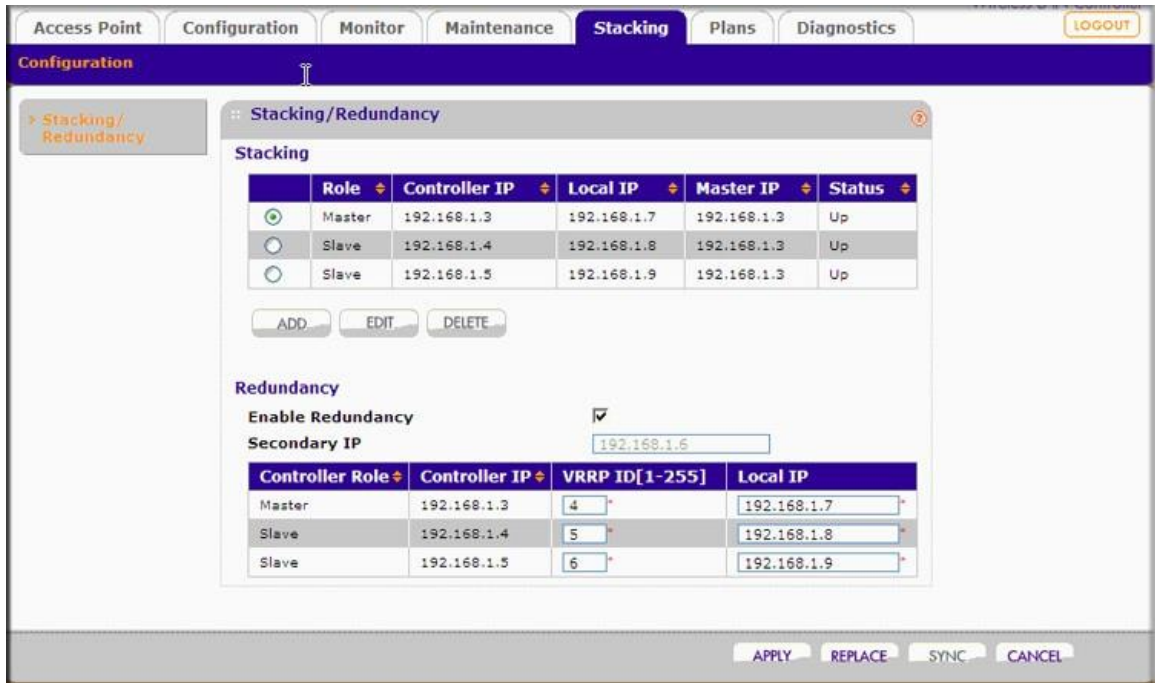
- 各プライマリコントローラーと冗長コントローラーの関係のための VRRP ID はネットワーク内の他の目的の VRRP ID に対しても一意である必要があります。冗長グループの各コントローラーは一意のローカルコントローラー IP アドレスを保つ必要があります。
- フェイルオーバーが発生し、冗長コントローラーがプライマリコントローラーを引き継いだ後、冗長グループの他のプライマリコントローラーには冗長性はありません。
- ファームウェアをリリース 2.2 よりも前からリリース 2.2 にアップグレードするときには、冗長設定を再設定する必要があります。

N:1 冗長構成の例

以下の図は N:1 冗長構成の 3 台のスタックされたコントローラーと 1 台の冗長コントローラーのフェイルオーバーが発生する前の設定を示しています。

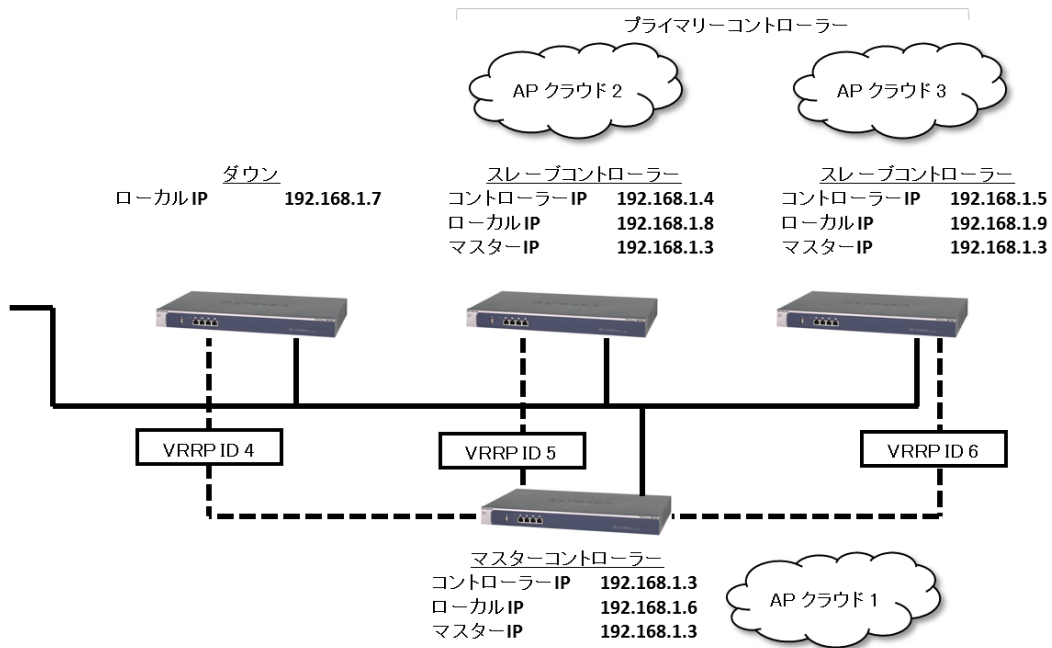


以下の図は **Stacking/Redundancy** 画面でのフェイルオーバーが発生する前の N:1 冗長設定を示しています。



以下の図は N:1 冗長構成の 3 台のスタックされたプライマリコントローラーと 1 台の冗長コントローラーのフェイルオーバーが発生後をあらわしています。

N:1 冗長 フェイルオーバー後

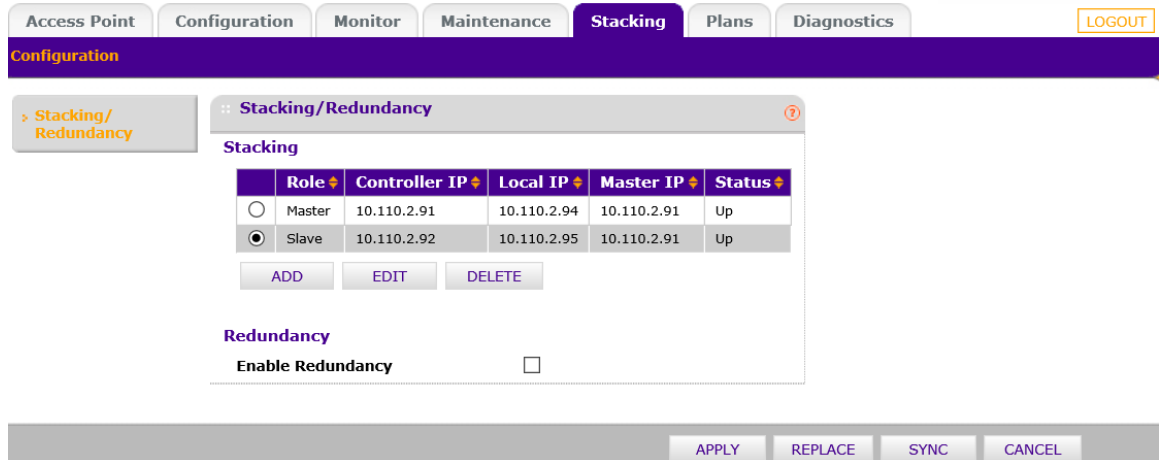


冗長設定

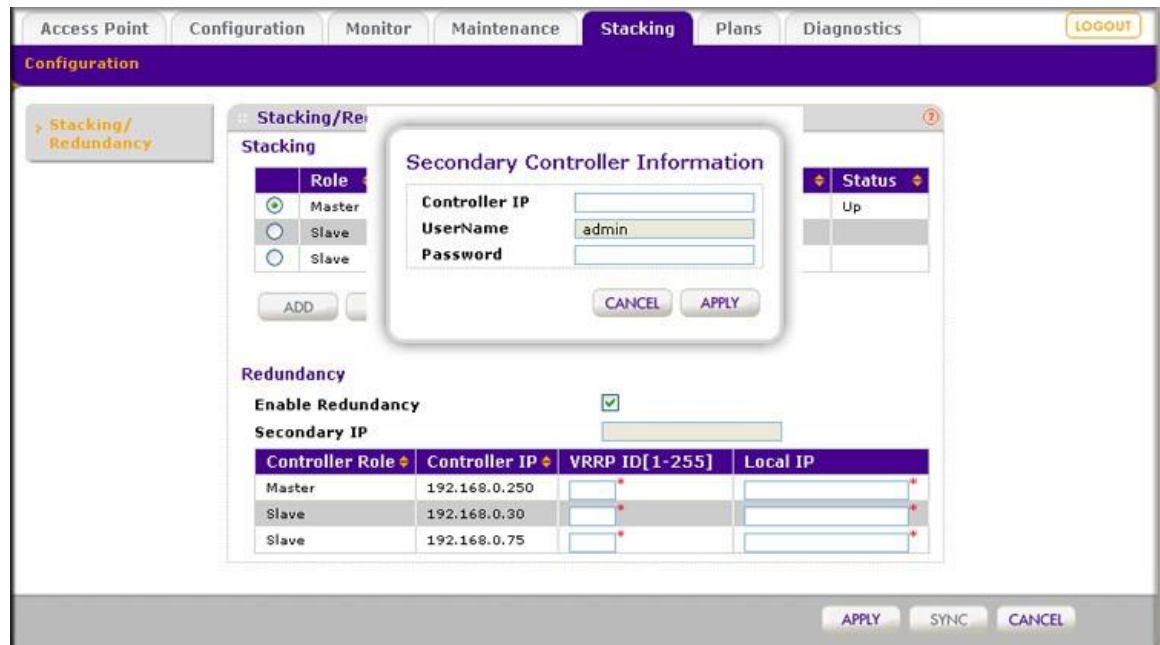
冗長化 (Redundancy) を有効にするには、プライマリーと冗長コントローラーの両方で冗長設定をします。2 台のコントローラーで冗長を設定すると、1 台のプライマリーコントローラーとなります。N:1 冗長の場合は、2 台または 3 台のプライマリーコントローラーとなります。

冗長を設定する

1. **Stacking > Stacking/Redundancy** を選択して **Stacking/Redundancy** 画面を表示します。



2. **Enable Redundancy** チェックボックスを選択します。**Stacking/Redundancy** 画面が拡張され **Redundancy** テーブルが表示され、**Secondary Controller Information** ポップアップウィンドウが表示されます。



3. 以下の表に従い設定をします。

Redundant (or secondary) controller settings

| 設定 | 説明 |
|---------------|--|
| Controller IP | 冗長コントローラーのローカル IP アドレスを指定します。この IP アドレスはフェイルオーバー前後での識別のために割り当ては変わりません。 |
| UserName | ワイヤレスコントローラーの Web 管理インターフェースにログインするための ID で admin 固定です。 |
| Password | 冗長コントローラーにアクセスするためのパスワードを指定します。 |

4. **Apply** ボタンをクリックします。**Redundancy** テーブルの上の **Secondary IP** 欄に冗長コントローラーの IP アドレスが表示されます。
5. スタック中のコントローラーの VRRP ID とローカル IP アドレスを設定し、冗長グループの一部になるようにします。以下の表にしたがい設定します。

Redundancy settings

| Setting | Description |
|-----------------|--|
| Controller Role | 変更不可の欄。プライマリコントローラーがマスターまたはスレーブのどちらかで動作するかを表示します。 メモ: シングルコントローラー冗長の場合、プライマリコントローラーの役割は常にマスターです。 |
| Controller IP | 変更不可の欄。プライマリコントローラーの IP アドレスを表示します。フェイルオーバーが発生した時にこの IP アドレスは冗長コントローラーに引き継がれます。 |
| VRRP ID [1-255] | 冗長グループのプライマリコントローラーに VRRP ID として 1~255 の値を設定します。これによってそれぞれのプライマリコントローラーは冗長コントローラーと一意の関係を持つことができます。 メモ: シングルコントローラー冗長の場合、プライマリコントローラーの役割は常にマスターです。プライマリコントローラーは 1 台であり VRRP ID も一つです。 |
| Local IP | 冗長グループの各プライマリコントローラーに対して、ローカル IP アドレスを指定します。フェイルオーバーが発生しても冗長コントローラーに移ることはありません。プライマリコントローラーのローカル IP アドレスは変更されません。 メモ: シングルコントローラー冗長の場合、1 台のプライマリコントローラーに一つのローカル IP アドレスを入力する必要があります。 |



警告！

冗長を有効にするとワイヤレスコントローラーは再起動し、一時的にネットワーク内の管理されたアクセスポイントのトラフィックに影響が出ます。

6. **Apply** ボタンをクリックして設定を保存します。

メモ: 冗長を設定した後で、**Network monitoring** 画面の **Refresh** ボタンをクリックして冗長設定情報を表示します。

冗長を設定後に冗長コントローラーを変更する

1. **Replace** ボタンをクリックします。**Replacing Controller Information** ポップアップウィンドウが表示されます。

メモ: **Replace** ボタンは冗長設定が有効になった後のみに表示されます。

A screenshot of a dialog box titled "Replacing Controller Information". It contains three input fields: "Local IP" (empty), "UserName" (containing "admin"), and "Password" (empty). At the bottom, there are two buttons: "CANCEL" and "APPLY".

