D-Link DWC-2000

Wireless Controller

ユーザマニュアル

D-Link
Building Networks for People

安全にお使いいただくために

ご自身の安全を確保し、システムを破損から守るために、以下に記述する安全のための指針をよくお読みください。

安全上のご注意　必ずお守りください

本製品を安全にお使いいただくために、以下の項目をよくお読みになり必ずお守りください。

⚠危険	この表示を無視し、間違った使い方をすると、死亡または重傷を負うおそれがあります。
⚠警告	この表示を無視し、間違った使い方をすると、火災や感電などにより人身事故になるおそれがあります。
⚠注意	この表示を無視し、間違った使い方をすると、傷害または物的損害が発生するおそれがあります。

記号の意味　🚫 してはいけない**「禁止」**内容です。　❗ 必ず実行していただく**「指示」**の内容です。

⚠危険

- 禁止　分解・改造をしない
  火災、やけど、けが、感電などの原因となります。
- 禁止　ぬれた手でさわらない
  感電の原因となります。
- 禁止　水をかけたり、ぬらしたりしない
  内部に水が入ると、火災、感電、故障の原因となります。
- 禁止　水などの液体（飲料水、汗、海水、ペットの尿など）でぬれた状態で触ったり、電源を入れたりしない
  火災、やけど、けが、感電、故障の原因となります。
- 禁止　各種端子やスロットに水などの液体（飲料水、汗、海水、ペットの尿など）をいれない。万が一、入ってしまった場合は、直ちに電源プラグをコンセントから抜く
  火災、やけど、けが、感電、故障の原因となります。
- 禁止　油煙、湯気、湿気、埃の多い場所、高温になる場所や熱のこもりやすい場所（火のそば、暖房器具のそば、こたつや布団の中、直射日光の当たる場所、炎天下の車内、風呂場など）、振動の激しい場所では、使用、保管、放置しない
  火災、やけど、けが、感電、故障の原因となります。
- 禁止　内部に金属物や燃えやすいものを入れない
  火災、感電、故障の原因となります。
- 禁止　砂や土、泥をかけたり、直に置いたりしない。また、砂などが付着した手で触れない
  火災、やけど、けが、感電、故障の原因となります。
- 禁止　電子レンジ、IH 調理器などの加熱調理機、圧力釜など高圧容器に入れたり、近くに置いたりしない
  火災、やけど、けが、感電、故障の原因となります。

⚠警告

- 禁止　落としたり、重いものを乗せたり、強いショックを与えたり、圧力をかけたりしない
  故障の原因となります。
- 禁止　発煙、焦げ臭い匂いの発生などの異常状態のまま使用しない
  感電、火災の原因になります。
  使用を止めて、ケーブル / コード類を抜いて、煙が出なくなってから販売店に修理をご依頼ください。
- 禁止　表示以外の電圧で使用しない
  火災、感電、または故障の原因となります。
- 禁止　たこ足配線禁止
  たこ足配線などで定格を超えると火災、感電、または故障の原因となります。
- ❗ 設置、移動のときは電源プラグを抜く
  火災、感電、または故障の原因となります。
- 禁止　雷鳴が聞こえたら、ケーブル / コード類にはさわらない
  感電の原因となります。
- 禁止　ケーブル / コード類や端子を破損させない
  無理なねじり、引っ張り、加工、重いものの下敷きなどは、ケーブル / コードや端子の破損の原因となり、火災、感電、または故障の原因となります。
- ❗ 本製品付属の AC アダプタもしくは電源ケーブルを指定のコンセントに正しく接続して使用する
  火災、感電、または故障の原因となります。
- 禁止　各光源をのぞかない
  光ファイバケーブルの断面、コネクタおよび本製品のコネクタや LED をのぞきますと強力な光源により目を損傷するおそれがあります。
- 禁止　各種端子やスロットに導電性異物（金属片、鉛筆の芯など）を接触させたり、ほこりが内部に入ったりしないようにする
  火災、やけど、けが、感電または故障の原因となります。
- 禁止　使用中に布団で覆ったり、包んだりしない
  火災、やけどまたは故障の原因となります。
- ❗ ガソリンスタンドなど引火性ガスが発生する可能性のある場所や粉じんが発生する場所に立ち入る場合は、必ず事前に本製品の電源を切る
  引火性ガスなどが発生する場所で使用すると、爆発や火災の原因となります。
- 禁止　カメラのレンズに直射日光などを長時間あてない
  素子の退色、焼付きや、レンズの集光作用により、火災、やけど、けがまたは故障の原因となります。
- ❗ 無線製品は病院内で使用する場合は、各医療機関の指示に従って使用する
  電子機器や医療電気機器に悪影響を及ぼすおそれがあります。
- 禁止　本製品の周辺に放熱を妨げるようなもの（フィルムやシールでの装飾を含む）を置かない
  火災、または故障の原因となります。
- ❗ 耳を本体から離してご使用ください
  大きな音を長時間連続して聞くと、難聴などの耳の障害の原因となります。
- ❗ 無線製品をご使用の場合、医用電気機器などを装着している場合は、医用電気機器メーカーもしくは、販売業者に、電波による影響について確認の上使用する
  医療電気機器に悪影響を及ぼすおそれがあります。
- ❗ 高精度な制御や微弱な信号を取り扱う電子機器の近くでは使用しない
  電子機器が誤作動するなど、悪影響を及ぼすおそれがあります。
- ❗ ディスプレイ部やカメラのレンズを破損した際は、割れたガラスや露出した端末内部に注意する
  破損部や露出部に触れると、やけど、けが、感電の原因となります。
- ❗ ペットなどが本機に噛みつかないように注意する
  火災、やけど、けがなどの原因となります。
- 禁止　コンセントに AC アダプタや電源ケーブルを抜き差しするときは、金属類を接触させない
  火災、やけど、感電または故障の原因となります。
- 禁止　AC アダプタや電源ケーブルに海外旅行用の変圧器等を使用しない
  発火、発熱、感電または故障の原因となります。

警告

ACアダプタもしくは電源プラグについたほこりは、拭き取る
ほこりが付着した状態で使用すると、火災、やけど、感電または故障の原因となります。

ACアダプタや電源ケーブルをコンセントにさしこむときは、確実に差し込む
確実に差し込まないと、火災、やけど、感電もしくは故障の原因となります。

接続端子が曲がるなど変形した場合は、直ちに使用を中止する。また、変形をもとに戻しての使用も行わない
端子のショートにより、火災、やけど、けが、感電または故障の原因となります。

各種接続端子を機器本体に接続する場合、斜めに差したり、差した状態で引っ張ったりしない
火災、やけど、感電または故障の原因となります。

使用しない場合は、ACアダプタもしくは電源ケーブルをコンセントから抜く
電源プラグを差したまま放置すると、火災、やけど、感電または故障の原因となります。

お手入れの際は、ACアダプタもしくは電源ケーブルをコンセントから抜く
抜かずに行うと、火災、やけど、感電または故障の原因となります。

禁止 **SDやMicroSDカード、USBメモリの使用中は、カードやメモリを取り外したり、本製品の電源を切ったりしない**
データの消失、機器本体の故障の原因となります。

禁止 **磁気カードや磁気を帯びたものを本製品に近づけない**
磁気カードのデータが消えてしまうおそれもしくは機器本体の誤作動の原因となります。

ディーリンクジャパンが販売している無線機器は国内専用のため、海外で使用しない
海外では国によって電波使用制限があるため、本製品を使用した場合、罰せられる場合があります。
海外から持ち込んだディーリンク製品や並行輸入品を日本国内で使用する場合も同様に、罰せられる場合があります。

注意

禁止 **乳幼児の手の届く場所では使わない**
やけど、ケガまたは感電の原因となります。

静電気注意
コネクタや電源プラグの金属端子に触れたり、帯電したものを近づけますと故障の原因となります。

禁止 **コードを持って抜かない**
コードを無理に曲げたり、引っ張ると、コードや機器本体の破損の原因となります。

禁止 **振動が発生する場所では使用しない**
故障の原因となります。

付属品の使用は取扱説明書に従う
本製品の付属品は、取扱説明書に従い、他の製品に使用しないでください。機器の破損の原因となります。

禁止 **破損したまま使用しない**
火災、やけどまたはけがの原因となります。

禁止 **ぐらついた台の上や傾いた場所などの不安定な場所や高所には置かない**
落下して、けがなどの原因となります。

禁止 **子供が使用する場合は、保護者が取扱いの方法を教え、誤った使い方をさせない**
けがや故障などの原因となります。

本製品を長時間連続使用する場合は、温度が高くなることがあるため、注意する。また、使用中に眠ってしまうなどして、意図せず長時間触れることがないようにする
温度の高い部分に直接長時間触れるとお客様の体質や体調によっては肌の赤みやかゆみ、かぶれ、低温やけどの原因となります。

禁止 **コンセントにつないだ状態で、ACアダプタや電源コンセントに長時間触れない**
やけど、感電の原因となります。

一般の電話機やコードレス電話、テレビ、ラジオなどをお使いになっている近くで使用しない
近くで使用すると、本製品が悪影響を及ぼす原因となる場合があるため、なるべく離れた場所で使用してください。

禁止 **D-Linkが指定したオプション品がある場合は、指定オプションを使用する**
不正なオプション品を使用した場合、故障、破損の原因となります。

電波障害自主規制について

本製品は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。
この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

ご使用上の注意

けがや感電、火災および装置の破損のリスクを減らすために、以下の注意事項を遵守してください。

- マニュアルなどに記載されている以外の方法でのご使用はやめてください。
- 食べ物や飲み物が本製品にかからないようにしてください。また、水気のある場所での運用は避けてください。
- 本製品の開口部に物をさしこまないでください。火事や感電を引き起こすことがあります。
- 付属の AC アダプタもしくは電源ケーブルのみを使用してください。
- 感電を防止するために、本製品と周辺機器の電源ケーブルは、正しく接地された電気コンセントに接続してください。
- やむなく延長コードや電源分岐回路を使用する場合においても、延長コードと電源分岐回路の定格を守ってください。延長コードまたは電源分岐回路に差し込まれているすべての製品の合計定格アンペア数が、その延長コードまたは、電源分岐回路の定格アンペア限界の 8 割を超えないことを確認してください。
- 一時的に急激に起こる電力の変動から本製品を保護するためには、サージサプレッサ、回線調整装置、または無停電電源装置（UPS）を使用してください。
- ケーブルと電源コードは慎重に取り付けてください。踏みつけられたり躓いたりしない位置に、ケーブルと電源コードを配線し、コンセントに差し込んでください。また、ケーブル上に物を置いたりしないようにしてください。
- 電源ケーブルや電源プラグを改造しないでください。システムに対応しているホットプラグ可能な電源装置に電源を接続したり、切り離したりする際には、以下の注意を守ってください。
  - 電源装置を取り付ける場合は、電源装置を取り付けてから、電源ケーブルを電源装置に接続してください。
  - 電源装置を取り外す場合は、事前に電源ケーブルを抜いておいてください。
  - システムに複数の電源がある場合、システムから電源を切り離すには、すべての電源ケーブルを電源装置から抜いておいてください。
- 抜け防止機構のあるコンセントをご使用の場合、そのコンセントの取り扱い説明書に従ってください。
- 本製品は動作中に高温になる場合があります。本製品の移動や取り外しの際には、ご注意ください。
- 本製品は動作中に高温になる場合がありますが、手で触れることができる温度であれば故障ではありません。ただし長時間触れたまま使用しないでください。低温やけどの原因になります。
- 市販のオプション品や他社製品を使用する場合、当社では動作保証は致しませんので、予めご了承ください。
- 製品に貼られている製品ラベルや認証ラベルをはがさないでください。はがしてしまうとサポートを受けられなくなります。

静電気障害を防止するために

静電気は、本製品内部の精密なコンポーネントを損傷する恐れがあります。静電気による損傷を防ぐため、本製品に触れる前に、身体から静電気を逃がしてください。
さらに、静電気放出（ESD）による損傷を防ぐため、以下の手順を実行することをお勧めします。

1. 機器を箱から取り出すときは、機器をシステム等に取り付ける準備が完了するまで、本製品を静電気防止包装から取り出さないでください。静電気防止包装から取り出す直前に、必ず身体の静電気を逃がしてください。

2. 静電気に敏感な部品を運ぶ場合、最初に必ず静電気対策を行ってください。

3. 静電気に敏感な機器の取り扱いは、静電気のない場所で行います。可能であれば、静電気防止床パッド、作業台パッド、および帯電防止接地ストラップを使用してください。

電源の異常

万一停電などの電源異常が発生した場合は、必ず本スイッチの電源プラグを抜いてください。電源が再度供給できる状態になってから電源プラグを再度接続します。

このたびは、弊社製品をお買い上げいただきありがとうございます。
本書は、製品を正しくお使いいただくための取扱説明書です。
必要な場合には、いつでもご覧いただけますよう大切に保管してください。
また、必ず本書、設置マニュアル、および弊社 WEB に掲載された製品保証規程をよくお読みいただき、内容をご理解いただいた上で、記載事項に従ってご使用ください。

製品保証規定は以下を参照ください。
https://www.dlink-jp.com/support/product-assurance-provision

- 本書の記載内容に逸脱した使用の結果発生した、いかなる障害や損害において、弊社は一切の責任を負いません。あらかじめご了承ください。
- 弊社製品の日本国外でご使用の際のトラブルはサポート対象外になります。

なお、本製品の最新情報やファームウェアなどを弊社ホームページにてご提供させていただく場合がありますので、ご使用の前にご確認ください。
製品保証、保守サービス、テクニカルサポートご利用について、詳しくは弊社ホームページのサポート情報をご確認ください。
https://www.dlink-jp.com/support

目次

安全にお使いいただくために........2
ご使用上の注意........4
静電気障害を防止するために........4
電源の異常........4

はじめに 11

本マニュアルの対象者........12
表記規則について........12

第 1 章　本製品のご利用にあたって 13

はじめに........13
特長と利点........14
ポートについて........14
前面パネル........15
　LED 表示........15
背面パネル........16

第 2 章　製品の設置 17

パッケージの内容........17
ネットワーク接続前の準備........17
　設置位置の選択........17
　設置時の注意........17
19 インチラックへの取り付け........18
　ブラケットの取り付け........18
　19 インチラックに本製品を取り付ける........18
無線コントローラの接続........19
電源の投入........19

第 3 章　Web ベース設定ユーティリティ 20

Web 管理インタフェースへのログイン........20
　システム要件........20
　ログイン前の準備........20
　ログイン方法........20
Web 管理インタフェースの画面構成........23
Web 管理インタフェースの機能について........24
ナビゲータ機能........25
　無線プロファイルの設定........25
　管理アクセスポイント設定........28
　外部認証設定........31
　システム設定........34
　WiFi チケットプラン設定........37
　キャプティブポータル設定........39

第 4 章　基本設定 42

基本設定の手順........42
　手順 1: DHCP サーバの有効化（オプション）........42
　手順 2: 国コードの設定........43
　手順 3: 管理するアクセスポイントの選択........44
　手順 4: SSID の変更とセキュリティの設定........45
　手順 5: MAC 認証モードの選択........52
　手順 6: 関連付けした AP プロファイルの確認........54
　手順 7: キャプティブポータルの設定........55
　手順 8: RADIUS サーバを持つ SSID をオーセンティケータとして使用する........61
　手順 9: ゲスト管理の設定........62
　手順 10: BYOD 環境の設定........69

第 5 章　高度な無線 LAN 設定 76

WLAN の一般的な設定........77
　WLAN の基本設定........77
チャンネル計画と送信出力........79
　チャンネル計画の設定........79
　送信出力設定........81
WIDS 設定........82
　AP WIDS の設定........82
　クライアントの WIDS 設定........84

Distributed トンネル....86
Distributed トンネルの設定....86
WLAN Visualization 87
画像のアップロード 87
起動 88
AP ディスカバリ方式 91
L2/ VLAN ディスカバリ 91
L3/IP ディスカバリ 93
管理対象のアクセスポイント....94
Valid AP の追加....94
Not Managed AP List からアクセスポイントを追加する 96
管理対象アクセスポイントのチャンネルと送信出力の手動変更 97
AP デバッグモードの設定 98
AP プロビジョニングの設定 99
AP グループの設定 101
AP プロファイル....102
AP プロファイルの設定....102
AP プロファイルの無線電波の設定 104
AP プロファイル SSID の設定 108
AP プロファイル QoS の設定 111
WDS 設定 114
WDS Managed AP の設定 115
WDS Managed AP の設定 116
WDS AP リンクの設定....117
無線スケジュール機能....118
スケジュールプロファイル 118
スケジュールルール 119
ピアグループ 120
ピアグループの設定 120
ピアグループの同期 121
コントローラ証明書リクエスト（X.509）....121
コントローラプロビジョニング....122
アクセスコントロースリスト（ACL）....123
IP アクセスコントロールリスト（IP ACL）....123
IP ACL ルール設定....124
MAC アクセスコントロールリスト（MAC ACL）....126
MAC ACL ルール設定 127
DiffServ 設定....129
DiffServ クラス 129
DiffServ ポリシー 131
DiffServ ポリシークラス設定....132
AP ファームウェアのアップグレード....134
AP ファームウェアのダウンロード 134
AP ファームウェアの状態 135

第 6 章　高度なネットワーク設定 137

IP モード設定....137
LAN 設定 138
IPv4 LAN 設定 138
IPv6 LAN 設定 141
IPv6 アドレスプール 142
IPv6 ルータ通知....144
IPv6 通知のプレフィックス 145
LAN DHCP の予約 IP....146
IGMP 設定 147
ジャンボフレームの設定....148
リンクアグリゲーション 149
VLAN 設定....150
VLAN の作成 150
マルチ VLAN サブネット 152
DHCP プール設定....153
ポート VLAN 154
MAC ベース VLAN 155
音声 VLAN....156
プロトコルベース VLAN....157
ダブル VLAN 158
GVRP 159

ルーティング設定 ... 160
IPv4 スタティックルーティングの設定 ... 160
IPv6 スタティックルーティングの設定 ... 161
QoS 設定 ... 163
QoS 優先度 ... 163
QoS モードの有効化 ... 163
各ポートの DSCP と CoS の定義 ... 165
802.1p 優先度の設定 ... 166
DSCP 優先度の設定 ... 167
ポートシェーピングレート ... 168
QoS ポリシー設定 ... 169
ポリシーベース QoS の設定 ... 169
フローベースコントロールの設定 ... 170
自動 VoIP QoS の設定 ... 171
キュースケジューラの設定 ... 172
キュー管理 ... 172
CoS と DSCP マーキングの設定 ... 173
第 7 章　ネットワークのセキュリティ設定 174
クライアントの管理 ... 175
既知の無線クライアントの参照 / 追加 ... 175
グループの管理 ... 177
ユーザグループ ... 177
ログインポリシー ... 179
ブラウザポリシー ... 180
IP ポリシー ... 181
ユーザ管理 ... 182
手動によるユーザの追加 ... 182
ユーザのインポート ... 183
ユーザの編集 ... 183
ユーザの削除 ... 184
パスワードのルール ... 184
ゲストアカウントの使用の管理 ... 185
ビリングプロファイル ... 186
ペイメントゲートウェイ ... 188
ログインプロファイル ... 189
キャプティブポータルのログインページのカスタマイズ ... 189
キャプティブポータルの SLA のカスタマイズ ... 192
カスタムキャプティブポータルプロファイルのアップロード ... 193
外部認証 ... 194
RADIUS サーバの設定 ... 194
RADIUS プロファイルの設定 ... 195
RADIUS アカウンティングサーバの設定 ... 196
POP3 サーバの設定 ... 197
POP3 のトラスト CA の設定 ... 198
LDAP サーバの設定 ... 199
RADIUS アカウンティンググローバル設定 ... 200
Facebook Wi-Fi 設定 ... 201
E-mail 設定 ... 202
証明書設定 ... 203
信頼済み証明書 ... 203
アクティブな自己署名証明書 ... 204
自己署名証明書のリクエスト ... 205
MAC バイパス設定 ... 206
OAuth サーバ設定 ... 207
クライアントのブロック ... 208
第 8 章　ステータスおよび統計情報 209
統計情報と利用率の参照 ... 209
ダッシュボードの管理 ... 210
システム状態の参照 ... 212
デバイス状態の参照 ... 212
USB 情報の参照 ... 213
ネットワーク情報の参照 ... 214
DHCP クライアントの参照 ... 214
キャプティブポータルセッションの参照 ... 215
インタフェースのトラフィックの参照 ... 216

リンクアグリゲーションの参照 217
コントローラの参照 218
コントローラの状態と統計情報の参照 218
関連クライアント 219
分散型トンネル 219
ピアコントローラの受信状態 220
ピアコントローラの送信状態 221
RADIUS アカウンティング統計 222
アクセスポイント情報の参照 223
Global Status 223
RF スキャンで検出されたアクセスポイント 224
De-Authentication Attacks 227
Hardware Capability 228
管理アクセスポイント 229
Connection Failed（接続失敗アクセスポイント） 241
Authentication Failed（認証エラー） 241
Peer Managed 244
接続クライアントのグローバル状態 244
接続するクライアント 245
アドホッククライアント 249
検出クライアント 250
クラスタ情報の参照 256
WDS グループ状態の参照 257
WDS グループのアクセスポイントの状態 258
WDS アクセスポイント状態の参照 259
WDS リンク状態の参照 260
WDS リンクの統計情報の参照 261
IP ACL 情報の参照 261
IP ACL ルール情報の参照 262
MAC ACL 情報の参照 262
MAC ACL ルール情報の参照 263
DiffServ クラス情報の参照 263
DiffServ ポリシー情報の参照 264
DiffServ ポリシー属性情報の参照 264

第 9 章　メンテナンス 265

システム設定 265
システム名の設定 265
システムの日付と時間の設定 266
ログインセッションタイムアウトの設定 267
USB 共有ポートの設定 267
パッケージマネージャ 268
言語設定 269
WEB GUI 管理の設定 270
ライセンスのアクティブ化 271
UI 管理 272
SNMP の使用 273
SNMP v3 ユーザリストの設定 273
SNMP トラップリストの設定 274
SNMP アクセスコントロールリストの設定 275
SNMP システム情報の設定 276
無線 SNMP 情報の設定 277
DDP クライアントの設定 278
コンフィグレーションの保存と復元 279
コンフィグレーションのバックアップ 279
コンフィグレーションの復元 280
工場出荷時設定の復元 281
無線コントローラの再起動 282
ファームウェアのアップグレード 283
無線コントローラのファームウェアのアップグレード 283
コマンドラインインタフェースの使用 285

第 10 章　トラブルシューティング 286

LED トラブルシューティング 286
Power LED が消灯 286
LAN ポート LED が消灯 286
Web GUI トラブルシューティング 286
リセットボタンを使用して工場出荷時設定に復元する 287
日付と時間に関する問題 287
アクセスポイントに関するディスカバリ問題 287
接続問題 287
ネットワークの性能と不正アクセスポイントの検出 288
無線コントローラにおける診断ツールの使用 288
IP アドレスの Ping 288
Traceroute の使用 289
DNS 検索の実行 290
ログパケットのキャプチャ 291
システムチェックの実施 293
ログ設定 294
ログ出力の定義 294
トラフィックの追跡 / ルーティングログ 295
リモートログ 296
Syslog サーバ構成 297
イベントログ 298
現在のログ 299
WLAN ログ 299
LAN ログ 300
Trap ログ 300

付録 301

付録 A 基本計画のワークシート 301
付録 B 工場出荷時設定 303
付録 C 用語解説 304

はじめに

本ユーザマニュアルでは、本製品の設置方法および操作方法を説明します。

- 第 1 章　本製品のご利用にあたって
  - 本製品の概要とその機能について説明します。また、前面、背面の各パネルと LED 表示について説明します。
- 第 2 章　製品の設置
  - 本製品の基本的な設置方法と接続方法について説明します。
- 第 3 章　Web ベース設定ユーティリティ
  - Web ベースの管理機能への接続方法および設定方法について説明します。
- 第 4 章　基本設定
  - 本製品の基本的な設定方法について説明します。
- 第 5 章　高度な無線 LAN 設定
  - 詳細な無線設定、Distributed トンネル、ピアコントローラ、WIDS などの設定について説明します。
- 第 6 章　高度なネットワーク設定
  - インタフェース、VLAN、ルーティング、QoS 設定について説明します。
- 第 7 章　ネットワークのセキュリティ設定
  - 本製品が使用するルールを作成および適用することによってネットワークを安全にする方法について説明します。
- 第 8 章　ステータスおよび統計情報
  - 本製品のシステム構成の詳細、トラフィック統計情報、アクティブなセッション情報について説明します。
- 第 9 章　メンテナンス
  - リモート管理、SNMP、コンフィグレーションのバックアップと復元、ファームウェアのアップグレードなど管理用の機能について説明します。
- 第 10 章　トラブルシューティング
  - 無線コントローラの使用時に発生する問題を解決する手順について説明します。
- 付録 A 基本計画のワークシート
  - 計画の取り組みを促進させる基本計画のワークシートの記載方法について説明します。
- 付録 B 工場出荷時設定
  - 本製品の工場出荷時設定を記載しています。
- 付録 C 用語解説
  - 本説明書の中で使用する用語について説明します。

本マニュアルの対象者

本マニュアルは、本製品の設置および管理についての情報を記載しています。また、ネットワーク管理の概念や用語に十分な知識を持っているネットワーク管理者を対象としています。

表記規則について

本項では、本マニュアル中での表記方法について説明します。

注意 注意では、特長や技術についての詳細情報を記述します。

警告 警告では、設定の組み合わせ、イベントや手順によりネットワークの接続状態やセキュリティなどに悪影響を及ぼす恐れのある事項について説明します。

表 1 に、本マニュアル中での字体、・記号についての表記規則を表します。

表 1　字体・記号の表記規則

<table>
<tr><th>字体・記号</th><th>解説</th><th>例</th></tr>
<tr><td>「」</td><td>メニュータイトル、ページ名、ボタン名。</td><td>「Submit」ボタンをクリックして設定を確定してください。</td></tr>
<tr><td>青字</td><td>参照先。</td><td>「ご使用になる前に」をご参照ください。</td></tr>
<tr><td><code>courier</code> フォント</td><td>CLI 出力文字、ファイル名。</td><td><code>(switch-prompt)#</code></td></tr>
<tr><td><code>courier</code> 太字</td><td>コマンド、ユーザによるコマンドライン入力。</td><td><code>show network</code></td></tr>
<tr><td><code>courier</code> 斜体</td><td>コマンド項目（可変または固定）。</td><td><code>value</code></td></tr>
<tr><td>< ></td><td>可変項目。< > にあたる箇所に値または文字を入力します。</td><td><<i>value</i>></td></tr>
<tr><td>[ ]</td><td>任意の固定項目。</td><td>[value]</td></tr>
<tr><td>[< >]</td><td>任意の可変項目。</td><td>[<<i>value</i>>]</td></tr>
<tr><td>{ }</td><td>{ } 内の選択肢から 1 つ選択して入力する項目。</td><td>{choice1 | choice2}</td></tr>
<tr><td>|（垂直線）</td><td>相互排他的な項目。</td><td>choice1 | choice2</td></tr>
<tr><td>Menu Name >
Menu Option</td><td>メニュー構造を示します。</td><td>Device > Port > Port Properties は、「Device」メニューの下の「Port」メニューの「Port Properties」メニューオプションを表しています。</td></tr>
</table>

第 1 章　本製品のご利用にあたって

- はじめに
- 特長と利点
- ポートについて
- 前面パネル
- 背面パネル

本製品の概要とその機能について説明します。また、前面、背面の各パネルと LED 表示について説明します。

はじめに

DWC-2000 は、中規模エンタープライズ環境向けの無線コントローラです。
デフォルトでは 64 台、AP 管理ライセンスの追加により最大 256 台のアクセスポイントの集中管理を行うことができます。

無線コントローラとそれに関連付けるアクセスポイントを使用して、以下の項目を実施できます。

- WLAN 上の D-Link アクセスポイントの発見と設定
- 一元的な RF 管理、セキュリティ、QoS、および他の設定機能を使用した無線アクセスポイントの性能の最適化
- セキュリティ設定のタスクを効率化して、ゲストアクセスを設定
- ネットワーク状態と統計情報のモニタリング
- 無線管理システムと無線ネットワークにある D-Link アクセスポイントに対する保守タスクとファームウェアのアップデートを実行
- トラブルシューティング手順の案内

本製品は、プロファイルを使用してアクセスポイントの設定を行います。
プロファイルによって、管理するアクセスポイントに無線モードや SSID などの設定を適用します。
本製品には設定済みのプロファイルが存在します。必要に応じて、プロファイルの編集や新規作成を行うことができます。

例：

- オフィスビルのエリアごとに配置したアクセスポイントに、異なるプロファイルを適用する。
- ビルや部署ごとに異なるセキュリティポリシー（ゲスト用、管理用など）を設定する。

特長と利点

DWC-2000 無線コントローラは、中規模エンタープライズ環境向けのワイヤレスコントローラです。別途ランセンスを購入することにより、無線コントローラは最大 256 台のアクセスポイントをサポートすることができます。無線コントローラにより、中央部から無線ネットワークの管理、セキュリティと QoS 機能の一元的な実行、ゲストアクセス用のキャプティブポータルの設定などが可能です。

スタックと冗長度を持つスケーラブルなアーキテクチャ

- 追加ライセンスなしで、1 つの無線コントローラは最大 64 台のアクセスポイントをサポートします。
- 単一の無線コントローラには 32/64/128 台単位で、256 台までのアクセスポイントに増加できる購入ライセンスパック（DWC-2000-AP32 / DWC-2000-AP64 / DWC-2000-AP128）が用意されています。
- クラスタグループのネットワークには最大 1,024 台のアクセスポイントをサポートします。
- IEEE 802.11a、802.11b、802.11g、802.11n、802.11ac、802.11ax プロトコルをサポートします。

集中型管理と設定

- L2 と L3 ドメインにおけるアクセスポイントの自動ディスカバリ
- 無線ネットワーク全体を 1 カ所で管理
- 簡易化されたプロファイルベースの設定
- ダイナミックに IP アドレスを配布する DHCP サーバ
- 管理 VLAN の設定
- アクセスポイントと関連するクライアントステーションのリアルタイムモニタ
- ネットワーク性能を管理、制御、最適化する、管理対象アクセスポイントにおけるシステムアラームと統計情報レポート

セキュリティ

- 外部 RADIUS サーバまたは内部認証サーバによる ID ベースのセキュリティ認証
- 不正なアクセスポイントの検出、分類、軽減
- キャプティブポータル認証
- ゲスト管理とチケット生成

サイトサーベイが完了した後に、収集したデータを使用して、「付録 A　基本計画のワークシート」をセットアップします。「基本計画のワークシート」の入力が完了した後に、無線コントローラの設置場所を決定します。

ポートについて

本製品は以下のポートを搭載しています。

ポート	DWC-2000
10BASE-T/100BASE-TX/1000BASE-T ポート	4
SFP ポート	4
RJ-45 コンソールポート	1
USB ポート	2
HDD モジュールスロット	1

前面パネル

前面パネルの各部名称と機能について説明します。LED の表示内容については「LED 表示」を参照してください。

図 1-1　　前面パネル図

各部名称	説明
Power LED	本無線コントローラの電源の状態を示します。
Fan LED	無線コントローラのファンの状態を示します。
USB ポート / LED	USB 1.1 または 2.0 のデバイスを接続できます。
LAN ポート	コンピュータ、スイッチおよびハブなどのイーサネットデバイスと UTP ケーブルで接続します。
SFP ポート	コンピュータ、スイッチおよびハブなどのイーサネットデバイスと光モジュールを経由して接続します。
コンソールポート	RJ45-to-DB9 コンソールケーブルを通じて CLI（コマンドラインインタフェース）にアクセスするために使用します。
HDD モジュールスロット	ハードディスクドライブモジュール用のスロットです。HDD は付属していません。
リセットボタン	本製品を工場出荷時設定にリセットします。

LED 表示

LED の表示によって、電源やポートの状態を判断できます。

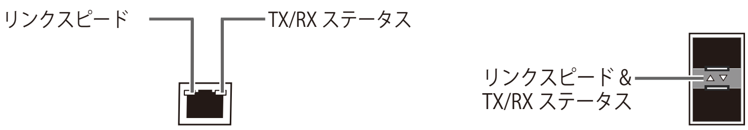


図 1-2　　LAN/SFP LED 図

ステータス LED は以下の状態を表示します。

LED	状態	色	状態説明
Power / ステータス	点灯	橙	起動中です。
	点滅	橙	クラッシュしました。リカバリモードになっています。
	点灯	緑	製品に電源が供給され正常に動作しています。
	点滅	緑	ファームウェアのアップグレードに失敗しました。
	消灯	ー	製品に電源が供給されていません。
Fan	点灯	緑	ファンは正常に動作しています。
	点灯	赤	ファンが故障しています。
LAN リンクスピード	点灯	橙	1000Mbps でリンクが確立しています。
	点灯	緑	100Mbps でリンクが確立しています。
	消灯	ー	10Mbps でリンクが確立しています。
LAN TX/RX ステータス	点灯	緑	リンクが確立しています。
	点滅		データを送受信しています。
	消灯	ー	リンクが確立していません。
SFP リンクスピード & TX/RX	点灯	緑	100Mbps でリンクが確立しています。
	点滅		100Mbps でデータを送受信しています。
	点灯	橙	1000Mbps でリンクが確立しています。
	点滅		1000Mbps でデータを送受信しています。
USB	点灯	緑	USB デバイスが接続されています。
	点滅		データを送受信しています。
	消灯		USB デバイスが接続されています。

背面パネル

背面パネルの各部名称と機能について説明します。

図 1-3　背面パネル図

各部名称	機能
電源コネクタ	付属の AC ケーブルを接続します。
電源スイッチ	本製品の電源スイッチです。
電源抜け防止クリップ挿入口	電源抜け防止クリップを挿入します。

第 2 章　製品の設置

- パッケージの内容
- ネットワーク接続前の準備
- 19 インチラックへの取り付け
- 無線コントローラの接続
- 電源の投入

パッケージの内容

ご購入いただいた製品の梱包箱を開け、同梱物を注意して取り出してください。以下のものが同梱されています。

- 本体
- AC 電源ケーブル
- マニュアル
- シリアルラベル
- CD-ROM
- RJ-45/DB9 変換ケーブル
- ネットワークケーブル
- ラックマウントキット
- 電源抜け防止クリップ
- ゴム足

万一、不足しているものや損傷を受けているものがありましたら、ご購入頂いた販売代理店までご連絡ください。

ネットワーク接続前の準備

設置位置の選択

製品の設置場所が性能に大きな影響を与えます。本製品を有効に使用するために、適切な設置場所を選択してください。
以下の通りサイトサーベイを行うことをお勧めします。

- 提供すべき Wi-Fi カバレッジを確認します。
- アクセスポイントの設置位置を決定し、追加アクセスポイントを必要とする弱信号やデッドスポットを持つエリアを確認します。
- 高密度のアクセスポイントカバレッジが必要とされる高負荷で利用するエリアを決定します。
- RF 信号の屋内伝搬を決定します。
- 潜在的な RF 障害と干渉の原因を確認します。
- サイトのチャンネルのスペクトル分析を実行して、現在の RF の挙動を確認します。そして、802.11 および non-802.11 ノイズの両方を検出します。
- クライアントの最大スループットを確認するために、アクセスポイントとクライアントの接続テストを行ってください。

サイトサーベイが完了した後に、収集したデータを使用して、「付録 A 基本計画のワークシート」をセットアップします。「基本計画のワークシート」の入力を完了した後に、無線コントローラの位置を選択します。以下のガイドラインに従って設置場所を決定します。

- ほこり、水、湿気がなく、直射日光にさらされることなく、振動のない平坦かつ清潔である。
- 適度に涼しく、湿気がなく、40℃を超えない。
- 温度と湿度の変化がなく、強力な磁場や電気ノイズを生成するデバイスの近くでない。
- 無線コントローラを発熱するデバイスの隣、上、下に置かない。無線コントローラの通気口をふさがない。
  コントローラの両サイドと背面に空間を 10cm 以上保つようにする。
- 無線コントローラとすべてのケーブルが接続できる。
- 電源を偶然にオフできないような電源コンセントがある。

設置時の注意

設置時には更に以下の項目に注意します。

- 製品は、しっかりとした水平面で耐荷重性のある場所に設置してください。
- 製品の上に重いものを置かないでください。
- 本製品から 1.82m 以内の電源コンセントを使用してください。
- 電源ケーブルが AC/DC 電源ポートにしっかり差し込まれているか確認してください。
- 製品を水平面に設置する際は、スイッチ底面に同梱のゴム足を取り付けてください。ゴム製の足はスイッチのクッションの役割を果たし、筐体自体や他の機器に傷がつくのを防止します。

19 インチラックへの取り付け

以下の手順に従って本製品を標準の 19 インチラックに設置します。

ブラケットの取り付け

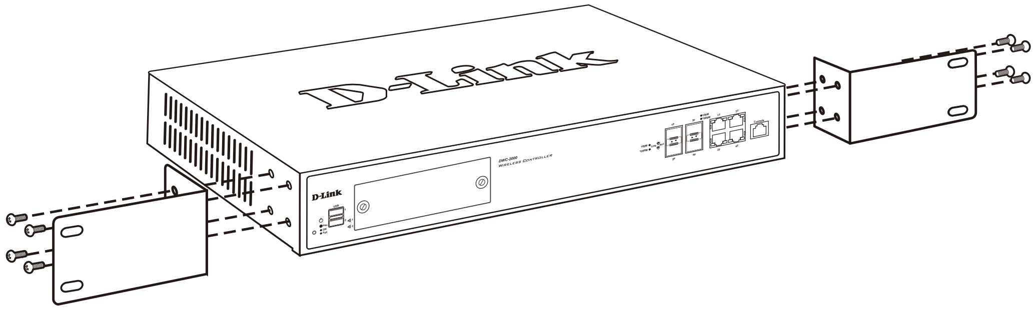


図 2-1　ブラケットの取り付け

ラックマウントキットに付属のネジを使用して、本製品にブラケットを取り付けます。完全にブラケットが固定されていることを確認し、本製品を以下の通り標準の 19 インチラックに固定します。

19 インチラックに本製品を取り付ける

警告　前面、側面にスタビライザを取り付けないで製品を設置すると、ラックが転倒し、場合によっては人身事故を引き起こすことがあります。そのため、ラック内に製品を取り付ける前に必ずスタビライザを取り付けてください。ラックにシステム / コンポーネントを取り付けた後は、一度にスライド・アセンブリに乗せて引き出すコンポーネントは 1 つだけとしてください。2 つ以上のコンポーネントが引き出されると、ラックがバランスを失い、倒れて重大な事故につながる恐れがあります。

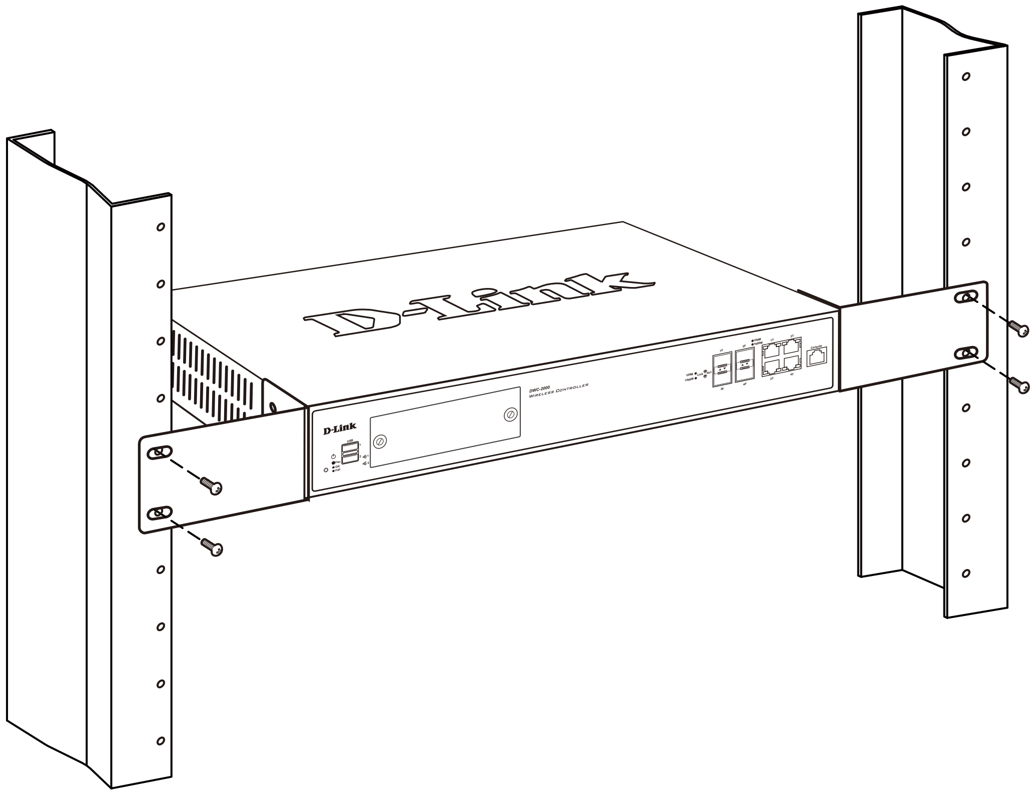


図 2-2　製品のラックへの設置

無線コントローラの接続

1. スイッチとアクセスポイントを設置します。

2. 無線コントローラの前面の LAN（1-4）ポートの 1 つにイーサネット LAN ケーブルの一端を接続します。LAN ネットワークセグメント上のスイッチにおいて利用可能な RJ-45 ポートにケーブルのもう一端を接続します。

3. 無線コントローラの LAN（1-4）ポートの 1 つをネットワーク、または、直接 PC に接続します。

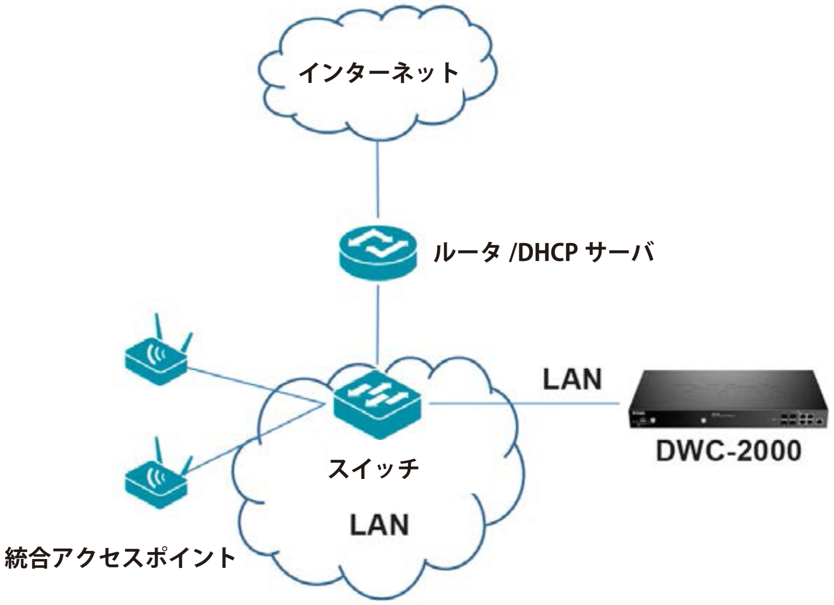


図 2-3　　製品接続図

電源の投入

1. 電源ケーブルを本製品の電源コネクタに接続します。電源ケーブルのプラグを電源コンセントに接続します。製品の起動中、Power LED は橙色に点灯します。
2. 起動すると、Power LED が緑色に点灯します。

第 3 章　Web ベース設定ユーティリティ

- Web 管理インタフェースへのログイン
- Web 管理インタフェースの画面構成
- Web 管理インタフェースの機能について
- ナビゲータ機能

Web 管理インタフェースへのログイン

本スイッチのすべてのソフトウェア機能は、実装されている Web ベース（HTML）インタフェース経由で管理、設定およびモニタできます。標準的なブラウザを使用してネットワーク上のリモートステーションから本スイッチを管理できます。ブラウザが普遍的なアクセスツールの役割をし、HTTP プロトコルを使用してスイッチと直接通信することが可能です。

システム要件

本製品が動作するためには、以下のシステム条件が必要です。

- ブラウザの起動
- イーサネットへの接続

ブラウザバージョン

- Microsoft Internet Explorer 11 以降
- Mozilla Firefox 23 以降
- Apple Safari 5.1.7 以降（Windows）
- Apple Safari 6.1.3 以降（iOS）
- Google Chrome 26 以降

ログイン前の準備

ログイン前に、以下の項目を確認します。

- サブネットマスク「255.255.255.0」を持つ「192.168.10.x」ネットワークの IP アドレスを使用するように、Web ブラウザが動作している PC を設定します。
- クッキーの受け付け、ポップアップの表示、および、JavaScript の動作を許可するように Web ブラウザを設定します。
- ご使用の無線コントローラのファームウェアをアップグレードします。（「AP ファームウェアのアップグレード」参照）
- 無線コントローラのファームウェアをアップグレードさせた後に、アクセスポイントのファームウェアをアップグレードさせます。（ご使用のアクセスポイントのドキュメント参照）

ログイン方法

本製品の設定は LAN ケーブルで接続した PC から行います。

1. 本製品の LAN ポートの 1 つと PC を接続します。

2. 「192.168.10.0/24」サブネットにあるスタティック IP アドレスを使用して PC が設定されていることをご確認ください。

注意 ブラウザの「ポップアップブロック」機能を無効にするか、または「ポップアップブロック」の許可リストに「http://192.168.10.1」を追加してください。

3. Web ブラウザを起動します。

4. 本製品の IP アドレスと HTTP ポートの番号をアドレスに入力し（http://192.168.10.1）、「Enter」キーを押下します。設定用 PC と本製品の IP アドレスが同じサブネット内であることに注意してください。

図 3-1　　アドレス入力画面

注意 ログインプロンプトが表示されない場合は、「Web GUI トラブルシューティング」を参照してください。

注意 本製品の IP アドレスを初期値から変更している場合は、変更後のアドレスを入力します。

5. 接続に成功すると、以下のログイン画面が表示されます。

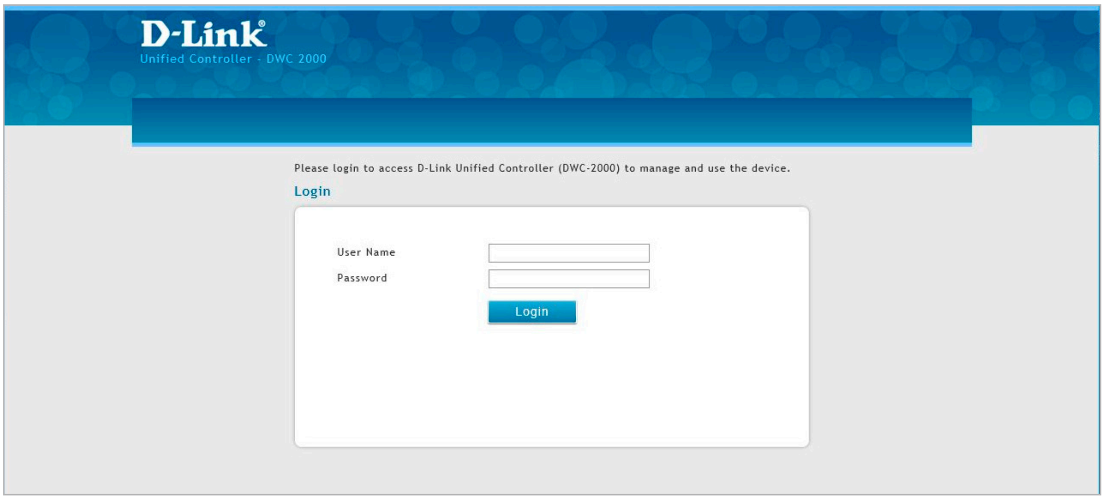


図 3-2　　Login 画面

6. 「Username」（ユーザ名）と「Password」（パスワード）を入力し、「Login」ボタンをクリックします。

注意　コントローラの IP アドレス、サブネットマスク、ユーザ名、パスワードの初期値は以下の通りです。

- IP アドレス : 192.168.10.1
- サブネットマスク : 255.255.255.0
- Username: admin
- Password: admin

7. 初回ログイン時には以下の画面が表示されます。

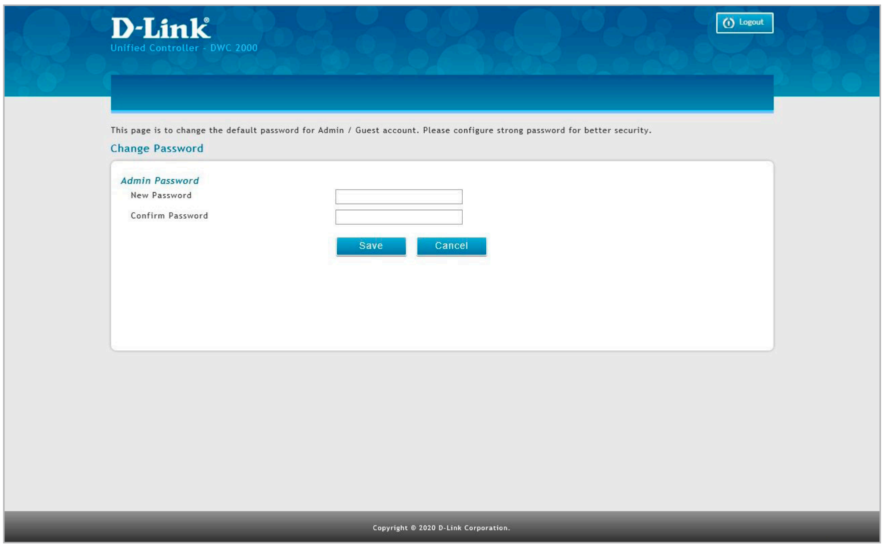


図 3-3　　パスワード変更画面

8. 新しいパスワードを入力し、「Save」をクリックします。

注意　ユーザ名とパスワードの両方とも大文字と小文字を区別します。パスワードをより安全なパスワードに変更し、「付録 A 基本計画のワークシート」に記録しておくことをお勧めします。

9. 再度ログイン画面が表示されますので、ユーザ名と新しいパスワードを入力してログインします。

10. ログインに成功すると以下の画面が表示されます。
本画面（**Status > Dashboard** 画面）には一般的なステータス情報、LAN/WLAN のステータス情報が表示されます。

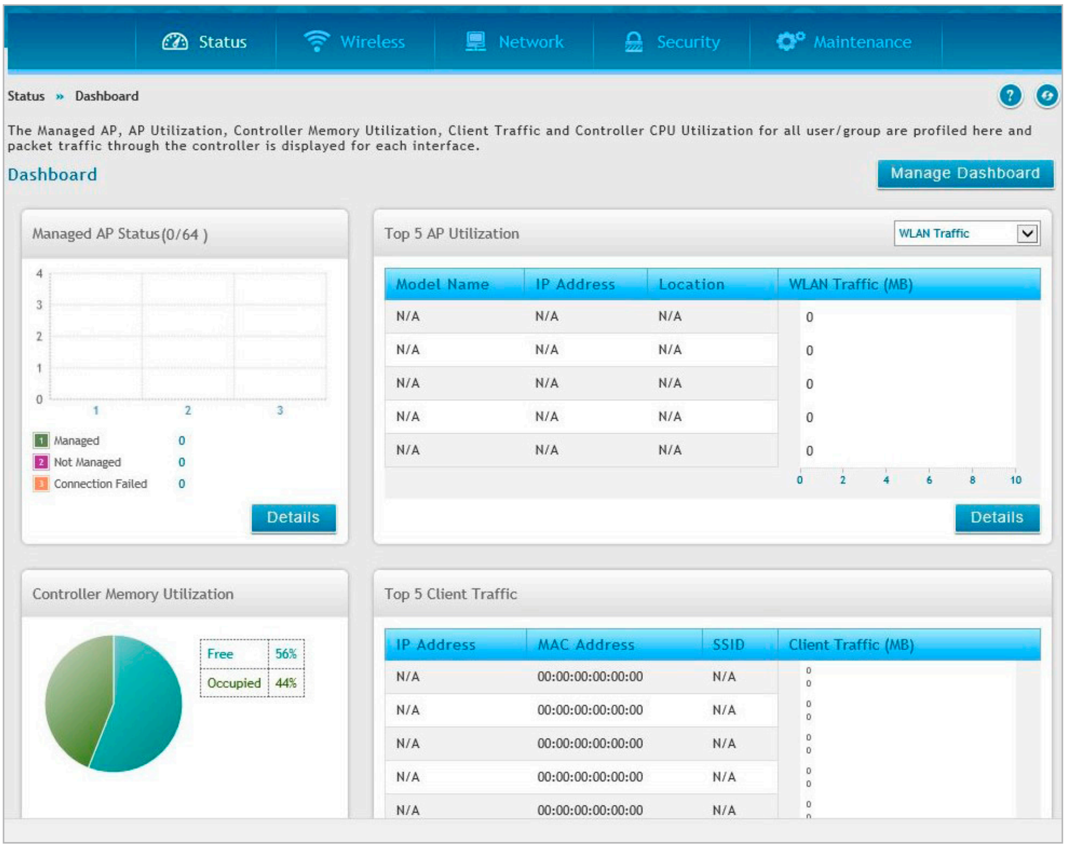


図 3-4　　ダッシュボード画面

11. 設定画面で変更を行った場合は、「Save」ボタンを押して変更した設定を保存します。

12. Web 管理インタフェースからログアウトするには、システムメニューエリアの右上隅にある「Logout」アイコンをクリックします。

図 3-5　　Logout アイコン

Web 管理インタフェースの画面構成

Web 管理インタフェース画面には、以下の項目があります。

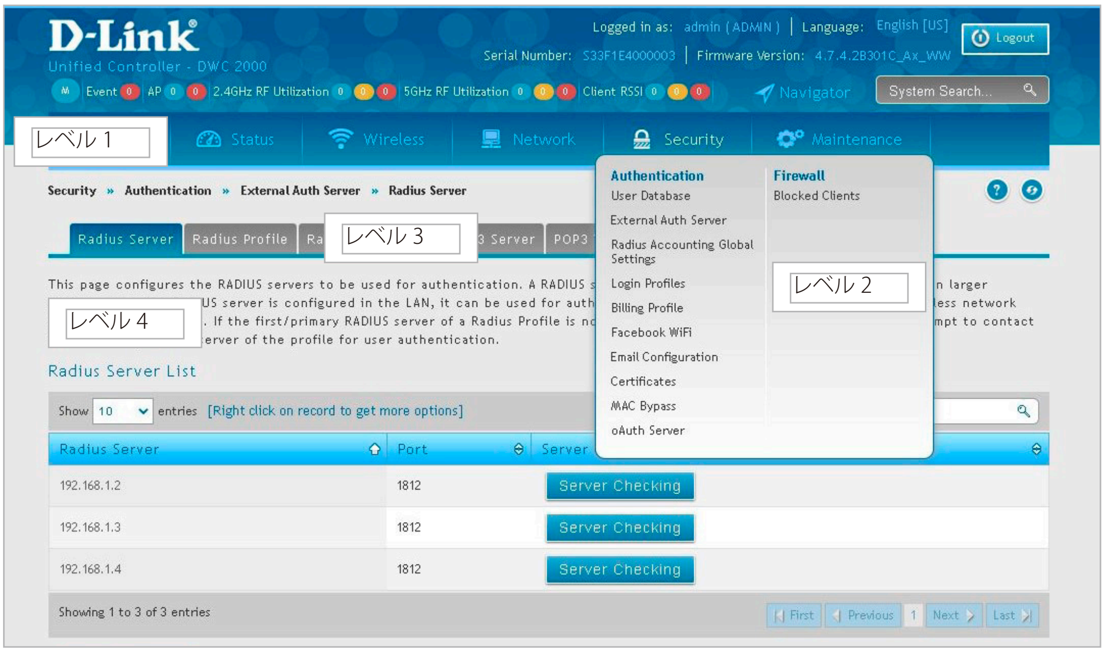


図 3-6　　メニュー構成

項目	コンポーネント	説明
レベル 1	メインナビゲーションメニュータブ	Web 管理インタフェースの上部に表示されます。このタブは、すべての設定メニューへのアクセスを提供しており、常に表示されています。
レベル 2	メインナビゲーションの サブメニュータブ	メインナビゲーションタブ上にマウスを移動すると、メインナビゲーションのサブメニューあ表示されます。
レベル 3	中央にあるメニューのタブ	ページによっては、メインナビゲーションメニュータブの下にメニュータブがあり、クリックすると、他のページに遷移します。
レベル 4	ワークスペース	選択したメニューとサブメニューに関連するパラメータを表示します。

ワークスペースには、以下のアクションボタン及びメニューが表示されます。
メニューは設定する項目を右クリックして表示します。

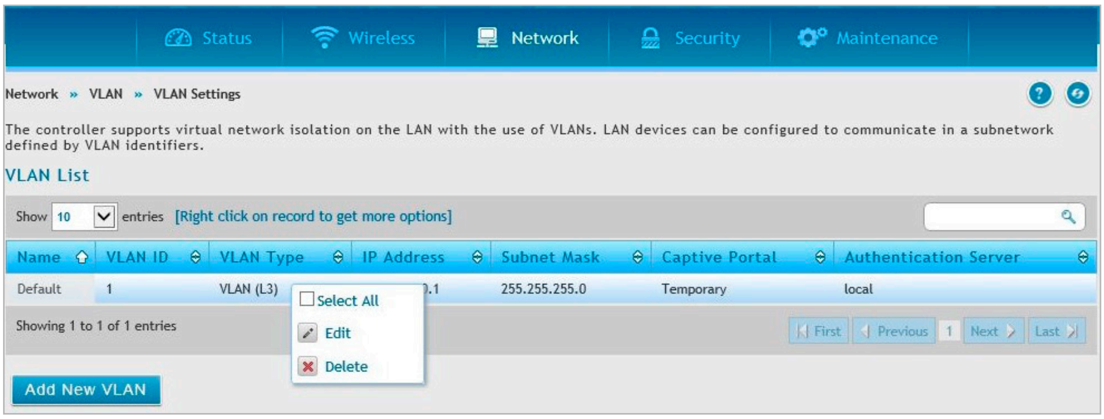


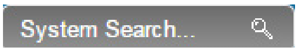
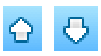
図 3-7　　ワークスペース

アクションボタンは、コンフィグレーションの変更などに適用されます。一般的なアクションボタンは以下の通りです。

アクションボタン	説明
Save	現在の画面に行ったコンフィグレーション変更のすべてを保存します。無線コントローラが電源オフまたは再起動されても、保存された設定は保持されます。未保存のコンフィグレーションの変更は失われます。
Cancel	現在の画面上のオプションは、最後に適用または保存された設定にリセットされます。
Add	現在の画面に新しく項目を追加します。
右クリックメニュー	右クリックメニューの項目を使用すると、既存の設定項目に対して様々なアクションを行うことができます。 ・Edit - 本項目のコンフィグレーションを編集します。 ・Delete - 本項目を削除します。 ・Move - 本項目を指定位置に移動します。 ・Enable - 本項目を有効にします。 ・Disable - 本項目を無効にします。 ・Apply - 既存のコンフィグレーションに本変更を適用します。 ・Copy - 本項目のコンフィグレーションをコピーして、新しく項目を作成します。 ・Manage - 検出されたアクセスポイントを管理します。 ・View Information - 項目によって異なる情報が表示されます。

Web 管理インタフェースの機能について

本製品の Web 管理インタフェースには以下の機能があります。

項目	説明
 ヘルプ機能	各種機能やインタフェースの設定について説明します。本アイコンをクリックして､ヘルプメニューを表示します。ヘルプ機能のアイコンは常に画面の右上にあります。
	検索ボックスに単語を入力することで、機能や特徴を検索できます。画面の右上にあります。
 ナビゲータ機能	無線プロファイルの設定、AP 管理の設定、外部認証の設定、システムの設定など、一般的なコンフィグレーションタスクに役立つガイドを提供します。本アイコンをクリックして、ウィザードを起動します。画面の右上隅の「System Search」ボックスの左にあります。
 Refresh 機能	本アイコンをクリックすると、変更を直ちに適用し、インタフェースを最新の情報に更新します。画面の右上隅にあり、「Help」アイコンの右に位置します。
	本アイコンをクリックすると、インタフェースから安全にログアウトします。画面の右上隅にあります。
 メニューナビゲーションルート	現在のページまでのメニュールートを表示します。
	1 ページに表示されるテーブルの項目数を表示します。1 ページに 10、25、50、100 のエントリを表示することができます。
 First/ Previous/ Next/ Last（テーブル上）	テーブルエントリが複数ページに渡る場合に､本項目が表示されます。First/ Previous/ Next/ Last（最初のページ /1 つ前のページ /1 つ後のページ / 最後のページ）を使用して、ページを切り替えます。テーブルの右下に位置しています。
 検索バー（テーブル上）	検索ボックスに単語を入力することで、テーブル内の情報を検索できます。検索ボックスは、テーブルの右上にあります。
 ランキング / ソート（テーブル上）	テーブルのヘッダをクリックすることで､テーブル上の値や情報の相対的な順序をランキング / ソートします。

また、画面上部にはアクセスポイントやクライアントの接続統計情報を示すアイコンが表示されます。各アイコンをクリックすると、詳細画面に遷移します。

項目	説明
	クラスタコントローラのステータス、イベント数が表示されます。
	「Managed APs」「Connection Failed APs」のアクセスポイントの台数を表示します。 詳細は「管理対象のアクセスポイント」を参照してください。
	2.4GHz 帯域における RF 利用率（Low/Medium/High）ごとのアクセスポイントの台数を表示します。
	5GHz 帯域における RF 利用率（Low/Medium/High）ごとのアクセスポイントの台数を表示します。
	RSSI のステータス（Low/Medium/High）ごとのクライアントの台数について表示します。

ナビゲータ機能

ナビゲータ機能を使用すると、セットアップウィザードの手順に従って、機能のカテゴリ別に基本的な設定を行うことが可能です。

Web インタフェース右上のナビゲータアイコン上にマウスを移動すると、以下のメニューが表示されます。

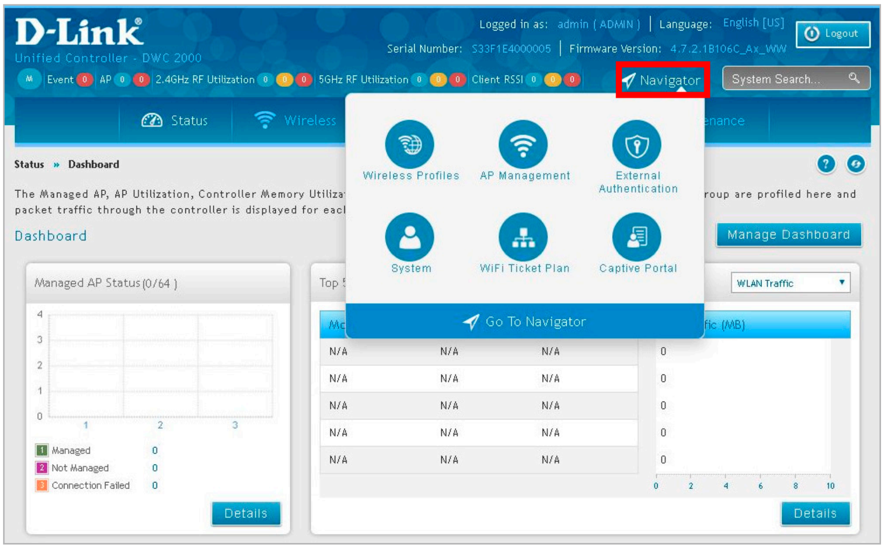


図 3-8　　ナビゲータメニュー

無線プロファイルの設定

無線プロファイル設定のウィザードを開始します。これらの設定の詳細については、「AP プロファイル」「AP プロファイル SSID の設定」を参照してください。

1. ナビゲータメニューから「Wireless Profiles」をクリックし、無線プロファイル設定のウィザードを開始します。

図 3-9　　ナビゲータメニュー

2. AP プロファイルの設定を行います。ウィザードを中断するには、右上の「×」ボタンをクリックし、「Abandon」を選択します。「Next」をクリックして次の画面に進みます。

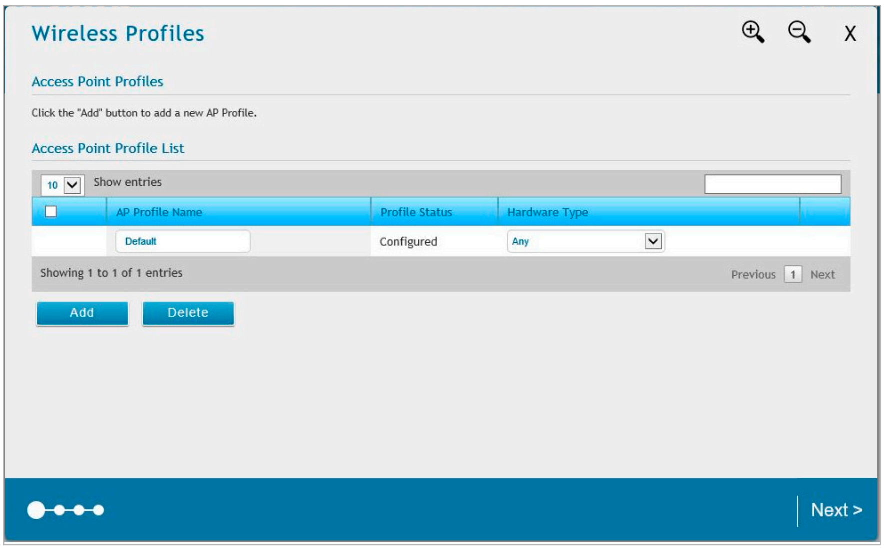


図 3-10　無線プロファイル設定 - AP プロファイル一覧

以下の項目を設定します。

項目	説明
AP Profile Name	AP プロファイル名が表示されます。
Profile Status	AP プロファイルの状態が表示されます。
Hardware Type	このプロファイルを使用するアクセスポイントのハードウェアタイプを選択します。

3.　新規の AP プロファイルを追加するには、「Add」をクリックして以下の画面を表示します。

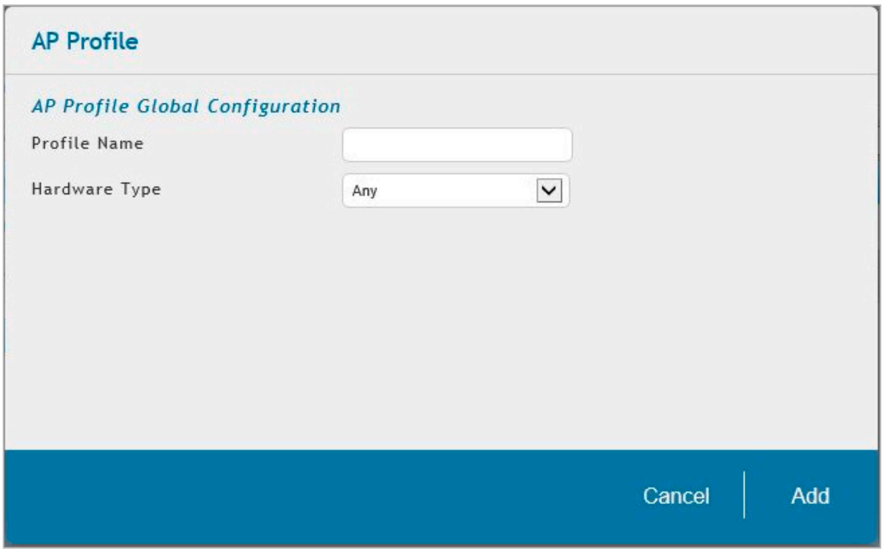


図 3-11　無線プロファイル設定 - AP プロファイルの追加

以下の項目を設定し、「Add」をクリックします。設定を破棄して元の画面に戻るには、「Cancel」をクリックします。

項目	説明
AP Profile Name	AP プロファイル名を入力します。
Hardware Type	このプロファイルを使用するアクセスポイントのハードウェアタイプを選択します。

4.　AP プロファイルの無線設定を行います。「Next」をクリックして次の画面に進みます。

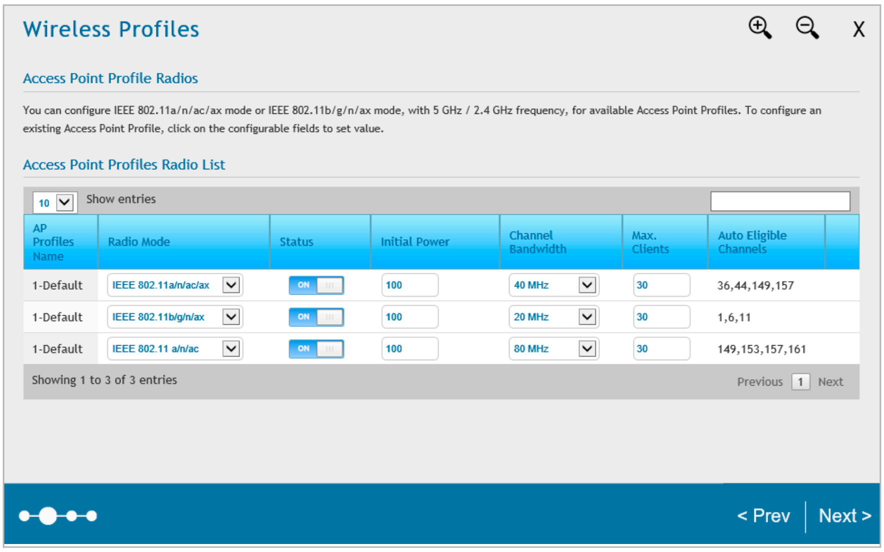


図 3-12　無線プロファイル設定 - AP プロファイルの無線設定

以下の項目を設定します。

項目	説明
AP Profiles Name	無線プロファイル名が表示されます。
Radio Mode	無線モードを指定します。 「Radio Mode」に表示される選択肢は「Channel Bandwidth」で指定されている内容によって異なります。 また、「Radio Mode」で選択した項目によって、「Channel Bandwidth」に表示される選択肢が変更されます。
Status	無線プロファイルを「ON」（有効）または「OFF」（無効）にします。
Initial Power	初期電力レベルを指定します。
Channel Bandwidth	チャンネル帯域を「20 Mhz」「40 Mhz」「80Mhz」「80+80Mhz」から選択します。
Max. Clients	本アクセスポイントに一度にアクセスできるステーションの最大数（0-200）を指定します。

5. AP プロファイルの SSID 設定を行います。「Next」をクリックして次の画面に進みます。

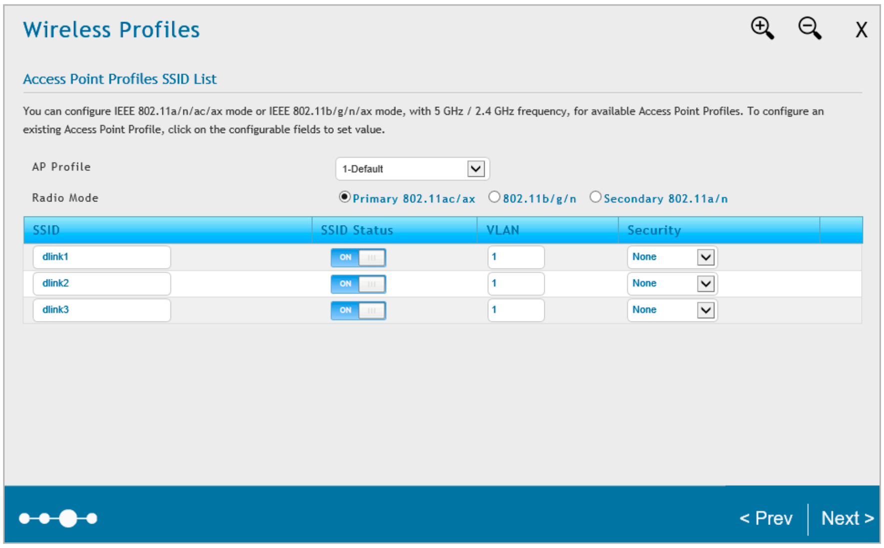


図 3-13　無線プロファイル設定 - AP プロファイルの SSID 設定

以下の項目を設定します。

項目	説明
AP Profile	設定する AP プロファイルを選択します。
Radio Mode	設定する無線モードを選択します。
SSID	無線ネットワーク名（大文字と小文字の区別あり）を入力します。
SSID Status	SSID のステータスを「ON」（有効）または「OFF」（無効）にします。
VLAN	VLAN ID を入力します。
Security	セキュリティタイプを選択します。ご使用のネットワークを保護するためには、セキュリティメカニズムを選択し、未認証の無線クライアントがネットワークにアクセスすることを防止することをお勧めします。 • None - セキュリティメカニズムを使用しません。 • OWE - OWE（Opportunistic Wireless Encryption）セキュリティを有効にします。 • WPA Personal - WPA Personal セキュリティを有効にします。 -「WPA Key」「Confirm Key」に WPA キーを入力します。 -「WPA3 Status」を「ON」にした場合は、「WPA3 Key」「Confirm WPA3 Key」に WPA3 キーを入力します。WPA キーと同じキーを使用する場合は「Same as WPA Key」をチェックします。 • WPA Enterprise - WPA Enterprise セキュリティを有効にします。 -「WPA3 Status」を「ON」または「OFF」にします。 - RADIUS サーバの IP アドレスとシークレットを入力します。

6. 設定した内容が表示されます。「Finish」をクリックすると、設定が保存されます。

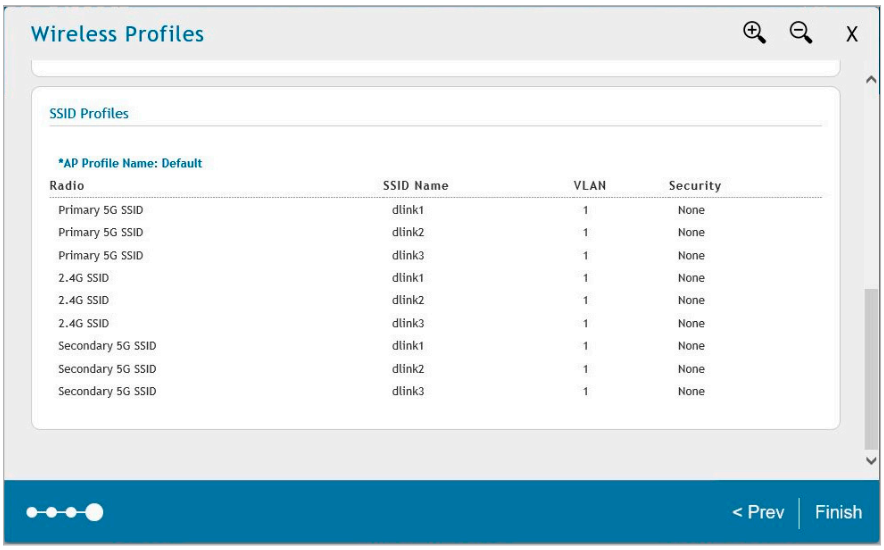


図 3-14　無線プロファイル設定 - 設定の確認

注意 DWL-7620AP/DWL-6620APS のみ、AP プロファイルで WMF(Wireless Multicast Forwarding) の設定を行うことができます。

管理アクセスポイント設定

管理対象のアクセスポイントを設定します。これらの設定の詳細は「Not Managed AP List からアクセスポイントを追加する」を参照してください。

1. ナビゲータメニューから「AP Management」をクリックし、AP 管理設定のウィザードを開始します。

図 3-15　ナビゲータメニュー

2. アクセスポイントが存在する IP 範囲及び VLAN に対して、L2/L3 ディスカバリを実行します。特定範囲を指定しない場合は、そのまま「Next」をクリックしてください。ウィザードを中断するには、右上の「×」ボタンをクリックし、「Abandon」を選択します。

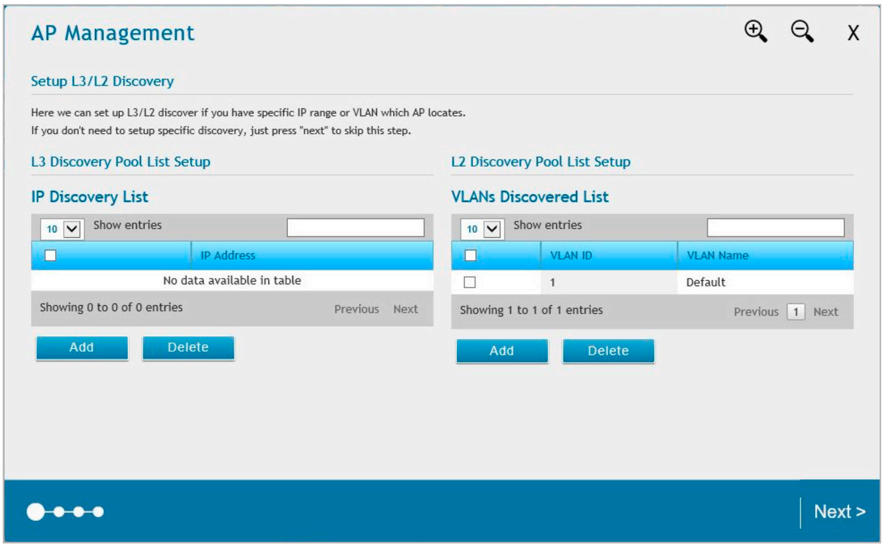


図 3-16　AP 管理設定 - L2/L3 ディスカバリ

3. IP 範囲を指定するには、「IP Discovery List」で「Add」をクリックし、以下の画面を表示します。

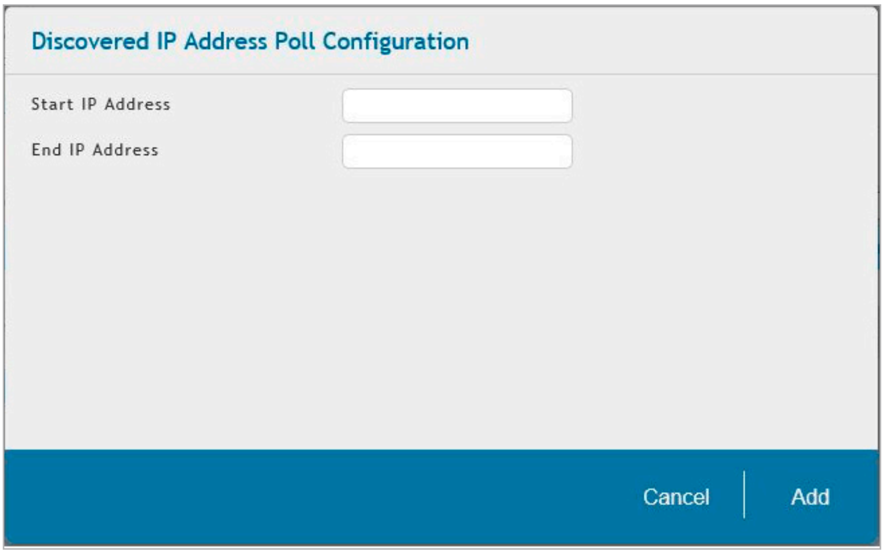


図 3-17　AP 管理設定 - L2/L3 ディスカバリ（IP アドレス）

以下の項目を設定し、「Add」をクリックします。

項目	説明
Start IP Address	IP 範囲の開始アドレスを指定します。
End IP Address	IP 範囲の終了アドレスを指定します。

4. VLAN を追加するには、「VLANs Discovery List」で「Add」をクリックし、以下の画面を表示します。

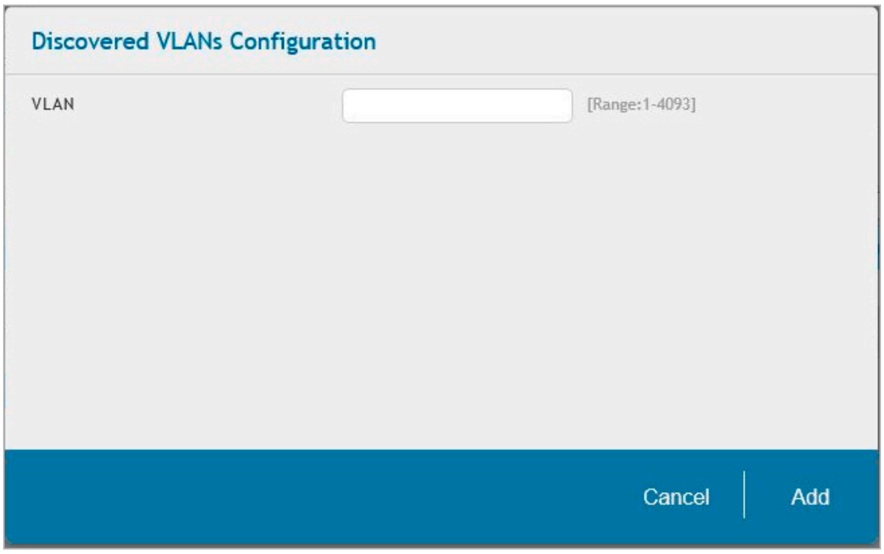


図 3-18　AP 管理設定 - L2/L3 ディスカバリ（VLAN）

以下の項目を設定し、「Add」をクリックします。

項目	説明
VLAN	VLAN ID を入力します。

5. 「Candidate AP List」に検出されたアクセスポイントが表示されます。管理対象のアクセスポイントを選択し、右矢印をクリックして「To be Managed AP List」に移動します。「Next」をクリックし、次に進みます。

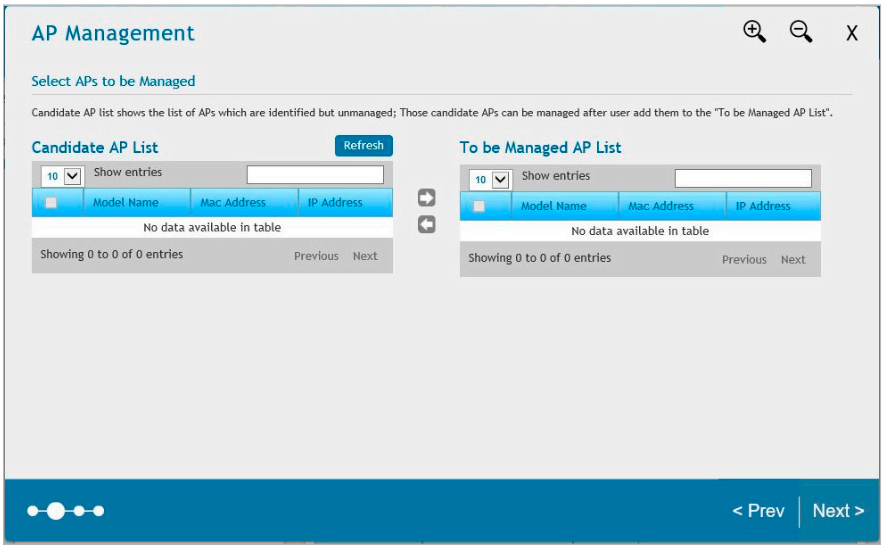


図 3-19　AP 管理設定 - 管理対象のアクセスポイントの選択

6.　以下の画面が表示されます。

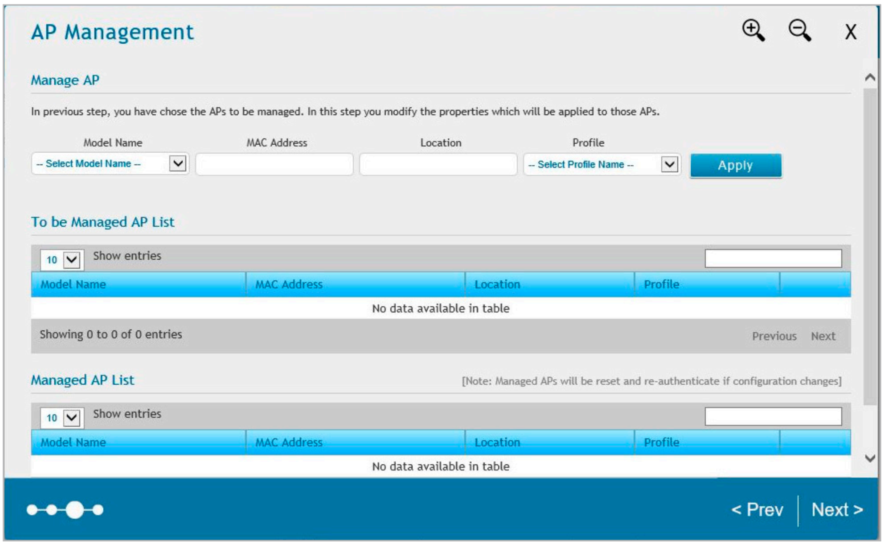


図 3-20　AP 管理設定 - プロファイルの適用

以下の項目を設定し、「Apply」をクリックします。

項目	説明
Model Name	プロファイルを適用するアクセスポイントのハードウェアタイプを選択します。
MAC Address	個別に設定する場合、アクセスポイントの MAC アドレスを入力します。
Location	アクセスポイントのロケーション（位置）を入力します。
Profile	指定したハードウェアタイプまたは MAC アドレスのアクセスポイントに適用する AP プロファイルを選択します。

「To be Managed AP List」「Managed AP」でアクセスポイント毎にプロファイルを指定することも可能です。

設定完了後、「Next」をクリックします。

7.　設定した内容が表示されます。「Finish」をクリックすると、設定が保存されます。

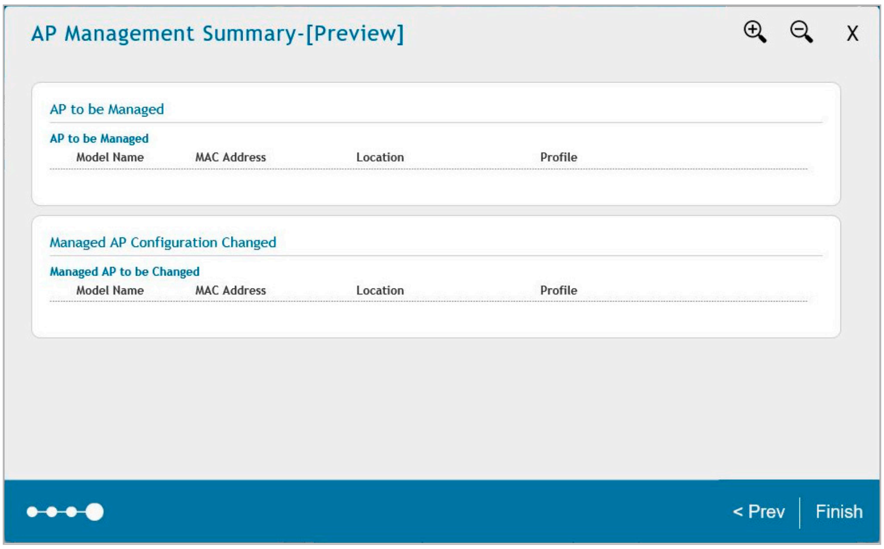


図 3-21　AP 管理設定 - 設定の確認

外部認証設定

外部認証サーバを設定します。外部認証サーバの詳細については、「外部認証」を参照してください。

1. ナビゲータメニューから「External Authentication」をクリックし、外部認証設定のウィザードを開始します。

図 3-22　ナビゲータメニュー

2. 外部認証サーバを選択し、「Next」をクリックします。「Radius Server」「LDAP Server」「POP3 Server」のいずれかを選択します。ウィザードを中断するには、右上の「×」ボタンをクリックし、「Abandon」を選択します。

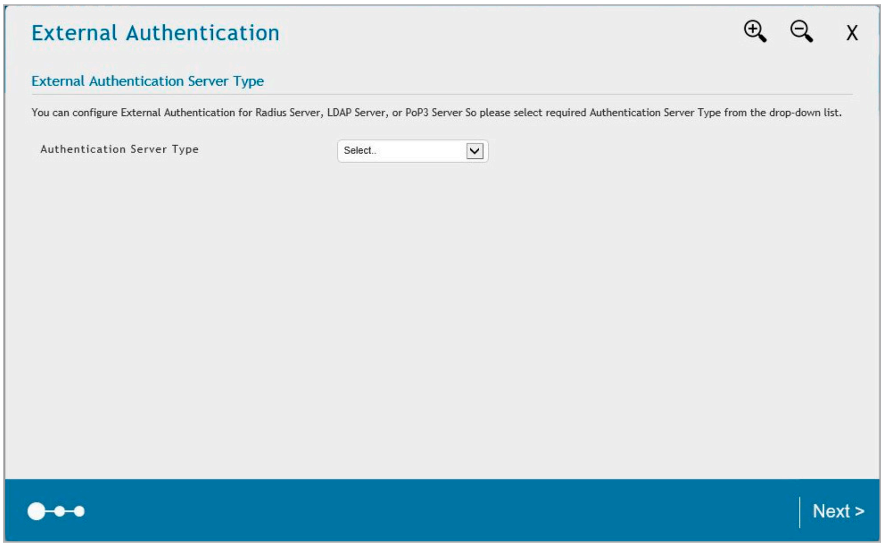


図 3-23　外部認証設定 - 外部認証サーバの選択

RADIUS サーバの設定

Radius Server を選択した場合、以下の画面が表示されます。

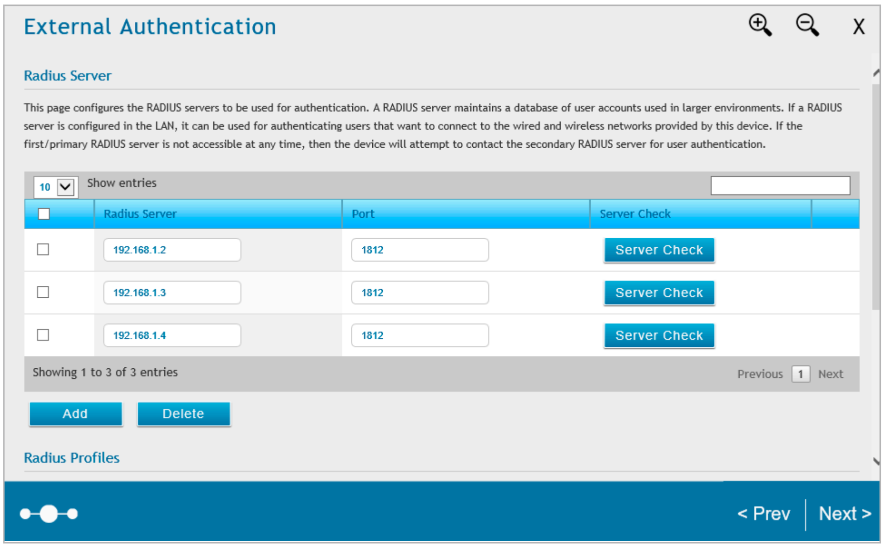


図 3-24　外部認証設定 - RADIUS サーバ

3. Radius サーバを追加するには、「Radius Server」セクションで「Add」をクリックし、以下の画面を表示します。

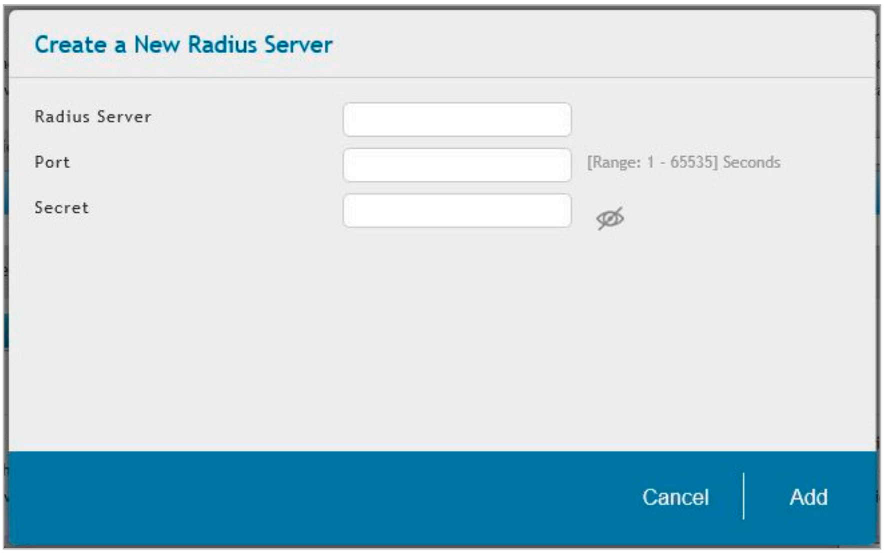


図 3-25　外部認証設定 - RADIUS サーバの追加

以下の項目を設定し、「Next」をクリックします。

項目	説明
Radius Server	RADIUS サーバの IP アドレスを指定します。
Port	RADIUS サーバのポート番号を指定します。
Secret	RADIUS サーバにログインするための秘密鍵を指定します。