2. 設定を変更します。
3. **Apply** ボタンをクリックします。冗長変更されたローカル IP アドレスは **Redundancy** テーブルに表示されます。

冗長グループを削除する

Enable Redundancy の選択をクリアします。この結果冗長グループの冗長コントローラーは再起動して IP アドレス以外は工場出荷状態に戻ります。

11. ワイヤレスネットワークと構成要素の監視

監視画面ではネットワークとその様々な構成要素のリードオンリーの状態情報を表示します。ほとんどの画面には **Refresh** ボタンがあり、ボタンをクリックして最新の情報を表示することができます。

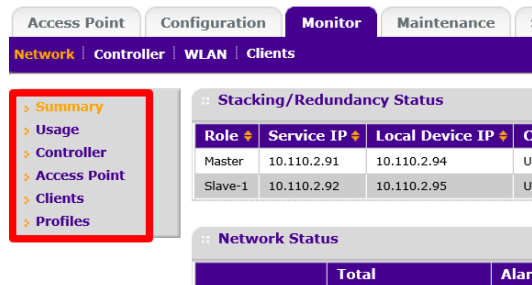
メモ: 多くの情報が表示される表で、表の左下にある **Entry Per Page** ドロップダウンリストの数字を選択することによって画面に表示される項目数を選択することができます。

メモ: この章で表示される画面の間には一貫性はありません。

ネットワーク監視

ネットワークを監視する

1. **Monitor > Network** を選択します。
2. 次のサブメニューリンクの一つを選択してネットワーク監視画面を表示します。



- **Summary:** Network Summary 画面を表示します。
- **Usage:** Network Usage 画面を表示します。
- **Controller:** Controllers 画面を表示します。
- **Access Point:** Access Point 画面を表示します。
- **Clients:** Clients 画面を表示します。
- **Profiles:** Profiles 画面を表示します。

Network Summary 画面を表示する

以下の図はスタックと冗長設定をした場合の Network Summary 画面の例です。

The screenshot displays the Network Summary page with the following data:

| Role | Service IP | Local Device IP | Controller Status | Secondary IP | Active Controller | Backup Status | Sync Status |
|---------|-------------|-----------------|-------------------|--------------|-------------------|---------------|-------------|
| Master | 192.168.1.3 | 192.168.1.7 | Up | 192.168.1.6 | Primary | Reachable | In Sync |
| Slave-1 | 192.168.1.4 | 192.168.1.8 | Up | 192.168.1.6 | Primary | Reachable | In Sync |
| Slave-2 | 192.168.1.5 | 192.168.1.9 | Up | 192.168.1.6 | Primary | Reachable | In Sync |

| Device | Total | Up | Down | Critical | Major |
|---------------|-------|----|------|----------|-------|
| Controllers | 3 | 0 | 0 | 0 | 0 |
| Access Points | 116 | 0 | 0 | 0 | 0 |
| Clients | 1 | NA | NA | NA | NA |

| Controller | Open | WEP | WPA | WPA2 |
|-------------|------|-----|-----|------|
| 192.168.1.3 | 0 | 0 | 0 | 0 |
| 192.168.1.4 | 0 | 0 | 0 | 0 |
| 192.168.1.5 | 0 | 0 | 0 | 1 |

| Rogue AP current | Rogue AP count 24hrs |
|------------------|----------------------|
| 0 | 0 |

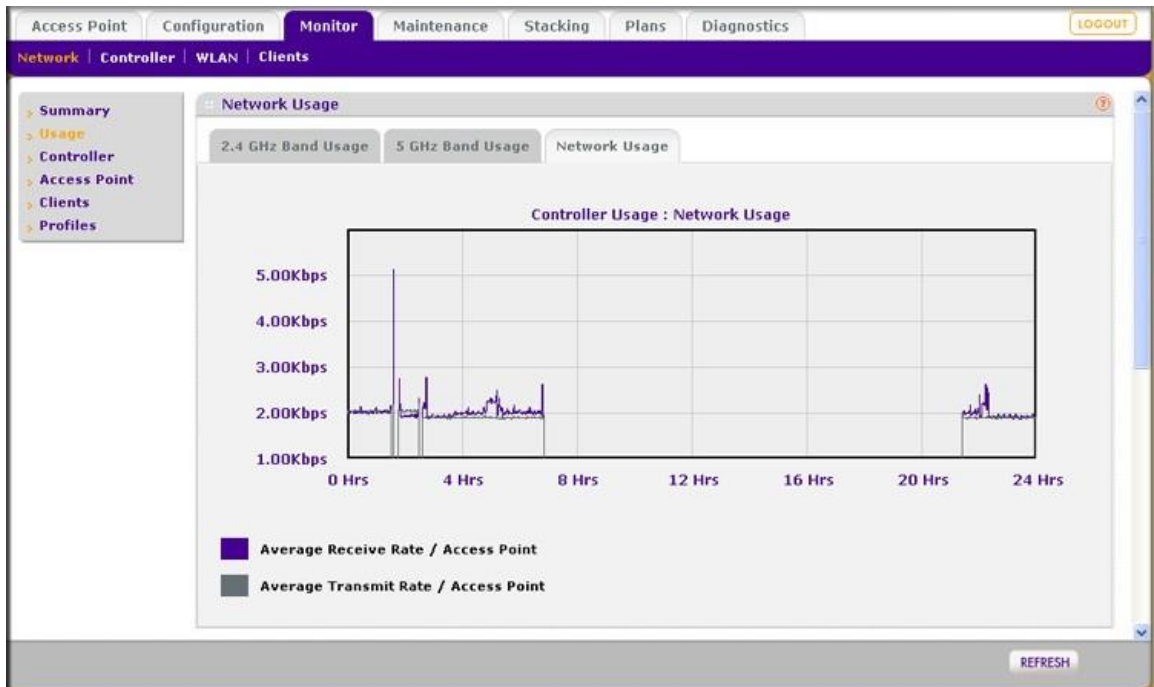
以下の表は Network Summary 画面中の Stacking/Redundancy Status、Network Status、Wireless Clients、Rogue Access Points テーブルの項目の説明です。

Network summary information

| 項目 | 説明 |
|---|---|
| Stacking/Redundancy Status section | |
| Role | スタック構成の時のワイヤレスコントローラーの役割 (Master または Slave) |
| Service IP | コントローラー IP アドレス。この IP アドレスはフェイルオーバー発生後にセカンダリーコントローラーに転送されます。 |
| Local Device IP | 冗長グループ中のプライマリーコントローラーのローカル IP アドレス。この IP アドレスはプライマリーコントローラーに割り当てられたままで、フェイルオーバーが発生してもセカンダリーコントローラーには転送されません。これによってフェイルオーバーの前でプライマリーコントローラーを識別することができます。 |
| Controller Status | ワイヤレスコントローラーの状態 (Up または Down)。 |
| Secondary IP | 冗長グループのセカンダリーコントローラーの IP アドレス。 |
| Active Controller | 冗長グループの中のアクティブなコントローラー (Primary または Secondary) |
| Backup Status | 冗長グループのセカンダリーコントローラーの状態 (Reachable または Not Reachable)。 |

| | | |
|--|--|--|
| Sync Status | 冗長グループ内のワイヤレスコントローラー間の同期 (synchronization) 状態。(In Sync または Not in Sync). | |
| Network Status section 各ワイヤレスコントローラー、アクセスポイント、クライアントについては以下の情報が表示されます。 | | |
| Total | Up | 正常に動作している管理されたデバイスの総数。 |
| | Down | Ping 応答のない管理されたデバイスの数。 |
| Alarms | Critical | ワイヤレスコントローラーはデバイスに Ping 可能だがログイン不可あるいは設定どおりに動作していないもの。 |
| | Major | ワイヤレスコントローラーに設定した設定とは異なっている管理されたデバイスの数。この状況はデバイスが古いファームウェアで動作していたり、デバイスが故障あるいはオフラインの時にコントローラーが設定を変更した時に発生し得ます。 |
| Wireless Clients section 各ワイヤレスコントローラーやワイヤレスクライアントに対して、以下の情報が表示されます。 | | |
| Controller | ワイヤレスクライアントが接続されているアクセスポイントを管理しているワイヤレスコントローラーの IP アドレス。 | |
| Open | Open モードで設定されたセキュリティプロファイルを使う管理されたアクセスポイントに接続されているワイヤレスクライアントの数。 | |
| WEP | WEP で設定されたセキュリティプロファイルを使う管理されたアクセスポイントに接続されているワイヤレスクライアントの数。 | |
| WPA | WPA で設定されたセキュリティプロファイルを使う管理されたアクセスポイントに接続されているワイヤレスクライアントの数。 | |
| WPA2 | WPA2 で設定されたセキュリティプロファイルを使う管理されたアクセスポイントに接続されているワイヤレスクライアントの数。 | |
| Rogue Access Points section | | |
| Rogue AP current | 現在検出された不正アクセスポイントと管理されていない隣接のアクセスポイントの数。 | |
| Rogue AP count 24hrs | 過去 24 時間に検出された不正アクセスポイントと管理されていない隣接のアクセスポイントの数。 | |

ネットワーク使用量 (Network Usage) 表示



Network Usage 画面はネットワーク内のすべてのアクセスポイントで過去 24 時間に送受信された平均データトラフィックレートをグラフィカルに表示します。以下のタブで表示したいデータを選択します。

- **2.4 GHz Band Usage**: 2.4GHz の 802.11b, 802.11bg, and 802.11ng モードの合計の使用量を表示します。
- **5 GHz Band Usage**: 5GHz の 802.11a, 802.11na モードの合計の使用量を表示します。
- **Network Usage**: イーサネットの使用量を表示します。

ワイヤレスコントローラー表示

| Controller IP | Name | Location | Type | Version | Status | Config Status | Config Sync Time |
|---------------|----------|----------|--------|---------------|-------------|---------------|------------------|
| 192.168.0.250 | ve85D102 | | Master | 2.0.11.0_1944 | Up | NA | NA |
| 192.168.0.30 | - | - | - | - | Unreachable | - | NA |

Network Controllers 画面でワイヤレスコントローラーのスタック状態を表示できます。

以下の表に **Network Controllers** 画面の **Controllers** テーブルの項目の説明を示します。

Network controllers information

| 項目 | 説明 |
|------------------|---|
| Controller IP | ワイヤレスコントローラーの IP アドレス |
| Name | ワイヤレスコントローラーの名前 |
| Location | ワイヤレスコントローラーのロケーション |
| Type | スタックでのワイヤレスコントローラーの役割 (Master または Slave) |
| Version | ワイヤレスコントローラーが実行しているファームウェアバージョン |
| Status | ワイヤレスコントローラーのスタック状態 (Up, Unreachable 等) |
| Config Status | ワイヤレスコントローラーのファームウェア設定状態 (Update や Successful 等). メモ: この欄はスレーブとして機能しているワイヤレスコントローラーのみに適用されま す。 |
| Config Sync Time | ワイヤレスコントローラーがファームウェアを同期した時間.. メモ: この欄はスレーブとして機能しているワイヤレスコントローラーのみに適用されま す。 |

アクセスポイント表示

Access Points 画面は横長のため、2 分割して表示します。

| Select | Name | Location | Status | MAC | IP | Model | Remote |
|----------------------------------|---------------|----------------|---------|-------------------|---------------|---------|--------|
| <input checked="" type="radio"/> | netgearA10668 | Administration | healthy | c4:3d:c7:a1:06:60 | 192.168.0.168 | WNAP360 | Remote |
| <input type="radio"/> | netgear782488 | Orthopedics | healthy | c0:3f:0e:7b:24:80 | 192.168.0.163 | WNAP210 | Local |
| <input type="radio"/> | netgear7826D8 | Surgery | healthy | c0:3f:0e:7b:26:d0 | 192.168.0.162 | WNAP210 | Local |



| Sentry | Building | Floor | 2.4 GHz Channel | 5 GHz Channel | Uptime | Controller IP |
|--------|-------------------|---------|-----------------|---------------|------------------|---------------|
| No | Building-Remote-1 | Floor-1 | 1 / 2.412Ghz | 36 / 5.180Ghz | 20 mins, 16 secs | 192.168.0.250 |
| No | Clinic | Floor-1 | 6 / 2.437Ghz | NA | 20 mins, 18 secs | 192.168.0.250 |
| No | Clinic | Floor-1 | 11 / 2.462Ghz | NA | 20 mins, 20 secs | 192.168.0.250 |

Access Point 画面でネットワーク内のすべてのアクセスポイントを監視できます。Next ボタンと Previous ボタンを使って追加のアクセスポイントを表示できます。

以下に Access Point テーブルに表示される項目の説明を示します。

Network access point information

| 項目 | 説明 |
|----------|--|
| Select | ラジオボタンでアクセスポイントを選択します。Details ボタンをクリックすると該当する AP Details ポップアップウィンドウが表示されます。 |
| Name | アクセスポイントの名前。 |
| Location | アクセスポイントのロケーション。 |
| Status | アクセスポイントの状態 (Healthy または Down)。 |
| MAC | アクセスポイントの MAC アドレス。 |
| IP | アクセスポイントの IP アドレス。 |
| Model | アクセスポイントのモデル (WNAP210, WNAP320, WNDAP350, WNDAP360)。(日本国内で販売されていないモデルもあります) |
| Remote | アクセスポイントのサイト設定 (Local または Remote)。 |
| Sentry | 見張りモード (Sentry mode) が有効かどうか。 |
| Building | アクセスポイントが設置されているビル。 |
| Floor | アクセスポイントが設置されているフロア。 |

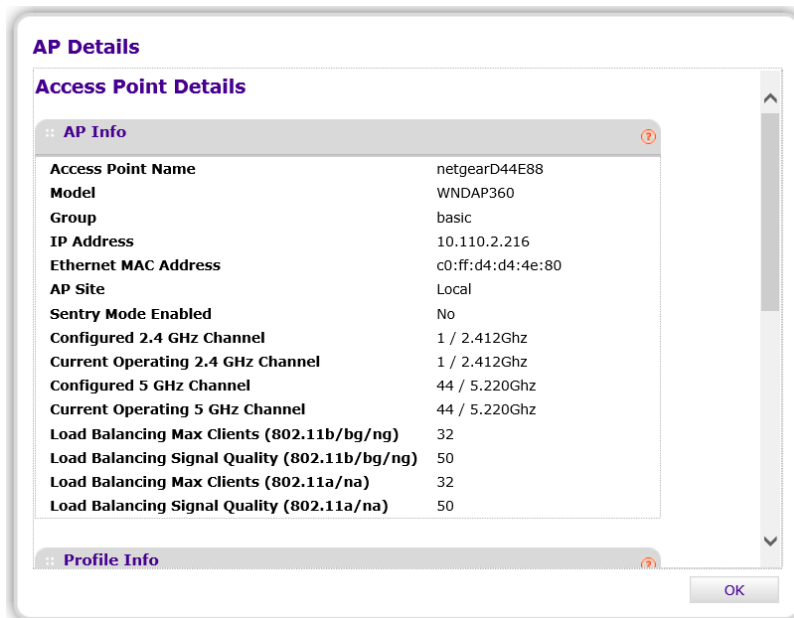
| | |
|-----------------|---|
| 2.4 GHz Channel | アクセスポイントで設定されている 2.4GHz チャンネル。この情報は自動チャンネル設定によって変更されます。 |
| 5 GHz Channel | アクセスポイントで設定されている 5GHz チャンネル。この情報は自動チャンネル設定によって変更されます。 |
| Uptime | アクセスポイントが再起動してからの時間。 |
| Controller IP | アクセスポイントを管理しているコントローラーの IP アドレス。 |

Export ボタンをクリックしてアクセスポイントのリストをエクスポートします。

アクセスポイントの詳細情報を表示するには、**Access Point** テーブルの **Select** 欄のラジオボタンでアクセスポイントを選択し、**Details** ボタンをクリックして **AP Details** ポップアップウィンドウを表示します。

OK ボタンをクリックして **AP Details** ウィンドウをクローズします。

(**AP Details** ウィンドウを 2 分割して表示します)



The screenshot shows the 'AP Details' window with the following sections:

- Profile Info:** A table with columns Type, SSID, Security, and VLAN. It lists two profiles: 802.11b/bg/ng with SSID WNDAP36024G and Security Wpa, and 802.11a/na with SSID WNDAP3605G and Security Wpa.
- Client Info:** A table with columns MAC, SSID, Channel, Mode, Auth, and Cipher.
- Rogue AP Info:** A table with columns Type, Reported, In Same Channel, and In Interfering Channel.
- Statistics:** A table with columns Device, Unicast Packets Received, and Broadcast Packets Received. It shows data for Wired Ethernet (17775 unicast, 122457 broadcast) and Wireless 11bg (0 unicast, 0 broadcast).

以下の表に AP Details ウィンドウの項目の説明を示します。

Network access point details information

| 項目 | 説明 |
|---|---|
| AP Info section | |
| 表示のとおり。 | |
| Profile Info section | |
| 選択されたアクセスポイントに設定されたセキュリティプロファイルについて以下の情報が表示されます。 | |
| Type | プロファイルのタイプ(802.11b/bg/ng または 802.11a/na)。 |
| SSID | セキュリティプロファイルの SSID。 |
| Security | セキュリティプロファイルのセキュリティモード(Open, WEP, WPA, WPA2, WPA/WPA2)。 |
| VLAN | セキュリティプロファイルの VLAN ID または VLAN 名。 |
| Client Info section | |
| 表示される情報はクライアントのアクセスポイントへの接続のセキュリティとタイプに依存します。 | |
| MAC | ワイヤレスクライアントの MAC アドレス。 |
| IP | ワイヤレスクライアントの IP アドレス。 |
| Channel | ワイヤレスクライアントがアクセスポイントにアクセスするために使っているチャンネル。 |
| SSID | ワイヤレスクライアントがアクセスポイントにアクセスするために使っている SSID。 |
| Security | ワイヤレスクライアントがアクセスポイントにアクセスするために使っているセキュリティモード(Open, WEP, WPA, WPA2, WPA/WPA2)。 |
| Rogue AP Info section | |
| 選択したアクセスポイントが検知したすべての不正アクセスポイントと管理されていない隣接のアクセスポイントの以下の情報が表示されます。 | |

| | |
|------------------------|---|
| Type | 不正アクセスポイントが使っているプロファイル(802.11b/bg/ng または 802.11a/na). |
| Reported | ワイヤレスモードでの合計の不正アクセスポイント数。 |
| In Same Channel | 同じチャンネルの不正アクセスポイント数。 |
| In Interfering Channel | 干渉するチャンネルの不正アクセスポイント数。 |
| Statistics | |
| | 送受信したパケット数。 |

クライアント表示

| Select | MAC | IP | AP Location | AP-Name | AP-IP | Building | Floor | Bssid | SSID | Security | Controller IP |
|-----------------------|-------------------|-------------|-------------|---------------|-------------|----------|---------|-------------------|----------|----------|---------------|
| <input type="radio"/> | 00:1E:4C:67:33:82 | 192.168.0.5 | Orthopedics | netgear782488 | 192.168.0.3 | Clinic | Floor-3 | C0:3F:0E:78:24:82 | HQ_11g-2 | Open | 192.168.0.250 |
| <input type="radio"/> | 00:40:F4:F4:7D:C2 | 192.168.0.6 | Orthopedics | netgear782488 | 192.168.0.3 | Clinic | Floor-1 | C0:3F:0E:78:24:81 | HQ_11g-1 | Open | 192.168.0.250 |

Clients でネットワークに接続されているすべてのクライアントを監視することができます。追加のクライアントを表示するには、**Next** ボタンをクリックし、前のクライアントを表示するには **Previous** ボタンをクリックします。以下に Clients テーブルに表示される情報の説明を示します。

Network clients information

| 項目 | 説明 |
|-------------|---|
| Select | ラジオボタンでクライアントを選択します。 Details ボタンをクリックすると該当する Client Details ポップアップウィンドウが表示されます。 Locate ボタンをクリックしてクライアントのフロアマップ上での位置を表示することができます。 |
| MAC | ワイヤレスクライアントの MAC アドレス。 |
| IP | ワイヤレスクライアントの IP アドレス。 |
| AP Location | ワイヤレスクライアントが接続されているアクセスポイントのロケーション。 |
| AP-Name | ワイヤレスクライアントが接続されているアクセスポイントの名前。 |
| AP-IP | ワイヤレスクライアントが接続されているアクセスポイントの IP アドレス。 |
| Building | ワイヤレスクライアントが接続されているアクセスポイントのビル。 |
| Floor | ワイヤレスクライアントが接続されているアクセスポイントのフロア。 |

| | |
|---------------|---|
| BSSID | ワイヤレスクライアントが接続されているアクセスポイントの電波の MAC アドレス。 |
| SSID | ワイヤレスクライアントが接続されているアクセスポイントが使っている SSID。 |
| Security | ワイヤレスクライアントがアクセスポイントに接続するために使っているセキュリティモード (Open, WEP, WPA, WPA2, WPA/WPA2) |
| Controller IP | ワイヤレスクライアントが接続されているアクセスポイントを管理しているワイヤレスコントローラーの IP アドレス。 |

フロアマップでクライアントのロケーションを表示するには、クライアントのラジオボタンを選択し、**Locate** ボタンをクリックします。

Export ボタンをクリックしてクライアントのリストをエクスポートします。

クライアントの詳細情報を表示するには、クライアントをラジオボタンで選択してから **Details** ボタンをクリックし **Client Details** ポップアップウィンドウを表示します。



Cancel ボタンをクリックして **Client Details** ウィンドウをクローズします。

以下に **Client Details** ウィンドウで表示される項目の説明を示します。

Network client details information

| 項目 | 説明 |
|--------------|---------------------------------|
| MAC | ワイヤレスクライアントの MAC アドレス。 |
| Access Point | ワイヤレスクライアントが接続されているアクセスポイントの名前。 |

| | |
|-------------|--|
| BSSID | ワイヤレスクライアントが接続しているアクセスポイントの電波の MAC アドレス。 |
| SSID | ワイヤレスクライアントがアクセスポイントに接続するために使っている SSID。 |
| Frequency | ワイヤレスクライアントがアクセスポイントに接続するために使っているチャンネル周波数。 |
| Auth | ワイヤレスクライアントがアクセスポイントに接続するために使っているセキュリティモード (Open, WEP, WPA, WPA2, WPA/WPA2)。 |
| Client Type | ワイヤレスクライアントがアクセスポイントに接続するために使っているワイヤレスモード (802.11a, b, g, n)。 |
| Cipher | ワイヤレスクライアントが使っている暗号化方式(WEP, AES, TKIP, TKIP + AES)。 |
| AID | クライアントの AID (association ID) |
| RSSI | ワイヤレスクライアントの RSSI(received signal strength indicator) |
| Tx Power | ワイヤレスクライアントの送信出力。 |
| Tx Rate | ワイヤレスクライアントの送信速度 (Mbps)。 |
| Tx Bytes | ワイヤレスクライアントが送信したバイト数。 |
| Rx Rate | ワイヤレスクライアントの受信速度 (Mbps)。 |
| Rx Bytes | ワイヤレスクライアントが受信したバイト数。 |
| Tx packets | ワイヤレスクライアントが送信したパケット数。 |
| Rx Packets | ワイヤレスクライアントが受信したパケット数。 |

セキュリティプロファイル監視

| SSID | Security | Radio Mode | Status | Controller IP | Group Name |
|----------|----------|---------------|----------|---------------|------------|
| NG_11g | Open | 802.11b/bg/ng | Active | 192.168.0.250 | basic |
| NG_11g-1 | Open | 802.11b/bg/ng | Active | 192.168.0.250 | basic |
| NG_11g-2 | Open | 802.11b/bg/ng | Active | 192.168.0.250 | basic |
| NG_11g-3 | Open | 802.11b/bg/ng | Active | 192.168.0.250 | basic |
| NG_11g-4 | Open | 802.11b/bg/ng | Active | 192.168.0.250 | basic |
| NG_11g-5 | Open | 802.11b/bg/ng | Active | 192.168.0.250 | basic |
| NG_11g-7 | Open | 802.11b/bg/ng | Active | 192.168.0.250 | basic |
| NG_11a | Open | 802.11a/na | Active | 192.168.0.250 | basic |
| NG_11a-1 | Open | 802.11a/na | Active | 192.168.0.250 | basic |
| NG_11g-0 | Wpa/Wpa2 | 802.11b/bg/ng | Inactive | 192.168.0.250 | Group-1 |
| NG_11g-1 | Wpa/Wpa2 | 802.11b/bg/ng | Inactive | 192.168.0.250 | Group-1 |
| NG_11a-0 | Open | 802.11a/na | Inactive | 192.168.0.250 | Group-1 |
| NG_11g-0 | Open | 802.11b/bg/ng | Inactive | 192.168.0.250 | Group-2 |
| NG_11a-0 | Open | 802.11a/na | Inactive | 192.168.0.250 | Group-2 |
| NG_11g-0 | Open | 802.11b/bg/ng | Inactive | 192.168.0.250 | Group-3 |
| NG_11a-0 | Open | 802.11a/na | Inactive | 192.168.0.250 | Group-3 |