LDAP サーバの設定

LDAP Server を選択した場合、以下の画面が表示されます。

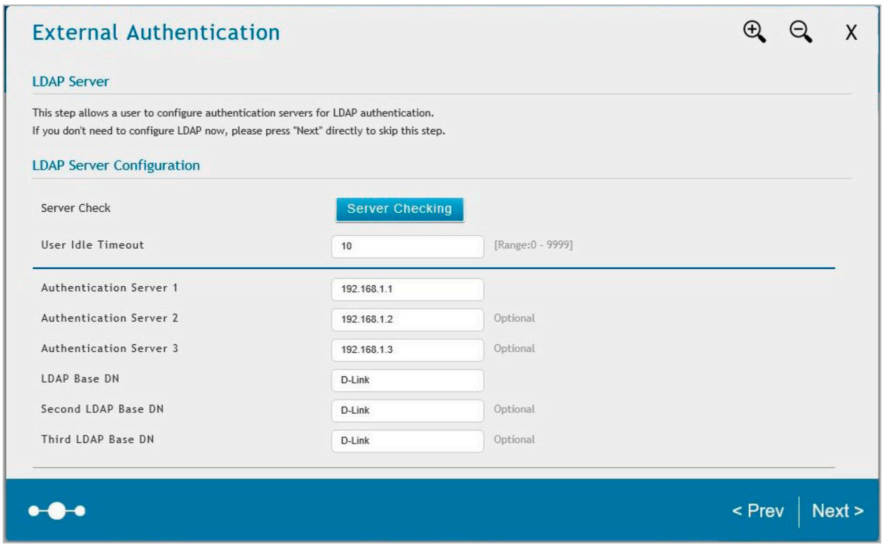


図 3-26　外部認証設定 - LDAP サーバ

以下の項目を設定し、「Next」をクリックします。

項目	説明
Server Check	コントローラと認証サーバ間の接続をテストします。
User Idle Timeout	アイドル状態になってからタイムアウトするまでの時間を指定します。
Authentication Server 1-3	LDAP 認証サーバの IP アドレスを指定します。
LDAP Base DN	LDAP 認証におけるベースドメイン名を指定します。
Second LDAP Base DN	セカンダリ LDAP サーバに対し、LDAP 認証におけるベースドメイン名を指定します。
Third LDAP Base DN	ターシャリ LDAP サーバに対し、LDAP 認証におけるベースドメイン名を指定します。

POP3 サーバの設定

POP3 Server を選択した場合、以下の画面が表示されます。

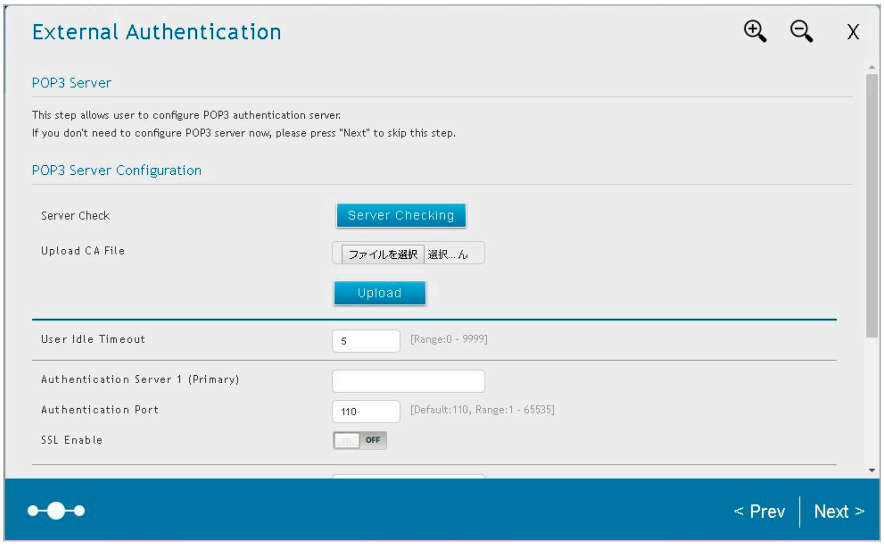


図 3-27　外部認証設定 - POP3 サーバ

以下の項目を設定し、「Next」をクリックします。

項目	説明
Server Check	コントローラと認証サーバ間の接続をテストします。
Upload CA File	CA 証明書を選択し、「Upload」をクリックしてファイルをアップロードします。
Authentication Server 1-3	POP3 認証サーバの IP アドレスを指定します。
Authentication Port	POP3 メッセージを送信する認証サーバのポートを指定します。
SSL Enable	POP3 の SSL サポートを有効にします。
Choose a CA file	SSL を有効化する場合、POP3 サーバの証明書を検証する CA（認証局）を指定します。

4. 設定した内容が表示されます。「Finish」をクリックすると、設定が保存されます。

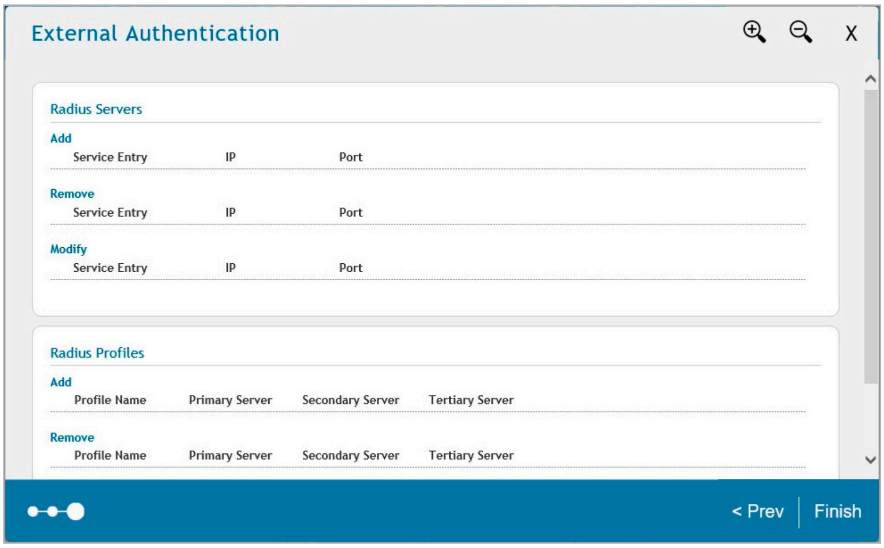


図 3-28　外部認証設定 - 設定の確認

システム設定

管理グループ、ユーザアカウント、システム時刻などのシステム設定を行います。システム設定の詳細については「システム設定」を参照してください。

1. ナビゲータメニューから「System」をクリックし、外部認証設定のウィザードを開始します。

図 3-29　ナビゲータメニュー

2. 管理ユーザグループの設定を行い、「Next」をクリックします。ウィザードを中断するには、右上の「×」ボタンをクリックし、「Abandon」を選択します。

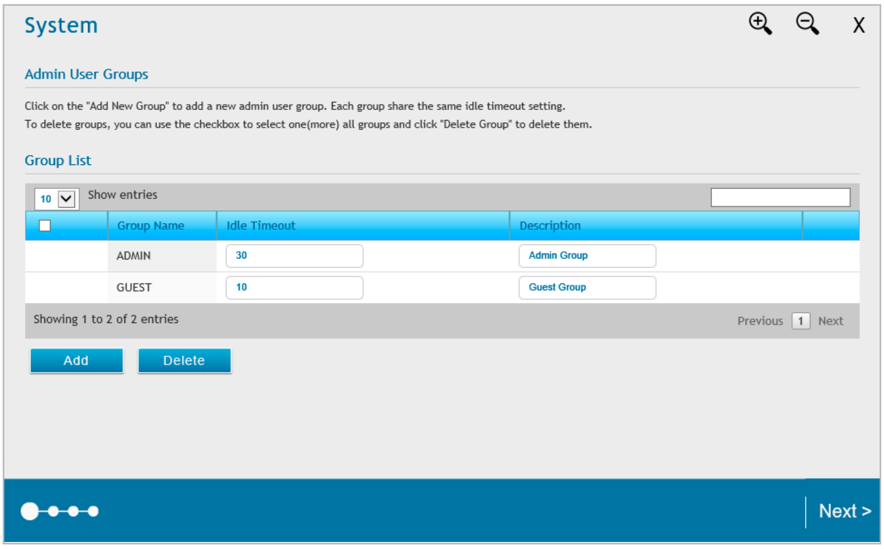


図 3-30　システム設定 - 管理ユーザグループ

以下の項目を設定します。

項目	説明
Group Name	グループ名が表示されます。
Idle Timeout	本項目で設定した時間内に Web 管理インタフェースで操作を行わなかった場合、自動的に Web 管理インタフェースからログアウトします。 0 に設定した場合はログアウトを行いません。
Description	ユーザグループの説明文を入力します。

3.　新規の管理ユーザグループを追加するには、「Add」をクリックして以下の画面を表示します。

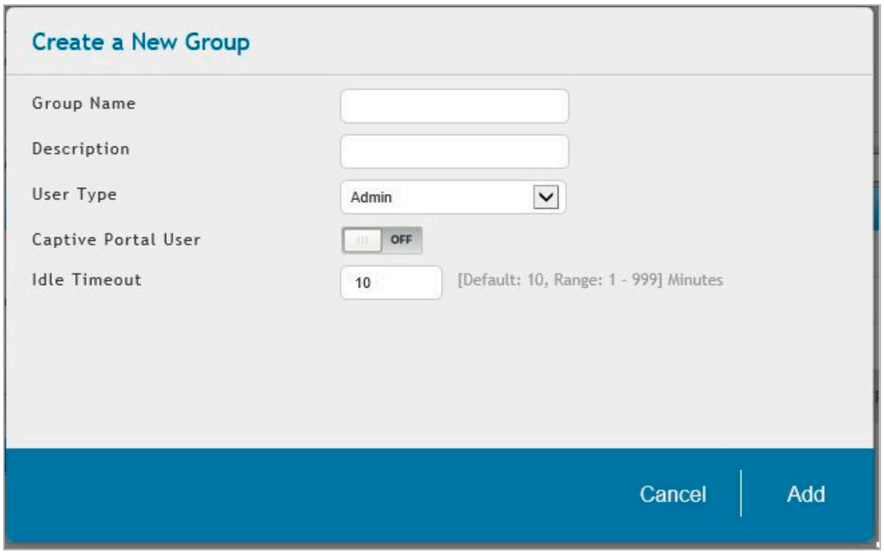


図 3-31　システム設定 - 管理ユーザグループの追加

以下の項目を設定し、「Add」をクリックします。設定を破棄して元の画面に戻るには、「Cancel」をクリックします。

項目	説明
Group Name	グループ名を入力します。
Description	グループの説明文を入力します。
User Type	ユーザタイプを選択します。 • Admin - このグループのユーザは管理者権限を持ちます。ユーザはデバイスを設定することができます。キャプティブポータルユーザを有効化すると、キャプティブポータル認証経由でのインターネット / ネットワークへの接続が可能になります。 • Network - このグループのユーザはネットワーク権限を持ち、キャプティブポータルユーザを有効化すると、キャプティブポータル認証経由でのインターネット / ネットワークへの接続が可能になります。 • Front Desk - このグループのユーザは、ホットスポットからインターネット / ネットワークにアクセスできる一時的ユーザを作成する権限を持ちます。 • Guest - このグループのユーザは、参照権限のみを持ちます。ユーザはデバイスを設定することができません。
Captive Portal User	Captive Portal 権限を持つグループのユーザは、Captive Portal 認証を通じてインターネット / ネットワークにアクセスする権限を持ちます。
Session Timeout	このプロファイルで生成される CP ユーザのアイドルタイムを指定します。
Idle timeout	本項目で設定した時間内に Web 管理インタフェースで操作を行わなかった場合、自動的に Web 管理インタフェースからログアウトします。 0 に設定した場合はログアウトを行いません。

4.　ユーザアカウントの設定を行い、「Next」をクリックします。

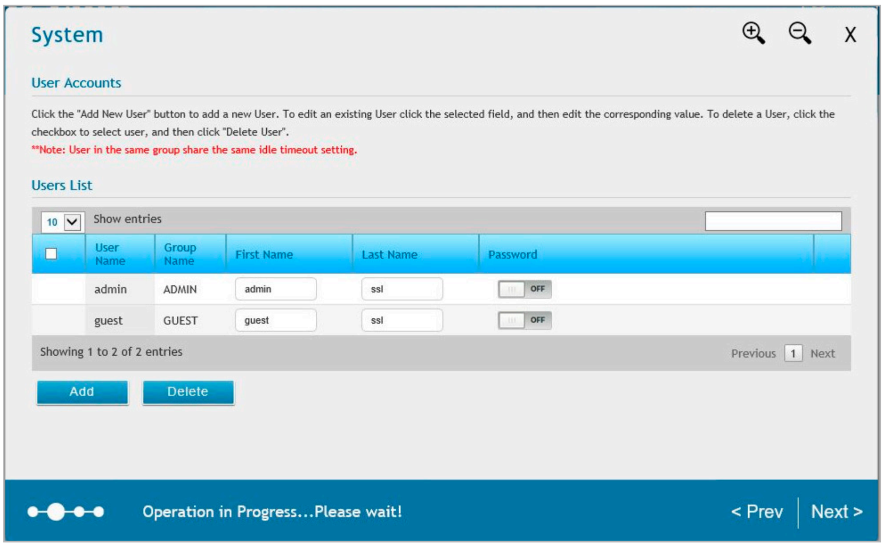


図 3-32　システム設定 - ユーザアカウント

既存ユーザの編集を行うには、以下の項目を設定します。

項目	説明
User Name	ユーザ名が表示されます。
Group Name	グループ名が表示されます。必要に応じて編集します。
First Name	ユーザの名前を入力します。
Last Name	ユーザの名字を入力します。
Password	「ON」に設定するとパスワードを変更することができます。1 番目の入力フィールドに現在のパスワードを入力し、2 番目と 3 番目の入力フィールドに新しいパスワードを入力します。

5.　システム時刻の設定を行い、「Next」をクリックします。

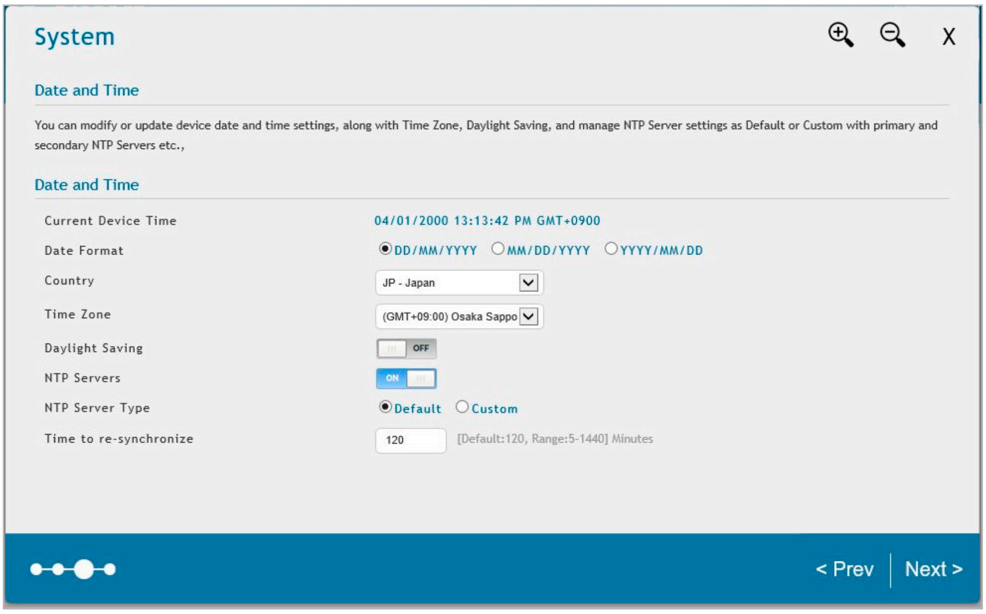


図 3-33　システム設定 - 時刻設定

以下の項目を設定します。

項目	説明
Current Device Time	現在のシステム時刻が表示されます。
Date Format	時刻の表示形式を選択します。
Country	無線ネットワークを使用する国を選択します。「Country Code」のプルダウンメニューから「JP-Japan」を選択します。
Time Zone	グリニッジ標準時（GMT）に対するコントローラのタイムゾーンを選択します
Daylight Saving	サマータイムを「ON（有効）/OFF（無効）」にします。
NTP Servers	NTP サーバの利用を「ON（有効）/OFF（無効）」にします。
NTP Server Type	NTP サーバのタイプ（Default または Custom）を選択します。「Custom」の場合、サーバのアドレスまたは FQDN を入力します。
Time to re-synchronize	NTP サーバが有効の場合、NTP サーバと同期する間隔を選択します。（単位：分、初期値：120 分）
Set Date and Time Manually	NTP サーバが無効の場合、手動で時刻を設定します。

以下の確認メッセージが表示されます。「OK」をクリックします。

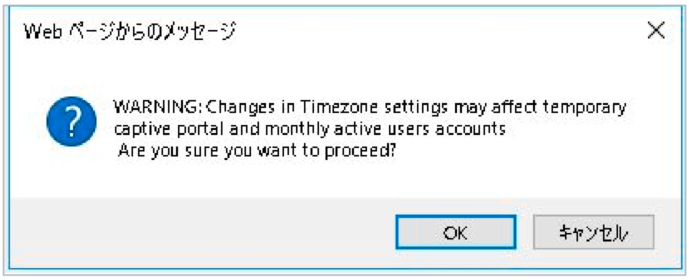


図 3-34　確認メッセージ

6. 設定した内容が表示されます。「Finish」をクリックすると、設定が保存されます。

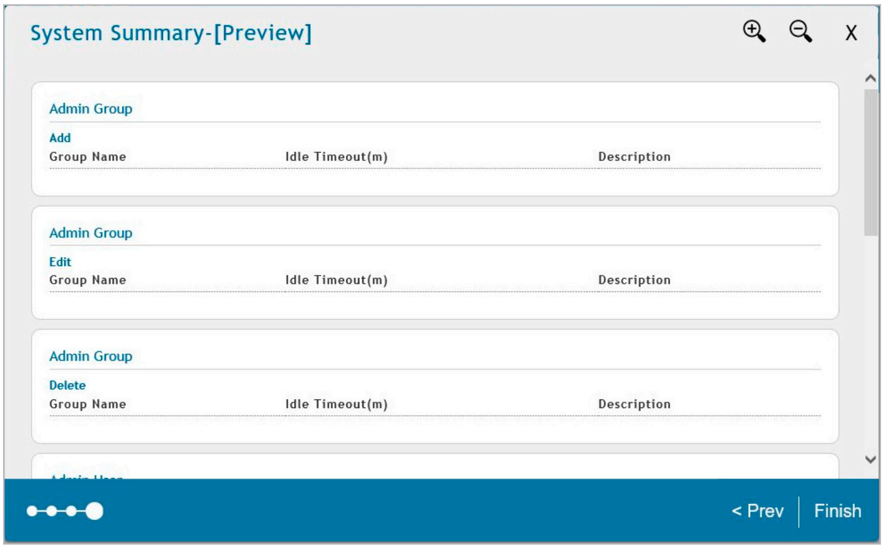


図 3-35　システム設定 - 設定の確認

WiFi チケットプラン設定

WiFi チケットプランの設定を行います。これらの設定の詳細については「ビリングプロファイル」を参照してください。

1. ナビゲータメニューから「WiFi Ticket Plan」をクリックし、WiFi チケットプラン設定のウィザードを開始します。

図 3-36　ナビゲータメニュー

2. チケットプランの設定を行います。ウィザードを中断するには、右上の「×」ボタンをクリックし、「Abandon」を選択します。

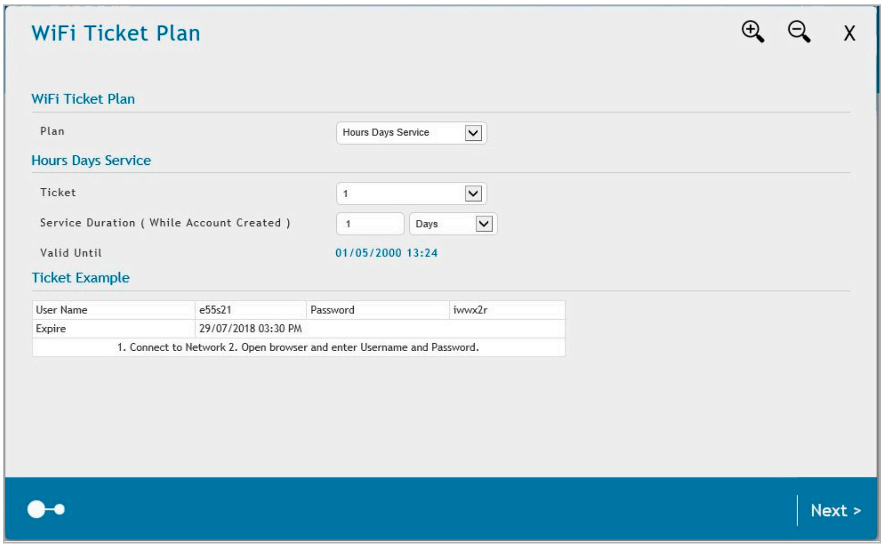


図 3-37　WiFi チケットプラン設定 - チケットプランの設定

以下の項目を設定し、「Next」をクリックします。

項目	説明
WiFi Ticket Plan	
Plan	サービスの利用を制限する単位を指定します。 ・ Hours Days Service - 時間単位でサービスの利用を制限します。 ・ MB GB Service - 容量単位でサービスの利用を制限します。
Hours Days Service	
Ticket	チケットの番号を選択します。
Service Duration (While Account Created)	単位（Hours または Days）を選択して、サービス利用時間を設定します。
Maximum usage Traffic	ユーザが使用できる最大トラフィック（MB または GB）を指定します。 「Plan」で「MB GB Service」を選択した場合に表示されます。
Valid Until	有効期限が表示されます。

3. 設定した内容が表示されます。設定した内容は、「Print」をクリックして印刷することができます。「Finish」をクリックすると、設定が保存されます。

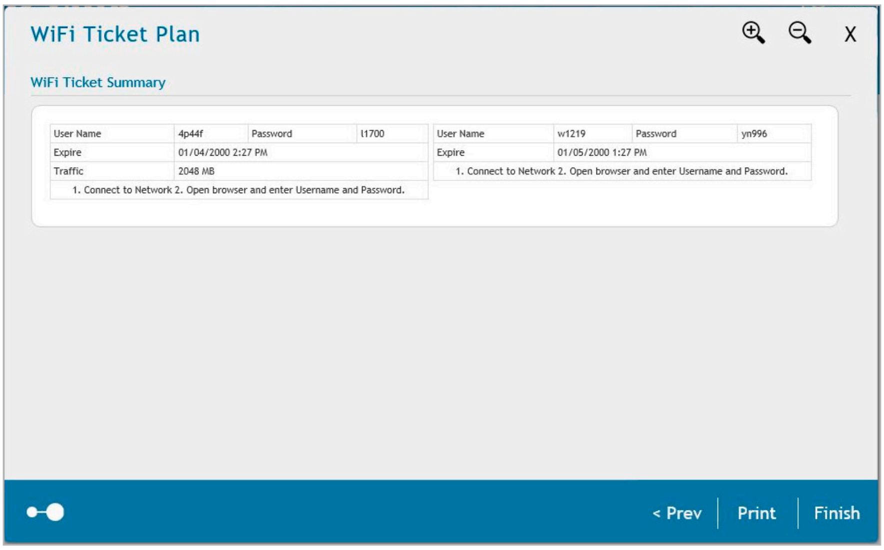


図 3-38　WiFi チケットプラン設定 - 設定の確認

キャプティブポータル設定

キャプティブポータルを設定します。これらの設定の詳細については、「AP プロファイル SSID の設定」を参照してください。

1. ナビゲータメニューから「Captive Portal」をクリックし、キャプティブポータル設定のウィザードを開始します。

図 3-39　ナビゲータメニュー

2. キャプティブポータルで使用するサーバを選択し、「Next」をクリックします。「Local User Database」「Radius Server」「LDAP Server」「POP3 Server」のいずれかを選択します。ウィザードを中断するには、右上の「×」ボタンをクリックし、「Abandon」を選択します。

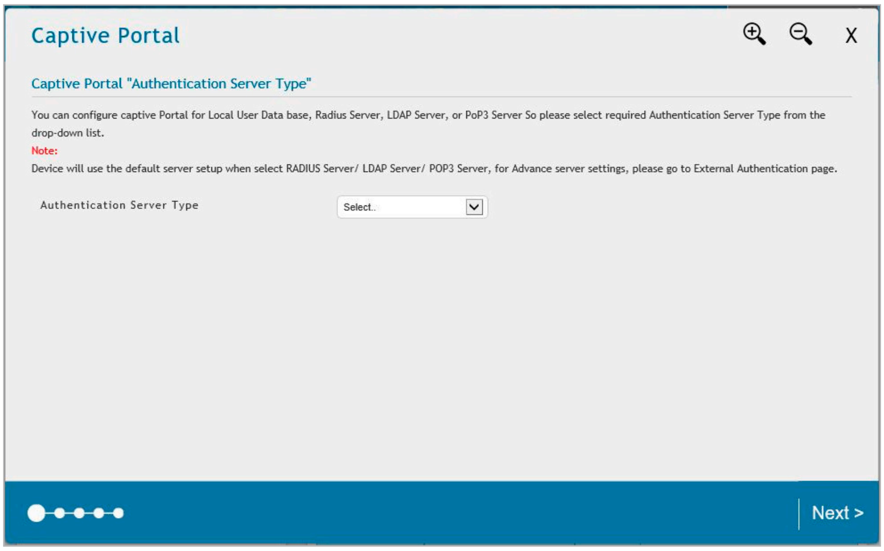


図 3-40　キャプティブポータル設定 - サーバの選択

3. Local User Database を選択した場合、以下の画面が表示されます。ユーザデータベースを CSV 形式でアップロードします。手動で追加する場合は次の画面で設定します。「Next」をクリックします。Local User Database 以外の場合、手順 6 に進んでください。

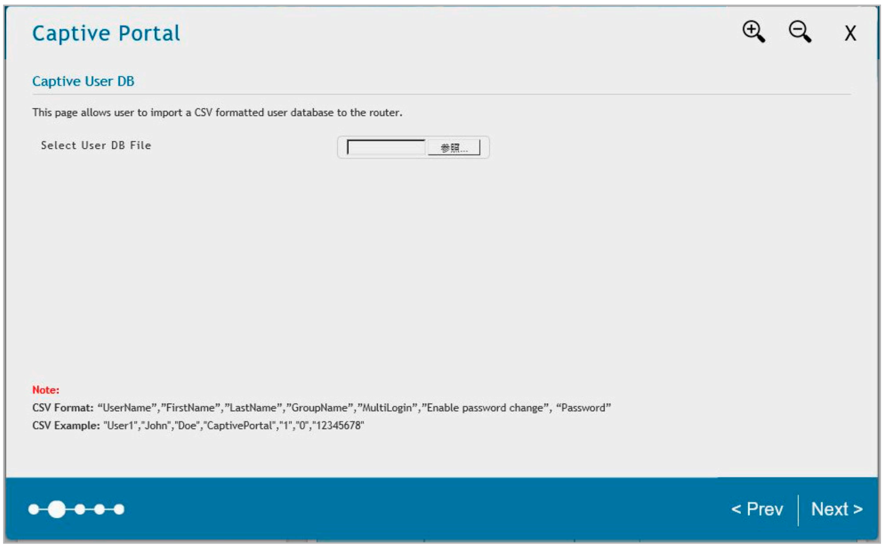


図 3-41　キャプティブポータル設定 - ローカル DB のアップロード

4. ユーザー一覧が表示されます。

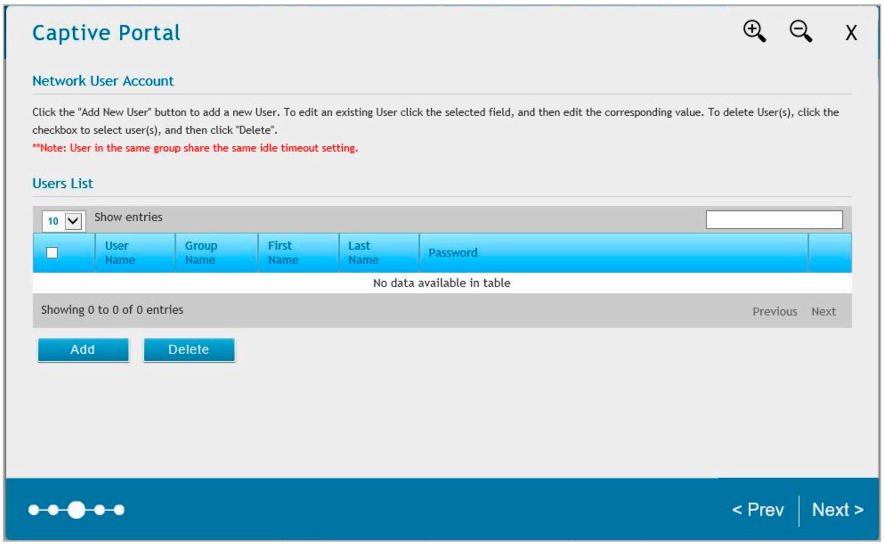


図 3-42　キャプティブポータル設定 - ユーザー覧

5. ユーザ追加するには、「Add をクリックして以下の画面を表示します。

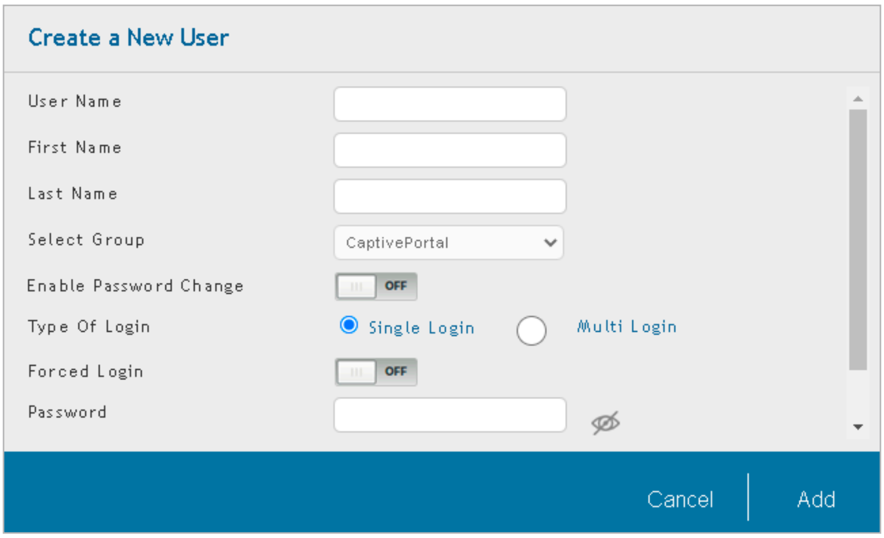


図 3-43　キャプティブポータル設定 - ユーザの追加

以下の項目を設定します。

項目	説明
User Name	ユーザ名を入力します。
First Name	ユーザの名前を入力します。
Last Name	ユーザの名字を入力します。
Select Group	ユーザが所属するキャプティブポータルグループを選択します。
Enable Password Change	「ON」を選択すると、ユーザがパスワードの変更を行うことができるようになります。
Type Of Login	ログインのタイプを以下から選択します。 • Single Login - ユーザが同一のユーザ名 / パスワードを使用して、複数のデバイスから同時にログインすることはできません。 • Multi Login - ユーザが同一のユーザ名 / パスワードを使用して、複数のデバイスから同時にログインすることができます。
Forced Login	強制ログインを「ON」または「OFF」に設定します。「Single Login」を選択した場合にのみ表示されます。
Max Login Uses	「Multi Login」を選択した場合、同時にログインできるユーザの最大数を入力します。
Password	パスワードを入力します。
Confirm Password	確認のためにパスワードを再度入力します。

6. キャプティブポータルで有効化する SSID を設定します。

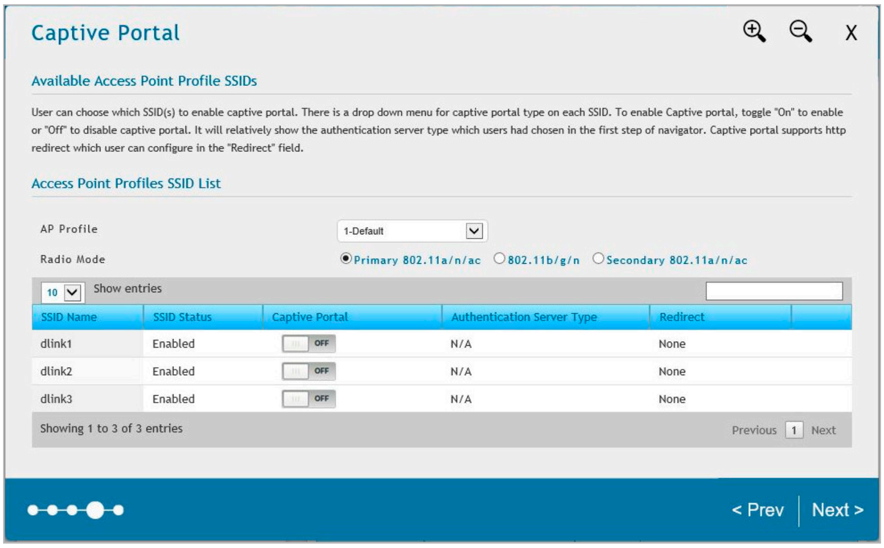


図 3-44　キャプティブポータル設定 - SSID の設定

以下の項目を設定します。

項目	説明
AP Profile	設定する AP プロファイルを選択します。
Radio Mode	設定する無線モードを選択します。
SSID Name	無線ネットワーク名を入力します。大文字と小文字は区別されます。
SSID Status	SSID のステータスを「ON」（有効）または「OFF」（無効）にします。
Captive Portal	キャプティブポータルを「ON」（有効）または「OFF」（無効）にします。
Authentication Server type	キャプティブポータルの認証サーバの種類が表示されます。
Redirect	キャプティブポータルのリダイレクト機能を「ON」（有効）または「OFF」（無効）にします。 「ON」にした場合、リダイレクト URL を入力します。

7. 「Next」をクリックします。

8. 設定した内容が表示されます。「Finish」をクリックすると、設定が保存されます。

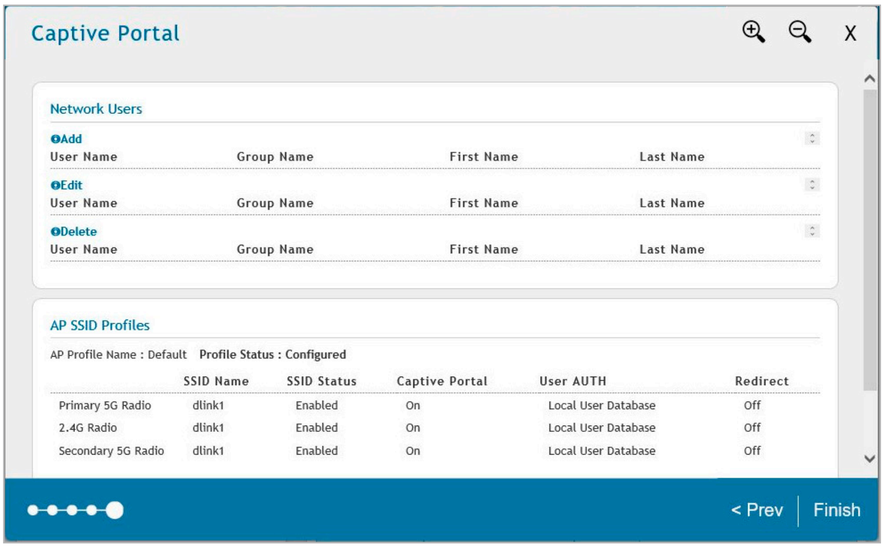


図 3-45　キャプティブポータル設定 - 設定の確認

第 4 章　基本設定

コントローラの基本設定を行うには、以下の手順を実行してください。

基本設定の手順

一般的な基本設定を行うには、以下の手順に従います。

- 手順 1: DHCP サーバの有効化（オプション）
- 手順 2: 国コードの設定
- 手順 3: 管理するアクセスポイントの選択
- 手順 4: SSID の変更とセキュリティの設定
- 手順 5: MAC 認証モードの選択
- 手順 6: 関連付けした AP プロファイルの確認
- 手順 7: キャプティブポータルの設定
- 手順 8: RADIUS サーバを持つ SSID をオーセンティケータとして使用する
- 手順 9: ゲスト管理の設定
- 手順 10: BYOD 環境の設定

手順 1: DHCP サーバの有効化（オプション）

初期値では、無線コントローラの DHCP（Dynamic Host Configuration Protocol）は無効です。スタティックな IP アドレスをアクセスポイントに設定していない場合、DHCP サーバまたは DHCP リレーサーバをネットワークに設定します。必要に応じて以下の手順を実行し、DHCP サーバとして機能するように無線コントローラを設定します。

1. **Network > LAN > LAN Settings > IPv4 LAN Settings** の順にメニューをクリックし、以下の画面を表示します。

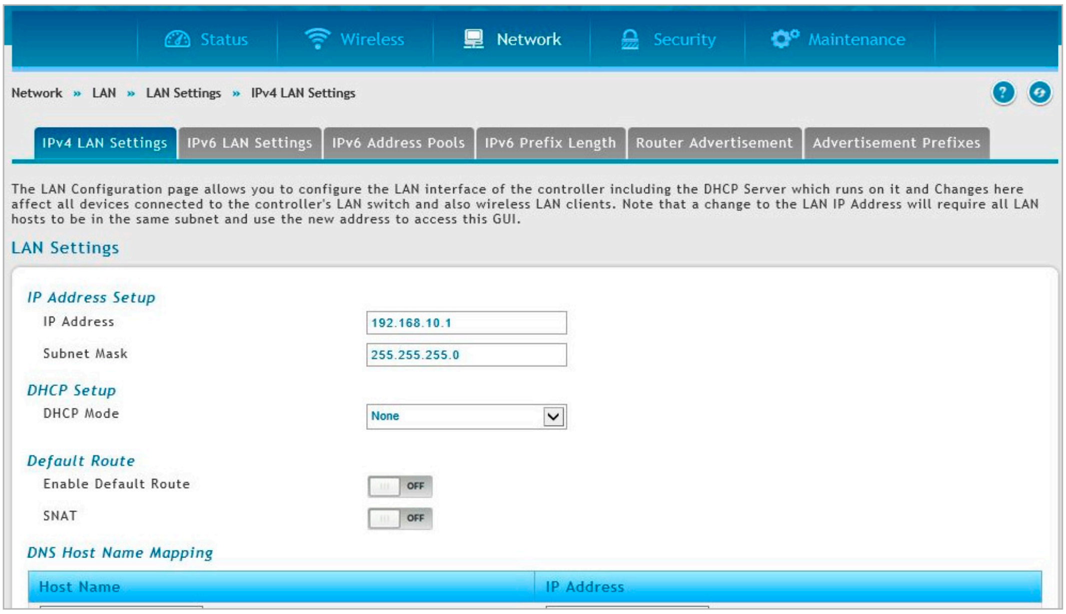


図 4-1　　LAN Settings 画面

2. 「IP Address Setup」セクションで、IP アドレスとサブネットマスクをご使用のネットワークで使用される値に変更します。変更後の値は記録しておいてください。
3. 「Save」ボタンをクリックして、設定を保存します。
4. 一旦 Web GUI 画面の接続が失われます。約 60 秒後に Web GUI が利用可能となりますのでそのままお待ちください。
5. Web ブラウザのアドレスフィールドに、手順 2 で登録した新しい IP アドレスを入力します。
6. **Network > LAN > LAN Settings > IPv4 LAN Settings** の順にメニューをクリックします。

7. 「LAN Settings」ページで、「DHCP Mode」を「DHCP Server」に変更すると、「DHCP Mode」の下に以下の新しいフィールドが表示されます。

項目	説明
Default Gateway	ご使用の LAN のゲートウェイの IP アドレスを入力します。
Domain Name	ドメイン名を入力します。
Lease Time	割り当て IP アドレスのリースタイムを入力します。
Configure DNS / WINS	「ON」にして、DNS または WINS サーバの IP アドレスを入力します。
Primary DNS Server	設定済みの DNS サーバが LAN で利用可能である場合、プライマリ DNS サーバの IP アドレスを入力します。
Secondary DNS Server	設定済みの DNS サーバが LAN で利用可能である場合、セカンダリ DNS サーバの IP アドレスを入力します。
WINS Server	設定済みの WINS サーバが LAN で利用可能である場合、WINS サーバの IP アドレスを入力します。

8. フィールドにデータを入力後、「Save」ボタンをクリックして、設定内容を保存および適用します。

手順 2: 国コードの設定

無線電波を使用するための規定は国によって異なります。以下の手順を使用して、無線ネットワークを使用する国を選択します。

1. **Wireless > General > General** の順にメニューをクリックし、以下の画面を表示します。

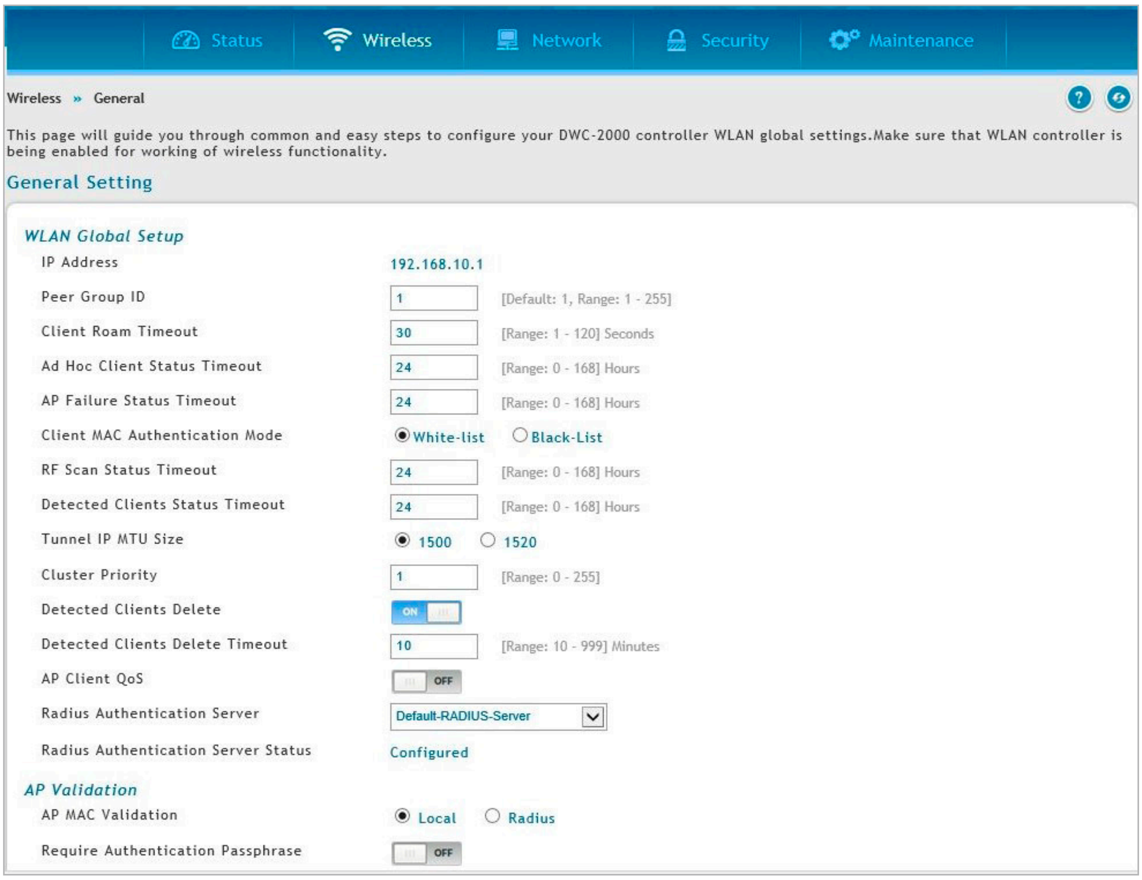


図 4-2　General Setting 画面

2. 「Country Code」のプルダウンメニューから「JP-Japan」を選択します。「Save」ボタンをクリックして、設定内容を保存および適用します。

手順 3: 管理するアクセスポイントの選択

無線コントローラは、同じ IP サブネットにある WLAN 上の管理 / 非管理のアクセスポイントを自動的に検出します。以下の手順に従って、無線コントローラが管理するアクセスポイントを選択します。

1. **Wireless > Access Point > AP List > Not Managed** の順にメニューをクリックし、以下の画面を表示します。

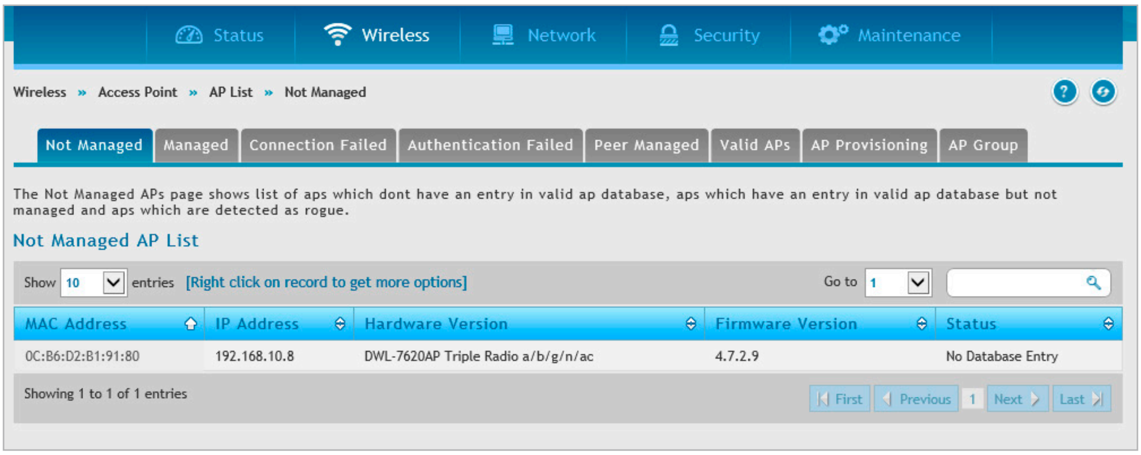


図 4-3　　Not Managed AP List 画面

無線コントローラが検出したアクセスポイントのリストを表示します。

2. 「Not Managed AP List」で、無線コントローラが管理するアクセスポイントを右クリックして、「Manage」を選択します。

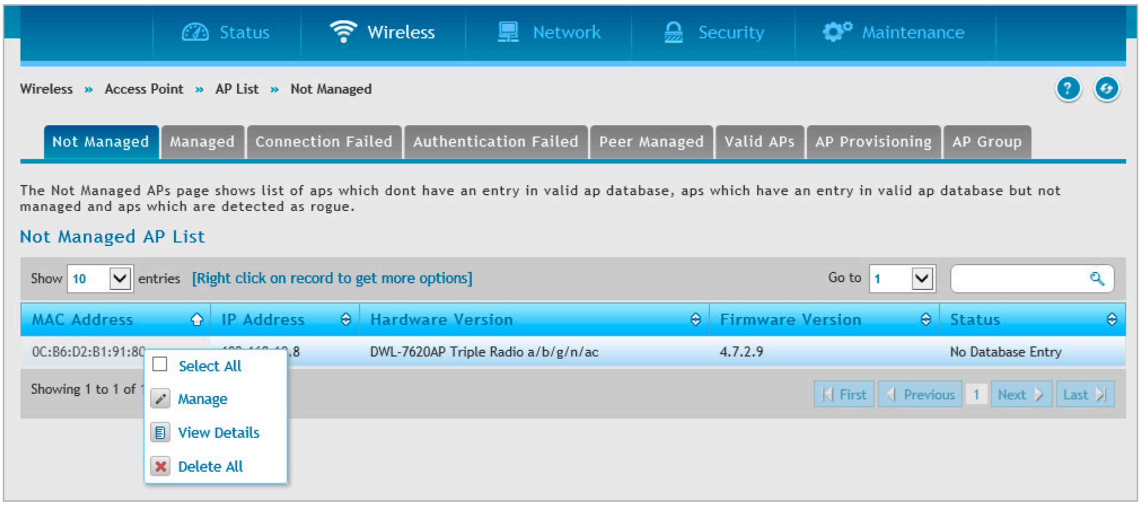


図 4-4　　Not Managed AP List 画面（右クリックメニュー）

以下の画面が表示されます。

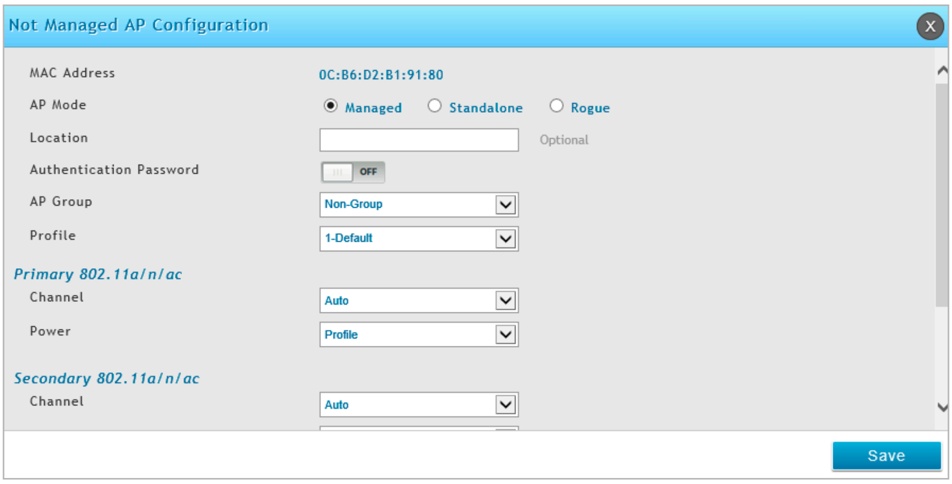


図 4-5　　Not Managed AP Configuration 画面

3. 以下の項目を設定後、「Save」ボタンをクリックして、設定内容を保存および適用します。

項目	説明
MAC Address	アクセスポイントの MAC アドレスが表示されます。
AP Mode	「Standalone」、「Managed」、または「Rogue」を選択します。 • Standalone - アクセスポイントをスタンドアロンモードに設定します。ネットワーク内で個別のアクセスポイントとして動作します。アクセスポイントは、各デバイスの管理インタフェースを使用して管理します。 • Managed - プロファイルが適用され、アクセスポイントはコントローラによって管理されます。アクセスポイント側の WebUI や SNMP サービスは無効になります。 • Rogue - アクセスポイントを Rogue（不正なアクセスポイント）として設定します。
Location	管理するアクセスポイントの位置を入力します。本項目はオプションです。
Expected SSID	「AP Mode」が「Standalone」である場合、アクセスポイントに設定される SSID を指定します。（参照用）
Expected Channel	「AP Mode」が「Standalone」である場合、無線通信に使用されるチャンネルを指定します。（参照用）
Expected WDS Mode	「AP Mode」が「Standalone」である場合、WDS（Wireless Distributed System）を使用時の WDS のモードを指定します。（参照用）
Expected Security Mode	「AP Mode」が「Standalone」である場合、使用するセキュリティモードを指定します。（参照用）
Expected Wired Network Mode	「AP Mode」が「Standalone」である場合、有線ネットワークを許可するかどうかを指定します。（参照用）
Authentication Password	「AP Mode」が「Managed」である場合に、認証用のパスワードを要求するように「ON」（有効）にします。
Profile	「AP Mode」が「Managed」である場合に、アクセスポイントのコンフィグレーションに適用するプロファイルを選択します。
Channel	「AP Mode」が「Managed」である場合、無線インタフェースで稼働するチャンネルを選択します。
Power	「AP Mode」が「Managed」である場合、無線インタフェースに使用する出力のパーセンテージを選択します。

4. 無線コントローラで管理する追加の各アクセスポイントに対し、手順 2 と 3 を繰り返します。

手順 4: SSID の変更とセキュリティの設定

無線コントローラには 50 個の異なるネットワークの設定が可能で、それらを複数の無線帯域および VAP インタフェースに適用できます。初期値では 16 個のネットワークが登録済みで、各無線帯域のアクセスポイントに適用されます。この手順では、事前に設定したネットワークの 1 つを編集して、SSID とセキュリティ設定をご利用のネットワーク要件に合うように変更します。

1. **Wireless > Access Point > AP Profile > AP Profile SSID** の順にメニューをクリックし、以下の画面を表示します。無線コントローラに設定済みの無線ネットワーク一覧が表示されます。

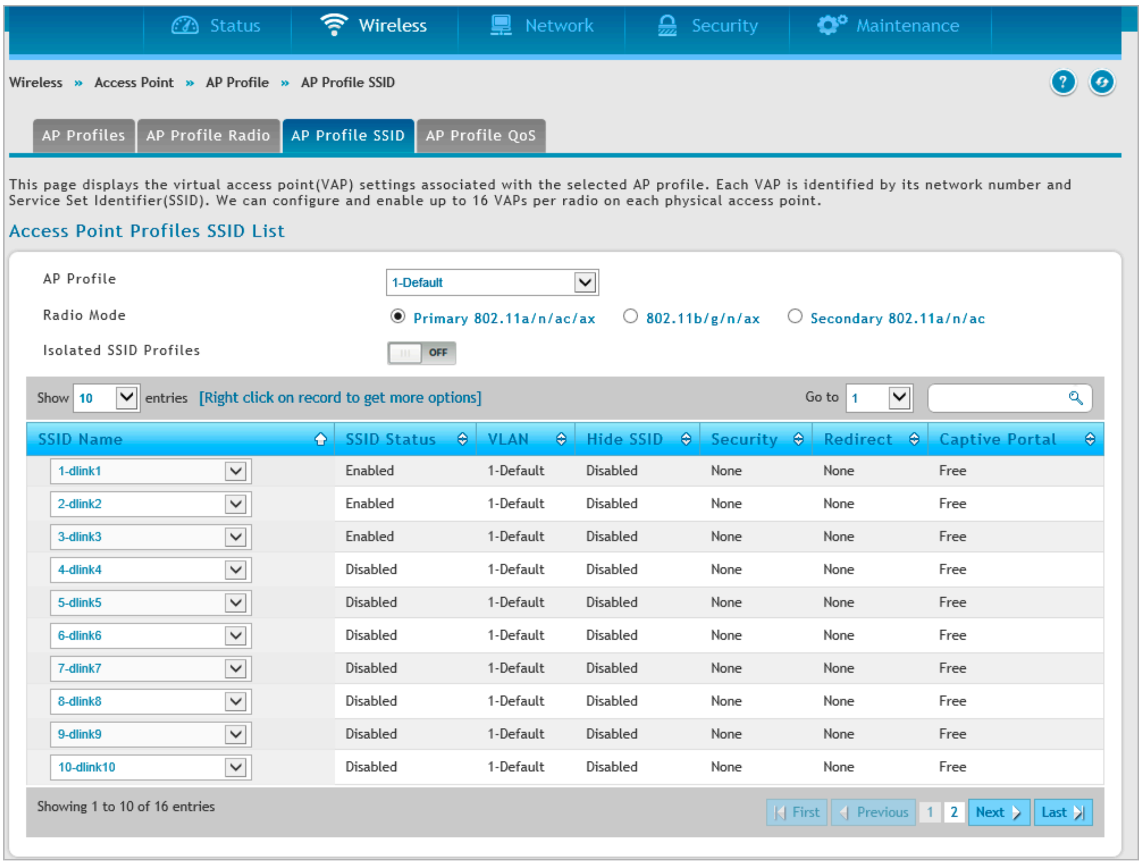


図 4-6　　Access Point Profiles SSID List 画面

2.　編集する SSID の「SSID Status」列で右クリックして「Edit」を選択し、以下の画面を表示します。

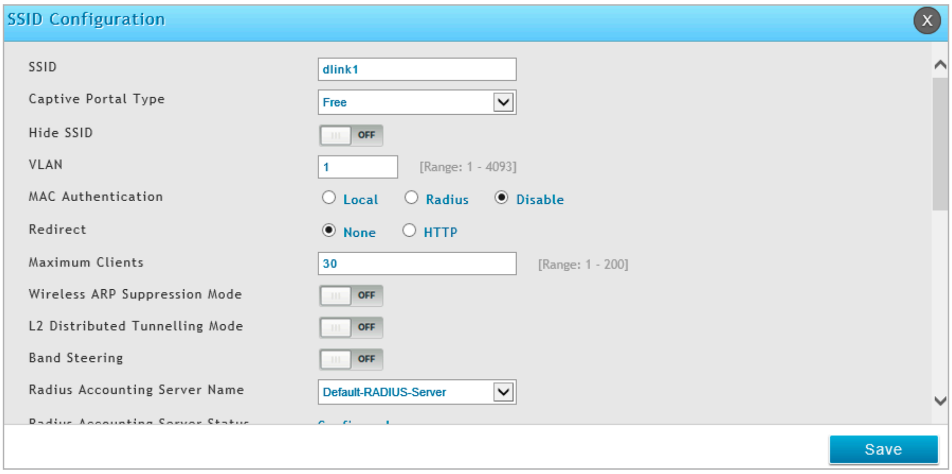


図 4-7　　SSID Configuration 画面

3.　以下の項目を入力します。

項目	説明
SSID	無線ネットワーク名（大文字と小文字の区別あり）を入力します。SSID は、ご使用の無線ネットワーク内のデバイスで同じであることをご確認ください。
VLAN	VLAN ID を入力します。この VLAN ID が VLAN 設定で作成済みであることをご確認ください。（**Network > VLAN > VLAN Setting** メニュー参照）
Security	デフォルトの AP プロファイルでは、セキュリティメカニズムを使用していません。ご使用のネットワークを保護するためには、セキュリティメカニズムを選択し、未認証の無線クライアントがネットワークにアクセスすることを防止することをお勧めします。 • None - セキュリティメカニズムを使用しません。 • OWE - OWE(Opportunistic Wireless Encryption) セキュリティを有効にします。 • WEP - WEP セキュリティを有効にします。「WEP の設定オプション」の項目を入力します。 • WPA/WPA2 - WPA/WPA2 セキュリティを有効にします。「WPA/WPA2 設定オプション」の項目を入力します。 • WPA2/WPA3 - WPA2/WPA3 セキュリティを有効にします。「WPA2/WPA3 設定オプション」の項目を入力します。

■ SSID 設定（WEP）

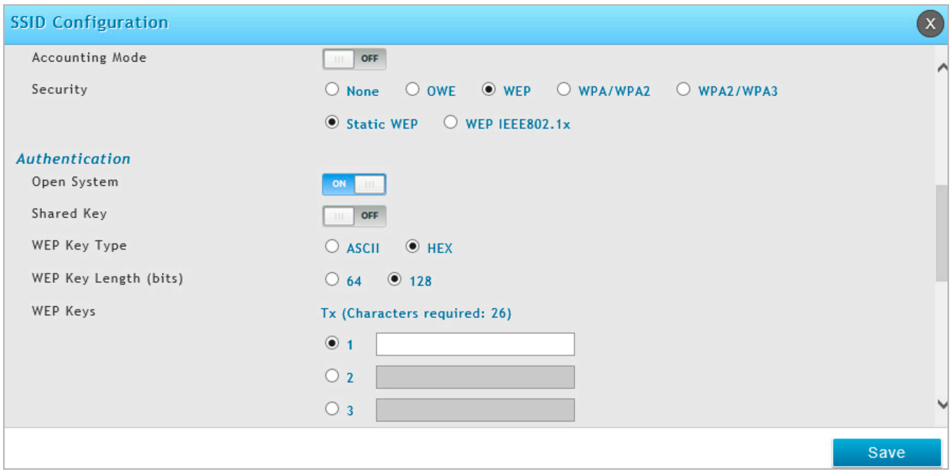


図 4-8　　SSID Configuration 画面（WEP）

WEP の設定オプション

項目	説明
Security	• Static WEP - スタティックなキー管理を使用します。無線クライアントとアクセスポイントの両方に、手動でデータ暗号化用の同一キーを設定します。ダイナミック WEP（IEEE 802.1X）では、クライアントからアクセスポイントへのトラフィックを暗号化するために動的に生成されたキーを使用します。 • WEP IEEE 802.1x - 設定が必要なフィールドはありません。アクセスポイントは、グローバル RADIUS サーバ、または無線ネットワークに指定した RADIUS サーバを使用します。
Authentication	認証タイプを選択します。 • Open System - 全ての無線ステーションが認証を要求できます。別の無線ステーションで認証する必要があるステーションは、送信ステーションの ID を含む認証管理フレームを送信します。受信するステーションは、送信ステーションと認識するか否かを示すフレームを返します。 • Shared Key - 各無線ステーションは、802.11 無線ネットワークの通信チャンネルから独立している安全なチャンネルで共有秘密キーを受信しているものと見なされます。
WEP Key Type	キータイプを選択します。 • ASCII - アルファベットの大文字、小文字、数字、および @# などの記号を含みます。 • HEX - 数字（0~9）と文字（A~F）を含みます。
WEP Key Length (bits)	WEP キーの長さを選択します。 • 64 - 64 ビット • 128 - 128 ビット
WEP Keys	送信キーインデックス（1-4）を指定します。アクセスポイントがどの WEP キーを送信するデータの暗号化に使用するかを示します。送信キーを選択するためには、キーを入力するフィールドのキー番号のラジオボタンをクリックします。続いて、WEP キーを入力します。
WEP キーの入力	4 つの WEP キーを指定できます。各テキストボックスでは、アクセスポイントを使用するステーションと共有する各 RC4 WEP キーに、文字列を入力します。各キーには同じ文字数を使用します。入力するキーの文字数は「WEP Key Type」と「WEP Key Length」の選択によって異なります。フィールドに入力するキーの文字数は以下の通りです。 • 64 bit - ASCII : 5 文字、Hex : 10 文字 • 128 bit - ASCII : 13 文字、Hex : 26 文字 各クライアントは、ここで指定したのと同じスロットに、これらの WEP キーのいずれかを使用するように設定します。

■ SSID 設定（WPA/WPA2）

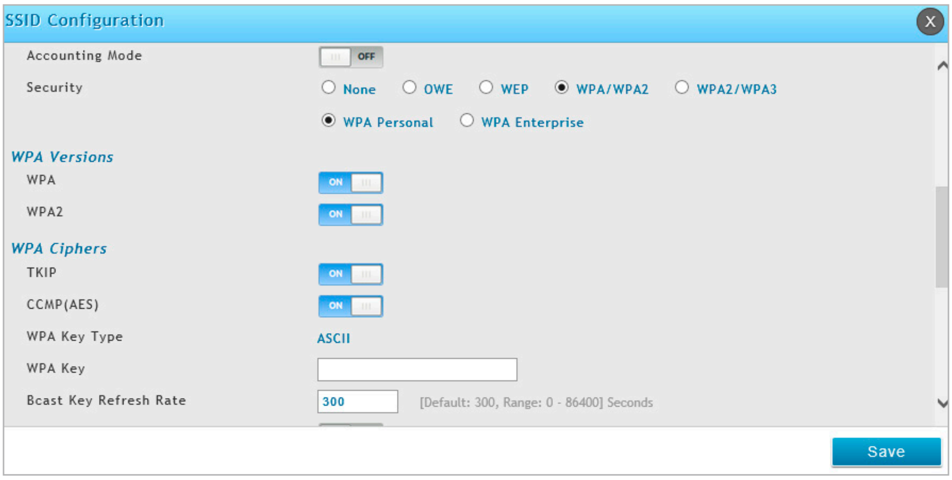


図 4-9　　SSID Configuration 画面（WPA/WPA2）

WPA/WPA2 設定オプション

項目	説明
Security	「Security」に「WPA/WPA2」を選択すると、以下の 2 つの追加セキュリティオプションが表示されます。 • WPA Personal - スタティックキー管理を使用します。無線クライアントとアクセスポイントの両方にデータを暗号化するための同じキーを手動で設定します。 • WPA Enterprise - WPA エンタープライズでは RADIUS サーバを使用し、ダイナミックにキーを生成してクライアントからアクセスポイントへのトラフィックを暗号化します。WPA パーソナルより安全性が高いですが、キーの管理に RADIUS サーバを必要とします。本オプションをクリックすると、画面は更新され、「WPA Key Type」と「WPA Key」のフィールドは非表示になります。アクセスポイントは、グローバル RADIUS サーバ、または無線ネットワークに指定した RADIUS サーバを使用します。
WPA Versions	サポートするクライアントステーションの WPA のタイプを選択します。 • WPA - ネットワーク上のすべてのクライアントステーションが WPA をサポートし、WPA2 をサポートしていない場合に選択します。 • WPA2 - ネットワーク上のすべてのクライアントステーションが WPA2 をサポートしている場合は、IEEE 802.11i 標準でより高いセキュリティを提供する WPA2 を使用します。 • WPA および WPA2 - WPA2 または WPA をサポートするクライアントが混在する場合には、両方のボックスを選択します。サポートする方式に関わらずクライアント間の接続および認証が可能となり、WPA2 サポートのクライアントに対しては、より堅牢なセキュリティを提供する WPA2 を使用します。本設定では相互運用性を実現する代わりに、セキュリティが若干低下します。
WPA Ciphers	使用する暗号化方式を選択します。 • TKIP • CCMP (AES) • TKIP と CCMP (AES) TKIP と AES サポートのクライアントのいずれもアクセスポイントへの接続が可能です。WPA クライアントは、アクセスポイントに接続するために、有効な TKIP キーまたは AES-CCMP キーを持つ必要があります。802.11n クライアントは TKIP 暗号を使用できません。TKIP だけを有効にすると、802.11 のクライアントはネットワークで認証されません。
WPA Key Type	WPA キータイプとして「ASCII」が設定されます。
WPA Key	WPA パーソナル用の共有秘密キー（8-62 文字）を入力します。アルファベットの大文字、小文字、数字、および @# などの記号を含みます。
Pre-Authentication	「Security」が「WPA Enterprise」の場合、本項目を「ON」にすると事前認証が有効になります。
Pre-Authentication Limit	アクセスポイントが同時に扱う事前認証数（0-192）を入力します。「Security」が「WPA Enterprise」の場合、本フィールドが表示されます。
Key Caching Hold Time	「Security」が「WPA Enterprise」の場合、アクセスポイントが PMK を保持している時間（1-1440 分）を入力します。この設定は、RADIUS サーバが生成し、事前認証からアクセスポイントに送信される PMK に適用されます。RADIUS サーバが特定のユーザ用の Session-Timeout 属性に、より長い時間を返してきた場合、この時間の制限は、RADIUS サーバに書き換えられることにご注意ください。値を設定しない場合、無線クライアントがローミングする場合を想定して、アクセスポイントは無線クライアントの PMK を他のアクセスポイントに送信しません。
Bcast Key Refresh Rate	この VAP に接続するクライアントが使用するブロードキャスト（グループ）キーの更新間隔時間（0- 86400 秒）を入力し 0 はブロードキャストキーを更新しません。
Session Key Refresh Rate	「Security」が「WPA Enterprise」の場合、VAP に接続する各クライアント用のセッション（ユニキャスト）キーを更新する間隔（0-86400 秒）を入力します。0 はブロードキャストキーが更新されないことを示します。

■ SSID 設定（WPA2/WPA3）

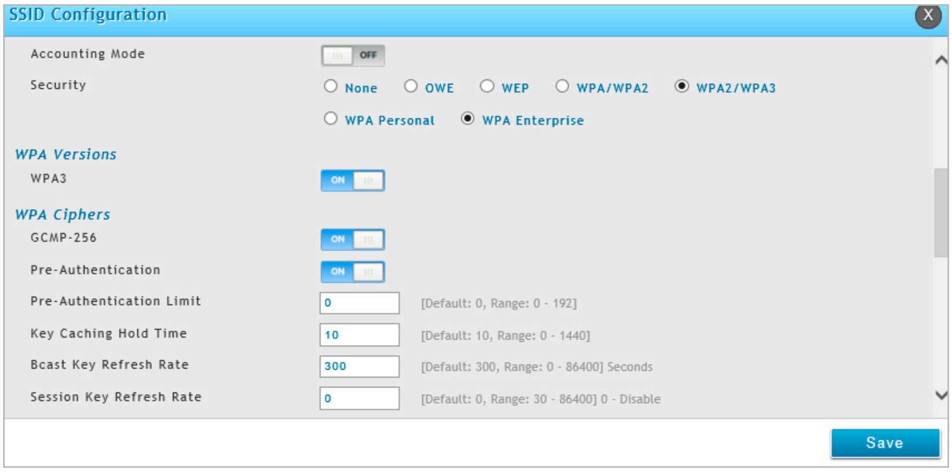


図 4-10　SSID Configuration 画面（WPA2/WPA3）

注意　GCMP-256 を解除できないため、WPA2 Enterprise と WPA3 Enterprise の混在環境では SSID を分ける必要があります。

WPA2/WPA3 設定オプション

項目	説明
Security	「Security」に「WPA2/WPA3」を選択すると、以下の 2 つの追加セキュリティオプションが表示されます。 • WPA Personal - スタティックキー管理を使用します。無線クライアントとアクセスポイントの両方にデータを暗号化するための同じキーを手動で設定します。 • WPA Enterprise - WPA エンタープライズでは RADIUS サーバを使用し、ダイナミックにキーを生成してクライアントからアクセスポイントへのトラフィックを暗号化します。WPA パーソナルより安全性が高いですが、キーの管理に RADIUS サーバを必要とします。本オプションをクリックすると、画面は更新され、「WPA Key Type」と「WPA Key」のフィールドは非表示になります。アクセスポイントは、グローバル RADIUS サーバ、または無線ネットワークに指定した RADIUS サーバを使用します。WPA3 Enterprise を選択した場合、WPA バージョンは WPA3 のみ設定可能です。
WPA Versions	サポートするクライアントステーションの WPA のタイプを選択します。「Security」の項目で「WPA Enterprise」を選択した場合は、「WPA3」のみ選択可能です。 • WPA2 - ネットワーク上のすべてのクライアントステーションが WPA2 をサポートしている場合は、IEEE 802.11i 標準で高いセキュリティを提供する WPA2 を使用します。 • WPA3 - ネットワーク上のすべてのクライアントステーションが WPA3 をサポートしている場合は、IEEE 802.11i 標準でより高いセキュリティを提供する WPA3 を使用します。 • WPA 2 および WPA3 - WPA2 または WPA3 をサポートするクライアントが混在する場合には、両方のボックスを選択します。サポートする方式に関わらずクライアント間の接続および認証が可能となり、WPA3 サポートのクライアントに対しては、より堅牢なセキュリティを提供する WPA3 を使用します。本設定では相互運用性を実現する代わりに、セキュリティが若干低下します。
WPA Ciphers	使用する暗号化方式を選択します。 • TKIP　• TKIP と CCMP (AES)　• CCMP (AES)　• GCMP-256 TKIP と AES サポートのクライアントのいずれもアクセスポイントへの接続が可能です。WPA クライアントは、アクセスポイントに接続するために、有効な TKIP キー、AES-CCMP キー、GCMP256 キーのいずれかを持つ必要があります。802.11n クライアントは TKIP 暗号を使用できません。TKIP だけを有効にすると、802.11 のクライアントはネットワークで認証されません。 WPA3 クライアントの場合、暗号は GCMP256 である必要があります。WPA2 クライアントの場合、GCMP256 は不要です。
WPA Key Type	WPA キータイプとして「ASCII」が設定されます。
WPA Key	WPA パーソナル用の共有秘密キー（8-62 文字）を入力します。アルファベットの大文字、小文字、数字、および @# などの記号を含みます。
WPA3 Key	WPA3 パーソナル用の共有秘密キー（8-62 文字）を入力します。アルファベットの大文字、小文字、数字、および @# などの記号を含みます。WPA Key と同じキーを使用する場合は「Same as WPA Key」にチェックをいれます。
Pre-Authentication	「Security」が「WPA Enterprise」の場合、本項目を「ON」にすると事前認証が有効になります。
Pre-Authentication Limit	アクセスポイントが同時に扱う事前認証数（0-192）を入力します。「Security」が「WPA Enterprise」の場合、本フィールドが表示されます。
Key Caching Hold Time	「Security」が「WPA Enterprise」の場合、アクセスポイントが PMK を保持している時間（1-1440 分）を入力します。この設定は、RADIUS サーバが生成し、事前認証からアクセスポイントに送信される PMK に適用されます。RADIUS サーバが特定のユーザ用の Session-Timeout 属性に、より長い時間を返してきた場合、この時間の制限は、RADIUS サーバに書き換えられることにご注意ください。値を設定しない場合、無線クライアントがローミングする場合を想定して、アクセスポイントは無線クライアントの PMK を他のアクセスポイントに送信しません。

項目	説明
Bcast Key Refresh Rate	この VAP に接続するクライアントが使用するブロードキャスト（グループ）キーの更新間隔時間（0- 86400 秒）を入力し 0 はブロードキャストキーを更新しません。
Session Key Refresh Rate	「Security」が「WPA Enterprise」の場合、VAP に接続する各クライアント用のセッション（ユニキャスト）キーを更新する間隔（0-86400 秒）を入力します。0 はブロードキャストキーが更新されないことを示します。

4. 新しく SSID を追加するには、**Wireless > Access Point > AP Profile > AP Profile SSID** の順にメニューをクリックし、以下の画面を表示します。

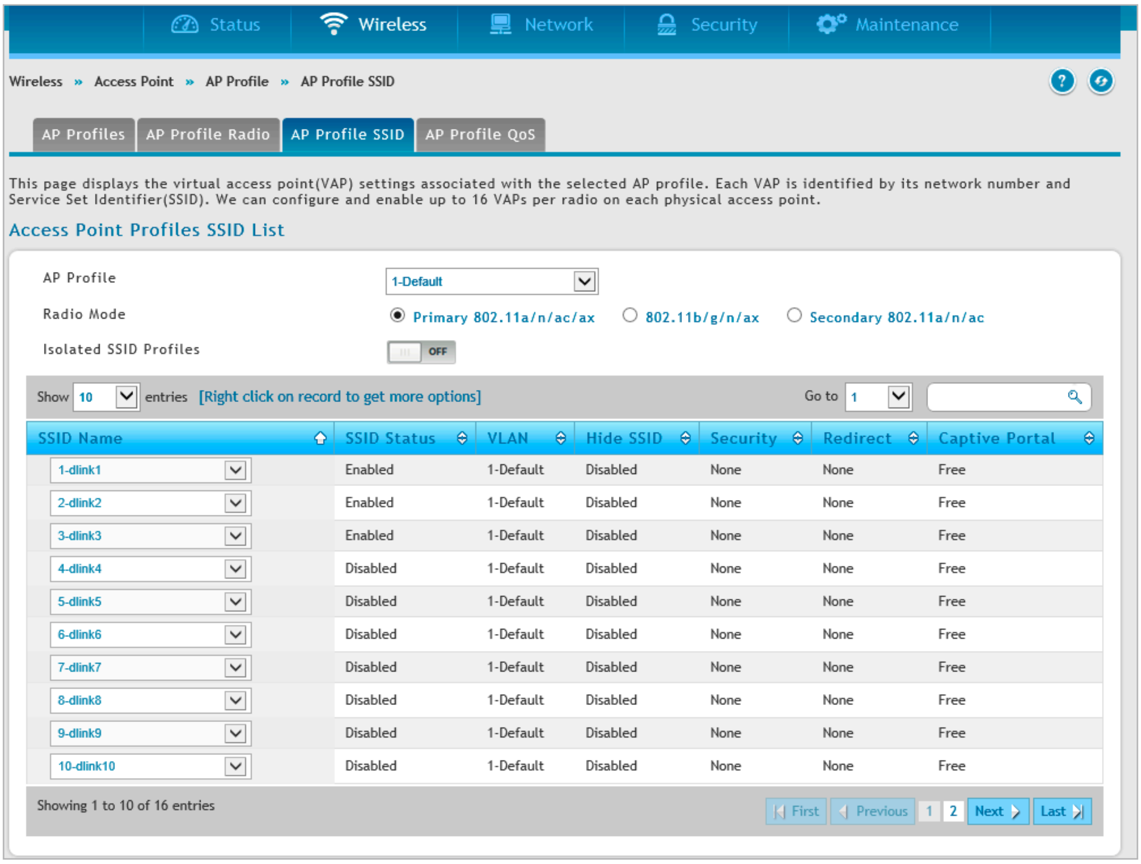


図 4-11　Access Point Profiles SSID List 画面

5. 「Add New SSID Profile」ボタンをクリックして、以下の画面を表示します。

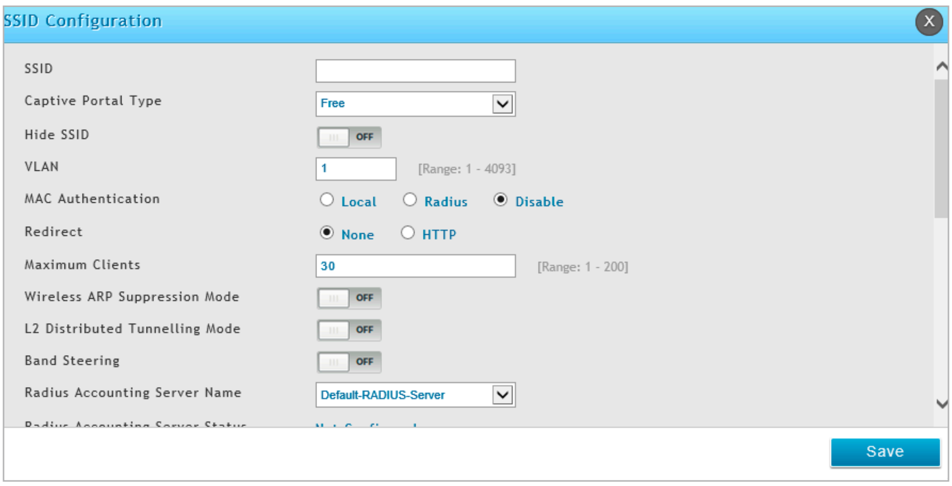


図 4-12　SSID Configuration 画面

6. フィールドを入力後、「Save」ボタンをクリックし、設定内容を保存します。

7. 以下の画面に戻ります。

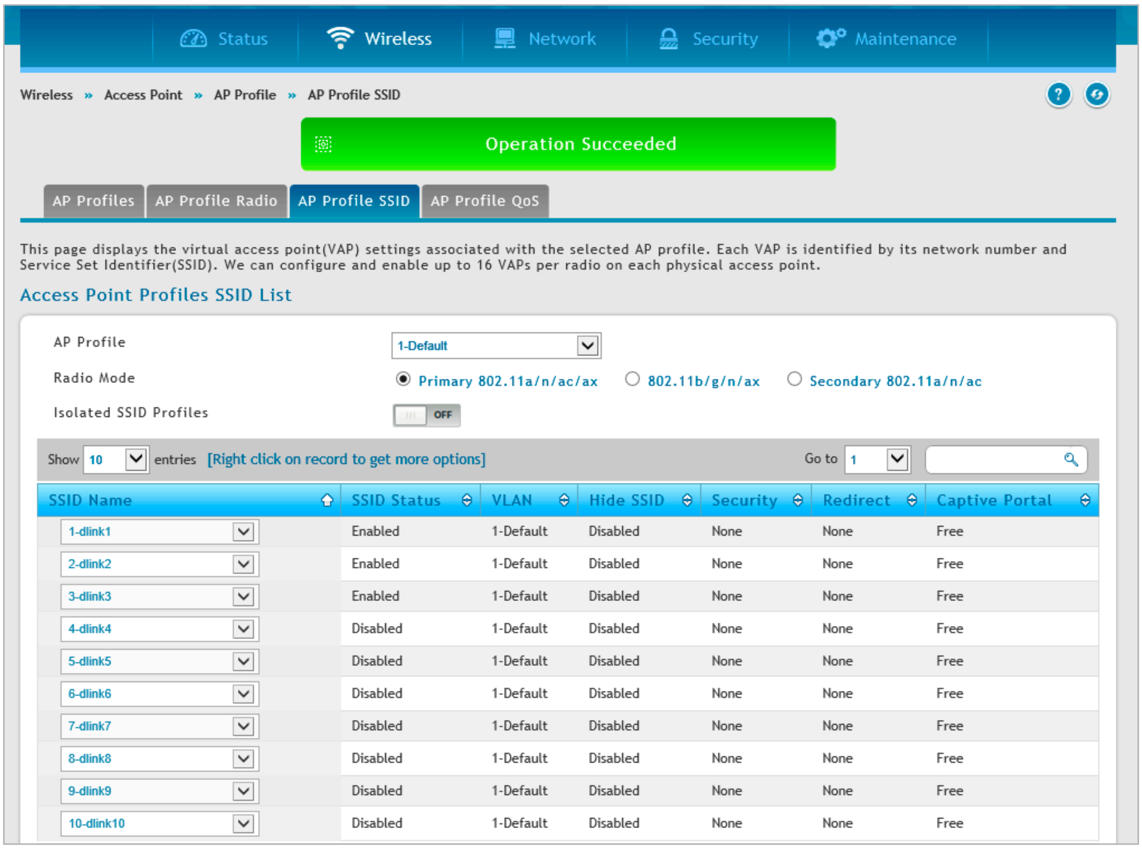


図 4-13　Access Point Profiles SSID List 画面

8. 「AP Profile」のプルダウンメニューから編集する項目を選択します。

9. 「Radio Mode」で、設定する無線帯域のラジオボタンをクリックします。

10. 「SSID Name」プルダウンメニューから無線インタフェースに設定する SSID を選択するか、または、有効にする SSID ネットワークを右クリックして、「Enable」をクリックします。

注意　SSID ID1 は常に有効です。初期値の 1 番目の SSID を無効化するには、新しい SSID を作成して最初のスロットに置き換えます。

手順 5: MAC 認証モードの選択

MAC 認証では特定の MAC アドレスを持つクライアントへのアクセスを許可または拒否することが可能であり、「Open」モードで動作するネットワークにおいて有用です。また、802.1X セキュリティ方式と一緒に使用することができます。その場合、802.1X 認証より先に MAC 認証が実行されます。MAC 認証が有効となるには、無線クライアントがネットワークに接続するためにまず統合アクセスポイント（UAP）により認証を受ける必要があります。

無線コントローラは、以下に示す 2 つの MAC 認証モード（ホワイトリストまたはブラックリスト）を提供します。

- White-list:

  「MAC Authentication」データベースまたは RADIUS サーバに登録されている MAC アドレスを持つ無線クライアントへのアクセスを許可します。データベースに MAC アドレスが存在しない場合、クライアントに対してアクセスが拒否されます。

- Black-list:

  「MAC Authentication」データベースまたは RADIUS サーバに登録されている MAC アドレスを持つ無線クライアントへのアクセスを拒否します。データベースに MAC アドレスが存在しない場合、クライアントに対してアクセスが許可されます。

1. **Wireless > General > General** の順にメニューをクリックし、以下の画面を表示します。

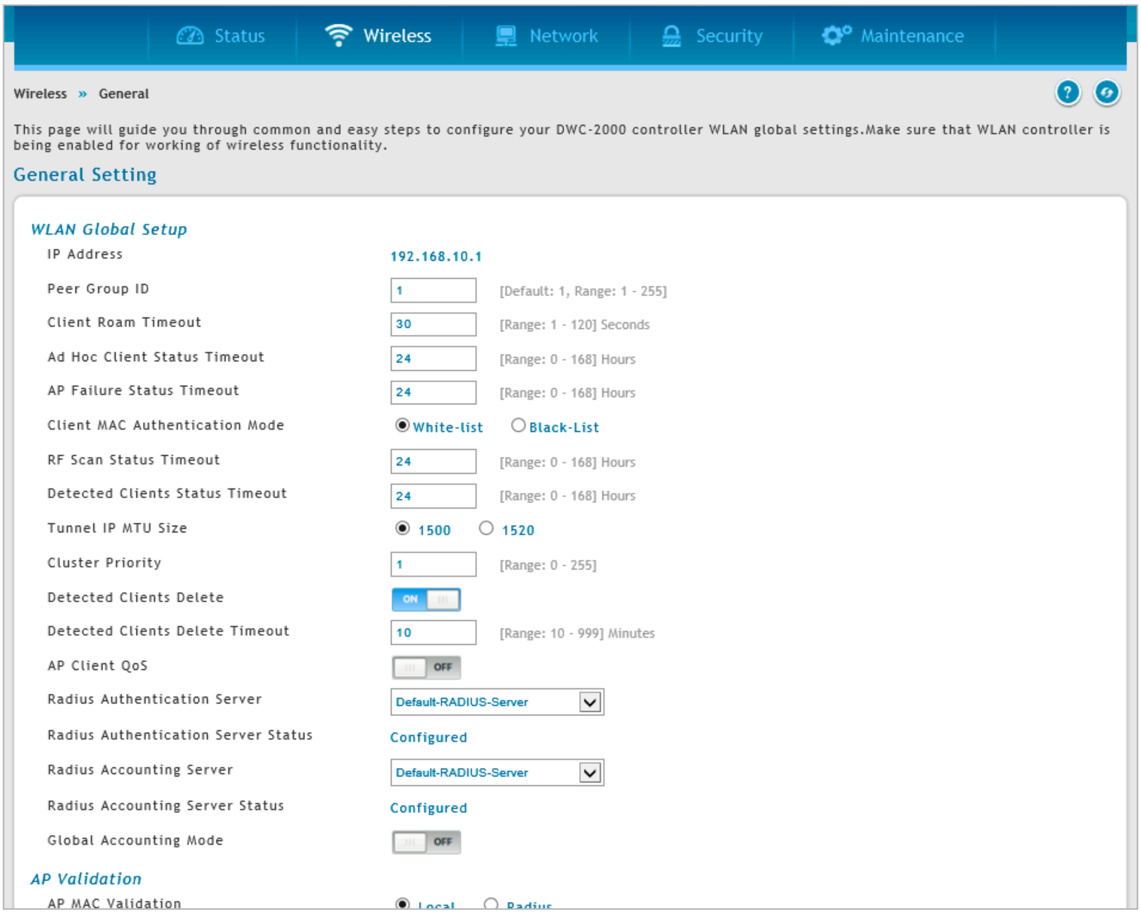


図 4-14　General Setting 画面

2. 「Client MAC Authentication Mode」で、「White-list」または「Black-List」を選択します。

3. 「Save」ボタンをクリックして、設定内容を保存および適用します。

4.　**Security > Authentication > User Database > MAC Authentication** の順にメニューをクリックし、以下の画面を表示します。

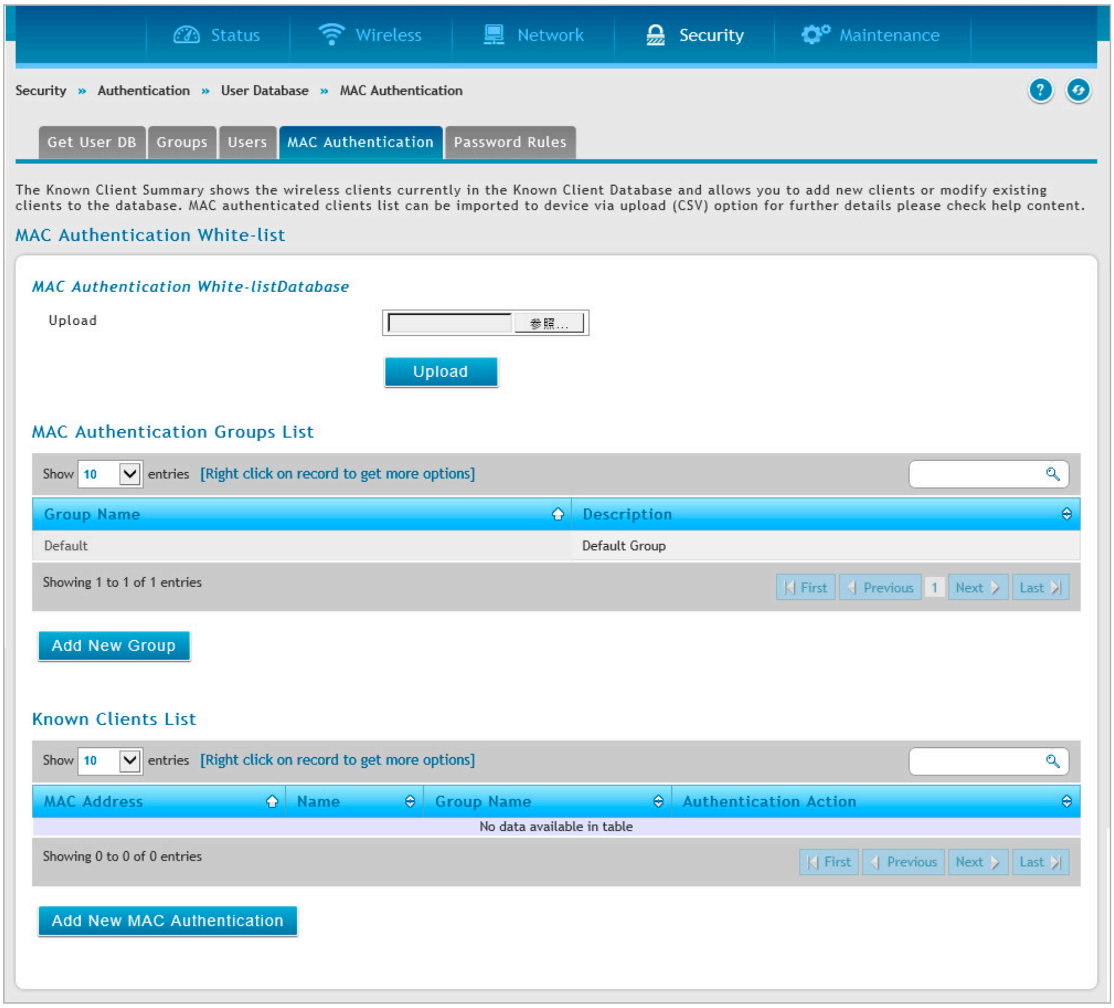


図 4-15　MAC Authentication White-List 画面

手順 2 で選択したリストタイプ（「White-list」または「Black-List」）に従って画面が表示されます。

5.　「Add New MAC Authentication」ボタンをクリックし、以下の画面を表示します。

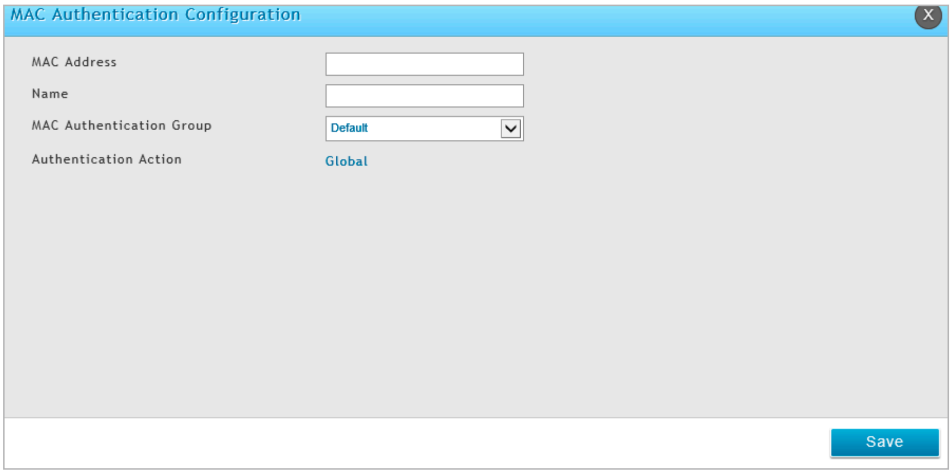


図 4-16　MAC Authentication Configuration 画面

クライアントの MAC アドレスと名前を入力し、「MAC Authentication Group」を選択します。
「Save」ボタンをクリックして設定を保存します。