Profiles 画面でネットワークのすべてのセキュリティプロファイルを表示できます。追加のセキュリティプロファイルを表示するには、Next ボタンをクリックし、前のセキュリティプロファイルを表示するには Previous ボタンをクリックします。以下に Profiles テーブルに表示される情報の説明を示します。

Network security profiles information

| 項目 | 説明 |
|---------------|---|
| SSID | セキュリティプロファイルの SSID。 |
| Security | セキュリティプロファイルのセキュリティモード(Open, WEP, WPA, WPA2, WPA/WPA2)。 |
| Radio Mode | セキュリティプロファイルのワイヤレスモード(802.11b/bg/ng または 802.11a/na)。 |
| Status | セキュリティプロファイルの状態 (Active または Inactive)。 |
| Controller IP | セキュリティプロファイルが設定されているワイヤレスコントローラーの IP アドレス。 |
| Group Name | セキュリティプロファイルグループ名。 |

Export ボタンをクリックしてセキュリティプロファイルのリストを表示します。

ワイヤレスコントローラー監視

特定のワイヤレスコントローラーを監視するには、そのコントローラーの Web 管理インターフェースにログインし、Monitor Controller 画面を使います。

メモ: ワイヤレスコントローラーをスタックしている場合、スタックについての似た情報を Network Monitor 画面で見ることができます。

ワイヤレスコントローラーを監視する

1. Monitor > Controller を選択します。
2. 次のサブメニューリンクの一つを選択してワイヤレスコントローラー監視画面を表示します。

The screenshot shows the web management interface for a wireless LAN controller. The top navigation bar includes tabs for Access Point, Configuration, Monitor, Maintenance, Stacking, Plans, and Diagnostics. The 'Monitor' tab is active, and the breadcrumb trail shows Network > Controller > WLAN > Clients. The left sidebar menu is highlighted with a red box, listing various sub-menus. The main content area displays several panels:

- Self +**: A dropdown menu for selecting the controller to monitor.
- Network Status**: A table showing the status of devices and alarms.

| Device | Total | | Alarms | |
|---------------|-------|------|----------|-------|
| | Up | Down | Critical | Major |
| Access Points | 2 | 0 | 0 | 0 |
| Clients | 0 | NA | NA | NA |
- Wireless Clients**: A table showing the status of wireless clients.

| Open | WEP | WPA | WPA2 |
|------|-----|-----|------|
| 0 | 0 | 0 | 0 |
- Rogue Access Points**: A table showing the status of rogue access points.

| | |
|----------------------|---|
| Rogue AP current | 0 |
| Rogue AP count 24hrs | 0 |
- Network Info**: A table showing network information.

| | |
|---------------------------|----------------------------|
| Firmware Version | 2.5.0.35 |
| Controller Uptime | 13 hours, 23 mins, 43 secs |
| Last Reboot | Sun Jan 24 19:31:10 2016 |
| Last Configuration Change | Mon Jan 25 00:00:20 2016 |
| Last Channel Allocation | Mon Jan 25 00:00:20 2016 |
| Last Admin Login | Mon Jan 25 08:54:40 2016 |
- Redundancy Status**: A table showing the redundancy status.

| | |
|----------------------|------------------|
| Controller Mode | Secondary |
| Redundancy State | Active |
| Primary Status | Reachable |
| Sync Status | Sync In Progress |
| Secondary IP Address | 10.110.2.93 |
| Primary IP Address | 10.110.2.94 |
| Virtual IP | 10.110.2.91 |

- Summary
- Usage.
- Access Points
- Clients
- Neighboring Clients
- Rogue AP
- Profiles
- DHCP Lease
- Captive Portal Users

Wireless Controller Summary 画面を表示する

The screenshot displays the 'Monitor' tab of the ProSAFE management interface. The 'Self' dropdown is set to 'Self'. The main content area is divided into several sections:

- Network Status:** A table showing device status.

| Device | Total | | Alarms | |
|---------------|-------|------|----------|-------|
| | Up | Down | Critical | Major |
| Access Points | 2 | 0 | 0 | 0 |
| Clients | 0 | NA | NA | NA |
- Wireless Clients:** A table showing client connection counts.

| Open | WEP | WPA | WPA2 |
|------|-----|-----|------|
| 0 | 0 | 0 | 0 |
- Rogue Access Points:** A table showing rogue AP counts.

| | |
|----------------------|---|
| Rogue AP current | 0 |
| Rogue AP count 24hrs | 0 |
- Network Info:** A list of system information.

| | |
|---------------------------|----------------------------|
| Firmware Version | 2.5.0.35 |
| Controller Uptime | 18 hours, 39 mins, 23 secs |
| Last Reboot | Sun Jan 24 19:31:10 2016 |
| Last Configuration Change | Mon Jan 25 00:00:20 2016 |
| Last Channel Allocation | Mon Jan 25 00:00:20 2016 |
| Last Admin Login | Mon Jan 25 14:09:16 2016 |
- Redundancy Status:** A list of redundancy-related information.

| | |
|----------------------|------------------|
| Controller Mode | Secondary |
| Redundancy State | Active |
| Primary Status | Reachable |
| Sync Status | Sync In Progress |
| Secondary IP Address | 10.110.2.93 |
| Primary IP Address | 10.110.2.94 |
| Virtual IP | 10.110.2.91 |

A 'REFRESH' button is located at the bottom right of the summary area.

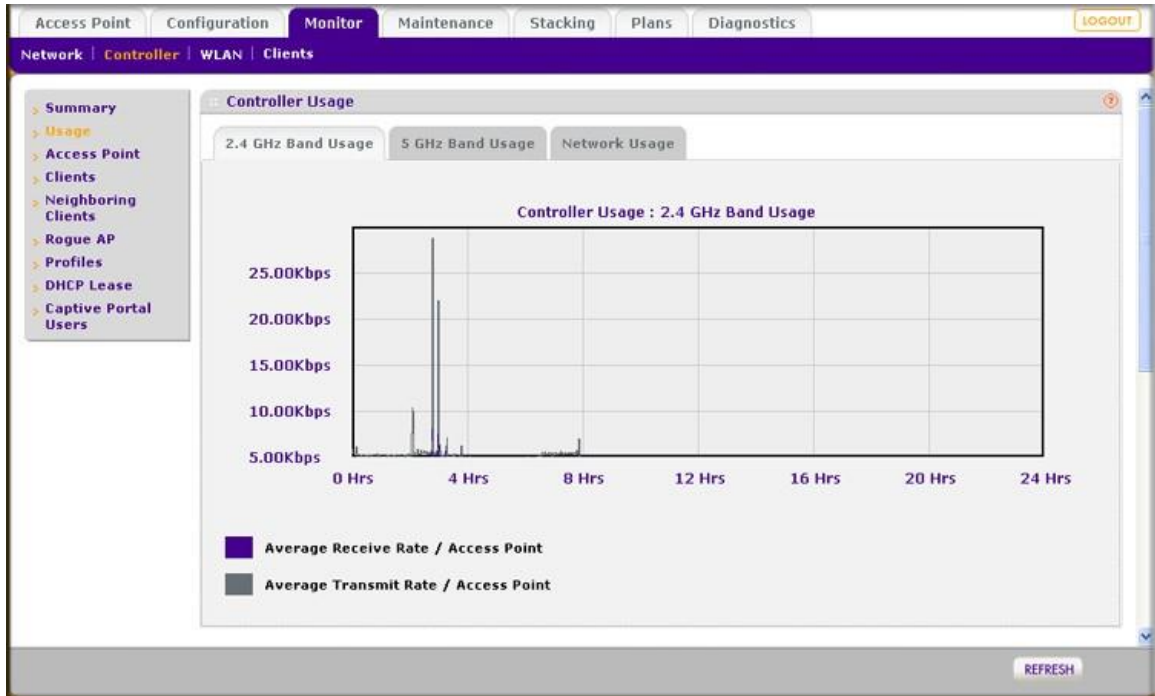
以下の表に Controller Summary 画面の Network Status, Wireless Clients, Rogue Access Points, Network Info, Redundancy Status タブに表示される情報の説明を示します。

Controller summary information

| 項目 | 説明 | |
|-----------------------------------|--|--|
| Network Status section | | |
| 各アクセスポイントとクライアントに関して以下の情報が表示されます。 | | |
| Total | Up | 正常に動作している管理されたデバイスの総数。 |
| | Down | Ping 応答のない管理されたデバイスの数。 |
| Alarms | Critical | ワイヤレスコントローラーはデバイスに Ping 可能だがログイン不可あるいは設定どおりに動作していないもの。 |
| | Major | ワイヤレスコントローラーに設定した設定とは異なっている管理されたデバイスの数。この状況はデバイスが古いファームウェアで動作していたり、デバイスが故障あるいはオフラインの時にコントローラーが設定を変更した時に発生し得ます。 |
| Wireless Clients section | | |
| 各アクセスポイントに関して以下の情報が表示されます。 | | |
| Open | Open モードで設定されたセキュリティプロファイルを使う管理されたアクセスポイントに接続されているワイヤレスクライアントの数。 | |
| WEP | WEP で設定されたセキュリティプロファイルを使う管理されたアクセスポイントに接続されているワイヤレスクライアントの数。 | |

| | |
|--|--|
| WPA | WPA で設定されたセキュリティプロファイルを使う管理されたアクセスポイントに接続されているワイヤレスクライアントの数。 |
| WPA2 | WPA2 で設定されたセキュリティプロファイルを使う管理されたアクセスポイントに接続されているワイヤレスクライアントの数。 |
| Rogue Access Points section | |
| Rogue AP current | 現在検出された不正アクセスポイントと管理されていない隣接のアクセスポイントの数。 |
| Rogue AP count 24hrs | 過去 24 時間に検出された不正アクセスポイントと管理されていない隣接のアクセスポイントの数。 |
| Network Info section | |
| 表示どおり。 | |
| Redundancy Status section この情報はワイヤレスコントローラーの冗長が設定されている時のみ表示されます。 | |
| Controller Mode | ワイヤレスコントローラーの冗長モード。(Primary または Secondary). |
| Redundancy State | 冗長グループの状態 (Active, Down, Sync in progress, Firmware mismatch). |
| Secondary Status | 冗長グループのセカンダリーコントローラーの状態 (Reachable or Not reachable). |
| Sync Status | 冗長グループのワイヤレスコントローラー間の同期状態 (In Sync または Not in Sync). |
| Primary IP Address | 冗長グループのプライマリーコントローラーの IP アドレス。 |
| Secondary IP Address | 冗長グループのセカンダリーコントローラーの IP アドレス。 |
| Virtual IP | 冗長グループのプライマリーとセカンダリーコントローラーが使う共通 IP アドレス、常にアクティブコントローラーが保有します。 |

ワイヤレスコントローラー使用量表示



Controller Usage 画面はネットワーク内のすべてのアクセスポイントで過去 24 時間に送受信された平均データトラフィックレートをグラフィカルに表示します。以下のタブで表示したいデータを選択します。

- **2.4 GHz Band Usage:** 2.4GHz の 802.11b, 802.11g, and 802.11n モードの合計の使用量を表示します。
- **5 GHz Band Usage:** 5GHz の 802.11a, 802.11n モードの合計の使用量を表示します。
- **Network Usage:** イーサネットの使用量を表示します。

アクセスポイント表示

Controller Access Point 画面は横長のため 2 分割で表示します。

Access Point Configuration **Monitor** Maintenance Stacking Plans Diagnostics

Network > **Controller** > WLAN > Clients

- Summary
- Usage
- Access Point**
- Clients
- Neighboring Clients
- Rogue AP
- Profiles
- DHCP Lease
- Captive Portal Users

Access Point

| Select | Name | Location | Status | MAC | IP | Model |
|----------------------------------|---------------|----------------|---------|-------------------|---------------|----------|
| <input checked="" type="radio"/> | netgearA10668 | Administration | healthy | c4:3d:c7:a1:06:60 | 192.168.0.168 | WNDAP360 |
| <input type="radio"/> | netgear7B2488 | Orthopedics | healthy | c0:3f:0e:7b:24:80 | 192.168.0.163 | WNAP210 |
| <input type="radio"/> | netgear7B26D8 | Surgery | healthy | c0:3f:0e:7b:26:d0 | 192.168.0.162 | WNAP210 |