6.　**Wireless > Access Point > AP Profile > AP Profile SSID** の順にメニューをクリックします。

7. エントリを右クリックして、「Edit」を選択すると、以下の画面が表示されます。

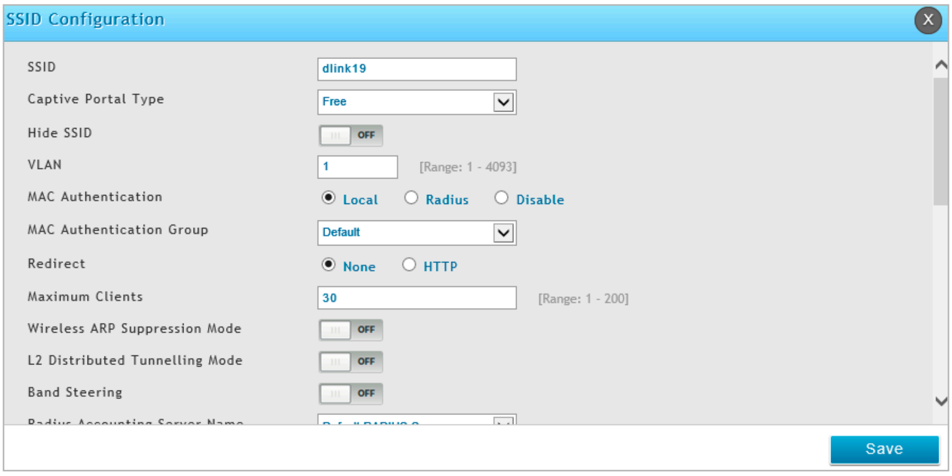


図 4-17　SSID Configuration 画面

「Local」を選択し、「Save」ボタンをクリックします。

手順 6: 関連付けした AP プロファイルの確認

以下の手順で、AP プロファイルが無線コントローラに関連付けられていること確認します。

注意　コンフィグレーション設定を変更するたびに、本手順を実行して、変更をアクセスポイントに適用してください。

1. **Wireless > Access Point > AP Profile** の順にメニューをクリックし、以下の画面を表示します。

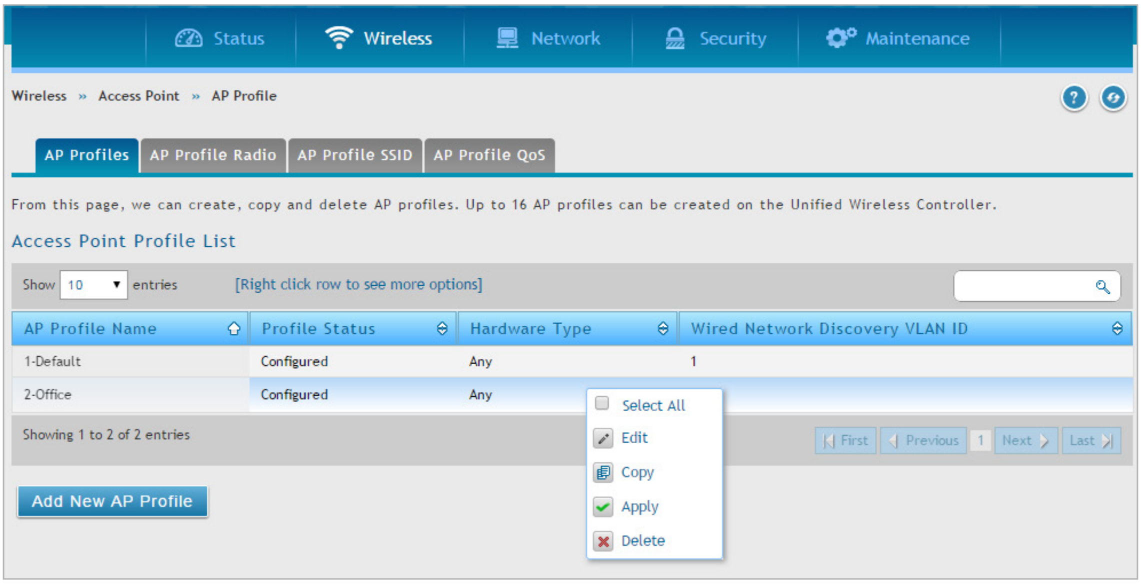


図 4-18　Access Point Profile List 画面

2. 「Access Point Profile List」で、更新する AP プロファイルを右クリックし、「Apply」を選択します。

3. 約 30 秒後、リフレッシュアイコン をクリックして、プロファイルが関連付けされたことを確認します。関連付けされたアクセスポイントは、設定済みで、無線ユーザを認証する準備ができています。

手順 7: キャプティブポータルの設定

無線コントローラに対し、ローカルデータベースを使用するキャプティブポータルの設定を行うには、以下の 4 つの手順を実行します。

1.　キャプティブポータルグループを作成する

a. Security > Authentication > User Database > Groups の順にメニューをクリックし、以下の画面を表示します。

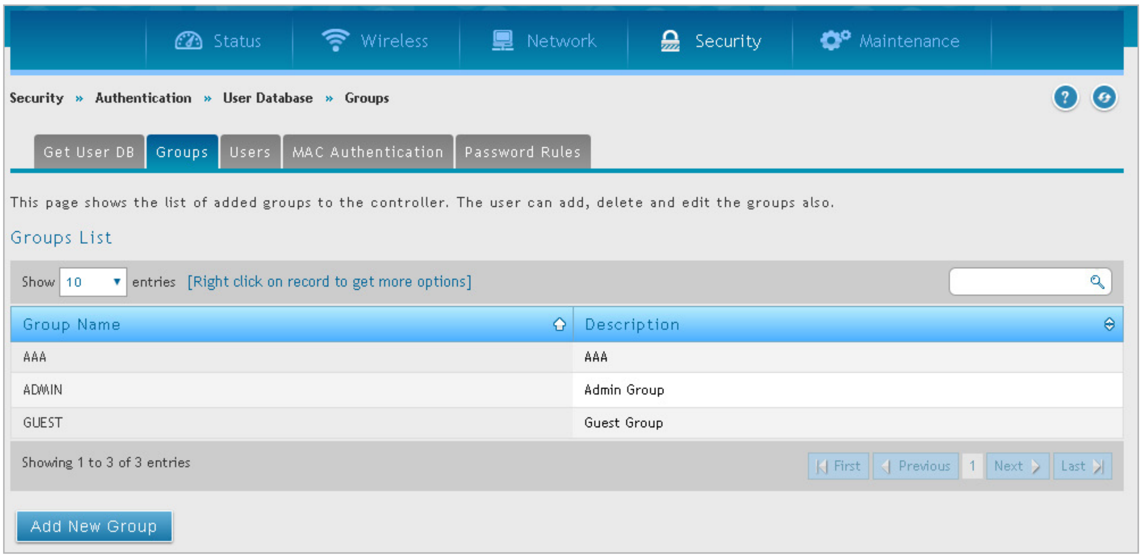


図 4-19　 Groups List 画面

b.「Add New Group」ボタンをクリックして、以下の画面を表示します。

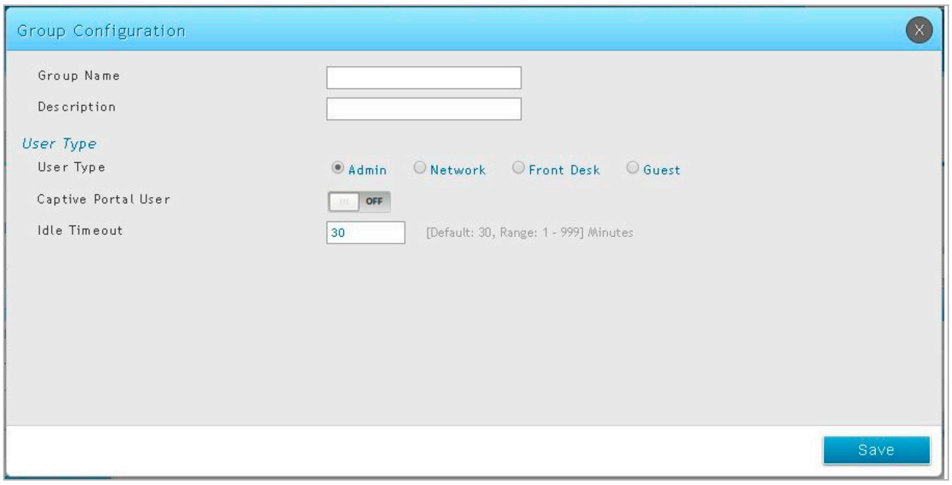


図 4-20　 Group Configuration 画面

以下の項目があります。

項目	説明
Group Name	グループ名を入力します。
Description	グループの説明を入力します。
User Type	
Captive Portal User	本オプションを有効または無効にします。

c. フィールドにデータを入力し、「Save」ボタンをクリックして、設定を保存します。

2.　キャプティブポータルユーザを追加する

a. Security > Authentication > User Database > Users の順にメニューをクリックし、以下の画面を表示します。

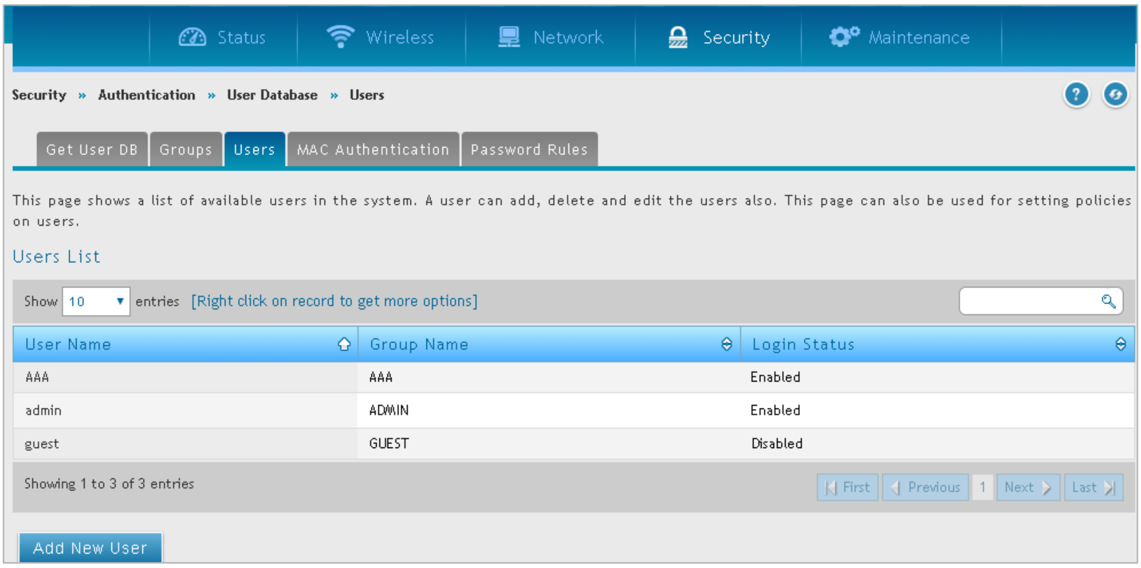


図 4-21　　Users List 画面

b.「Add New User」ボタンをクリックし、以下の画面を表示します。

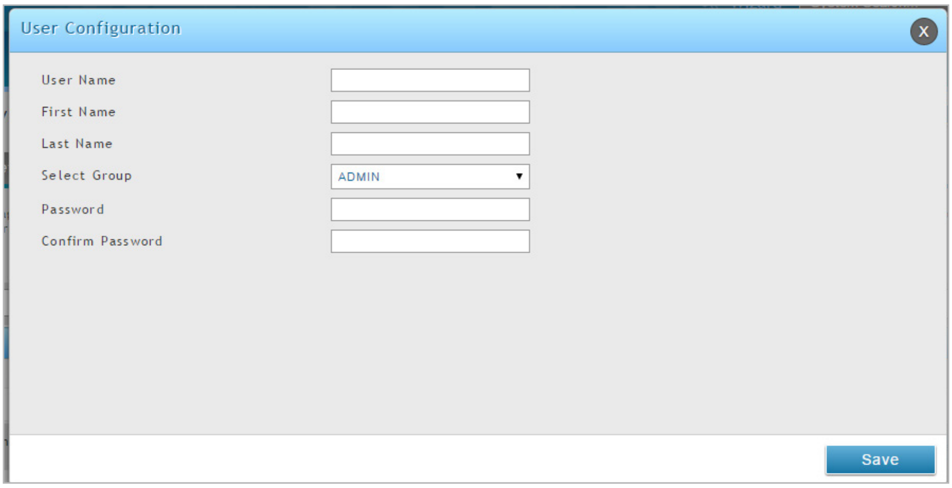


図 4-22　　User Configuration 画面

以下の項目があります。

項目	説明
User Name	ユーザの固有の名称を入力します。名前は、追加する可能性のある他のユーザとこのユーザを簡単に識別できるようにする必要があります。
First Name	ユーザの名前を入力します。これは、認証ドメインが RADIUS などの外部サーバである場合に役立ちます。
Last Name	ユーザの名字を入力します。これは、認証ドメインが RADIUS などの外部サーバである場合に役立ちます。
Select Group	ユーザが所属するキャプティブポータルグループを選択します。
Enable Password Change	本項目は「Select Group」で Captive Portal グループを選択した場合にのみ表示されます。「ON」を選択すると、ユーザがパスワードの変更を行うことができるようになります。
MultiLogin	本項目は「Select Group」で Captive Portal グループを選択した場合にのみ表示されます。「ON」を選択すると、ユーザが同一のユーザ名 / パスワードを使用して、複数のデバイスから同時にログインすることができます。
Password	インターネットへのアクセス権を得る前に、ユーザが指定すべきパスワード（大文字、小文字区別あり）を入力します。セキュリティのために、各入力したパスワード文字は、ドット「.」でマスクされます。
Confirm Password	確認のために「Password」フィールドに入力したものと同じパスワード（大文字､小文字区別あり）を入力します。セキュリティのために、各入力したパスワード文字は、ドット「.」でマスクされます。

c. フィールドにデータを入力し、「Save」ボタンをクリックします。

3.　キャプティブポータルグループに SSID プロファイルを関連付ける

a. **Wireless > Access Point > AP Profile > AP Profile SSID** の順にメニューをクリックし、以下の画面を表示します。

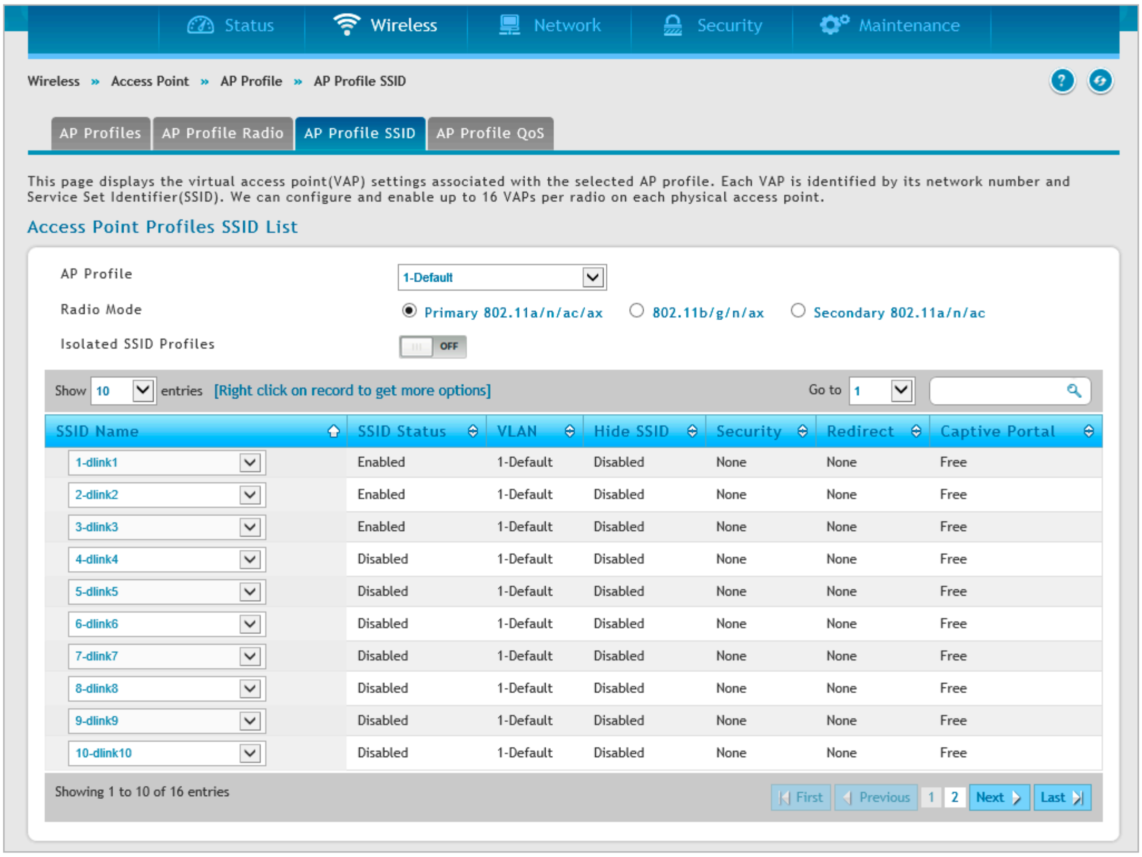


図 4-23　Access Point Profiles SSID List 画面

b.「SSID Status」で、キャプティブポータル機能を使用する SSID を右クリック →「Edit」を選択し、以下の画面を表示します。

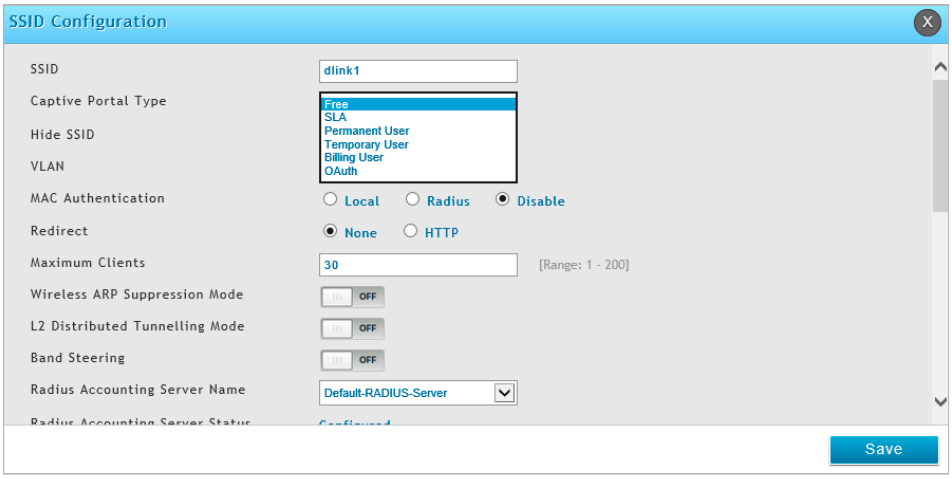


図 4-24　SSID Configuration 画面

c.「Captive Portal Type」横のプルダウンメニューからユーザタイプを選択します。

- 「Free」- キャプティブポータルを経由した即時のアクセスが許可されます。
- 「SLA」- エンドユーザは、アクセスを許可される前にサービスレベルの同意が必要となります。
- 「Permanent User」- ローカルユーザのデータベース、RADIUS、LDAP、または POP3 などの認証方式の選択が可能となります。
- 「Temporary User」または「Billing User」- 認証方式を選択します。
- 「OAuth」- Facebook、Google などのアカウントによるログインを行います。

ここでは、ローカルデータベースのユーザアカウントがパーマネントユーザのアカウントとします。
「Captive Portal Type」で「Permanent User」を選択し、「Authentication Server」で「Local User Database」を選択します。

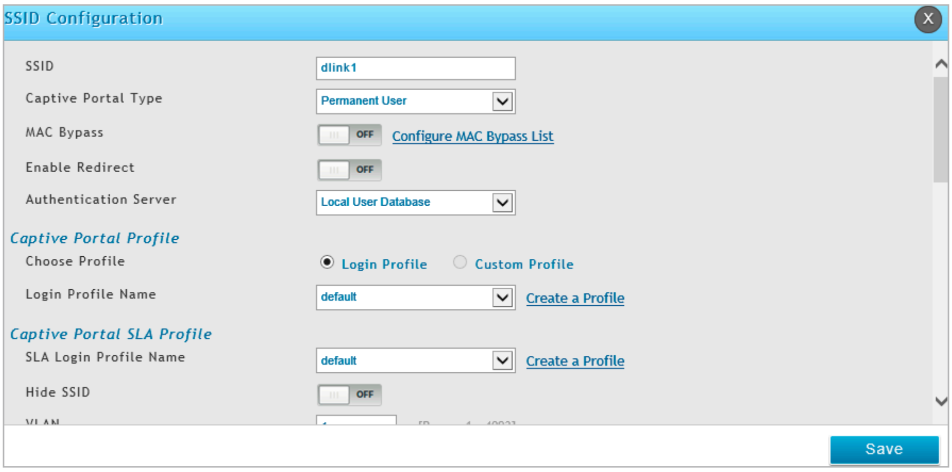


図 4-25　SSID Configuration 画面

d.「Login Profile Name」プルダウンメニューから、カスタマイズしたログインページを選択します。

e.「Save」ボタンをクリックします。

キャプティブポータルは選択した SSID と関連付けられます。クライアントから設定をテストする場合、キャプティブポータルにログインするために、キャプティブポータル SSID に接続してください。キャプティブポータルネットワークで IP アドレスを入力すると、コントローラによってキャプティブポータルページへリダイレクトされます。

認証データベースとして RADIUS サーバを使用している場合、上の手順 c では、「Captive Portal Type」に「Permanent User」を選択し、「Authentication Server」に「RADIUS Server」を選択します。

4.　キャプティブポータルのログインページのカスタマイズ

a. Security > Authentication > Login Profiles の順にクリックし、以下の画面を表示します。

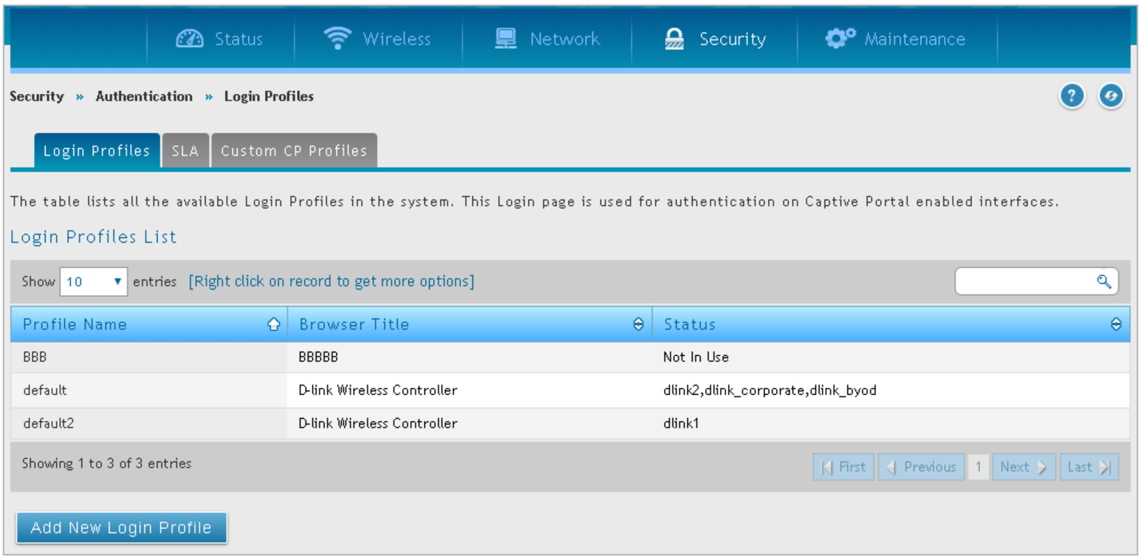


図 4-26　Login Profiles List 画面

b.「Add New Login Profile」ボタンをクリックします。
新しいプロファイルを追加するか、既存のプロファイルを右クリックし、「Edit」を選択して、プロファイルを編集します。
以下の画面が表示されます。

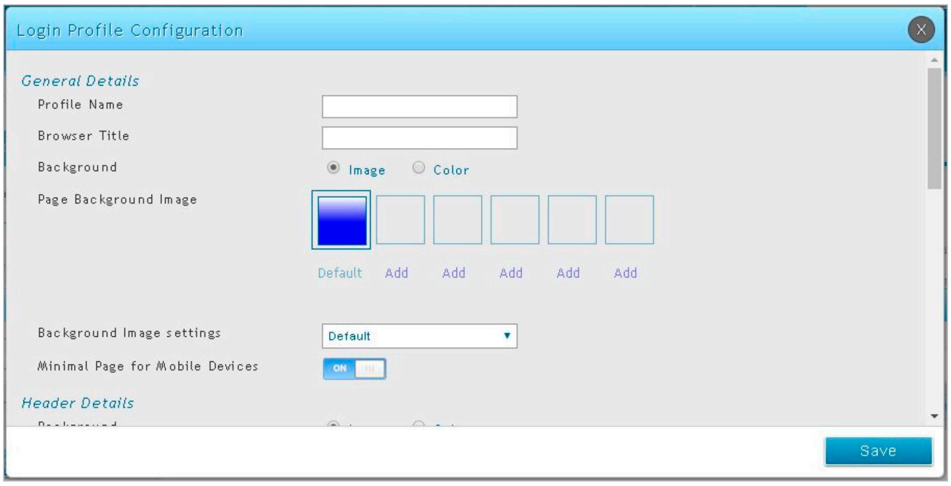


図 4-27　Login Profile Configuration 画面

以下の項目があります。

項目	説明
General Details	
Profile Name	キャプティブポータルプロファイルの名前を入力します。名前は、追加する可能性のある他のプロファイルとこのプロファイルを簡単に識別できるようにする必要があります。
Browser Title	キャプティブポータルセッション中にブラウザのタイトルに表示される文字列を入力します。
Background	キャプティブポータルセッション中に表示されるログインページの背景として、画像またはカラーを選択します。 ・ Image - ページの背景として画像を表示します。 ・ Color - ページの背景色を設定します。
Page Background Image	「Background」で「Image」を設定した場合、**Add >「ファイル選択」**の順にクリックして、画像ファイルをアップロードします。画像を選択して「開く」をクリックし、「Upload」ボタンをクリックします。アップロード可能な画像の最大サイズは 50KBytes です。
Background Image settings	「Background」で「Image」を設定した場合、画像の表示方法を指定します。 ・ Default - 画像を垂直・水平方向に繰り返して、ログイン画面全体に表示します。 ・ Simple - 画像をログイン画面にそのまま表示します。 ・ Strech - 画像をログイン画面全体に引き延ばして表示します。 ・ Vertical Repeat - 画像を垂直方向に繰り返して、ログイン画面に表示します。 ・ Horizontal Repeat - 画像を水平方向に繰り返して、ログイン画面に表示します。
Page Background Color	「Background」で「Color」を設定した場合、キャプティブポータルセッション中に表示されるページの背景色をプルダウンメニューから選択します。
Custom Color	「Page Background Color」で「Custom」を選択した場合、HTML のカラーコードを入力します。
Minimal Page for Mobile Devices	「ON」にするとページをモバイルデバイス用（必要最小表示）に設定します。
Header Details	
Background	キャプティブポータルセッション中に表示されるログインページのヘッダとして、画像またはカラーを選択します。 ・ Image - ページのヘッダとして画像を表示します。 ・ Color - ヘッダの背景色を設定します。
Header Background Image	「Background」で「Image」を設定した場合、**Add >「ファイル選択」**の順にクリックして、画像ファイルをアップロードします。画像を選択して「開く」をクリックし、「Upload」ボタンをクリックします。アップロード画像の最大サイズは 50KBytes です。
Header Background Color	「Background」で「Color」を設定した場合、ヘッダの色をプルダウンメニューから選択します。 「Page Background Color」で「Custom」を選択した場合、「Custom Color」に HTML のカラーコードを入力します。
Custom Color	「Page Background Color」に「Custom」を選択した場合、HTML のカラーコードを入力します。
Header Caption	キャプティブポータルセッション中にログインページのヘッダに表示されるテキストを入力します。
Caption Font	ヘッダテキストのフォントを選択します。
Font Size	ヘッダテキストのフォントサイズを選択します。
Font Color	ヘッダテキストのフォント色を選択します。

項目	説明
Login Details	
Login Section Title	（オプション）キャプティブポータルセッションへのログイン時に表示されるログインボックスのタイトルに表示されるテキストを入力します。
Welcome Message	（オプション）キャプティブポータルセッションへのログインに成功した場合に表示されるウエルカムメッセージを入力します。
Error Message	（オプション）キャプティブポータルセッションへのログインに失敗した場合に表示されるエラーメッセージを入力します。
Footer Details	
Change Footer Content	ログインページのフッターコンテンツへの変更を有効または無効にします。
Footer Content	「Change Footer Content」をチェックした場合、フッターに表示されるテキストを入力します。
Footer Font Color	「Change Footer Content」がチェックした場合、フッターに表示される色を入力します。
External Payment Gateway	
Enable External Payment Gateway	外部のペイメントゲートウェイおよびログインページからのオンライン無線サービスの購入を有効または無効にします。
Session Title 1	ユーザがキャプティブポータルセッションへのログイン時に、オンライン購入のログインボックスのタイトルに表示されるテキストを入力します。
Message	ユーザがキャプティブポータルセッションへのログイン時に、オンライン購入ログインボックスに表示されるテキストを入力します。
Session Title2	オンライン購入が完了した時に、メッセージボックスのタイトルに表示されるテキストを入力します。
Success Message	オンライン購入が完了した時に、メッセージボックスに表示されるテキストを入力します。
Session Title3	オンライン購入に失敗した時に、メッセージボックスのタイトルに表示されるテキストを入力します。
Failure Message	オンライン購入が失敗した時に、メッセージボックスに表示されるテキストを入力します。
Enable Billing Profile	
ログインページに表示されるビリングプロファイルを選択します。テーブルには「Unit Price」を設定したビリングプロファイルのみ表示されます。状態を「ON」に切り替えて、ビリングプロファイルを有効にします。	
Service Disclaimer Text	無線サービスを選択および購入する前に表示されるサービスに関する免責事項のテキストを入力します。
Payment Server	支払いアカウントおよび支払い代行サーバを選択します。

c. フィールドにデータを入力し、「Save」ボタンをクリックします。設定に成功すると、「Operation Succeeded」メッセージが表示されます。

d.「Login Profiles List」でプロファイルを右クリックし、「Show Preview」を選択すると、設定したプロファイルを参照することができます。ログインページの表示内容が要件に沿っていることを確認します。要件に合わない場合、必要に応じて手順の 4b と 4c を繰り返します。

手順 8: RADIUS サーバを持つ SSID をオーセンティケータとして使用する

RADIUS 認証が設定された SSID を使用するには、以下の手順を実行します。

1. **Security > Authentication > External Auth Server > RADIUS Server** の順にメニューをクリックし、以下の画面を表示します。

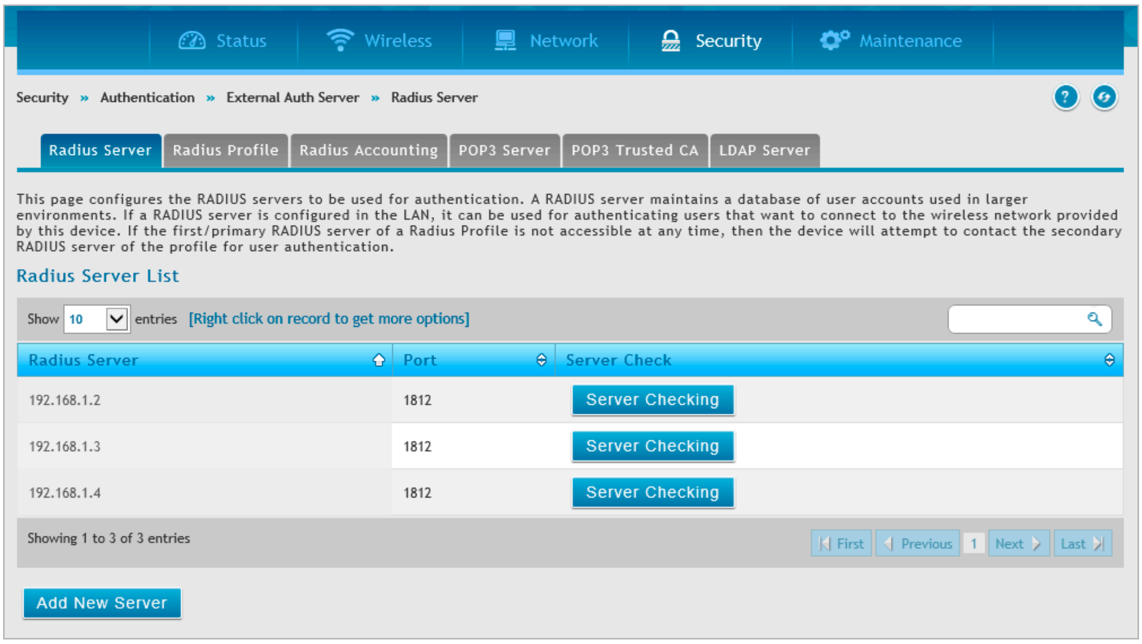


図 4-28　RADIUS Server List 画面

2. 新しい Radius サーバを追加するには、「Add New Server」をクリックします。既存エントリの設定を編集するには、該当エントリ上で右クリックし、「Edit」を選択します。

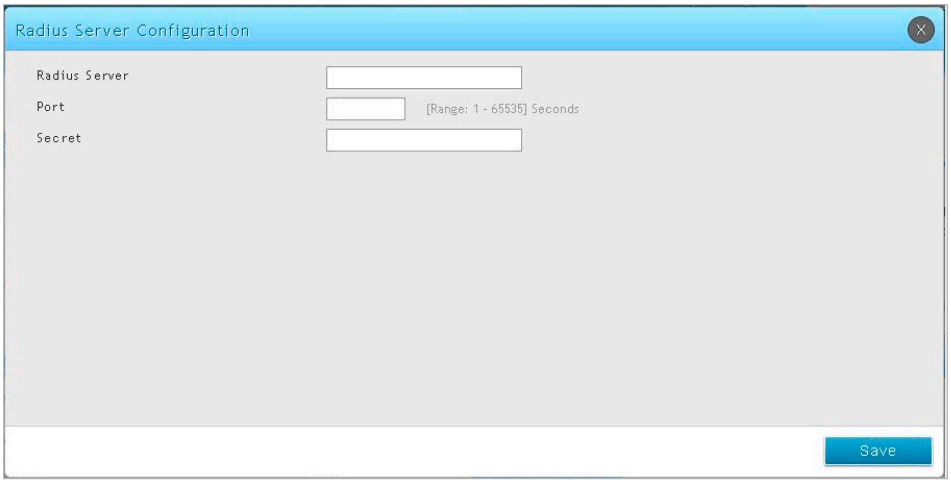


図 4-29　RADIUS Server Configuration 画面

以下の項目があります。

項目	説明
Radius Server	RADIUS 認証サーバの IP アドレスを指定します。
Port	RADIUS メッセージを送信する RADIUS 認証サーバのポート番号を指定します。
Secret	デバイスが設定済みの RADIUS サーバにログインできる秘密鍵を入力します。これは RADIUS サーバの秘密鍵に一致する必要があります。

3. フィールドにデータを入力し､「Save」ボタンをクリックします。RADIUS 認証サーバを使用するために､使用するアクセスポイントが設定されます。
4. 「Server Checking」ボタンをクリックして、DWC-2000 と RADIUS サーバ間の接続をテストします。

手順 9: ゲスト管理の設定

フロントデスクの管理アカウントから一時的なゲストアカウントを生成することができます。ゲスト管理を設定するには、以下の手順を実行します。

1. フロントデスクグループを作成する

a. **Security** > **Authentication** > **User Database** > **Groups** の順にメニューをクリックし、以下の画面を表示します。

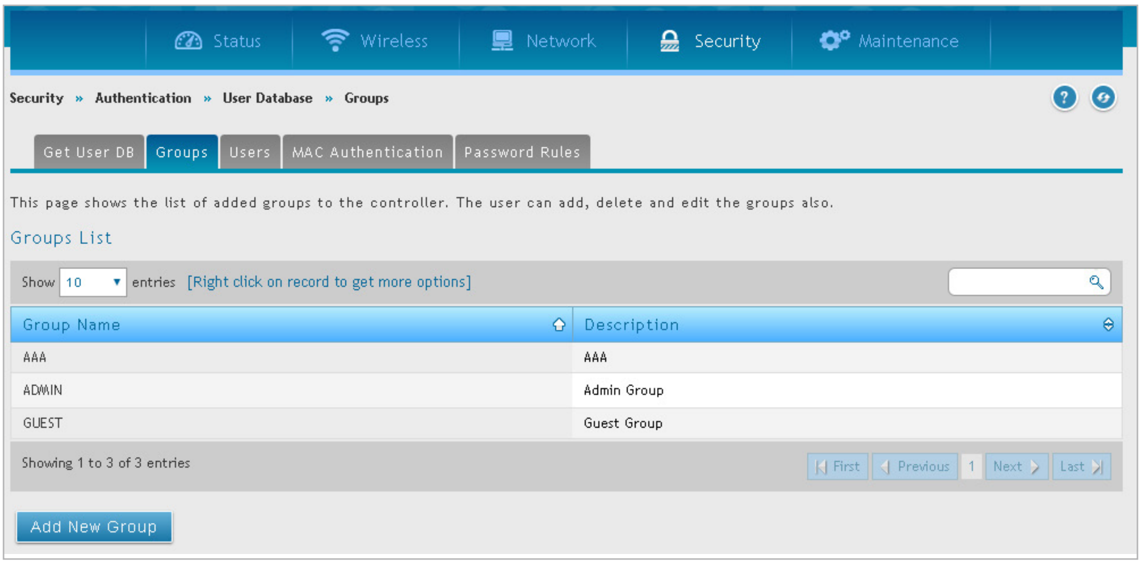


図 4-30　Groups List 画面

b.「Add New Group」ボタンをクリックして、以下の画面を表示します。

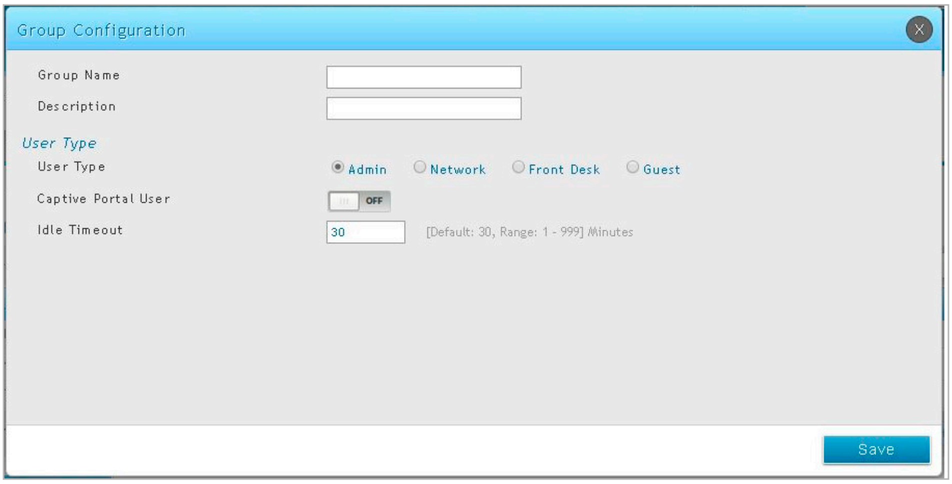


図 4-31　Group Configuration 画面

c. グループ名と説明を入力し、「User Type」で「Front Desk」を選択後、「Save」ボタンをクリックします。

2.　フロントユーザの追加

a. Security > Authentication > User Database > Users の順にメニューをクリックし、以下の画面を表示します。

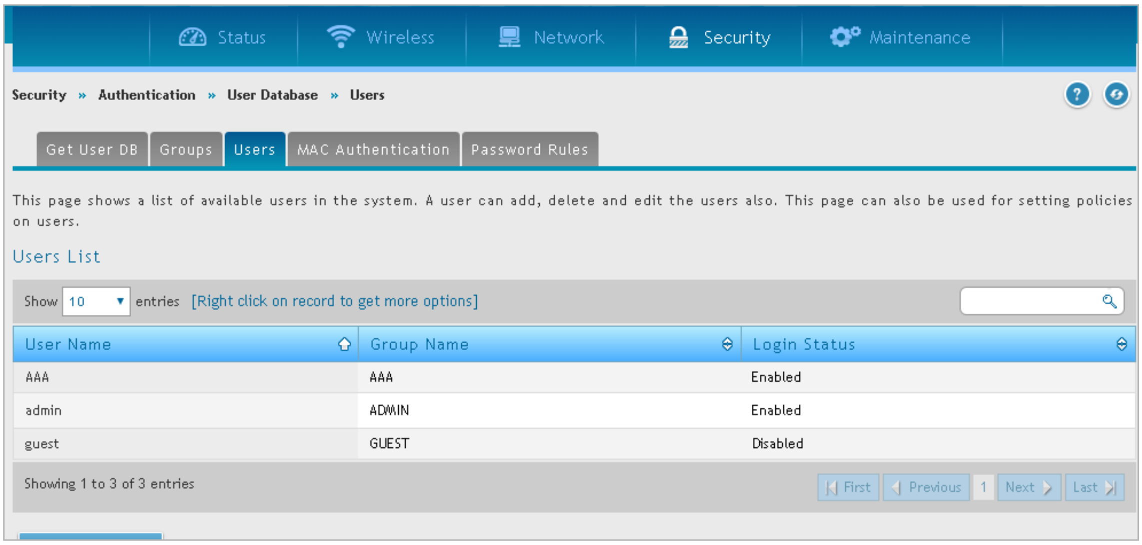


図 4-32　Users List 画面

b.「Add New User」ボタンをクリックし、以下の画面を表示します。

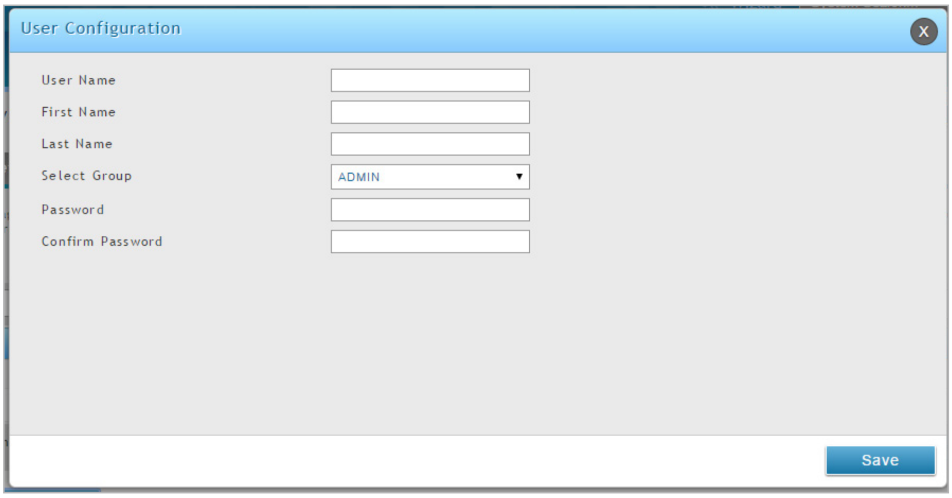


図 4-33　User Configuration 画面

c. フィールドにデータを入力し、「Save」ボタンをクリックします。
「Select Group」には前の手順で作成したフロントデスクのグループを選択します。

3.　ビリングプロファイルの作成

a. Security > Authentication > Billing Profile の順にクリックし、以下の画面で「Add New Billing Profile」をクリックします。

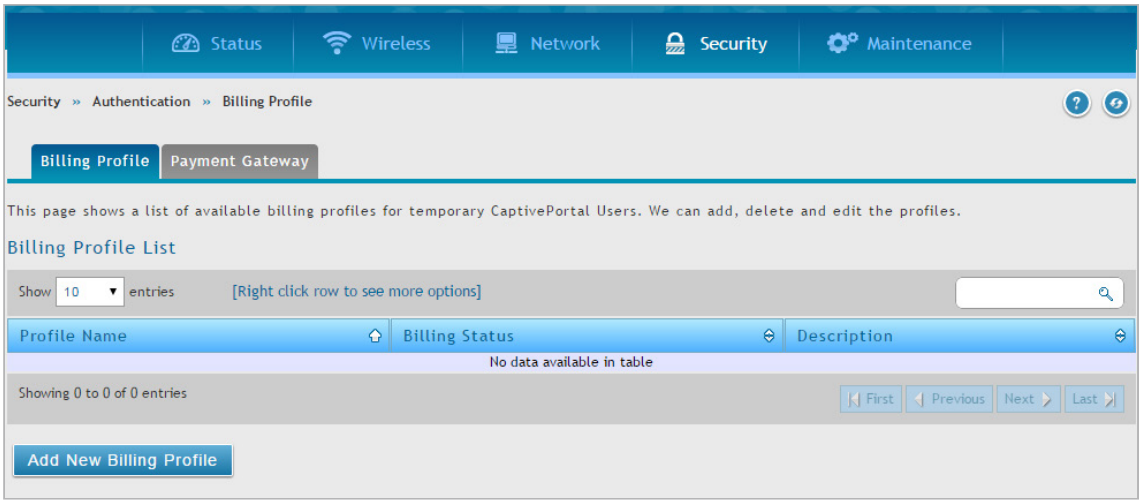
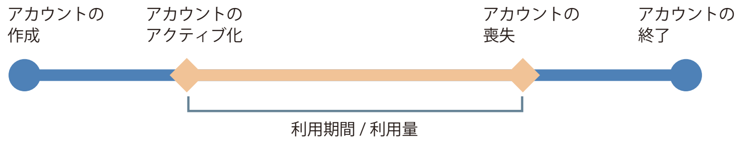


図 4-34　Billing Profile List 画面

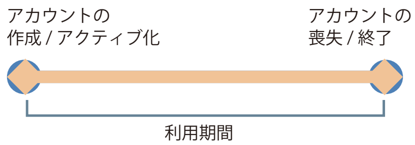
b. ビリングプロファイル設定には、以下の通り 4 つの手順があります。



- アカウントの作成 : 一時的なアカウントは、ローカルデータベースのフロントデスクアカウントによって生成されます。
- アカウントのアクティブ化 : 一時的なアカウントがアクティブ化され、有効になります。
- アカウントの喪失 : 一時的なアカウントは、利用期間または従量の期限（上限）に到達します。
- アカウントの終了 : 一時的なアカウントは、利用期間 / 従量に到達するかどうかに関わらず終了し、ローカルのデータベースから削除されます。

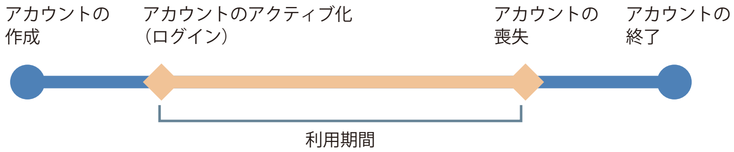
最も一般的なビリングプロファイルとして以下の 5 つのタイプがあります。

I. 一時的なアカウントの利用時間は、アカウントの存続時間によって制限されます。アカウントには期限があり、アカウントが存在している間は有効です。



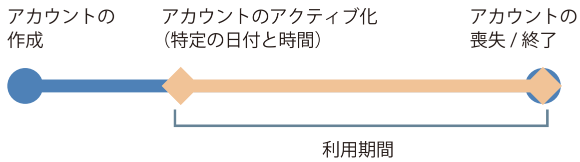
このビリングプロファイルは、ホテルで使用するというシナリオに適しています。一時的なアカウントがカスタマのチェックイン時に作成され、有効になります。

II. 一時的なアカウントの利用時間は、アカウントの存続時間によって制限されます。アカウントには期限があり、最初のログインの間、有効になります。



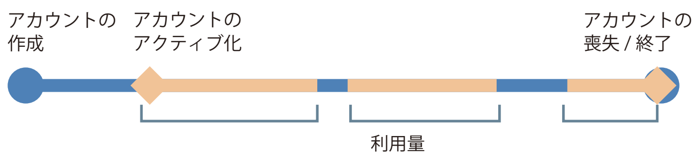
このビリングプロファイルは、カフェや空港などで使用するというシナリオに適しています。カスタマは、最初のログインから計算した時間内で、無線インターネットサービスを使用できます。

III. 一時的なアカウントは特定の日時に有効です。アカウントには期限があります。



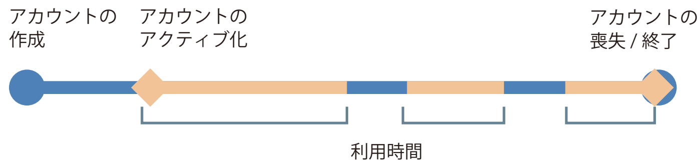
このビリングプロファイルは、プレスカンファレンスで使用するというシナリオに適しています。必要に応じて、主催者がイベント前にアカウントを生成し、 事前に関係者に情報を引き渡します。一時的なアカウントは特定の日時から有効になります。

IV. 一時的なアカウントは使用時間が制限されます。アカウントには利用終了までの期限はありません。



このビリングプロファイルは、ホットスポットで使用するというシナリオに適しています。サービスプロバイダは、利用時間に基づいて無線サービスに課金します。このアカウントでは複数のデバイスが同時にログインすることができます。

V. 一時的なアカウントは使用トラフィックも制限されます。アカウントには利用終了までの期限はありません。



このビリングプロファイルは、ホットスポットで使用するというシナリオに適しています。サービスプロバイダは、使用量に基づいて無線サービスに課金をします。

c. フィールドにデータを入力します。

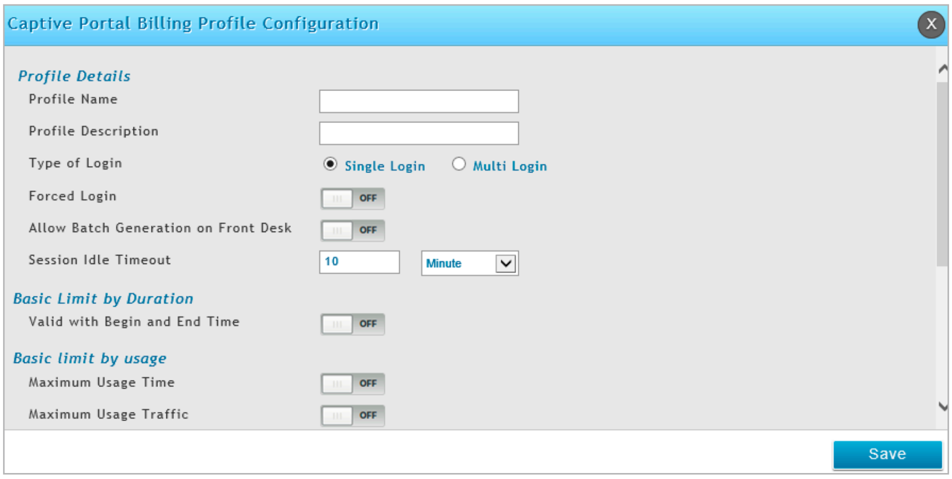


図 4-35　Captive Portal Billing Profile Configuration 画面

以下の項目があります。

項目	説明
Profile Details	
Profile Name	プロファイル名を入力します。
Profile Description	プロファイルの説明文を入力します。
Type of Login	ログインのタイプを以下から選択します。 • Single Login - 複数のユーザがこのプロファイルで生成される同じキャプティブポータルのログイン証明書を使用して、同時にログインすることはできません。 • Multi Login - 複数のユーザがこのプロファイルで生成される同じキャプティブポータルのログイン証明書を使用して、同時にログインできるようになります。
Forced Login	「Single Login」を選択した場合に、強制ログインを「ON」または「OFF」にします。
Allow Batch Generation on Front Desk	「ON」にすると、フロントデスクユーザは、ワンクリックで一時的なキャプティブポータルユーザを一括して生成できます。
Max Login Users	「Multi Login」を選択した場合に、同時にログインできるユーザの最大数を設定します。
Session Idle Timeout	このプロファイルで生成された CP ユーザのアイドルタイムを指定します。
Basic Limit by Duration	
Valid with Begin and End time	Duration（期間）ベースの制限を有効または無効にします。
Valid Begin	「Valid with Begin and End Time」を有効にした場合に、期間によるユーザアクセス制限として以下のいずれかを選択します。 • Start while Account Created - ユーザが作成された時にアカウントをアクティブにします。 • Start While Account Login - 証明書を使用してユーザが最初にログインした時にアカウントをアクティブ化します。 • Begin From - 指定した日付からアカウントをアクティブ化します。
Start while Account Created	「Start while Account Created」を選択した場合、フィールドに値を入力し、単位（Hours または Days）を選択して、利用時間を設定します。
Start While Account Login	「Start While Account Login」を選択した場合、フィールドに値を入力し、単位（Hours または Days）を選択して、利用時間を設定します。
Begin From	「Begin From」を選択した場合、アカウントが有効になる日時を設定します。
Allow Front Desk to Modify Duration	「Valid with Begin and End Time」を有効にする場合、このオプションを「ON」にすることで、フロントデスクユーザは利用時間の期限を編集できます。
Basic Limit by usage	
Maximum Usage Time	アカウントの期限が切れる前に、ユーザがログインを維持できる最大時間を有効または無効にします。「ON」を指定した場合、フィールドに値を入力し、単位（Hours または Days）を選択し、利用時間を設定します。
Maximum Usage Traffic	アカウントの期限が切れる前に、ユーザが使用できる最大トラフィックを有効または無効にします。「ON」を指定した場合、フィールドに値を入力し、単位（MB または GB）を選択します。内向きトラフィックに対してのみ帯域幅について考慮されるものとします。
Show Alert Message on Login Page while Rest of Usage Time / Traffic under	利用時間 / トラフィック量が所定の制限に到達した時に警告メッセージを受け取るために、Hours/MB に値を入力します。「0」を指定すると、警告メッセージが表示されません。

項目	説明
Allow Front Desk to Modify Usage	「Maximum Usage Time」または「Maximum Usage Traffic」を有効にする場合、このオプションを「ON」にすることで、フロントデスクユーザは利用トラフィックの制限を編集できます。
Ticket Printing Options	
Header	「ON」にしてヘッダを指定します。
Customized Note	「ON」にしてカスタム項目を指定します。
Time Stamp	「ON」にしてタイムスタンプを有効にします。
Footer	「ON」にしてフッターを指定します。
Ticket Logo	「ON」にしてチケットロゴを指定します。「Add」をクリックすると画像を追加できます。
Unit Price	
Set Price	「ON」にして値段の指定を有効にします。
Price	「Set Price」を有効にすると表示されます。値段を指定します。
Monetary Unit	金銭の単位を指定します。

4. ゲストキャプティブポータルのインタフェースを選択する
   a. Wireless > Access Point > AP Profile > AP Profile SSID の順にクリックし、「Access Point Profiles SSID List」画面を表示します。

   b. キャプティブポータル機能を使用する「SSID」を右クリックして、「Edit」を選択します。

   c.「Captive Portal Type」のプルダウンメニューでキャプティブポータルタイプを選択します。

   d.「Save」ボタンをクリックします。

注意 SSID が古い AP プロファイルに関連付けられている場合、コンフィグレーションを変更するためには、**Wireless > Access Point > AP Profile** で AP プロファイルを適用します。

5. ゲストアカウントを生成します。

   a.「http://<ip_address>/frontdesk」（例 http://192.168.10.1/ frontdesk）、または「http://<ip_address>/platform.cgi?page=billingDeskLogin.html」を入力して、「Front Desk」ページにログインします。「Front Desk」グループに作成したユーザのユーザ名とパスワードを入力します。

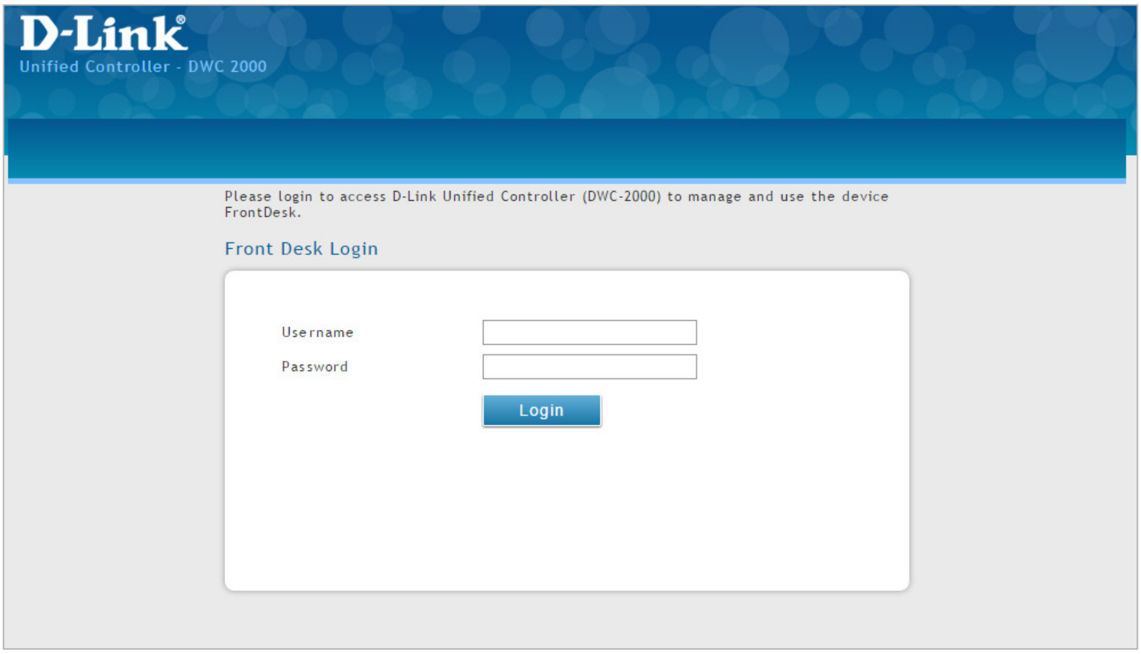


図 4-36　フロントデスク画面

b.「Billing Form」タブを選択し、ビリングプロファイルを選択します。
必要に応じて、設定内容を変更します。「Generate」ボタンをクリックします。

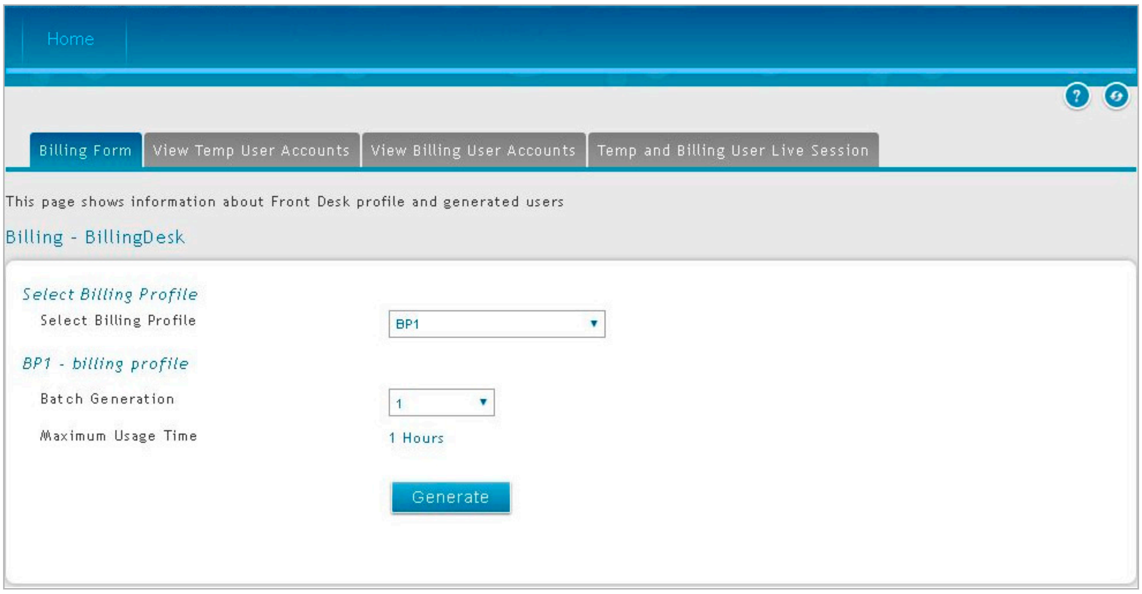


図 4-37　Billing - Generate 画面

c.「Print」をクリックすると、課金情報を印刷することができます。
情報はインターネットプリンタに送信されます。一度に作成できるユーザアカウントは 1 つです。

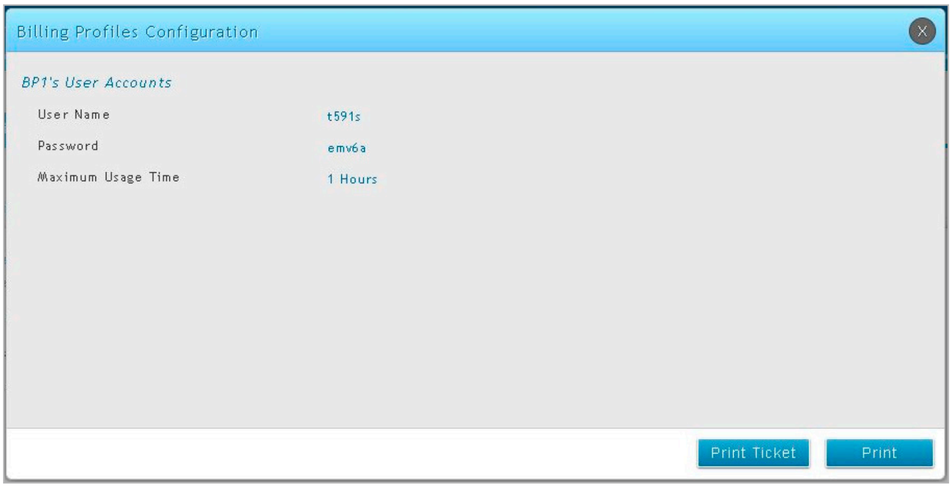


図 4-38　Billing Profiles Configuration 画面

6.　ユーザアカウントの状態をモニタリングします。

a. 一時的なアカウントの状態およびアカウント利用時間や利用量まで広くモニタリングします。生成された一時的な状態を確認するには、「View Temp User Accounts」や「View Billing User Accounts」タブを開き、以下の画面を表示します。

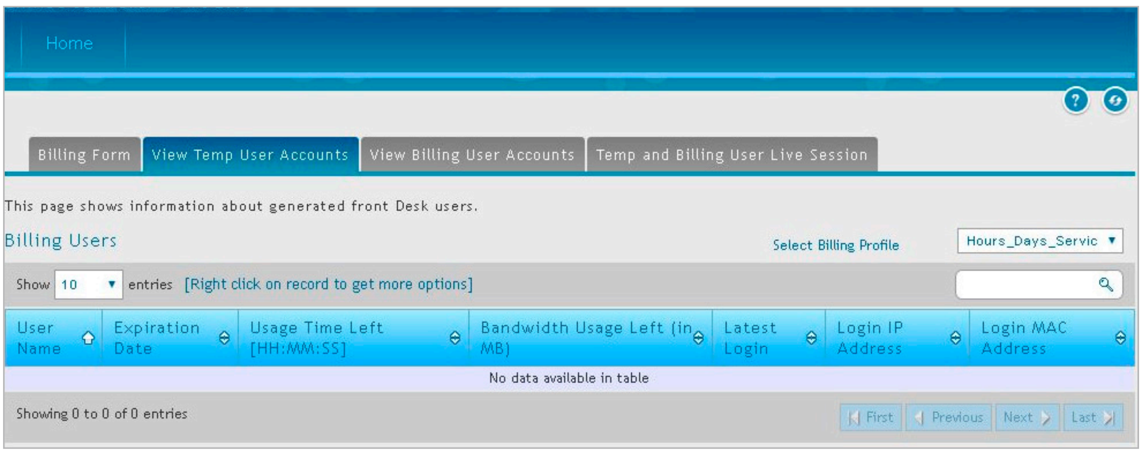


図 4-39　Billing Users 画面

b. アカウントを選択し、右クリックメニューから「View Details」を選択して、詳しい情報を参照します。

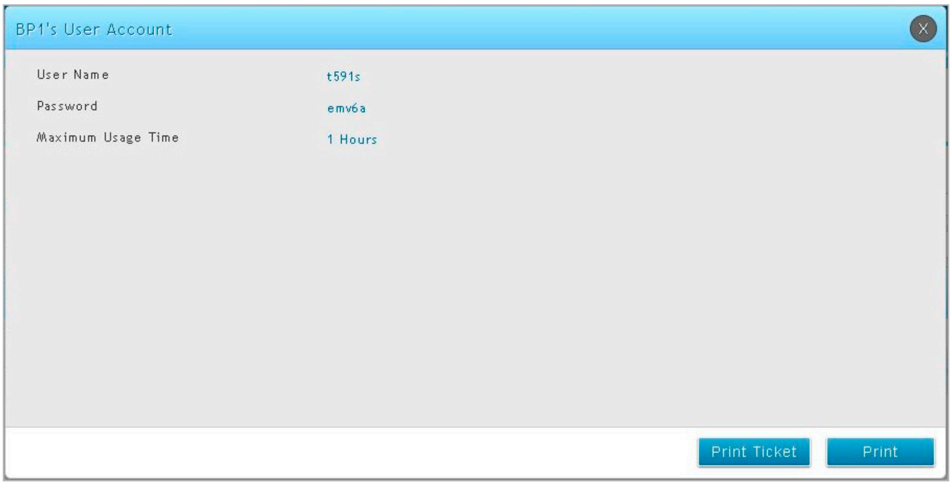


図 4-40　Billing User Account 画面

7.　ユーザアカウントの利用の拡張設定

a. アカウントを右クリックし、「Extend Session」を選択します。利用時間 / トラフィックを手動で変更します。

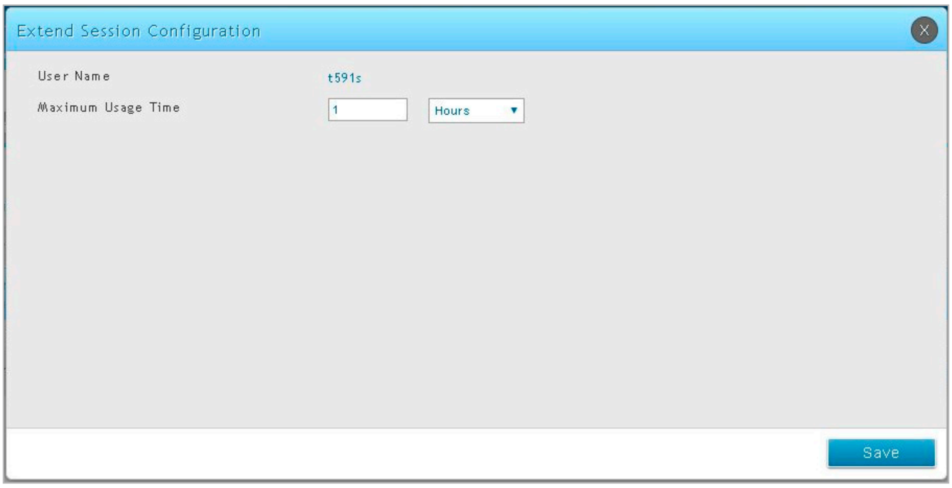


図 4-41　Extend Session Configuration 画面

注意　**Security > Authentication > Billing Profile > Billing Profile** の「Captive Portal Billing Profile Configuration」画面で「Allow Front Desk to Modify Usage」を「ON」に必ず切り替えてください。

b.「Save」ボタンをクリックします。

手順 10: BYOD 環境の設定

職場における BYOD（Bring Your Own Device）のトレンドは、ネットワークセキュリティや管理における新しい挑戦です。従業員が仕事に個人のデバイスを使用することを許可する会社の多くでは、より高いパフォーマンスと生産性を期待しています。その反面で、ネットワークセキュリティや、個人のデバイスを使用することによる情報漏洩について、会社が検討する必要も出てきます。会社が提供したデバイスと個人のデバイス（BYOD デバイス）を見分ける方法は、IT チームの主要な課題となっています。

デバイスが会社提供のものか個人で保有するものかに基づいて、MAC 認証を使用してクライアントと特定の SSID との紐づけを行います。SSID を使用したすべての接続には、権限を付与する前に、認証の実行が必要とされます。BYOD 環境を設定するには、以下の手順を実行します。

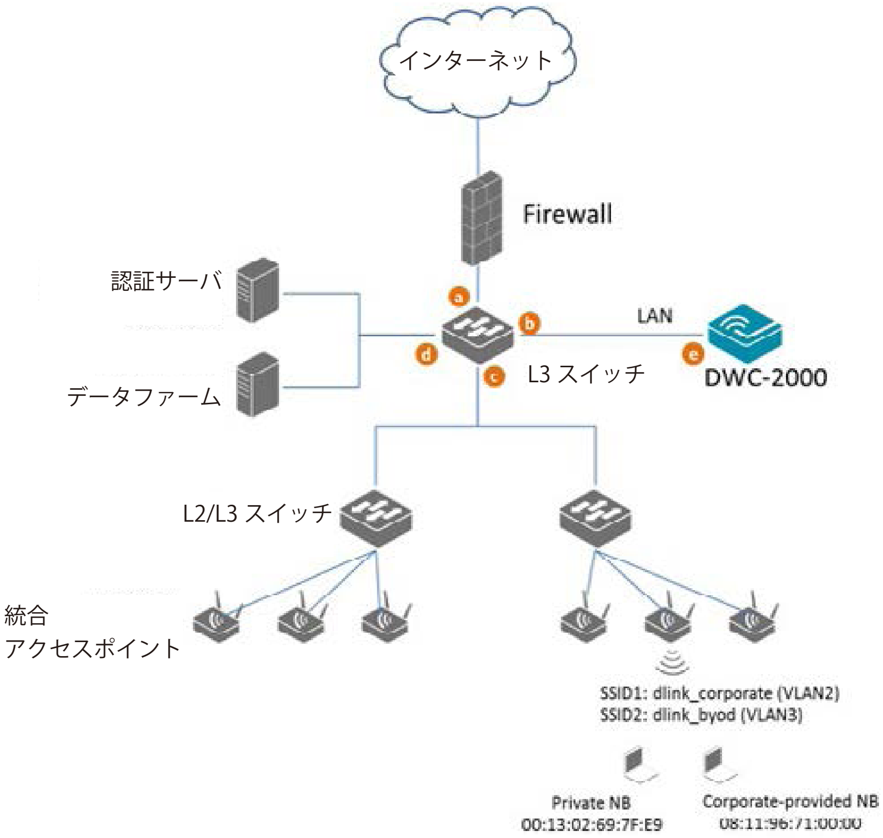


図 4-42　BYOD Configuration 画面

各 SSID における認証方式は異なります。

- **dlink_corporate SSID**
  この SSID は、会社で提供したデバイスを使用して作業する D-Link の従業員用です。認証処理を完了するには、デバイスの MAC 認証とキャプティブポータルを必要とします。
- **dlink_byod SSID**
  この SSID は、個人のデバイス（BYOD デバイス）を使用して作業する D-Link の従業員用です。認証処理を完了するには、キャプティブポータルを必要とします。

1.　ネットワークアーキテクチャに基づいて VLAN を設定する

3 つの VLAN を作成します。VLAN1 はアクセスポイント管理のためのデフォルト VLAN で、VLAN2 は SSID「dlink_corporate」に関連するトラフィック用、VLAN3 は SSID「dlink_byod」に関連するトラフィック用です。VLAN1 をポート 1 の 3 つのメンバシップに関連付けます。

a. **Network > VLAN > VLAN Settings** の順にメニューをクリックし、以下の画面を表示します。

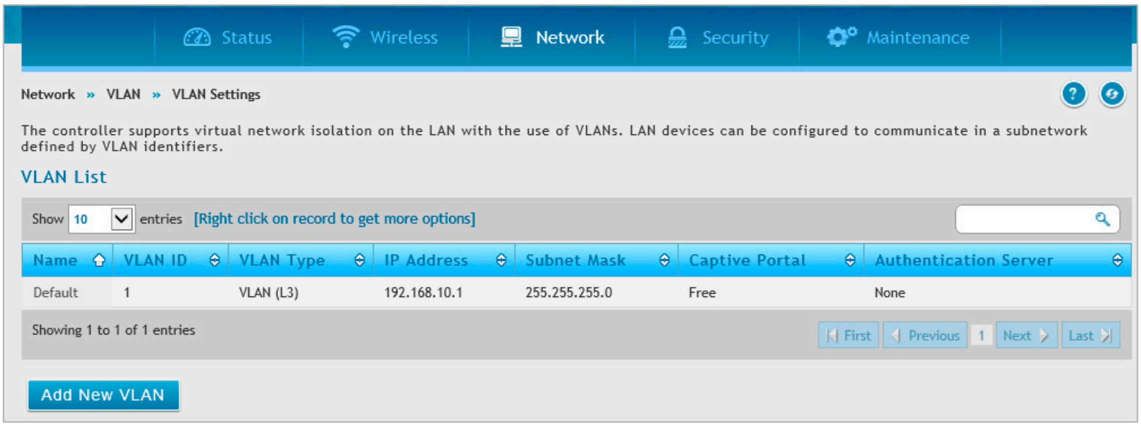


図 4-43　VLAN List 画面

b.「Add New VLAN」ボタンをクリックし、以下の画面を表示します。

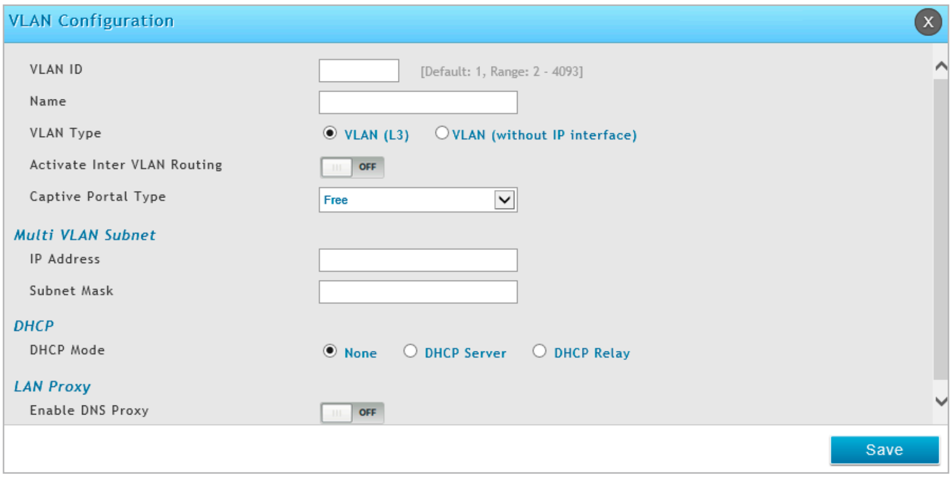


図 4-44　VLAN Configuration 画面

c. VLAN ID と VLAN 名 を入力します。

d. VLAN の IP アドレス範囲を入力します。

e.「Save」ボタンをクリックします。

2.　VLAN1 をポート 1 における Trunk モードの 3 つのメンバシップに関連付ける

a. Network > VLAN > Port VLAN の順にメニューをクリックし、以下の画面を表示します。

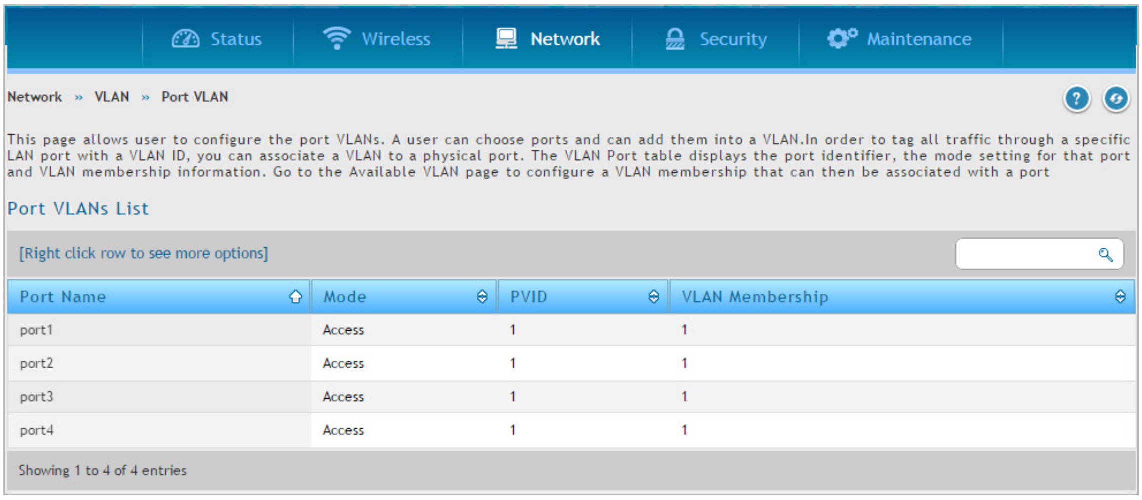


図 4-45　Port VLANs List 画面

b. ポート 1 を右クリックし、「Edit」を選択して、以下の画面を表示します。

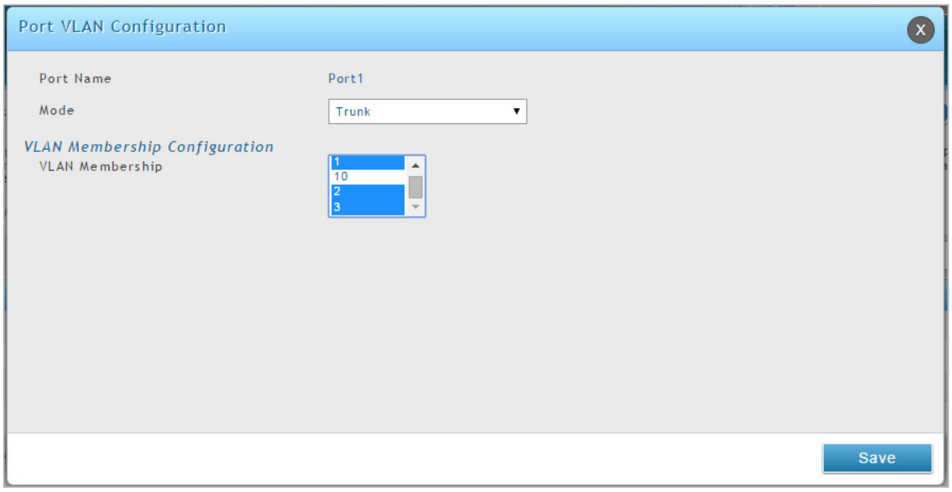


図 4-46　Port VLAN Configuration 画面

「Mode」プルダウンメニューから「Trunk」を選択し、「VLAN Membership」横の VLAN1-3（Ctrl キーを押したまま、1、2、3 をクリック）を選択します。

c.「Save」ボタンをクリックします。

3. 2 つの SSID（dlink_corporate および dlink_byod）を作成し、これら 2 つの SSID にそれぞれ VLAN2 と VLAN3 を割り当てます。さらに、SSID「dlink_corporate」における MAC 認証を有効にします。

a. **Wireless > Access Point > AP Profile > AP Profile SSID** の順にメニューをクリックし、以下の画面を表示します。

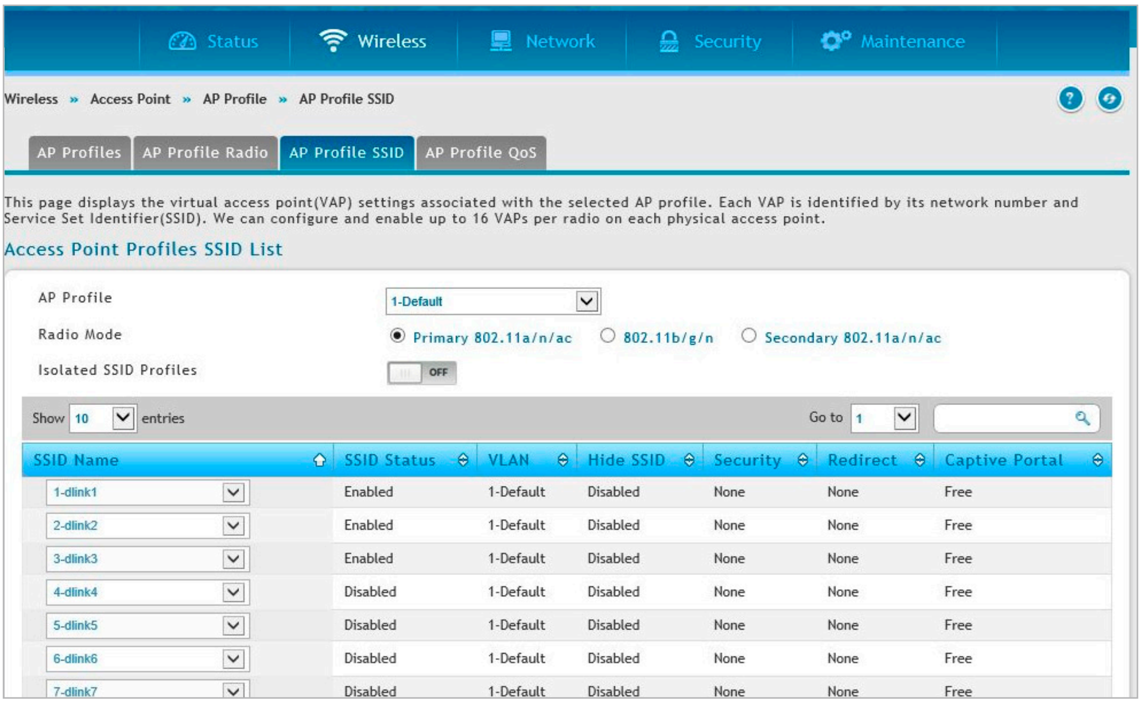


図 4-47　Access Point Profiles SSID List 画面

b.「Add New SSID Profile」ボタンをクリックします。SSID「dlink_corporate」と「dlink_byod」を作成します。

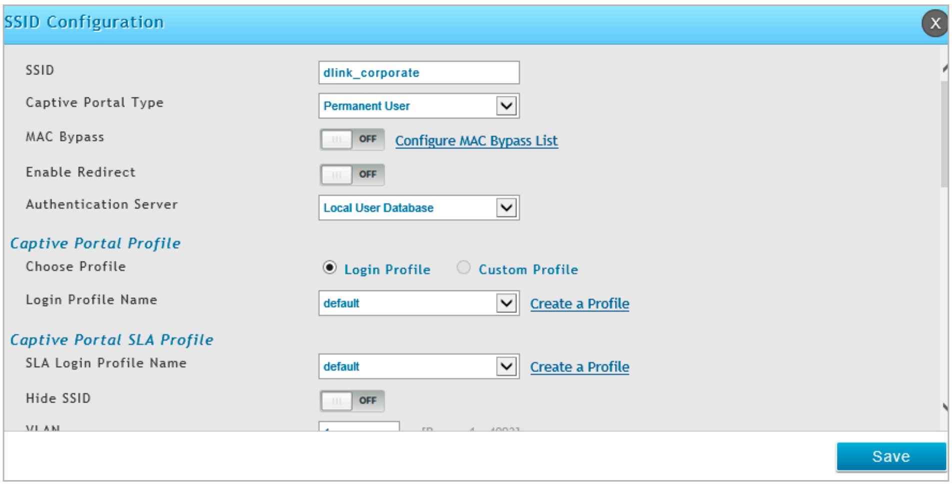


図 4-48　SSID Configuration 画面 - dlink_corporate

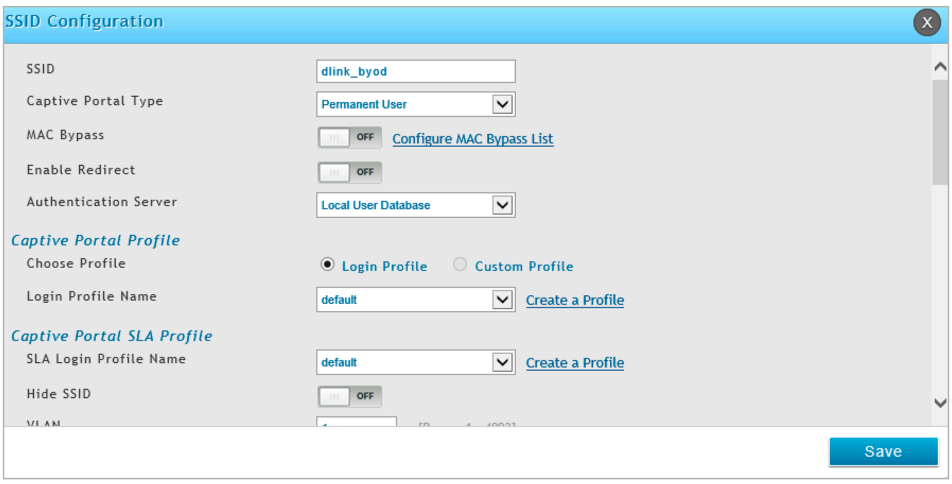


図 4-49　SSID Configuration 画面 -dlink_byod

c. 両方の SSID の「Captive Portal」を有効にして、「Captive Portal Type」に「Permanent User」を選択します。

d. 認証サーバを選択します。認証サーバは、ローカルのデータベースまたは外部認証サーバ（RADIUS）のいずれかです。

e. VLAN2 と VLAN3 をそれぞれ「dlink_corporate」と「dlink_byod」に割り当てます。

f.「dlink_corporate」における MAC 認証を有効にします。

g.「Save」ボタンをクリックします。

4. AP プロファイル「BYOD」を作成し、このプロファイルに SSID を関連付けます。

a. Wireless > Access Point > AP Profile の順にメニューをクリックします。

b.「Add New AP Profile」ボタンをクリックします。プロファイル「BYOD」を作成します。

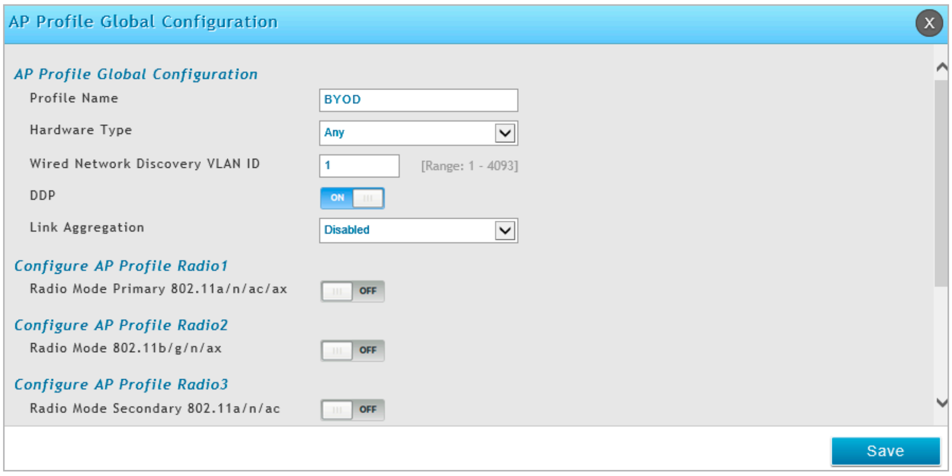


図 4-50　AP Profile Global Configuration 画面

c.「Save」ボタンをクリックします。

d.「AP Profile SSID」タブをクリックします。「AP Profile」のドロップダウンリストで「BYOD」を選択します。

e.「SSID」リストで「dlink_corporate」のエントリを右クリックして、「Enable」を選択します。

f.「dlink_byod」のエントリを右クリックして、「Enable」を選択します。

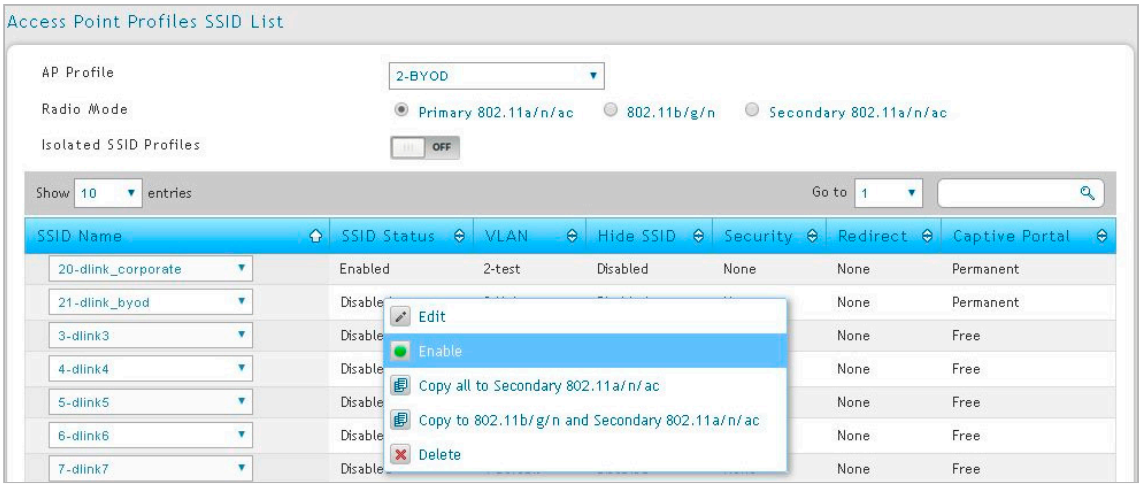


図 4-51　AP Profile SSID List 画面

g. 両方の SSID は、これで「BYOD」SSID プロファイルに関連付けられました。

5. ローカルデータベースにキャプティブポータルアカウントを作成します。

a. ユーザグループを作成するには、**Security > Authentication > User Database > Group** の順にメニューをクリックします。

b.「Add New Group」ボタンをクリックし、以下の画面を表示します。

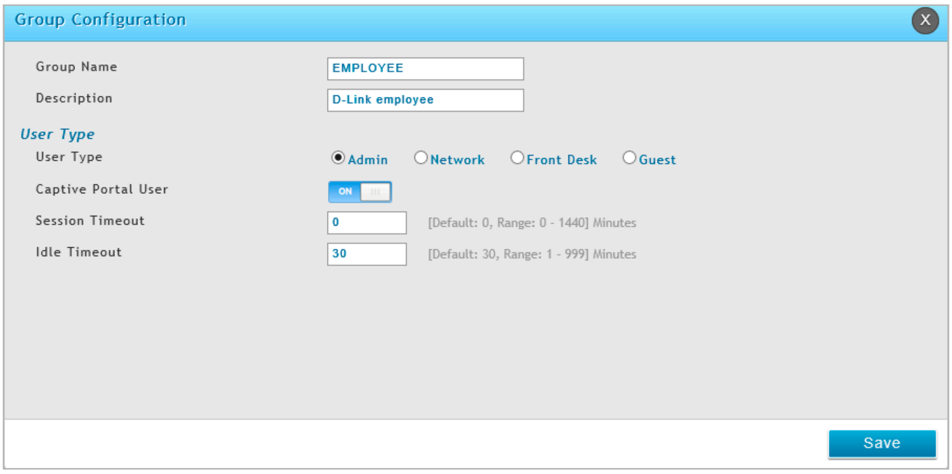


図 4-52　Group Configuration 画面

グループ「EMPLOYEE」を作成します。「User Type」横で「Network」を選択し、「Captive Portal User」を「ON」に切り替えます。「Idle Timeout」の値（分）を入力します。

c.「Save」ボタンをクリックします。

d. ユーザアカウントを作成します。**Security > Authentication > User Database > Users** の順にメニューをクリックします。

e.「Add New User」ボタンをクリックして、以下の画面を表示します。

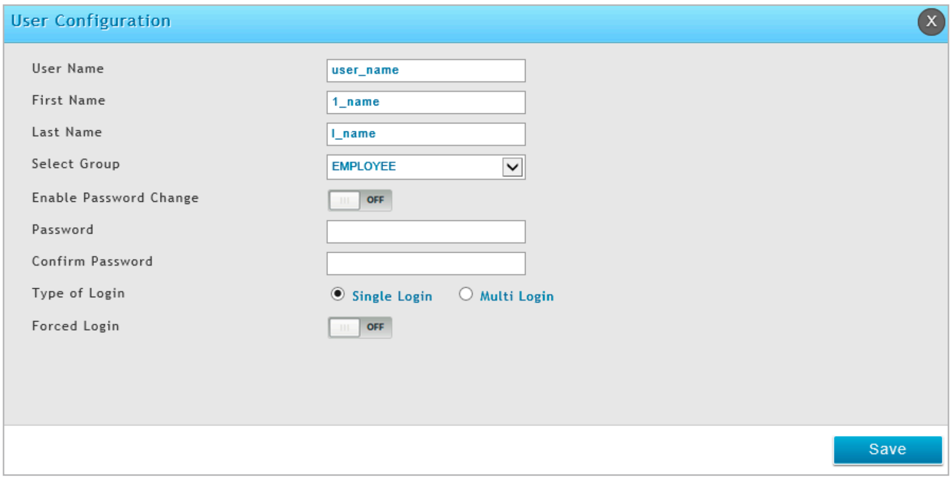


図 4-53　User Configuration 画面

フィールドに入力後、「Select Group」横の「EMPLOYEE」を選択します。

f.「Save」ボタンをクリックします。

6.　ローカルのデータベースにデバイスの MAC 認証データベースを作成します。

a. **Security > Authentication > User Database > MAC Authentication** の順にメニューをクリックします。

b. 現在の設定に基づいてリストのタイプ（White-List または Black-List）表示されます。
設定を変更するには、「手順 5: MAC 認証モードの選択」を参照してください。