LOGOUT

| Remote | Sentry | Building | Floor | 2.4 GHz Channel | 5 GHz Channel | Uptime |
|--------|--------|-------------------|---------|-----------------|---------------|------------------|
| Remote | No | Building-Remote-1 | Floor-1 | 1 / 2.412Ghz | 36 / 5.180Ghz | 20 mins, 16 secs |
| Local | No | Clinic | Floor-1 | 6 / 2.437Ghz | NA | 20 mins, 18 secs |
| Local | No | Clinic | Floor-1 | 11 / 2.462Ghz | NA | 20 mins, 20 secs |

REFRESH DETAILS EXPORT

LOGOUT

| Sentry | Building | Floor | 2.4 GHz Channel | 5 GHz Channel | Uptime | Controller IP |
|--------|-------------------|---------|-----------------|---------------|------------------|---------------|
| No | Building-Remote-1 | Floor-1 | 1 / 2.412Ghz | 36 / 5.180Ghz | 20 mins, 16 secs | 192.168.0.250 |
| No | Clinic | Floor-1 | 6 / 2.437Ghz | NA | 20 mins, 18 secs | 192.168.0.250 |
| No | Clinic | Floor-1 | 11 / 2.462Ghz | NA | 20 mins, 20 secs | 192.168.0.250 |

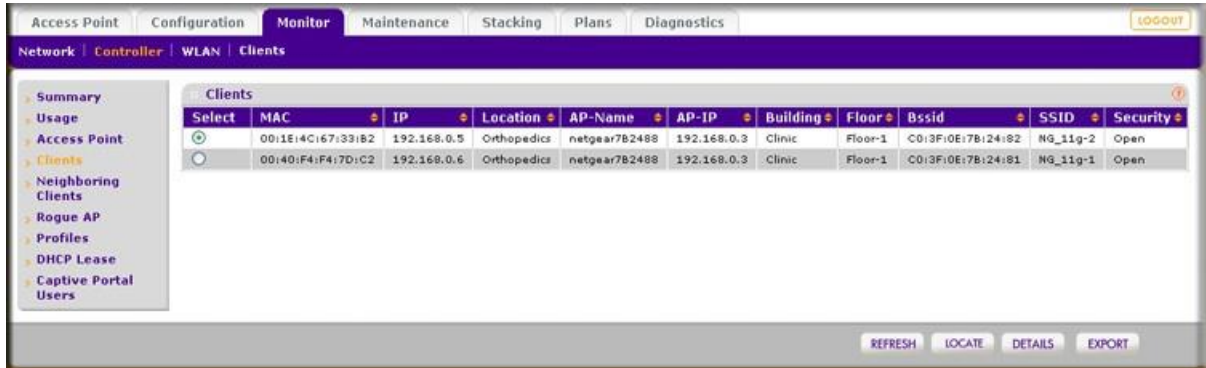
REFRESH DETAILS EXPORT

Controller Access Point 画面でネットワーク内のワイヤレスコントローラーが管理しているすべてのアクセスポイントを監視できます。**Next** ボタンと **Previous** ボタンを使って追加のアクセスポイントを表示できます。

Export ボタンをクリックしてアクセスポイントのリストをエクスポートすることができます。

アクセスポイントの詳細情報を表示するには、**Access Point** テーブルの **Select** 欄のラジオボタンでアクセスポイントを選択し、**Details** ボタンをクリックして **AP Details** ポップアップウィンドウを表示します。

クライアント表示



Controller Clients 画面ではワイヤレスコントローラーで管理されているアクセスポイントに接続しているすべてのクライアントを表示することができます。追加のクライアントを表示するには、**Next** ボタンをクリックし、前のクライアントを表示するには **Previous** ボタンをクリックします。

フロアマップでクライアントのロケーションを表示するには、クライアントのラジオボタンを選択し、**Locate** ボタンをクリックします。

Export ボタンをクリックしてクライアントのリストをエクスポートします。

クライアントの詳細情報を表示するには、クライアントをラジオボタンで選択してから **Details** ボタンをクリックし **Client Details** ポップアップウィンドウを表示します。

近隣クライアント表示



Controller Neighboring Clients 画面でワイヤレスコントローラーが検知した不正アクセスポイントまたは既知のアクセスポイントに接続しているクライアントを表示することができます。追加の近隣ク

クライアントを表示するには、**Next** ボタンをクリックし、前の近隣クライアントを表示するには **Previous** ボタンをクリックします。

以下に **Controller Neighboring Clients** 画面の **Neighboring Clients** テーブルの項目の説明を示します。

Neighboring clients information

| 項目 | 説明 |
|--------|--|
| Locate | ラジオボタンでフロアマップ上に表示する近隣クライアントを選択します。 |
| MAC | 近隣クライアントの MAC アドレス。 |
| BSSID | 近隣クライアントが接続されているアクセスポイントの電波の MAC アドレス。 |
| RSSI | 近隣クライアントの RSSI(received signal strength indicator) |
| Rogue | 近隣クライアントの接続しているアクセスポイントが不正アクセスポイントか否か。(Yes または No) |

フロアマップで近隣クライアントのロケーションを表示するには、近隣クライアントのラジオボタンを選択し、**Locate** ボタンをクリックします。

近隣クライアントを切断するには、近隣クライアントをチェックボックスで選択し、**Disconnect** ボタンをクリックします

Export ボタンをクリックして近隣クライアントのリストをエクスポートします。

不正アクセスポイント表示

| Select | MAC | SSID | Channel | Privacy | Last Beacon | Category | Known/Unknown | Name |
|----------------------------------|-------------------|-------------|---------|-----------|--------------------------|----------|---------------|------|
| <input checked="" type="radio"/> | c0:3f:0e:b4:66:da | | 11 | Secured | Tue Sep 21 15:55:28 2010 | Neighbor | Unknown | |
| <input type="radio"/> | 00:18:f3:ef:db:98 | Customer ID | 11 | Secured | Tue Sep 21 15:55:28 2010 | Neighbor | Unknown | |
| <input type="radio"/> | c0:3f:0e:85:c5:40 | ng wlan | 11 | Secured | Tue Sep 21 15:55:28 2010 | Neighbor | Unknown | |
| <input type="radio"/> | c0:3f:0e:85:cd:60 | ng wlan | 11 | Secured | Tue Sep 21 15:55:28 2010 | Neighbor | Unknown | |
| <input type="radio"/> | c0:3f:0e:85:c5:41 | ngguest | 11 | Secured | Tue Sep 21 15:55:28 2010 | Neighbor | Unknown | |
| <input type="radio"/> | c0:3f:0e:85:cd:61 | ngguest | 11 | Secured | Tue Sep 21 15:55:28 2010 | Neighbor | Unknown | |
| <input type="radio"/> | 00:14:6c:08:5e:fa | TMOHSSEFF | 6 | Unsecured | Tue Sep 21 15:55:28 2010 | Neighbor | Unknown | |
| <input type="radio"/> | 00:24:b2:64:8e:70 | TS350-2G | 6 | Secured | Tue Sep 21 15:54:28 2010 | Neighbor | Unknown | |
| <input type="radio"/> | 06:24:b2:51:b0:d9 | FryaDemo | 44 | Unsecured | Tue Sep 21 15:55:28 2010 | Neighbor | Unknown | |
| <input type="radio"/> | c0:3f:0e:b4:66:d6 | Bell66D6 | 11 | Secured | Tue Sep 21 15:55:28 2010 | Neighbor | Unknown | |
| <input type="radio"/> | 00:18:f3:ef:db:8c | Wireless | 11 | Secured | Tue Sep 21 15:55:28 2010 | Neighbor | Unknown | |
| <input type="radio"/> | 00:24:b2:5c:81:d6 | NTGR24GR | 9 | Secured | Tue Sep 21 15:55:28 2010 | Neighbor | Unknown | |
| <input type="radio"/> | 00:18:f3:ef:da:8a | Customer ID | 11 | Secured | Tue Sep 21 15:55:28 2010 | Neighbor | Unknown | |
| <input type="radio"/> | c0:3f:0e:85:c5:50 | ng wlan | 48 | Secured | Tue Sep 21 15:55:28 2010 | Neighbor | Unknown | |
| <input type="radio"/> | c0:3f:0e:85:cd:70 | ng wlan | 36 | Secured | Tue Sep 21 15:55:28 2010 | Neighbor | Unknown | |
| <input type="radio"/> | c0:3f:0e:b4:66:cc | | 11 | Secured | Tue Sep 21 15:55:28 2010 | Neighbor | Unknown | |

Controller Rogue AP 画面でワイヤレスコントローラーが検知したすべての不正アクセスポイントを表示することができます。追加の不正アクセスポイントを表示するには、**Next** ボタンをクリックし、前の不正アクセスポイントを表示するには **Previous** ボタンをクリックします。

以下に **Controller Rogue AP** 画面の **Rogue AP** テーブルの項目の説明を示します。

Controller rogue AP information

| 項目 | 説明 |
|---------------|---|
| Select | ラジオボタンをつかってフロアマップで位置を表示する不正アクセスポイントを選択します。 |
| MAC | 不正アクセスポイントの MAC アドレス。 |
| SSID | 不正アクセスポイントの使っている SSID。 |
| Channel | 不正アクセスポイントが使っているチャンネル。 |
| Privacy | 不正アクセスポイントのセキュリティ (Secured または Unsecured)。 |
| Last Beacon | 不正アクセスポイントが送信した最後のビーコン。 |
| Category | 不正アクセスポイントの区分。ドロップダウンリストで Neighbor , Rogue , または All をフィルターできます。 |
| Known/Unknown | 不正アクセスポイントの状態。ドロップダウンリストで Known または Unknown を選択できます。 |
| Name | 不正アクセスポイントの (割り当てた) 名前。 |

フロアマップで不正アクセスポイントの位置を表示するには、不正アクセスポイントのラジオボタンを選択し、**Locate** ボタンをクリックします。

Export ボタンをクリックして不正アクセスポイントのリストをエクスポートします。

セキュリティプロファイル表示

The screenshot shows the 'Monitor' tab of the ProSAFE Controller interface. The 'Profiles' section is active, displaying a table of wireless profiles. The table has the following columns: SSID, Security, Radio Mode, Status, and Group Name. The profiles listed include various NG_11g and NG_11a configurations with different security settings (Open, Wpa/Wpa2) and radio modes (802.11b/bg/ng, 802.11a/na). Some profiles are marked as 'Active' while others are 'Inactive'. Navigation buttons for 'PREVIOUS' and 'NEXT' are visible at the bottom of the table, along with 'REFRESH' and 'EXPORT' buttons.

| SSID | Security | Radio Mode | Status | Group Name |
|----------|----------|---------------|----------|------------|
| NG_11g | Open | 802.11b/bg/ng | Active | basic |
| NG_11g-1 | Open | 802.11b/bg/ng | Active | basic |
| NG_11g-2 | Open | 802.11b/bg/ng | Active | basic |
| NG_11g-3 | Open | 802.11b/bg/ng | Active | basic |
| NG_11g-4 | Open | 802.11b/bg/ng | Active | basic |
| NG_11g-5 | Open | 802.11b/bg/ng | Active | basic |
| NG_11g-7 | Open | 802.11b/bg/ng | Active | basic |
| NG_11a | Open | 802.11a/na | Active | basic |
| NG_11a-1 | Open | 802.11a/na | Active | basic |
| NG_11g-0 | Wpa/Wpa2 | 802.11b/bg/ng | Inactive | Group-1 |
| NG_11g-1 | Wpa/Wpa2 | 802.11b/bg/ng | Inactive | Group-1 |
| NG_11a-0 | Open | 802.11a/na | Inactive | Group-1 |
| NG_11g-0 | Open | 802.11b/bg/ng | Inactive | Group-2 |
| NG_11a-0 | Open | 802.11a/na | Inactive | Group-2 |
| NG_11g-0 | Open | 802.11b/bg/ng | Inactive | Group-3 |
| NG_11a-0 | Open | 802.11a/na | Inactive | Group-3 |

Controller Profiles 画面でワイヤレスコントローラーが管理しているアクセスポイントのすべてのセキュリティプロファイルを表示することができます。追加のセキュリティプロファイルを表示するには、**Next** ボタンをクリックし、前のセキュリティプロファイルを表示するには **Previous** ボタンをクリックします。