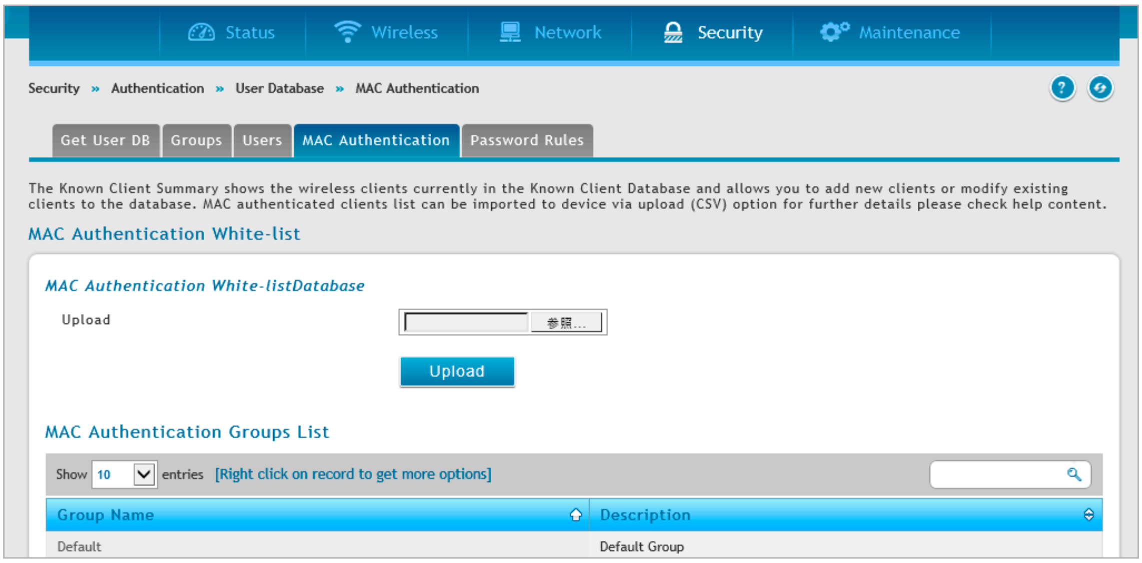


図 4-54　MAC Authentication White-List 画面

c.「Add New MAC Authentication」ボタンをクリックして、以下の画面を表示します。

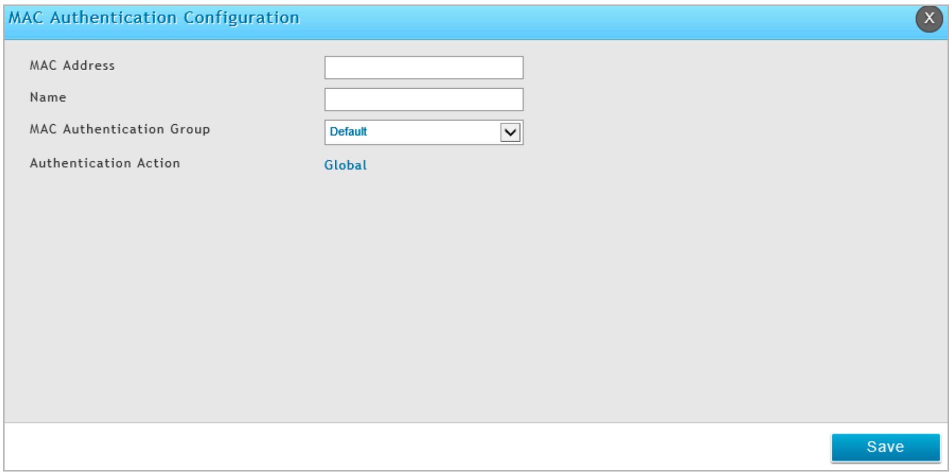


図 4-55　MAC Authentication Configuration 画面

d. デバイスの AMC アドレスと名称を入力し、グループを選択します。

e.「Save」ボタンをクリックします。

注意　ユーザ認証と MAC 認証データベースが外部認証サーバ（RADIUS）である場合、「手順 8: RADIUS サーバを持つ SSID をオーセンティケータとして使用する」を参照してください。

7.　ネットワークからアクセスポイントを検出して、管理します。「手順 3: 管理するアクセスポイントの選択」を参照してください。

これらの基本設定が完了すると、無線コントローラで稼働の準備が整います。これらの設定は、多くのユーザおよび状況に適しています。

また、無線コントローラは、より高度な機能を利用したいユーザに高度なコンフィグレーションを提供します。次のセクションでは無線コントローラの高度な設定について記載しています。これらの機能を理解していないユーザは、技術サポートスタッフがアドバイスしない限り、無線コントローラの再設定を試みるべきではありません。

第 5 章　高度な無線 LAN 設定

多くのユーザは、前章で説明した基本設定で十分ですが、大規模な無線ネットワークや複雑な配置では、無線コントローラの高度な設定が必要となります。本章では、以下に示した一般的に使用される高度な設定について記載しています。

項目	説明
WLAN の一般的な設定	すべての管理対象アクセスポイントおよび無線コントローラにグローバルな設定を行います。
チャンネル計画と送信出力	チャンネルアルゴリズムと送信出力を設定します。
WDS 設定	無線ネットワークへの侵入を検出し、ネットワークを保護するために自動的にアクションを実行します。
Distributed トンネルの設定	Distributed トンネルの設定、トンネルクライアントに関する情報を表示します。
WLAN Visualization	無線ネットワークの情報を図式化して表示します。
AP ディスカバリ方式	無線コントローラとアクセスポイントの検出を行います。
管理対象のアクセスポイント	コントローラが管理するアクセスポイントをデータベースに追加、変更、削除します。
AP プロファイル	アクセスポイントのコンフィグレーションファイルを設定します。
WDS 設定	WDS の管理グループとそのリンクを設定します。
無線スケジュール機能	管理する AP の無線をタイムフレームで ON/OFF するスケジュールルールと、そのルールを管理するスケジュールプロファイルの設定を行います。
ピアグループ	ピアコントローラの設定を行います。
アクセスコントロースリスト（ACL）	「IP ACL」「MAC ACL」について設定します。
DiffServ 設定	「DiffServ」について設定します。
AP ファームウェアのアップグレード	アクセスポイントのファームウェアの更新を行います。

注意　ネットワークの概念と専門用語を理解している熟練したユーザのみ本章の手順を実行してください。

WLAN の一般的な設定

「WLAN Global Setup」、「AP Validation」および「Country Configuration」など、すべての管理対象アクセスポイントおよび無線コントローラに適用されるグローバルな設定を行います。

WLAN の基本設定

Wireless > General > General メニュー

WLAN の基本的な設定を行います。

1. **Wireless > General > General メニュー**の順にメニューをクリックし、以下の画面を表示します。

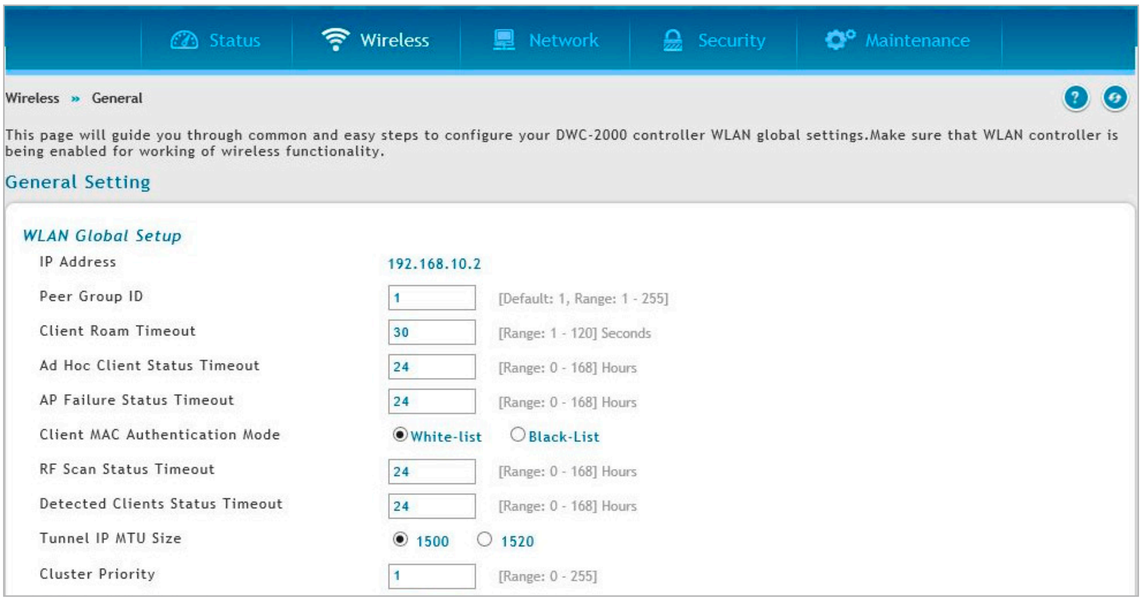


図 5-1　　General Setting 画面

2. 以下の項目を入力します。

項目	説明
WLAN Global Setup	
IP Address	無線コントローラの現在の IP アドレスを表示します。
Peer Group ID	大規模なネットワークを運用するために、クラスタ（ピアグループ）内で 8 台のコントローラまでピアとして無線コントローラを設定することができます。ピアコントローラ同士は、アクセスポイントに関する情報を共有することで L3 ローミングを実現します。ピアはグループ ID によりグループ分けされます。
Client Roam Timeout	クライアントとアクセスポイント間の接続が切れてから、「Associated Client Status」リストからエントリが削除されるまでの時間を指定します。リストには RF スキャンによる検出から経過した時間（Age）が表示され、その値がここで指定した値に到達した時に、エントリがリストから削除されます。
Ad Hoc Client Status Timeout	「Ad Hoc Client Status」リストにエントリを保持する時間を指定します。リストには RF スキャンによる検出から経過した時間（Age）が表示され、その値がここで指定した値に到達した時に、エントリがリストから削除されます。
AP Failure Status Timeout	「Ad Failure Client Status」リストにエントリを保持する時間を指定します。リストには RF スキャンによる検出から経過した時間（Age）が表示され、その値がここで指定した値に到達した時に、エントリがリストから削除されます。
Client MAC Authentication Mode	「White-list」または「Black-list」を選択します。
RF Scan Status Timeout	「RF Scan Status」リストにエントリを保持しておく時間を指定します。リストには RF スキャンによる検出から経過した時間（Age）が表示され、この値がこのフィールドで指定した値に到達した時にエントリがリストから削除されます。
Detected Clients Status Timeout	「Detected Client Status」リストにエントリを保持しておく時間を指定します。リストには RF スキャンによる検出から経過した時間（Age）が表示され、この値がこのフィールドで指定した値に到達した時にエントリがリストから削除されます。
Tunnel IP MTU Size	ネットワークに処理される IP パケットの最大サイズを指定します。MTU はトンネル VAP 上だけで実施されます。IP パケットがアクセスポイントと無線コントローラ間をトンネリングする場合、トンネルを通過中にパケットサイズは 20 バイトずつ増加します。これは、1500 バイトの IP MTU サイズに設定されているクライアントが、既存のネットワークインフラの最大 MTU サイズを超えて、1518（1522 のタグ付き）バイトのフレームに変換され、送信される可能性があることを意味します。トンネル IP MTU サイズを増やす場合、トラフィックが流れるポートに対して物理的な MTU を増やす必要があります。 **注意**　以下の条件を満たす場合、トンネル IP の MTU サイズを増やす必要はありません。 • 無線ネットワークは L3 トンネリングを使用しません。 • トンネリングモードは、通常小さいパケットを持つ音声トラフィックにだけ使用されます。 • トンネリングモードは、HTTP などの TCP ベースのプロトコルにだけ使用されます。これはすべての TCP 接続がトンネルに合うようにアクセスポイントが自動的に最大セグメントサイズを減少させるためです。

項目	説明
Cluster Priority	クラスタコントローラの選出のために本コントローラの優先度を指定します。クラスタ内で最も高い優先度を持つ無線コントローラがクラスタコントローラになります。優先度がすべての無線コントローラで同じである場合、最も低い IP アドレス値を持つ無線コントローラがクラスタコントローラになります。優先度 0 は、無線コントローラがクラスタコントローラになれないことを意味します。最も高い優先度は 255 です。
Detected Clients Delete	「ON」にすると定期的に自動検出された AP を削除します。初期値は無効です。
Detected Clients Delete Timeout	「Detected Clients Delete」の削除間隔（分）を指定します。
AP Client QoS	クライアント QoS 機能を有効または無効にします。無効にすると、クライアント QoS 設定はそのまま残りますが、無線トラフィックに適用されるどんな ACL または DiffServ ポリシーも実行されません。 クライアント QoS 機能は、無線コントローラのプライマリ QoS 機能を無線ドメインまで拡張します。より具体的には、アクセスコントロールリスト（ACL）と DiffServ ポリシーはアクセスポイントに接続する無線クライアントに適用されます。
Radius Authentication Server	AP クライアント認証に使用する認証 RADIUS サーバを指定します。
Radius Authentication Server Status	認証 RADIUS サーバの設定状況です。
AP Validation	
AP MAC Validation	無線コントローラがアクセスポイントを管理するためには、Valid AP データベースにアクセスポイントの MAC アドレスを追加します。これは、コントローラ上のローカルまたは外部 RADIUS サーバで保持されます。コントローラが他の無線コントローラの管理下にないアクセスポイントを検出すると、Valid AP データベースにあるアクセスポイントの MAC アドレスを検索します。データベースに MAC アドレスが存在すれば、コントローラはアクセスポイントの認証を行い、自分の管理対象とします。 アクセスポイントの認証に使用するデータベースを選択します。 ・Local - ローカルの Valid AP データベースに各アクセスポイントの MAC アドレスを追加します。 ・RADIUS - 外部 RADIUS サーバに各アクセスポイントの MAC アドレスを設定します。
Require Authentication Passphrase	本オプションを選択すると、アクセスポイントがコントローラと接続する前に認証が必要となります。また、スタンドアロンモードおよび Valid AP データベースにある場合、アクセスポイントにパスフレーズを設定する必要があります。スタンドアロンのアクセスポイントにパスフレーズを設定するためには、アクセスポイントの管理 Web UI にログインして、「Managed Access Points」画面に移動します。 ローカルなValid APデータベースにあるアクセスポイントにパスフレーズを設定するためには、「Basic Setup」画面から「Valid AP」タブをクリックします。次に、アクセスポイントの MAC アドレスをクリックして、「Authentication Password」フィールドにパスフレーズを入力します。認証を有効に設定すると、コントローラがアクセスポイントを認知した直後に認証を行います。
Manage AP with Previous Release Code	古いファームウェアを持つアクセスポイントを検出して、管理します。
Mutual Authentication	
Controller Provisioning Mode	有効にするとコントローラはプロビジョニングメッセージを送受信できるようになります。セキュリティ機能としてコントローラの本機能を無効にすることも可能です。本モードが無効の場合、プロビジョニングメッセージは送受信されません。
Network Mutual Authentication Mode	有効にすると無線ネットワークにおける相互認証が必要になります。無効にすると相互認証は不要になります。本項目の変更はクラスタ内の全管理 AP/ コントローラの設定を自動的にアップデートします。有効にするとコントローラプロビジョニングによる新規コントローラのクラスタ追加が可能になります。無効にするとクラスタは新しいコントローラから、証明書を受信しなくなります。
Unmanaged AP Reprovisioning Mode	有効にすると、管理されていない AP の再プロビジョニングが可能になります。 本項目の変更はクラスタ内の全管理 AP/ コントローラの設定を自動的にアップデートします。本機能は「Network Mutual Authentication Mode」が有効な場合にのみ、設定可能です。
Country Configuration	
Country Code	コントローラとアクセスポイントを運用する国を示す国コードを選択します。無線通信に関する規則は国ごとに異なります。正しい国コードを選択し、WLAN システムが運用される国の規則を遵守するようにしてください。

3. 「Save」ボタンをクリックして、コントローラの設定を更新します。

チャンネル計画と送信出力

無線コントローラには、RF 干渉を最小限に抑えるために、各アクセスポイントがどの RF チャンネルを使用すべきかを自動で判断する、チャンネルプランアルゴリズムがあります。チャンネルプランアルゴリズムを有効にすると、無線コントローラは、管理下にある各アクセスポイントが使用しているチャンネルを定期的に評価し、現在のチャンネルに干渉が認められる場合には、そのチャンネルを変更します。

チャンネル計画の設定

Wireless > General > Channel Algorithm メニュー

チャンネルアルゴリズムを設定する手順は以下の通りです。

1. Wireless > General > Channel Algorithm > Channel Setting の順にメニューをクリックし、以下の画面を表示します。

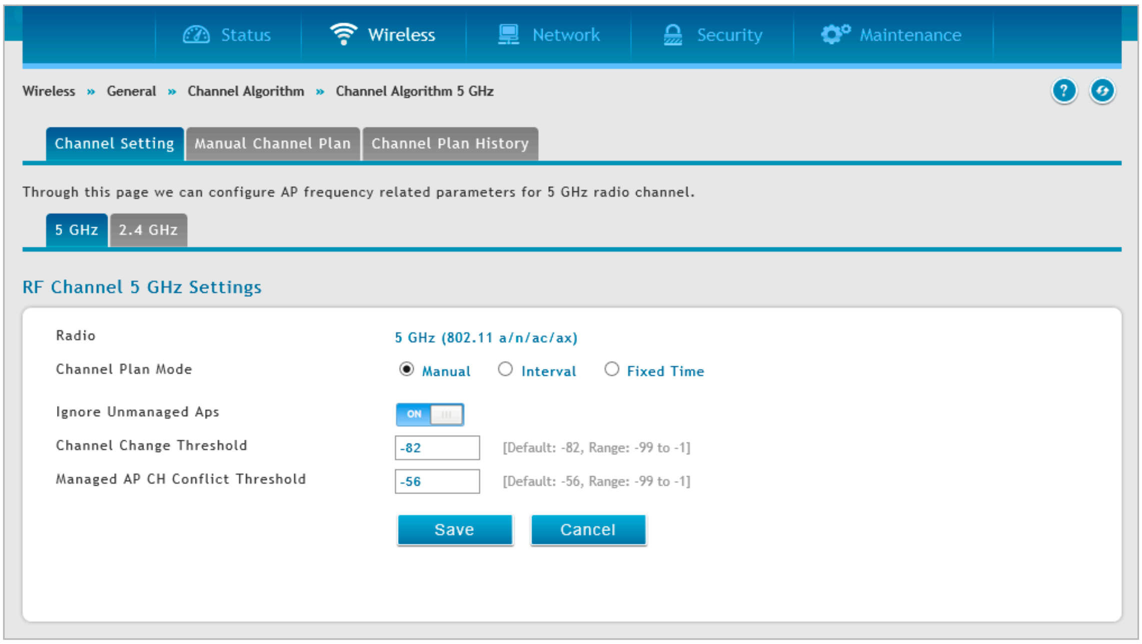


図 5-2　　RF Channel Settings 画面 - Manual

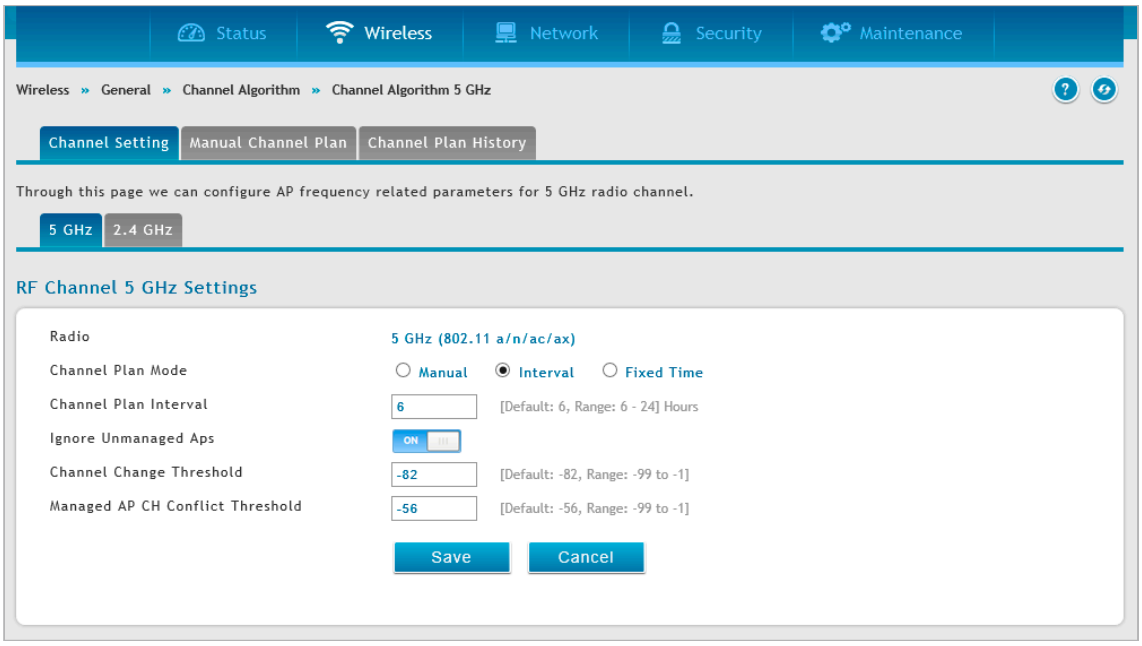


図 5-3　　RF Channel Settings 画面 - Interval

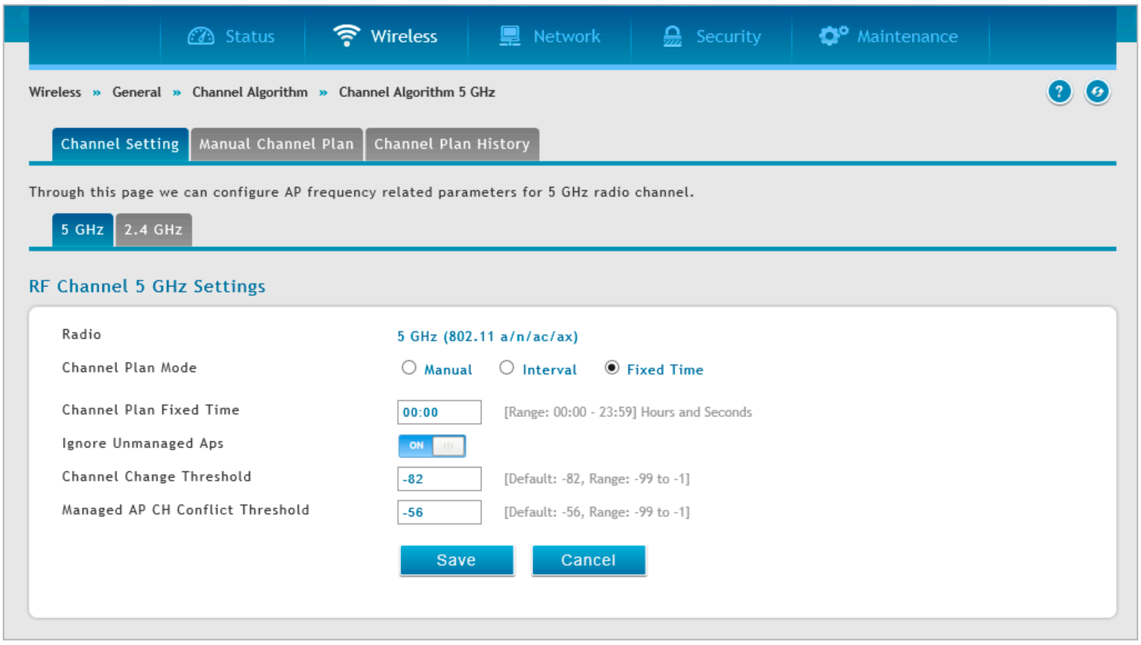


図 5-4　　RF Channel Settings 画面 - Fixed Time

以下の項目があります。

項目	説明
Radio	各アクセスポイントは 2.4GHz と 5GHz の周波数帯で動作できるデュアルバンド（またはトライバンド）です。「5GHz」「2.4GHz」タブで選択した内容によって、無線の接続モードが表示されます。
Channel Plan Mode	チャンネルプランのモードを選択します。 • Manual - チャンネルプランの計算と割り当てを手動で制御および開始します。手動でチャンネルプランアルゴリズムを実行し、アクセスポイントに適用します。 • Interval - コントローラは定期的にチャンネルプランを計算して適用します。実行間隔を 6~24 時間の間で指定します。実行間隔は、「Save」ボタンをクリックした時からカウントされます。 • Fixed Time - チャンネルプランとチャンネル割り当ての時間を指定します。1 日のうちの指定した時刻に実行されます。
Channel Plan Interval	「Channel Plan Mode」で「Interval」を指定した場合、チャンネルプランの計算と割り当てを実行する間隔（6~24 時間）を指定します。
Channel Plan Fixed Time	「Channel Plan Mode」で「Fixed Time」を指定した場合、チャンネルプランの計算と割り当てを実行する時刻を指定します。1 日のうちの本フィールドで指定した時刻に実行されます。
Ignore Unmanaged APs	コントローラがその無線帯域に対してチャンネルを決定する場合、クラスタが管理するアクセスポイントだけに注意を払うべきか、または検出したアクセスポイントのすべてに注意を払うべきか指定します。初期値は有効です。
Channel Change Threshold	現在の動作チャンネルを再評価するための、検出した Neighbor の信号強度（-99 ～ 1dBm）を設定します。 同じチャンネルで動作する Neighbor アクセスポイントがこのしきい値を下回る信号を持っていることを動作チャンネルが検出すると、アクセスポイントはその無線帯域で新しいチャンネルを選択することはありません。このしきい値の初期値：-82dBm
Managed AP CH Conflict Threshold	コントローラのチャンネル干渉の計算が行われると、アクセスポイントは、無線電波をより干渉の少ないチャンネルに変更するように準備します。近接する 2 つ以上のアクセスポイントが、同時に同じチャンネルに変更されることを回避するために、信号強度が「Managed AP CH conflict Threshold」を上回るアクセスポイントが近接する場合、アクセスポイントはチャンネルの変更をキャンセルします。

2. 「Save」ボタンをクリックします。

Manual Channel Plan タブ

「Channel Plan Mode」で「Manual」を選択した場合、「Manual Channel Plan」タブをクリックします。ここで、選択したアクセスポイントにチャンネルアルゴリズムを適用および開始できます。

Channel Plan History タブ

コントローラがアクセスポイントの 2.4GHz および 5GHz 帯域で自動チャンネル調整アルゴリズムを使用しているか否かを示します。

送信出力設定

Wireless > General > Power Algorithm メニュー

アクセスポイントの無線送信出力は、AP プロファイル、ローカルデータベース、または RADIUS サーバで指定できます。AP プロファイルの送信出力レベルは、アクセスポイントの初期値のレベルであり、送信出力は AP プロファイルの値以下には調整されません。ローカルデータベースと RADIUS サーバの設定は、常にプロファイルの設定より優先されます。手動で送信出力をセットした場合は、その値が固定され、そのアクセスポイントでは自動送信出力アルゴリズムを使用できなくなります。

チャンネルアルゴリズムを設定する手順は以下の通りです。

1. **Wireless > General > Power Algorithm > Power Setting** の順にメニューをクリックし、以下の画面を表示します。

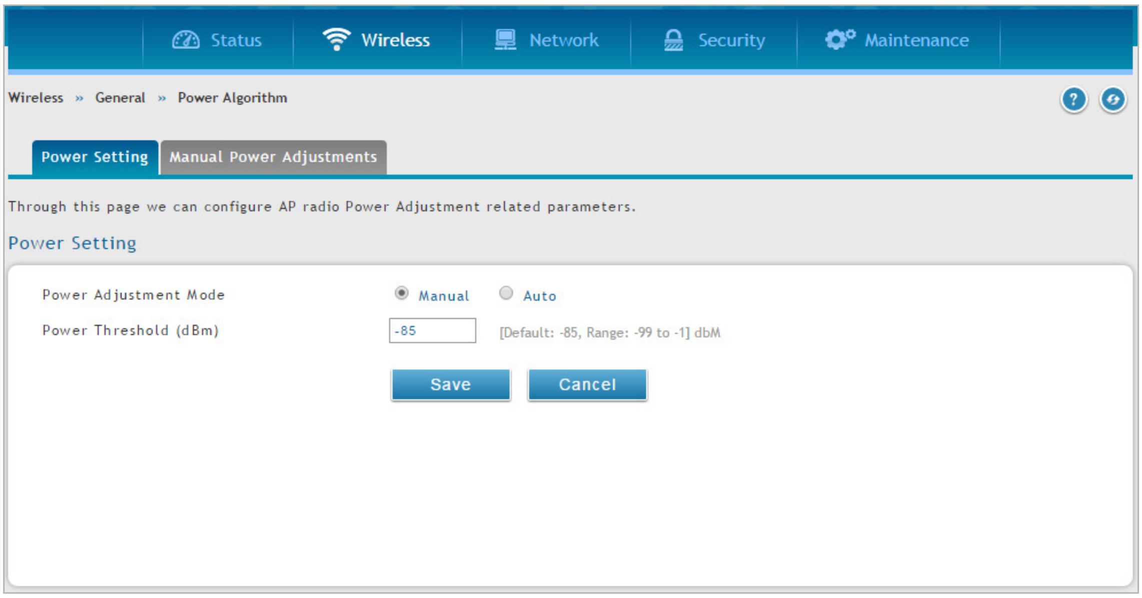


図 5-5　　Power Setting 画面

2. 最大送信出力が、規制範囲（地域）やハードウェアの性能により、チャンネルに許可される最低の電力レベルになるように、最大送信出力のパーセンテージ（%）単位で設定できます。「Manual」または「Auto」モードを選択します。

3. 送信出力の変更のしきい値を入力します。初期値は -85dBm です。Neighbor の無線電波が、しきい値と同じかそれ以上の信号強度を持った送信無線電波を受信した場合にだけ、送信出力の変更を始動します。しきい値を下回る信号は無視されます。

4. 「Manual」を選択した場合、「Manual Power Adjustments」タブをクリックします。 ここで、選択したアクセスポイントに電力アルゴリズムを適用および開始できます。

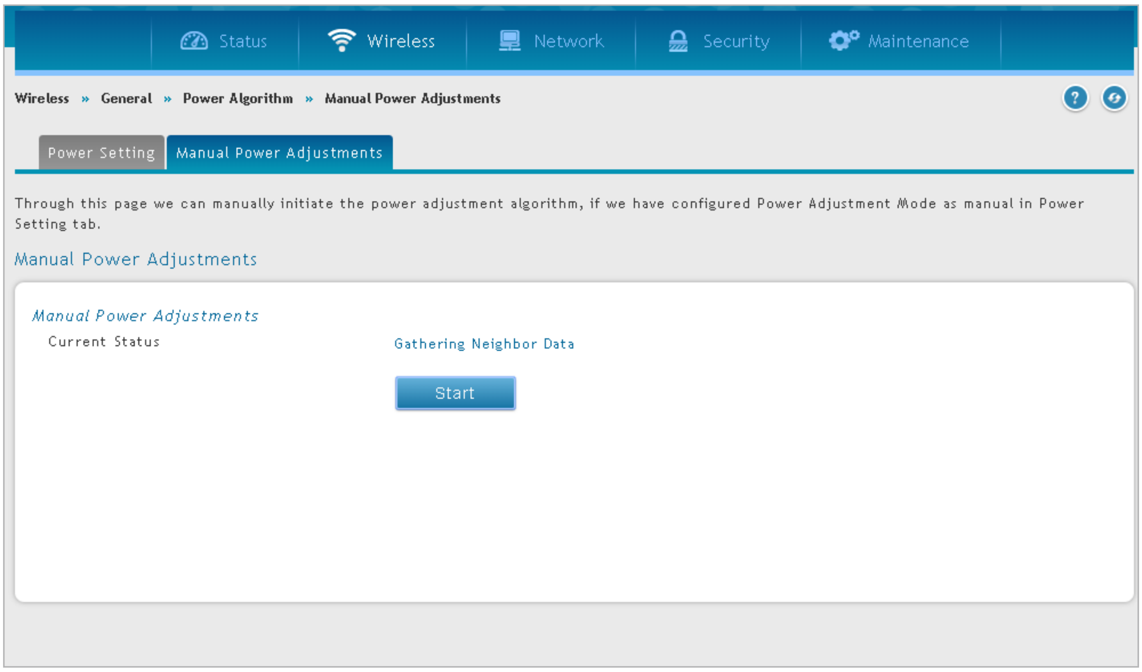


図 5-6　　Manual Power Adjustments 画面

WIDS 設定

Wireless Intrusion Detection システム（WIDS）は、無線ネットワークへの侵入の試みを検出するのを補助し、ネットワークを保護するために自動的にアクションを実行することができます。

AP WIDS の設定

Wireless > General > WIDS > AP WIDS Security メニュー

無線ネットワークにおいて不正なアクセスポイントの検出を補助するために、様々な脅威検知に対するテストのアクティブ化の有無、および脅威検知のしきい値の設定を行います。これらの変更はネットワークの接続を中断しないで行うことができます。いくつかの処理はアクセスポイント側で実行されるため、WIDS の操作プロパティを変更するためにコントローラからアクセスポイントにメッセージを送信する必要があります。

注意 「AP WIDS Security」画面の分類設定は、コントローラにおけるグローバルなコンフィグレーションの一部であり、そのコンフィグレーションを同期させるために手動で他のコントローラにもプッシュする必要があります。

多くのテストでは、管理 SSID を通知しているにもかかわらず実際は管理されていないアクセスポイントを識別することに焦点が当てられています。こうしたアクセスポイントが検出されるということは、ネットワークが誤って設定されているか、またはハッカーがパスワードや他のセキュアな情を集めようとしてハニーポットアクセスポイントを設定したことを意味します。

運用モードの無線電波においてほとんどの脅威を検出することが可能ですが、管理 AP 周波数帯とは別のチャンネルで潜在的に不正なアクセスポイントが動作する場合には特に、sentry モードで脅威をより早く見つけることができます。ネットワーク内の各地域に対して sentry 無線電波でカバーされるように、十分な数の sentry 無線電波を提供する必要があります。不正または信号の干渉の測定を改善するためには、sentry の配置の密度をより高くすることが望ましいかもしれません。

WIDS AP の設定手順は以下の通りです。

1. **Wireless > General > WIDS > AP WIDS Security** の順にメニューをクリックし、以下の画面を表示します。

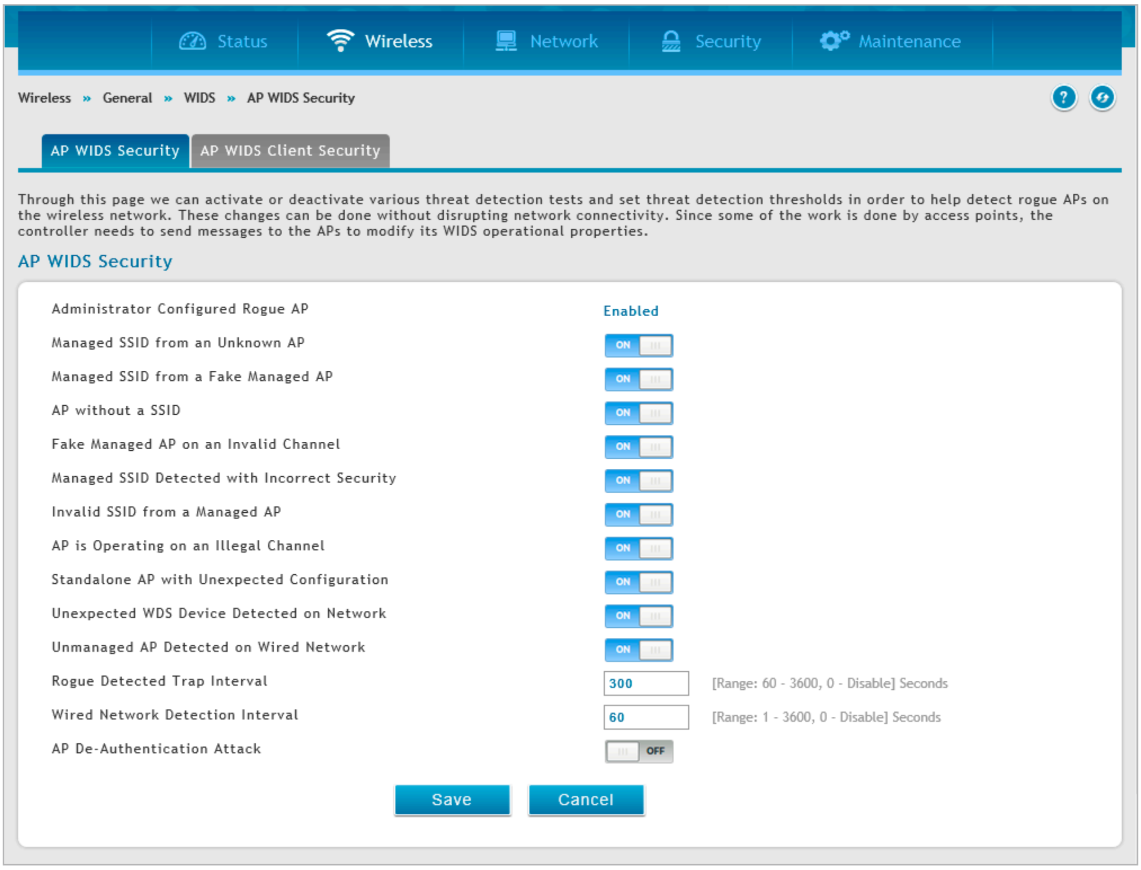


図 5-7　　AP WIDS Security 画面

以下の項目があります。

項目	説明
Administrator Configured Rogue AP	送信元 MAC アドレスが、コントローラまたは RADIUS サーバの Valid-AP データベースにあり、AP タイプが Rogue としてマークされる場合、アクセスポイントの状態は「Rogue」です。
Managed SSID from an Unknown AP	未知のアクセスポイントが管理ネットワーク SSID を使用しているかどうかチェックします。ハッカーは、管理 SSID を持つアクセスポイントを設定することでユーザをだましてアクセスポイントへ接続し、パスワードや他のセキュアな情報を暴くかもしれません。複数のクラスタを使用している大規模ネットワークの管理者は、各クラスタで異なるネットワーク名を使用するか、またはこのテストを無効にするべきです。そうでないと、最初のクラスタが 2 番目のクラスタに対して、最初のクラスタのアクセスポイントと同じ SSID を送信するアクセスポイントを検出すると、これらのアクセスポイントは「Rogue」（不正）として報告されます。
Managed SSID from a Fake Managed AP	ハッカーは、管理アクセスポイントの 1 つと同じ MAC アドレスでアクセスポイントを設定し、また、その管理 SSID の 1 つを送信するように設定します。このテストは、管理アクセスポイントが通常送信するビーコンのベンダフィールドをチェックします。ベンダフィールドが存在しない場合、アクセスポイントは偽のアクセスポイントとして確認されます。
AP without a SSID	SSID はビーコンフレームのオプションフィールドです。ハッカーは検出されることを回避するために、管理されたネットワークの SSID をアクセスポイントに設定し、ビーコンフレームの SSID 伝送を無効にするかもしれません。アクセスポイントは、クライアントがハッカーのアクセスポイントに接続するように偽装している管理 SSID に対してプローブ要求を送信するクライアントにプローブ応答を送信し続けます。このテストでは、SSID フィールドのないビーコンを送信するアクセスポイントを検出して、フラグを付けます。プロファイル内の無線インタフェースのいずれかが「SSID」を送信しないように設定されていると、このテストは自動的に無効になります。これは、実際にはセキュリティを提供せず、本テストを無効にするため推奨されません。
Fake Managed AP on an Invalid Channel	このテストでは管理対象のアクセスポイントのうち 1 台の送信元 MAC アドレスからビーコンを送信する不正なアクセスポイントを検出します。このアクセスポイントは、管理対象アクセスポイントが動作すると想定されるチャンネルとは異なるチャンネルで検出されます。
Managed SSID Detection with Incorrect Security	アクセスポイントは、RF スキャン中に他のアクセスポイントから受信したビーコンフレームを検証して、検出されたアクセスポイントがオープン中のネットワーク、WEP、または WPA を通知しているかどうか判断します。RF スキャンで報告された SSID が、管理されたネットワークの 1 つであり、セキュリティ設定が検出されたセキュリティと一致していないと、本テストは、アクセスポイントを Rogue（不正）としてマークします。
Invalid SSID from a Managed AP	既知の管理対象のアクセスポイントが予期しない SSID を送信しているかどうかをチェックします。RF スキャンで報告された SSID は、管理対象のアクセスポイントに割り当てられたプロファイルが使用する、すべての SSID コンフィグレーションのリストと比較されます。検出された SSID が設定済みのどの SSID にも一致しないと、アクセスポイントを Rogue（不正）としてマークします。
AP Is Operating on an Illegal channel	無線システムが設定される国では合法ではないチャンネルで動作する、不正に設定されたデバイスやハッカーを検出します。 **注意** 無線システムでこの脅威を検出するためには、無線ネットワークは sentry モードで動作する 1 個以上の周波数帯域を持つ必要があります。
Standalone AP with Unexpected Configuration	アクセスポイントが既知のスタンドアロンアクセスポイントとして分類される場合、コントローラは、アクセスポイントが想定される設定パラメータを使用して動作しているかどうかチェックします。ローカルまたは RADIUS Valid AP データベースにスタンドアロンアクセスポイントで想定されるパラメータを設定します。このテストは潜在的な侵入試みと共にネットワークの構成ミスを検出する可能性があります。以下のパラメータがチェックされます。 ・Channel Number ・SSID ・Security Mode ・WDS Mode ・Presence on a wired network
Unexpected WDS Device Detected on Network	アクセスポイントが、「Managed AP」または「Unknown AP」として分類され、WDS（Wireless Distribution System）トラフィックがアクセスポイントで検出される場合、アクセスポイントは「Rogue」（不正）と見なされます。WDS モードで明示的に動作が許可されているスタンドアロンのアクセスポイントのみ、このテストで「Rogue」（不正）として報告されません。
Unmanaged AP Detected on Wired Network	アクセスポイントが有線ネットワークで検出されるかどうかチェックします。アクセスポイントの状態が「Unknown」であれば、テストはこれを「Rogue」（不正）に変更します。アクセスポイントが有線ネットワークで検出されるかどうかを示すフラグは、RF スキャンレポートの一部として報告されます。アクセスポイントが管理されていて、ネットワークで検出されると、コントローラは、単にこの事実を報告して、アクセスポイントの状態を「Rogue」（不正）に変更しません。無線システムでこの脅威を検出するためには、無線ネットワークは sentry モードで動作する 1 個以上の無線帯域を持つ必要があります。
Rogue Detected Trap Interval	不正なアクセスポイントが RF スキャンデータベースに存在している場合に管理者に通知する SNMP トラップの伝送間隔（秒）を指定します。値に 0 を設定すると、トラップは送信されません。
Wired Network Detection Interval	新しい有線ネットワーク検出サイクルを開始するまで、アクセスポイントが待機する時間（秒）を指定します。値に 0 を設定すると、有線ネットワーク検出は無効になります。
AP De-Authentication Attack	アクセスポイント認証解除攻撃を有効または無効にします。無線コントローラは、認証解除メッセージを不正なアクセスポイントに送信することで、不正なアクセスポイントから防御できます。無線システムが本機能を動作するためには、認証解除機能をグローバルに有効にする必要があります。攻撃機能を有効にする前に、正当なアクセスポイントが「Rogue」として分類されていないことにご注意ください。本機能は初期値では「OFF」（無効）になっています。

2.　セキュリティオプションを有効または無効にして、「Save」ボタンをクリックします。

クライアントの WIDS 設定

Wireless > General > WIDS > AP WIDS Client Security メニュー

Wireless Intrusion Detection システム（WIDS）は、無線ネットワークへの侵入の試みを検出するために利用され、ネットワークを保護するために自動的にアクションを実行することができます。「AP WIDS Client Security」画面で行う設定は、検出されたクライアントが不正として分類されるかどうかの決定を行うために役に立ちます。不正として分類されたクライアントは、ネットワークセキュリティへの脅威であると見なされます。

注意 「AP WIDS Client Security」画面の（脅威の）分類設定は、コントローラにおけるグローバルなコンフィグレーションの一部であり、そのコンフィグレーションを同期させるように手動で他のコントローラにも行われる必要があります。

一般的な接続と認証プロセスの一部として、無線クライアントは 802.11 の管理メッセージをアクセスポイントに送信します。
WIDS 機能は、各検出クライアントが送信する以下に示す管理メッセージのタイプを追跡します。

- プローブ要求
- 802.11 認証要求
- 802.11 認証解除要求

管理トラフィックを使用してネットワークをフラッドすることで、クライアントがネットワークに脅威を引き起こしているかどうか判断するために、システムはアクセスポイントが各タイプのメッセージを受信した回数、および 1 つの RF スキャンレポートに検出された最も高いメッセージレートを追跡します。「AP WIDS Client Security」画面では、送信される各メッセージタイプのしきい値を設定し、アクセスポイントはクライアントがこのしきい値を超えていないかどうか監視またはテストします。

WIDS クライアントの設定手順は以下の通りです。

1. **Wireless > General > WIDS > AP WIDS Client Security** の順にメニューをクリックし、以下の画面を表示します。

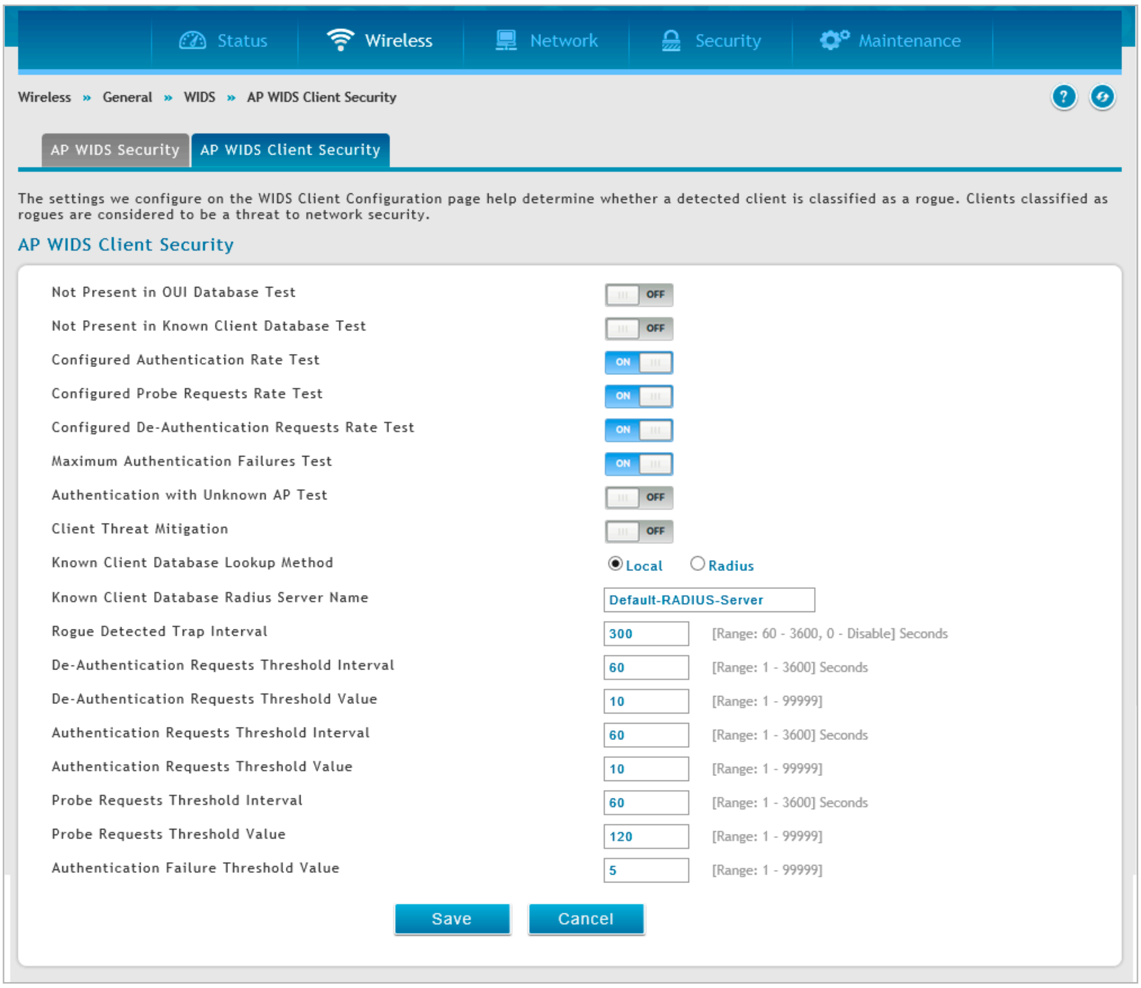


図 5-8　　AP WIDS Client Security 画面

以下の項目があります。

項目	説明
Not Present in OUI Database Test	クライアントの MAC アドレスが OUI データベースで特定される定義済みメーカのものであるかどうかをチェックします。
Not Present in Known Client Database Test	MAC アドレスによって特定されるクライアントが、Known Client データベースに表示され、Authentication Action の Grant、または、ホワイトリストのグローバルアクションのいずれかを通じてアクセスポイントへのアクセスを許可されるかどうかをチェックします。クライアントが Known Client データベースにあり、Deny の機能を持つ場合、または、動作がグローバルアクションであり、それがブラックリストにグローバルに設定される場合、クライアントはこのテストに失敗します。
Configured Authentication Rate Test	クライアントが 802.11 認証要求の送信のための設定レートを超えているかどうかチェックします。
Configured Probe Requests Rate Test	クライアントがプローブ要求の送信のための設定レートを超えているかどうかチェックします。
Configured De-Authentication Requests Rate Test	クライアントが認証解除要求の送信のための設定レートを超えているかどうかチェックします。
Maximum Authentication Failures Test	クライアントが認証失敗の最大数を超えているかどうかチェックします。
Authentication with Unknown AP Test	Known Client データベースのクライアントが Unknown（未知）のアクセスポイントで認証されるかどうかをチェックします。
Client Threat Mitigation	• ON - Known Clients データベースに存在し、Unknown（未知）のアクセスポイントに接続しているクライアントに認証解除メッセージを送信します。脅威の軽減のために Unknown AP の認証テストを有効にする必要があります。 • OFF - Known Clients データベース内のクライアントは、Unknown（未知）のアクセスポイントで認証されたままとなります。
Known Client Database Lookup Method	コントローラがネットワークでクライアントを検出する場合に、Known Client データベースの検索を実行します。コントローラがこれらの検索にローカル（Local）または RADIUS データベースを使用するべきかどうかを指定します。
Known Client Database Radius Server Name	Known Client データベースの検索方法が RADIUS の場合、本フィールドには RADIUS サーバ名を指定します。
Rogue Detected Trap Interval	不正なアクセスポイントが RF スキャンデータベースに存在していると管理者に通知する SNMP トラップの伝送間隔（秒）を指定します。値に 0 を設定すると、トラップは送信されません。
De-Authentication Requests Threshold Interval	無線クライアントが送信した認証解除メッセージをアクセスポイントがカウントする時間（秒）を指定します。
De-Authentication Requests Threshold Value	しきい値の間にコントローラがここで指定したメッセージよりも多く受信すると、テストが始動します。
Authentication Requests Threshold Interval	無線クライアントが送信した認証メッセージをアクセスポイントがカウントする時間（秒）を指定します。
Authentication Requests Threshold Value	しきい値の間に、コントローラがここで指定したメッセージよりも多く受信すると、テストが始動します。
Probe Requests Threshold Interval	無線クライアントが送信したプローブメッセージをアクセスポイントがカウントする時間（秒）を指定します。
Probe Requests Threshold Value	イベントが脅威として報告される前に、無線クライアントがしきい値の間に送信を許可されるプローブ要求数を指定します。
Authentication Failure Threshold Value	イベントが脅威として報告される前に、無線クライアントがしきい値の間に許可される 802.1X 認証エラー数を指定します。

2.　セキュリティオプションを有効または無効にして、「Save」ボタンをクリックします。

Distributed トンネル

Distributed Tunneling モードは AP-AP トンネリングモードとしても知られ、どんなデータも無線コントローラに送信せずに無線クライアント用に L3 ローミングをサポートするために使用されます。

AP-AP トンネリングモードで、クライアントが最初に無線システム内のアクセスポイントに接続する場合、アクセスポイントは、VLAN のフォワーディングモードを使用することで無線クライアントのデータを転送します。クライアントが最初に接続するアクセスポイントはホーム AP です。クライアントがローミングするアクセスポイントはアソシエーション AP です。

クライアントが異なるサブネットで別のアクセスポイントにローミングする場合、CAPWAP L2 トンネルを使用することでアソシエーション AP はすべてのトラフィックをクライアントからホーム AP までにトンネリングします。ホーム AP はトンネルを経由してトラフィックを有線ネットワークにフローします。クライアントが同じサブネットで別のアクセスポイントにローミングする場合、トンネルは作成されず、新しいアクセスポイントはクライアント用のホーム AP になります。

Distributed トンネルの設定

Wireless > General > Distributed Tunnels メニュー

1. **Wireless > General > Distributed Tunnels** の順にメニューをクリックし、以下の画面を表示します。

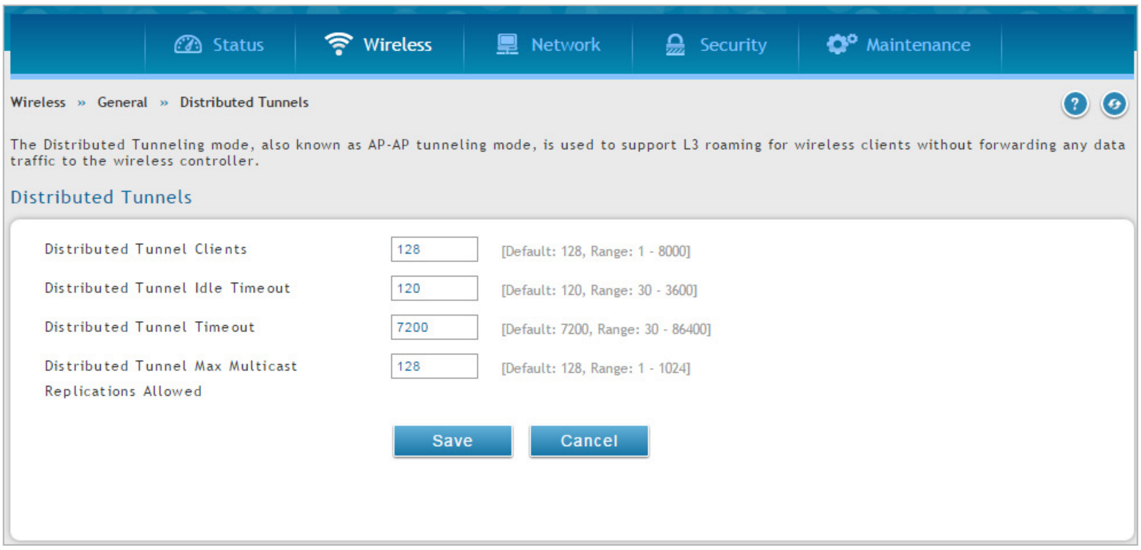


図 5-9　　Distributed Tunnels 画面

2. 以下の設定を行います。

項目	説明
Distributed Tunnel Clients	ホーム AP から同時に移動できる分散型トンネリングを行うクライアントの最大数を指定します。
Distributed Tunnel Idle Timeout	クライアントへのトンネルが終了し、クライアントが強制的に IP アドレスを変更されるまでのクライアントの無通信時間（秒）を指定します。
Distributed Tunnel Timeout	ローミングクライアントへのトンネルが終了し、クライアントが強制的に IP アドレスを変更されるまでの時間（秒）を指定します。
Distributed Tunnel Max Multicast Replications Allowed	マルチキャストフレームがホーム AP にコピーされるトンネルの最大数を指定します。

3. 「Save」ボタンをクリックします。

WLAN Visualization

WLAN Visualization（WLAN 視覚化）は、Web ブラウザを通じて無線ネットワークを図で表示するツールです。

画像のアップロード

Wireless > General > WLAN Visualization Image メニュー
オフィスの見取り図などの画像をアップロードし、アクセスポイントやコントローラの配置図をします。

推奨する画像ファイル形式：
- GIF
- JPG

アクセスポイントや無線コントローラを示すアイコンを見やすくするため、アップロードする画像はモノクロのものをお勧めします。

画像の登録

1. **Wireless > General > WLAN Visualization Image** の順にメニューをクリックし、以下の画面を表示します。

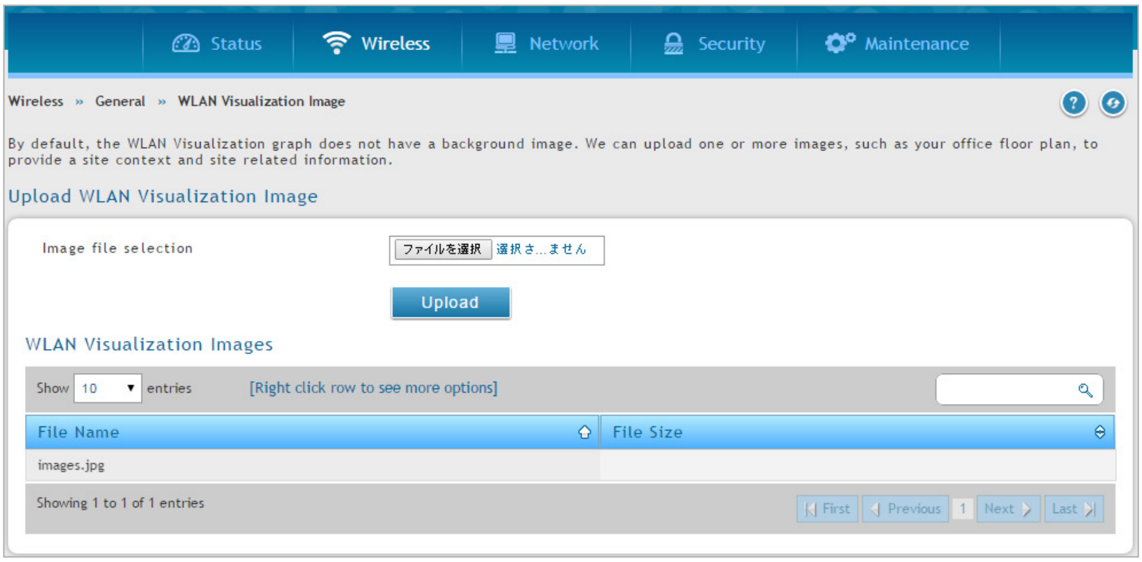


図 5-10　Upload VLAN Visualization Image 画面

2. 「Image file selection」で「ファイルを選択」をクリックします。

3. ファイルを選択して、「開く」をクリックします。

4. 「Upload」ボタンをクリックして、画像ファイルを登録します。登録に成功すると、「WLAN Visualization Images」に表示されます。

画像の削除

1. 削除する画像のファイル名上で右クリックします。複数の画像をすべて削除する場合は「Select All」にチェックを入れます。
2. 「Delete」をクリックします。

起動

Wireless > General > WLAN Visualization

1. **Wireless > General > WLAN Visualization** の順にメニューをクリックして WLAN Visualization ツールを起動します。

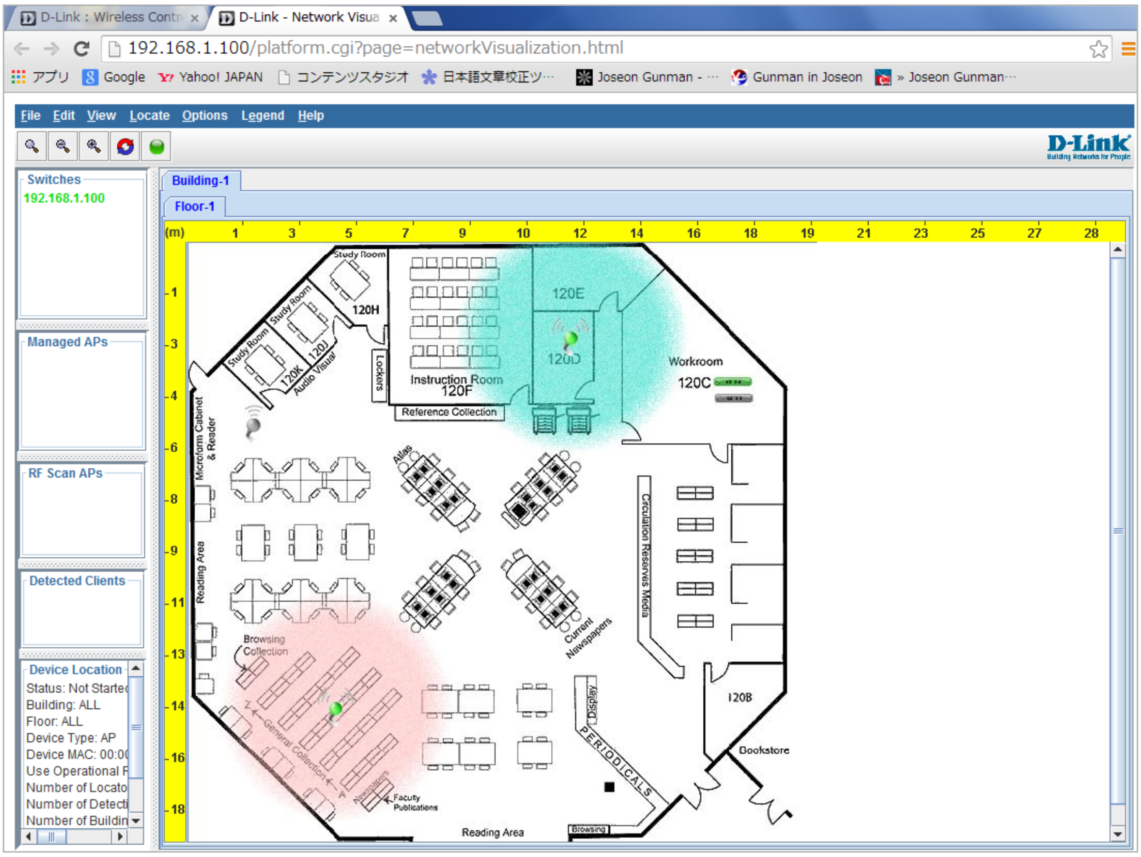


図 5-11　 WLAN Visualization 画面

新しいブラウザ画面が開き、アクセスポイントと無線コントローラの配置を表す図を作成できます。

メニューバー

図 5-12　D-Link WLAN Visualization 用のメニューバー

以下の表は、WLAN Visualization ツールで使用できるメニューの概要です。

メニュー項目		説明
File	Force refresh.	手動で更新し、Java クライアントアプリケーションを再同期します。グラフの編集後、本メニューを実行して、画面を更新します。
	Reconnect and Refresh	クライアントアプリケーションを一旦コントローラから切断して、再接続します。
	Exit	WLAN Visualization アプリケーションを終了します。
Edit	New Graph	新規のグラフを作成し、グラフ名、背景画像、縮尺を設定するための画面を開きます。
	Edit Graph	作成済みのグラフを開きます。背景画像と縮尺は変更可能ですが、グラフ名を変更するためには、新規のグラフを作成する必要があります。
	Delete Graph	作成済みのグラフを削除します。本項目を選択すると、本当に削除を実行するかどうか確認するダイアログボックスが表示されます。
	Image Management	使用可能な背景画像のリストを表示します。また、画像の削除も本項目から行います。

メニュー項目		説明
View	Ungraphed Components	左区画の図示化されていないコンポーネント群の表示方法を選択します。 • Tab View - 1 種類のコンポーネントのみを表示し、他の種類をタブにまとめて表示します。 • List View - すべての種類のコンポーネントを表示します。
	AP Power Display	アクセスポイントの出力エリアイメージを選択します。 • Disable Power Display - 出力エリアイメージの表示を行いません。 • Show 5GHz Band - 5GHz で動作している無線インタフェースの出力エリアイメージを表示します。 • Show 2.4GHz Band - 2.4GHz で動作している無線インタフェースの出力エリアイメージを表示します。 出力エリアイメージのサイズは、無線インタフェースの送信出力に基づき、3 種類（低、中、高）が用意されています。また、そのサイズは現在使用している背景画像の倍率にも依存します。 1 つのモードがアクセスポイントの 2 つの無線インタフェースに設定されている場合は、2 つの出力エリアイメージが表示されます。 **注意** 出力エリアイメージの色は、接続に使用するチャンネルによって異なります。 もし、2 台のアクセスポイントが、お互いの伝送範囲内において同じチャンネル（または近隣のチャンネル）を使用していれば、アクセスポイント同士が干渉し合い、無線クライアントの通信品質は悪くなります。そのような干渉を防ぐために、以下のいずれかを実行してください。 • アクセスポイントの送信出力を低く設定する。 • アクセスポイント同士を物理的に離して設置する。 • アクセスポイント上で自動チャンネル調整アルゴリズムを使用する。または干渉を起こさないように手動でチャンネルを調整する。 **警告** 出力エリアイメージは例示を目的としており、あくまでもイメージです。実際の電力分布は、オフィスの壁などの伝播特性やバックグラウンドの RF ノイズなどにより異なります。
Locate	Target Access Point	本オプションを選択すると、無線システムはアクセスポイントを検索し、受信した検索情報を元に位置を更新します。また、検索するアクセスポイントの MAC アドレスの選択や位置検索パラメータの指定を行う画面が開きます。
	Target Client	本オプションを選択すると、無線システムはクライアントを検索し、受信した検索情報を元に位置を更新します。また、検索するクライアントの MAC アドレスの選択や位置検索パラメータの指定を行う画面が開きます。
Options	Show Managed APs	グラフにアクセスポイントを表示するかどうか指定します。チェックボックスのチェックを外すと、見えなくなりますが、オブジェクトはグラフからなくなりません。
	Show RF Scan APs	グラフ上に RF スキャンにより検出されたアクセスポイントを表示するかどうかを指定します。チェックボックスのチェックを外すと、見えなくなりますが、オブジェクトはグラフからなくなりません。
	Show Managed AP Clients	グラフ上にアクセスポイントと接続中のクライアントを表示するかどうかを指定します。チェックボックスのチェックを外すと、見えなくなりますが、オブジェクトはグラフからなくなりません。
	Show Detected Clients	選択すると検出された無線クライアントを表示します。チェックボックスのチェックを外すと、見えなくなりますが、オブジェクトはグラフからなくなりません。
	Show Location Result	グラフ上の点または円のソリューションを表示します。ポイントと円のソリューションでは、検索の結果として予測されるデバイスの位置を示しています。
Legend	Images	WLAN コンポーネントとアイコンの対応を表示します。
	Channel Color	伝送に使用されているチャンネルと、出力エリアイメージで使用する色の対応を表示します。

「Legend」メニューについて

「Legend」メニューでは、グラフ上に表示されるアイコンと、アイコンの色についての情報を確認できます。
「Images」を選択すると、グラフ上で各 WLAN コンポーネントを表すアイコンを表示します。

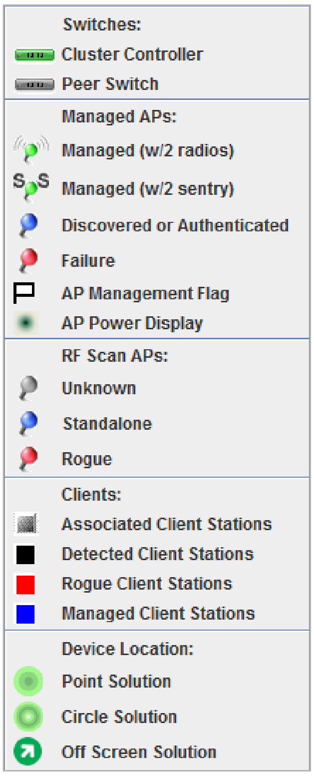


図 5-13　アイコンの凡例

アクセスポイントのアイコンの色は以下の状態を表します。

- 青 -（Discovered or Authenticated）無線コントローラに検出されましたが、管理はされていません。認証待ち、または認証済でも設定がされていない状態です。
- 緑 -（Managed）AP プロファイルが適用されており、「Managed」モードで動作中です。
- 赤 -（Failure）無線コントローラとの通信が切断されました。アクセスポイントが再起動中であるか、または認証に失敗しました。

「Sentry」モードでの動作中は、以下の通りアクセスポイントのアイコンのアンテナが「S」という文字に変わって表示されます。

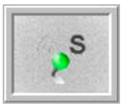


図 5-14 「Sentry」モード - 詳細図

「Sentry」モード中は、アクセスポイント周囲の出力イメージはグレーで表示されます。
チャンネルカラーの凡例では、出力イメージと各チャンネルを表す色の対応を示します。無線インタフェースが通信に使用している各チャンネルはそれぞれ色が割り当てられています。利用できるチャンネルは、無線モードおよび国によって異なります。

図 5-15　チャンネルの色

使用中のチャンネルを表示するためには、管理対象のアクセスポイント上にマウスをポイントして、ポップアップ画面を表示させます。画面中に使用中のチャンネルを含む、アクセスポイントの諸情報が確認できます。

AP ディスカバリ方式

無線コントローラとアクセスポイントは、以下の方式を使用して相互に検出を行います。

- レイヤ 2 検出
- アクセスポイントの IP アドレスを無線コントローラに登録
- 無線コントローラの IP アドレスをアクセスポイントに登録

L2/ VLAN ディスカバリ

アクセスポイントと無線コントローラが直接接続されるか、同じレイヤ 2 ブロードキャストドメインにあり、デフォルト VLAN 設定を使用する場合、無線コントローラは、L2 ディスカバリメッセージのブロードキャストを通して自動的にアクセスポイントを発見します。レイヤ 2 でのデバイス検出は、デバイスが直接接続された時、またはレイヤ 2 ブリッジを使用して接続された時に自動的に実行されます。最大 16 個の VLAN で検出プロトコルを有効にすることができます。

初期値では、VLAN1 はアクセスポイントで有効で、無線コントローラにおける検出も有効になっています。無線コントローラとアクセスポイントが同じレイヤ 2 マルチキャストドメインに存在している場合、AP 検出を有効にする操作は必要ありません。また、無線コントローラは L2/VLAN 検出を使用して、L2 マルチキャストドメインでピアコントローラを検索します。

アクセスポイントは、管理用 VLAN からの Discovery メッセージのみを処理します。また、アクセスポイントは無線メディアへの Discovery メッセージ転送は行いません。

L2/VLAN ディスカバリの検出状況

Wireless > Access Point > AP List メニュー

無線コントローラからアクセスポイントとピアコントローラの検出状況を確認できます。

Wireless > Access Point > AP List > Not Managed の順にメニューをクリックし、以下の画面を表示します。

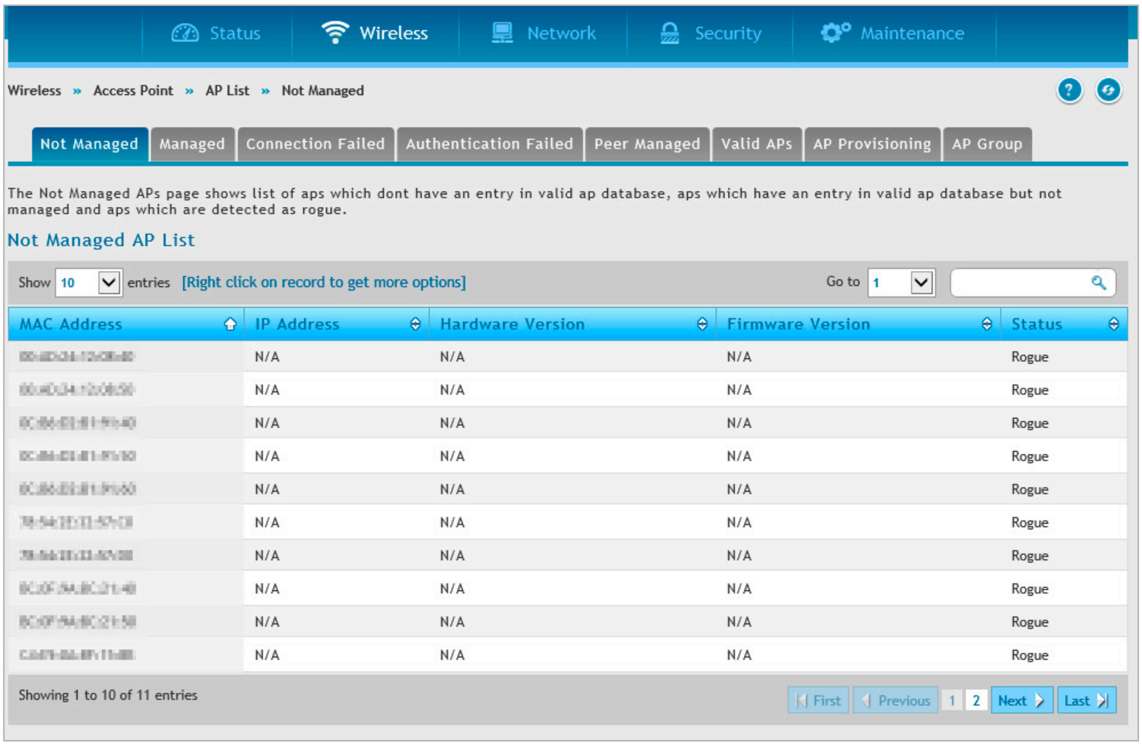


図 5-16　Not Managed AP List 画面

検出されたアクセスポイントが表示されます。

L2/ VLAN ディスカバリの設定

Wireless > Access Point > AP Poll List > VLANs Discovery メニュー

アクセスポイントを検出するように無線コントローラを設定します。

VLAN 検出の設定

1. **Wireless > Access Point > AP Poll List > VLANs Discovery** の順にメニューをクリックし、以下の画面を表示します。

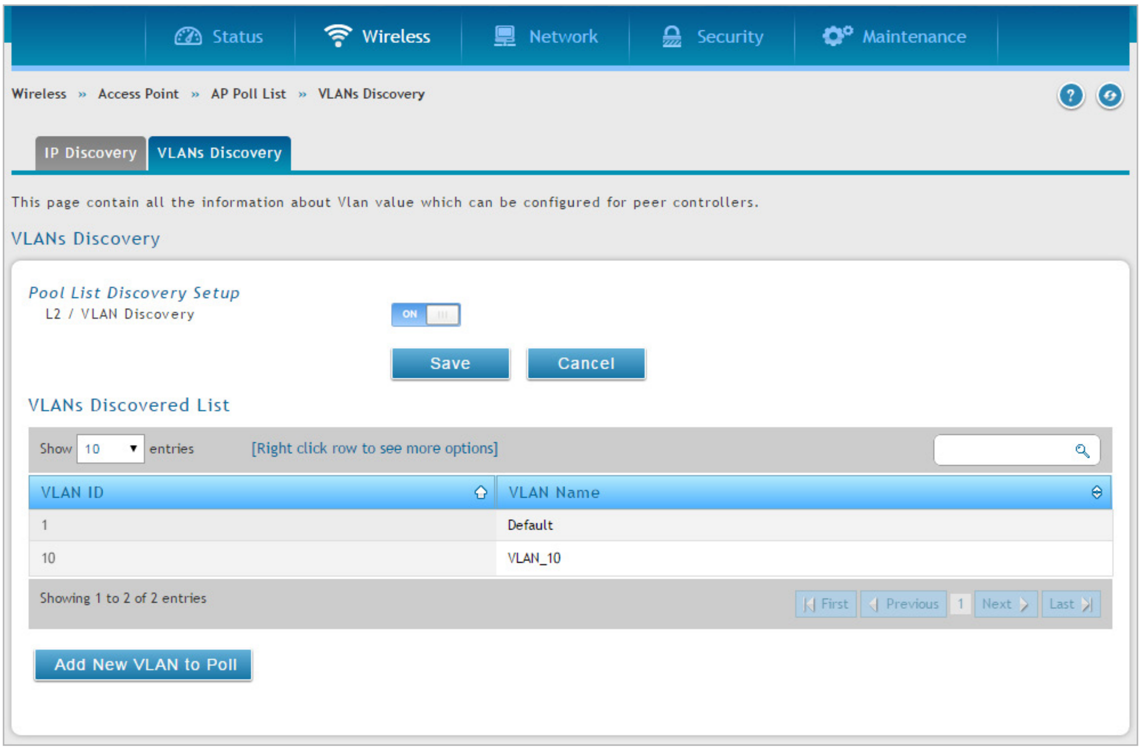


図 5-17　VLANs Discovery 画面

2. 「L2/ VLAN Discovery」を「ON」にし、「Save」ボタンをクリックします。

3. 「Add New VLAN to Poll」ボタンをクリックして、以下の画面を表示します。

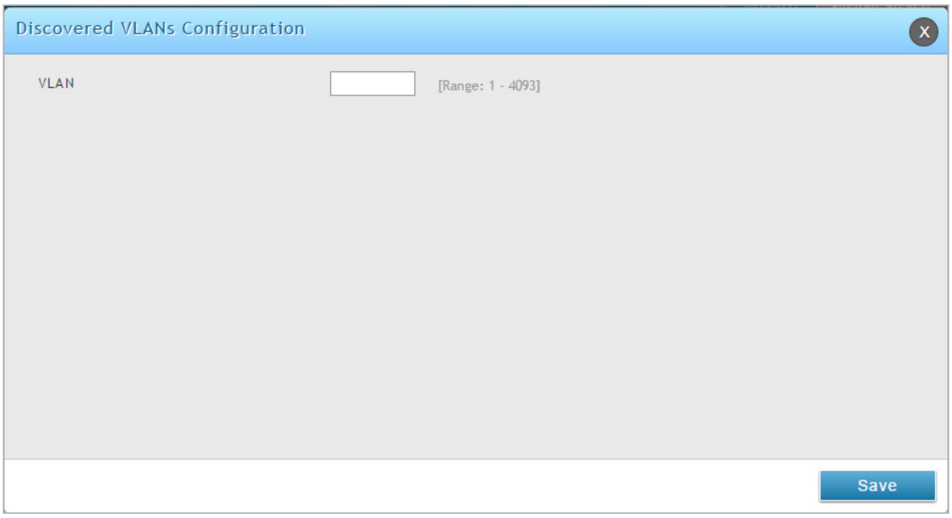


図 5-18　Discovered VLANs Configuration 画面

4. VLAN 番号を入力して、「Save」ボタンをクリックします。

VLAN 検出の削除

対象となる VLAN ID を右クリックして、「Delete」を選択します。すべての VLAN を削除するには、「Select All」をチェック後、「Delete」を選択します。

L3/IP ディスカバリ

ピアコントローラとアクセスポイント用に、無線コントローラに 256 個までの IP アドレスを設定できます。無線コントローラは、このリストにあるすべての IP アドレスに対して Association Invitation を送信します。デバイスがこの Invitation を受け取り、コントローラによる認証をパスすると、コントローラとアクセスポイント / ピアコントローラは接続します。

この検出方式は、デバイスが異なる IP サブネットにある場合、ピア無線コントローラおよびアクセスポイントを検出するのに便利です。事実、無線コントローラが、同じサブネットにないピアを認識するためには、ピアのレイヤ 3 検出リストに各コントローラの IP アドレスを登録する必要があります。

L3/IP ディスカバリの設定

Wireless > Access Point > AP Poll List ＞ IP Discovery メニュー

1. **Wireless > Access Point > AP Poll List > IP Discovery** の順にメニューをクリックし、以下の画面を表示します。

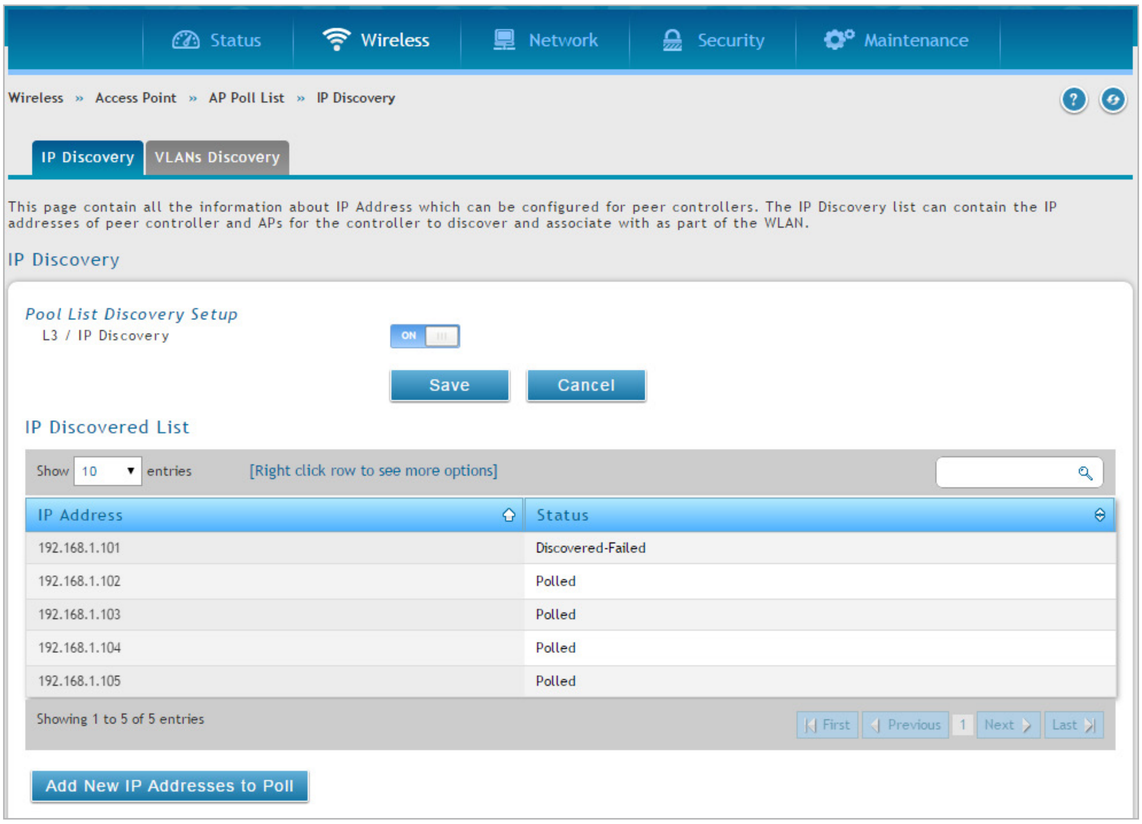


図 5-19　IP Discovery 画面

2. 「L3/ IP Discovery」を「ON」に切り替えて、「Save」ボタンをクリックします。
3. 「Add New IP Addresses to Poll」ボタンをクリックします。

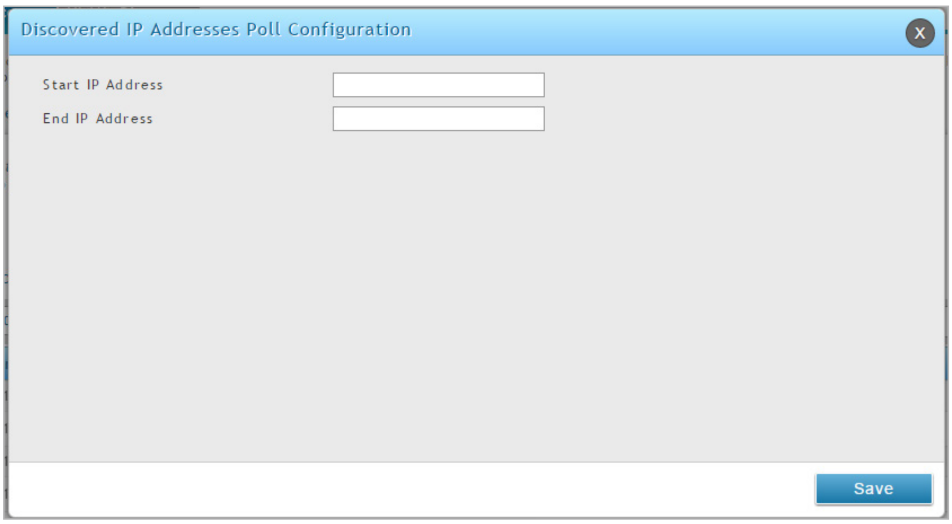


図 5-20　Discovered IP Addresses Poll Configuration 画面

4. IP 範囲を入力して、「Save」ボタンをクリックします。

管理対象のアクセスポイント

管理対象のアクセスポイント情報は、コントローラのローカルデータベースに保存されます。送信出力・チャンネルの追加 / 削除 / 変更、または個別に AP プロファイルを変更することが可能です。

ここでは、アクセスポイント認証にローカルデータベースを使用するか、または RADIUS データベースを使用するかを指定します。「Valid AP Configuration」画面には、ローカルデータベースに設定したアクセスポイントの情報が含まれます。アクセスポイント認証が RADIUS に設定されている場合は、コントローラが管理するアクセスポイントの情報を必ず外部 RADIUS データベースに追加してください。

Valid AP の追加

Wireless > Access Point > APs List > Valid APs メニュー

1. **Wireless > Access Point > APs List > Valid APs** の順にクリックし、以下の画面を表示します。

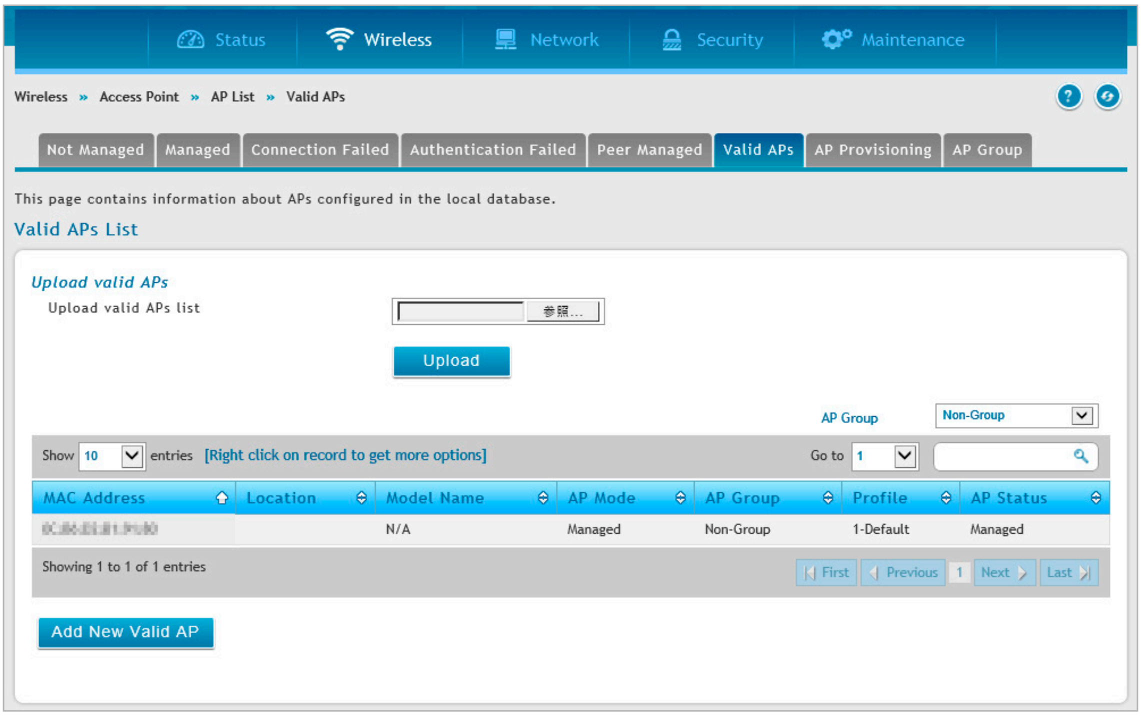


図 5-21　Valid APs List 画面

2. 有効なアクセスポイントのリストをアップロードする場合、「Upload valid APs」で csv ファイルを選択し、「Upload」をクリックします。
3. アクセスポイントを追加する場合は、「Add New Valid AP」ボタンをクリックします。画面は「AP Mode」で選択した内容によって異なります。

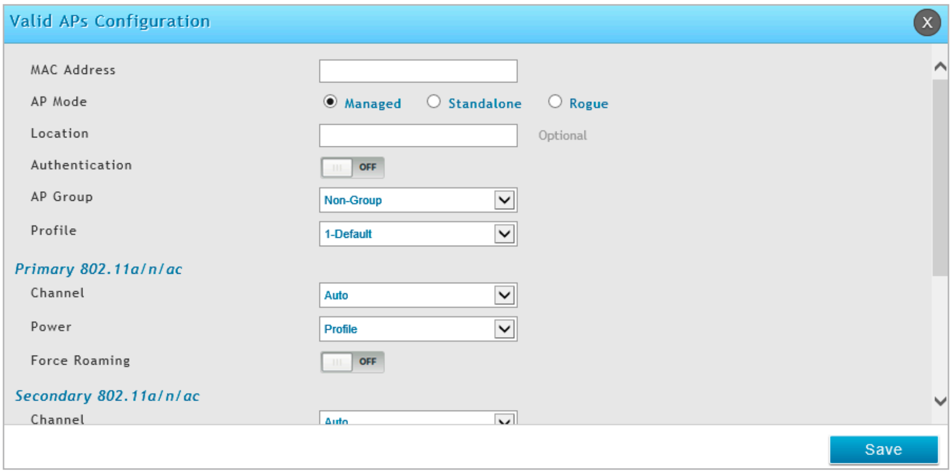


図 5-22　Valid APs Configuration 画面 - Managed モード

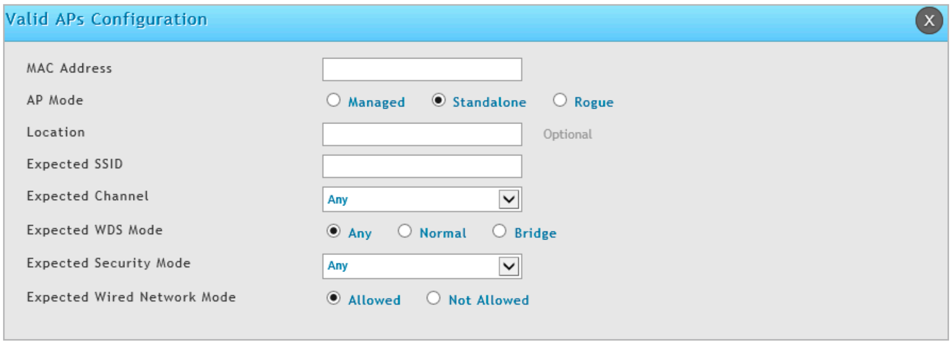


図 5-23　Valid APs Configuration 画面 - Standalone モード

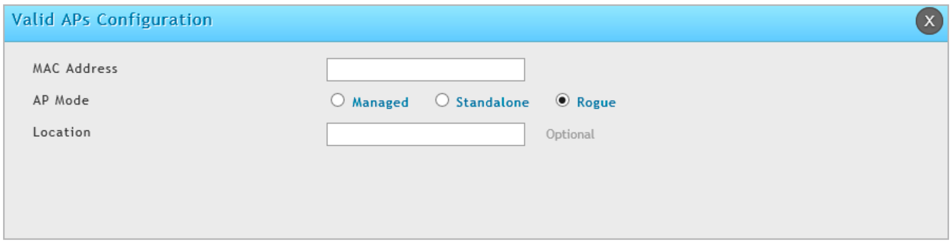


図 5-24　Valid APs Configuration 画面 - Rogue モード

以下の項目があります。

項目	説明
MAC Address	アクセスポイントの MAC アドレスを指定します。
AP Mode	AP モードを選択します。「Standalone」または「Managed」を選択すると、いくつかのフィールドに入力が必要です。 • Standalone - アクセスポイントはスタンドアロンモードで管理されています。 • Managed - AP プロファイル設定がアクセスポイントに適用されており、アクセスポイントは Managed モードで動作しています。 • Rogue - アクセスポイントは、無線コントローラに接続を試みていません。また、アクセスポイントの MAC アドレスは Valid AP データベース内に存在しません。
Location	管理されるアクセスポイントの位置を特定するオプションのフィールド。
Expected SSID	「AP Mode」が「Standalone」である場合に、アクセスポイントに設定される SSID。（参照用）
Expected Channel	「AP Mode」が「Standalone」である場合に、無線通信に使用されるチャンネル。（参照用）
Expected WDS Mode	「AP Mode」が「Standalone」である場合に、WDS（Wireless Distributed System）使用時の WDS のモード。（参照用）
Expected Security Mode	「AP Mode」が「Standalone」である場合に、使用するセキュリティモード。（参照用）
Expected Wired Network Mode	「AP Mode」が「Standalone」である場合に、有線ネットワークを許可するかどうか選択します。（参照用）
Authentication	「AP Mode」が「Managed」である場合に、認証用のパスワードを要求するようにオンにします。
Password	認証用のパスワードを入力します。
AP Group	「AP Mode」が「Managed」である場合に、アクセスポイントのグループを選択します。
Profile	「AP Mode」が「Managed」である場合に、アクセスポイントのコンフィグレーションに適用するプロファイルを選択します。
Channel	「AP Mode」が「Managed」である場合、無線電波が稼働するチャンネルを指定します。
Power	「AP Mode」が「Managed」である場合、無線電波が使用する電力の割合を指定します。
Force Roaming	「AP Mode」が「Managed」である場合、強制ローミングを「ON」または「OFF」に設定します。

4.　フィールドにデータを入力し、「Save」ボタンをクリックします。

注意　Valid AP リストでアクセスポイントを編集、または削除するには、アクセスポイントを右クリックして、「Edit」または「Delete」を選択します。すべてのリストを削除する場合は、「Select All」をチェック後、「Delete」を選択します。

Not Managed AP List からアクセスポイントを追加する

Wireless > Access Point > AP List メニュー

1. Wireless > Access Point > AP List > Not Managed の順にメニューをクリックし、以下の画面を表示します。

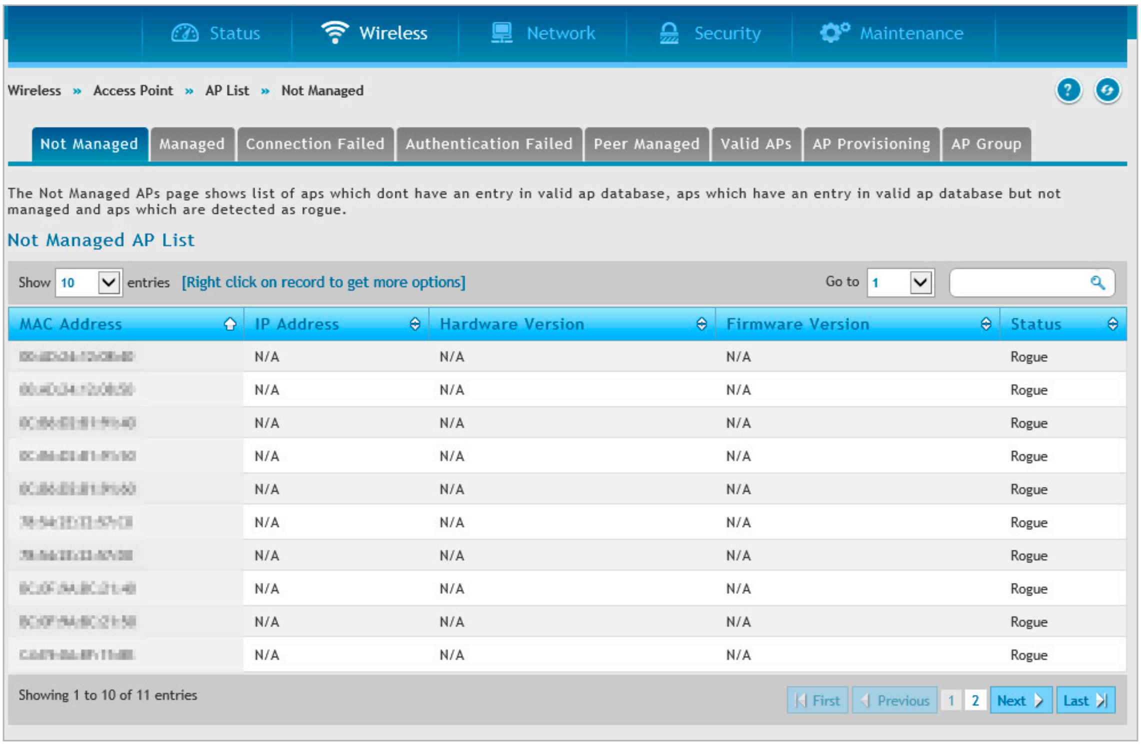


図 5-25　Not Managed AP List 画面

2. アクセスポイントを右クリックして、「Manage」を選択すると、以下の画面が表示されます。

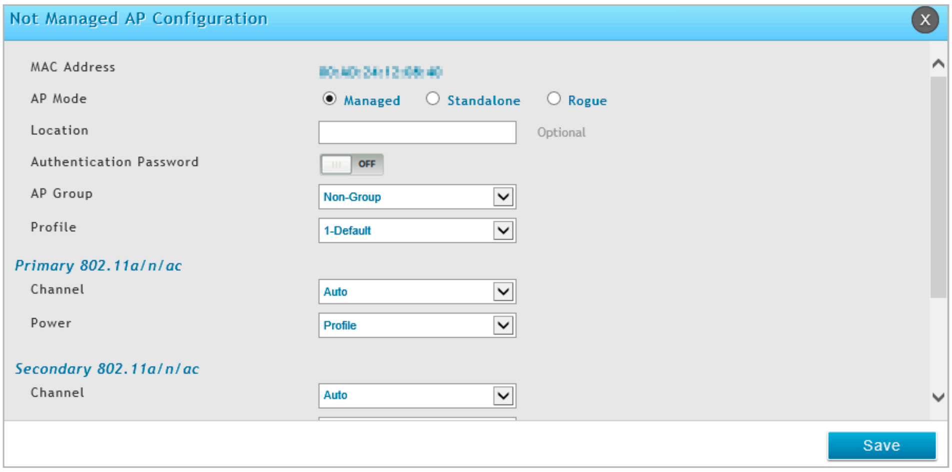


図 5-26　Not Managed AP Configuration 画面

3. 「AP Mode」と「Profile」を選択し、「Save」ボタンをクリックします。

管理対象アクセスポイントのチャンネルと送信出力の手動変更

Wireless > Access Point > AP List > Managed メニュー

Wireless > Access Point > AP List > Managed 画面では、アクセスポイントのチャンネルと送信出力を手動で設定できます。
手動で行った設定は、アクセスポイントのプロファイルに設定された内容に上書きされ、直ちに適用されます。
以下の場合は手動で行った設定は保持されません。

- アクセスポイントが無線コントローラと切断され、再度接続する場合
- プロファイルがアクセスポイントに再度適用される場合

1. Wireless > Access Point > AP List > Managed の順にメニューをクリックし、以下の画面を表示します。

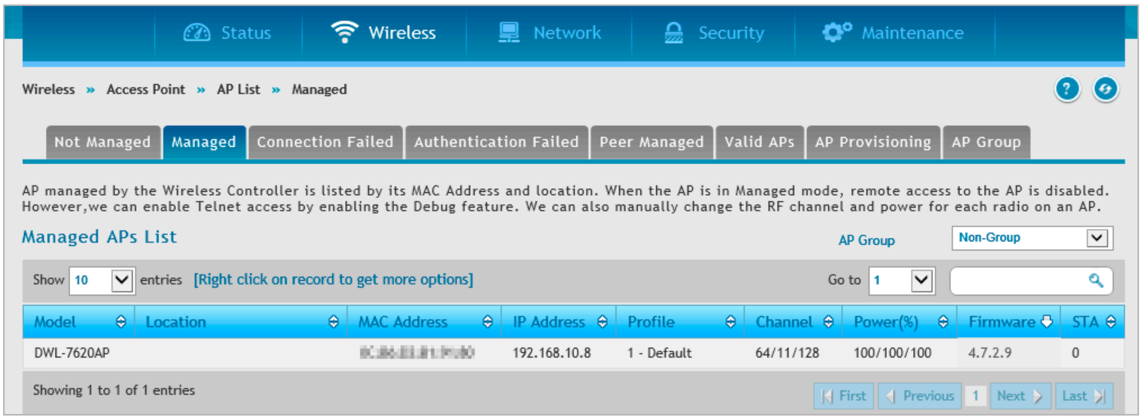


図 5-27　Managed APs List 画面

2. エントリ上で右クリックし、「Channel & Power」から設定する帯域を選択します。

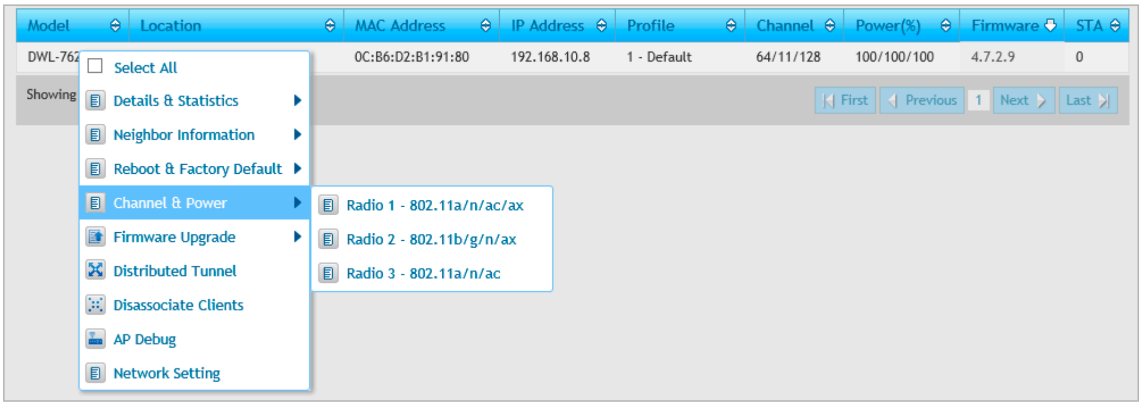


図 5-28　Managed APs List 画面

3. 以下の画面で設定を行います。

図 5-29　Channel and Power Configuration 画面

4. 「Channel」で希望するチャンネルを選択します。
5. 「Power」で送信出力を選択します。
6. 「Save」ボタンをクリックします。

AP デバッグモードの設定

Wireless > Access Point > AP List > Managed メニュー

アクセスポイントが「Managed」モードである場合、アクセスポイントへのリモートアクセスは無効です。
ただし、**Wireless > Access Point > AP List > Managed** 画面でデバッグ機能を有効にした場合は、Telnet によりアクセスできるようになります。

1. **Wireless > Access Point > AP List > Managed** の順にメニューをクリックし、以下の画面を表示します。

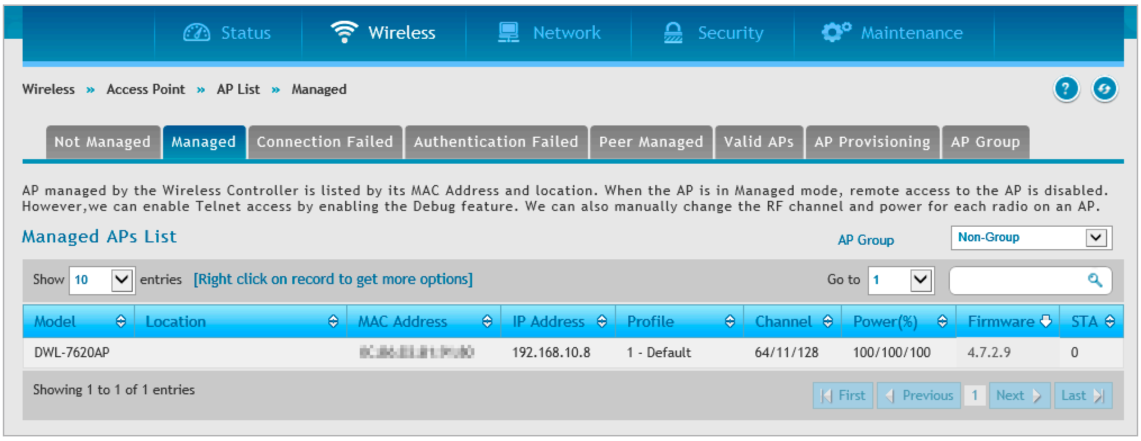


図 5-30　Managed APs List 画面

2. エントリの 1 つで右クリックし、「AP Debug」を選択します。

図 5-31　Managed AP Debug Configuration 画面

3. 「Enable Debug」を「ON」に切り替え、パスワードを設定します。

4. 「Save」ボタンをクリックします。

AP プロビジョニングの設定

Wireless > Access Point > AP List > AP Provisioning メニュー

AP プロビジョニング機能は、既存のスイッチのクラスタに新しいアクセスポイントを追加することを補助します。AP プロビジョニングを使用して、無線ネットワークに接続するのに必要なパラメータをアクセスポイントに設定することができます。

AP プロビジョニングを使用して、相互認証（**Wireless > Peer Group > Peer Configuration**）が有効なネットワークにデバイスを接続します。ネットワークで相互認証が無効である場合、ローカル Valid AP データベースまたは RADIUS AP データベースおよび検出オプションを適切に設定することで、アクセスポイントをネットワークに接続することができます。プロビジョニング機能は、相互認証が有効化されていないネットワークにおいて、クラスタにアクセスポイントを簡単に追加するためにオプションで使用することができます。

本ページを使用して、アクセスポイントに関する詳しいプロビジョニング情報を参照します。また、右クリックメニューの「Edit」を使用して、アクセスポイントにプロビジョニング情報を提供するプライマリまたはバックアップスイッチの IP アドレスを指定します。

1. **Wireless > Access Point > AP List > AP Provisioning** の順にメニューをクリックし、以下の画面を表示します。

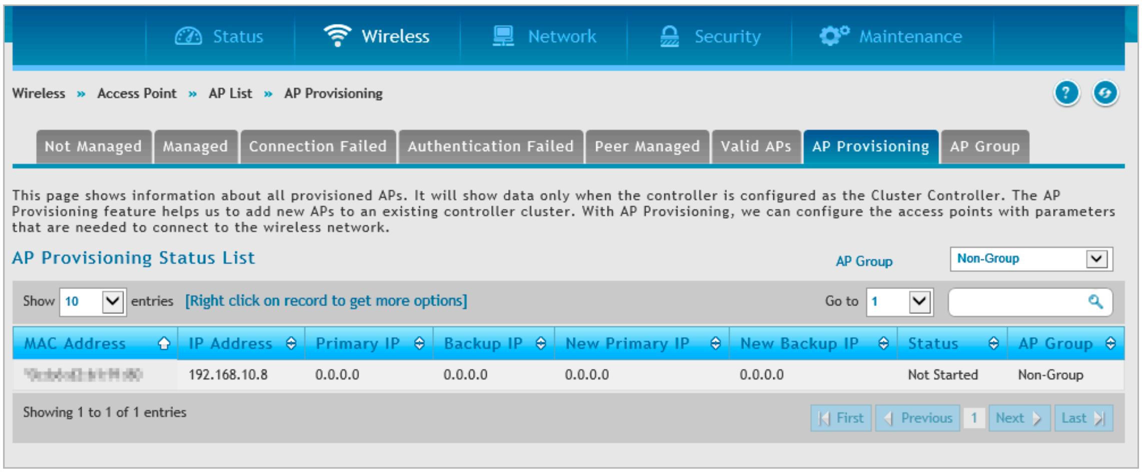


図 5-32　AP Provisioning Status List 画面

2. 管理対象のアクセスポイントを右クリックして、「Edit」を選択します。

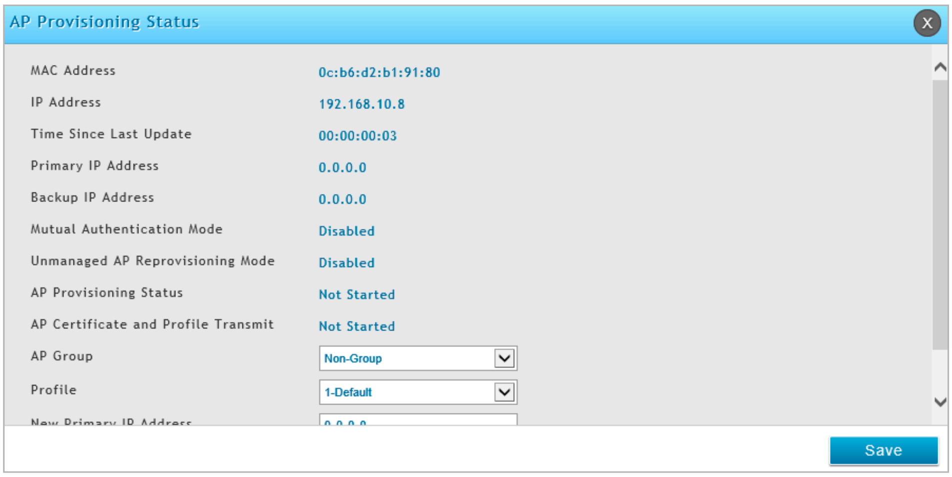


図 5-33　AP Provisioning Status 画面

以下の項目があります。

項目	説明
MAC Address	アクセスポイントの MAC アドレス。
IP Address	アクセスポイントの IP アドレス。
Time Since Last Update	このアクセスポイントから情報を受信した時間。
Primary IP Address	アクセスポイントによって報告されるプライマリプロビジョンスイッチの IP アドレス。
Backup IP Address	アクセスポイントによって報告されるバックアッププロビジョンスイッチの IP アドレス。
Mutual Authentication Mode	Mutual Authentication モードが現在有効であるかどうかを示します。
Unmanaged AP Reprovisioning Mode	アクセスポイントに設定した再プロビジョニングモードを表示します。 • Enabled - アクセスポイントは、管理されていない場合に再プロビジョニングが行われます。 • Disabled - アクセスポイントは、管理されていない場合に再プロビジョニングが行われません。
AP Provisioning Status	最も新しく発行された AP プロビジョニングコマンドのステータス。 • Not Started - プロビジョニングが本アクセスポイントに対して開始されていません。 • Success - 本無線コントローラでプロビジョニングの実行に成功しました。AP Provisioning Status テーブルは最新のプロビジョニング設定を反映する必要があります。 • In Progress - 本アクセスポイントでプロビジョニングを実行中です。 • Invalid Switch IP Address - プライマリまたはバックアップ無線コントローラの IP アドレスがクラスタにないか、相互認証モードが有効です。また、プライマリの無線コントローラの IP アドレスが指定されていません。 • Provisioning Rejected - アクセスポイントは管理されておらず、Unmanaged モードではプロビジョニングデータを受け付けないように設定されています。 • Timed Out - 最後のプロビジョニング要求はタイムアウトしました。
AP Certificate and profile Transmit	最後の AP プロファイルとプライマリ / バックアップスイッチへの X.509 証明書の配布の状態。この状態は、AP プロビジョニングコマンドの結果で変わります。相互認証が有効である場合にだけ、X.509 証明書はプライマリおよびバックアップスイッチに送信されます。以下の状態の 1 つが表示されます。 • Not Started - 本アクセスポイントのどんな情報もプライマリおよびバックアップスイッチに送信されていません。 • Success - AP プロファイルと X.509 証明書は、プライマリおよびバックアップスイッチに送信されます。 • Failed - 本スイッチが情報の送信を試みた時に、プライマリまたはバックアップスイッチがクラスタにありませんでした。
AP Group	アクセスポイントのグループを選択します。
Profile	使用する AP プロファイルを選択します。
New Primary IP Address	アクセスポイントを管理する無線コントローラの IP アドレスを入力します。
New backup IP Address	プライマリ無線コントローラに接続できない場合に、アクセスポイントが接続を試みるべきスイッチの IP アドレスを入力します。

3. 「Save」ボタンをクリックします。

注意 DWL-x620AP では、AP Provisioning は動作しません。

AP グループの設定

Wireless > Access Point > AP List > AP Group メニュー

管理アクセスポイントのグループを作成します。

1. **Wireless > Access Point > AP List > AP Group** の順にメニューをクリックし、以下の画面を表示します。

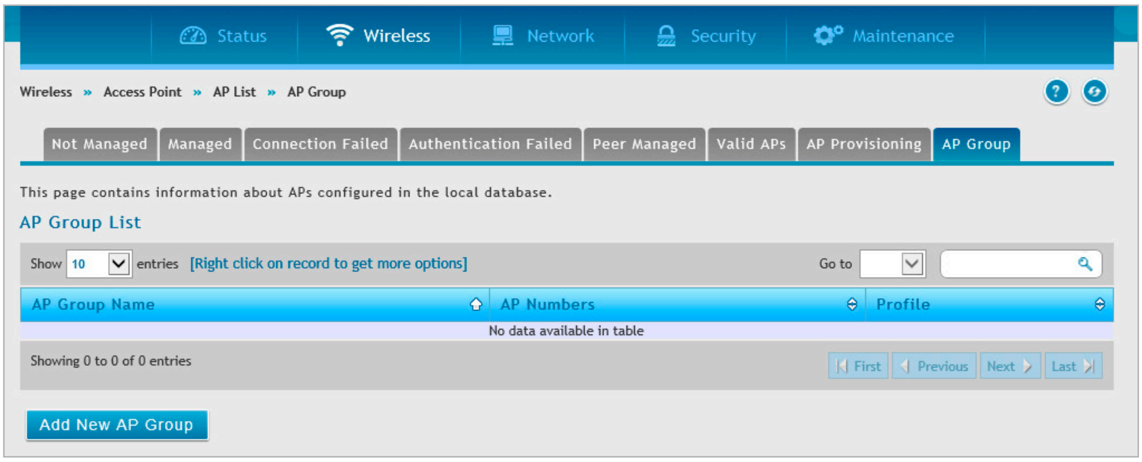


図 5-34　AP Group List 画面

2. グループを作成する場合は、「Add New AP Group」をクリックします。
3. 以下の画面で設定を行います。

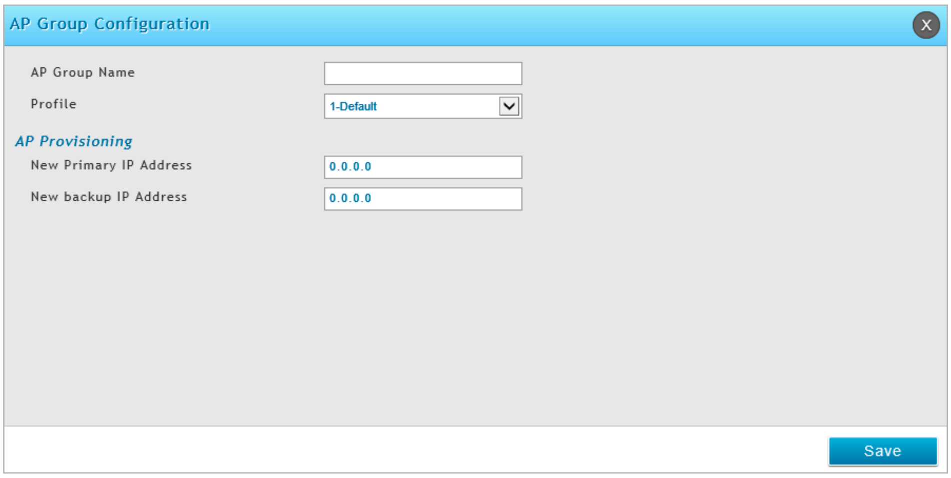


図 5-35　AP Group Configuration 画面

以下の項目があります。

項目	説明
AP Group Name	グループ名を入力します。
Profile	プロファイルを選択します。
AP Provisioning	
New Primary IP Address	プライマリ IP アドレスを入力します。
New backup IP Address	バックアップ IP アドレスを入力します。

4. 「Save」ボタンをクリックします。

AP プロファイル

プロファイルとは、SSID、チャネル設定等、ネットワーク機器へ配信する設定をまとめたものです。
無線コントローラ上に複数の AP プロファイルを作成することにより、設置場所や機能などに応じてアクセスポイントをカスタマイズできます。 規模の大きい無線ネットワークを管理する場合に便利な機能です。

各 AP プロファイルには、以下の機能を設定することができます。
- プロファイル設定（名称、ハードウェアタイプ番号、有線ネットワークのディスカバリ VLAN ID）
- 帯域設定
- SSID 設定
- QoS 設定

AP プロファイルの設定

Wireless > Access Point > AP Profile > AP Profiles メニュー

1. **Wireless > Access Point > AP Profile > AP Profiles** の順にメニューをクリックし、以下の画面を表示します。

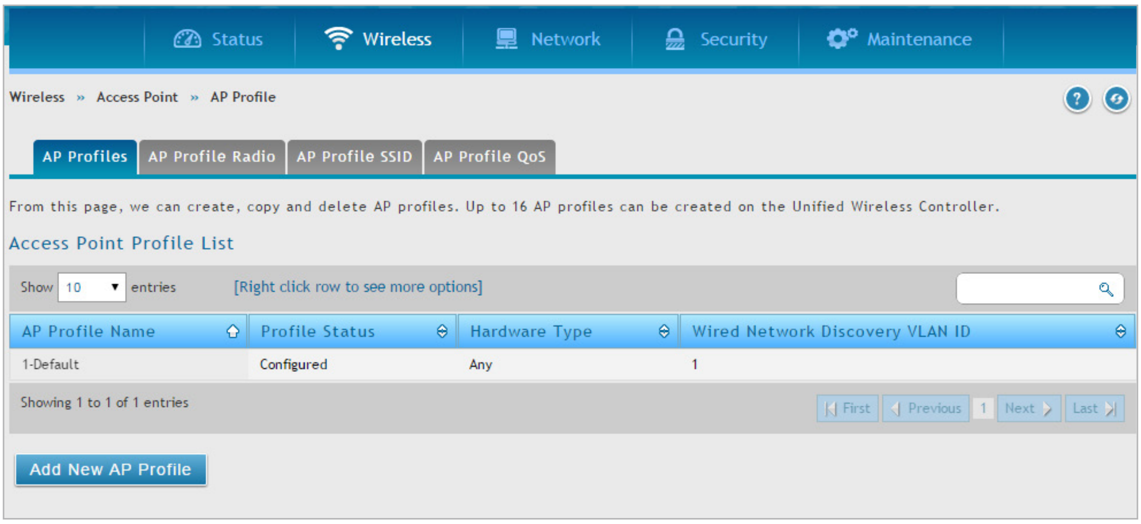


図 5-36　Access Point Profile List 画面

2. 「Add New AP Profile」ボタンをクリックします。

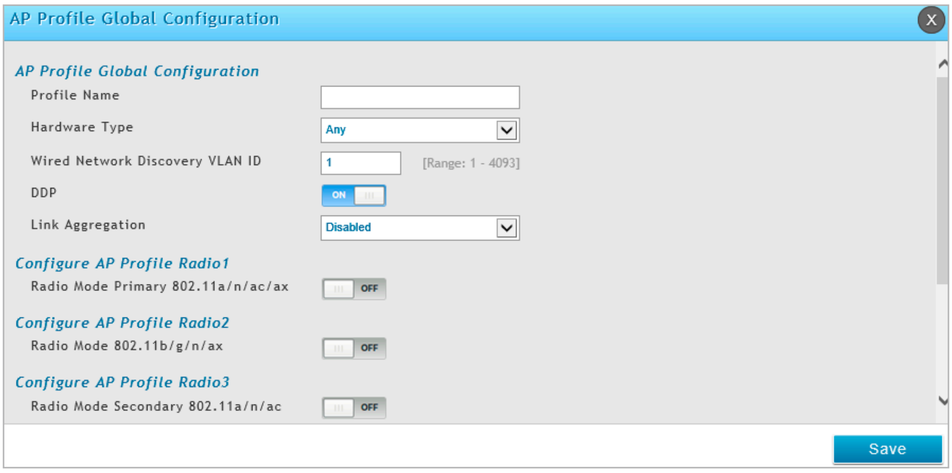


図 5-37　AP Profile Global Configuration 画面

3. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
AP Profile Global Configuration	
Profile Name	プロファイル名を指定します。
Hardware Type	このプロファイルを使用するアクセスポイントのハードウェアタイプを選択します。ハードウェアタイプは、アクセスポイントがサポートする無線インタフェース数（シングル、デュアルまたはトリプル）と無線インタフェースがサポートする IEEE 802.11 モード により決定されます。 • すべて（any） • DWL-8600AP Dual Radio a/b/g/n • DWL-3600AP Single Radio b/g/n • DWL-3610AP Single Radio dual band a/b/g/n/ac • DWL-6600AP Dual Radio a/b/g/n • DWL-2600AP Single Radio b/g/n • DWL-8610AP Dual Radio a/b/g/n/ac • DWL-6610AP Dual Radio a/b/g/n/ac • DWL-6700AP Dual Radio a/b/g/n • DWL-6610AP B1 Dual Radio a/b/g/n/ac • DWL-6620APS Dual Radio a/b/g/n/ac • DWL-7620AP Triple Radio a/b/g/n/ac • DWL-8710AP Dual Radio a/b/g/n/ac • DWL-8620AP Dual Radio a/b/g/n/ac • DWL-6720AP Outdoor Dual Radio a/b/g/n/ac • DWL-8720AP Outdoor Dual Radio a/b/g/n/ac • DWL-X8630AP Dual Radio a/b/g/n/ac/ax 注意 DWL-2600AP、DWL-3600AP はアクセスポイント側のファームウェアが DWC-2000 をサポートしていないため未サポートです。
Wired Network Discovery VLAN ID	コントローラが有線ネットワークに接続するアクセスポイントを検出するためにトレーサパケットを送信するのに使用する VLAN ID を指定します。
Wireless Multicast Forwarding	ワイヤレスマルチキャストフォワーディングを「ON」または「OFF」にします。 DWL-6620APS/DWL-7620AP を選択した場合にのみ表示されます。
DDP	DDP を「ON」または「OFF」にします。
Link Aggregation	リンクアグリゲーションの設定を以下から選択します。 • Disabled - リンクアグリゲーションを無効にします。 • LACP - LACP によるリンクアグリゲーションを行います。 • Static - スタティックリンクアグリゲーションを行います。
Configure AP Profile Radio 1-3	
無線の設定を行います。設定したい項目を「ON」にすると、下に設定項目が表示されます。「AP Profile Radio」からも設定可能です。 詳細は「AP プロファイルの無線電波の設定」を参照してください。	
Configure AP Profile QoS 1-3	
QoS の設定を行います。設定したい項目を「ON」にすると、下に設定項目が表示されます。「AP Profile Radio」からも設定可能です。 詳細は「AP プロファイルの無線電波の設定」を参照してください。	

AP プロファイルの無線電波の設定

Wireless > Access Point > AP Profile > AP Profile Radio メニュー

プロファイルの無線接続モードを設定します。アクセスポイントは、2.4GHz と 5GHz の 2 つの周波数帯域をサポートしています。
初期値は以下のとおりです。

- Radio 1：IEEE 802.11a/n/ac/ax モードで動作します。（2.4GHz 帯を使用）
- Radio 2：IEEE 802.11b/g/n/ax モードで動作します。（5GHz 帯を使用）

1. **Wireless > Access Point > AP Profile > AP Profile Radio** の順にメニューをクリックし、以下の画面を表示します。

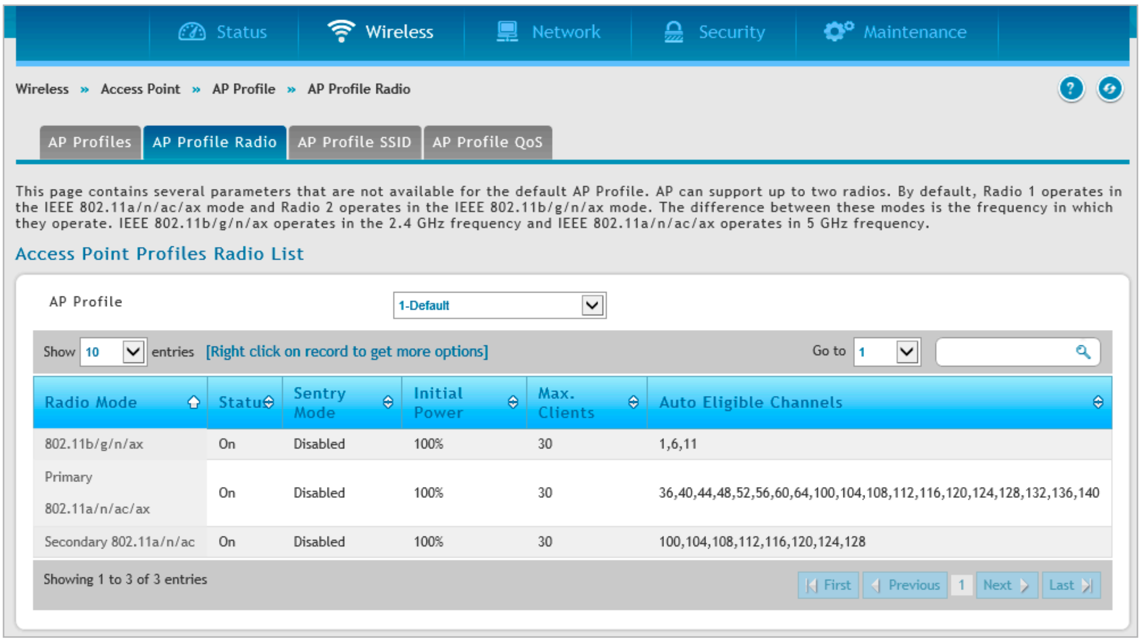


図 5-38　Access Point Profiles Radio List 画面

2. 変更する無線電波を選択し、編集する列を右クリックして「Edit」を選択します。

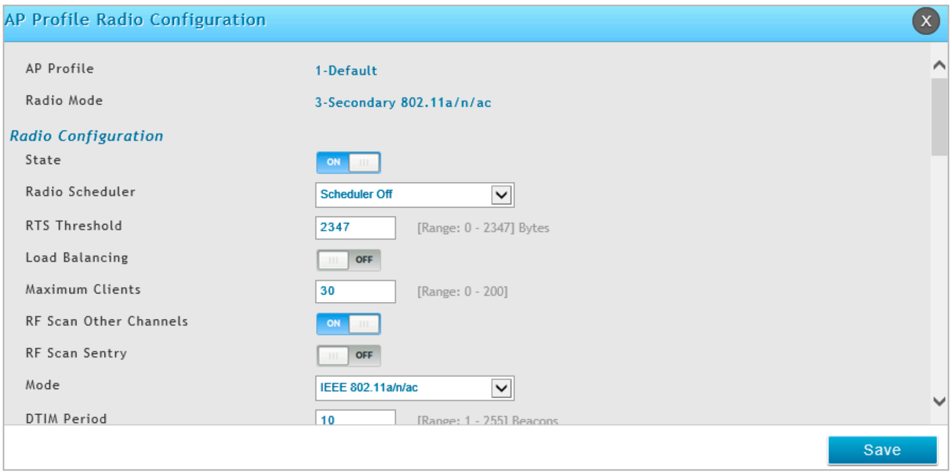


図 5-39　AP Profile Radio Configuration 画面

3. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
AP Profile	プロファイル名を表示します。
Radio Mode	無線帯域を表示します。
Radio Configuration	
State	無線インタフェースを「ON」（有効）または「OFF」（無効）にします。 無線インタフェースをオフにすると、アクセスポイントは配下の全無線クライアントに向けて接続解除フレームを送信します。この手順で無線インタフェースのシャットダウンが行われ、クライアントは他のアクセスポイントとの間で接続プロセスを開始します。
Radio Scheduler	無線のスケジュール設定を指定します。

項目	説明
RTS Threshold	Request to Send（RTS）しきい値（0-2347）を指定します。 RTS しきい値は、MPDU 内のオクテット数を示します。設定値より低いと RTS/CTS ハンドシェークは実行されません。 この値を変更することで、特に多数のクライアントを抱えるアクセスポイントを通過するトラフィックフローの制御をすることができます。低い値を指定すると、RTS パケットは頻繁に送信されるようになります。これにより消費する帯域幅は増大し、パケットのスループットは低下します。一方、RTS パケットの送信数を増やすと、混雑したネットワーク内で起こり得る干渉や衝突からの回避や、電磁波による干渉を軽減できるようになります。
Load Balancing	ロードバランシング機能を有効にすると、アクセスポイントにおけるトラフィック量を制御することができます。
Load Utilization	「Load Balancing」が「ON」の場合、許可されるネットワーク帯域使用率（1-100%）のしきい値を設定できます。このしきい値に使用率が到達すると、アクセスポイントは新しいクライアントとの接続を拒否します。
Maximum Clients	本アクセスポイントに一度にアクセスできるステーションの最大数（0-200）を指定します。
RF Scan Other Channels	アクセスポイントは RF スキャンを実行し、通信範囲内の他の無線デバイスに関する情報を集め、無線コントローラに報告します。 • ON - 無線電波は定期的に運用中のチャンネルから移動して、他のチャンネルのスキャンも行います。これにより、ユーザトラフィックの遮断が発生し、特に音声通信中はそれが顕著になります。 • OFF - アクセスポイントは運用中のチャンネルのみスキャンします。
RF Scan Sentry	「ON」にした場合、アクセスポイントは Sentry（監視）モードで動作し、RF スキャンを実行します。 無線インタフェースは送信されてくるビーコンフレーム、およびクライアントと他のアクセスポイント間のトラフィックを受動的に学習していますが、クライアントからの接続には応じません。Sentry（監視）モードでは、すべての VAP は無効になります。Sentry AP を配置するネットワークまたは無線インタフェースは、ネットワーク上のデバイスをより迅速に検出して、より徹底的なセキュリティ分析を行うことができます。本モードでは、スキャンはチャンネル間を移動して行われます。 各チャンネルに費やす時間は「RF Scan Duration」（スキャン時間）によって制御されます。
Mode	無線の接続モードを選択します。表示される項目は手順 2 で選択した内容によって異なります。
DTIM Period	DTIM メッセージはビーコンフレームに含まれる要素です。これは、現在省電力モードでスリープ状態のクライアントステーションに対し、アクセスポイント上に送信待ちとしてバッファされているデータがあることを示すメッセージです。ここで指定する DTIM Period（DTIM 間隔）は、本アクセスポイントの配下にあるクライアントが、アクセスポイントにバッファされているデータを確認する間隔を示します。 DTIM 間隔（1-255）を指定します。数字はビーコンの数で表します。例えば、本欄に「1」と入力した場合、バッファされたデータの確認は、ビーコンフレーム送信ごとにアクセスポイントで行われます。「10」と入力した場合は 10 回のビーコンフレーム送信に 1 度の確認となります。
Beacon Interval	ビーコン間隔（20-2000 ミリ秒）を指定します。ビーコンフレームは無線ネットワークの存在を通知するために、アクセスポイントから定期的に送信されます。初期値では、ビーコンフレームは 100（ミリ秒）に 1 度（1 秒に 10 回）送信されます。
Automatic Channel	チャンネルとは、無線インタフェースがデータの送受信に使用する無線スペクトラムのある一部分を定義するものです。チャンネルの範囲やチャンネルの初期値は無線インタフェースのモードにより異なります。アクセスポイントが再起動する時、アクセスポイントは RF エリア内で使用されているチャンネルをスキャンし、有効な干渉のないチャンネルまたは空きチャンネルを選択します。ただし、チャンネルの状況は刻々と変化しています。「Automatic Channel」を有効にすると、本プロファイルを適用したアクセスポイントでは、自動チャンネル選択が可能になります。自動的に、または手動で自動チャンネル選択アルゴリズムを実行させ、コントローラが、WLAN 状態の変化に従いアクセスポイント上のチャンネル調整をできるようにします。初期値では、グローバル自動チャンネルモードは自動に設定されています。自動チャンネル選択モードを有効にする場合は、**Wireless > General > Channel Algorithm > Channel Setting** の「Channel Plan Mode」に「Fixed time」または「Interval」を選択して実行タイミングを指定します。また、「Manual Channel Plan」ページで、手動で自動チャンネル選択アルゴリズムを実行させることも可能です。 **注意**　「Valid APs」または「Advanced AP Management」ページでアクセスポイントにスタティックチャンネルを割り当てている場合、そのアクセスポイントでは自動チャンネル選択を有効にできません。
Automatic Power	送信出力レベルは、アクセスポイントがどれだけ遠くまで RF 信号をブロードキャストできるかということに影響します。電力レベルが低すぎると、無線クライアントが信号を検知できなかったり、WLAN のパフォーマンスの低下が発生したりします。逆に、電力レベルが高すぎると、RF 信号が通信範囲内の他のアクセスポイントとの間に干渉を起こす可能性が出てきます。自動送信出力調整機能では、独自のアルゴリズムを使用して、RF 信号がなるべく遠くの無線クライアントまで到達し、かつ他のアクセスポイントがブロードキャストする RF 信号と干渉を起こすほど遠くまでは到達しないように、自動的に調整します。電力レベルアルゴリズムはパケット再送エラーの有無に基づき送信出力を 10% の割合で増減します。
Initial Power	初期電力レベルを指定します。自動電力調整アルゴリズムは、本フィールドで指定した送信出力の割合以下に電力を落とすことはありません。初期値は 100% です。この場合、自動電力調整を有効にしても、RF 信号送信電力が減少することはありません。単位は RF 信号の最大送信出力に対する割合（%）です。

項目	説明
Minimum Power	設定した無線インタフェースにおける送信出力の最小値（1-100%）を指定します。
APSD Mode	「ON」を選択して、電源管理方法である自動省電力機能（APSD）を有効にします。APSD は、VoIP 電話がアクセスポイントを通じてネットワークにアクセスする場合にお勧めします。
RF Scan Interval	RF スキャン中のチャンネル変更の間隔（秒）を制御します。
Frag Threshold	フラグメントしきい値（256-2345）を指定します。ネットワーク上で伝送されるパケットサイズを制限するもので、本フィールドで指定したサイズ以下のパケットはフラグメント化されません。2346 は、パケットはフラグメント化されないことを示します。
RF Scan Sentry Channels	無線インタフェースは 802.11b/g 周波数帯（2.4 GHz）と 802.11a 周波数帯（5 GHz）または両帯域内のチャンネルのスキャンを行います。スキャンの対象となる周波数帯域のチャンネルを選択します。 **注意**　帯域選択は、Sentry モードの帯域だけに適用し、無線の周波数帯域の機能に依存します。
Short Retries	RTS Threshold と同じ、またはそれより小さいサイズのフレーム送信の最大リトライ回数（1-255）を示します。
RF Scan Duration	RF スキャン時に他のチャンネルのスキャンに要する時間（ミリ秒）を指定します。
Long Retries	RTS Threshold より大きいサイズのフレーム送信の最大リトライ回数（1-255）を示します。
Rate Limiting	マルチキャストとブロードキャスト速度制限を有効にすると、ネットワークを経由して送信されるパケット数を制限することによって、全体的なネットワーク性能を改善することができます。初期値は「OFF」（無効）です。 **注意**　利用可能な速度制限値は多くの環境で非常に低くなるため、本機能を有効とすることをお勧めしません。 ・ON - マルチキャストとブロードキャストの速度制限を有効にします。 ・OFF - マルチキャストとブロードキャストの速度制限を無効にします。
Transmit Lifetime	最初の MSDU の送信開始から送信終了までの時間（ミリ秒）を表示します。
Rate Limit	マルチキャストとブロードキャストトラフィックに設定する速度制限を入力します。制限値は 1 秒あたり 1 以上 50 未満のパケット数とすべきです。この速度制限を下回るトラフィックはすべて適切な宛先に送信されます。初期値と最大速度制限値は 50 パケット / 秒です。「Rate Limiting」を無効にすると、本欄は無効になります。
Receive Lifetime	最初のフラグメント化された MMPDU または MSDU を受信してから、MMPDU または MSDU の再構築を終了するまでの時間（ミリ秒）を指定します。
Rate Limit Burst	速度を制限するバースト値を設定すると、すべてのトラフィックが速度制限を超える前のトラフィックバーストの量を決定します。このバースト制限は、設定した速度制限を超えるネットワーク上のトラフィックの間欠バーストを容認します。初期値と最大速度制限バースト設定は 70（パケット / 秒）です。「Rate Limiting」を無効にすると、本欄は無効になります。
Station Isolation	本オプションを選択すると、アクセスポイントは無線クライアント間の通信をブロックします。無線クライアント内ではなくネットワークの無線クライアントと有線デバイス間のデータトラフィックは許可します。初期値は「OFF」（無効）です。
Channel Bandwidth	802.11n 仕様では他のモードで利用可能な既存の 20MHz のチャンネルに加えて 40MHz 帯域のチャンネルの使用を許可しています。40MHz のチャンネルは、より高いデータ速度を可能にしますが、他の 2.4GHz および 5GHz デバイスが使用できるチャンネルが少なくなります。40MHz のオプションは、802.11a/n モードでは初期値で有効です。また、802.11b/g/n モードでは 20MHz オプションが有効です。チャンネル帯域幅の使用を 20MHz に制限するためには本設定を使用します。
Primary Channel	チャンネルを選択し、チャンネル帯域幅を 40MHz に設定する場合にだけ、本設定を変更することができます。40MHz のチャンネルは、周波数領域で隣接している 2 個の 20MHz のチャンネルから構成されていると見なすことができます。これらの 2 個の 20MHz のチャンネルは、多くの場合 Primary と Secondary チャンネルと呼ばれます。Primary Channel は 20MHz のチャンネル帯域幅だけをサポートする 802.11n クライアントとレガシークライアントに使用されます。これにより、40MHz 帯域の上位または下位 20MHz のチャンネルとして Primary Channel を設定します。
Protection	保護機能は、802.11 の伝送がレガシーステーションまたはアプリケーションで干渉を起こさないことを保証するルールを含んでいます。初期値では、これらの保護メカニズムは有効（Auto）です。保護が有効な場合、アクセスポイントの適用範囲内にレガシーデバイスがあると、保護メカニズムが呼び出されます。これらの保護メカニズムを無効（OFF）にすることができますが、802.11n 保護をオフにすると、適用範囲内のレガシークライアントまたはアクセスポイントが 802.11n 伝送によって影響を受けることがあります。モードが 802.11b/g である場合にも、802.11n 保護機能は利用可能です。保護をこのモードで有効とすると、802.11b クライアントとアクセスポイントを 802.11g の伝送から保護します。
Short Guard Interval	ガードインターバルは OFDM シンボル間のデッドタイム（ナノ秒）です。ガードインターバルは符号間干渉と搬送波間干渉（ISI、ICI）を防ぎます。802.11n モードでは、802.11a/g の定義する 800（ナノ秒）から 400（ナノ秒）にこのガードインターバルを短縮することが許容されています。ガードインターバルの短縮によって、データ処理性能において 10% の改善をもたらすことができます。 ・ON - アクセスポイントは、400ns のガードインターバルをサポートするクライアントと通信する場合に 400ns のガードインターバルを使用してデータを送信します。 ・OFF - アクセスポイントは、800ns のガードインターバルを使用してデータを送信します。

項目	説明
Space Time Block Code	Space Time Block Coding（STBC）はデータ伝送の信頼性を改善することを意図した 802.11n の技術です。データストリームが複数アンテナの上に転送されるため、受信システムは、少なくともデータストリームの 1 つを検出する可能性が高くなります。 • ON - アクセスポイントは、同時に、複数アンテナに同じデータストリームを転送します。 • OFF - アクセスポイントは、複数アンテナに同じデータストリームを転送しません。
Radio Resource Management	Radio Resource Measurement（RRM）モードでは、無線システムに対してビーコン内の追加情報、プローブ応答、および関連する応答の送信を要求します。AP プロファイルにおける帯域リソース測定機能のサポートを有効または無効にします。本機能は、各帯域に個別に設定され、初期値では有効です。
No ACK	「ON」を選択して、アクセスポイントがサービスクラス値として QosNoAck を持つフレームを承認するべきでないことを指定します。
Force Roaming	無線信号の強さが指定した Force Roaming Threshold 値を下回った場合、接続済みの AP からクライアントが切断されます。
Force Roaming Threshold	Force Roaming のしきい値を 20-50（%）の範囲で指定します。
Multicast Tx Rate (Mbps)	帯域がマルチキャストフレームを転送するのに 802.11 レート（Mbps）を選択します。5GHz 帯域で最も低いレートは 6Mbps です。
Channel	
Auto Eligible Channels	本画面で現在選択している無線モードおよび「General Settings」画面で設定した国コードでサポートされるチャンネルを表示します。「Ctrl」を押すことで、複数のチャンネルを選択できます。
Basic Rate Set (Mbps)	これらの値はアクセスポイントに接続するすべてのステーションがサポートすべきデータ速度を示しています。
Supported Rate Set (Mbps)	アクセスポイントがサポートする通信速度で、複数の速度を選択できます。エラー率やアクセスポイントとクライアントとの距離などの要素をもとに、アクセスポイントは最も効率の良い速度を自動的に選択します。
Multicast to Unicast	マルチキャスト / ユニキャスト変換を有効にします。
DHCP Offer/ ACK to Unicast	DHCP Offer/ACK パケットのユニキャスト送信を有効にします。
Airtime Fairness	エアタイムフェアネス機能を有効にします。

注意　DWL-x620AP においては Basic Rate は反映されません。

AP プロファイル SSID の設定

Wireless > Access Point > AP Profile> AP Profile SSID メニュー

選択した AP プロファイルに関連付けられた仮想アクセスポイント（VAP）設定を表示します。各 VAP は、ネットワーク番号や SSID（Service Set Identifier）により識別されます。各物理アクセスポイントの無線インタフェースごとに 16 個までの VAP を定義できます。

1. **Wireless > Access Point > AP Profile > AP Profiles SSID** の順にメニューをクリックし、以下の画面を表示します。

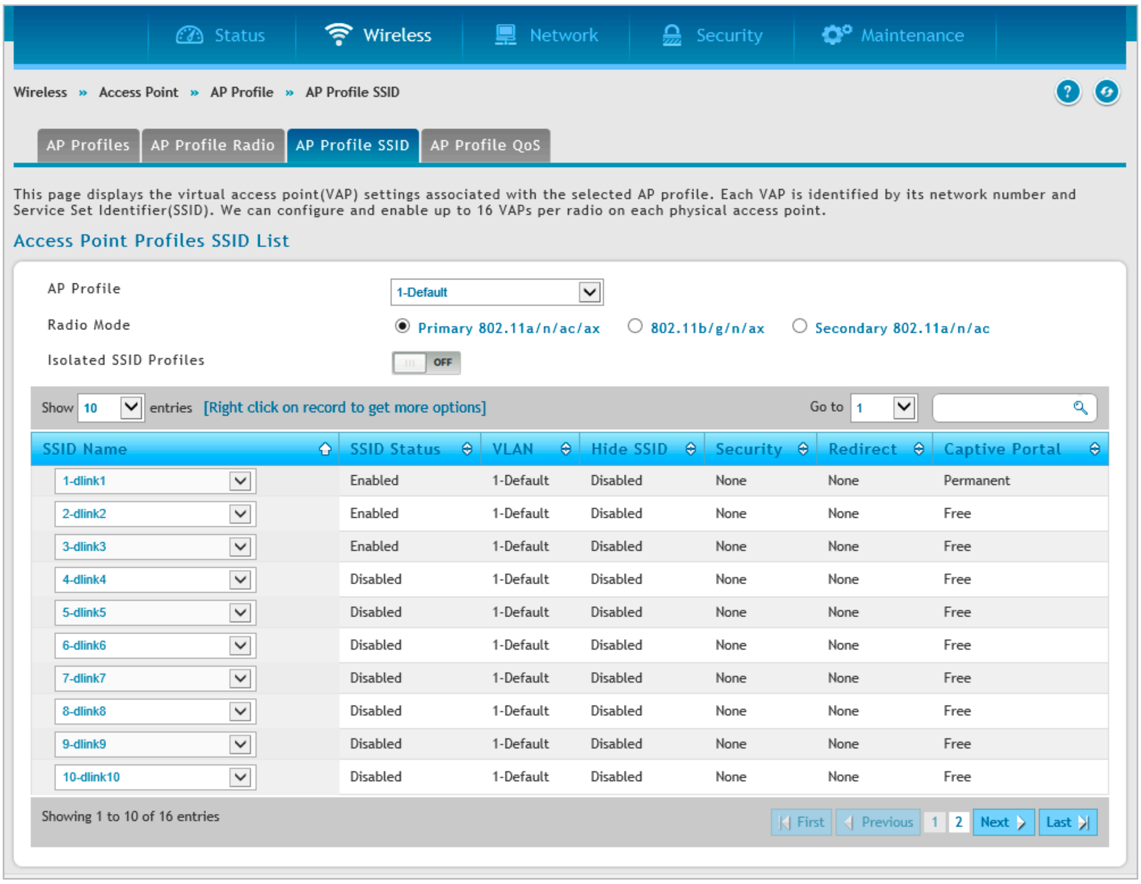


図 5-40　Access Point Profiles SSID List 画面

2. プルダウンメニューから AP プロファイルを選択します。

3. 「Radio Mode」で無線の接続モードを選択します。

4. 「SSID Name」のドロップダウンリストで SSID を選択します。

5. SSID のエントリを右クリックし、「Enable」または「Disable」を右クリックすることで、SSID を有効または無効にします。

注意 SSID ID1 は常に有効です。最初の SSID を有効にしないと、最初のスロットで別の SSID に交換できるように新しい SSID を作成する必要があります。

6. 既存の SSID を編集するために、右クリックし、「Edit」を選択します。新しく SSID プロファイルを作成するには、「Add New SSID Profile」ボタンをクリックします。

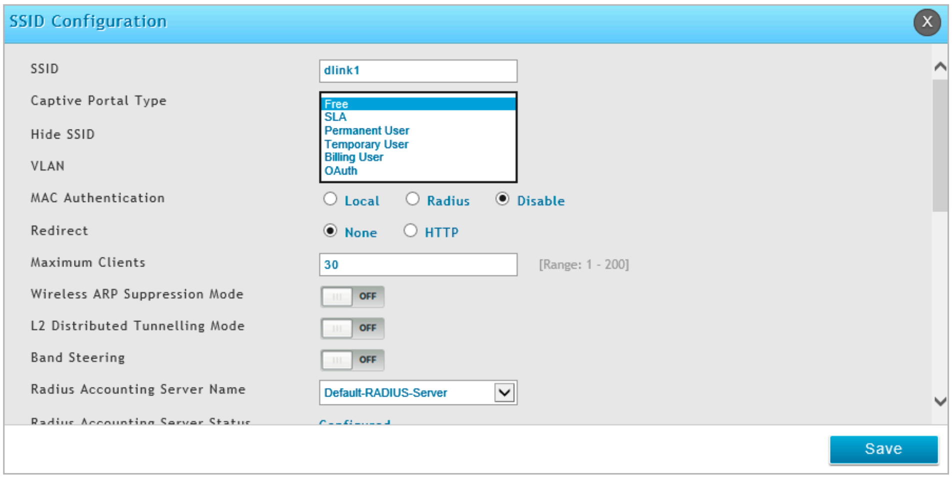


図 5-41　SSID Configuration 画面

注意 SSID ID1 は常に有効です。最初の SSID を有効にしないと、最初のスロットで別の SSID に交換できるように新しい SSID を作成する必要があります。

7. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
SSID	無線ネットワーク名を入力します。SSID はご使用の無線ネットワーク内の全デバイスで同じであり、大文字と小文字を区別していることをご確認ください。
Captive Portal Type	SSID をもとにキャプティブポータルのタイプを選択します。SSID へのアクセスには以下のタイプがあります。 ・ Free - この SSID に接続するユーザは認証の必要がありません。 ・ SLA - この SSID に接続するユーザは、この SSID 以外の何かにアクセスする前に「Service Level Agreement」を受け入れる必要があります。 ・ Permanent User - ユーザは、この SSID 以外のデータにアクセスする前に認証される必要があります。パーマネントキャプティブポータルユーザのみ、この SSID からログインできます。 ・ Temporary User - ユーザは、この SSID 以外のデータにアクセスする前に認証される必要があります。フロントデスクユーザが作成した一時的なキャプティブポータルユーザのみ、この SSID からログインできます。 ・ Billing User - ユーザは、この SSID 以外のデータにアクセスする前に認証される必要があります。オンラインの無線サービスの購入を通じて作成された一時的なキャプティブポータルの課金ユーザです。無線サービスパッケージは「Login Profile」で定義されます。 ・ OAuth - Facebook、Google などのアカウントによるログインを行います。
MAC Bypass	「Captive Portal Type」が「Permanent User」の場合、SSID で MAC バイパス機能を有効 / 無効に設定します。「Configure MAC Bypass List」をクリックすると、クライアントの MAC アドレスの設定画面に遷移します。
Enable Redirect	「Captive Portal Type」が「Free」以外 の場合、キャプティブポータル認証後の指定 Web ページへのリダイレクトを有効 / 無効に設定します。
URL	キャプティブポータルユーザが認証後にリダイレクトされる Web ページの URL を入力します。
Authentication Server	「Captive Portal Type」が「Permanent User」の場合、認証サーバを選択します。この SSID のキャプティブポータルにログインするすべてのユーザは、選択したサーバを通して認証されます。利用可能な認証サーバは、「Local User Database」、「RADIUS Server」、「LDAP Server」、または「POP3」です。
Authentication Type	「Captive Portal Type」が「Permanent User」で、「Authentication Server」が「RADIUS Server」の場合、次の認証タイプを選択します。：PAP、CHAP、MSCHAP、または MSCHAPv2
Primary/Secondary/Third LDAP Server	「Captive Portal Type」が「Permanent User」で、「Authentication Server」が「LDAP Server」の場合、LDAP サーバを指定します。
Captive Portal (SLA) Profile	
(SLA) Login Profile Name	「Captive Portal Type」が「Permanent User」または「Temporary User」の場合、「Login Profile」を選択します。利用可能なプロファイルのいずれもこの SSID で使用できます。
Hide SSID	SSID のブロードキャストを隠すと、ステーションによるアクセスポイントの自動検出を阻止します。アクセスポイントのブロードキャスト SSID を隠すと、クライアントステーションで使用可能な SSID の一覧に SSID 名が表示されません。その代わりに、クライアントは接続前に、サプリカントに設定されている正確な SSID 名を持つ必要があります。ブロードキャスト SSID を無効にすることで、あるクライアントが偶然ネットワークに入ってくることを防ぐことができます。ただし、暗号化されていないトラフィックに対するハッカーからの簡単な攻撃（接続や監視）を防ぐことはできません。 ・ ON - SSID は隠されます。 ・ Off - SSID はブロードキャストされます。
VLAN	VLAN ID を入力します。この VLAN ID が作成済みであることを確認してください。（**Network > VLAN > VLAN Settings**）

項目	説明
MAC Authentication	有効な場合、無線クライアントがネットワークに接続するためには、アクセスポイントによる認証が必要です。MAC 認証を使用するには、以下のデータベースの 1 つにクライアントの MAC アドレスを設定します。 ・Local ・Radius データベースでは、初期アクションをそのクライアントの許可または拒否に設定するか、または定義済みのグローバルアクションを使用します。MAC 認証は特定の MAC アドレスを持つクライアントへのアクセスを許可または拒否するために「Open」モードで動作するネットワークで役に立ちます。また、MAC 認証は 802.1X セキュリティ方式に関連して使用され、802.1X 認証より前に行われます。 「RADIUS」を選択した場合はパスワードを入力します。
Wireless ARP Suppression Mode	モードを有効にすると、アクセスポイントは、無線インタフェースにブロードキャストされた ARP リクエスト数を減少させることができます。ブロードキャストを減少させると、無線クライアントの電力の節約を助けます。省電力モードを使用する無線クライアントは、ブロードキャストフレームを検出すると起動して、より多くの電力を使用する必要があります。 注意　本機能を有効にすると、DHCP パケットを検索する余分なパケットフィルタリングと ARP リクエスト並びに応答パケットへの余分な処理のためにパケットフォワーディング性能をわずかに低下させます。IPv4 を使用しないネットワークでは、本機能を有効にするべきではありません。
L2 Distributed Tunneling Mode	L2 トンネルモードは、統合無線コントローラに何もデータトラフィックを送信しないで、無線クライアントに L3 ローミングをサポートするために使用されます。メニューを使用して、モードを有効または無効にします。統合無線コントローラが、ハードウェアアクセラレーションまたはハードウェアベースの L2 トンネルをサポートしない場合には、L2 トンネリングを推奨します。 注意 **1.** すべてのアクセスポイントを管理するコントローラがただ 1 つあり、そのコントローラがダウンしてしまうと、すべてのアクセスポイントがその帯域でシャットダウンし、トンネルは終了します。コントローラが回復して、アクセスポイントが再び管理状態になった後に、前にトラフィックをトンネリングしていたクライアントは、現在位置するネットワークで、再度関連付けられて、IP アドレスを取得します。この IP アドレスは、トンネルに使用された IP アドレスとは異なり、トラフィックはトンネルされません。 **2.** ネットワークにはピアコントローラがあり、ピアコントローラが管理するアクセスポイント間でトンネルを確立する場合、コントローラがホーム AP の管理に失敗すると、アソシエーション AP を管理するコントローラは、失敗を検出して、トンネルを終了します。この時点で、クライアントは切断されます。クライアントが再接続する場合、新しい IP アドレスを取得します。 **3.** アソシエーション AP を管理するコントローラがエラーになると、シナリオは上の項目 1 と同じになります。アクセスポイントはすべての無線電波をダウンして、クライアントを切断します。
Band Steering	VAP ベースの 5GH 優先機能を有効 / 無効に設定します。
Radius Accounting Server Name	RADIUS Use Network Configuration を ON にした場合、Radius Accounting サーバを選択します。
Radius Accounting Server Status	RADIUS Use Network Configuration を ON にした場合、RADIUS 認証サーバが VAP に設定されているかどうかを示します。
Accounting Mode	RADIUS Use Network Configuration を ON にした場合、無線クライアントに対する Radius アカウンティングを有効にします。
Security	デフォルトの AP プロファイルでは、セキュリティメカニズムを使用していません。ご使用のネットワークを保護するためには、セキュリティメカニズムを選択し、未認証の無線クライアントがネットワークにアクセスすることを防止することをお勧めします。 ・None - セキュリティメカニズムを使用しません。 ・OWE - OWE(Opportunistic Wireless Encryption) セキュリティを有効にします。 ・WEP - WEP セキュリティを有効にします。「WEP の設定オプション」の項目を入力します。 ・WPA/WPA2 - WPA/WPA2 セキュリティを有効にします。「WPA/WPA2 設定オプション」の項目を入力します。 ・WPA2/WPA3 - WPA2/WPA3 セキュリティを有効にします。「WPA2/WPA3 設定オプション」の項目を入力します。
Client QoS	ネットワークレベルで AP Client QoS を有効 / 無効に設定します。
Client QoS Bandwidth Limit Down.	アクセスポイントからのクライアントの最大受信レート（bps/ 秒）を設定します。
Client QoS Bandwidth Limit Up.	クライアントからアクセスポイントへの最大送信レート（bps/ 秒）を設定します。
Client QoS Access Control Down	外向き（ダウンストリーム）トラフィックにおいて、VAP が紐づくクライアントに適用されるアクセスコントロールリストのルール。
Client QoS Access Control Up	内向き（アップストリーム）トラフィックにおいて、VAP が紐づくクライアントに適用されるアクセスコントロールリストのルール。

項目	説明
Client QoS Diffserv Policy Down	外向き（ダウンストリーム）トラフィックにおいて、VAP が紐づくクライアントに適用される Diffserve ポリシー。
Client QoS Diffserv Policy Up	内向き（アップストリーム）トラフィックにおいて、VAP が紐づくクライアントに適用される Diffserve ポリシー。

AP プロファイル QoS の設定

Wireless > Access Point > AP Profile > AP Profile QoS メニュー

QoS（Quality of Service）機能は、複数のキューにパラメータを指定することで、従来の IP データをはじめ VoIP（Voice over IP）や他の音声、映像、ストリーミングメディアタイプなど無線コントローラを経由する様々な無線トラフィックに対して、より高いスループットとパフォーマンスの向上を可能にします。

無線コントローラに QoS を設定すると、様々な無線トラフィックタイプの既存キューにパラメータを設定し、伝送時の最大 / 最小待ち時間を（コンテンション画面により）効果的に指定することができます。ここで説明する設定は、アクセスポイントのデータ伝送動作、クライアントステーションには適用されません。

アクセスポイントの EDCA（Enhanced Distributed Channel Access）パラメータは、アクセスポイントからクライアントステーションへのトラフィックフローに影響します。ステーションの EDCA パラメータは、クライアントステーションからアクセスポイントへのトラフィックフローに影響します。

カスタム QoS 設定を指定できます。または、データトラフィックあるいは音声トラフィックのために最適化された定義済み設定を持つ AP プロファイルを設定するテンプレートを選択できます。

1. **Wireless > Access Point > AP Profile > AP Profiles QoS** の順にメニューをクリックし、以下の画面を表示します。

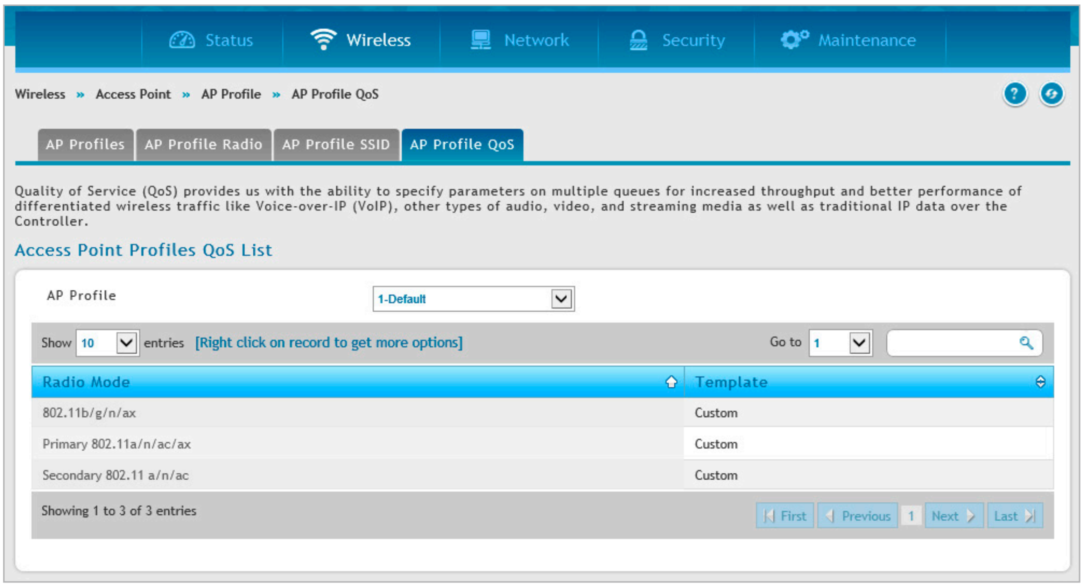


図 5-42　Access Point Profiles QoS List 画面

2. AP プロファイルを右クリックして、「Edit」を選択します。

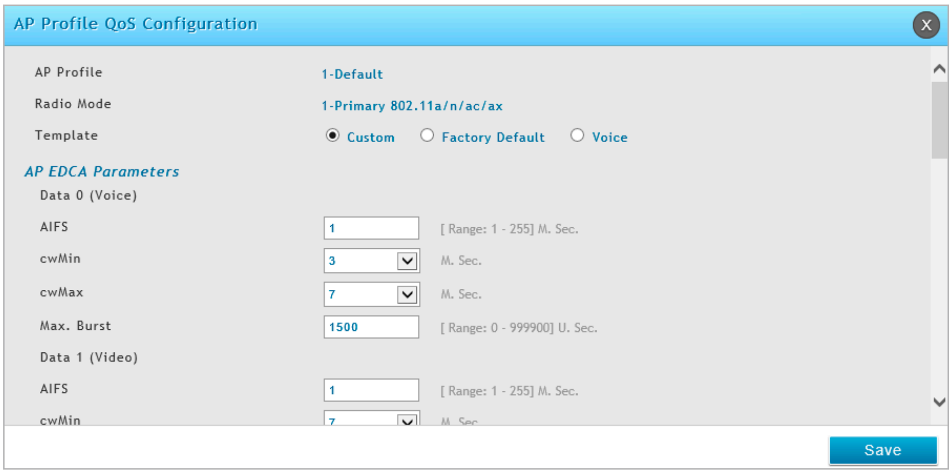


図 5-43　AP Profiles QoS Configuration 画面

3. 以下のフィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
AP Profile	AP プロファイル名を表示します。
Radio Mode	無線の接続モードを表示します。
Template	QoS テンプレートを選択して、AP プロファイルに適用します。 • Custom - アクセスポイントおよびステーションのパラメータを変更できます。 • Voice または Factory Default - 無線コントローラは選択したテンプレートに定義済み設定を使用します。
AP EDCA Parameters	
Queue	アクセスポイントからステーションに送信する様々なデータタイプにキューを定義します。 • Data 0（Voice）- 高優先度キュー、最小遅延。VoIP やストリーミングメディアなどの遅延に敏感なデータは自動的に本キューに送られます。 • Data 1（Video）- 高優先度キュー、最小遅延。遅延に敏感なビデオデータは自動的に本キューに送られます。 • Data 2（Best Effort）- 中間の優先度キュー、中間のスループットおよび中間の遅延。一般的な IP データは本キューに送られます。 • Data 3（Background）- 最低優先度キュー、高スループット。高いスループットを必要とする大容量データや、遅延に敏感ではないデータは本キューに送られます（例 : FTP データなど）。
AIFS	AIFS（Arbitration Inter-Frame Spacing）では、データフレーム間の待ち時間（1-255）を指定します。 待機時間はスロットで測定されます。
cwMin	cwMin（最小コンテンションウィンドウ）は、伝送リトライの「初回ランダムバックオフ待ち時間」（画面）を定義するアルゴリズムに使用します。本フィールドの値は、「初回ランダムバックオフ待ち時間」の範囲の上限として指定します。単位はミリ秒です。1 番目のランダム（任意）番号は、0 から本フィールドで指定する値の中から生成されます。データフレームが送信される前に、1 番目のランダムバックオフ待ち時間が失効すると、リトライカウンタは 1 増加し、ランダムバックオフ値（画面）は 2 倍の値になります。このランダムバックオフ値が、次のフィールドの cwMax で定義する値に到達するまで、失効に伴って値を倍にしていきます。 有効な値は、1、3、7、15、31、63、127、255、511、または 1024 です。 cwMin 値には cwMax で定義する値より小さい値を指定してください。
cwMax	cwMax（最大コンテンションウィンドウ）は、ランダムバックオフ値の上限です。 このランダムバックオフ値が、ここで定義する値に到達するまで、またはデータ送信に成功するまで、終了に伴って値を倍にしていきます。ランダムバックオフ値が、本フィールドで指定した値に到達すると、リトライは「リトライ許可最大回数」に到達するまで継続されます。 有効な値は、1、3、7、15、31、63、127、255、511、または 1024 です。 本値には「cwMin」で定義する値より大きい値を指定してください。
Max. Burst	AP EDCA パラメータ用。本フィールドに指定する値はアクセスポイントからクライアントへのトラフィックフローに対してのみ適用されます。 本値は無線ネットワークでのパケットバーストに認められる最大バースト長です。パケットバーストとはヘッダ情報なしで送信できる複数のフレームの集まりです。オーバヘッドを少なくすることにより、高スループットと高パフォーマンスを実現できます。 • 設定可能範囲：0-999900
WMM Mode	WMM（Wi-Fi Multimedia）機能は初期値では有効です。WMM が有効であると、QoS 優先制御や無線メディアアクセスの調整も有効になります。また、D-Link 社のコントローラの QoS 設定は、下り（アクセスポイントからクライアントステーション [AP EDCA パラメータ]）と上り（クライアントステーションからアクセスポイント [Station EDCA パラメータ]）両方のトラフィックフローを制御します。WMM を無効に設定すると、QoS 制御は上りのトラフィック（クライアントからアクセスポイント [Station EDCA パラメータ]）に対して無効になります。下りについては、いくつかのパラメータ [AP EDCA パラメータ] の設定が有効です。WMM が無効状態の時でも、アクセスポイントからクライアントへの下り方向（AP EDCA パラメータ）のいくつかのパラメータは設定可能です。 • ON - WMM 拡張機能を有効にします。 • OFF - WMM 拡張機能を無効にします。

項目	説明
Station EDCA Parameters	
Queue	ステーションからアクセスポイントに送信する様々なデータタイプにキューを定義します。 • Data 0（Voice）- 最高優先度キュー、最小遅延。VoIP やストリーミングメディアなどの遅延に敏感なデータは自動的に本キューに送られます。 • Data 1（Video）- 最高優先度キュー、最小遅延。遅延に敏感なビデオデータは自動的に本キューに送られます。 • Data 2（Best Effort）- 中間の優先度キュー、中間のスループットおよび中間の遅延。一般的な IP データは本キューに送られます。 • Data 3（Background）- 最低優先度キュー、高スループット。高いスループットを必要とする大容量データや、遅延に敏感ではないデータは本キューに送られます（例 : FTP データなど）。
AIFS	AIFS（Arbitration Inter-Frame Spacing）では、データフレーム間の待ち時間（1-255 ミリ秒）を指定します。待機時間はスロットで測定されます。
cwMin	cwMin（最小コンテンションウィンドウ）は、コンテンション期間のデータ転送のために「初回ランダムバックオフ待ち時間」（画面）を決定するアルゴリズムに使用されます。本フィールドの値は、「初回ランダムバックオフ待ち時間」の範囲の上限（ミリ秒）として「Minimum Contention Window」画面で指定します。1 番目のランダム（任意）番号は、0 から本フィールドで指定する値の中から生成されます。データフレームが送信される前に、1 番目のランダムバックオフ待ち時間が失効すると、リトライカウンタは 1 増加し、ランダムバックオフ値（画面）は 2 倍の値になります。このランダムバックオフ値が、次のフィールドの cwMax で定義する値に到達するまで、失効に伴って値を倍にしていきます。
cwMax	cwMax（最大コンテンションウィンドウ）は、ランダムバックオフ値の上限で、「Maximum Contention Window」画面で指定します。このランダムバックオフ値が、ここで定義する値に到達するまで、またはデータ送信に成功するまで、終了に伴って値を倍にしていきます。ランダムバックオフ値が、本フィールドで指定した値に到達すると、リトライは「リトライ許可最大回数」に到達するまで継続されます。
TXOP Limit	ステーション EDCA パラメータ用。本フィールドに指定する値はクライアントステーションからアクセスポイントへのトラフィックフローに対してのみ適用されます。TXOP（Transmission Opportunity : 送信権）は、WME クライアントが無線メディア上で送信を始める権利が発生する間隔です。この値は、クライアントステーションに対して指定します。つまり、WMM クライアントステーションが無線ネットワーク上に送信する権利を持つ時間（ミリ秒）です。

WDS 設定

WDS は、アクセスポイント同士を無線で接続し、相互に通信する機能です。
他の管理対象のアクセスポイントを経由した無線通信の WDS リンクを使用して、クラスタに管理対象のアクセスポイントを追加することができます。この機能はクライアントのローミングや複数の無線ネットワークの管理をシームレスに行うために重要です。また、必要とされるケーブル接続の量を削減することでネットワーク構造を簡素化できます。WDS を使用すると、ネットワークへの有線接続ができない屋外などにアクセスポイントを設置することが可能になります。

WDS AP グループは 2 つのアクセスポイントのタイプ（ルート AP とサテライト AP）から成ります。
ルート AP は、無線メディアにおいてブリッジまたはリピータとして機能し、有線リンクを通じてコントローラと通信します。サテライト AP は、ルート AP への WDS リンクを通してコントローラと通信します。アクセスポイントが「Managed」モードにある時は、アクセスポイントへのリモートアクセスは無効です。しかし、「Managed APs List」ページで、「Debug」機能を有効にすることで「Telnet」によるアクセスが可能です。統合化有線 / 無線アクセスシステム内の WDS - managed AP 機能のサポートには、以下の項目が含まれます。

- 無線システムには最大 12 個の WDS - managed AP グループを含むことができます。
- 各 WDS - managed AP グループには最大 4 つのアクセスポイントを含むことができます。
- 各アクセスポイントはそれぞれ 1 つの WDS AP グループにのみメンバとして所属することができます。
- 各サテライト AP は、サテライト AP 上に 1 つの WDS リンクのみ持てます。これは、1 つのサテライト AP を 1 つのルート AP に関連付ける必要があることを意味します。別のサテライト AP にサテライト AP を関連付けることはできません。

注意 DWL-8610AP のみ「Managed」モードの WDS 機能をサポートしています。その他のアクセスポイントの WDS についてはスタンドアロンモードのみサポートされます。

初期値では、アクセスポイントはルート AP として設定されます。アクセスポイントがサテライト AP として無線システムに関連付けられるためには、スタンドアロンモードでアクセスポイントに以下の設定を行います。

- サテライト AP モード。本設定により、サテライト AP は、ルート AP との WDS リンクを発見して、確立することが可能となります。初期値では、「WDS Managed Mode」は「Root AP」です。
- WDS リンクを確立するのに使用される WPA2 Personal のパスワード。サテライト AP だけが本設定を必要とします。ルート AP が管理されると、コントローラからパスワードを取得します。
- スタティックチャンネル。WDS リンクの各終端のアクセスポイントは、通信のために同じ無線帯域とチャンネルを使用する必要があります。サテライト AP を設定して、スタティックなチャンネルを使用します。ルート AP の場合、コントローラの Valid AP データベースにアクセスポイントを追加する時にはスタティックなチャンネルを設定します。
- オプションで、サテライト AP のイーサネットポートが LAN への有線アクセスを提供するためには、「WDS Managed Ethernet Port」を有効に設定する必要があります。初期値では無効です。

WDS の管理グループとそのリンクを設定するには、以下の一般的な手順を使用します。

1. アクセスポイントがスタンドアロンモードである場合、アクセスポイント管理インタフェースに接続して、サテライト AP を設定します。「WDS Managed Mode」を「Satellite AP」に指定して、「WDS Group Password」を設定します。
2. コントローラの CLI または Web ベースのインタフェースから、WDS グループを作成します。
3. WDS グループのパスワードを設定します。コントローラに設定するパスワードは、各サテライト AP に設定するパスワードと同じにする必要があります。
4. 各アクセスポイントの MAC アドレスを WDS グループに追加します。
5. リンクの各終端にあるアクセスポイントの MAC アドレスと無線インタフェースを指定することによって、WDS リンクを設定します。

WDS グループを設定および管理する際には、以下の考慮すべき事項を念頭におきます。

- WDS リンクに参加する無線インタフェースが、同じチャンネルを使用していることを確認します。チャンネルを制御するには、以下の方式のいずれかを使用します。
  - スタンドアロンモードでサテライト AP を設定する場合、「Radio」ページを開き、スタティックなチャンネルを設定します。
  - Valid AP データベースのアクセスポイントを設定する場合、無線インタフェースが使用すべきチャンネルを指定します。初期値では、チャンネルは「Auto」に設定されています。
  - AP プロファイルのための「Radio」ページでは、Auto Eligible チャンネルのリストで 1 つのチャンネルのみ選択します。初期値では、複数のチャンネルが有効です。
- サテライト AP が無線コントローラに有線で接続しないことをお勧めします。
- アクセスポイントに対する WDS AP への設定については、完了するのに最大 3 分かかる可能性があります。

WDS Managed AP の設定

Wireless > Access Point > WDS Groups > WDS Groups メニュー

1. **Wireless > Access Point > WDS Groups** の順にメニューをクリックし、以下の画面を表示します。

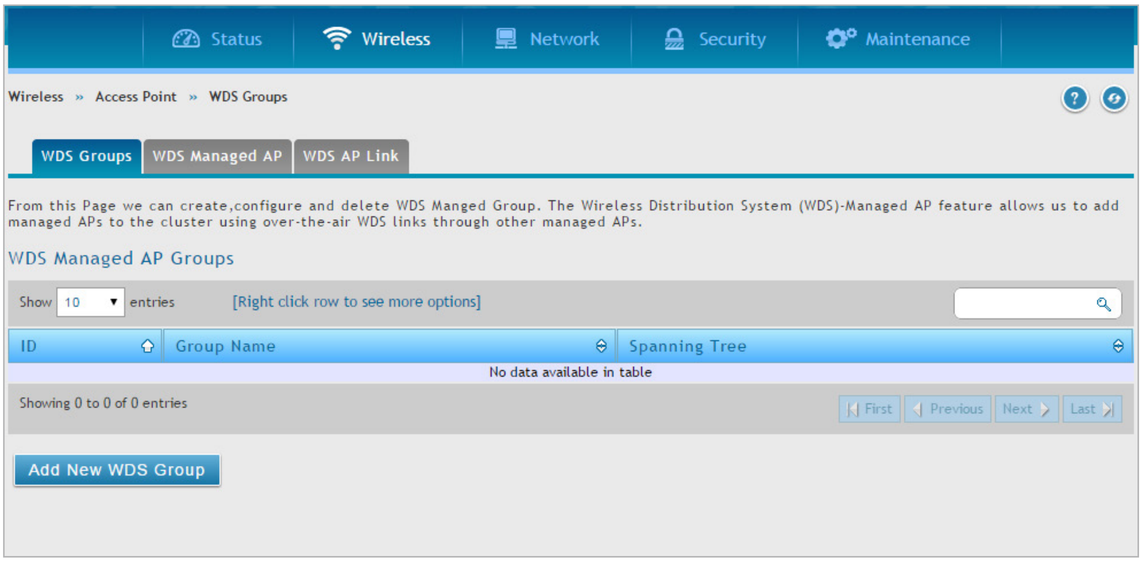


図 5-44　WDS Managed AP Groups 画面

2. 「Add New WDS Group」ボタンをクリックします。

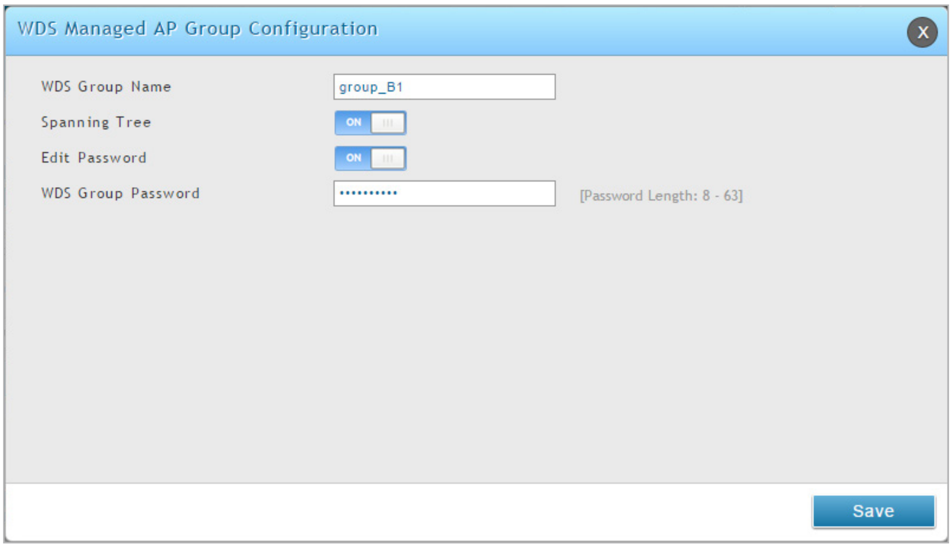


図 5-45　WDS Managed AP Group Configuration 画面

3. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
WDS Group Name	WDS AP グループの記述名（半角英数字 32 文字以内）を入力します。
Spanning Tree	スパニングツリーをこの WDS AP グループ内のすべてのアクセスポイントに有効にするかどうかを指定します。ネットワークにループの可能性がある場合、スパニングツリーを有効にする必要があります。例えば、サテライト AP が 2 つのルート AP にリンクを持つ場合、スパニングツリーは有効でなければなりません。 注意　アクセスポイントで動作するスパニングツリープロトコルは、アクセスポイントが接続するエッジスイッチで動作するスパニングツリープロトコルと通信します。
Edit Password	「ON」にすると、WDS リンクで WPA2-Personal セキュリティの確保ために使用されるパスワードを指定できます。続くフィールドにパスワードを入力します。
WDS Group Password	パスワード（8-63 文字の ASCII 文字列）を指定します。 パスワードを作成または変更するためには、「Edit Password」を「ON」にします。このパスワードは、このグループのサテライト AP に設定されたパスワードに一致する必要があります。パスワードの初期値は「AP-Group-n」（「n」は AP グループの ID）です。

WDS Managed AP の設定

Wireless > Access Point > WDS Groups > WDS Managed AP メニュー

WDS - Managed AP グループの作成後、グループのメンバであるアクセスポイントの参照、新しいメンバの追加、および既存メンバの STP 優先度値を変更します。

1. **Wireless > Access Point > WDS Groups > WDS Managed AP** の順にメニューをクリックし、以下の画面を表示します。

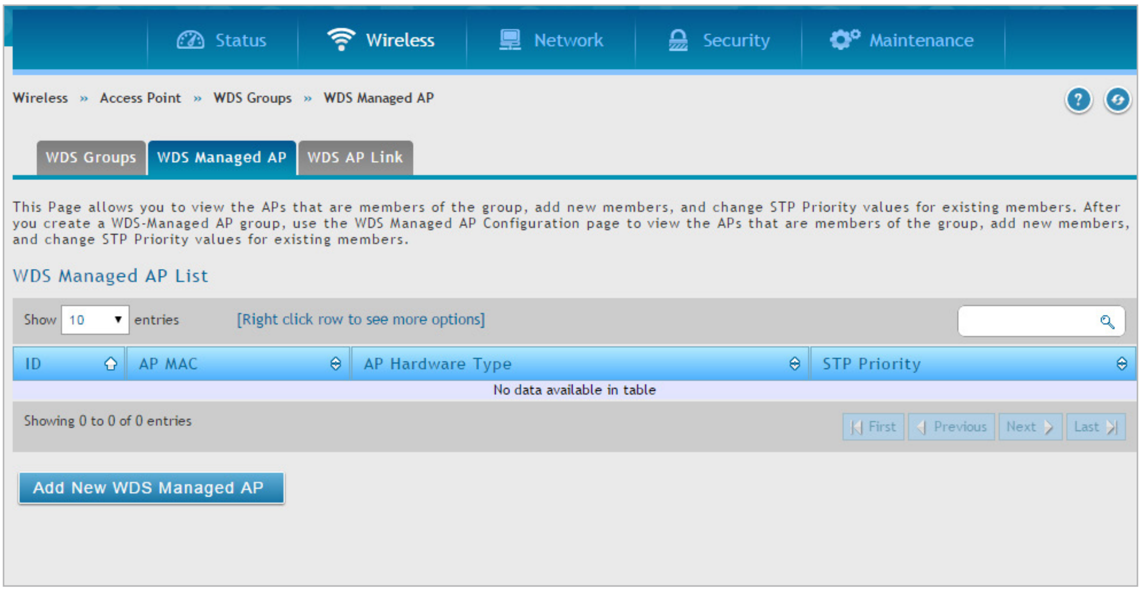


図 5-46　WDS Managed AP List 画面

2. 「Add New WDS Manage AP」ボタンをクリックし、以下の画面を表示します。

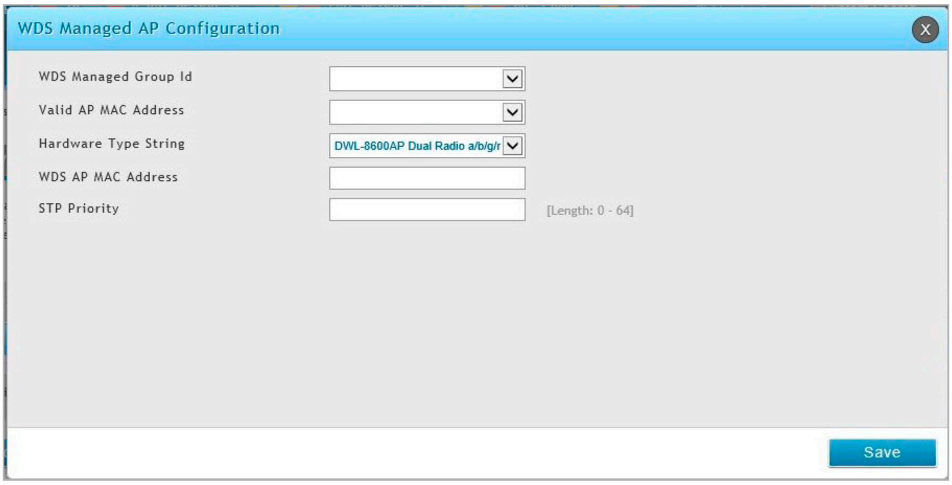


図 5-47　WDS Managed AP Configuration 画面

3. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
WDS Managed Group ID	グループに関連付ける ID を選択します。
Valid AP MAC Address	アクセスポイントの MAC アドレスを選択します。
Hardware Type String	アクセスポイントを選択します。
WDS AP MAC Address	WDS AP の MAC アドレスを入力します。
STP Priority	本アクセスポイントのスパニングツリー優先度を指定します。スパニングツリーモードが有効である時にだけ、STP 優先度は使用されます。 STP 優先度は、どのアクセスポイントがスパニングツリーのルートとして選択されるか、また、複数の等しいコストパスがトポロジに存在する場合に、どのアクセスポイントが別のアクセスポイントより上の優先度を持つかを決定します。スパニングツリー優先度の値が低いほど、そのアクセスポイントがキャンパスネットワークへのブリッジデータ用に使用されやすいことを意味します。有線ネットワークに接続するアクセスポイントに対しては、サテライト AP よりも低い優先度を割り当てるべきです。 STP 優先度値の範囲は 0-61440 で、4096 の倍数に丸められます。初期値は 36864 です。

WDS AP リンクの設定

Wireless > Access Point > WDS Groups > WDS AP Link メニュー

WDS - Managed AP グループの作成後、グループのメンバであるアクセスポイント間にリンクを設定します。

1. **Wireless > Access Point > WDS Groups > WDS AP Link** の順にメニューをクリックし、以下の画面を表示します。

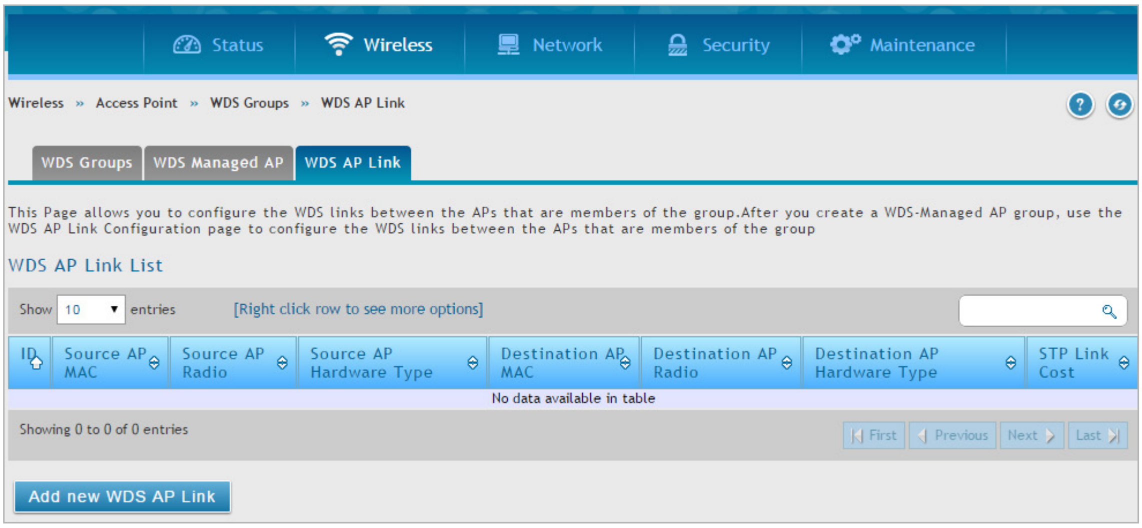


図 5-48　WDS AP Link List 画面

2. 「Add New WDS AP Link」ボタンをクリックし、以下の画面を表示します。

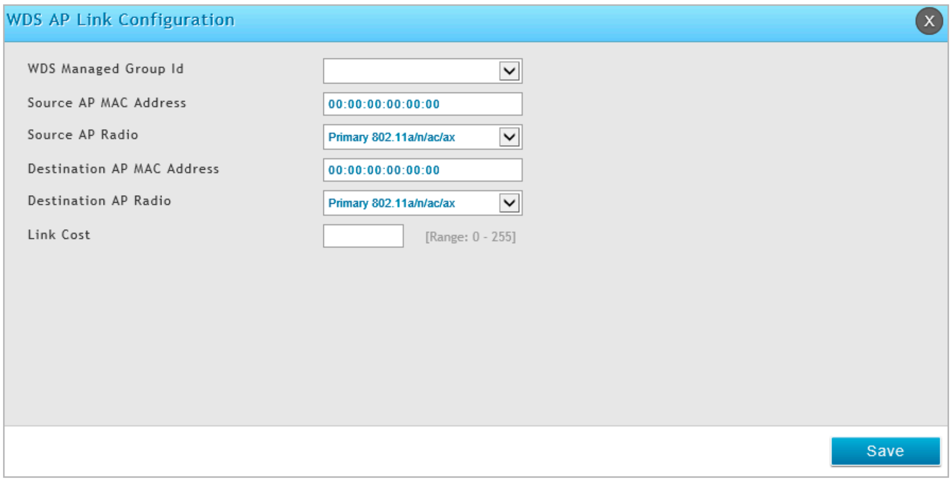


図 5-49　WDS AP Link Configuration 画面

3. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
WDS Managed Group ID	グループに関連付ける ID を選択します。
Source AP MAC Address	送信元アクセスポイントの MAC アドレスを指定します。 **注意** WDS リンクは双方向です。「Source」と「Destination」の項目は、単純に WDS リンクの終端を区別します。
Source AP Radio	送信元アクセスポイントの WDS リンク終端の無線インタフェースを指定します。
Destination AP MAC Address	グループ内の送信先アクセスポイントの MAC アドレスを指定します。
Destination AP Radio	送信先アクセスポイントの WDS リンク終端の無線接続モードを指定します。
Link Cost	WDS リンクのスパニングツリーパスコスト（0-255）を指定します。 複数の代替パスが WDS グループで定義される場合、リンクコストは、どのリンクがプライマリリンクやセカンダリリンクであるかを示すために使用されます。スパニングツリーは最も低いリンクコストを持つパスを選択します。