Export ボタンをクリックしてプロファイルのリストをエクスポートできます。

DHCP リース表示

The screenshot shows the 'Monitor' tab of the ProSAFE Controller interface. The 'DHCP Leases' section is active, displaying a table of DHCP lease information. The table has the following columns: Host Name, IP, End Time, End Date, MAC, and VLAN. The leases listed include various MAC addresses and IP addresses (192.168.0.29 to 192.168.0.28) with their respective end times and dates (2010/09/21 to 2010/09/22). All leases are assigned to the 'Management' VLAN. Navigation buttons for 'REFRESH' and 'EXPORT' are visible at the bottom of the table.

| Host Name | IP | End Time | End Date | MAC | VLAN |
|---------------------------|--------------|----------|------------|-------------------|------------|
| Unknown | 192.168.0.29 | 09:55:17 | 2010/09/22 | 00:26:f2:9a:1b:a0 | Management |
| VWC-0004-MAC-000201040000 | 192.168.0.20 | 17:43:02 | 2010/09/21 | 00:02:01:04:00:00 | Management |
| VWC-0002-MAC-000201020000 | 192.168.0.21 | 17:43:02 | 2010/09/21 | 00:02:01:02:00:00 | Management |
| Unknown | 192.168.0.30 | 11:37:02 | 2010/09/22 | 00:26:f2:8b:2d:80 | Management |
| VWC-0001-MAC-000201010000 | 192.168.0.22 | 17:43:02 | 2010/09/21 | 00:02:01:01:00:00 | Management |
| VWC-0003-MAC-000201030000 | 192.168.0.23 | 17:43:02 | 2010/09/21 | 00:02:01:03:00:00 | Management |
| VWC-0005-MAC-000201050000 | 192.168.0.24 | 17:42:52 | 2010/09/21 | 00:02:01:05:00:00 | Management |
| VWC-0001-MAC-000101060000 | 192.168.0.25 | 17:43:02 | 2010/09/21 | 00:01:01:06:00:00 | Management |
| VWC-0001-MAC-001f33e98044 | 192.168.0.26 | 14:25:26 | 2010/09/22 | 00:1f:33:e9:80:44 | Management |
| VWC-0002-MAC-001f33e9804b | 192.168.0.27 | 14:25:26 | 2010/09/22 | 00:1f:33:e9:80:4b | Management |
| VWC-0001-MAC-000101010000 | 192.168.0.28 | 14:25:27 | 2010/09/22 | 00:01:01:01:00:00 | Management |

DHCP Leases 画面でワイヤレスコントローラーの DHCP サーバーから IP アドレスが割り当てられた現在の DHCP クライアントを表示することができます。追加の DHCP リースを表示するには、**Next** ボタンをクリックし、前の DHCP リースを表示するには **Previous** ボタンをクリックします。

以下に **Controller DHCP Leases** 画面の DHCP Leases テーブルの項目の説明を示します。

Controller DHCP lease information

| 項目 | 説明 |
|-----------|------------------------------------|
| Host Name | DHCP クライアントのホスト名。 |
| IP | DHCP クライアントに割り当てられている IP アドレス。 |
| End Time | DHCP クライアントの DHCP リース終了時間。 |
| End Date | DHCP クライアントの DHCP リース終了日。 |
| MAC | DHCP クライアントの MAC アドレス。 |
| VLAN | DHCP サーバーとクライアントが接続するのに使っている VLAN。 |

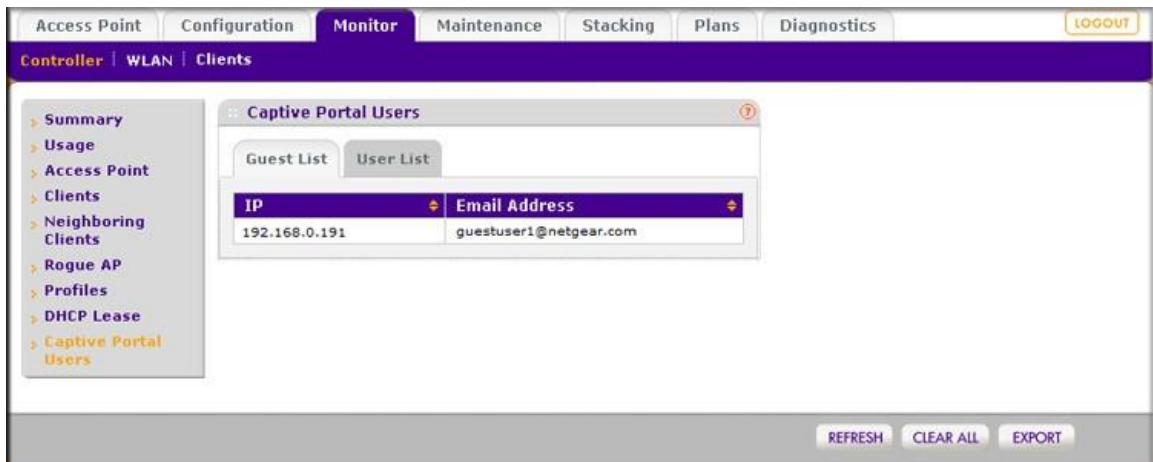
Export ボタンをクリックして DHCP リースのリストをエクスポートします。

キャプティブポータルゲストとユーザー

Controller Captive Portal Users 画面でワイヤレスコントローラーが管理しているアクセスポイントのキャプティブポータルにログインしている現在のゲストとユーザーを表示することができます。

ゲストリストを表示する

Guest List タブをクリックします。**Guest List** 画面が表示されます。



Guest List テーブルはログインしているゲストの IP アドレスとメールアドレスを表示します。追加のゲストを表示するには、**Next** ボタンをクリックし、前のゲストを表示するには **Previous** ボタンをクリックします。

Clear All ボタンをクリックしてすべてのユーザー情報をクリアします。

Export ボタンをクリックしてキャプティブポートあるゲストのリストをエクスポートします。

キャプティブポータルユーザーリストを表示する

User List タブをクリックします。**User List** 画面が表示されます。



Guest List テーブルはユーザー名とパスワードを使ってキャプティブポータルにログインする必要のあるログインしたキャプティブポータルユーザーの情報を示します。追加のユーザーを表示するには、**Next** ボタンをクリックし、前のユーザーを表示するには **Previous** ボタンをクリックします。

以下の表に **User List** テーブルの項目の説明を示します。

Captive portal user information

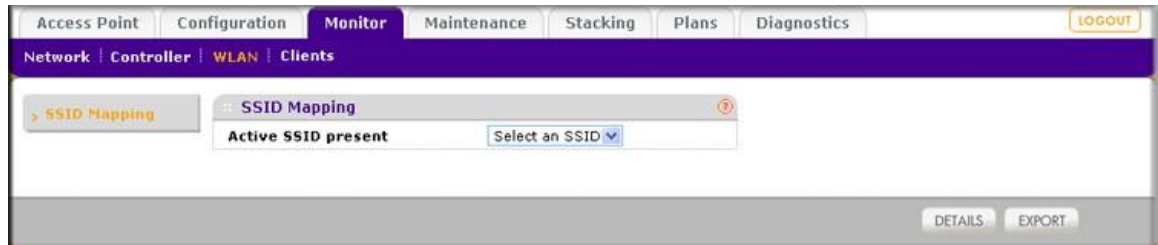
| 項目 | 説明 |
|--------------|------------------------------|
| User Name | ユーザーのログイン名。 |
| Account Name | ユーザーに関連付けられたアカウント名(存在するならば)。 |
| User IP | ユーザーの IP アドレス。 |
| User MAC | ログインしているユーザーのデバイスの MAC アドレス。 |
| Login Time | ユーザーがログインした時間。 |
| Expiry Time | ユーザーのログインアクセスが失効する時間。 |

Export ボタンをクリックしてキャプティブポータルユーザーのリストをエクスポートします。

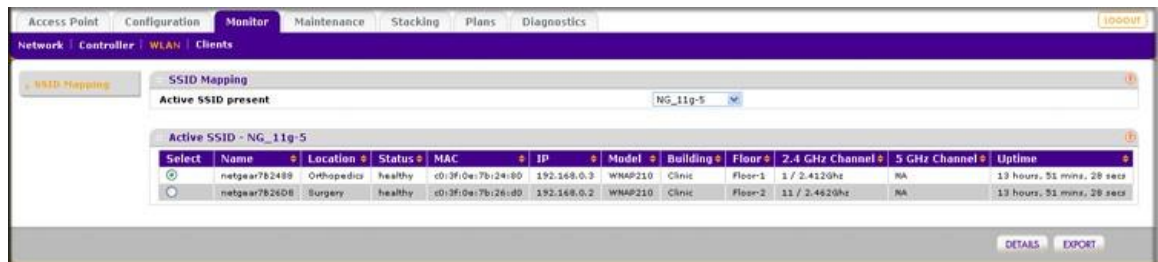
SSID 監視

SSID を監視する To monitor the active SSIDs in the network:

1. **Monitor > WLAN** を選択して **SSID Mapping** 画面を表示します。



2. **Active SSID present** ドロップダウンリストで SSID を選択します。選択した SSID の **Active SSID** テーブルが表示されます。



SSID Mapping 画面の **Active SSID** テーブルで選択した SSID で機能しているすべてのアクセスポイントを表示することができます。追加のアクセスポイントを表示するには、**Next** ボタンをクリックし、前のアクセスポイントを表示するには **Previous** ボタンをクリックします。

Export をクリックしてアクセスポイントのリストをエクスポートします。

アクセスポイントの詳細情報を表示するには、アクセスポイントをラジオボタンで選択してから **Details** ボタンをクリックし **AP Details** ポップアップウィンドウを表示します。

クライアント監視

クライアントを監視する

1. **Monitor > Clients** を選択します。
2. 以下のメニューから選択します。
 - **Local Clients List**
 - **Blacklisted Clients**

ローカルクライアント表示

| Select | MAC | IP | Location | AP-Name | AP-IP | AP MAC | Building | Floor | Bssid | SSID | Security |
|----------------------------------|----------------------|-------------|-------------|---------------|-------------|-------------------|----------|---------|-------------------|----------|----------|
| <input checked="" type="radio"/> | 00:1E:4C:67:33:B2 | 192.168.0.5 | Orthopedics | netgear782488 | 192.168.0.3 | C0:3F:0E:78:24:80 | Clinic | Floor-1 | C0:3F:0E:78:24:82 | NG_11g-2 | Open |
| <input type="radio"/> | 00:14:01:F4:F4:7D:C2 | 192.168.0.6 | Orthopedics | netgear782488 | 192.168.0.3 | C0:3F:0E:78:24:80 | Clinic | Floor-1 | C0:3F:0E:78:24:81 | NG_11g-1 | Open |
| <input type="radio"/> | 20:D6:07:2C:70:7E | 0.0.0.0 | Surgery | netgear7826D8 | 192.168.0.2 | C0:3F:0E:78:26:D0 | Clinic | Floor-2 | C0:3F:0E:78:26:D2 | NG_11g-2 | Open |

Local Client List 画面ではワイヤレスコントローラーに管理されているアクセスポイントに認証されて接続されているすべてのクライアントを監視することができます。追加のクライアントを表示するには、**Next** ボタンをクリックし、前のクライアントを表示するには **Previous** ボタンをクリックします。

メモ: **Local Client List** 画面ではネットワークのすべてのクライアントを表示します（すなわち、ネットワークのすべてのワイヤレスコントローラーに管理されているクライアントです）。それに対して、**Controller Clients** 画面では1台のコントローラーに管理されているクライアントのみを表示します。

フロアマップでクライアントの位置を表示するには、クライアントのラジオボタンを選択し、**Locate** ボタンをクリックします。

Export ボタンをクリックしてクライアントのリストをエクスポートします。

クライアントの詳細情報を表示するには、クライアントをラジオボタンで選択してから **Details** ボタンをクリックし **Client Details** ポップアップウィンドウを表示します。

ブラックリストクライアント表示

| Select | MAC | TYPE | AP-Name | AP-IP | SSID | RSSI | Count | Last Seen |
|----------------------------------|-------------------|-----------------------|------------|--------------|------------|------|-------|--------------------------|
| <input checked="" type="radio"/> | 00:02:01:02:00:00 | Authentication Failed | ap1-8b2d80 | 192.168.0.30 | veriWave_g | 49 | 2 | Mon Sep 20 17:55:25 2010 |
| <input type="radio"/> | 00:02:01:04:00:00 | Authentication Failed | ap1-8b2d80 | 192.168.0.30 | veriWave_g | 49 | 3 | Mon Sep 20 18:02:25 2010 |
| <input type="radio"/> | 00:02:01:01:00:00 | Authentication Failed | ap1-8b2d80 | 192.168.0.30 | veriWave_g | 49 | 2 | Mon Sep 20 18:02:10 2010 |

Blacklisted Clients 画面ではアクセスポイントに接続しようとして認証情報が異なっていて接続を拒否されたクライアントと MAC ACL によって MAC アドレスがブロックされたクライアントを監視することができます。追加のクライアントを表示するには、**Next** ボタンをクリックし、前のクライアントを表示するには **Previous** ボタンをクリックします。表示します。

以下の表に **Blacklisted Clients** 画面の **Blacklisted Clients** テーブルで表示される項目の説明を示します。

Blacklisted clients information

| 項目 | 説明 |
|-----------|---|
| Select | ラジオボタンでブラックリストされたクライアントを選択してフロアマップに表示します。 |
| MAC | ブラックリストされたクライアントの MAC アドレス。 |
| Type | アクセス拒否された理由、認証失敗(Authentication Failed)またはブロックされた MAC アドレス (Denied Client)。 |
| AP-Name | ブラックリストされたクライアントが接続しようとしたアクセスポイントの名前。 |
| AP-IP | ブラックリストされたクライアントが接続しようとしたアクセスポイントの IP アドレス。 |
| RSSI | ブラックリストされたクライアントの RSSI。 |
| SSID | ブラックリストされたクライアントが接続しようとしたアクセスポイントの SSID。 |
| Count | クライアントが認証に失敗した回数。 |
| Last Seen | 最後のブラックリストされたクライアントがログインしようとした時間。 |

フロアマップでブラックリストされたクライアントの位置を表示するには、クライアントのラジオボタンを選択し、**Locate** ボタンをクリックします。

Export ボタンをクリックしてブラックリストされたクライアントのリストをエクスポートします。

12. トラブルシューティング

基本機能のトラブルシューティング

ワイヤレスコントローラーの電源を入れた後、以下のイベントが順に発生します。

1. 電源を入れた直後、Power LED が点灯します。
2. 約 2 分後、以下を確認します。
 - a. Test LED が消灯します。
 - b. 機器が接続されている LAN ポートの左側の LED が点灯します。

左側の LED が点灯している LAN ポートで、1000Mbps(1Gbps)の機器がつながっているポートの右側の LED は緑色の LED が点灯します。100Mbps の場合はオレンジ、10Mbps の場合は消灯します。

上の状態にならない場合は以降の項目を確認します。

Power LED が点灯しない

ワイヤレスコントローラーの電源を入れても、どの LED も点灯しない場合は、電源ケーブルがワイヤレスコントローラーとコンセントに接続されていることを確認します。

問題が解消しない場合は、ハードウェア障害の可能性があります。サポートに連絡してください。

Test LED が消灯しない

ワイヤレスコントローラーの電源を入れ、Test LED は約 2 分間点灯後、ワイヤレスコントローラーの起動が終了すると消灯します。Test LED が消灯しない場合はワイヤレスコントローラーの内部に問題がある可能性があります。

数分待っても Test LED が消灯しない場合は、以下のことを試します。

- 電源を切り、再度電源を入れてワイヤレスコントローラーが正常に起動するかどうかを見る。
- ワイヤレスコントローラーの設定を工場出荷状態に戻してみる。ワイヤレスコントローラーの IP アドレスはデフォルト(192.168.0.250)に戻ります。

問題が解消しない場合は、ハードウェア障害の可能性があります。サポートに連絡してください。

LAN ポートの LED が点灯しない

イーサネット接続をしても LAN ポートの LED が点灯しない場合、以下を試してみます。

- ワイヤレスコントローラーと接続されているルーター、スイッチのコネクターが接続されていることを確認します。

- 接続されているルーター、スイッチの電源が入っていることを確認します。
- 正しいケーブルを使っていることを確認します。

Web 管理インターフェースのトラブルシューティング

ワイヤレスコントローラーの Web 管理インターフェースにアクセスできない場合、以下の問題判別を試します。多くの場合は以下のどれかです。

イーサネットケーブル

PC とワイヤレスコントローラー（または接続されているスイッチ等）とのイーサネット接続を確認します。

IP アドレス設定

- PC の IP アドレスがワイヤレスコントローラーのサブネットと同じであることを確認します。推奨のアドレス形態を使っている場合は、PC の IP アドレスは固定で 192.168.0.210、サブネットマスクは 255.255.255.0 です。

メモ: お使いの PC のアドレスが 169.254.x.x のような場合:

Windows や Mac は DHCP サーバーから返答がない場合、自分で IP アドレスを設定します。これらの IP アドレスは 169.254.x.x となります。このアドレスになっていた場合、接続を確認して PC を再起動してみます。

-
- ワイヤレスコントローラーの IP アドレスが変更されており、その IP アドレスが不明の場合、ワイヤレスコントローラーの設定を工場出荷状態にリセットします。工場出荷時のワイヤレスコントローラーの IP アドレスは 192.168.0.250 です。

メモ: ワイヤレスコントローラーを初期化して設定を失いたくない場合は、ワイヤレスコントローラーを再起動し、その際のワイヤレスコントローラーが送信するパケットをキャプチャーし (Wireshark 等を利用)、パケットから IP アドレスを見つけます。ARP パケットからワイヤレスコントローラーの IP アドレスを発見することができます。

インターネットブラウザ

- Web 管理インターフェースにログインするときに [https://\(IP アドレス\)](https://(IP アドレス))ではなく、[http://\(IP アドレス\)](http://(IP アドレス))を使っているか確認します。
- お使いのブラウザで Java, JavaScript または ActiveX が有効になっているか確認します。インターネットエクスプローラーをお使いの場合は、更新ボタンをクリックして Java アプレットがロードされていることを確認します。
- ブラウザーを終了し、再起動してみます。
- 正しいログイン情報を使っているか確認します。工場出荷設定はログイン名: **admin**, パスワード: **password** となります。ログイン名、パスワードは大文字と小文字を区別します。キーボードの CapsLock がオンになっていないか確認します。

Web 管理インターフェースで変更した情報がワイヤレスコントローラー保存されていない場合、以下を確認してください。

- 設定を変更、入力した場合、忘れずに **Apply** ボタンをクリックしてください。Apply ボタンをクリックせずに他の設定画面に移動すると、変更は失われます。
- Web ブラウザーの **Refresh(更新)** または **Reload(リロード)** ボタンをクリックします。変更は適用されていても画面情報が更新されていない場合があります。

ファームウェアのアップグレード後、ブラウザが Web 管理インターフェースで最新の機能を表示していない場合、ブラウザのキャッシュを消去してから画面を更新してみてください。

Ping ユーティリティを使って TCP/IP ネットワークをトラブルシュートする

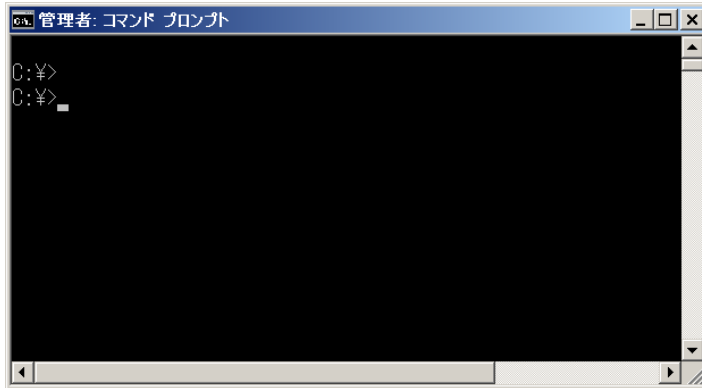
ほとんどの TCP/IP でベースやルーターは Ping ユーティリティを持っていて、エコーリクエストパケット (Ping) を宛先デバイスに送信することができます。デバイスはそれに対してエコーリプライで返答します。Ping ユーティリティを使うことよって容易に TCP/IP ネットワークのトラブルシュートができます。

ワイヤレスコントローラーへの LAN 接続を確認する

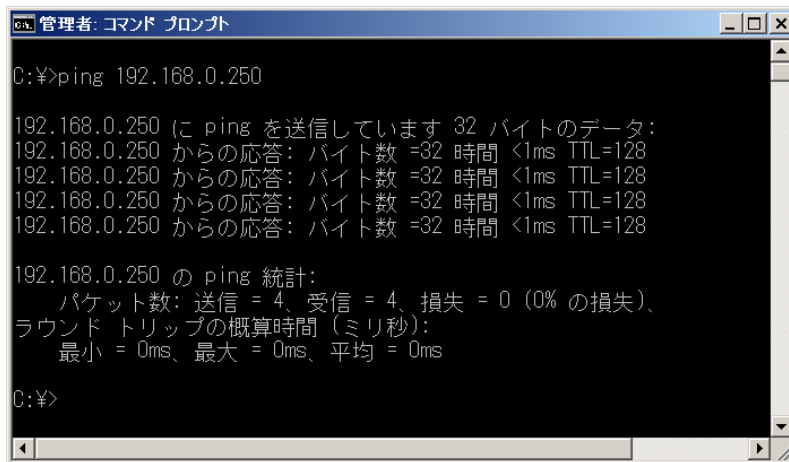
お使いの PC からワイヤレスコントローラーに対して Ping してワイヤレスコントローラーへの LAN 接続が正しく設定されているかを確認することができます。

WindowsPC からワイヤレスコントローラーに Ping する

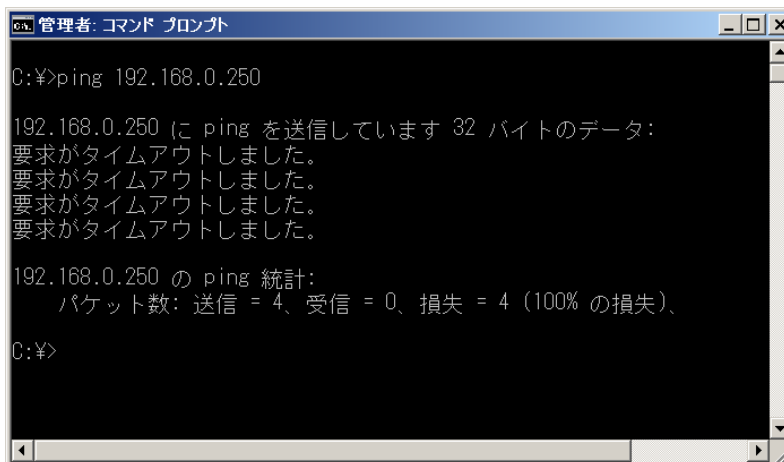
1. コマンドプロンプトを開きます。



2. コマンドプロンプトに Ping (IP アドレス)と入力して Enter キーを押します。以下は 192.168.0.250 に Ping した例です。



3. 上のような結果が表示されていれば接続されています。
4. 以下のような結果の場合は接続できていません。



接続ができていない場合は、以下の原因が考えられます。

物理接続不良

- LAN LED が点灯していることを確認します。
- 対向のインターフェースやスイッチの LED が点灯していることを確認します。

誤ったネットワーク設定

- イーサネットカードドライバーソフトウェアと TCP/IP ソフトウェアがインストールされて設定されていることを確認します。
- ワイヤレスコントローラーとコンピューターの IP アドレスが正しく設定され、同じサブネット上にあることを確認します。

ファクトリーデフォルトボタンを使ってデフォルト設定を復元する

ワイヤレスコントローラーにアクセスできるならば、**Reboot/Reset Controllers** 画面(Maintenance > Backup/Restore を選択)を使ってソフトまたはハードリセットをすることができます。

ワイヤレスコントローラーにアクセスできない時は、リアパネルの **Factory Default** ボタンを長押しして工場出荷状態に戻します。

すべての情報を消去し、工場出荷設定を復元する

1. **Factory Default** ボタンを Test LED が点灯し、その後点滅するまで(約 8 秒以上)押したままにします。
2. **Factory Default** ボタンから手を離します。数分後 Test LED が消灯してリセットが完了します。

メモ: 工場出荷後ワイヤレスコントローラーのデフォルト LAN IP アドレス者 192.168.0.250 になります。デフォルトログインユーザー名: admin, パスワード: password になります。

日時の問題

Time Settings 画面は現在の日時を表示します。ワイヤレスコントローラーは NTP(Network Time Protocol)を使ってインターネット上のタイムサーバーから現在の時間を取得します。各ログの項目は日時情報と一緒に記録されます。

時間表示がおかしい時はコントローラーがタイムサーバーに接続できていません。ワイヤレスコントローラーがインターネットに接続できることを確認してください。ワイヤレスコントローラーを設定した時は、最低 5 分待って日時を確認してください。

アクセスポイントの問題

発見 (Discovery) の問題

ワイヤレスコントローラーがアクセスポイントを一つも発見できない時、以下を確認します。

すべてのアクセスポイントに対して

- ワイヤレスコントローラーが LAN に接続されていることを確認します。
- アクセスポイントが異なる VLAN 内で動作していたり、異なるサブネットに属していたり、既にスタンドアロンモードで動作している時には、正しい IP アドレスの範囲を入力しているか確認してください。
- 既にインストールされていてスタンドアロンモードで動作しているアクセスポイントが SSH および SNMP が有効になっていることを確認してください。
- UDP ポート 7890 がファイヤーウォールでブロックされていないことを確認します。
- ファクトリーデフォルト設定のアクセスポイントが同じレイヤー2 ネットワークに存在する場合は一度に発見されるアクセスポイントは 1 台のみとなります。1 台を管理リストに追加し、IP アドレスを変更し再度ディスカバリーをするという手順を繰り返すこととなります。
- アクセスポイントのファームウェアが前提バージョンを満たしているかを確認します。