無線スケジュール機能

Wireless > Access Point > Radio Scheduler メニュー
無線スケジュール機能は、管理する AP の無線をタイムフレームで ON/OFF するスケジュールルールと、そのルールを管理するスケジュールプロファイルで構成されています。

スケジュールプロファイル

Wireless > Access Point > Radio Scheduler > Schedules Profiles メニュー
スケジュールプロファイルでは、AP の無線をタイムフレームで ON/OFF するスケジュールルールを管理します。まずスケジュールプロファイルを作成し、そのプロファイルにスケジュールルールを割り当てます。

1. **Wireless > Access Point > Radio Scheduler > Schedules Profiles** の順にメニューをクリックし、以下の画面を表示します。

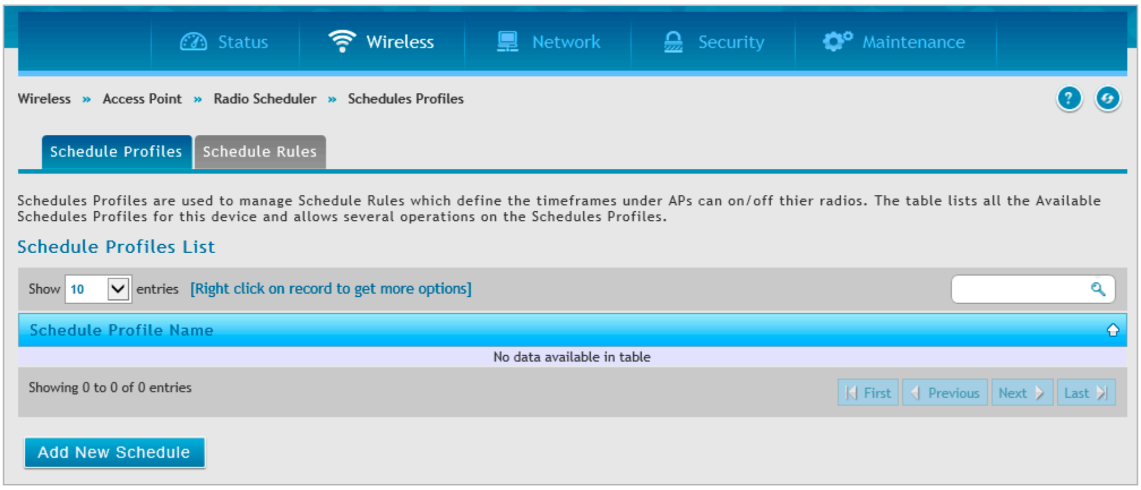


図 5-50　Schedule Profiles List 画面

2. 「Add New Schedule」ボタンをクリックします。

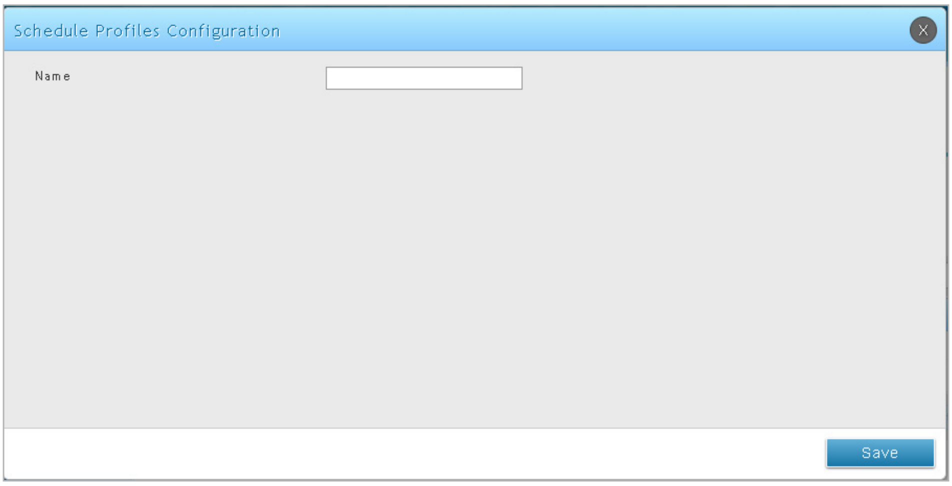


図 5-51　Schedules Profile Configuration 画面

3. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
Name	スケジュールプロファイル名を指定します。

スケジュールルール

Wireless > Access Point > Radio Scheduler > Schedules Rules メニュー

スケジュールプロファイルに割り当てる AP 無線のタイムフレームスケジュールルールを作成します。

1. **Wireless > Access Point > Radio Scheduler > Schedules Rules** の順にメニューをクリックし、以下の画面を表示します。

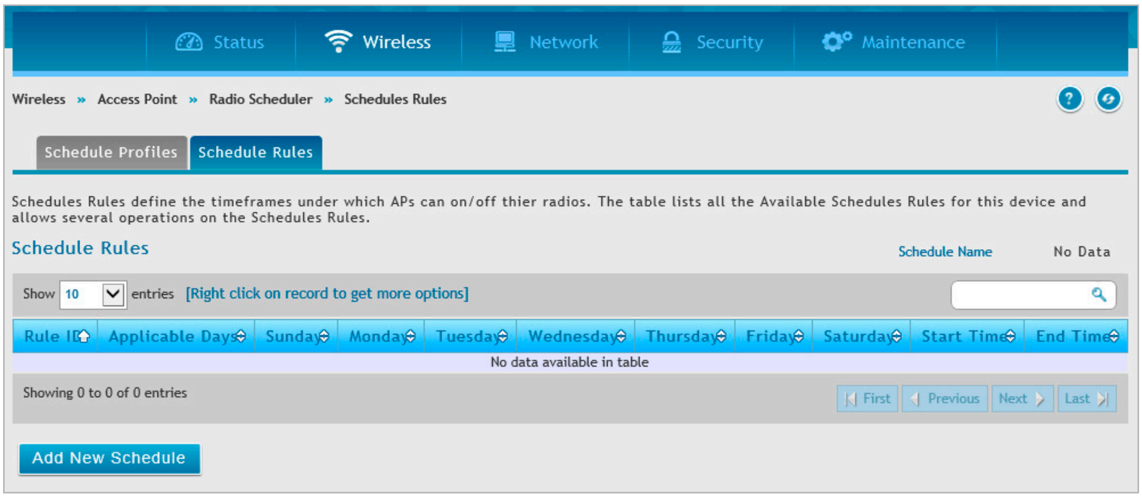


図 5-52　Schedules Rules 画面

2. 「Schedule Name」でルールを割り当てる「Schedule Profile」を選択し、「Add New Schedule」ボタンをクリックします。既にルールが割り当てられている場合は、「Schedule Rules」のリストにあるルールを右クリック、「Edit」を選択しルールを編集します。

図 5-53　Schedule Rule Configuration 画面

3. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
Schedule Profiles	「Schedule Name」で選択した、設定するスケジュールプロファイルが表示されます。
Entry ID	スケジュールルールのエントリ ID を選択します。
Applicable Days	「Daily」（毎日）、「WeekDays」（平日）、「WeekEnd」（週末）、「Day of Week」（指定曜日）から選択します。
Start Day / End Day	「Day of Week」（指定曜日）を選択した場合、開始 / 終了曜日をそれぞれ指定します。
Start Time / End Time	開始 / 終了時間をそれぞれ指定します。

ピアグループ

ピアグループ設定機能を使用すると、1 つの無線コントローラから他のすべての無線コントローラに様々な設定情報を送信できるようになります。無線コントローラの同期を維持することに加え、1 つのコントローラからクラスタ内のすべての無線コントローラを管理することができます。

ピアグループの設定

Wireless > Peer Group > Peer Configuration メニュー

クラスタ内の 1 つのコントローラから別のコントローラに、コントローラのコンフィグレーションの指定部分をコピーすることができます。本画面では、グループ内の 1 つ以上のピアコントローラにコピーするコンフィグレーションの種類を選択します。

1 つ以上のピアコントローラに送信されるコンフィグレーションに対しては変更を行うことが可能です。また、ピアコントローラから受信したコンフィグレーションを変更することもできます。コントローラからクラスタに対し、変更を自動的に伝達することはできません。コンフィグレーションをピアにコピーするためには、コントローラに対して手動でリクエストを行う必要があります。

1. **Wireless > Peer Group > Peer Configuration** の順にメニューをクリックし、以下の画面を表示します。

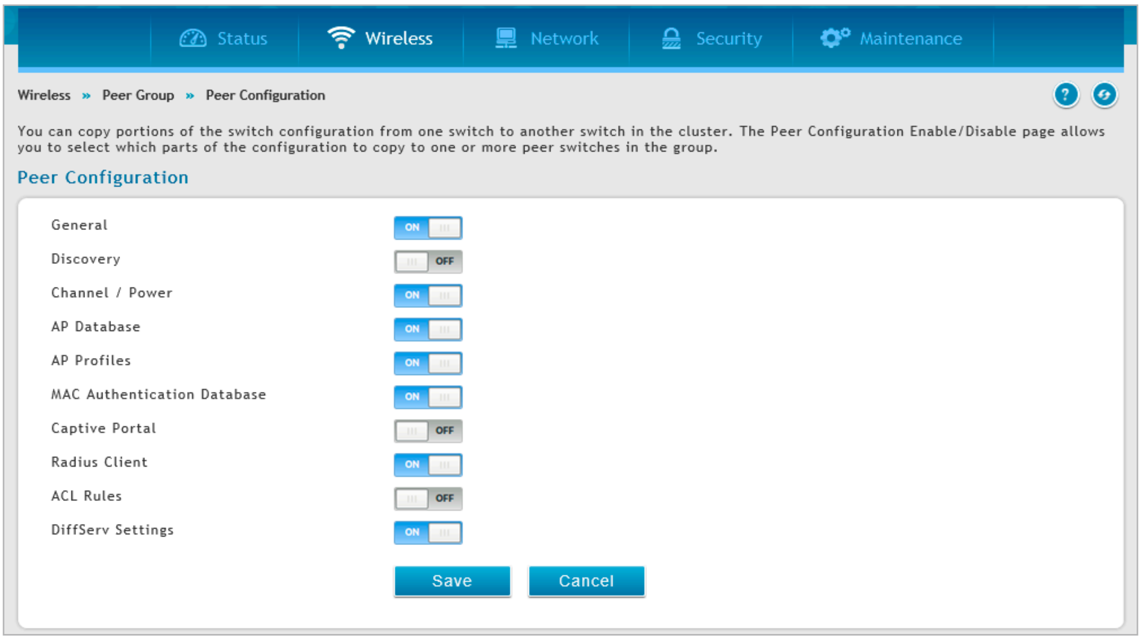


図 5-54　Peer Configuration 画面

2. 各オプションを「ON」または「OFF」に切り替え、「Save」ボタンをクリックします。

項目	説明
General	有効にすると、コントローラがピアに送信するコンフィグレーションに、基本および高度なグローバル設定を含めます。コントローラの IP アドレスは固有の設定であるため含めません。
Discovery	有効にすると、コントローラがピアに送信するコンフィグレーションに、VLAN リストおよび IP リストを含む L2、L3 ディスカバリ情報を含めます。
Channel / Power	有効にすると、コントローラがピアに送信するコンフィグレーションに RF 管理情報を含めます。
AP Database	有効にすると、コントローラがピアに送信するコンフィグレーションに AP Database（Valid AP）を含めます。
AP Profiles	有効にすると、コントローラがピアに送信するコンフィグレーションに、すべての AP プロファイルを含めます。AP プロファイルにはハードウェアタイプ、無線電波設定、SSID プロファイル、および QoS 設定などの一般的なアクセスポイント設定があります。
MAC Authentication Database	有効にすると、コントローラがピアに送信するコンフィグレーションに MAC 認証データベースを含めます。
Captive Portal	有効にすると、コントローラがピアに送信するコンフィグレーションにキャプティブポータル情報を含めます。
Radius Client	有効にすると、コントローラがピアに送信するコンフィグレーションに Client RADIUS 情報を含めます。
ACL Rules	有効にすると、コントローラがピアに送信するコンフィグレーションに ACL ルールを含めます。
DiffServ Settings	有効にすると、コントローラがピアに送信するコンフィグレーションに DiffServ 設定を含めます。

ピアグループの同期

Wireless > Peer Group > Peer Status メニュー

ピアグループで設定を同期します。

1. **Wireless > Peer Group > Peer Status** の順にメニューをクリックし、以下の画面を表示します。

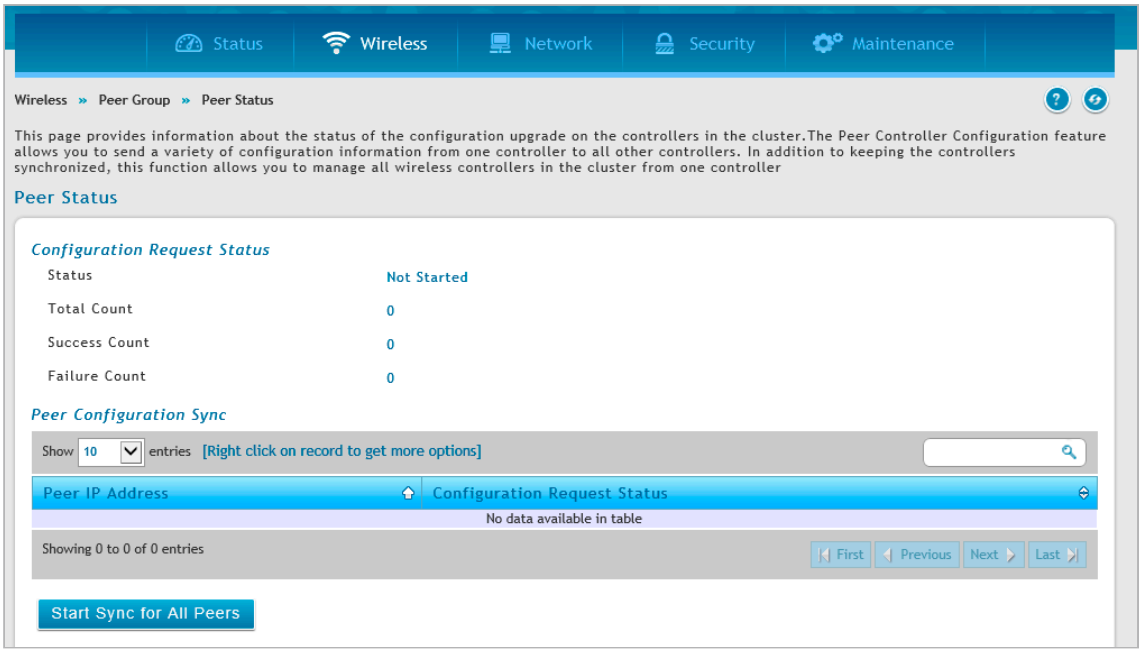


図 5-55　Peer Status 画面

2. 「Start Sync for All Peers」ボタンをクリックして、すべてのコントローラに設定を同期するか、ピアグループの 1 つを右クリックして「Start Sync」を選択して同期します。

コントローラ証明書リクエスト（X.509）

Wireless > Peer Group > Controller Provisioning > Controller Certificate Request メニュー

クラスタコントローラからの X.509 証明書リクエストを行います。コントローラ間におけるパスフレーズ認証はサポートされないため、X.509 相互証明書交換がピアコントローラ間の唯一の認証方法となります。

1. **Wireless > Peer Group > Controller Provisioning > Controller Certificate Request** の順にメニューをクリックし、以下の画面を表示します。

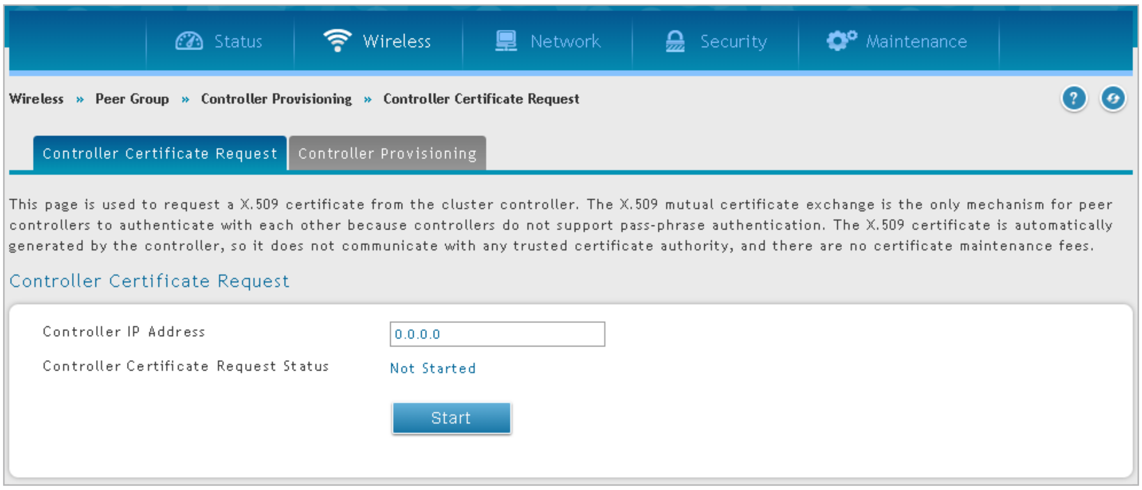


図 5-56　Controller Certificate Request 画面

2. フィールドにデータを入力し、「Start」ボタンをクリックします。

項目	説明
Controller IP Address	証明書を要求するコントローラの IP アドレスを指定します。
Controller Certificate Request Status	証明書リクエストの状況です。 • Not Started - 証明書交換が開始されていません。 • Invalid IP Address - IP アドレスが有効ではありません。 • In Progress - 証明書交換のリクエストが進行中です。 • Success - 証明書ファイルの取得に成功しました。 • Timed Out - 証明書リクエストがタイムアウトしました。

コントローラプロビジョニング

Wireless > Peer Group > Controller Provisioning メニュー

クラスタコントローラからのプロビジョニング情報リクエストを行います。新しいコントローラがプロビジョニング情報を取得した場合、クラスタに参加できるようになります。

1. **Wireless > Peer Group > Controller Provisioning** の順にメニューをクリックし、以下の画面を表示します。

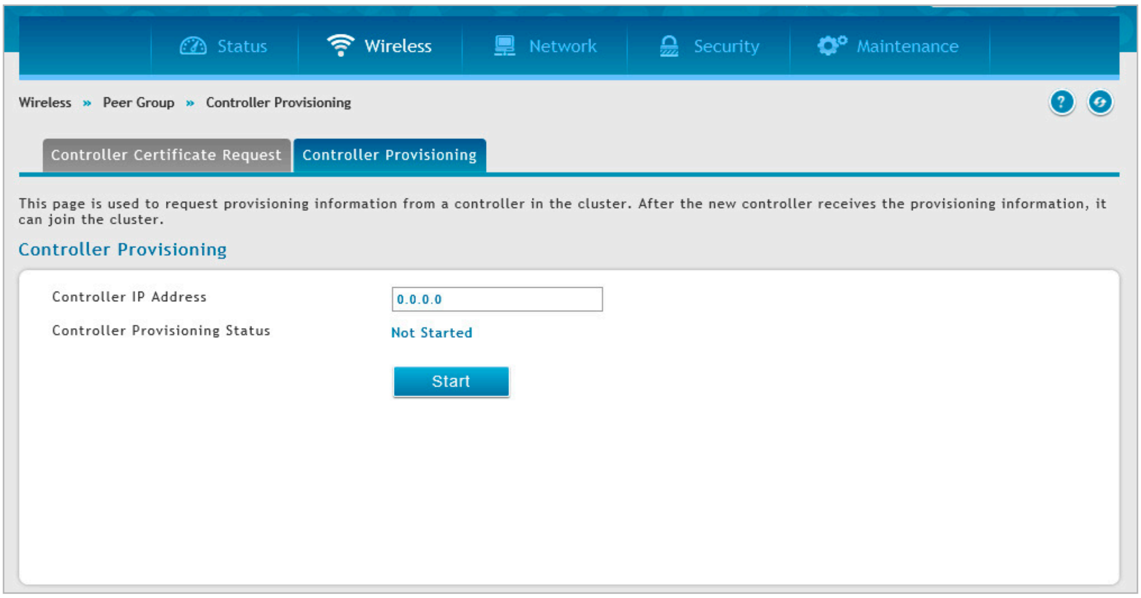


図 5-57　Controller Provisioning 画面

2. フィールドにデータを入力し、「Start」ボタンをクリックします。

項目	説明
Controller IP Address	プロビジョニングを要求するクラスタコントローラの IP アドレスを指定します。
Controller Provisioning Status	プロビジョニングリクエストの状況です。 • Not Started - リクエストが開始されていません。 • Connection Failed - クラスタコントローラとの TLS 接続に失敗しました。 • In Progress - リクエストが進行中です。 • Success - プロビジョニングに成功しました。 • Requested - プロビジョニングリクエストを実行しました。 • Failed - クラスタコントローラによる適切な回答が得られませんでした。本コントローラの起動モードがプロビジョニングに対応していないか、クラスタコントローラのプロビジョニングが無効になっていることが考えられます。

アクセスコントロースリスト（ACL）

本コントローラの「IP ACL」「MAC ACL」について設定します。
Wireless > ACL メニュー

IP アクセスコントロールリスト（IP ACL）

Wireless > ACL > IP ACL メニュー
「IP ACL」はパケットに対して連続的に合致するルールセットで構成されます。パケットがルールの判断基準に合致した場合、指定のルール動作（Permit（許可）/Deny（拒否））が実行され、他のルールはチェックされなくなります。まず IP ACL を作成し、そこに IP ACL ルールを割り当てます。IP ACL のルールは「IP ACL Rule」を使用して作成、設定されます。

1. **Wireless > ACL > IP ACL** の順にメニューをクリックし、以下の画面を表示します。

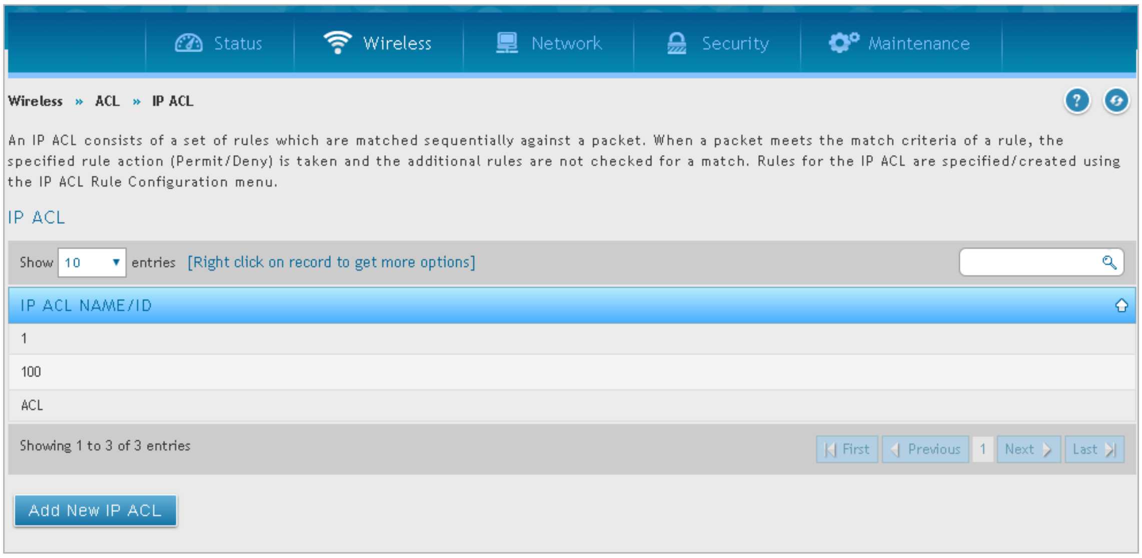


図 5-58　IP ACL 画面

2. 「Add New ACL」ボタンをクリックします。

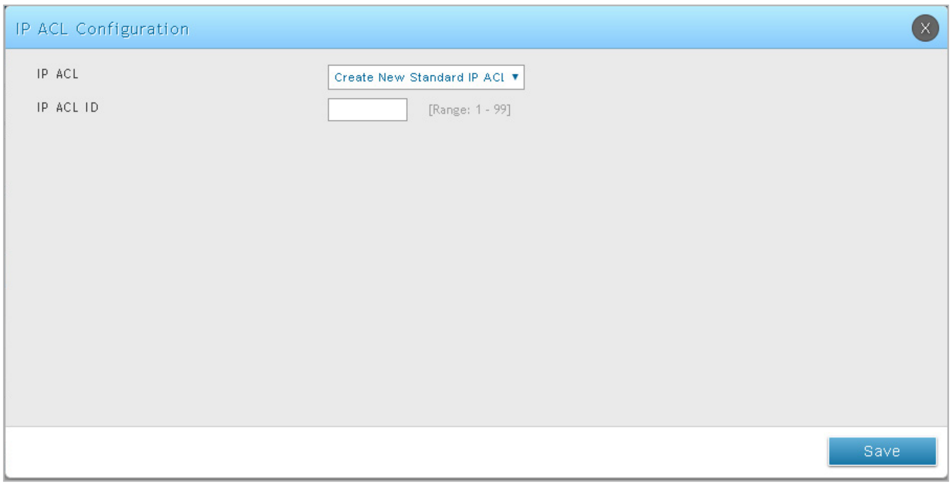


図 5-59　IP ACL Configuration 画面

3. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
IP ACL	IP ACL の種類を選択します。 • Create New Standard IP ACL - 送信元 IP アドレスからのトラフィックを許可または拒否する ACL です。 • Create New Extended IP ACL - 指定した送信元 IP アドレスから送信先 IP アドレスへのレイヤ 3 またはレイヤ 4 のトラフィックタイプを許可または拒否する ACL です。この ACL タイプは、標準の IP ACL より、詳細で高いフィルタリング性能を提供します。 • Create New Named IP ACL - IP ACL を番号ではなく名称で指定します。
IP ACL ID / IP ACL Name	• IP ACL ID - 設定する ACL の ID 番号を入力します。「IP ACL」で「Create New Standard IP ACL」または「Create Extended IP ACL」を選択すると、本項目が表示されます。標準の IP ACL に有効な ID は 1-99 です。拡張 IP ACL に有効な ID は 100-199 です。 • IP ACL Name -「IP ACL」で「Create New Named IP ACL」を選択すると、本項目が表示されます。

IP ACL ルール設定

Wireless > ACL > IP ACL Rules メニュー

「IP ACL Configuration」画面で作成した「IP ACL」を使用して、「IP Access Control Lists」（IP ACL）のルールを設定します。ルールの設定プロセスにより表示される項目は異なります。ルールを設定するには、最初に IP ACL を選択します。次に、「Rule ID（ルール ID）」「Action（動作）」「Match Every（全一致）」を設定する必要があります。「Match Every」が「False」に設定された場合、追加のオプション設定が必要になります。

1. **Wireless > ACL > IP ACL Rules** の順にメニューをクリックし、以下の画面を表示します。

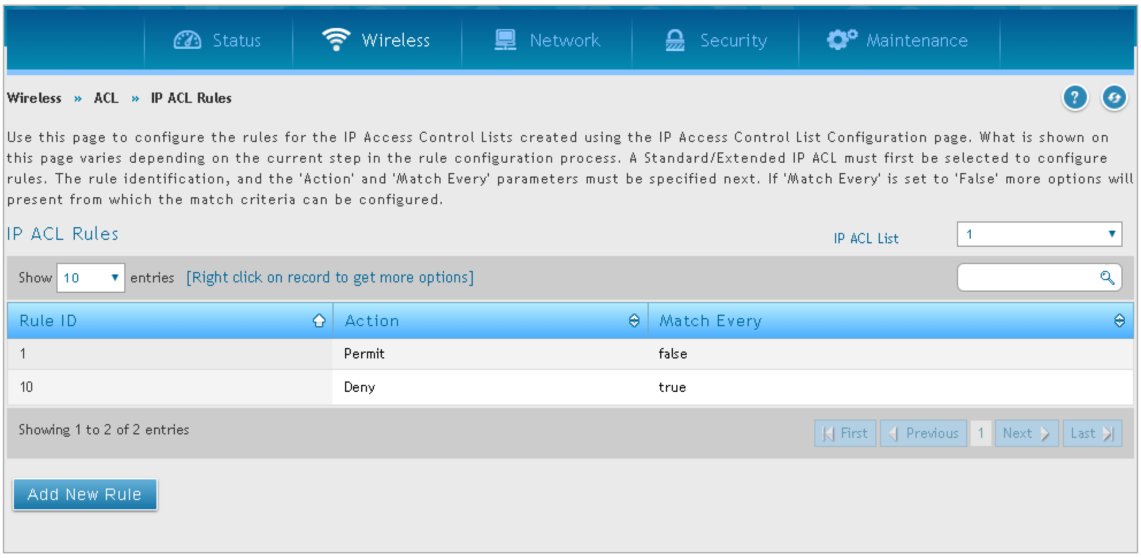


図 5-60　IP ACL Rules 画面

2. 「IP ACL List」で「IP ACL」で作成した IP ACL を選択し、「Add New Rule」ボタンをクリックします。既に割り当てられているルールを編集する場合は、「IP ACL Rules」のリストにあるルールを右クリック→「Edit」を選択し、ルールを編集します。

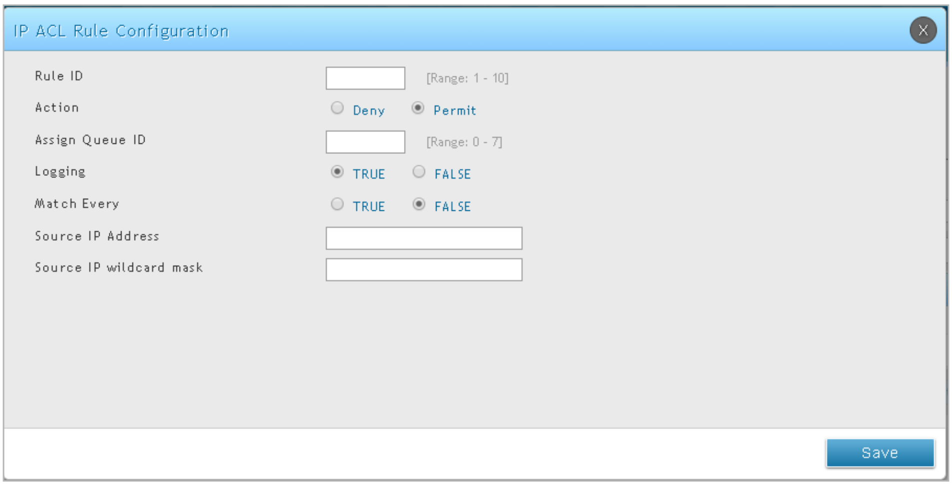


図 5-61　IP ACL Rule Configuration（Standard IP ACL）画面

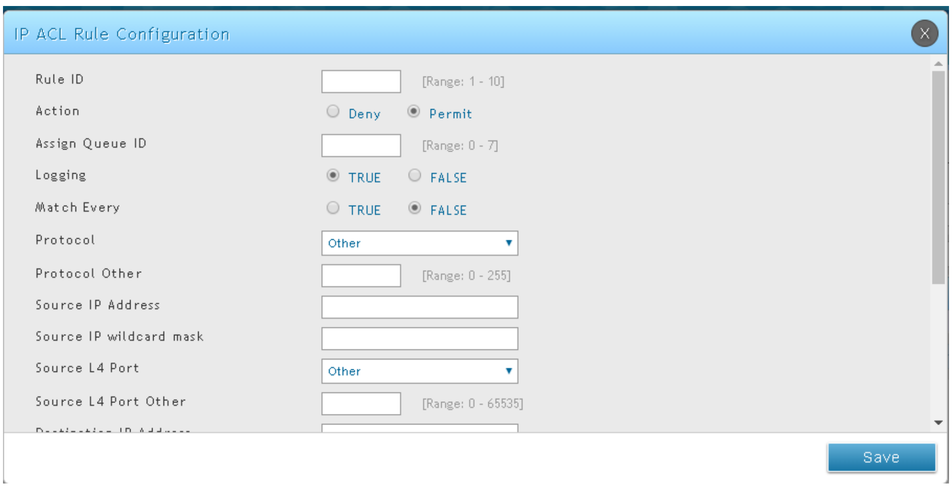


図 5-62　IP ACL Rule Configuration（Extended IP ACL / Named IP ACL）画面

3.　フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
Rule ID	新しい「Rule ID」を 1-10 の範囲で入力し、ルールを識別するために使用します。
Action	アクションを選択します。 • Permit - ACL 基準に適合するパケットを転送します。 • Deny - ACL 基準に適合するパケットを破棄します。
Assign Queue ID	「Action」に「Permit」を選択した場合に表示されます。この AP ACL ルールに適合するすべてのパケットを処理するために使用されるハードウェアイーグレスキューの識別子を指定します。キューを識別する番号（0-7）を入力します。
Logging	ログ設定を行います。「True」に設定すると、ACL ルールに対してログが有効になります。
Match Every	この ACL の基準に一致することをパケットに要求します。「True」または「False」を選択します。「True」は、すべてのパケットが選択した IP ACL に一致し、許可または拒否されること意味します。この場合、すべてのパケットがルールに一致するため、追加の一致条件は表示されません。「False」に設定すると、追加のオプションで一致条件を指定することができます。
Protocol （Extended/Named のみ）	選択した IP ACL ルールに対して一致させるパケットの IP プロトコルを指定します。指定可能な値は Other、IP、ICMP、IGMP、TCP、および UDP です。
Protocol Other （Extended/Named のみ）	「Protocol」で「Other」を指定すると表示されます。 0 から 255 の範囲で IP ACL ルールに対して一致させるパケットの IP プロトコルを指定します。
Source IP Address	パケットの送信元 IP アドレスを「.」で区切った形式で入力します。
Source IP wildcard mask	送信元 IP アドレスのワイルドカードマスクを「.」で区切った形式で入力します。
Source L4 Port （Extended/Named のみ）	パケットの送信元TCP/UDP ポートを選択します。「None」「Other」「Domain」「echo」「FTP」「FTPDATA」「http or WWW」「SMTP」「SNMP」「TELNET」「TFTP」から選択します。
Source L4 Port Other （Extended/Named のみ）	「Source L4 Port」で「Other」を指定すると表示されます。パケットの送信元 TCP/UDP ポートを 0 から 65535 の範囲で指定します。
Destination IP Address （Extended/Named のみ）	パケットの宛先 IP アドレスを「.」で区切った形式で入力します。
Destination IP wildcard mask （Extended/Named のみ）	宛先 IP アドレスのワイルドカードマスクを「.」で区切った形式で入力します。
Destination L4 Port （Extended/Named のみ）	パケットの宛先 TCP/UDP ポートを選択します。「None」「Other」「Domain」「echo」「FTP」「FTPDATA」「http or WWW」「SMTP」「SNMP」「TELNET」「TFTP」から選択します。
Destination L4 Port Number （Extended/Named のみ）	「Destination L4 Port」で「Other」を指定すると表示されます。パケットの宛先 TCP/UDP ポートを 0 から 65535 の範囲で指定します。
Service Type （Extended/Named のみ）	サービスの種類を選択します。IP ヘッダに含まれる Service Type フィールドに対する一致条件の代わりとなる方法です。ただし、それぞれで異なるユーザ表記を使用しています。サービスの種類を選択後、適切な設定を行います。 • IP DSCP - パケットの DSCP 値をルールと照合します。DSCP は、IP ヘッダの「Service Type」オクテットの上位 6 ビットとして定義されます。これはオプション設定であり、0-63 の整数で入力します。IP DSCP は、プルダウンメニューから DSCP キーワードの 1 つを選択します。「Other」オプションを選択すると DSCP 値を入力するテキストボックスが表示されます。 • IP Precedence - パケット内の「IP Precedence」は、IP ヘッダの「Service Type」オクテットの上位 3 ビットとして定義されます。「IP Precedence」値は、0-7 の整数です。 • IP TOS - パケット内の IP TOS フィールドは、IP ヘッダの「Service Type」オクテットの全 8 ビットとして定義されます。TOS Mask の 0 ビットは、TOS Bits 値におけるビットの位置を示し、パケットの IP TOS フィールドと比較に使用されます。例えば、ビット 7（ビット 7 は非常に重要です。）と 5 を設定した IP TOS 値をチェックし、ビット 1 をクリアするためには、TOS ビット値「a0」と TOS Mask「00」を使用します。 　- TOS Bits - この値は、00-FF までの 16 進数です。パケットの TOS フィールド内のビットがここで入力した 2 桁の 16 進数と一致することが必要です。 　- TOS Mask - この値は 00-FF までの 16 進数で、マスクを表します。パケット内の IP TOS フィールドと比較するために使用されるビット位置を指定します。

MAC アクセスコントロールリスト（MAC ACL）

Wireless > ACL > MAC ACL メニュー

「MAC ACL」はパケットに対して連続的に照合されるルールセットで構成されます。パケットがルールの判断基準に合致した場合、指定のルール動作（Permit（許可）または Deny（拒否））が実行され､後続のルールではチェックされなくなります。まず MAC ACL を作成し､そこに MAC ACL ルールを割り当てます。MAC ACL のルールは「MAC ACL Rule」を使用して作成、設定されます。

1. **Wireless > ACL > MAC ACL** の順にメニューをクリックし、以下の画面を表示します。

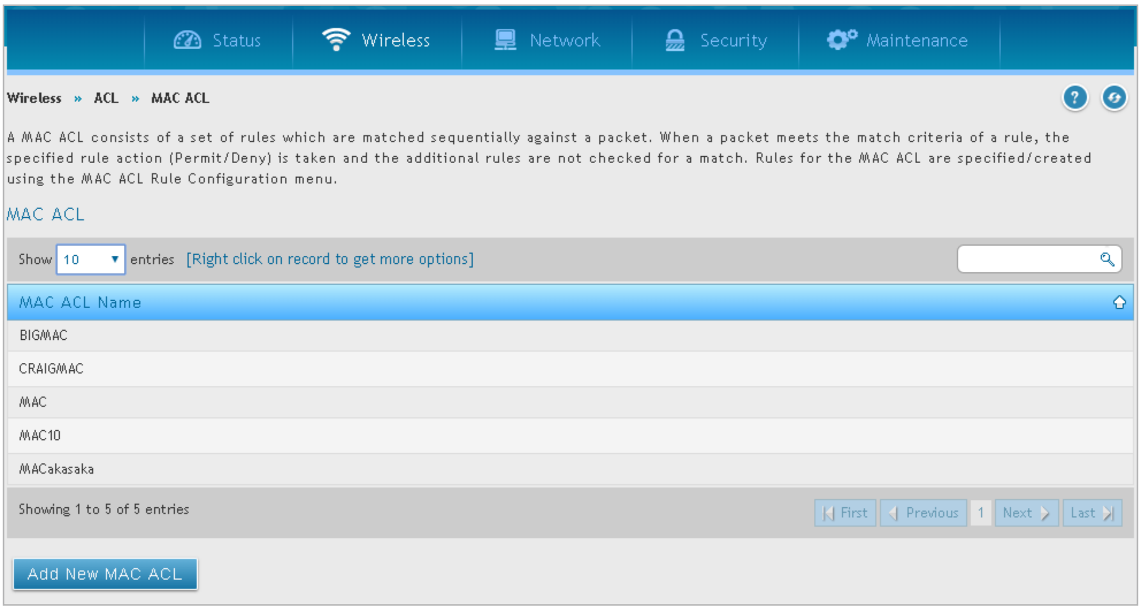


図 5-63　MAC ACL 画面

2. 「Add New MAC ACL」ボタンをクリックします。既存の MAC ACL を編集する場合は、「MAC ACL Names」のリストにあるエントリを右クリック→「Edit」を選択し、ルールを編集します。

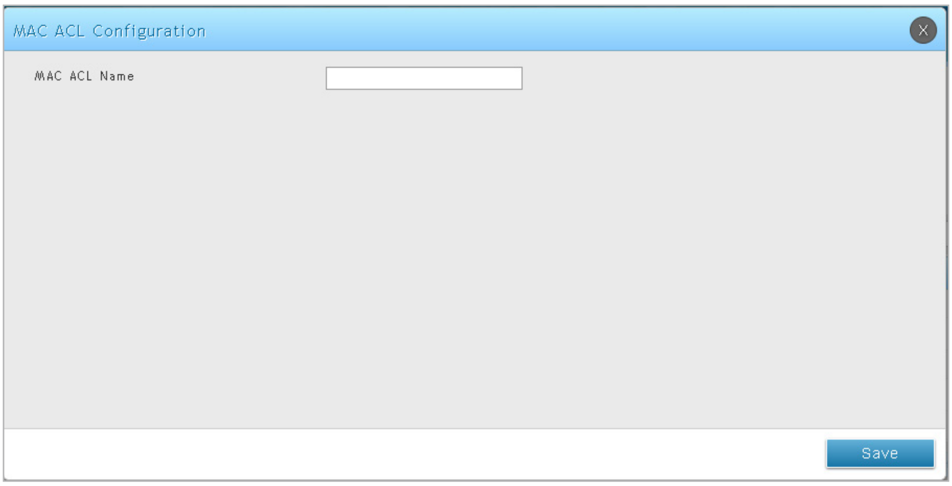


図 5-64　MAC ACL Configuration 画面

3. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
MAC ACL Name	MAC ACL 名を入力します。

MAC ACL ルール設定

Wireless > ACL > MAC ACL Rules メニュー

MAC ACL Configuration で作成した「MAC ACL」を使用して、「MAC Access Control Lists」（MAC ACL）のルールを設定します。ルールの設定プロセスにより表示される項目は異なります。「Rule ID（ルール ID）」「Action（動作）」「Match Every（全一致）」を設定する必要があります。「Match Every」が「False」に設定された場合、追加のオプションを設定します。

1. **Wireless > ACL > MAC ACL Rules** の順にメニューをクリックし、以下の画面を表示します。

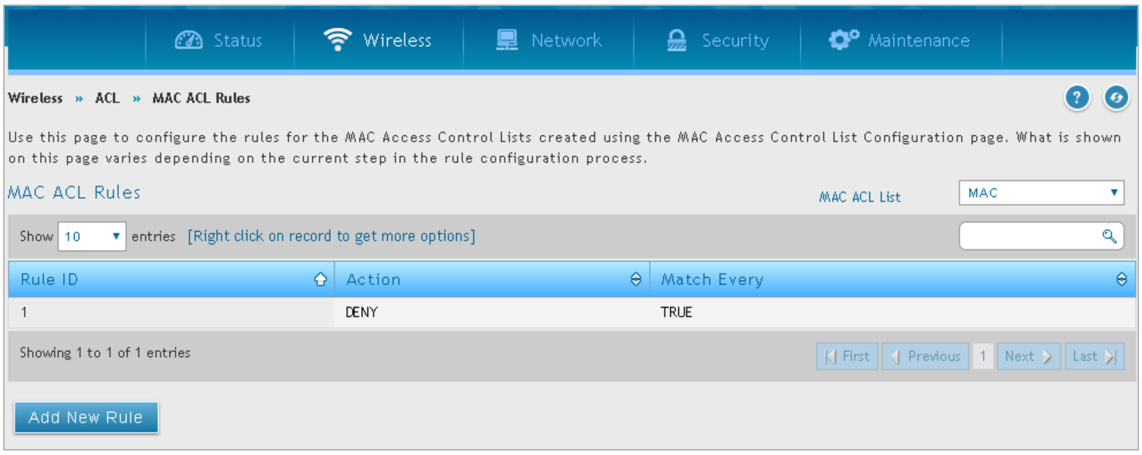


図 5-65　MAC ACL Rules 画面

2. 「MAC ACL List」で「MAC ACL」で作成した MAC ACL を選択し、「Add New Rule」ボタンをクリックします。既に割り当てられているルールを編集する場合は、「MAC ACL Rules」のリストにあるルールを右クリック→「Edit」を選択し、ルールを編集します。

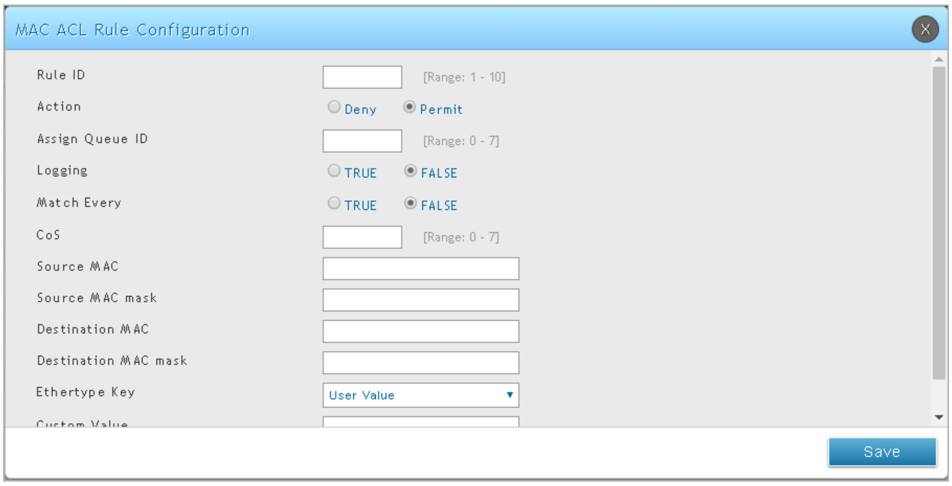


図 5-66　MAC ACL Rule Configuration 画面

3. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
Rule ID	新しい「Rule ID」を 1-10 の範囲で入力し、ルールを識別するために使用します。
Action	アクションを選択します。 • Permit - ACL 基準に適合するパケットを転送します。 • Deny - ACL 基準に適合するパケットを破棄します。
Assign Queue ID	「Action」に「Permit」を選択した場合に表示されます。この AP ACL ルールに適合するすべてのパケットを処理するために使用されるハードウェアイーグレスキューの識別子を指定します。キューを識別する番号（0-7）を入力します。
Logging	ログ設定を行います。「True」に設定すると、ACL ルールに対してログが有効になります。
Match Every	この ACL の基準に一致することをパケットに要求します。「True」または「False」を選択します。「True」は、すべてのパケットが選択した MAC ACL に一致し、許可または拒否されること意味します。この場合、すべてのパケットがルールに一致するため、追加の一致条件は表示されません。「False」に設定すると、追加のオプションで一致条件を指定することができます。
CoS	CoS 値を 0-7 の範囲で入力します。CoS（Class of Service）は、通信の優先度を表す値です。 0 が一番低く、7 が一番高い優先度を表します。
Source MAC	パケットの送信元ポートの MAC アドレスを指定します。
Source MAC mask	必要に応じて、照合する送信元 MAC に関連する MAC マスクを入力します。MAC マスクには、ワイルドカードフォーマットで「F」と「0」を使用します。「F」はビットがチェックされないことを意味し、ビット位置の「0」はデータがそのビットに与えられた値と等しくなければならないことを意味しています。有効なフォーマットは xx:xx:xx:xx:xx:xx です。
Destination MAC	パケットの宛先ポートの MAC アドレスを指定します。
Destination MAC Mask	必要に応じて、照合する宛先 MAC に関連する MAC マスクを入力します。
Ethertype Key	パケットの EtherType がこの EtherType に一致する必要があります。「Appletalk」「ARP」「IBM SNA」「IPv4」「IPv6」「IPX」「MPLS multicast」「MPLS unicast」「NetBIOS」「Novell」「PPPoE」「RARP」「User Value」から選択します。「User Value」を選択すると、カスタム EtherType 値を入力することができます。
Custom Value	「Ethertype Key」で「User Value」を指定すると表示されます。

DiffServ 設定

Wireless > DiffServ メニュー
本コントローラの「DiffServ」について設定します。

DiffServ クラス

Wireless > DiffServ > DiffServ Class メニュー
本項目では DiffServ クラス設定とマッチセレクタの設定を行います。定義された評価基準に従いパケットはフィルタ / 処理されます。フィルタの基準はクラスにより定義されます。まず、クラスの一つ以上のマッチ評価基準を定義します。

1. **Wireless > DiffServ > DiffServ Class** の順にメニューをクリックし、以下の画面を表示します。

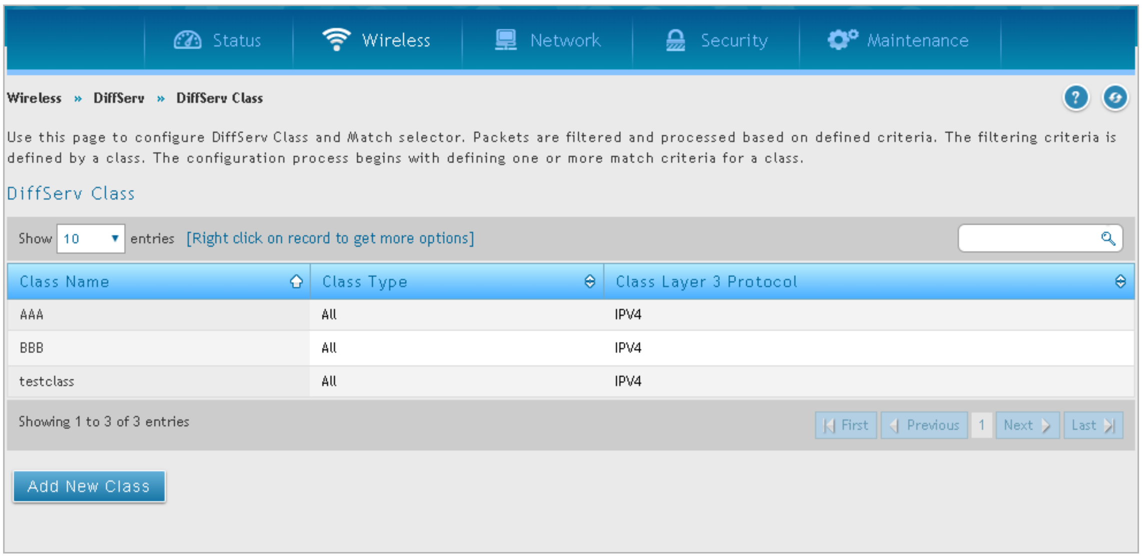


図 5-67　DiffServ Class 画面

2. 「Add New Class」ボタンをクリックします。既存の DiffServ Class を編集する場合は、「DiffServ Class」のリストにあるエントリを右クリック→「Rename」を選択し、ルールを編集します。

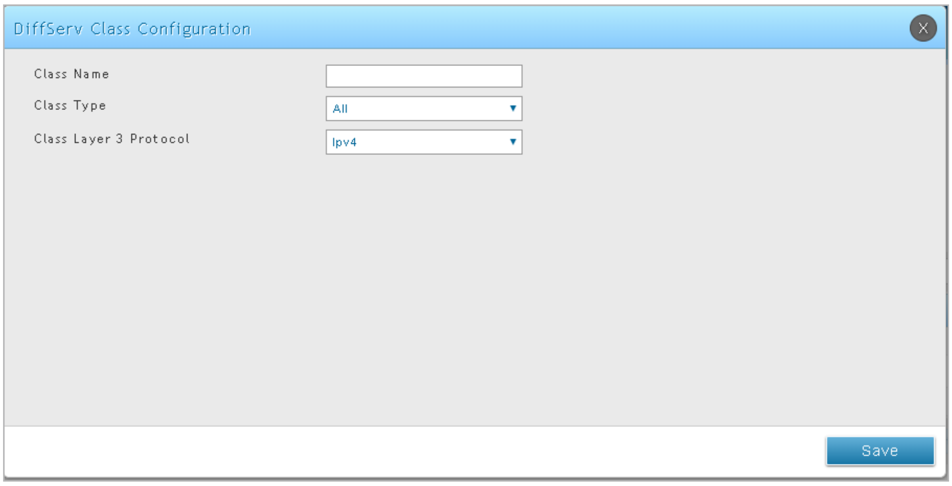


図 5-68　DiffServ Class Configuration 画面

3. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
Class Name	DiffServ Class 名を入力します。
Class Type	DiffServ Class 種類を指定します。現在、本ハードウェアは、クラスタイプに「All」だけをサポートしています。これは、パケットの一致のために、クラスに対して定義された様々な一致基準のすべてが満たされる必要があることを意味します。「All」は、すべての一致基準の論理和を表しています。
Class Layer 3 Protocol	Class Layer 3 プロトコルを指定します。IPv6 が有効な場合選択可能です。

4. 「DiffServ Class」のリストにあるエントリを右クリックし「Add Match Selector」を選択、Class Selector を追加します。

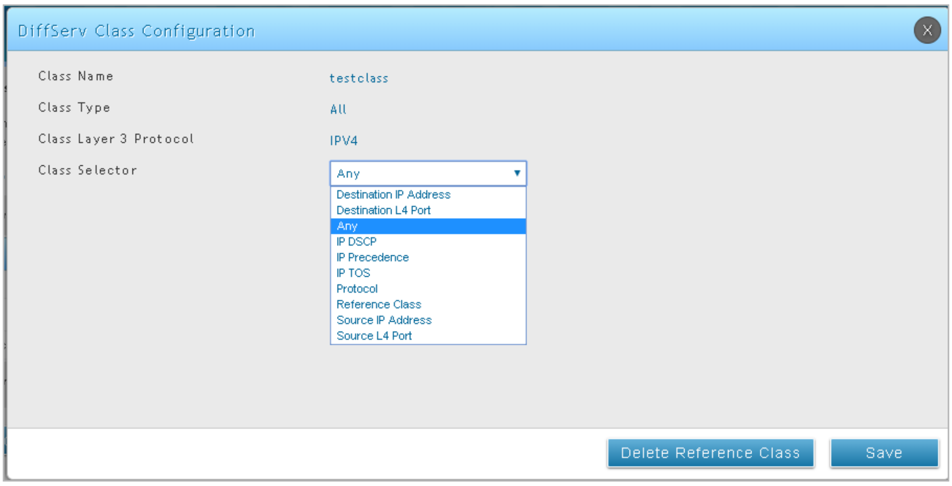


図 5-69　Diffserv Class Configuration - Class Selector 画面

項目	説明
Class Selector	指定クラスに追加できるすべての一致基準を示します。リストから一致基準を選択し追加します。一致基準と設定の各項目は以下の通りです。 • Destination IP Address - パケットの宛先ポートの IP アドレスがこのアドレスに一致する必要があります。「Destination IP Address」に、有効な宛先 IP アドレス、「Destination IP Mask」に、サブネットマスクを入力します。 • Destination Layer 4 Port - パケットの TCP/UDP 送信元ポートがこのポートに一致する必要があります。L4 キーワードとして「Other」「Domain」「echo」「FTP」「FTPDATA」「http」「SMTP」「SNMP」「TELNET」「TFTP」「WWW」から選択します。「Other」を選択すると、画面が更新されて「Destination L4 Port Number」が表示されます。（設定可能範囲：0-65535） • Any - すべてのパケットが指定クラスに一致すると見なされ、追加入力情報は必要とされません。 • IP DSCP - パケットの DSCP をクラスの一致基準に指定します。メニューから DSCP タイプを選択するか、または一致させる DSCP 値を入力します。「Other」を選択すると、「IP DSCP Value」が表示され、カスタム値を入力することができます。 • IP Precedence - パケットの IP 優先度値をクラスの一致基準に指定します。「0-7」の範囲で値を入力します。 • IP TOS - パケットの IP ヘッダ内のサービスのタイプビットをクラスの一致基準に指定します。「ToS Bits」に、パケットの「ToS」内のビットに一致する 2 桁の 16 進数を入力します。「ToS Mask」に、パケットの「IP ToS」と比較するために使用されるビット位置を指定します。 • Protocol - パケットのレイヤ 4 プロトコルが選択したプロトコルに一致する必要があります。「Other」を選択した場合は「Protocol Other」にプロトコル値を入力します。（設定可能範囲：0-255） • Reference Class - 現在のクラスに対して参照クラスとして割り当てるクラスを選択します。 • Source IP Address - パケットの送信元 IP アドレスがこのアドレスに一致する必要があります。「IP Address」に送信元 IP アドレス、「IP Mask」にサブネットマスクを入力します。 • Source Layer 4 Port - パケットの TCP/UDP 送信元ポートがこのポートに一致する必要があります。 • ルールに基づくリストから L4 キーワードを選択します。「Other」を選択した場合は画面が更新され、「Source L4 Port Other」が表示されます。パケットがルールに一致するユーザ定義の Port ID を入力します。（設定可能範囲：0-65535）

5. 「DiffServ Class」のリストにあるエントリを右クリックし「Match Criteria List」を選択すると、設定した Match Criteria の内容を表示します。

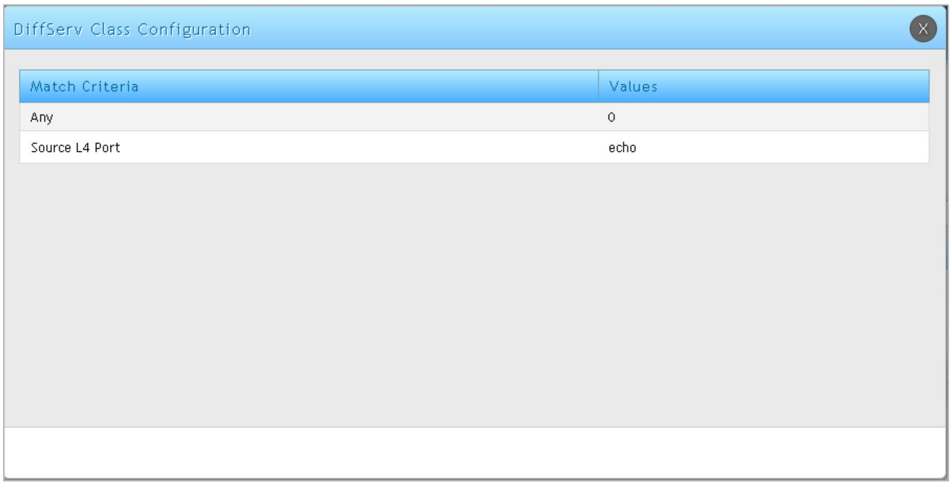


図 5-70　Diffserv Class Configuration - Match Criteria 画面

DiffServ ポリシー

Wireless > DiffServ > DiffServ Policy メニュー

本項目では DiffServ クラスを 1 つ以上のポリシーステートメントと関連付けます。

1. **Wireless > DiffServ > DiffServ Policy** の順にメニューをクリックし、以下の画面を表示します。

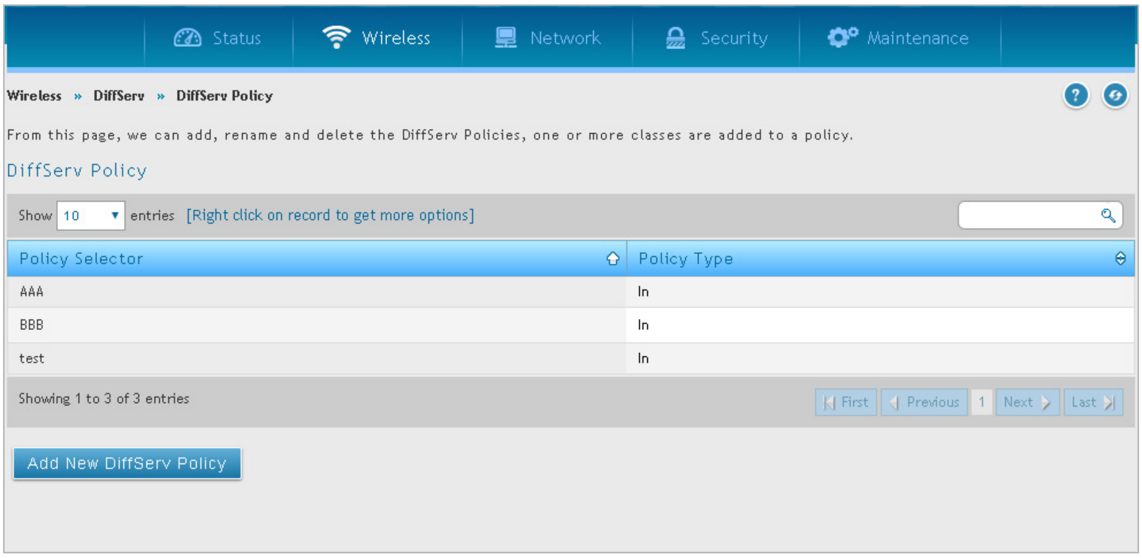


図 5-71　DiffServ Policy 画面

2. 「Add New DiffServ Policy」ボタンをクリックします。既存の DiffServ Policy を編集する場合は、「DiffServ Policy」のリストにあるエントリを右クリック→「Rename」を選択し、ルールを編集します。

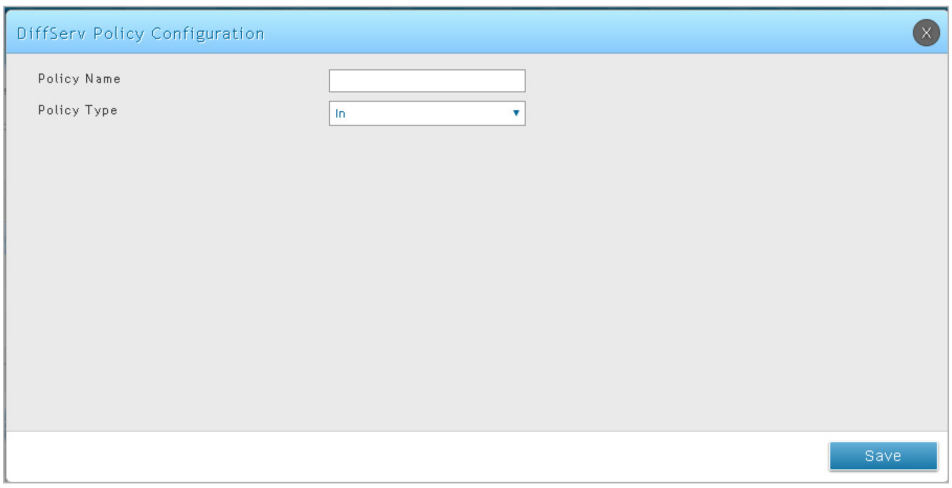


図 5-72　DiffServ Policy Configuration 画面

3. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
Policy Name	DiffServ Policy 名を入力します。
Policy Type	DiffServ Policy 種類を指定します。利用可能なポリシータイプは「In」です。これは、タイプが内向きトラフィック用であることを示しています。

4. 「DiffServ Policy」のリストにあるエントリを右クリックし「Add Selected Class」（追加）、「Remove Selected Class」（削除）を選択すると、それぞれ、ポリシーからクラスを追加、削除することができます。

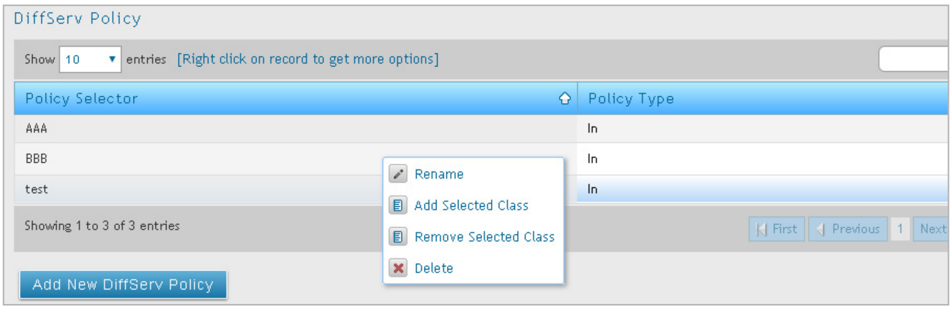


図 5-73　DiffServ Policy 画面

DiffServ ポリシークラス設定

Wireless > DiffServ > DiffServ Policy Class Defination メニュー

ポリシーにクラスを関連付けて、そのポリシークラスインスタンスに属性を定義します。

1. **Wireless > DiffServ > DiffServ Policy Class Defination** の順にメニューをクリックし、以下の画面を表示します。

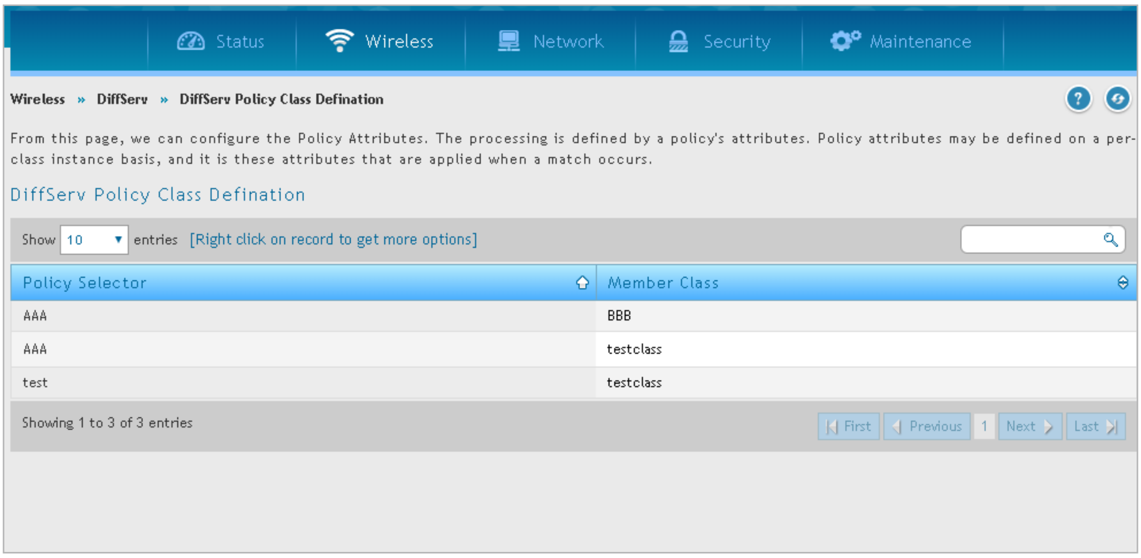


図 5-74　DiffServ Policy Class Defination 画面

2. 「Policy Selector」のリストにあるエントリを右クリック→「Configure Attribute」をクリックし設定を行います。

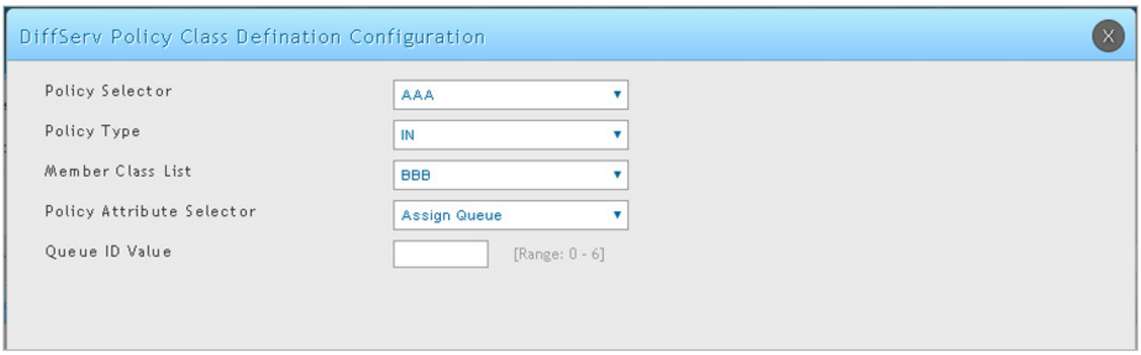


図 5-75　DiffServ Policy Class Defination Configuration 画面

3. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
Policy Selector	メンバクラスに関連付けるポリシーを選択します。
Policy Type	ポリシータイプを表示します。
Member Class List	このポリシー名に関連付けるメンバクラスを選択します。
Policy Attribute Selector	このポリシータイプにサポートされているすべての属性を表示します。ここから 1 つ選択することができます。属性を設定するためには、リストから属性を選択します。属性と設定の各項目は以下の通りです。 • Assign Queue - このポリシークラスのパケットをキューに割り当てます。「Queue ID Value」に 0-7 を入力します。 • Drop - Drop を選択すると、このポリシークラスのパケットが破棄されます。 • Mark CoS - 指定した「Class of Service」キュー番号を入力し、802.1p ヘッダの優先度フィールドに指定したサービスクラスを割り当てられているトラフィックストリームに対するパケットのすべてにマークを付けます。（単一のタグ付きパケットにはタグだけ、ダブル VLAN のタグ付きパケットには first または outer 802.1Q タグ）パケットがこのヘッダを持っていない場合、1 つ挿入されます。CoS 値は、0-7 の整数です。 • Mark IP DSCP - システムのフォワーディングエレメントに提供される前に、Diffserv によって指定の DSCP 値でマークされます。DSCP 値を設定する必要があります。 • Mark IP Precedence - システムのフォワーディングエレメントに提供される前に、Diffserv によって指定の IP Precedence 値でマークされます。IP Precedence 値を設定する必要があります。 • Police Simple - この属性を使用して、指定クラスのためにトラフィックポリシングスタイルを設定します。police コマンドのシンプルな形式では、単一のデータレートとバーストサイズを使用します。適合と違反の 2 つの結果がもたらされます。適合するデータレートは 1-4294967295（Kbps）で示されます。違反するバーストサイズは 1-128（KB）で示されます。「Police Simple」画面には以下の項目があります。 - Color Mode - カラーモードが表示されます。初期値は Color Blind です。 - Committed Rate：1 - 1000000 Kbps の間で指定します。のクラスの入力パケットの受信レートを監視するために使用されます。 - Committed Burst Size：1 - 200000 KB の間で指定します。適合トラフィックの最大値を指定します。 - Conform Action 適合していると見なされた場合のパケットに対するアクションを決定します。 • Send -（初期値）これらのパケットは DiffServ によって変更されずにシステムのフォワーディングエレメントに提供されます。 • Drop - これらのパケットは直ちに破棄されます。 • Mark IP DSCP - これらのパケットは、システムのフォワーディングエレメントに提供される前に、DiffServe によって指定済みの DSCP 値にマークされます。「Confirm Action Mark IP DSCP」で DSCP を選択する必要があります。 • Mark IP Precedence - これらのパケットは、システムのフォワーディングエレメントに提供される前に、DiffServe によって指定済みの IP Precedence 値にマークされます。「Confirm IP Precedence Value」で IP Precedence を選択する必要があります。 - Violate Action 適合していると見なされない場合のパケットに対するアクションを決定します。 • Send -（初期値）これらのパケットは DiffServ によってシステムのフォワーディングエレメントに変更されずに提供されます。 • Drop - これらのパケットは直ちに破棄されます。 • Mark IP DSCP - これらのパケットは、システムのフォワーディングエレメントに提供される前に、DiffServe によって指定済みの DSCP 値にマークされます。「Confirm Action Mark IP DSCP」でこれを選択する必要があります。 • Mark IP Precedence - これらのパケットは、システムのフォワーディングエレメントに提供される前に、DiffServe によって指定済みの IP Precedence 値にマークされます。「Confirm IP Precedence Value」でこれを選択する必要があります。

AP ファームウェアのアップグレード

無線コントローラは、管理下にあるアクセスポイントのソフトウェアをアップグレードすることができます。また、クラスタコントローラはピア無線コントローラに管理されたアクセスポイントのプログラムを更新することができます。

AP ファームウェアのダウンロード

Maintenance > Firmware > AP Firmware Download > AP Firmware Download メニュー

1. **Maintenance > Firmware > AP Firmware Download > AP Firmware Download** の順にメニューをクリックし、以下の画面を表示します。

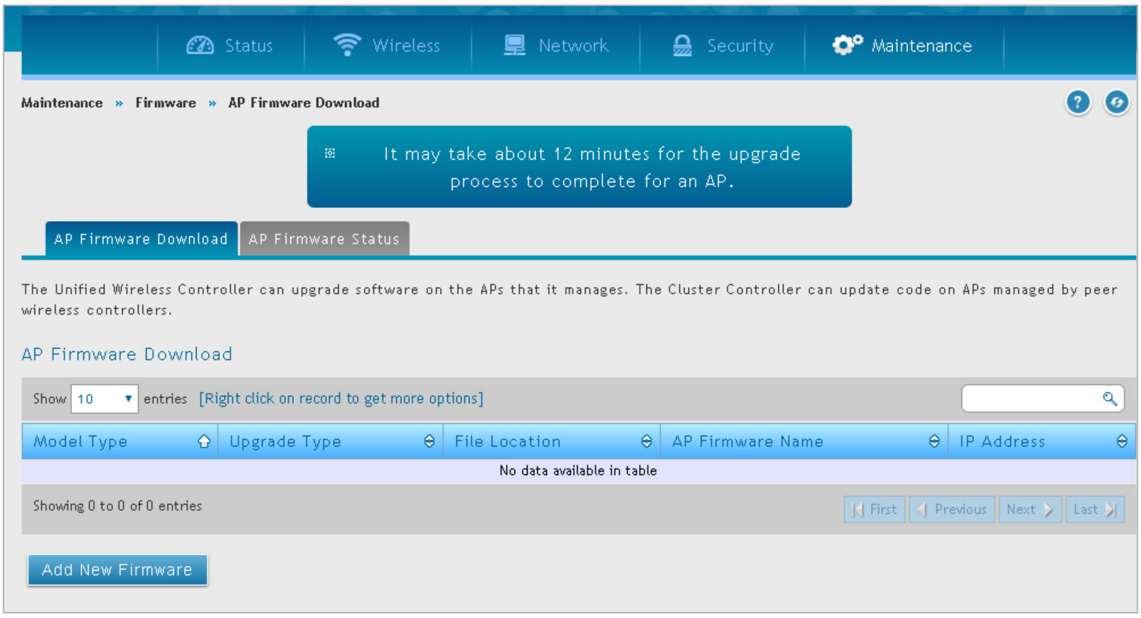


図 5-76　AP Firmware Download 画面

2. 「Add New Firmware」をクリックし、以下の項目を設定します。

項目	説明
Model (AP Type)	ダウンロードするイメージタイプを指定します。
Upgrade Type	アップグレードタイプを選択します。
External Devices	「Upgrade Type」で USB を選択した場合、USB 1 または USB 2 を選択します。
File Name	「Upgrade Type」で HTTP または TFTP を選択した場合、アップグレードするファイルの名称（半角英数字 32 文字以内）を入力します。ファイルの拡張子「.tar」の入力が必要です。
File Path	「Upgrade Type」で TFTP を選択した場合、ファイルが保存されている TFTP サーバのパス（96 文字以内）を指定します。
IP Address	「Upgrade Type」で TFTP を選択した場合、TFTP サーバの IP アドレスを入力します。

3. 「Save」をクリックします。

アップロードしたファイルを適用するには、エントリを右クリックし、「Upgrade」を選択します。

AP ファームウェアの状態

Maintenance > Firmware > AP Firmware Download > AP Firmware Status メニュー

ファームウェアのダウンロードの開始後、本画面でアップグレードに関する情報を確認することができます。

Maintenance > Firmware > AP Firmware Download > AP Firmware Status の順にメニューをクリックし、以下の画面を表示します。

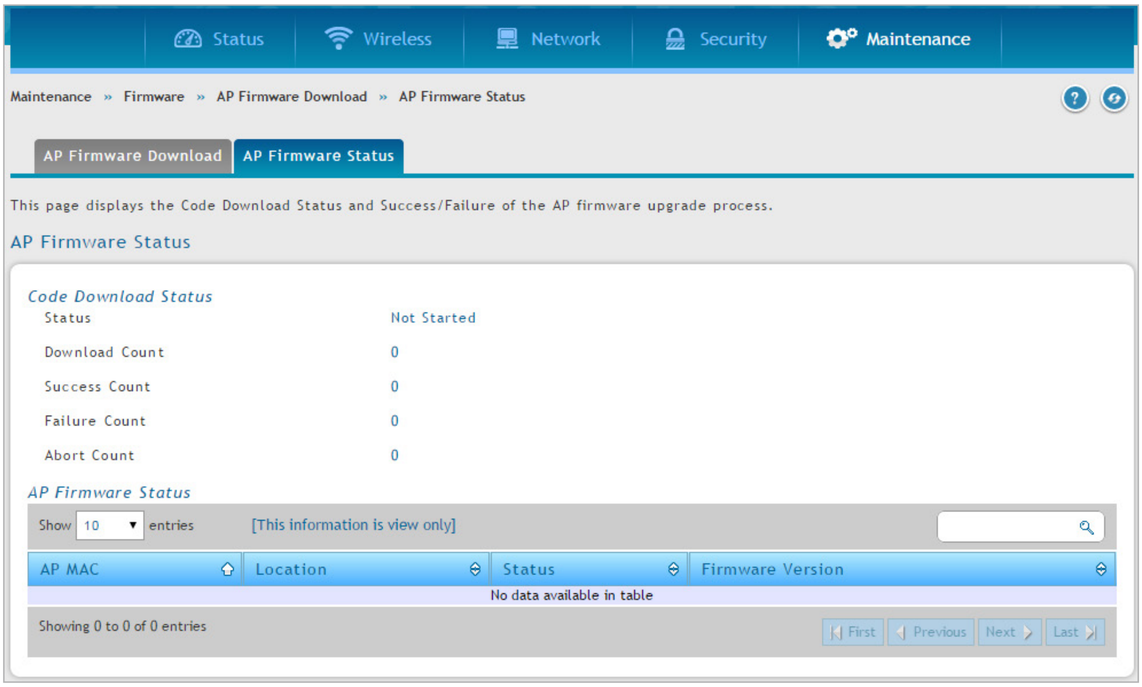


図 5-77　AP Firmware Status 画面

以下の項目を表示します。

項目	説明
Code Download Status	
Status (Global)	全アクセスポイントのアップグレードプロセスの状況を表示します。 • Not Started - 無線コントローラはダウンロードプロセスを開始していません。 • Requested - アクセスポイントのソフトウェアにリクエストが発行されましたが、コントローラはまだダウンロードをしていません。 • Code Transfer in Progress - ダウンロード中です。 • Failure - すべてのアクセスポイントでダウンロードに失敗しました。 • Aborted - アクセスポイントが TFTP サーバからソフトウェアをロードする前にダウンロードは中止されました。 • NVRAM-Update-in-Progress - ダウンロードに成功しました。アクセスポイントに Reset コマンドを送信しました。 • Success - すべてのアクセスポイントが無線コントローラに接続しています。
Download Count	ダウンロードリクエストにより現時点でソフトウェアのダウンロードを行った管理下のアクセスポイント数が表示されます。「AP Firmware Download」画面の「Managed AP」フィールドで「All」を選択した場合は、ダウンロードリクエストを開始した時点で、無線コントローラの管理下にあった全アクセスポイント数が表示されます。1 台がアップグレードされている場合、「1」と表示されます。
Success Count	新しいプログラムのダウンロードに成功したアクセスポイントの数が表示されます。はじめは「0」と表示されていますが、アクセスポイントがダウンロードに成功するごとに数値が増加していきます。
Failure Count	新しいプログラムのダウンロードに失敗したアクセスポイントの数が表示されます。0 から開始して、失敗する度に増えていきます。
Abort Count	新しいプログラムのダウンロードを中止したアクセスポイントの数が表示されます。0 から開始して、ダウンロードを中止する度に増えていきます。

項目	説明
AP Firmware Status	
Status (per-AP)	アクセスポイントごとにダウンロードの状況とダウンロード中のソフトウェアのバージョンが表示されます。各アクセスポイントの「Status」欄には以下のステータスが表示されます。 • Requested - このアクセスポイントにダウンロードが計画されていますが、アクセスポイントが現在のダウンロードグループにないため、まだダウンロードの開始が伝えられていません。 • Code-Transfer-In-Progress - アクセスポイントはソフトウェアのダウンロードを通知しました。 • Failure - アクセスポイントはソフトウェアのダウンロードの失敗を報告しました。 • Aborted - アクセスポイントが TFTP サーバからソフトウェアをロードする前にダウンロードは中止されました。 • Waiting-For-APs-To-Download - ダウンロードはこのアクセスポイントで終了し、他のアクセスポイントがダウンロードを終了するのを待っています。Reset コマンドはこの状態ではアクセスポイントに送信されません。 • NVRAM-Update-In-Progress - ダウンロードに成功しました。Reset コマンドがアクセスポイントに送信されました。 • Timed-Out - アクセスポイントは所定の時間内に無線コントローラに再接続しませんでした。
AP MAC	管理されるアクセスポイントの MAC アドレスを表示します。
Location	管理されるアクセスポイントの位置を表示します。
Status	アクセスポイントの状態を表示します。上記の「Status（per-AP）」を参照してください。
Firmware Version	管理されるアクセスポイントの現在のファームウェアバージョンを表示します。

第 6 章　高度なネットワーク設定

多くのユーザは、前章で説明した基本設定で十分ですが、大規模な無線ネットワークや複雑な配置では、無線コントローラの高度な設定が必要となります。本章では、以下に示した一般的に使用される高度な設定について記載しています。

設定項目	説明
IP モード設定	コントローラで使用される IP プロトコルのバージョンを設定します。
LAN 設定	IPv4/IPv6 ネットワーク用の LAN 設定、IPv6 通知、DHCP 予約 IP アドレスの設定などを行います。
VLAN 設定	ポート VLAN、マルチ VLAN サブネット設定などを行います。
ルーティング設定	IPv4/IPv6 スタティックルーティングの設定を行います。
QoS 設定	QoS 優先度の設定を行います。
QoS ポリシー設定	LAN の照合基準に基づいてトラフィックの優先度を設定します。

注意 ネットワークの概念と専門用語を理解している熟練したユーザのみ本章の手順を実行してください。

IP モード設定

Network > LAN > IP Mode メニュー

コントローラで使用される IP プロトコルのバージョンを設定します。 LAN 上で IPv6 をサポートするためには、コントローラを IPv4/IPv6 モードとするように設定する必要があります。このモードにより、IPv4 ノードはこのコントローラを経由して IPv6 デバイスと通信できます。

1. **Network > LAN > IP Mode** の順にメニューをクリックし、以下の画面を表示します。

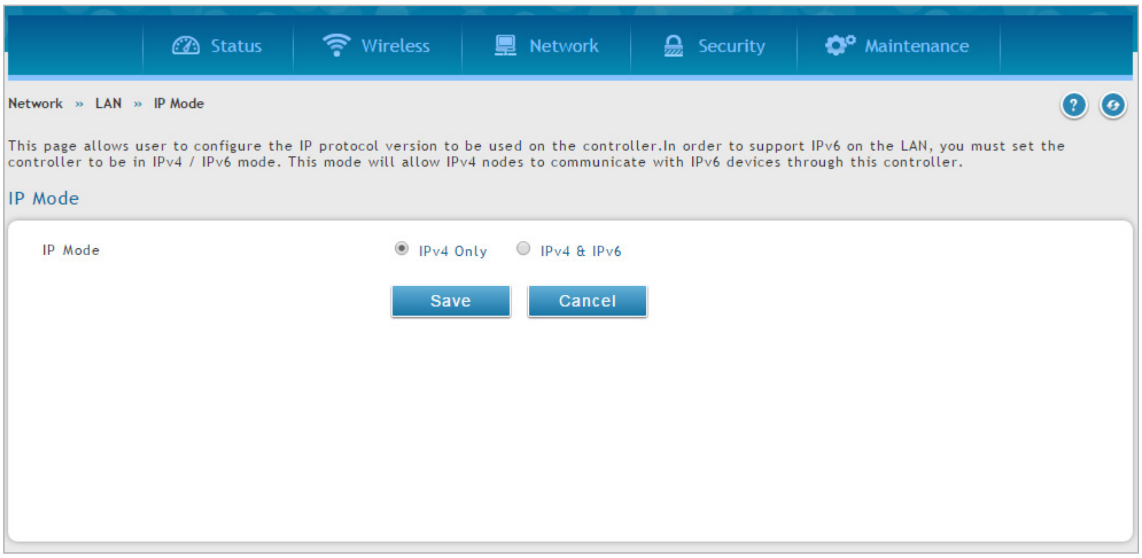


図 6-1　　IP Mode 画面

2. 「IPv4 Only」または「IPv4 & IPv6」を選択します。

3. 「Save」ボタンをクリックします。

LAN 設定

IPv4 LAN 設定

Network > LAN > LAN Settings > IPv4 LAN Settings メニュー

初期値では、コントローラの DHCP（Dynamic Host Configuration Protocol）モードは「None」（なし）に設定されています。DHCP モードを DHCP サーバまたは DHCP リレーに設定できます。「DHCP Mode」を「DHCP Server」に設定すると、コントローラは、WLAN または LAN 上のホストに IP アドレスリースを割り当てるために DHCP サーバとして機能します。また、DHCP を使用して、DNS サーバ、WINS（Windows Internet Naming Service）サーバ、およびデフォルトゲートウェイに対するアドレスに加え、PC とその他の LAN デバイスに IP アドレスを割り当てることができます。DHCP サーバが有効な場合、コントローラの IP アドレスは LAN と WLAN クライアントのためのゲートウェイアドレスとして機能します。LAN 内の PC には、この手順で指定されるアドレスプールから IP アドレスが割り当てられます。各プールアドレスは LAN 上でアドレスの重複を避けるために割り当て前にテストされます。

多くのアプリケーションでは、DHCP と TCP/IP 設定の初期値で十分です。ご使用のネットワークにある別の PC を DHCP サーバにしたい場合、または手動で全 PC のネットワーク設定を行う場合には、DHCP モードを「None」に設定します。DHCP リレーは、ネットワーク上の DHCP サーバである別の LAN デバイスから DHCP のリース情報を転送するために使用されます。これは特に無線クライアントに役立ちます。

DNS サーバを使用する代わりに、WINS（Windows Internet Naming Service）サーバを使用することもできます。WINS サーバは、DNS サーバと同等ですが、ホスト名の解決のために NetBIOS プロトコルを使用します。DHCP クライアントからの DHCP 要求を承諾する際に、コントローラは DHCP 設定内に WINS サーバの IP アドレスを含めます。

また、LAN で DNS プロキシを有効にすることができます。有効にすると、コントローラは、すべての DNS 要求に対してプロキシとして動作し、ISP の DNS サーバと通信します。 無効にすると、すべての DHCP クライアントが ISP の DNS IP アドレスを受信します。

1. **Network > LAN > LAN Settings > IPv4 LAN Settings** の順にメニューをクリックし、以下の画面を表示します。

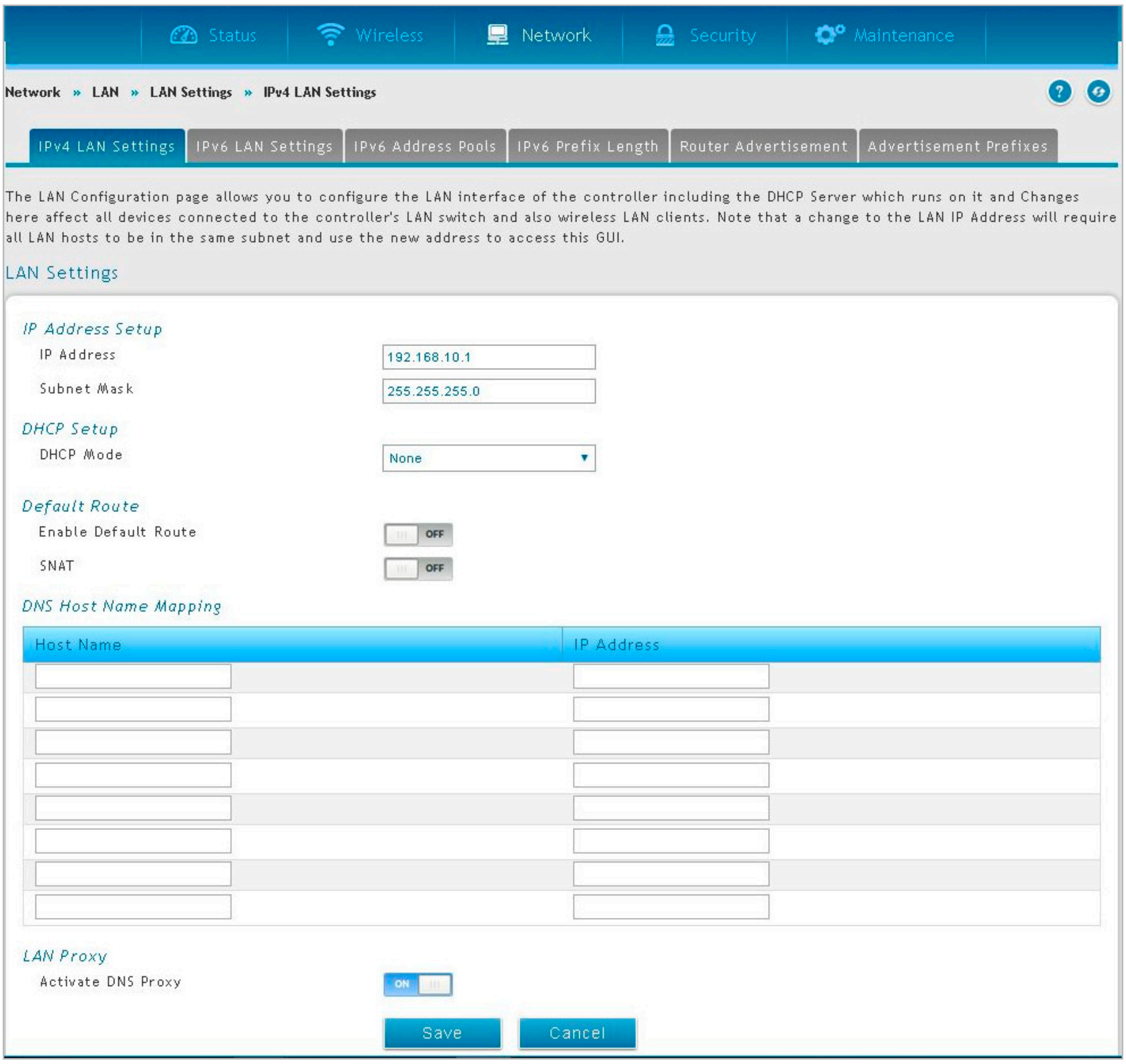


図 6-2　　LAN Settings 画面（DHCP Mode が「None」の場合）

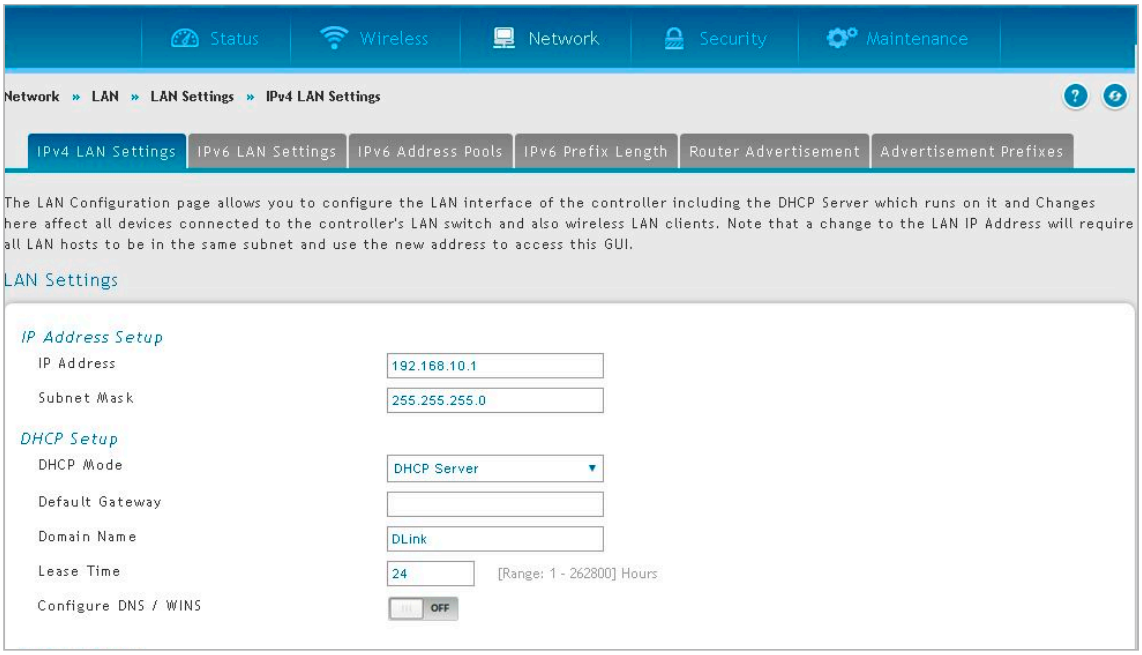


図 6-3　　LAN Settings 画面（DHCP Mode が「DHCP Server」の場合）

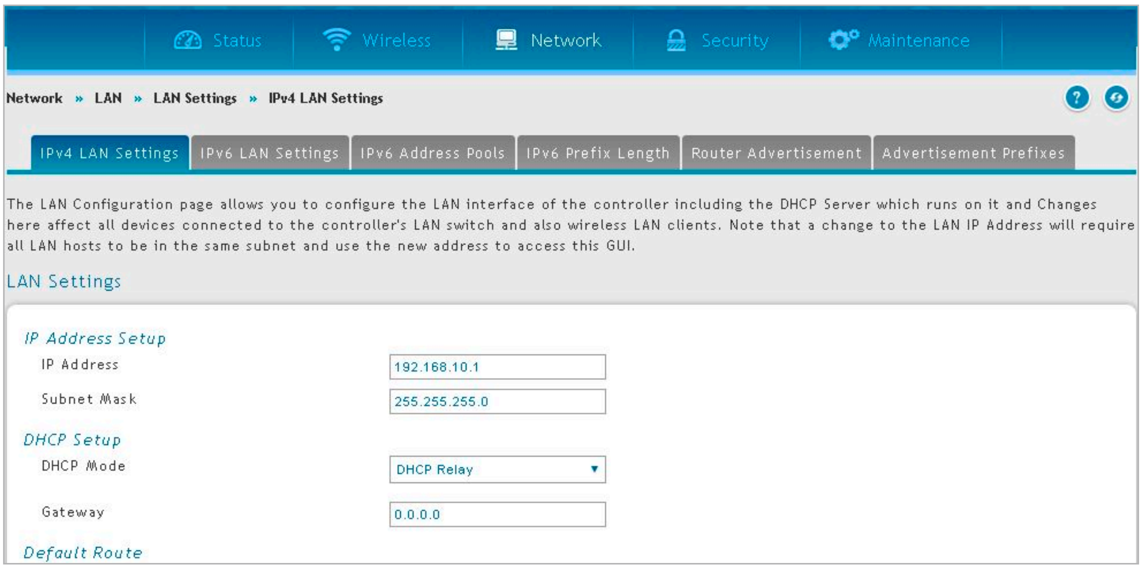


図 6-4　　LAN Settings 画面（DHCP Mode が「DHCP Relay」の場合）

2.　フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
IP Address Setup	
IP Address	無線コントローラの LAN インタフェースの IP アドレスを指定します。
Subnet Mask	サブネットマスクを指定します。初期値は「255.255.255.0」です。
DHCP Setup	
DHCP Mode	DHCP モードを指定します。 • None - コントローラの DHCP サーバを LAN に対して無効にします。 • DHCP Server - コントローラは、DHCP が供給するアドレスを希望する LAN デバイスに対し、指定内の IP アドレスおよび追加情報を割り当てます。 • DHCP Relay - LAN 上の DHCP クライアントは、異なるサブネットにある DHCP サーバから IP アドレスリースと対応する情報を受け取ることができます。リレーゲートウェイを指定します。これにより LAN クライアントが DHCP 要求を行うと、リレーゲートウェイ IP アドレスを通してアクセス可能なサーバに送られます。
Default Gateway	「DHCP Mode」が「DHCP Server」の場合にデフォルトゲートウェイを入力します。
Domain Name	「DHCP Mode」が「DHCP Server」の場合、ドメイン名を入力します。
Lease Time	クライアントに IP アドレスをリースする時間（時）を指定します。
Configure DNS / WINS	DNS/WINS を有効または無効にします。
Primary DNS Server	プライマリ DNS サーバの IP アドレスを指定します。