レイヤー3 ネットワークにインストールされているアクセスポイントに対して

次の中のどれかが有効になっていることを確認します。

- ワイヤレスコントローラーとアクセスポイント間で IP アドレス 254.0.100.250 のマルチキャストルーティングが有効であることを確認します。
- DHCP サーバーで DHCP オプション 43 (vendor-specific information) が有効であることを確認します。

リモートアクセスポイントに対して

- DHCP サーバーで DHCP オプション 43 (vendor-specific information) が有効であることを確認します。
- 以下のポートがファイヤーウォールでブロックされていないことを確認します。
 - TCP ポート 22.
 - UDP ポート 69, 123, 138, 161, 6650. (ポート 7890 に加えて)
- NAT 配下に配置するアクセスポイントは NAT ルーター配下に設置する前に管理されたアクセスポイントに変換されていることを確認します。

接続問題

アクセスポイントがスタンドアロン AP モードから管理 AP モードに変換されるとき、アクセスポイントの固定 IP アドレスは DHCP サーバーから割り当てられる IP アドレスに変更されます。この動作によって管理されたアクセスポイントが重複のない IP アドレスを持つことを確実にします。

DHCP サーバーが存在しない、あるいはアクセスポイントが DHCP サーバーに接続できない場合、アクセスポイントは IP アドレスを取得しようとする Connecting 状態のままになります。DHCP サーバーがネットワークに存在しない場合、ワイヤレスコントローラーの DHCP サーバーを設定します。DHCP サーバーが利用可能になると、アクセスポイントは Connecting 状態から Connected 状態に変わります。

ネットワークパフォーマンスと不正アクセスポイント検出

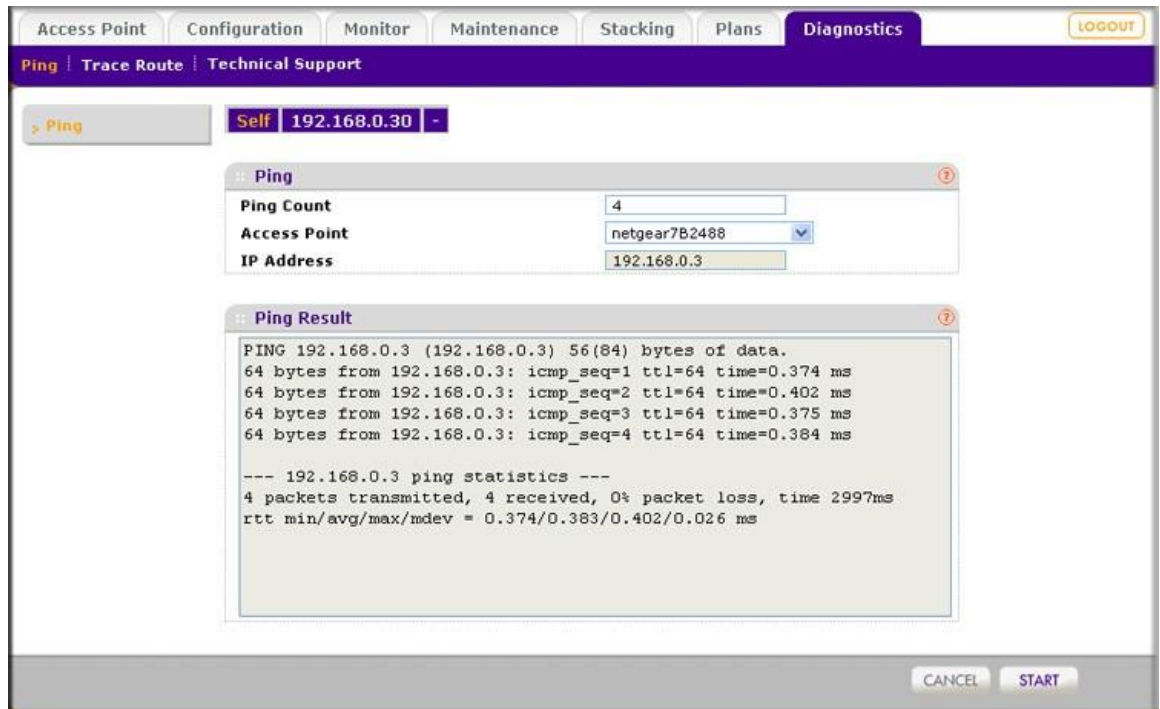
不正アクセスポイント検出が有効になると、有効になっているアクセスポイントは短い時間オフチャネルとなり、ネットワークパフォーマンスに影響を与えます。セキュリティに対する懸念がネットワークパフォーマンスに優先されるなら、一時的に High または Aggressive な不正アクセスポイント周期を選択できます。ネットワークパフォーマンスがセキュリティの懸念よりも優先されるなら、Low または Medium の周期を選択します。通常は Low を推奨します。

ワイヤレスコントローラーで診断ツールを使う

ワイヤレスコントローラーの診断機能の一つとして、ワイヤレスコントローラーから管理されたアクセスポイントに Ping あるいはトレースルートをすることができます。

アクセスポイントに Ping する

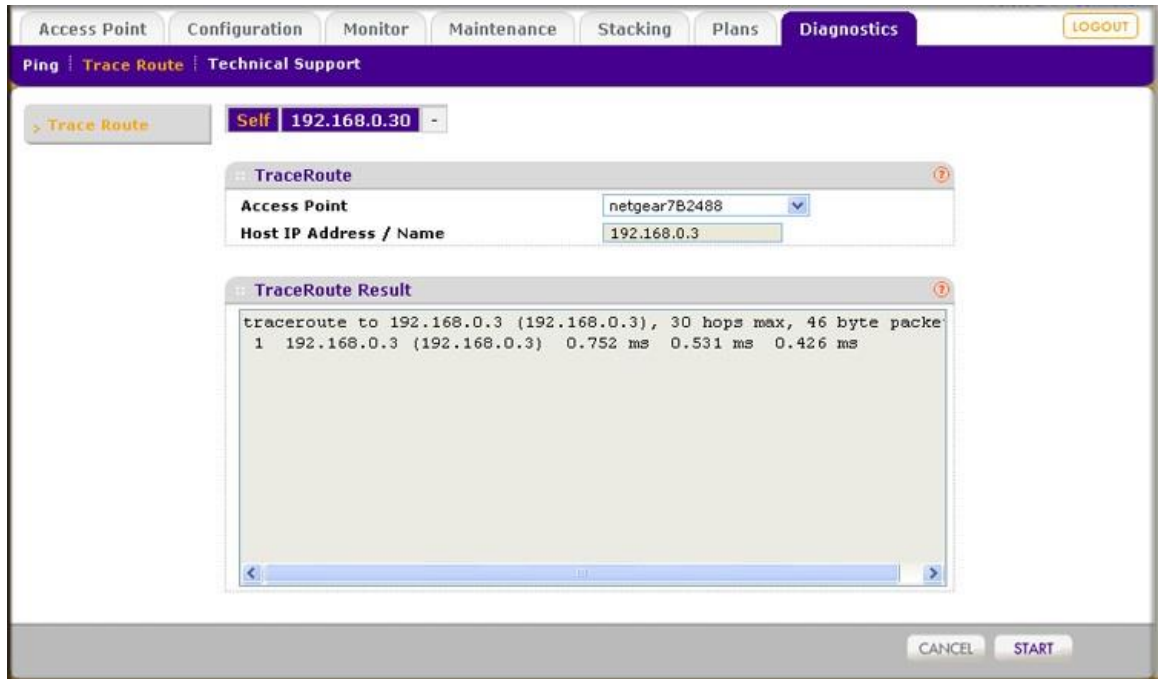
1. **Diagnostics** > **Ping** を選択して Ping 画面を表示します。



2. **Ping Count** 欄に送信する Ping パケット数を記入します。(デフォルトは 10 です)
3. **Access Point** ドロップダウンリストで Ping するアクセスポイントを選択します。選択後、**IP Address** 欄に IP アドレスが表示されます。
4. **Start** ボタンをクリックします。**Ping Result** 欄に結果が表示されます。

アクセスポイントにトレースルートする

1. **Diagnostics** > **Trace Route** を選択して **Trace Route** 画面を表示します。
2. **Access Point** ドロップダウンリストでトレースルートするアクセスポイントを選択します。選択後、**IP Address** 欄に IP アドレスが表示されます。
3. **Start** ボタンをクリックします。**Trace Route Result** 欄に結果が表示されます。



13. 工場出荷設定と技術仕様

仕様

You can restore the wireless controller to its factory default settings on the **Reboot/Reset Controllers** 画面またはリアパネルの **Factory Defaults** ボタンでワイヤレスコントローラーの工場出荷設定を復元することができます。ワイヤレスコントローラーは以下の表の工場出荷設定に戻ります。

Factory default settings

| 機能 | | デフォルト設定 |
|------|-------------------------|----------------------|
| ログイン | ユーザーログイン URL | http://192.168.0.250 |
| | ユーザー名(大文字小文字を識別します) | admin |
| | ログインパスワード(大文字小文字を識別します) | password |
| LAN | LAN IP | 192.168.0.250 |
| | サブネットマスク | 255.255.255.0 |
| | デフォルトゲートウェイ | 192.168.0.1 |
| | タイムゾーン | PST |
| | SNMP | 無効 |

技術仕様

| 機能 | 仕様 |
|---------------|--|
| 電氣的仕様 | 100-240V, AC/50-60 Hz DC 5V/8A (内部電源装置) |
| 寸法(W x H x D) | 26.1 x 4.3 x 44 (cm) |
| 重量 | 2.912kg |
| 動作温度・湿度 | 0° ~45°C 相対湿度 90%以下 (結露なきこと) |
| 保管温度・湿度 | -20° ~70°C 相対湿度 95%以下 (結露なきこと) |
| 取得規格 | FCC Class A, CE, WEEE, RoHS |

以下にパスワードの要件を示します。

Password requirements

| Web 管理インターフェースパス | | ユーザータイプまたはデータ暗号化 | 制限 | |
|--|--------------------|---|--------------------|-------|
| | | | 可能な文字 | 長さ |
| Maintenance > User Management > Management tab | | <ul style="list-style-type: none"> Administrator Read Only Guest Provisioning License Management Only | 英数字と特殊文字 | 最大 31 |
| Maintenance > User Management > Captive Portal tab | | Captive portal user | 英数字と特殊文字 | 最大 31 |
| Maintenance > User Management > WiFi Clients tab | | Wi-Fi user | 英数字 | 最大 31 |
| Basic Profile: 1. Configuration > Profile > Basic > Radio. 2. Select a profile. 3. Make a selection from the Network Authentication drop-down list. | Shared Key | 64-bit WEP | 16 進数 | 10 固定 |
| | | 128-bit WEP | 16 進数 | 26 固定 |
| | | 152-bit WEP | 16 進数 | 32 固定 |
| | WPA-PSK | TKIP | 英数字と特殊文字、引用符(')は除く | 最大 63 |
| | | TKIP + AES | | |
| | WPA2-PSK | AES | 英数字と特殊文字、引用符(')は除く | 最大 63 |
| | | TKIP + AES | | |
| | WPA-PSK & WPA2-PSK | TKIP + AES | 英数字と特殊文字、引用符(')は除く | 最大 63 |
| | | | | |
| Advanced Profile: 1. Configuration > Profile > Advanced > Radio. 2. Select a group. 3. Click Edit. 4. Select a profile. 5. Make a selection from the Network Authentication drop-down list. | Shared Key | 64-bit WEP | 16 進数 | 10 固定 |
| | | 128-bit WEP | 16 進数 | 26 固定 |
| | | 152-bit WEP | 16 進数 | 32 固定 |
| | WPA-PSK | TKIP | 英数字と特殊文字、引用符(')は除く | 最大 63 |
| | | TKIP + AES | | |
| | WPA2-PSK | AES | 英数字と特殊文字、引用符(')は除く | 最大 63 |
| | | | | |

| | | | | |
|---|------------------------------|-------------------|----------|--------|
| | | TKIP + AES | | |
| | WPA-PSK & WPA2-PSK | TKIP + AES | | |
| Configuration > Security > Authentication Server | External RADIUS Server | Shared Secret | 英数字と特殊文字 | 最大 127 |
| | External LDAP Server | Domain Admin User | 英数字と特殊文字 | 最大 32 |