項目	説明
Secondary DNS Server	セカンダリ DNS サーバの IP アドレスを指定します。
WINS Server	（オプション）WINS サーバの IP アドレスを指定します。
Gateway	「DHCP Mode」が「DHCP Relay」の場合にリレーゲートウェイのアドレスを入力します。
Default Route	
Enable Default Route	デフォルトルート機能を有効または無効にします。（ON は有効）
Gateway	「Enable Default Route」が「ON」の場合、ゲートウェイ IP アドレスを入力します。
Primary DNS Server	「Enable Default Route」が「ON」の場合、DNS サーバの IP アドレスを入力します。
Secondary DNS Server	「Enable Default Route」が「ON」の場合、セカンダリ DNS サーバの IP アドレスを入力します。
SNAT	SNAT（Source Network Address Translation）を有効または無効にします。ご使用の LAN ネットワークに VLAN を設定していて、送信元ソースとオリジンアドレスを変換する NAT が必要である場合に有効にします。
DNS Host Name Mapping	
Host Name	DNS ホスト名を入力します。
IP Address	DNS ホストの IP アドレスを入力します。
LAN Proxy	
Active DNS Proxy	この LAN の DNS プロキシを有効または無効にします。 • ON - コントローラは、すべての DNS 要求に対するプロキシとして動作し、ISP の DNS サーバと通信します。すべての DHCP クライアントは、DNS プロキシが実行されている IP（システムの LAN IP）と一緒に、プライマリ / セカンダリの DNS IP を受信します。 • OFF - すべての DHCP クライアントが DNS プロキシ IP アドレスを除いた ISP の DNS IP アドレスを受信します。 本機能は「自動ロールオーバ」モードの場合に特に役に立ちます。例えば、各接続用の DNS サーバが異なる場合、リンク障害により DNS サーバへのアクセスが不可能になるかもしれません。しかし、DNS プロキシが有効であると、クライアントは要求をコントローラに対して行うことができます。そして、順番にアクティブな接続の DNS サーバにそれらの要求を送信します。

IPv6 LAN 設定

Network > IPv6> LAN Setting> IPv6 LAN Settings メニュー

IPv6 モードでは、LAN DHCP サーバは（IPv4 モードと同様に）初期値で無効です。DHCPv6 サーバは LAN に割り当てられている IPv6 プレフィックス長を使用して定義済みアドレスプールから IPv6 アドレスを供給します。

コントローラの IPv6 LAN アドレスの初期値は「fec0::1」です。ご使用のネットワークの要件に基づいて、この 128 ビットの IPv6 アドレスを変更することができます。コントローラに LAN 設定を定義する他のフィールドには、プレフィックス長があります。IPv6 ネットワーク（サブネット）はプレフィックスと呼ばれるアドレスの開始ビットにより特定されます。初期値は 64 ビット長です。

ネットワーク内のすべてのホストは、IPv6 アドレスに共通の開始ビットを持っています。ネットワークアドレスの共通の開始ビット番号はプレフィックス長フィールドによって設定されます。

1. **Network > IPv6 > LAN Settings > IPv6 LAN Settings** の順にメニューをクリックし、以下の画面を表示します。

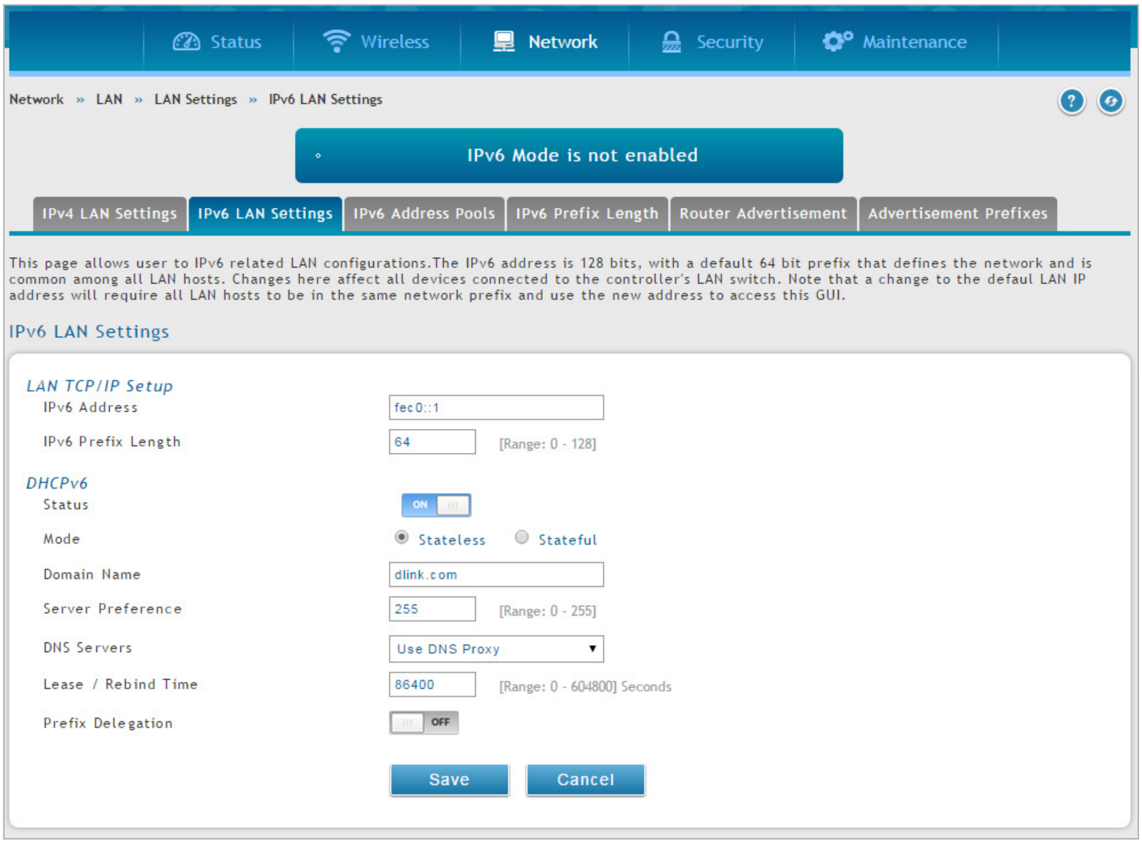


図 6-5　　IPv6 LAN Settings 画面

2. 以下のフィールドにデータを入力します。

項目	説明
LAN TCP/IP Setup	
IPv6 Address	無線コントローラの LAN IPv6 アドレスを指定します。
IPv6 Prefix Length	IPv6 ネットワーク（サブネット）はプレフィックスと呼ばれるアドレスの開始ビットにより特定されます。ネットワーク内のすべてのホストは、IPv6 アドレスに同じ開始ビットを持っています。ネットワークアドレスの共通の開始ビット番号はプレフィックス長フィールドによって設定されます。
DHCPv6	
Status	DHCPv6 を有効にするには、「ON」に切り替えます。初期値では無効です。
DHCPv6 が有効（ON）の場合	
Mode	ゲートウェイに対し適切なアドレスを取得する方法を選択します。 • Stateless - アドレスの割り当てにルータの通知を使用します。DHCPv6 クライアントとしてこのコントローラを通知するために IPv6 RADVD プロトコルが有効にされます。 • Stateful - ISP で利用可能な DHCPv6 サーバから IPv6 アドレスを要求します。
Domain Name	DHCPv6 サーバのドメイン（オプション）名を指定します。
Server Preference	サーバの優先度（0-255）を指定します。この DHCP サーバの優先度レベルを示すためにステートレス DHCP で使用されます。DHCPv6 クライアントは最も高い優先度値を持っている DHCPv6 サーバをピックアップします。

項目	説明
DNS Servers	DHCPv6 クライアントに DNS サーバのオプションを選択します。 • Use DNS Proxy - この LAN の DNS プロキシを有効にします。有効にすると、コントローラはすべての DNS 要求に対するプロキシとして動作し、ISP の DNS サーバと通信します 。 • Use Below - 本項目を選択すると、本フィールドに続くプライマリとセカンダリ DNS サーバの設定が DHCPv6 クライアントに対して使用されます。
Primary DNS Server	プライマリ DNS サーバの IP アドレスを入力します。
Secondary DNS Server	セカンダリ DNS サーバの IP アドレスを入力します。
Lease / Rebind Time	IP アドレスがクライアントにリースされる期間（秒）を指定します。
Prefix Delegation	プレフィックス委譲機能を有効または無効にします。

3. 「Save」ボタンをクリックします。

IPv6 アドレスプール

Network > IPv6> LAN Setting> IPv6 Address Pools/ IPv6 Prefix Length メニュー

ゲートウェイの DHCPv6 サーバが供給する IP アドレスの範囲に IPv6 デリゲーション（権限委譲）プレフィックスを定義します。デリゲーションプレフィックスを使用して、LAN 上の他のネットワークデバイスに対し、割り当てプレフィックス固有の DHCP 情報を通知する処理を自動化できます。

1. **Network > LAN > LAN Settings > IPv6 Address Pools** の順にメニューをクリックし、以下の画面を表示します。

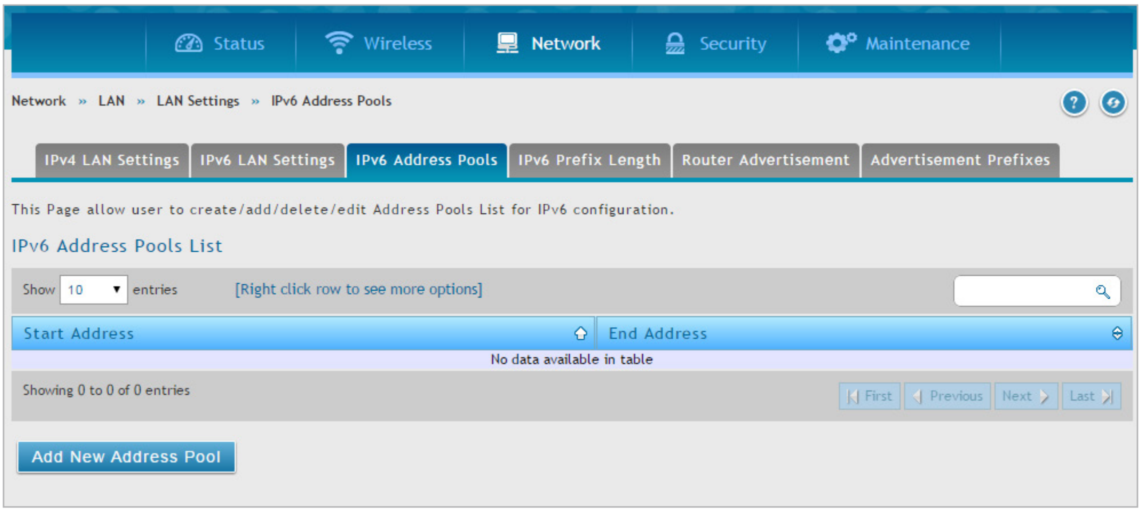


図 6-6　　IPv6 Address Pools List 画面

2. 「Add New Address Pool」ボタンをクリックします。

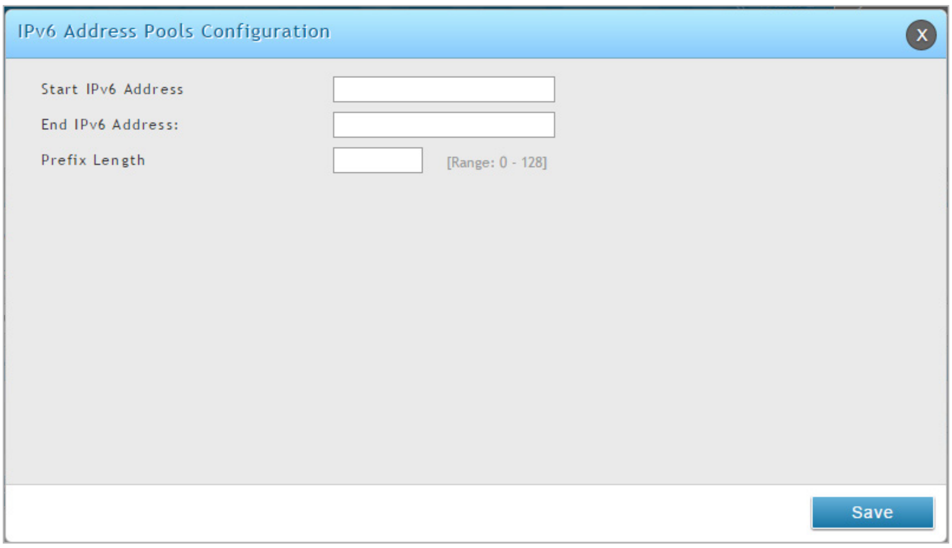


図 6-7　　IPv6 Address Pools Configuration 画面

3. 開始の IPv6 アドレス、終点の IPv6 アドレス、およびプレフィックス長を入力します。

4. 「Save」ボタンをクリックします。

5. **Network > LAN > LAN Settings > IPv6 Prefix Length** の順にメニューをクリックし、以下の画面を表示します。

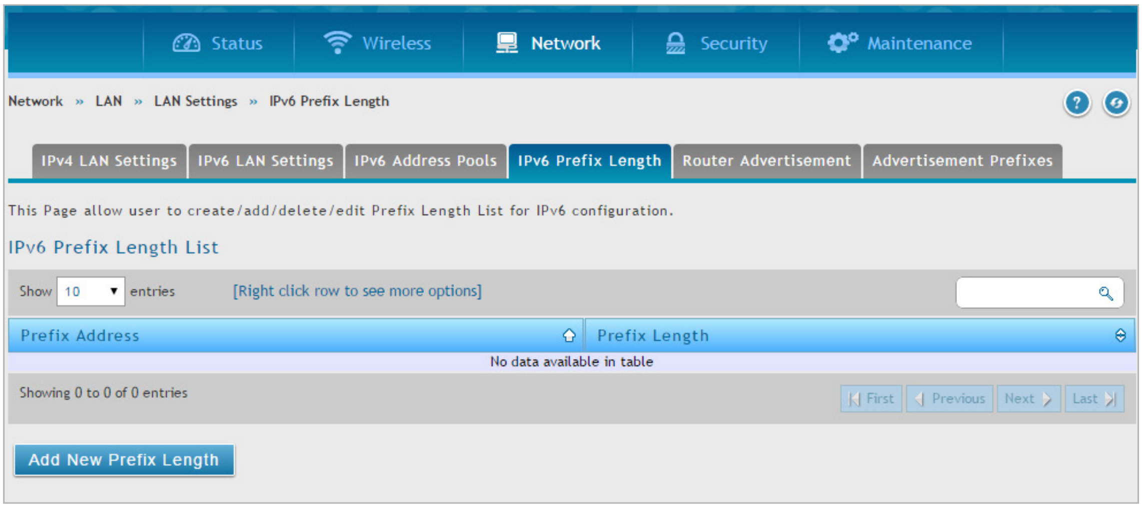


図 6-8　　IPv6 Prefix Length List 画面

6. 「Add New Prefix Length」ボタンをクリックし、以下の画面を表示します。

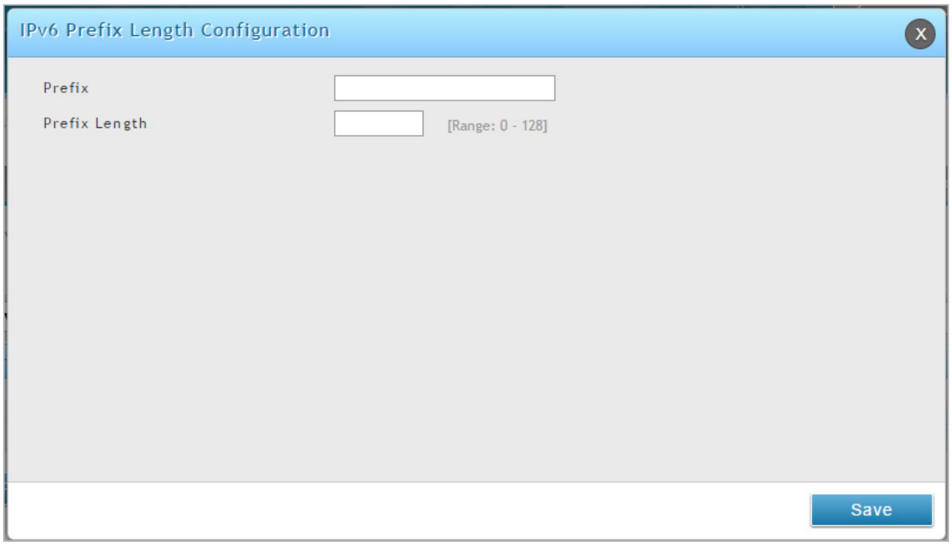


図 6-9　　IPv6 Prefix Length Configuration 画面

7. IPv6 プレフィックスとプレフィックス長を入力し、「Save」ボタンをクリックします。

IPv6 ルータ通知

Network > LAN > LAN Settings > Router Advertisement メニュー

ルータ通知は LAN クライアント用の IPv4 DHCP 割り当てに似ているもので、IP アドレスおよびサポートされるネットワーク情報を受け付けるように設定されたデバイスに対し、コントローラはそれらの情報を割り当てます。ルータ通知は、IPv6 LAN のステートレスな自動設定のために IPv6 ネットワークで必要とされます。このコントローラにルータ通知デーモンを設定することによって、デバイスは、ルータ要請に対して LAN をリッスンして、ルータ通知でこれらの LAN ホストに応答します。

1. **Network > LAN > LAN Settings > Router Advertisement** の順にメニューをクリックし、以下の画面を表示します。

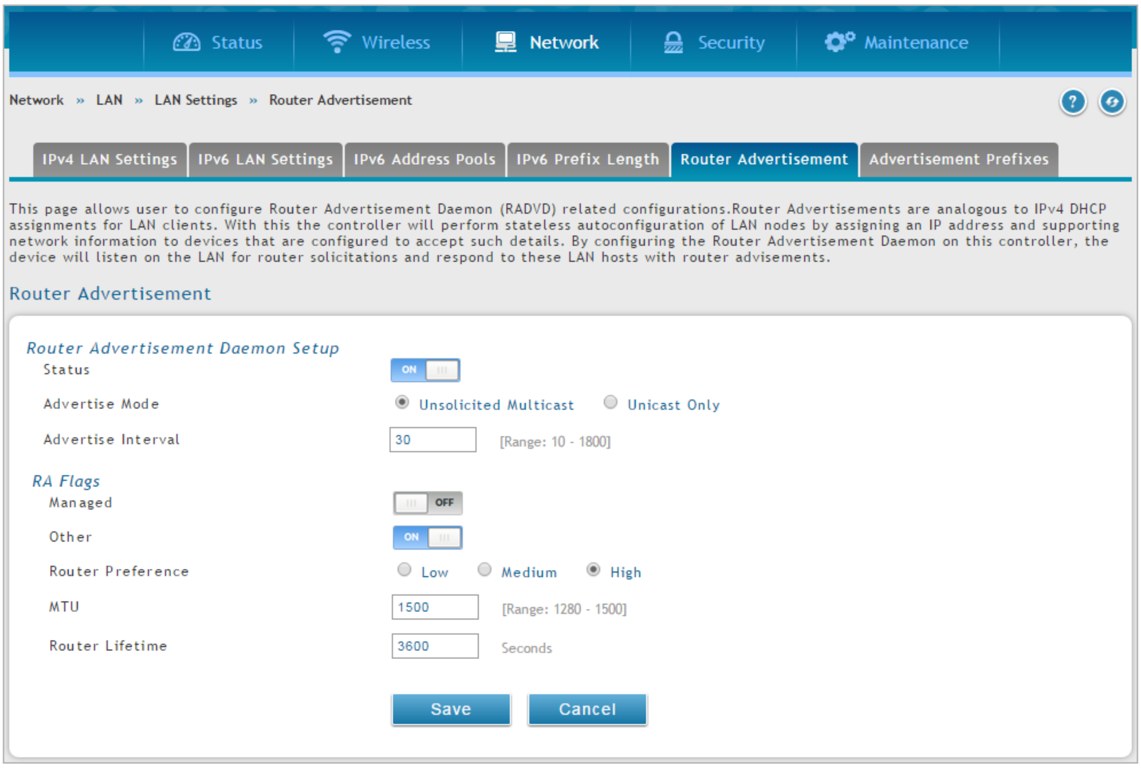


図 6-10　Router Advertisement 画面

2. フィールドにデータを入力します。

項目	説明
Router Advertisement Daemon Setup	
Status	IPv6 LAN ネットワークのステートレス自動設定を許可するために RADVD 処理を有効にします。
Advertise Mode	通知モードを選択します。 • Unsolicited Multicast - ルータ通知（RA）をマルチキャストグループに所属する全インタフェースに送信します。 • Unicast Only - 通知を既知の IPv6 アドレスだけに制限します（RA は既知のアドレスに所属するインタフェースに対してのみ送信されます）。
Advertise Interval	「Advertise Mode」が「Unsolicited Multicast」の場合、最大通知間隔を設定します。RADVD が有効な場合に使用される通知間隔は、最小ルータ通知間隔と最大ルータ通知間隔の間のランダムな値となります。最小のルータ通知間隔はこの設定の 1/3 で、初期値は 30（秒）です。
RA Flags	
RA Flags	以下のフラグの 1 つ、または両方と共にルータ通知（RA）を送信することができます。 • Managed - アドレス自動設定に管理 / ステートフルプロトコルを使用します。 • Other - ホストは（アドレス以外の）他の情報自動設定の管理 / ステートフルプロトコルを使用します。
Router Preference	コントローラの RADVD 処理に関連付けられている優先度を Low/Medium/High から選択します。LAN 上に他の RADVD が有効なデバイスがある場合、この機能は役に立ちます。初期値は「High」です。
MTU	LAN MTU が既知でない場合に、ネットワークの全ノードが同じ MTU 値を使用することを保証するために RA で使用されます。初期値は 1500 です。
Router Lifetime	ルートのライフタイム（秒）を指定します。初期値は 3600（秒）です。

3. 「Save」ボタンをクリックします。

IPv6 通知のプレフィックス

Network > LAN Setting > Advertisement Prefixes メニュー

通知プレフィックスと共に設定されたルータ通知により、コントローラはステートレスアドレス自動設定を実行する方法をホストに知らせることができます。ルータ通知にはサブネットプレフィックスのリストが含まれており、これによりルータは Neighbor の決定と、ホストがコントローラと同じリンクに存在するかどうかの判別を行うことができます。

1. **Network > LAN Settings > Advertisement Prefix** の順にメニューをクリックし、以下の画面を表示します。

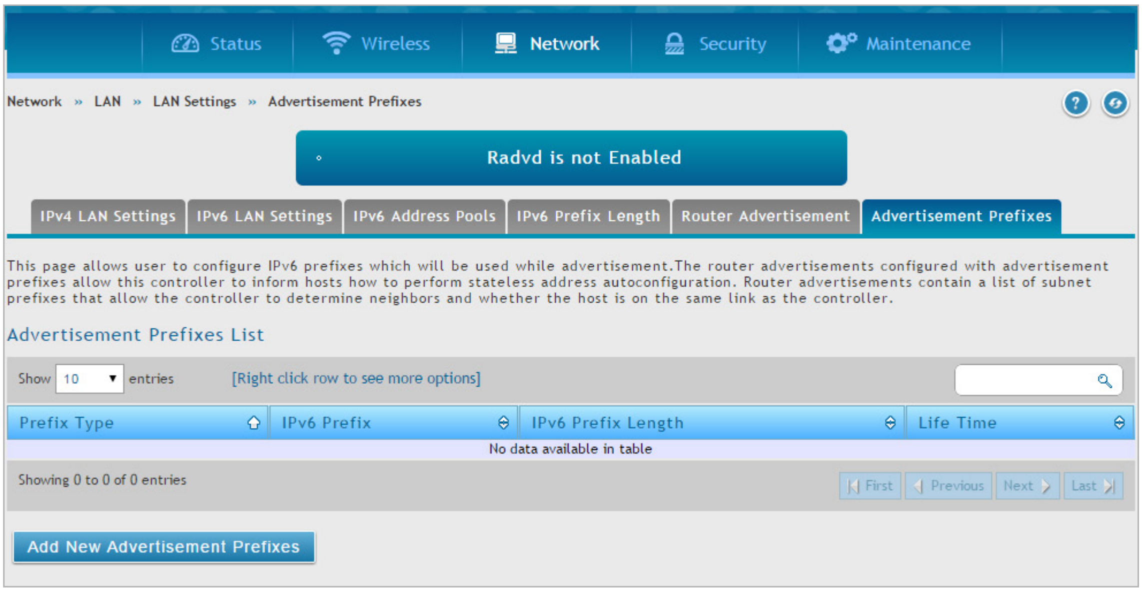


図 6-11　Advertisement Prefixes List 画面

2. 「Add New Advertisement Prefixes」ボタンをクリックします。

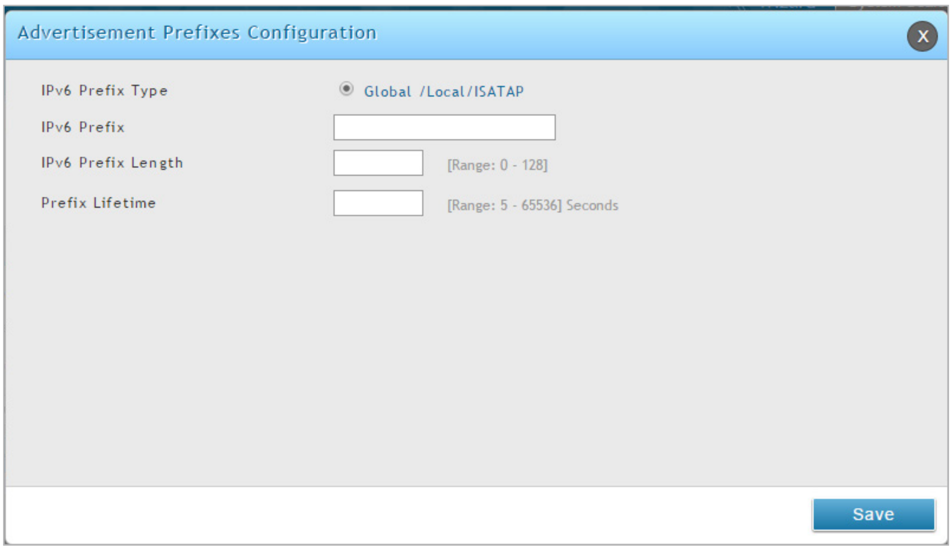


図 6-12　Advertisement Prefixes Configuration 画面

3. フィールドにデータを入力します。

項目	説明
IPv6 Prefix Type	プレフィックスタイプを選択します。
IPv6 Prefix	IPv6 ネットワークアドレスを指定します。
IPv6 Prefix Length	IPv6 プレフィックス長を指定します。アドレスのネットワーク部分を構成する連続したアドレスの中で高位のビット数を示す数値です。
Prefix Lifetime	要求側のコントローラがプレフィックスを使用できる時間を指定します。

4. 「Save」ボタンをクリックします。

LAN DHCP の予約 IP

Network > LAN > LAN DHCP Reserved IPs メニュー

コントローラの DHCP サーバでは、DHCP サーバのデータベースに対して、そのクライアントに割り当てられているネットワークインタフェースのハードウェアアドレスと IP アドレスを追加することで、明示的に LAN 上のコンピュータに TCP/IP 設定を割り当てることができます。DHCP サーバがクライアントからリクエストを受信する場合には常に、クライアントのハードウェアアドレスとデータベース内に存在するハードウェアアドレスリストを比較します。IP アドレスがデータベース内のコンピュータまたはデバイスに割り当てられていると、カスタマイズされた IP アドレスが設定され、そうでない場合は、IP アドレスは DHCP プールから自動的にクライアントに割り当てられます。

1. **Network > LAN > LAN DHCP Reserved IPs** の順にメニューをクリックし、以下の画面を表示します。

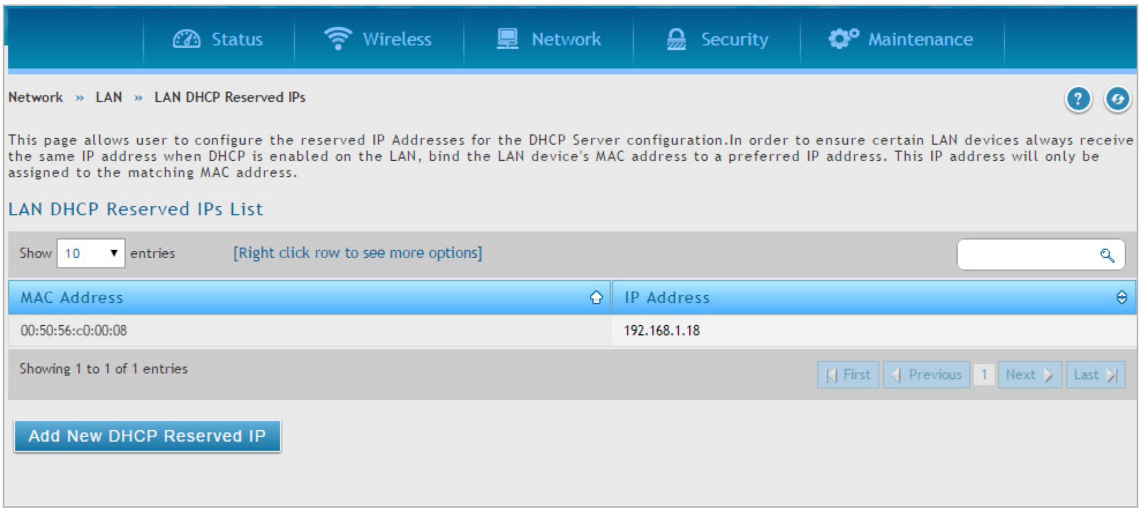


図 6-13　LAN DHCP Reserved IPs List 画面

2. 「Add New DHCP Reserved IP」ボタンをクリックします。

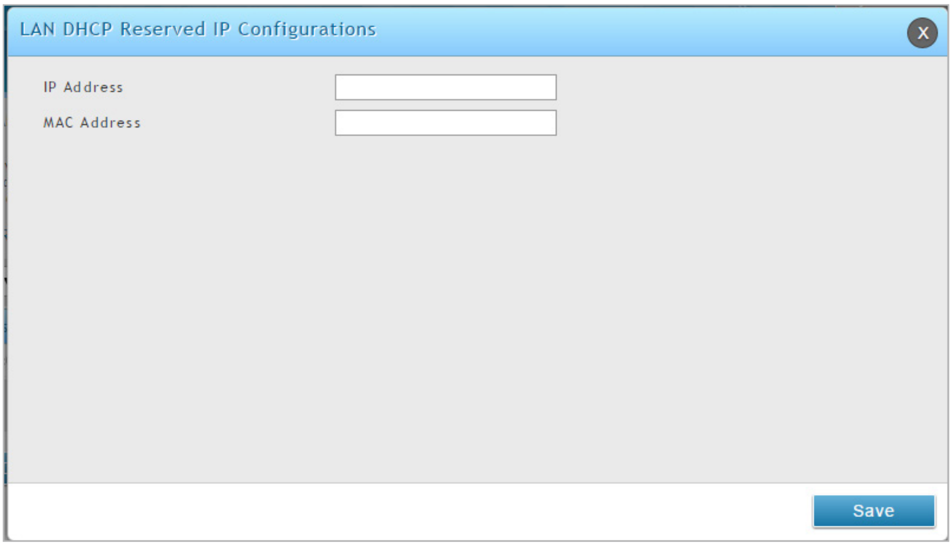


図 6-14　LAN DHCP Reserved IP Configuration 画面

3. 予約を希望する IP アドレスとその IP アドレスに割り当てるクライアントの MAC アドレスを入力します。

4. 「Save」ボタンをクリックします。

IGMP 設定

Network > LAN > IGMP Setup メニュー

IGMP Snooping により、コントローラを通じた IGMP ネットワークトラフィックのリッスンを可能にします。また、マルチキャストトラフィックをフィルタして、このストリームを必要とするホストのみに送信します。これは、すべての LAN ホストがこのマルチキャストトラフィックを受信する必要のないネットワークに（例えば IPTV アプリケーションからの）大量のマルチキャストトラフィックが流れる場合に役立ちます。IGMP Snooping を有効にすると、コントローラがネットワーク上のマルチキャストトラフィックの量を規制して、すべての LAN ホストにフラッドすることを防止します。アクティブな IGMP Snooping は IGMP プロキシに参照され、使用するコントローラで利用可能となります。

1. **Network > LAN > IGMP Setup** の順にメニューをクリックし、以下の画面を表示します。

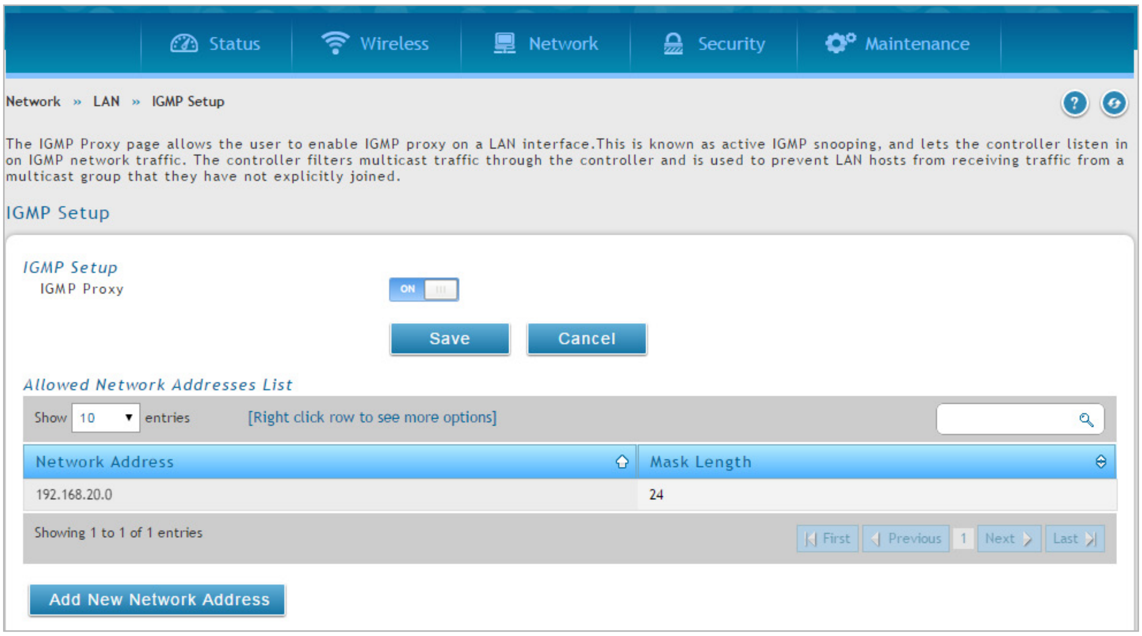


図 6-15　IGMP Setup 画面

2. 「IGMP Proxy」を「ON」にして、「Save」ボタンをクリックします。

エントリの追加

1. 「Add New Network Address」ボタンをクリックして、マルチキャスト送信元の IP ネットワークとホストアドレスを指定します。

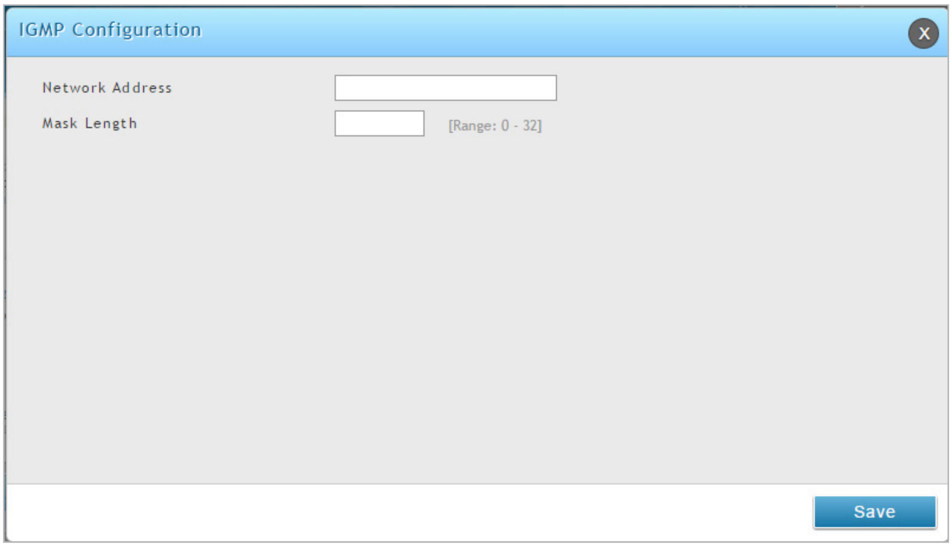


図 6-16　IGMP Configuration 画面

2. ネットワークアドレスとマスク長を入力し、「Save」ボタンをクリックします。

エントリの削除

削除するアドレスを右クリックして、「Delete」を選択します。エントリのすべてを削除する場合は、「Select All」をチェック後、「Delete」をクリックします。

エントリの編集

編集するアドレスを右クリックして、「Edit」を選択します。編集後、「Save」ボタンをクリックします。

ジャンボフレームの設定

Network > LAN > Jumbo Frame メニュー

ジャンボフレームは 1500 バイト以上のペイロードを持つイーサネットフレームです。このオプションが有効な場合、LAN デバイスはジャンボフレームレートで情報を交換することができます。

1. **Network > LAN > Jumbo Frame** の順にメニューをクリックし、以下の画面を表示します。

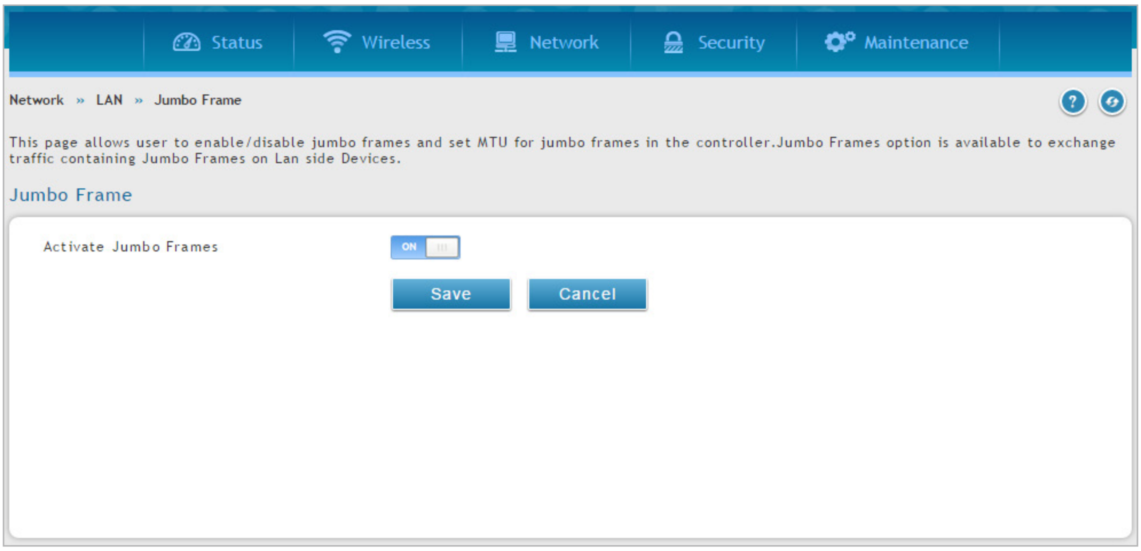


図 6-17　Jumbo Frame 画面

2. 「Activate Jumbo Frames」を「ON」に切り替えます。

3. 「Save」ボタンをクリックします。

リンクアグリゲーション

Network > LAN > Link Aggregation メニュー

リンクアグリゲーションは、複数のポートを結合して 1 つの広帯域のデータパイプラインを作成するために使用されます。コントローラはトランクグループ内のすべてのポートを 1 つのポートとみなします。

LACP（Link Aggregation Control Protocol）は、コントローラと 802.3ad をサポートする他のネットワークデバイス間にダイナミックに収集されたリンクをネゴシエートするために使用されます。この機能が動作するためには、コントローラは、収集されたリンクのネゴシエーションを許可する LACP に従う必要があります。

注意 リンクアグリゲーション機能を使用する際は、当該ポートには、必ず VLAN1 のみが「Access Mode」で設定されている必要があります。また、リンクアグリゲーションに関する下記の設定は変更できません。

- LACP Port Mode：Active（変更不可）
- LACP 配送タイミング：Short（1 秒）（変更不可）
- LACP タイムアウト：Short（3 秒）（変更不可）
- LACP アルゴリズム：MAC-Source-Dest（変更不可）

Network > LAN > Link Aggregation の順にメニューをクリックし、以下の画面を表示します。「Static Mode」を「ON」にすると、スタティックモードを使用します。「OFF」だとダイナミックモード（LACP）を使用します。選択後「Save」をクリックします。

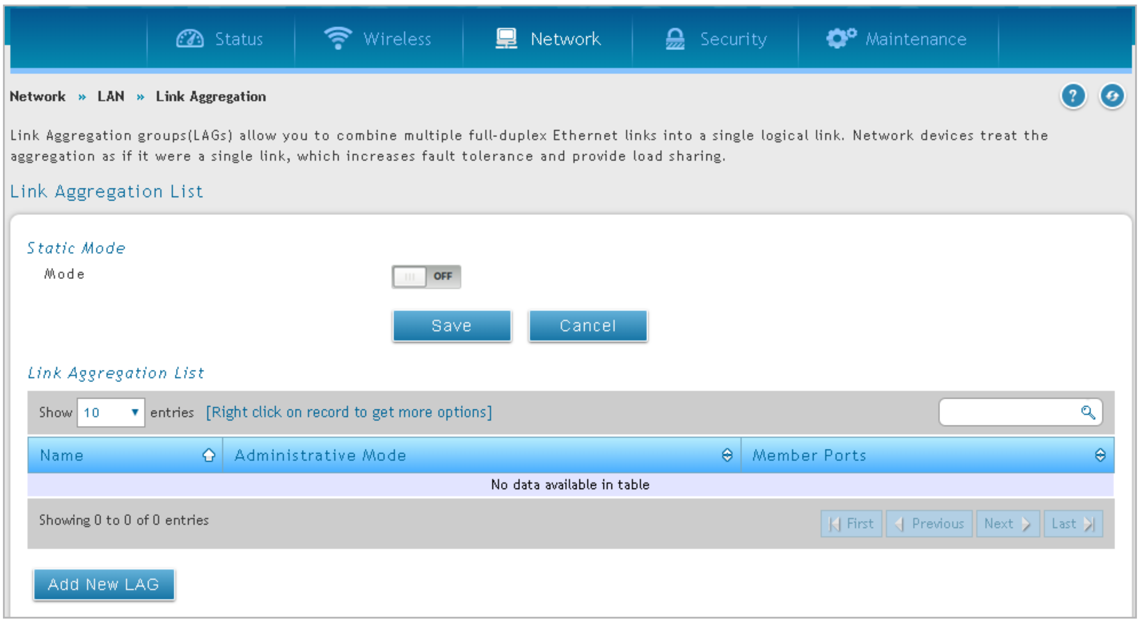


図 6-18　Link Aggregation List 画面

エントリの追加

1. 「Add New LAG」ボタンをクリックして、以下の画面を表示します。

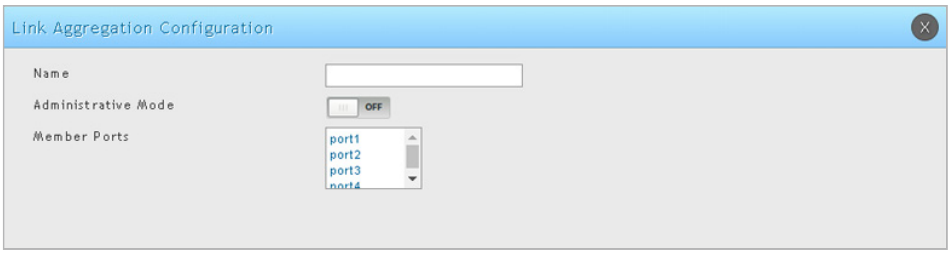


図 6-19　Link Aggregation Configuration 画面

2. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
Name	本設定の名称を入力します。
Administrative Mode	管理モードを「ON」（有効）または「OFF」（無効）にします。
Member Ports	設定に追加するポート（1-4）を選択します。複数のポートを選択するためには、「CTRL」を押したままポートをクリックします。

*1 つの論理インタフェースには最大 4 個のインタフェースをまとめられます。

エントリを削除する場合、削除するエントリを右クリックして、「Delete」を選択します。
エントリのすべてを削除する場合は、「Select All」をチェック後、「Delete」をクリックします。
エントリを編集する場合、編集するエントリを右クリックして、「Edit」を選択します。編集後、「Save」ボタンをクリックします。

VLAN 設定

仮想のローカルエリアネットワーク（VLAN）は、交換網の論理的なセグメントです。1 つの物理ネットワーク内に複数の独立した論理ネットワークを作成することが可能になります。VLAN は、異なるブロードキャストドメインとレイヤ 3 サブネットにデバイスを分離します。VLAN 内のデバイスは、ルーティングせずに通信できます。VLAN の一番の用途は、大きなブロードキャストドメインである、規模の大きな交換網を分割することです。

無線コントローラは、物理ポートから（へ）のトラフィックを一般の LAN から隔離できるように、固有の VLAN ID を LAN ポートに割り当てる VLAN 機能を提供します。VLAN フィルタリングは、大規模なネットワークにあるデバイスのブロードキャストパケットを制限するために特に役に立ちます。

VLAN の作成

Network > VLAN > VLAN Settings メニュー

VLAN を作成します。VLAN の作成後、同じページを使用して、VLAN の参照、編集、および削除ができます。

エントリの作成

1. **Network > VLAN > VLAN Settings** の順にメニューをクリックし、以下の画面を表示します。

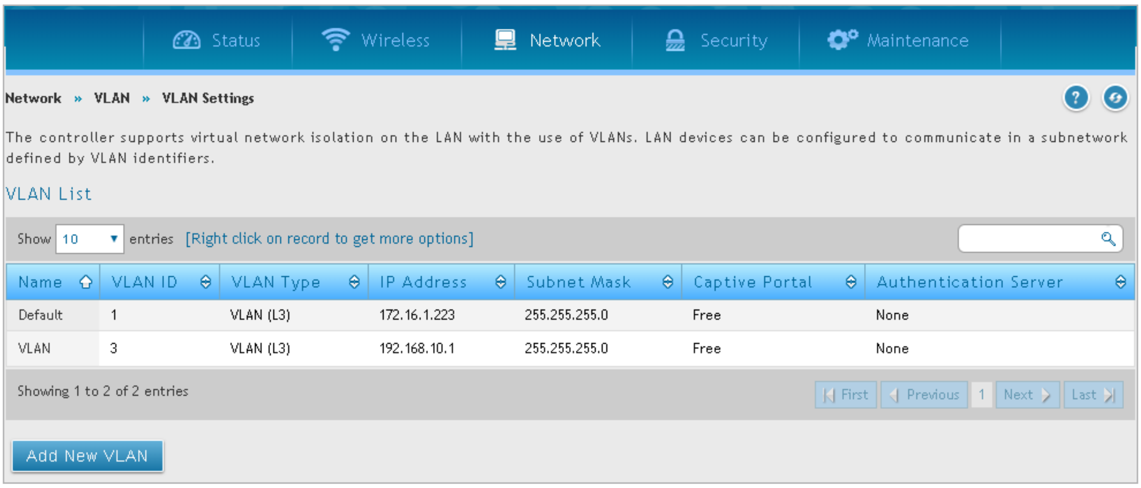


図 6-20　VLAN List 画面

2. 「Add New VLAN」ボタンをクリックします。

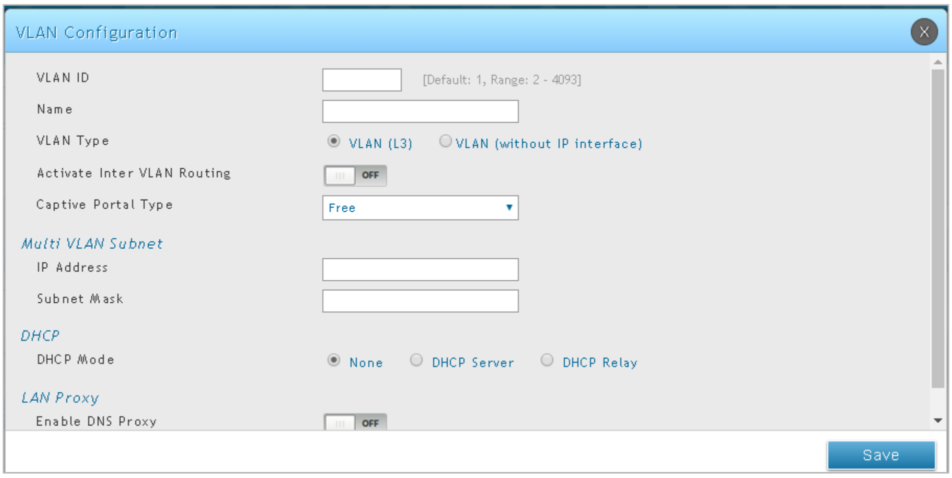


図 6-21　VLAN Configuration 画面

3. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
VLAN ID	本 VLAN に固有の ID（2-4093）を入力します。
Name	本 VLAN の固有の名称を入力します。 名前は、追加する可能性のある他の VLAN とこの VLAN を簡単に識別できるようにする必要があります。
VLAN Type	VLAN Type を「VLAN (L3)」「VLAN (without IP interface)」から指定します。
Activate InterVLAN Routing	VLAN ネットワーク間の通信を許可または拒否します。 ・ ON - 異なる VLAN 間の通信を許可します。 ・ OFF - 異なる VLAN 間の通信を拒否します。
Captive Portal Type	キャプティブポータルのタイプを以下から選択します。 ・ 「Free」「SLA」「Permanent User」「Temporary User」「Billing User」「OAuth」 「OAth」を選択した場合は、ログインに使用するアカウントを「ON」にしてください。

項目	説明
MAC Bypass	「Captive Portal Type」が「Permanent User」の場合、SSID で MAC バイパス機能を有効 / 無効に設定します。「Configure MAC Bypass List」をクリックすると、クライアントの MAC アドレスの設定画面に遷移します。
Enable Redirect	「Captive Portal Type」が「Free」以外 の場合、キャプティブポータル認証後の指定 Web ページへのリダイレクトを有効 / 無効に設定します。
URL	キャプティブポータルユーザが認証後にリダイレクトされる Web ページの URL を入力します。
Authentication Server	「Captive Portal Type」が「Permanent User」の場合、認証サーバのタイプを選択します。: Local User Database、Radius Server、LDAP Server、POP3
Authentication Type	「Authentication Server」に「Radius Server」を選択した場合、認証タイプ（PAP、CHAP、MSCHAP、MSCHAPv2）を選択します。
Primary/Secondary/Third LDAP Server	「Authentication Server」が「LDAP Server」の場合、LDAP サーバを指定します。
Captive Portal Profile	
Choose Profile	キャプティブポータルのプロファイルを「Login Profile」「Custom Profile」から指定します。
Login Profile Name	プルダウンメニューからキャプティブポータルを選択します。「Create a Profile」をクリックして、新しいプロファイルを作成します。
Captive Portal SLA Profile	
SLA Login Profile Name	SLA ログインプロファイル名を選択します。「Create a Profile」をクリックして、新しいプロファイルを作成します。
Multi VLAN Subnet	
IP Address	マルチ VLAN のサブネットの IP アドレスを入力します。
Subnet Mask	マルチ VLAN のサブネットの IP サブネットマスクを入力します。
DHCP	
DHCP Mode	DHCP サーバまたは DHCP リレーを有効または無効にします。
Domain Name	VLAN のドメイン名を入力します。
Default Gateway	使用する LAN のゲートウェイの IP アドレスを入力します。
Primary DNS Server	設定済みの DNS サーバが LAN で利用可能である場合、プライマリ DNS サーバの IP アドレスを入力します。
Secondary DNS Server	設定済みの DNS サーバが LAN で利用可能である場合、セカンダリ DNS サーバの IP アドレスを入力します。
Lease Time	割り当てられる IP アドレスのリースタイムを入力します。
Relay Gateway	「DHCP Mode」が「DHCP Relay」の場合、リレーゲートウェイのアドレスを入力します。
LAN Proxy	
Enable DNS Proxy	「ON」をクリックして DNS プロキシを有効にします。

エントリの編集

1. VLAN リストから編集する VLAN を右クリックし、「Edit」をクリックして、以下の画面を表示します。

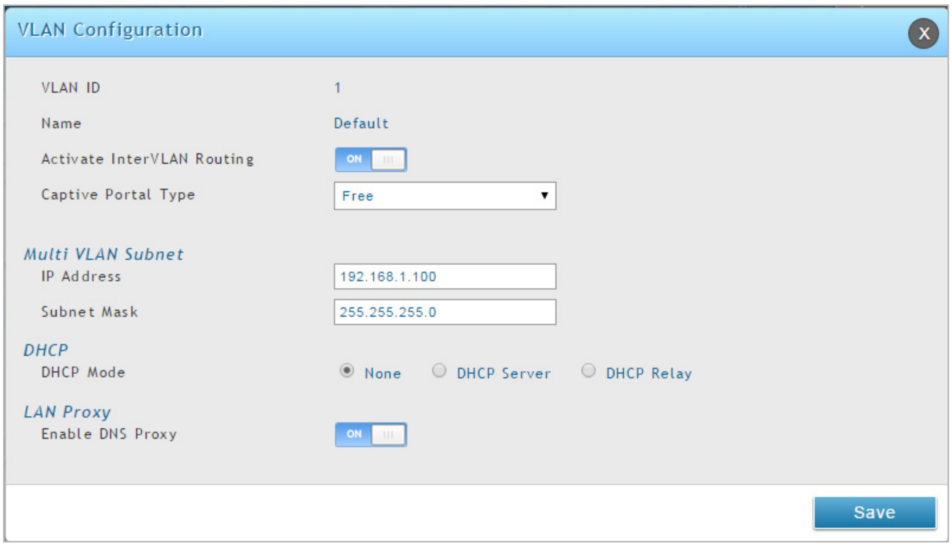


図 6-22　VLAN Configuration 画面

2. フィールドを編集し、「Save」ボタンをクリックします。

エントリの削除

必要でない VLAN エントリを削除します。

注意 VLAN を削除する前に、注意のメッセージは表示されません。そのため、削除する前に、VLAN が不要であることを必ず確認してください。

削除するエントリを右クリックして、「Delete」を選択します。エントリのすべてを削除する場合は、「Select All」をチェック後、「Delete」をクリックします。

マルチ VLAN サブネット

Network > VLAN > VLAN Settings メニュー

各 VLAN には、仮想的に分離しているネットワーク用に固有の IP アドレスとサブネットを割り当てることができます。VLAN のインター VLAN ルーティングが有効でない場合、VLAN サブネットにより、この VLAN に対応するデバイスと通信できる LAN 上のネットワークアドレスが決定されます。

利用可能なマルチ VLAN サブネットの参照および編集

1. **Network > VLAN > VLAN Settings** の順にメニューをクリックし、以下の画面を表示します。

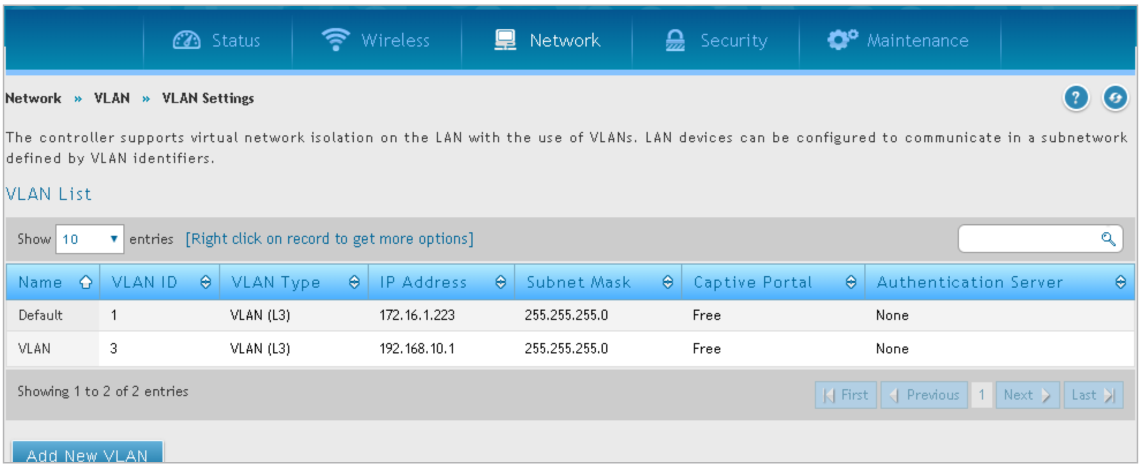


図 6-23　VLAN List 画面

2. マルチサブネット VLAN を編集するためには、VLAN を右クリックして、「Edit」をクリックします。

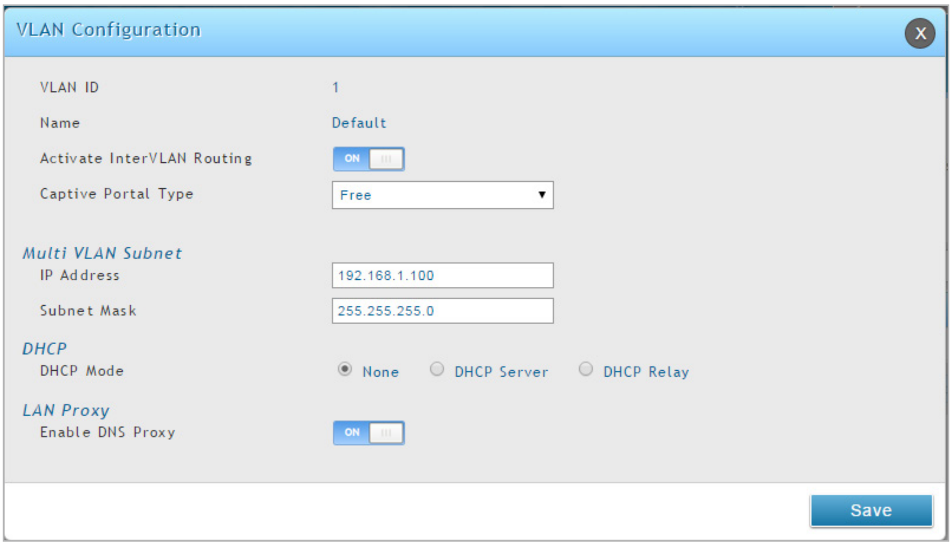


図 6-24　VLAN Configuration 画面

3. 必要な設定を編集して、「Save」ボタンをクリックします。

項目	説明
Multi VLAN Subnet	
IP Address	マルチ VLAN サブネットの IP アドレスを編集します。
Subnet Mask	マルチ VLAN サブネットのサブネットマスクを編集します。
DHCP	
DHCP Mode	VLAN の DHCP モードを選択します。 • None - LAN 上のコンピュータがスタティック IP アドレスで設定されている場合、または別の DHCP サーバを使用するように設定されている場合、本設定を選択します。残りのフィールドは使用できません。 • DHCP Server - DHCP サーバとして無線コントローラを使用するには、本設定を選択します。残りのフィールドを入力します。 • DHCP Relay - 本設定を選択すると、リレーゲートウェイ情報のみ入力が必要です。
Domain Name	VLAN のドメイン名を入力します。
Default Gateway	（オプション）使用している LAN におけるゲートウェイの IP アドレスを入力します。
Primary DNS Server	（オプション）設定済みの DNS サーバが VLAN で利用可能である場合、プライマリ DNS サーバの IP アドレスを入力します。
Secondary DNS Server	（オプション）設定済みの DNS サーバが VLAN で利用可能である場合、セカンダリ DNS サーバの IP アドレスを入力します。
Lease Time	DHCP サーバから受信する IP アドレスを DHCP クライアントが使用できる時間（時）を入力します。リースタイムの期限が切れそうになると、クライアントは、新しいリースを取得するために DHCP サーバに要求を送信します。

項目	説明
Relay Gateway	ゲートウェイアドレスを入力します。「DHCP Mode」に「DHCP Relay」を選択している場合に、このセクションで必要とされる唯一の設定パラメータです。
LAN Proxy	
Enable DNS Proxy	この LAN の DNS プロキシを有効または無効にします。本機能は「自動ロールオーバ」モードの場合に特に役に立ちます。例えば、各接続用の DNS サーバが異なる場合、リンク障害によって DNS サーバへのアクセスが不可能になります。しかし、DNS プロキシが有効であると、クライアントは要求を無線コントローラに行うことができます。また、コントローラは、順番にアクティブな接続の DNS サーバにそれらの要求を送信します。 ・ ON - 無線コントローラは、すべての DNS 要求に対してプロキシとして動作し、ISP の DNS サーバと通信します。すべての DHCP クライアントは、DNS プロキシが実行されている IP（システムの LAN IP）と一緒に、プライマリ / セカンダリの DNS IP を受信します。 ・ OFF - すべての DHCP クライアントが、DNS プロキシ IP アドレスを除いた ISP の DNS IP アドレスを受信します。

エントリの削除

削除するエントリを右クリックして、「Delete」を選択します。エントリのすべてを削除する場合は、「Select All」をチェック後、「Delete」をクリックします。

DHCP プール設定

Network > VLAN > VLAN Settings メニュー

VLAN の DHCP プールを設定します。

1. VLAN Settings 画面で「Add New Pool」をクリックします。

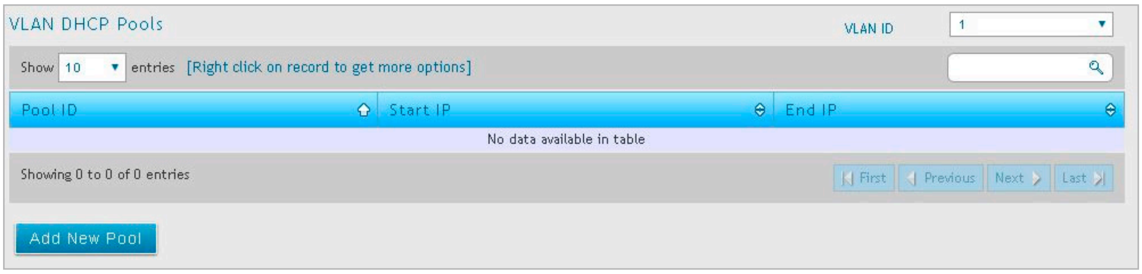


図 6-25　VLAN Settings 画面

2. マルチサブネット VLAN を編集するためには、VLAN を右クリックして、「Edit」をクリックします。

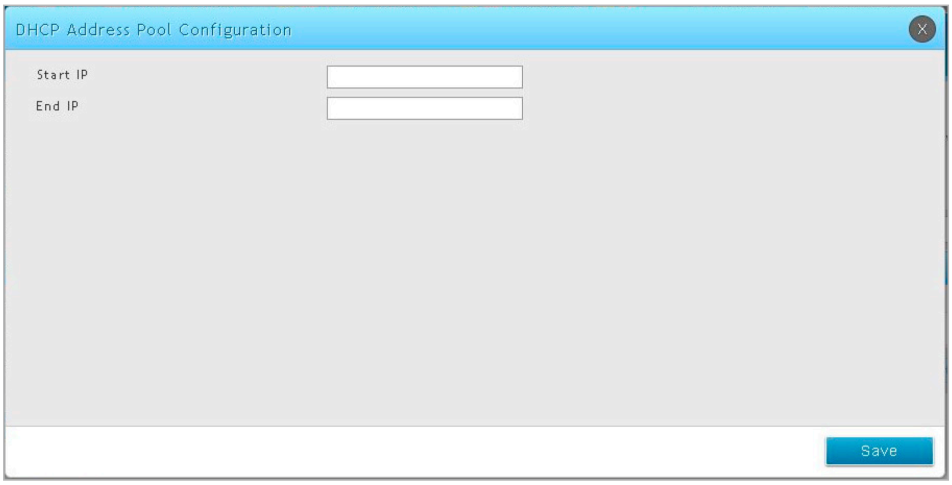


図 6-26　DHCP Address Pool Configuration 画面

3. 必要な設定を編集して、「Save」ボタンをクリックします。

項目	説明
Start IP	VLAN DHCP プールの開始アドレスを入力します。VLAN に参加する DHCP クライアントは「Start IP」から「End IP」までの範囲の IP アドレスが割り当てられます。
End IP	VLAN DHCP プールの終了アドレスを入力します。VLAN に参加する DHCP クライアントは「Start IP」から「End IP」までの範囲の IP アドレスが割り当てられます。

ポート VLAN

Network > VLAN > Port VLAN メニュー

無線コントローラの VLAN 機能を有効にした後に、VLAN に参加するポートを設定します。

1. **Network > VLAN > Port VLAN** の順にメニューをクリックし、以下の画面を表示します。

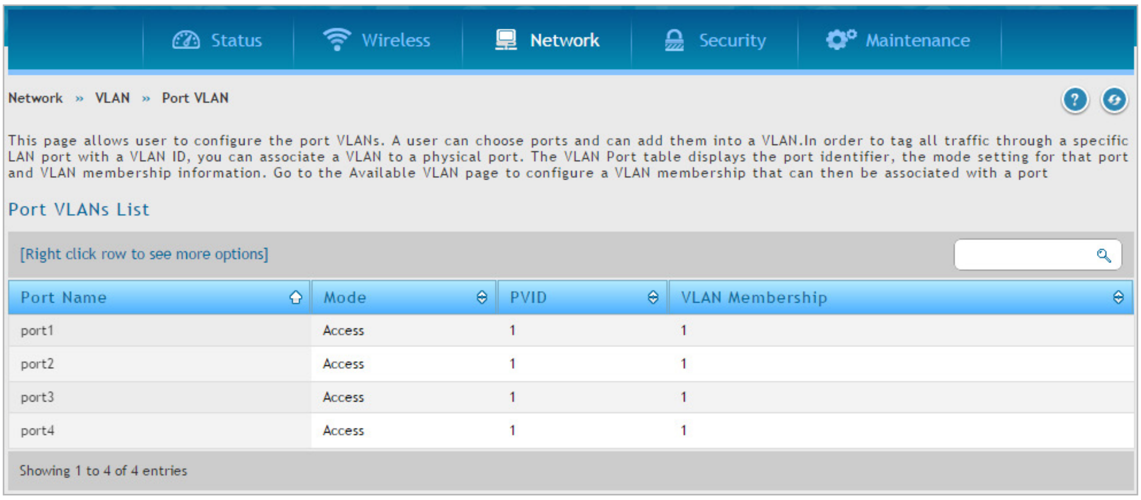


図 6-27　Port VLANs List 画面

2. ポートを右クリックして「Edit」を選択し、以下の画面を表示します。

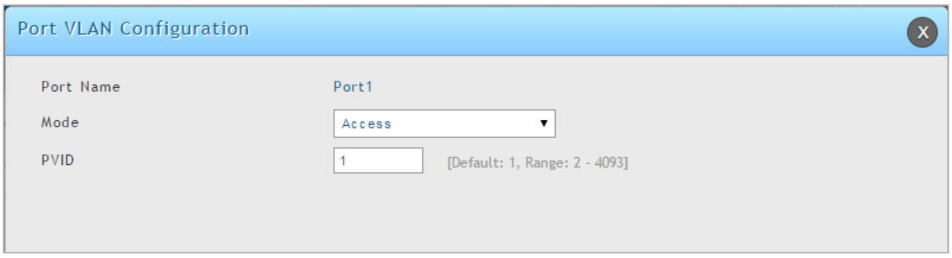


図 6-28　Port VLAN Configuration 画面（Access）

図 6-29　Port VLAN Configuration 画面（Interface）

3. 「Mode」と「PVID」を変更します。

項目	説明
Access	他の VLAN からこのポートを分離します。ポートで送受信するすべてのデータがタグなしとなります。アクセスモードのポートを経由するトラフィックはイーサネットフレームに類似しています。
General	ポートはユーザが選択可能な VLAN セットのメンバになることができます。ポートは VLAN ID を持つタグ付きまたはタグなしデータを送受信します。ポートへのデータがタグなしであると、定義済みの PVID が割り当てられます。ポートから送信された同じ PVID を持つすべてのタグ付きデータは、タグ取りされます。
Trunk	同じ物理リンクにある複数のVLANのトラフィックを多重送信します。ポートで送受信するすべてのデータがタグ付けされます。ポートに入力するタグなしデータはポート PVID=1 を持つデフォルト VLAN を除き転送されません。これはタグなしとなります。
Interface	スタンドアロンインタフェースを選択します。手動でインタフェースの IP アドレス、サブネット、およびゲートウェイを定義します。

4. 「Save」ボタンをクリックします。

MAC ベース VLAN

Network > VLAN > Advanced VLAN > MAC Based VLAN メニュー

パケットにタグ取りまたはプライオリティのタグ付けが行われる場合、デバイスは MAC ベース VLAN テーブルにある送信元 MAC アドレスに対応する VLAN に関連付けします。テーブルに一致するエントリがないと、パケットはデバイスの通常の VLAN 分類ルールの対象となります。

本画面を使用して、MAC エントリを VLAN テーブルにマップします。
送信元 MAC アドレスと VLAN ID の指定後、設定はコントローラのすべてのポートを経由して共有されます。

1. **Network > VLAN > Advanced VLAN > MAC Based VLAN** の順にメニューをクリックし、以下の画面を表示します。

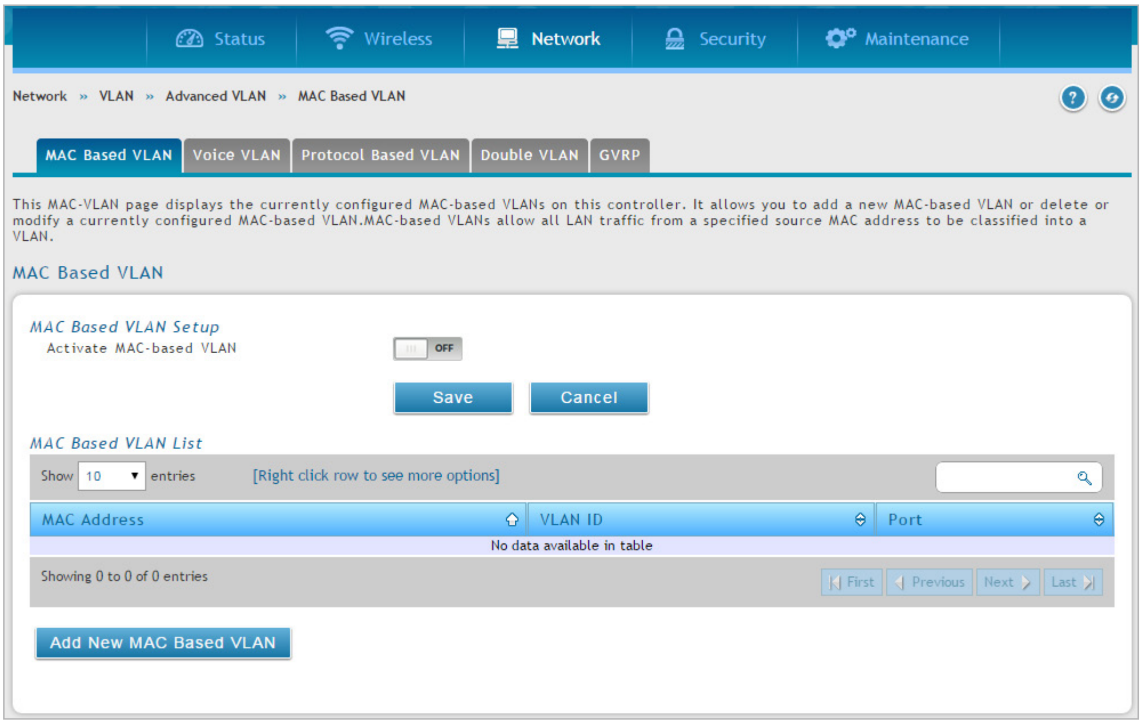


図 6-30　MAC Based VLAN 画面

2. 「Activate MAC-based VLAN」を「ON」に切り替えて、「Save」ボタンをクリックします。
3. 「Add New MAC Based VLAN」ボタンをクリックし、以下の画面を表示します。

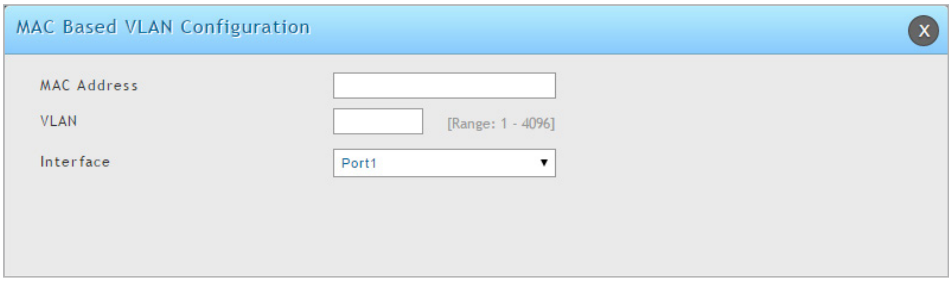


図 6-31　MAC Based VLAN Configuration 画面

4. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
MAC Address	VLAN に追加するクライアントの MAC アドレスを入力します。
VLAN	VLAN ID を入力します。
Interface	プルダウンメニューからポートを選択します。

音声 VLAN

Network > VLAN > Advanced VLAN > Voice VLAN メニュー

音声 VLAN 機能では、定義した設定に基づいて音声トラフィックを処理することができます。これにより、音声とデータのトラフィックはコントローラのポートを経由する際に分割されます。音声 VLAN は、ポートのデータトラフィック量が多い場合に、IP 電話の音声品質の劣化から確実に保護します。

VLAN が提供する隔離機能は、インター VLAN トラフィックを管理制御下におき、ネットワークに接続するクライアントが音声コンポーネントに直接攻撃を開始できないようにします。IEEE 802.1P class-of service（CoS）プロトコルに基づいた QoS プロトコルは、分類とスケジューリングを使用し、予測できる方法でコントローラからのネットワークトラフィックを送信します。システムは、IP 電話データのフローを識別するために、ポートを経由して移動するトラフィックの送信元 MAC を使用します。

音声 VLAN はポート単位で有効にされます。ポートは一度に 1 つの音声 VLAN にのみ参加することができます。音声 VLAN 機能は、初期値では「OFF」（無効）になっています。

1. **Network > VLAN > Advanced VLAN > Voice VLAN** の順にメニューをクリックし、以下の画面を表示します。

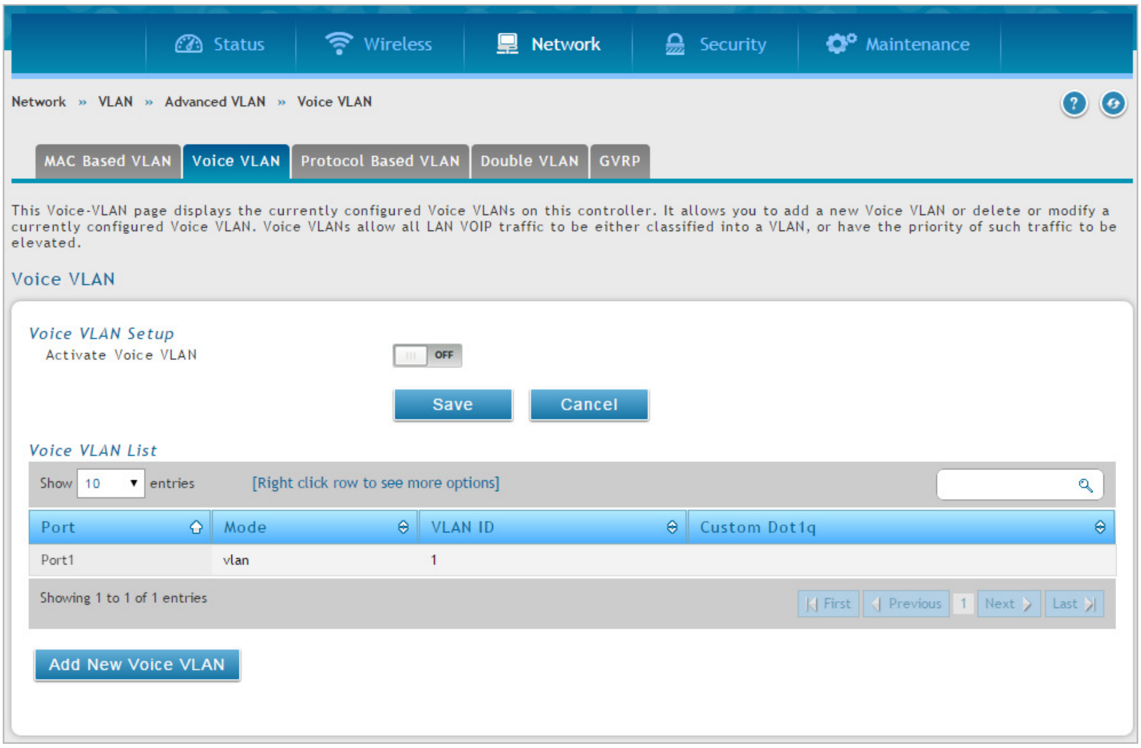


図 6-32　Voice VLAN 画面

2. 「Activate Voice VLAN」を「ON」に切り替えて、「Save」ボタンをクリックします。

3. 「Add New Voice VLAN」ボタンをクリックし、以下の画面を表示します。

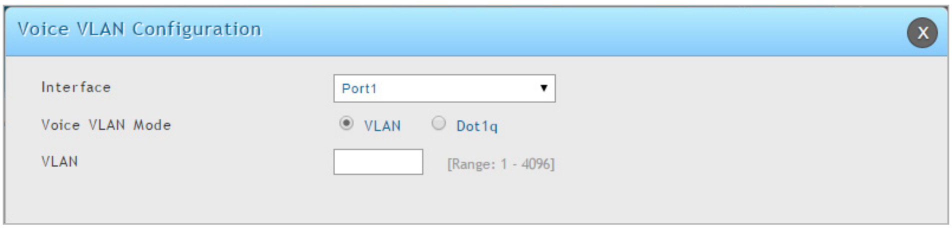


図 6-33　Voice VLAN Configuration 画面

4. インタフェースと音声 VLAN モードを選択します。音声 VLAN モードには以下の項目があります。

項目	説明
VLAN	音声 VLAN パケットは割り当てる番号によって一意に識別されます。すべての音声トラフィックは、ポートのデフォルト VLAN ID が割り当てられる他のデータトラフィックと区別するためにこの VLAN ID が設定されます。しかし、音声トラフィックは他のトラフィックと区別して優先されるわけではありません。
Dot1q	音声データとその他のトラフィックを区別するために、VoIP デバイスによって全ての VoIP トラフィックに対して設定されるパラメータです。他のすべてのトラフィックは、ポートのデフォルトプライオリティを割り当てられます。選択すると「Custom Dot1q Value」を指定します。

5. 「Save」ボタンをクリックします。

プロトコルベース VLAN

Network > VLAN > Advanced VLAN > Protocol Based VLAN メニュー

プロトコルベースの VLAN では、トラフィックは VLAN に関連付けたプロトコルに基づいて指定ポートを通じてブリッジされます。ユーザ定義のパケットフィルタは、特定のパケットが特定の VLAN に所属するかどうかを決定します。多くの場合、プロトコルベースの VLAN は、ネットワークセグメントにおいて複数のプロトコルを実行しているホストが存在するシナリオで使用されます。タグなしパケットのフィルタリング基準を定義するためにプロトコルベースの VLAN を使用することができます。ポートベース（IEEE 802.1Q）またはプロトコルベース VLAN を設定しないと、初期値では、タグなしパケットは VLAN 1 に割り当てられます。ポートベース VLAN、プロトコルベース VLAN、または両方を定義することによって、この動作を変更することができます。タグ付きパケットは、常に IEEE 802.1Q 標準に従って処理され、プロトコルベースの VLAN には含まれません。

特定のプロトコルに対し、プロトコルベース VLAN にポートを割り当てると、そのプロトコル用のポートで受信したタグなしフレームは、プロトコルベースの VLAN ID が割り当てられます。他のプロトコル用のポートで受信したタグなしフレームには PVID が割り当てられます。これは、(1) デフォルト PVID または（2）「Port VLAN Configuration」画面を使用してポートに割り当てた PVID のいずれかです。「Protocol Based VLAN Configuration」画面を使用して、割り当てるプロトコルと VLAN を設定し、次にこれらの設定を使用するポートを有効にします。

グループを作成することで、プロトコルベースの VLAN を定義します。各グループは、VLAN ID を使用した 1 対 1 の関係を持っていて、1 つ以上のプロトコル定義を含むことができ、また複数のポートを含むことができます。

1. **Network > VLAN > Advanced VLAN > Protocol Based VLAN** の順にメニューをクリックし、以下の画面を表示します。

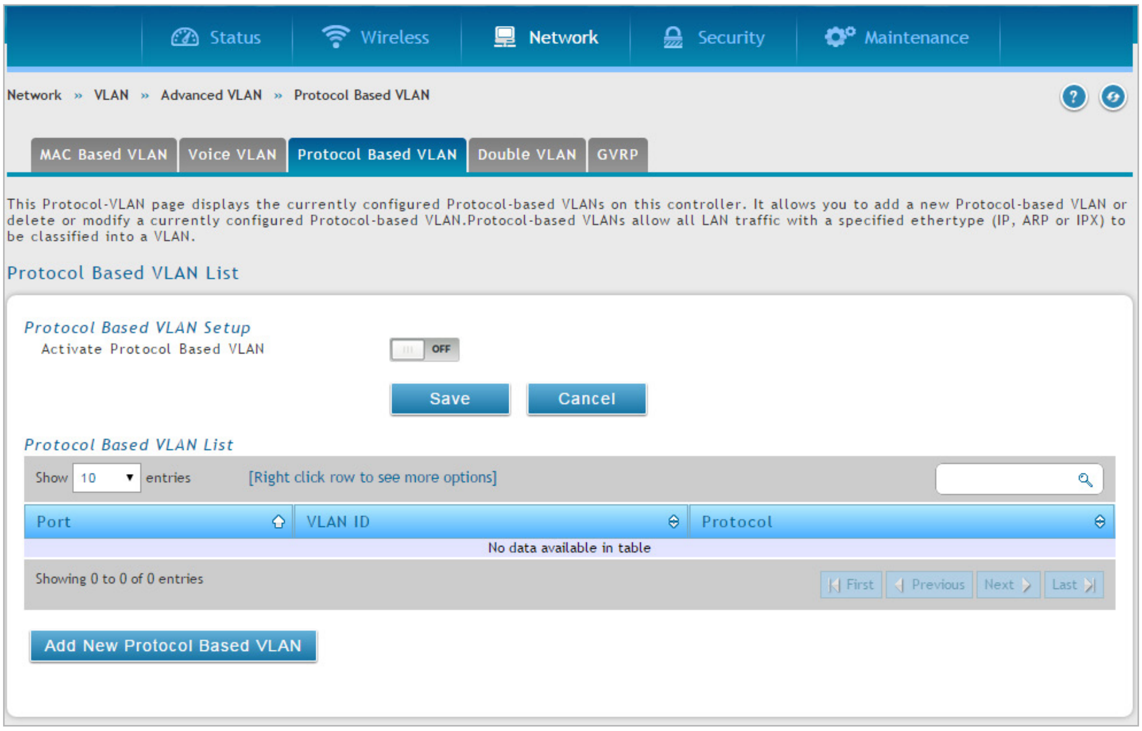


図 6-34　Protocol Based VLAN List 画面

2. 「Activate Protocol Based VLAN」を「ON」に切り替えて、「Save」ボタンをクリックします。
3. 「Add New Protocol Based VLAN」ボタンをクリックし、以下の画面を表示します。

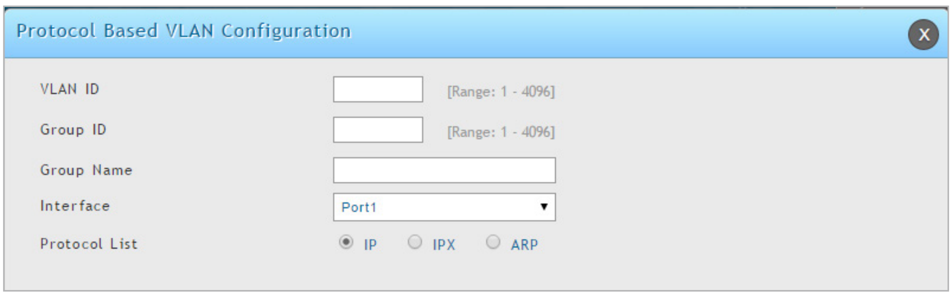


図 6-35　Protocol Based VLAN Configuration 画面

4. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
VLAN ID	このグループに割り当てる VLAN ID（1-4096）を指定します。
Group ID	グループを識別する番号を指定します。
Group Name	（オプション）プロトコルグループ ID に割り当てる名前（16 文字以内）を入力または編集します。
Interface	グループに追加するインタフェースを選択します。
Protocol List	このグループに関連させるプロトコルを選択します。

ダブル VLAN

Network > VLAN > Advanced VLAN > Double VLAN メニュー

ダブル VLAN トンネリングでは、ネットワークトラフィックで 2 個目のタグを使用することができます。追加のタグを使用することで、メトロポリタンネットワーク（MAN）において、カスタマが自身の 802.1Q ドメインに接続する際に個別のカスタマの VLAN 識別子を保持し、カスタマ間を識別することが可能になります。

この 2 個目のタグの挿入を行うと、イーサネットベースの MAN にトラフィックを送信するために 4k VLAN ID のスペースを分割する必要がなくなります。ダブル VLAN トンネリングが有効な場合、インタフェースから転送されるすべてのパケットには DVlan タグが割り当てられ、インタフェースで受信するすべてのパケットのタグは（1 つ以上のタグが存在する場合）削除されます。

本画面を使用して、1 つ以上のポートにダブル VLAN フレームのタグを設定します。

1. **Network > VLAN > Advanced VLAN > Double VLAN** の順にメニューをクリックし、以下の画面を表示します。

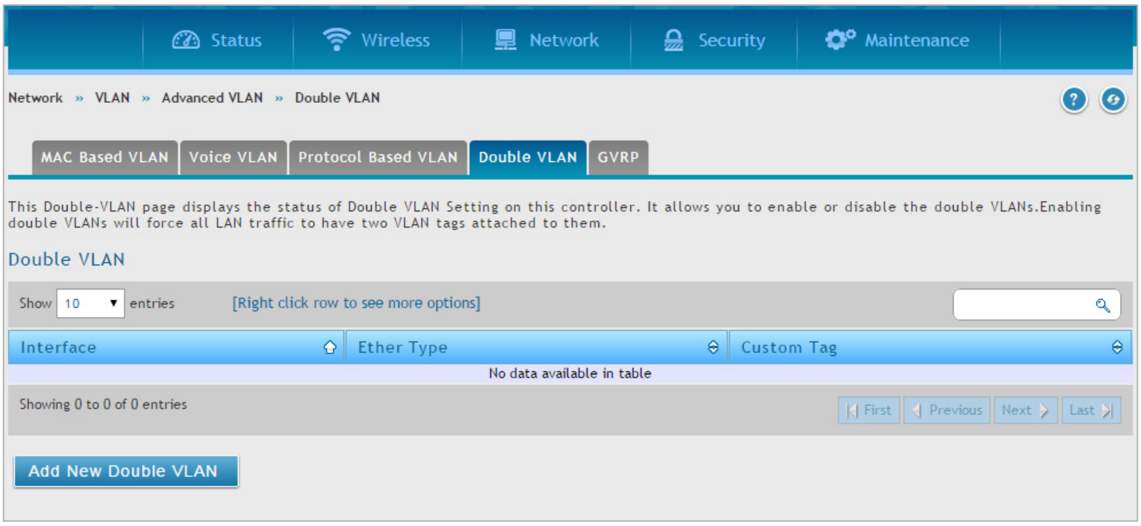


図 6-36　Double VLAN 画面

2. 「Add New Double VLAN」ボタンをクリックし、以下の画面を表示します。

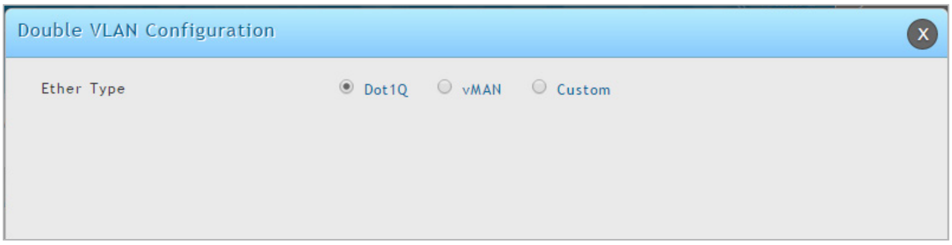


図 6-37　Double VLAN Configuration 画面

3. 「Ether Type」を「Dot1q」「vMAN」「Custom」から選択します。「Custom」を選択した場合は「Custom Tag」を指定します。
4. 「Save」ボタンをクリックします。

GVRP

Network > VLAN > Advanced VLAN > GVRP メニュー

GVRP（GARP VLAN Registration Protocol）は、ネットワークコントローラが、同じセグメントに所属するネットワークデバイスに対して VLAN メンバシップ情報をダイナミックに登録（および登録解除）し、GMRP をサポートするブリッジ LAN 内のすべてのネットワークコントローラを経由してその情報を広められるネットワークメカニズムを提供します。

1. **Network > VLAN > Advanced VLAN > GVRP** の順にメニューをクリックし、以下の画面を表示します。

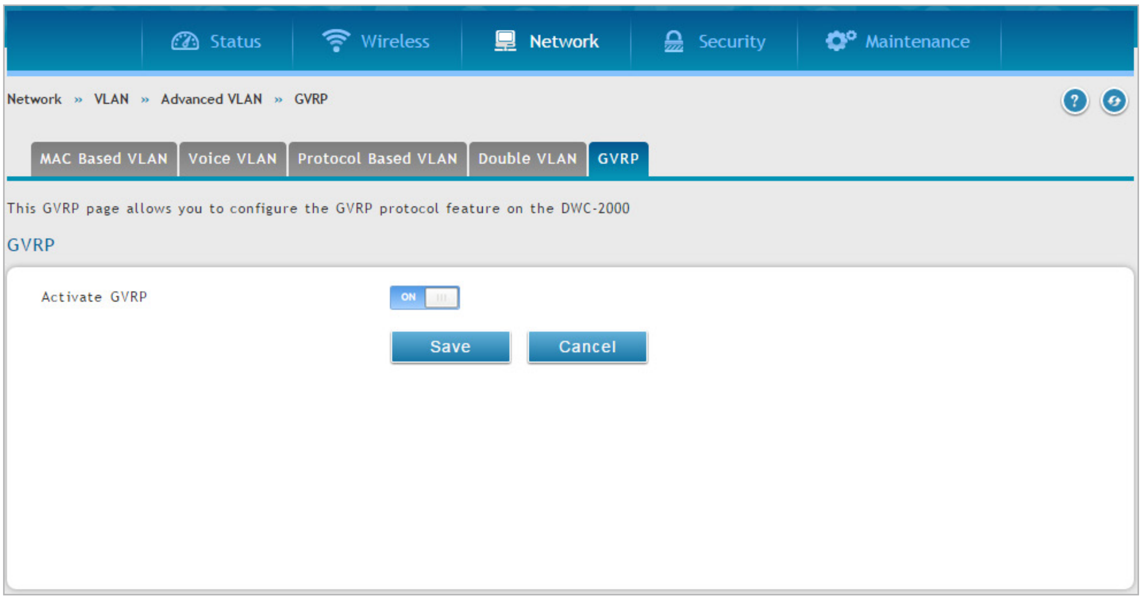


図 6-38　GVRP 画面

2. 「Activate GVRP」を「ON」に切り替えて、「Save」ボタンをクリックします。

ルーティング設定

スタティックルートは、ネットワークデバイスに対して、正確で固定 された（変更不可の）送信先について通知します。スタティックルートは小規模のネットワークで適切に動作します。「Static Route」および「Protocol-Binding」という 2 種類のスタティックルートがあります。

スタティックルートでは、ネクストホップの場所を決定するために IP アドレスを使用しますが、プロトコルバインディングではプロトコルを使用します。スタティックルーティングに無線コントローラを設定すると、ダイナミックルーティングプロトコルを使用せずに、コントローラとルーティングデバイス間のデータ転送を可能にします。

IPv4 スタティックルーティングの設定

Network > Routing > IPv4 Static Routes メニュー

■ スタティックルートの追加

1. **Network > Routing > IPv4 Static Routes** の順にメニューをクリックし、以下の画面を表示します。

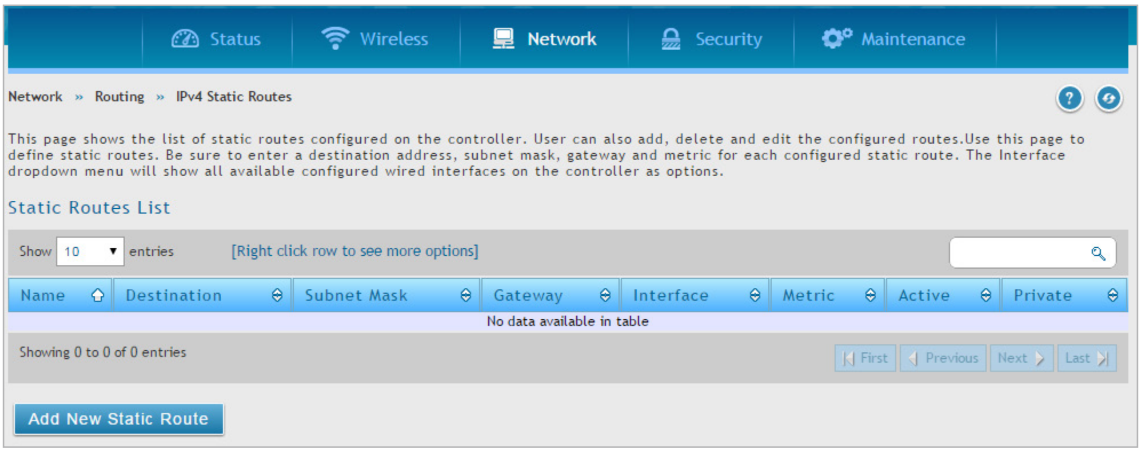


図 6-39　Static Route List 画面

2. 「Add New Static Route」ボタンをクリックし、以下の画面を表示します。

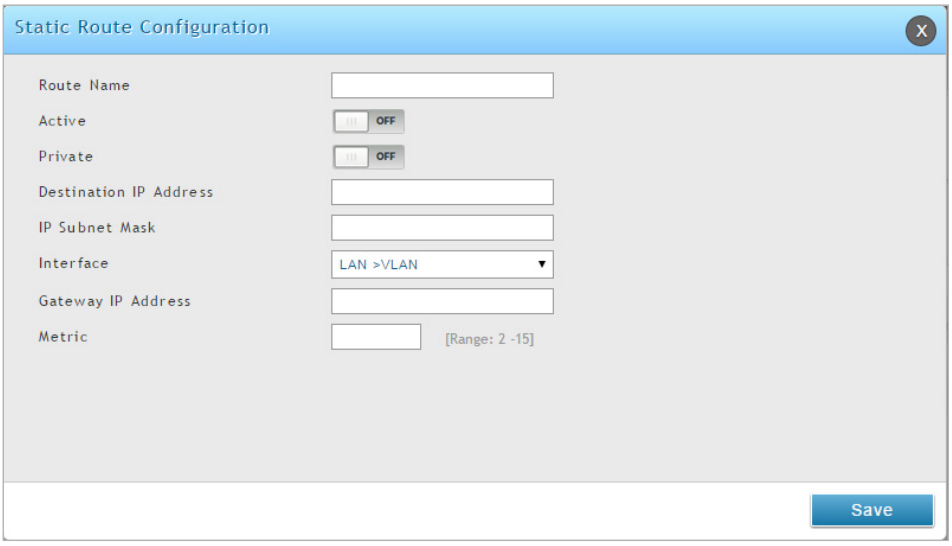


図 6-40　Static Route Configuration 画面

3. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
Route Name	スタティックルートの固有の名称を入力します。名前は、追加する可能性のある他のルートとこのルートを簡単に識別できるようにする必要があります。
Active	ルートの状態をアクティブ化または非アクティブ化します。 • ON - スタティックルートをアクティブ化します。 • OFF - スタティックルートを非アクティブ化します。
Private	スタティックルートをプライベートに指定します。 • ON - スタティックルートはプライベートです。 • OFF - スタティックルートはプライベートではありません。
Destination IP Address	スタティックルートの送信先 IP アドレスを入力します。
IP Subnet Mask	スタティックルートのサブネットマスクを入力します。
Interface	パケットの送信先インタフェースを選択します。
Gateway IP Address	ゲートウェイルータの IP アドレスを入力します。これは、無線コントローラのネクストホップアドレスです。
Metric	ルートの管理ディスタンスを入力します。

IPv6 スタティックルーティングの設定

Network > Routing > IPv6 Static Routes メニュー

このデバイスに手動でスタティックルートを追加すると、1 つのインタフェースから別のインタフェースまでのトラフィック経路の選択を定義できます。このコントローラと他のデバイス間には、経路の変更を通知するための通信はありません。スタティックルートが設定されると、ネットワークの変更があるまで、ルートはアクティブで有効となります。

スタティックルートのリストでは、管理者が手動で登録した全ルートが表示され、そのスタティックルートに対して操作を行うことができます。IPv4 スタティックルートのリストと IPv6 スタティックルートのリストは、一部の例外を除き同じフィールドを共有します。

■ IPv6 スタティックルーティングの設定

1. **Network > Routing > IPv6 Static Routes** の順にメニューをクリックし、以下の画面を表示します。

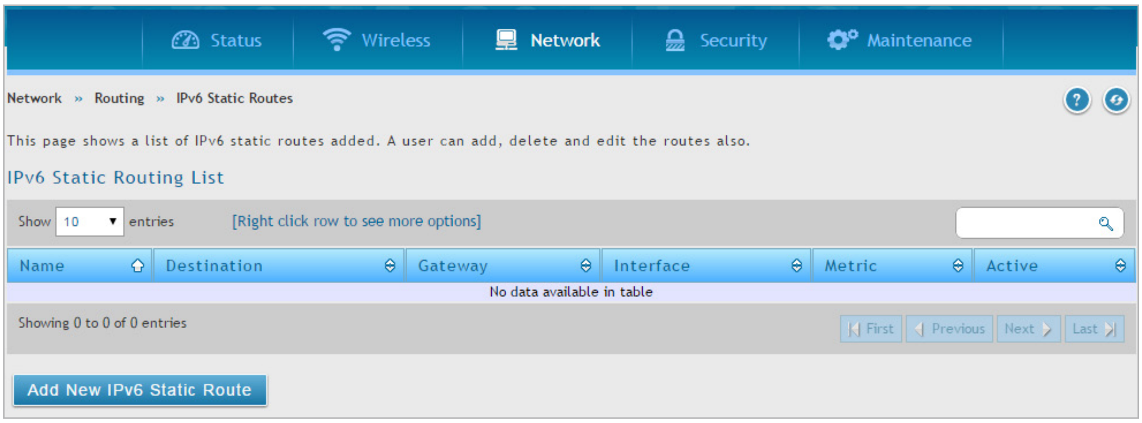


図 6-41　IPv6 Static Routing List 画面

2. 「Add New IPv6 Static Route」ボタンをクリックし、以下の画面を表示します。

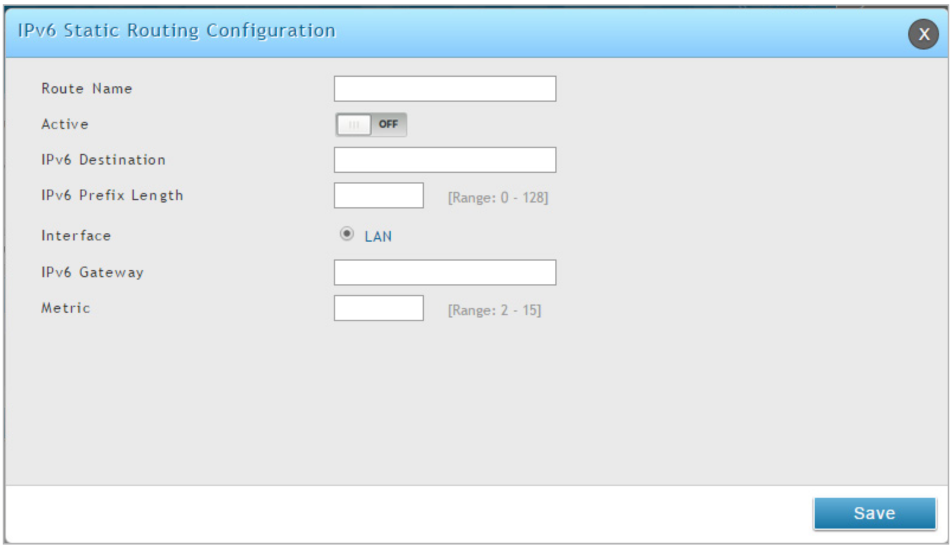


図 6-42　IPv6 Static Routing Configuration 画面

3. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
Route Name	スタティックルートの固有の名称を入力します。名前は、追加する可能性のある他のスタティックルートとこのスタティックルートを簡単に識別できるようにする必要があります。
Active	ルートの状態をアクティブ化または非アクティブ化します。 • ON - スタティックルートをアクティブ化します。 • OFF - スタティックルートを非アクティブ化します。
IPv6 Destination	スタティックルートの送信先 IPv6 アドレスを入力します。
IPv6 Prefix Length	サブネットを定義する IPv6 アドレス内のプレフィックスビット数を指定します。
Interface	スタティックルートに接続する無線コントローラのインタフェースを選択します。 • LAN - 無線コントローラの LAN または VLAN ポートがスタティックルートに接続します。
IPv6 Gateway	宛先ホストまたはネットワークに到達できるゲートウェイの IP アドレスを指定します。
Metric	ルートの優先度を決定します。同じ宛先に対して複数のルートが存在している場合、最も低いメトリックを持つルートが選択されます。

スタティックルートの編集 / 削除

スタティックルートの追加後、スタティックルートを編集するためには、編集するスタティックルートを右クリックして、「Edit」を選択します。

スタティックルートを削除するためには、削除するスタティックルートを右クリックして、「Delete」を選択します。スタティックルートのすべてを削除する場合は、「Select All」をチェック後、「Delete」を選択します。

スタティックルートの有効化

有効にするスタティックルートを右クリックして、「Enable」を選択します。

QoS 設定

標準のコントローラでは、各物理ポートは、接続するネットワーク上でパケットを送信するための 1 つ以上のキューで構成されます。多くの場合、ポートごとに複数のキューが提供され、ユーザ定義の基準に基づいて特定のパケットが他のパケットより優先されます。パケットがポート内の送信キューにある場合、これを処理する速度は、キューの設定方法やポートのその他のキューに存在するトラフィック量に依存します。遅延する必要がある場合、パケットは、スケジューラがそのキューの送信を許可するまでキューに保持されます。キューが一杯になると、送信用にパケットを保持するスペースがないため、パケットはコントローラによって破棄されます。

QoS は、リアルタイム性が要求されるパケットと、遅延が許容されるパケットとを識別することで、一貫性があり予測可能な送信を提供する方法です。リアルタイム性が要求されるパケットは、QoS をサポートするネットワークでは「特別扱い」を受けます。この点を考慮して、ネットワークのすべての要素が QoS 対応である必要があります。QoS 対応でないノードが少なくとも 1 つ存在すると、ネットワークパスに不具合が起こり、パケットフロー全体のパフォーマンスが低下します。

QoS 優先度

QoS 優先度の設定には、次の 3 段階の手順があります。

1. QoS モードを有効にします。
2. 各ポートで「Trust Mode」を定義します。（「各ポートの DSCP と CoS の定義」参照）
3. DHCP または CoS 設定を定義します。（「DSCP 優先度の設定」または「802.1p 優先度の設定」参照）

QoS モードの有効化

Network > QoS > QoS Priority メニュー

無線コントローラにおける QoS 機能を有効にします。通常､ネットワークはベストエフォートデリバリ型で運用します。これは､すべてのトラフィックには同じ優先度があり、いずれもタイムリーに送信される可能性があることを意味します。輻輳が起こると、すべてのトラフィックは等しく破棄される可能性があります。

QoS 機能で優先処理を設定するには、特定のネットワークトラフィックを選択して、相対的な重要度に従って優先順位を付け、輻輳管理と輻輳回避技術を使用します。ご使用のネットワークに QoS を実装すると、ネットワーク性能をさらに予測できるようになり、帯域幅使用がより効率的になります。無線コントローラの LAN ポートでトラフィックの輻輳が予想される場合に、特に役に立ちます。

QoS 分類は、レイヤ 2 またはレイヤ 3 フレームに適用できます。このため、レイヤ 2 の CoS 設定またはレイヤ 3 の DSCP 設定を使用するために無線コントローラを設定することができます。

注意　また、無線コントローラは、入力パケットの CoS 値を（QoS がトラフィックの優先度を表すために内部的に使用する）DSCP 値にマップするために CoS-to-DSCP マップを提供します。この機能にアクセスするには、**Network > QoS > QoS Priority** の順にメニューをクリックし、以下の画面を表示します。

■ QoS モードの設定

1. **Network > QoS > QoS Priority** の順にメニューをクリックし、以下の画面を表示します。

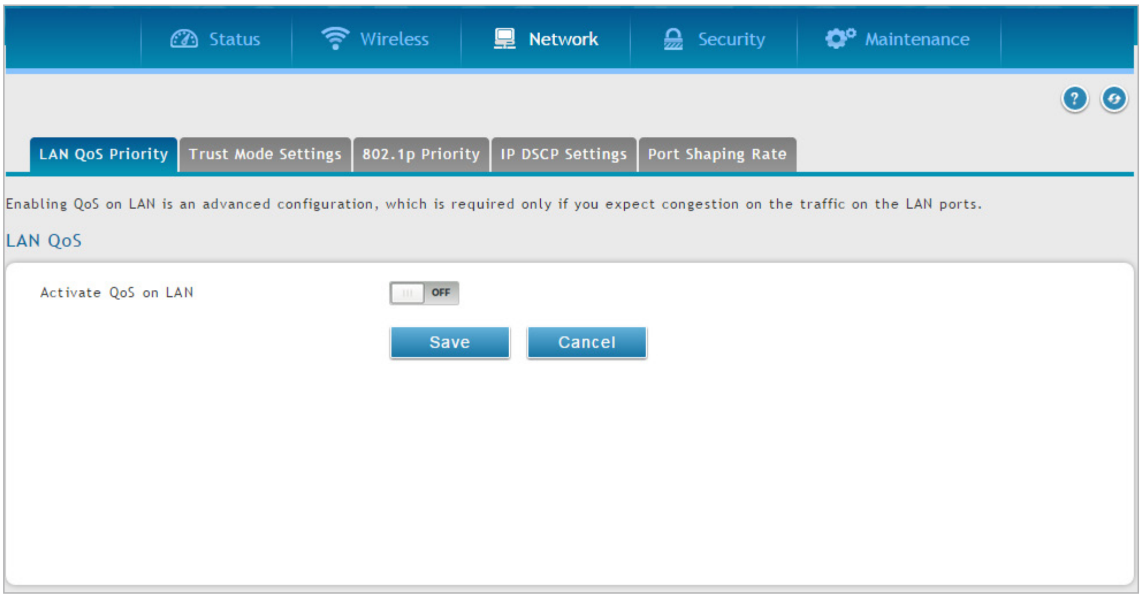


図 6-43　LAN QoS 画面

2. 「Activate QoS on LAN」を「ON」に切り替えて、「Save」ボタンをクリックします。

3.　「Trust Mode Settings」タブをクリックします。

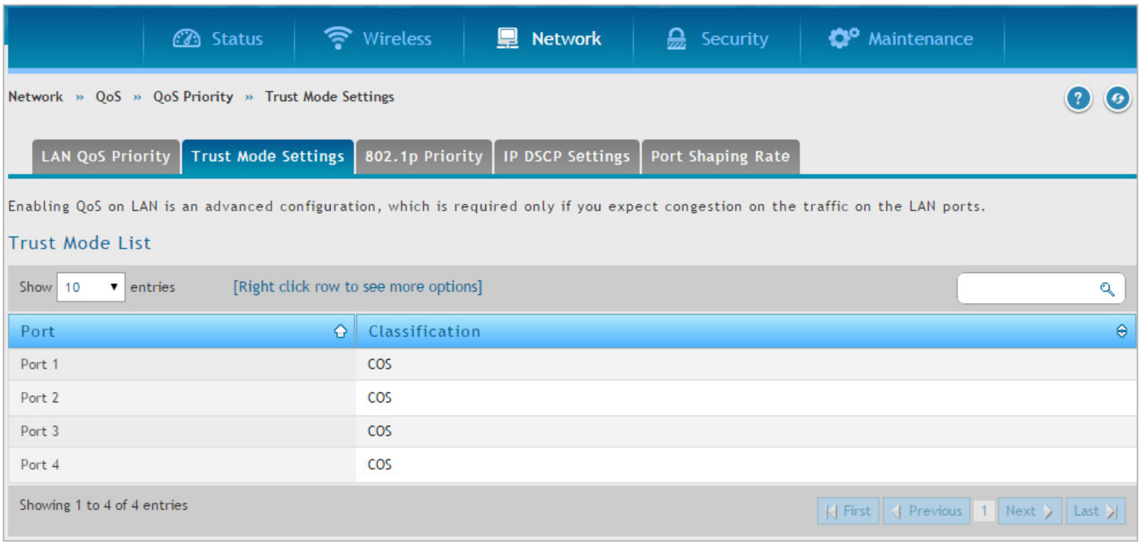


図 6-44　Trust Mode List 画面

4.　「Trust Mode List」でポートを右クリックして「Edit」を選択すると、以下の画面が表示されます。

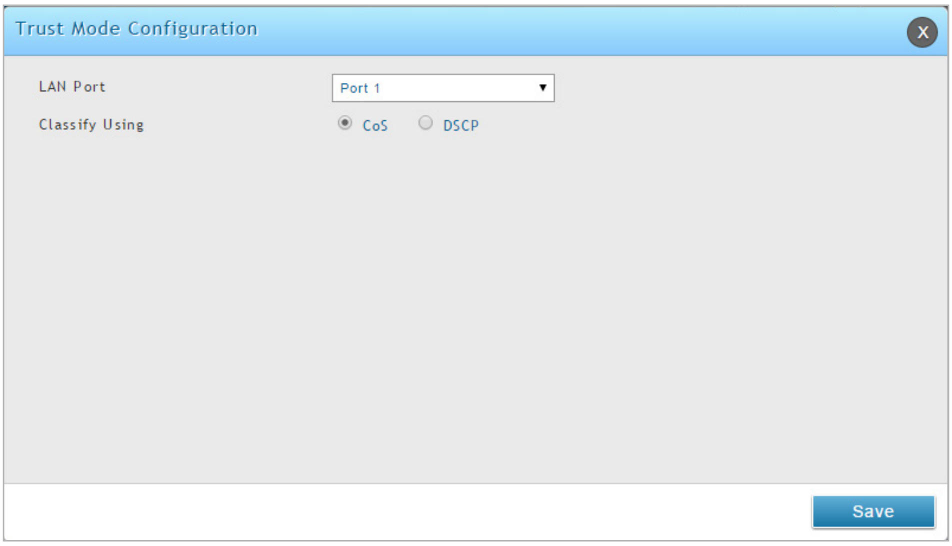


図 6-45　Trust Mode Configuration 画面

5.　「LAN Port」でポート番号を入力し、「Classify Using」で「CoS」または「DSCP」を選択します。

6.　「Save」ボタンをクリックします。

7.　DSCP と CoS、およびその優先度を設定するには、「DSCP 優先度の設定」または「802.1p 優先度の設定」に進みます。

各ポートの DSCP と CoS の定義

Network > QoS > QoS Priority > Trust Mode Settings メニュー

ポートに CoS、または DSCP を選択します。ポートに輻輳が発生している場合、LAN ポートは、パケット内のこのフィールドの値をチェックして、そのパケットに対する優先度で判断を行います。DSCP および CoS の個々の値と、それらに付与される優先度は、QoS の「802.1p Priority List」および「IP DSCP List」ページで設定されます。

1. **Network > QoS > QoS Priority > Trust Mode Settings** の順にメニューをクリックし、以下の画面を表示します。

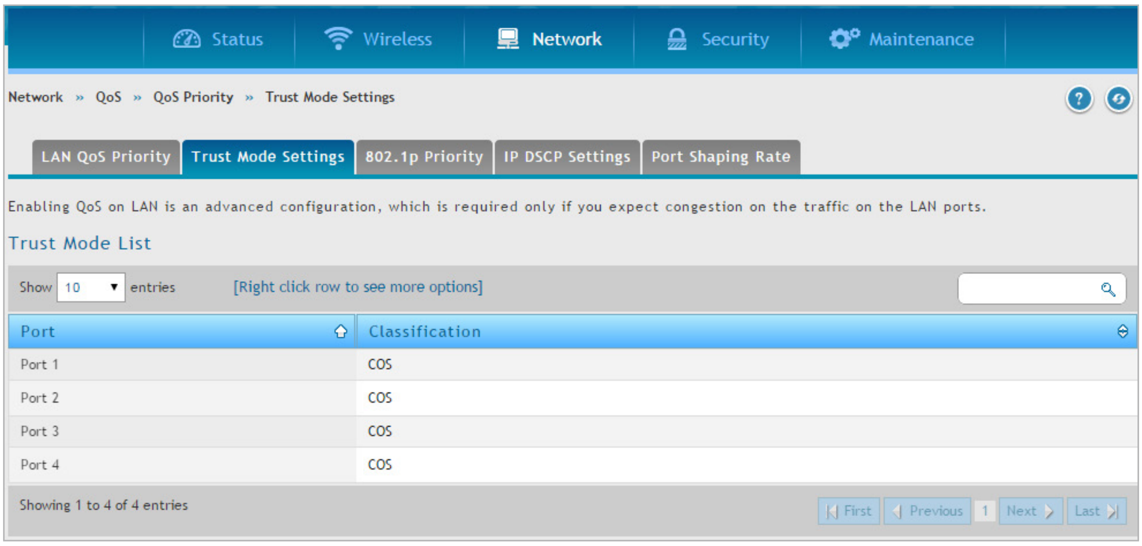


図 6-46　Trust Mode List 画面

2. ポートを右クリックして、「Edit」を選択すると、以下の画面が表示されます。

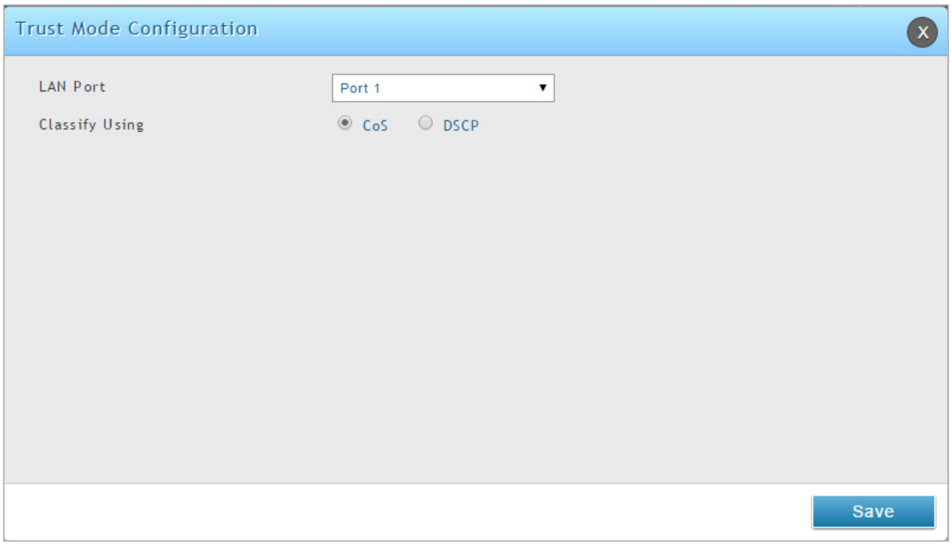


図 6-47　Trust Mode Configuration 画面

3. 「CoS」または「DSCP」モードを選択し、「Save」ボタンをクリックします。

QoS モードを有効にした後に、次のセクションの手順を使用して、DSCP および CoS に使用される値と優先度を設定します。

802.1p 優先度の設定

Network > QoS > QoS Priority > 802.1p Priority メニュー

QoS 設定で CoS を選択した場合、以下の手順を使用して、IP パケットの CoS フィールドに優先度を設定し割り当てることができます。

1. **Network > QoS > QoS Priority > 802.1p Priority** の順にメニューをクリックし、以下の画面を表示します。

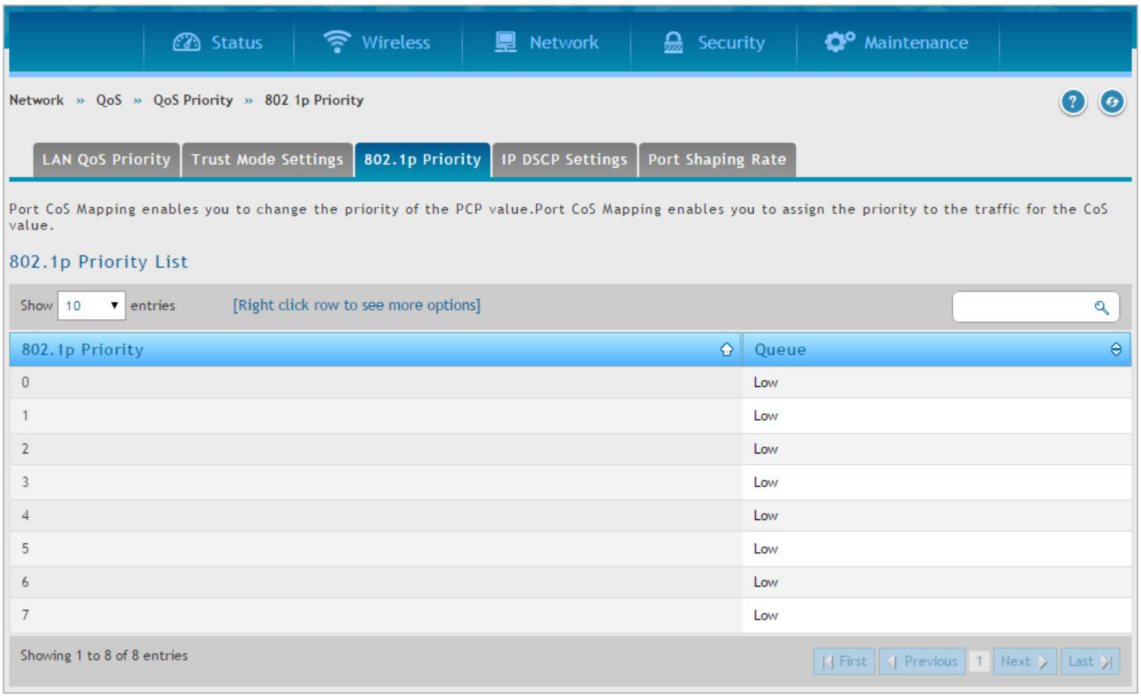


図 6-48　802.1p Priority List 画面

各列は IP パケットの CoS フィールドに対応しています。

2. CoS フィールドを右クリックして、「Edit」を選択すると、以下の画面が表示されます。

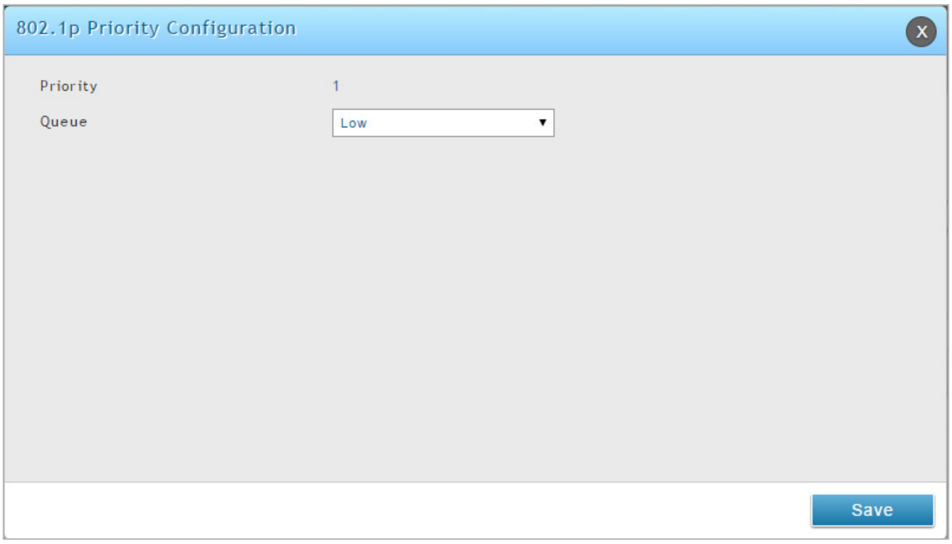


図 6-49　802.1p Priority Configuration 画面

3. 「Queue」プルダウンメニューで、優先度を選択し、「Save」ボタンをクリックします。
   - Highest（最高）
   - Medium（中）
   - Low（低）
   - Lowest（最低）

4. 優先度を付与する追加の各 CoS フィールドに対して手順を繰り返します。

DSCP 優先度の設定

Network > QoS > QoS Priority > IP DSCP Settings メニュー

QoS 設定で DSCP を選択した場合、以下の手順を使用して、IP パケットの DSCP フィールドに優先度を設定し割り当てることができます。

1. **Network > QoS > QoS Priority > IP DSCP Settings** の順にメニューをクリックし、以下の画面を表示します。

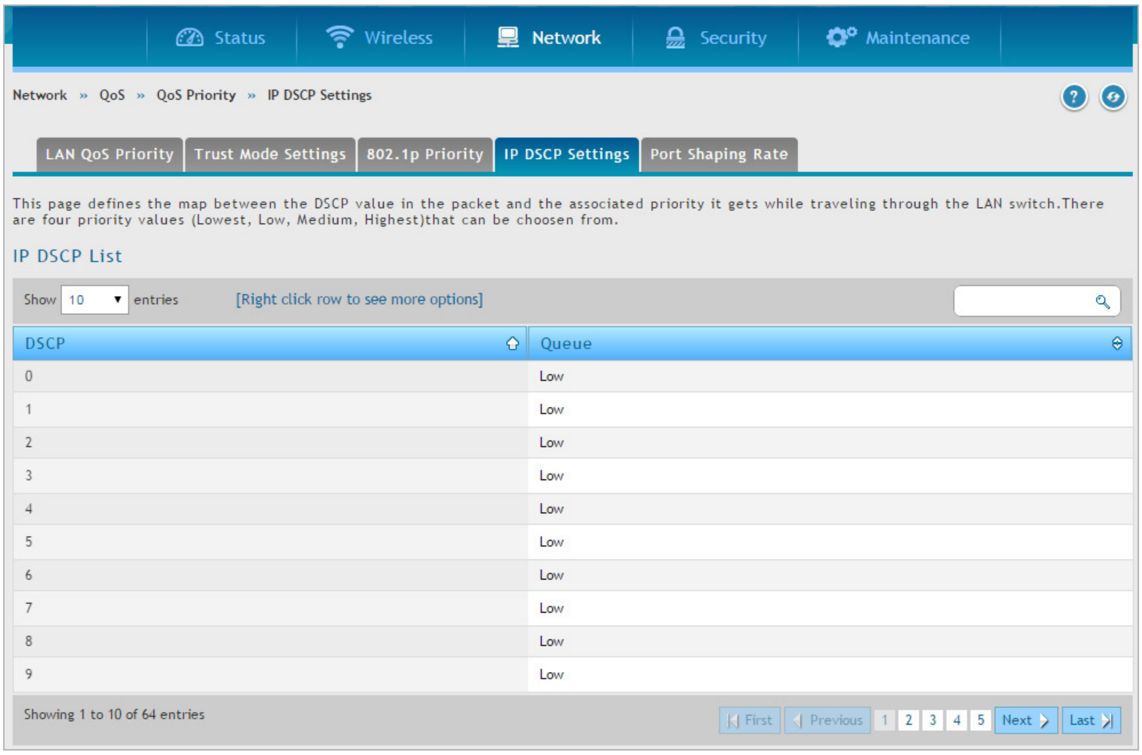


図 6-50　IP DSCP List 画面

2. 「DSCP」を右クリックして、「Edit」を選択すると、以下の画面が表示されます。

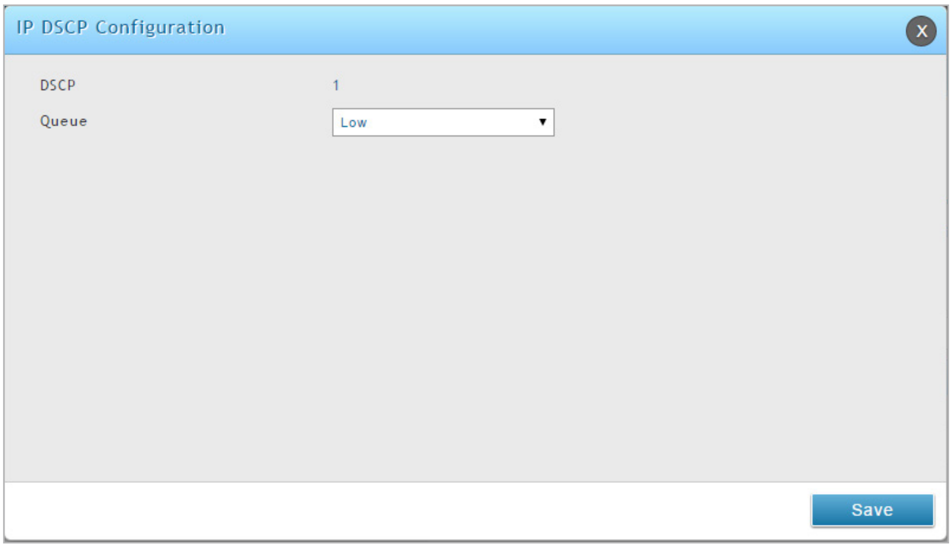


図 6-51　IP DSCP Configuration 画面

3. 「Queue」プルダウンメニューで優先度を選択し、「Save」ボタンをクリックします。
   - Highest（最高）
   - Medium（中）
   - Low（低）
   - Lowest（最低）

4. 優先度を付与する追加の DSCP フィールドのそれぞれに対して手順を繰り返します。

ポートシェーピングレート

Network > QoS > QoS Priority > Port Shaping Rate メニュー

すべてのポート、または、指定ポートにインタフェースのシェーピングレートを設定します。右クリックして、割合を編集します。

1. **Network > QoS > QoS Priority > Port Shaping Rate** の順にメニューをクリックし、以下の画面を表示します。

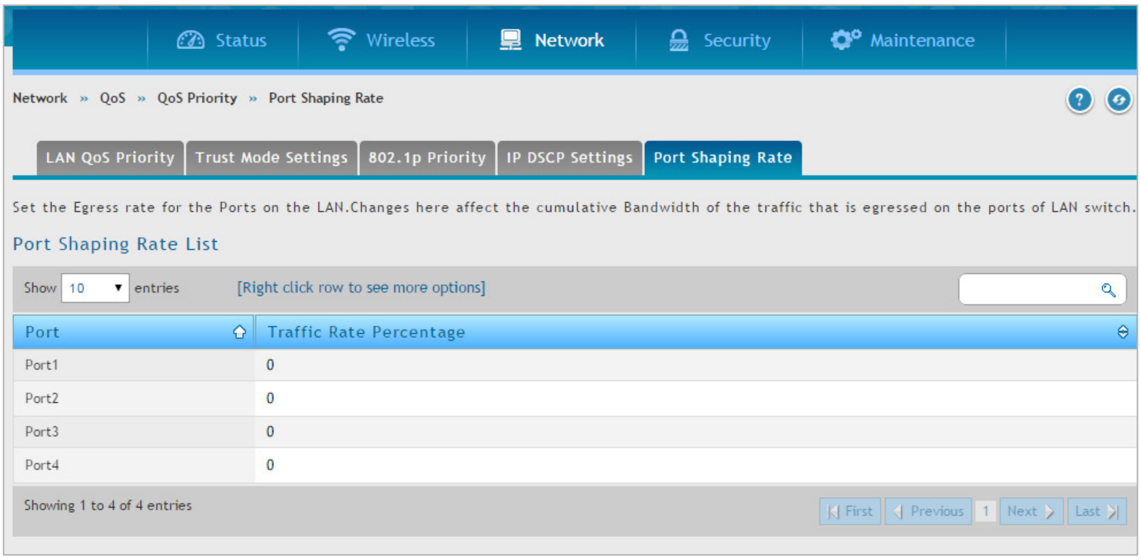


図 6-52　Port Shaping Rate List 画面

2. 編集するポートを右クリックして、「Edit」を選択すると、以下の画面が表示されます。

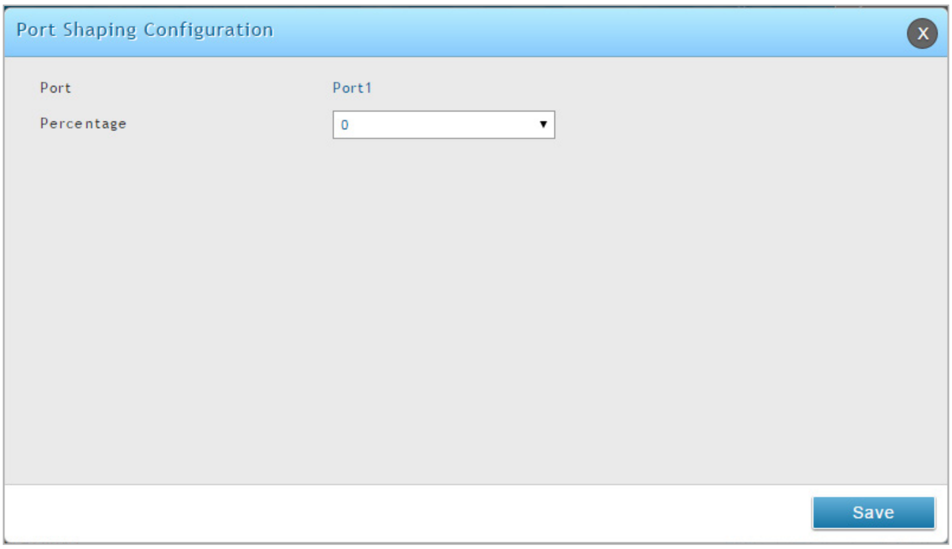


図 6-53　Port Shaping Configuration 画面

3. プルダウンメニューからポートに割り当てる割合を選択し、「Save」ボタンをクリックします。

項目	説明
Port	ポートシェーピングレートが作用するポートを表示します。
Percentage	ポート上で送信可能なトラフィック量の上限を設定します。最大の伝送帯域幅の制限は、通常のトラフィック転送の中で発生する一時的なトラフィックバーストを平滑化する効果があるため、転送されるトラフィックレートが制限されます。

QoS ポリシー設定

QoS ポリシーでは、LAN の照合基準に基づいてトラフィックの優先度を設定します。これを変更するとポートに出力されるトラフィックに影響します。優先度の変更はイーグレストラフィックの優先度に影響することにご注意ください。

ポリシーベース QoS の設定

Network > QoS > QoS Policy > Policy Based QoS メニュー

1. **Network > QoS > QoS Policy > Policy Based QoS** の順にメニューをクリックし、以下の画面を表示します。

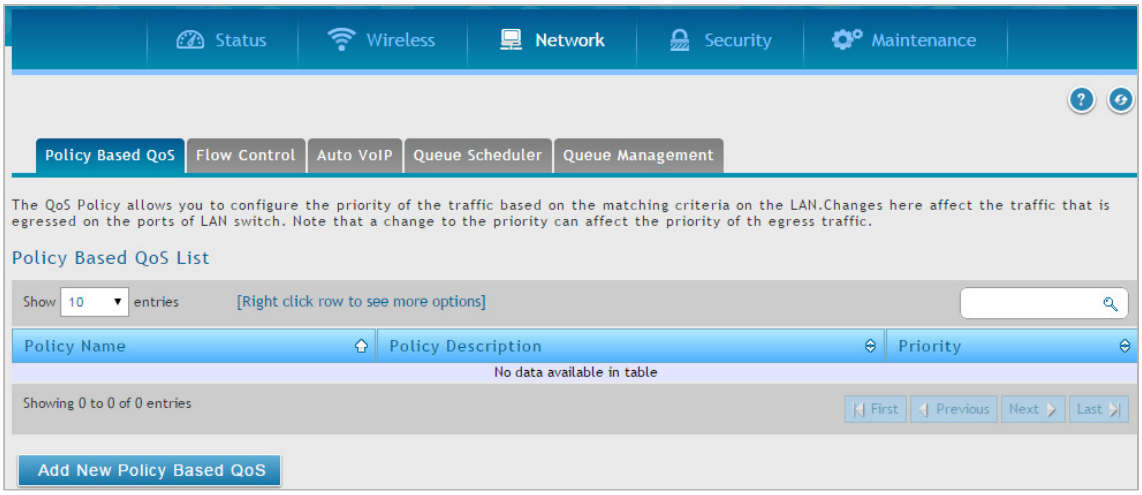


図 6-54　Policy Based QoS List 画面

2. 「Add New Policy Based QoS」ボタンをクリックし、以下の画面を表示します。

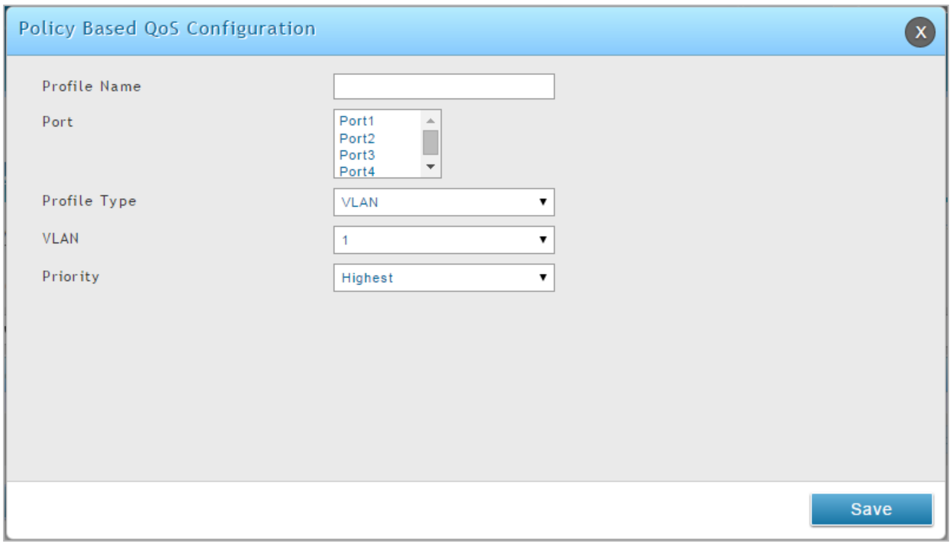


図 6-55　Policy Based QoS Configuration 画面

3. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
Profile Name	プロファイル名を指定します。
Port	ポートを選択します。「CTRL」を押しながら複数のポートを選択することができます。

項目	説明
Profile Type	本プロファイルの照合基準を選択します。 • VLAN • Destination MAC Address（送信先 MAC アドレス） • Source MAC Address（送信元 MAC アドレス） • Destination IP Address（送信先 IP アドレス） • Source IP Address（送信元 IP アドレス） • Destination TCP Port（送信先 TCP ポート） • Source TCP Port（送信元 TCP ポート） • Destination UDP Port（送信先 UDP ポート） • Source UDP Port（送信元 UDP ポート）
VLAN	「Profile Type」が「VLAN」の場合、定義済みの VLAN 番号を選択します。
MAC Address	「Profile Type」が「Destination MAC Address」または「Source MAC Address」の場合、MAC アドレスを入力します。
IP Address	「Profile Type」が「Destination IP Address」または「Source IP Address」の場合、IP アドレスを入力します。
L4 Port	「Profile Type」が「Source TCP Port」、「Destination TCP Port」、「Source UDP Port」または「Destination UDP Port」の場合、ポート番号を入力します。
Priority	QoS ルールの優先度を選択します。 • Highest（最高） • High（高） • Low（低） • Lowest（最低）

フローベースコントロールの設定

Network > QoS > QoS Policy > Flow Control メニュー

フローベースの QoS ポリシーは、特定のサービス用の帯域を制限します。これを変更するとポートに出力される定義済みサービスのトラフィックに影響します。

1. **Network > QoS > QoS Policy > Flow Control** の順にメニューをクリックし、以下の画面を表示します。

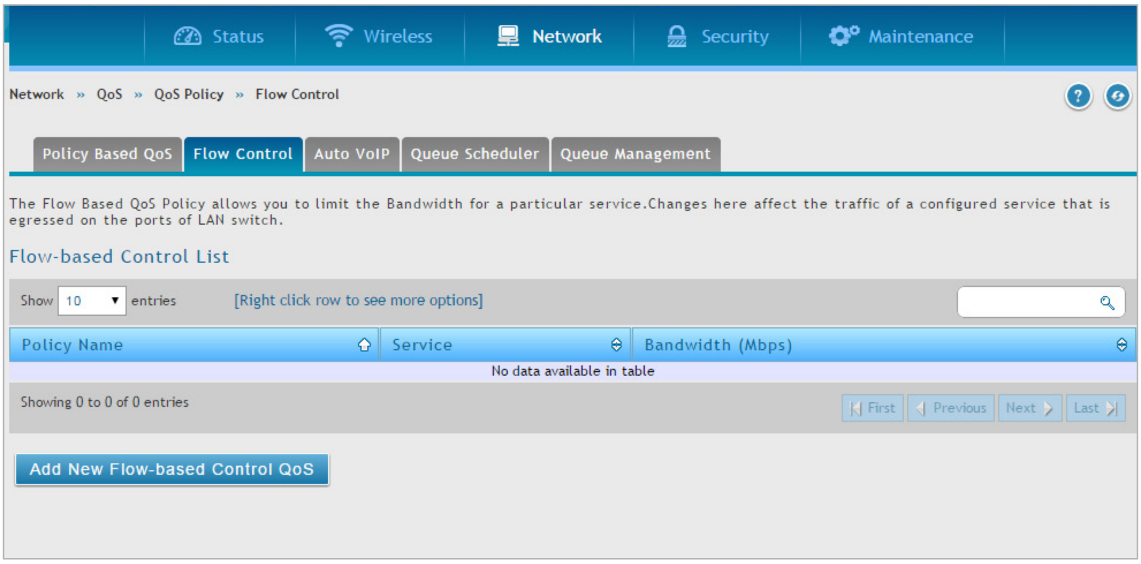


図 6-56　Flow-based Control List 画面

2. 「Add New Flow-based Control QoS」ボタンをクリックし、以下の画面を表示します。

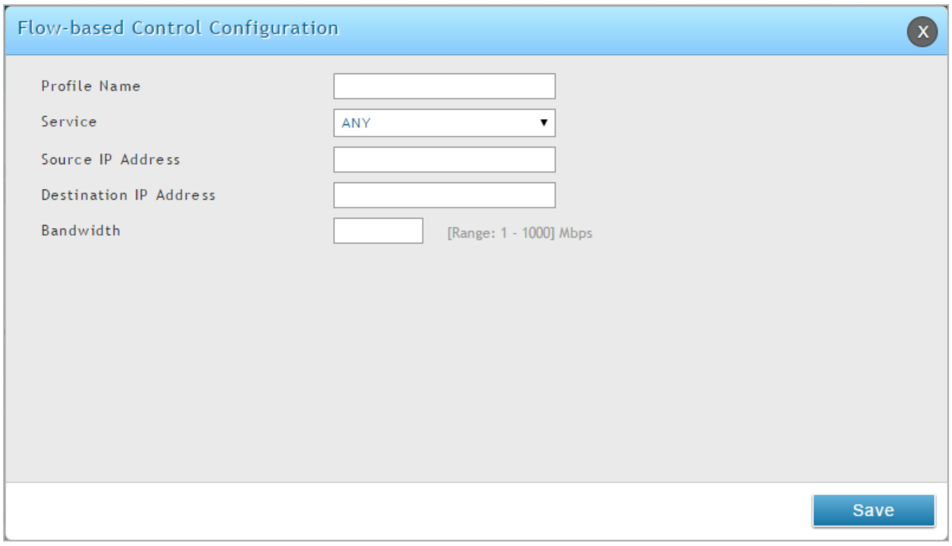


図 6-57　Flow-based Control Configuration 画面

3. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
Profile Name	プロファイル名を指定します。
Service	使用するサービスのタイプを選択します。 Any、aim、bgp、bootp_client、bootp_server、cu-seeme udp、cu-seeme:tcp、dns:udp、dns:tcp、finger、ftp、http、https、icmp、icq、imap2、imap3、irc、news、nfs、nntp、ping、pop3、pptp、rcmd、rea-audio、rexec、rlogin、rtelnet、rtsp:tcp、rtsp:udp、sftp、smtp、snmp:tcp、snmp:udp、snmp-traps:tcp、snmp-traps:udp、sql-net、ssh:tcp、ssh:udp、strmworks、tacacs、telnet、tftp、rip、ike、shttpd、ipsec-udp-encap、ident、vddolive、ssh、sip:tcp、sip:udp、または icmpv6
Source IP Address	送信元 IP アドレスを指定します。
Destination IP Address	送信先 IP アドレスを指定します。
Bandwidth	特定のサービスの帯域を制限します。

自動 VoIP QoS の設定

Network > QoS > QoS Policy > Auto VoIP メニュー

優先度の割り当てのために QoS ルールを有効にします。これを変更すると、LAN における SIP と H.323 トラフィックの優先度に影響します。

1. **Network > QoS > QoS Policy > Auto VoIP** の順にメニューをクリックし、以下の画面を表示します。

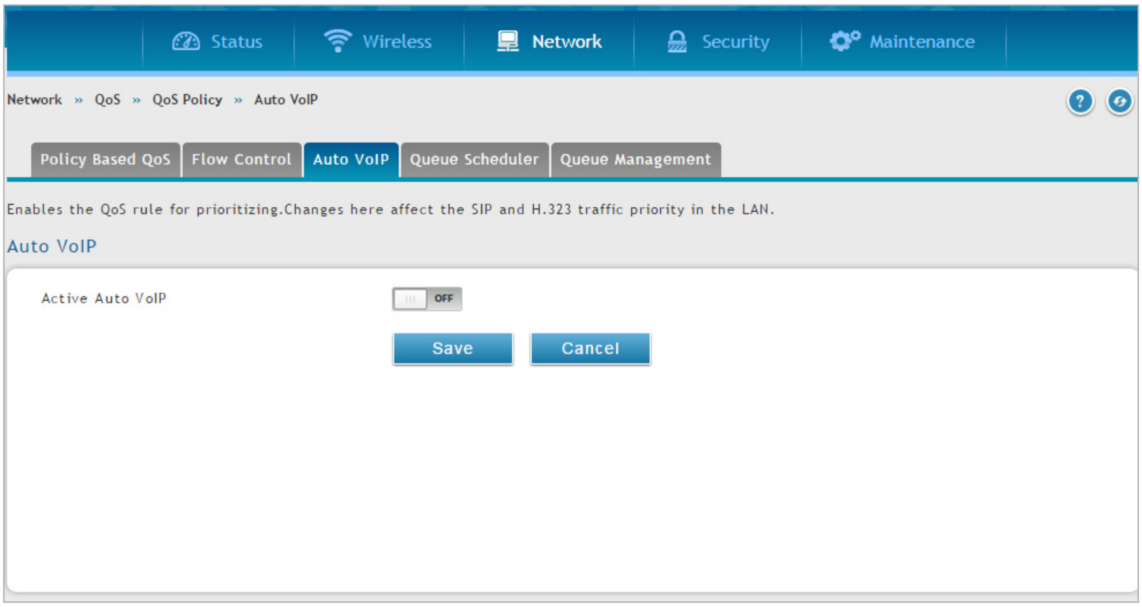


図 6-58　Auto VoIP 画面

2. 「Active Auto VoIP」を有効にして、「Save」ボタンをクリックします。

キュースケジューラの設定

Network > QoS > QoS Policy > Queue Scheduler メニュー

サポートしているアルゴリズムは「Strict」および「Weighted Round Robin」（重み付けラウンドロビン）のみです。デバイスは、ここで設定したアルゴリズムを使用してトラフィックを処理するようにプログラムされます。

1. **Network > QoS > QoS Policy > Queue Scheduler** タブの順にメニューをクリックし、以下の画面を表示します。

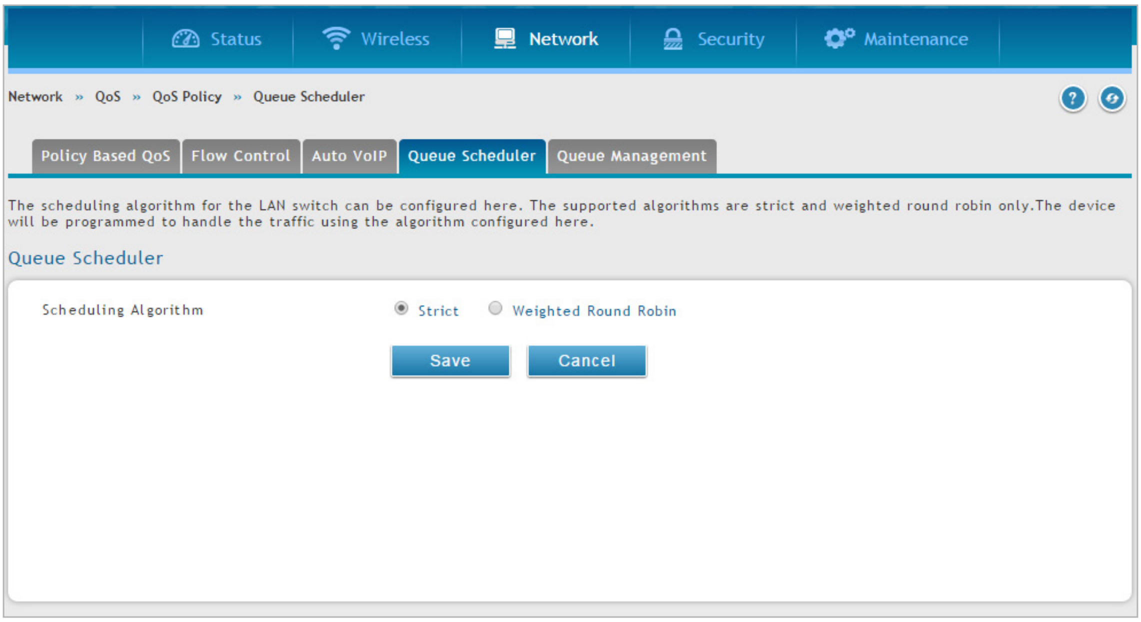


図 6-59　Queue Scheduler 画面

2. スケジューリングアルゴリズム（Strict または Weighted Round Robin）を選択して、「Save」ボタンをクリックします。

キュー管理

Network > QoS > QoS Policy > Queue Management メニュー

無線コントローラで使用される現在のキュー管理アルゴリズムを表示します。

1. **Network > QoS > Option QoS > Queue Management** の順にメニューをクリックし、以下の画面を表示します。

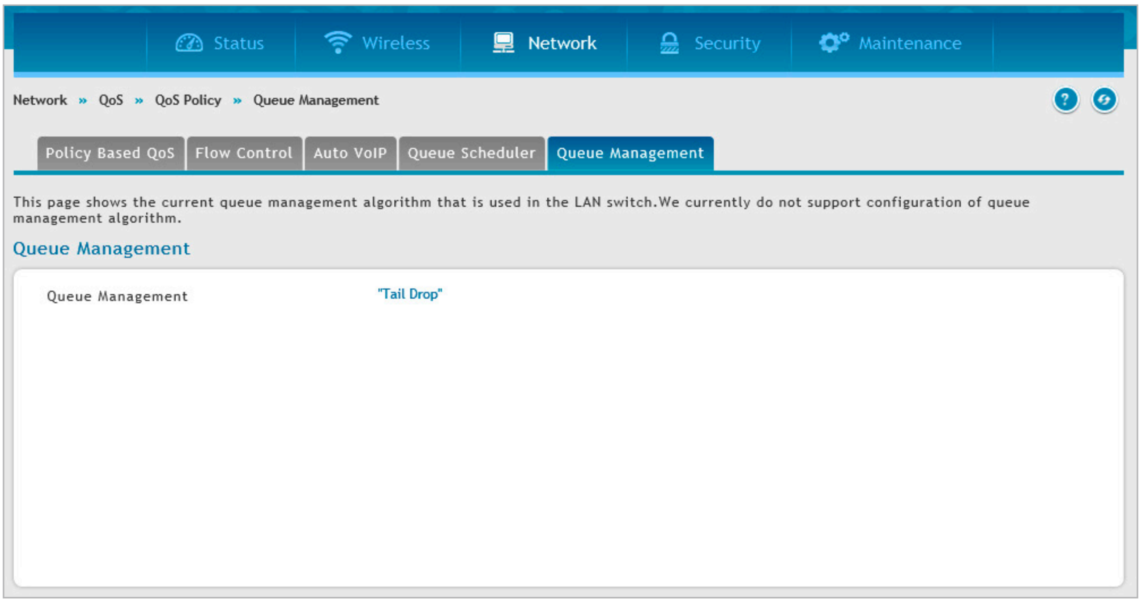


図 6-60　Queue Management 画面

使用する現在のキュー管理アルゴリズムを表示します。

注意　キュー管理アルゴリズムの設定は未サポートです。

CoS と DSCP マーキングの設定

Network > QoS > CoS DSCP Marking メニュー

DSCP への CoS のリマークは高度な QoS 設定です。これにより、パケットのレイヤ 2 の QoS フィールドがレイヤ 3 の QoS フィールドに変換され、上流ルータがパケットの DSCP フィールドセットに基づいて QoS 決定を行うことができます。DSCP への CoS リマークを有効化した後、特定の CoS 値に対して適切な DSCP 値を選択することができます。

1. **Network > QoS > CoS DSCP Marking** の順にメニューをクリックし、以下の画面を表示します。

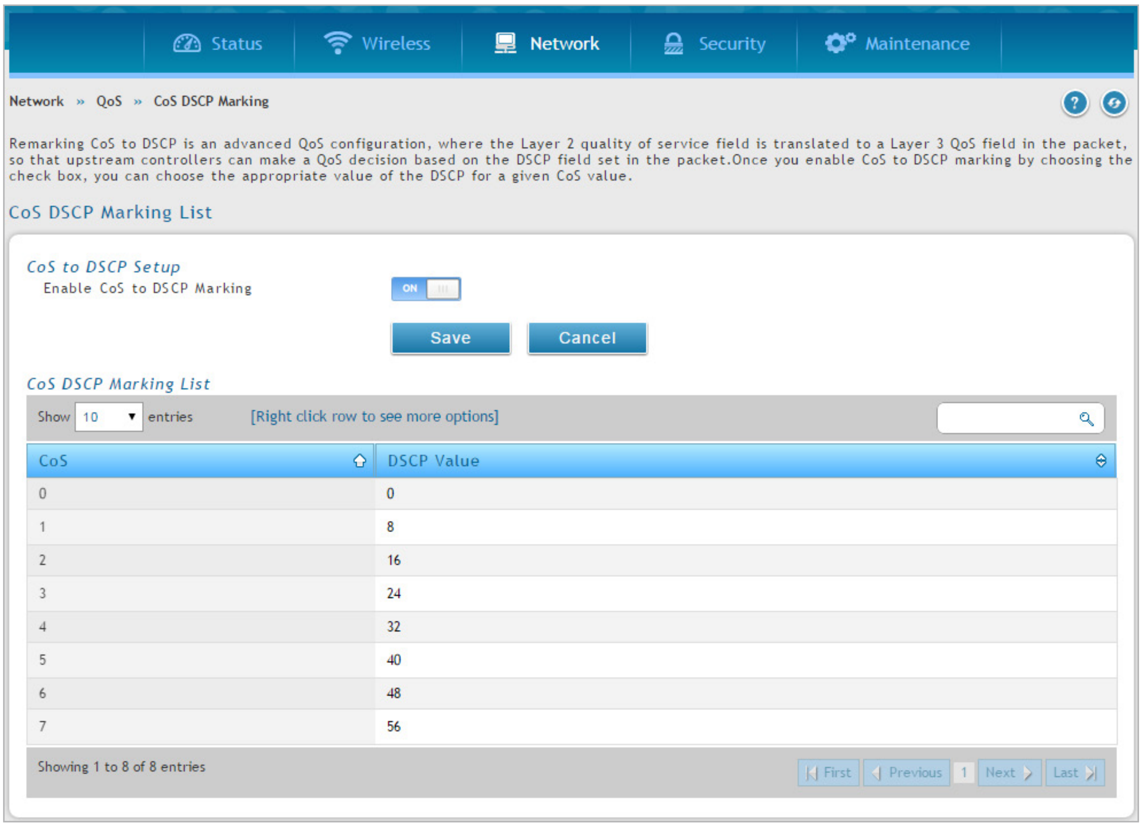


図 6-61　CoS DSCP Marking List 画面

2. 「Enable CoS and DSCP Marking」を「ON」にして、「Save」ボタンをクリックします。

3. 「CoS」で右クリックして、「Edit」を選択すると、以下の画面が表示されます。

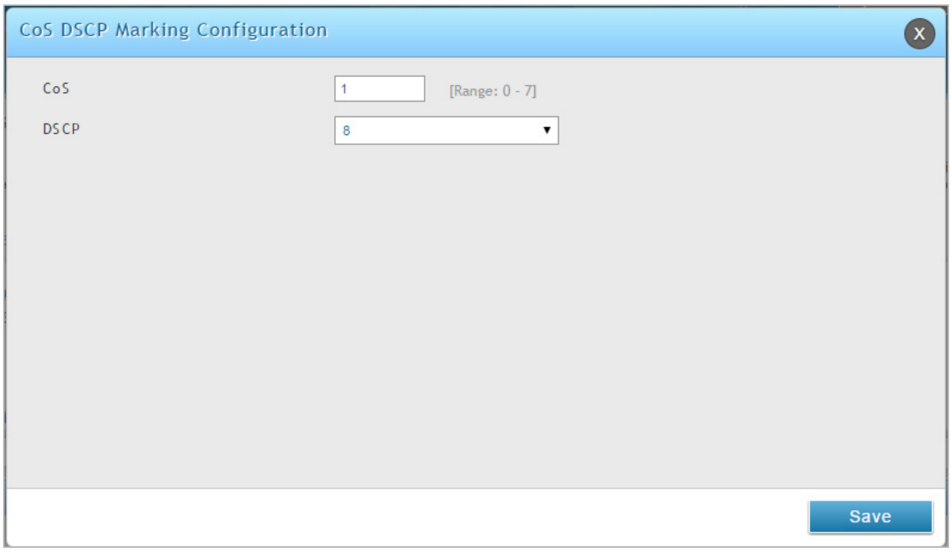


図 6-62　CoS DSCP Marking Configuration 画面

4. CoS と DSCP 間のマッピングの値を変更し、「Save」ボタンをクリックします。

第 7 章　ネットワークのセキュリティ設定

無線コントローラは、ご使用のネットワークの安全を確保するための多くの機能をサポートしています。本章では以下の一般的に使用されるセキュリティ機能について説明します。

設定項目	説明
クライアントの管理	データベースにある無線クライアントの追加、編集、削除、または参照を行います。
グループの管理	ユーザグループ、ブラウザポリシー、IP ポリシーの追加、編集、または削除を行います。
ユーザ管理	ユーザの追加、編集、または削除を行います。
ゲストアカウントの使用の管理	ゲストアカウントの追加、編集、または削除を行います。
ログインプロファイル	ユーザログイン画面をカスタマイズします。
外部認証	認証サーバを設定します。
RADIUS アカウンティンググローバル設定	RADIUS アカウンティングサーバのグローバル設定、表示を行います。設定 SSID においてアカウンティングをグローバルに有効 / 無効に指定するために、「Accounting Mode」を使用します。
Facebook Wi-Fi 設定	Facebook WiFi は「facebook.com」を使用した認証用キャプティブポータルメカニズムです。
E-mail 設定	コントローラからキャプティブポータルユーザへ E メールを送信する SMTP サーバの設定を行います。
証明書設定	CA 証明書、自己署名証明書の追加を行います。
クライアントのブロック	コントローラがブロックするクライアントを設定します。
OAuth サーバ設定	OAuth サーバの設定を行います。

注意　ネットワークの概念と専門用語を理解している熟練したユーザのみ本章の手順を実行してください。

クライアントの管理

「MAC Authentication」ページを使用して、「MAC Authentication」データベースにある無線クライアントを参照できます。データベースには無線クライアントの MAC アドレスと名前があります。データベースは、RADIUS サーバからクライアントの記述名の取得や MAC 認証の実行のために使用されます。さらにクライアントの追加、編集、削除もできます。

既知の無線クライアントの参照 / 追加

Security > Authentication > User Database > MAC Authentication メニュー

■ 既知の無線クライアントの参照と追加

1. Security > Authentication > User Database > MAC Authentication の順にメニューをクリックし、以下の画面を表示します。

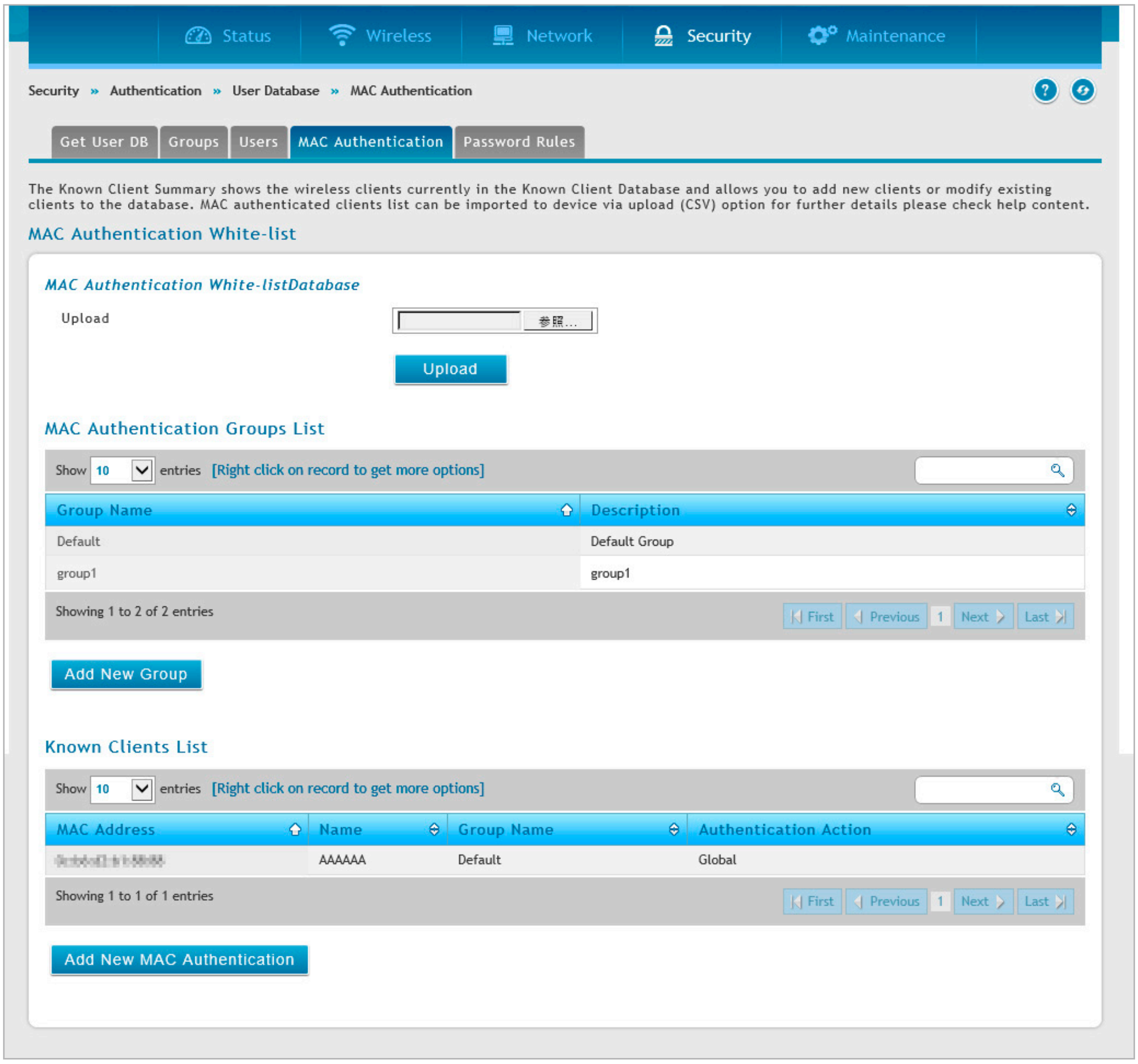


図 7-1　MAC Authentication White-List 画面

「MAC Authentication」データベースにある無線クライアントのリストを表示します。

MAC 認証は、クライアントの MAC アドレスがホワイトリストまたはブラックリストにある場合に、クライアントのネットワークへのアクセスを許可または拒否する機能です。MAC 認証はネットワークレベルで有効にされます。また、ネットワーク設定は、MAC アドレスがローカルデータベース、または、RADIUS サーバで検索されるかどうかを定義します。
「Upload」で CSV ファイル形式での MAC 認証ホワイトリストをアップロードできます。「MAC アドレス」「名前」の二つの項目を記載したファイルで有効です。 "MAC Address","Name" の様に「"」で項目を括り「,」で区別します。

2. 「Add New MAC Authentication」ボタンをクリックし、以下の画面を表示します

図 7-2　MAC Authentication Configuration 画面

3. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
MAC Address	既知のクライアントの MAC アドレスを入力します。
Name	既知のクライアントの名前を入力します。他のクライアントとの区別ができる識別名を設定してください。
MAC Authentication Group	MAC アドレスのグループを選択します。
Authentication Action	認証のアクションを表示します。

■ MAC アドレスグループの追加

1. **Security > Authentication > User Database > MAC Authentication** の順にメニューをクリックします。
2. 「Add New Group」をクリックし、以下の画面を表示します。

図 7-1　MAC Authentication Group Configuration 画面

3. 以下の項目を入力します。
   - Group Name - MAC アドレスのグループ名を入力します。
   - Description - グループの説明を入力します。
4. Save をクリックします。

■ クライアントの編集 / 削除

クライアントを追加後に設定を変更する必要がある場合、編集または削除することができます。

クライアントの編集

1. **Security > Authentication > User Database > MAC Authentication** の順にメニューをクリックします。
2. 「MAC Authentication White-list」で、クライアントを右クリックし、「Edit」を選択します。
3. 設定を変更し、「Save」ボタンをクリックします。

クライアントの削除

1. **Security > Authentication > User Database > MAC Authentication** の順にメニューをクリックします。
2. 「MAC Authentication List」で、クライアントを右クリックし、「Delete」を選択します。
   クライアントのすべてを削除する場合は、「Select All」をチェック後、「Delete」をクリックします。

グループの管理

ユーザグループは同じ特権を共有するユーザの集まりです。以下のセクションではユーザグループを追加する方法について説明します。ユーザグループの追加後に、ログインポリシー、ブラウザのポリシー、および IP ごとのポリシーを設定することができます。また、変更が必要なユーザグループの編集や、不要なユーザグループの削除ができます。

ユーザグループ

Security > Authentication > User Database > Groups メニュー

ユーザグループの追加する場合に、以下の項目を割り当てます。

- ユーザグループを識別する名前
- オプションのユーザグループの説明文
- 少なくとも 1 つの権限（または、「ユーザタイプ」）
- アイドルタイムアウト値

ユーザグループの定義後に、「ユーザ管理」の手順を使用して、ユーザにグループを設定することができます。

ユーザグループの追加

1. Security > Authentication > User Database > Groups の順にメニューをクリックし、以下の画面を表示します。

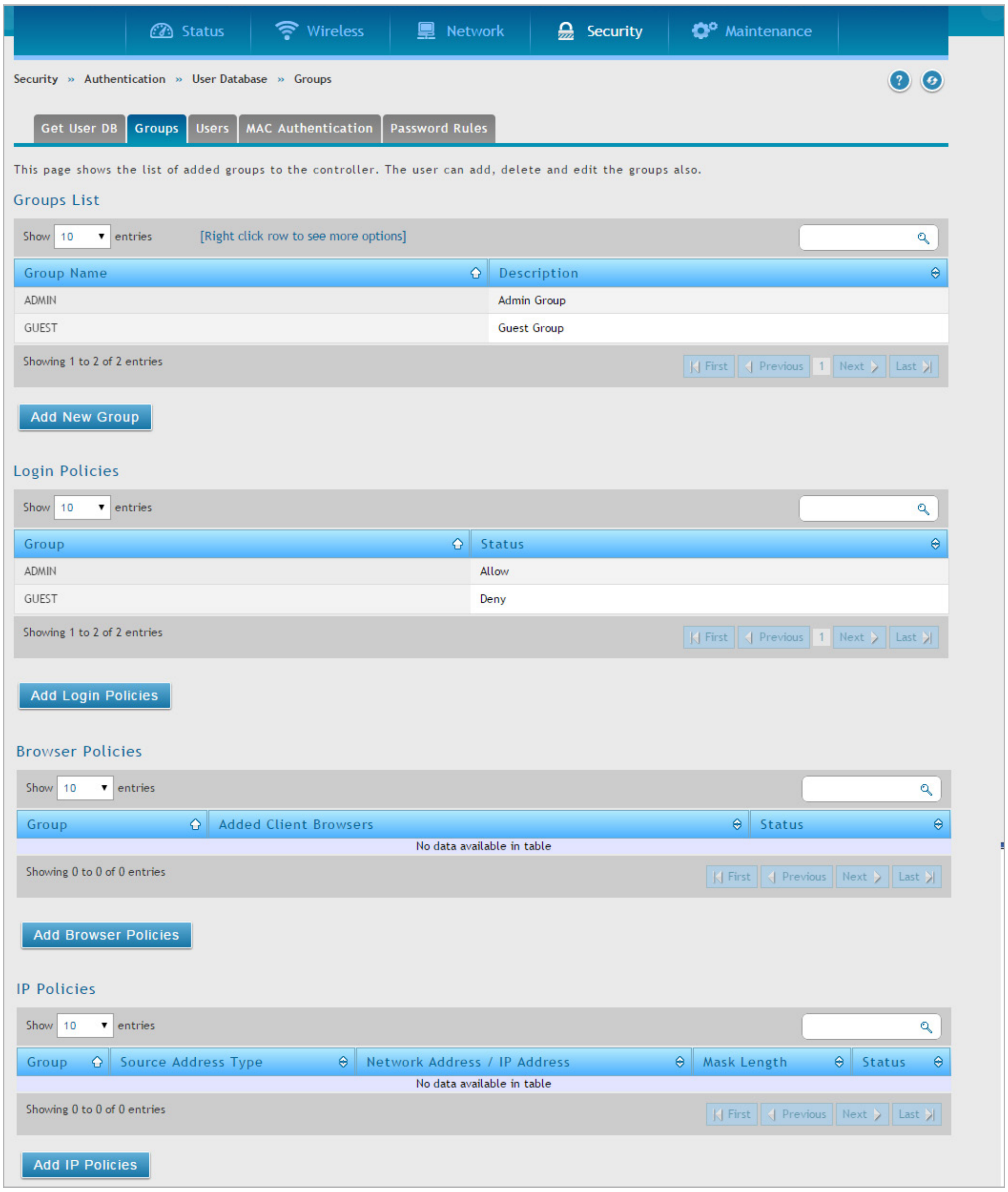


図 7-2　　Group List 画面

2.　「Add New Group」ボタンをクリックすると、以下の画面が表示されます。

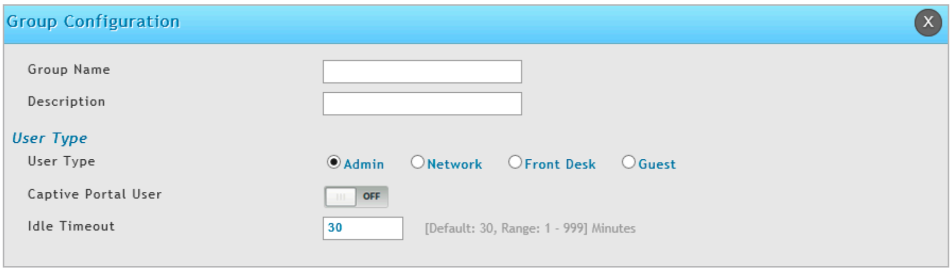


図 7-3　　Group Configuration 画面

3.　フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
Group Name	グループの固有の名称を入力します。名前は、追加する可能性のある他のグループとこのグループを簡単に識別できるようにする必要があります。
Description	本ユーザグループの説明文を入力します。
User Type	
User Type	• Admin - このグループのすべてのユーザに管理者権限を付与します。初期値では、1 つの Admin ユーザが用意されています。キャプティブポータルユーザを有効化すると、キャプティブポータル認証経由でのインターネット / ネットワークへの接続が可能になります。 • Network - 追加のオプションが有効になります。キャプティブポータルユーザを有効化すると、キャプティブポータル認証経由でのインターネット / ネットワークへの接続が可能になります。 • Front Desk - このグループのユーザは、ホットスポットからインターネット / ネットワークにアクセスできる一時的ユーザを作成する権限を持ちます。 • Guest - このグループのユーザは、参照するだけの権限を持ちます。ユーザはデバイスを設定することができません。
Captive Portal User	Captive Portal 権限を持つグループのユーザは、Captive Portal 認証を通じてインターネット / ネットワークにアクセスする権限を持ちます。
Session Timeout	Captive Portal ユーザを有効化した場合、本項目が指定可能になります。キャプティブポータルグループのセッションタイムアウトを指定します。ユーザは指定時間後に期限切れとなります。
Idle Timeout	ユーザグループ内のユーザが Web 管理セッションを自動的にログアウトするまでの無通信の時間を入力します。「0」はログアウトしないことを意味します。

ユーザグループの編集

ユーザグループの編集を行います。例えば、ユーザグループの権限やアイドルタイムアウトを変更する場合に使用します。

1.　**Security > Authentication > User Database > Groups** の順にメニューをクリックします。

2.　編集するユーザグループを右クリックし、「Edit」ボタンを選択すると、以下の画面が表示されます。

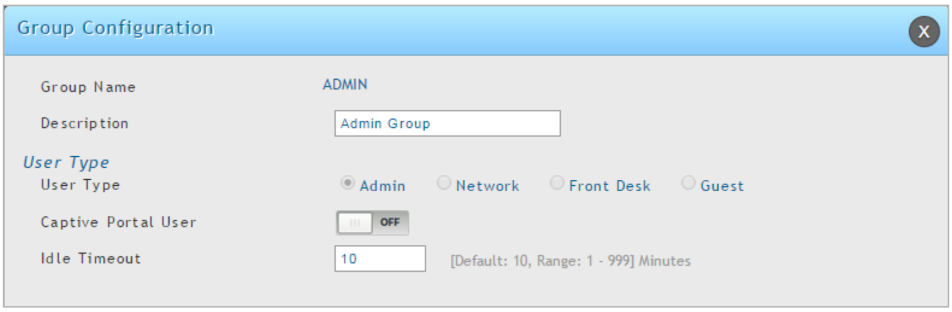


図 7-4　　Group Configuration 画面

3.　フィールドを編集し、「Save」ボタンをクリックします。

ユーザグループの削除

必要としないユーザグループを削除します。ユーザグループを削除する前に、グループ内のすべてのユーザを削除する必要があります。（「クライアントの編集 / 削除」参照）

注意　ユーザグループを削除する前に、注意のメッセージは表示されません。そのため、削除する前に、ユーザグループを必要としないことを必ず確認してください。

1.　**Security > Authentication > User Database > Groups** の順にメニューをクリックします。

2.　削除するユーザグループを右クリックし、「Delete」を選択します。
すべてのグループを削除する場合は「Select All」をチェックし、「Delete」を選択します。

ログインポリシー

Security > Authentication > User Database > Groups メニュー

ログインポリシーの設定

ユーザグループに対して、Web 管理インタフェースへのログインアクセスを許可または拒否することができます。

1. **Security > Authentication > User Database > Groups** の順にメニューをクリックし、以下の画面を表示します。

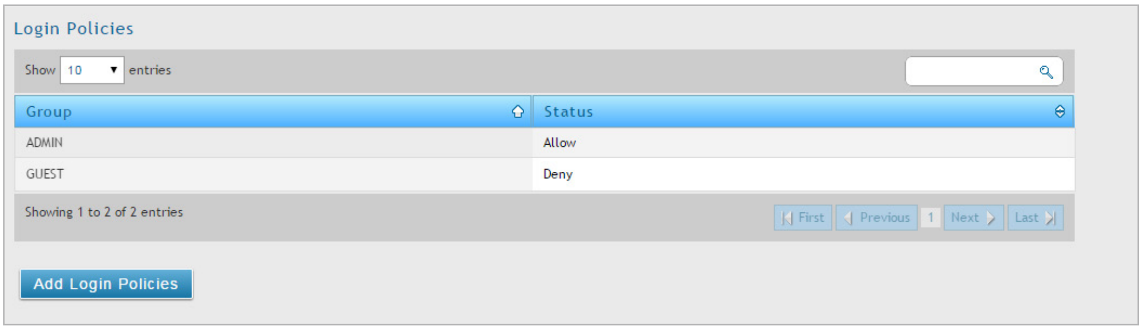


図 7-5　Login Policies 画面

2. 「Add Login Policies」ボタンをクリックすると、以下の画面が表示されます。

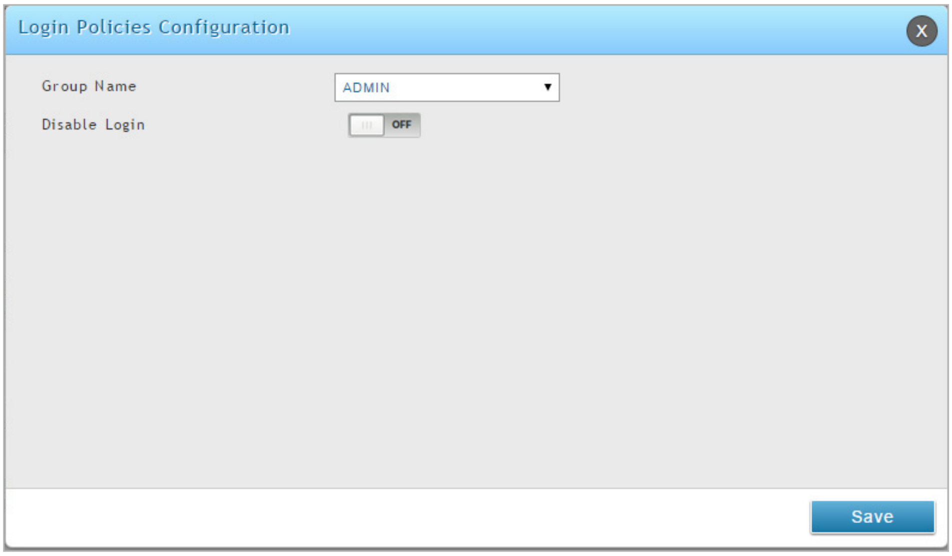


図 7-6　Login Policies Configuration 画面

3. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
Group Name	グループ名を選択します。
Disable Login	選択したグループ内の全ユーザに対して Web 管理インタフェースへのログインアクセスを許可または拒否します。 • ON - ログインアクセスを無効にします。 • OFF - ログインアクセスを有効にします。

ログインポリシーの削除

削除するエントリを右クリックし、「Delete」を選択します。すべてのエントリを削除するために、「Select All」をチェックし、その後「Delete」を選択します。

ブラウザポリシー

Security > Authentication > User Database > Groups メニュー

ブラウザポリシーの設定

ユーザグループにブラウザの詳細なポリシーを設定します。ユーザグループ内のユーザが、特定の Web ブラウザを使用することにより、無線コントローラの Web 管理インタフェースにログインすることを許可または拒否することができます。

1. **Security > Authentication > User Database > Groups** の順にメニューをクリックし、以下の画面を表示します。

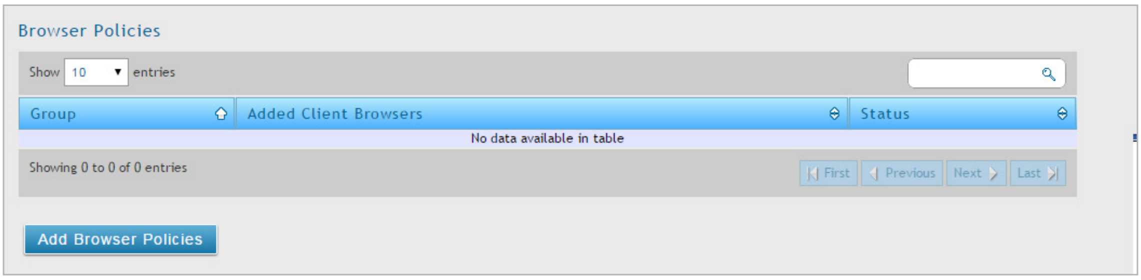


図 7-7　　Browser Policies 画面

2. 「Add Browser Policies」ボタンをクリックし、以下の画面を表示します。

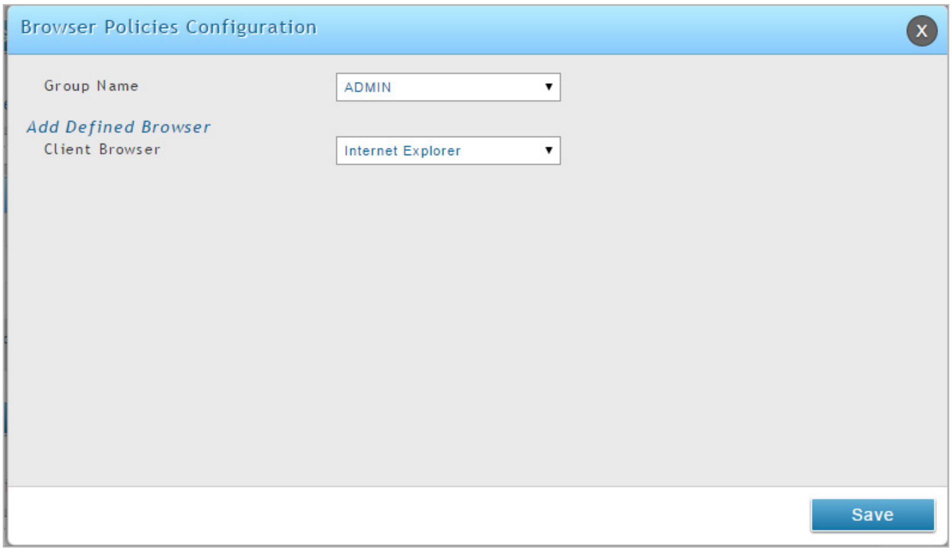


図 7-8　　Browser Policies Configuration 画面

3. 「Add Defined Browser」の「Client Browser」プルダウンメニューからブラウザを選択して、「Save」ボタンをクリックします。選択したブラウザがリストに表示されます。

項目	説明
Group Name	プルダウンメニューからグループ名を選択します。
Client Browser	プルダウンメニューから Web ブラウザを選択します。

ブラウザポリシーには、以下のメニューがあります。ブラウザポリシーリストで右クリックして、選択することができます。

項目	説明
Select All	すべてのグループを選択します。
Allow	ブラウザを許可します。
Deny	ブラウザを拒否します。
Delete Browsers	ブラウザを削除します。
Add Browsers	ブラウザを追加します。

IP ポリシー

Security > Authentication > User Database > Groups メニュー

IP ポリシーの設定

ユーザグループに IP の詳細なポリシーを設定します。この手順を使用して、ユーザグループ内のユーザが、特定のネットワークまたは IP アドレスから無線コントローラの Web 管理インタフェースにログインすることを許可または拒否することができます。

1. **Security > Authentication > User Database > Groups** の順にメニューをクリックし、以下の画面を表示します。

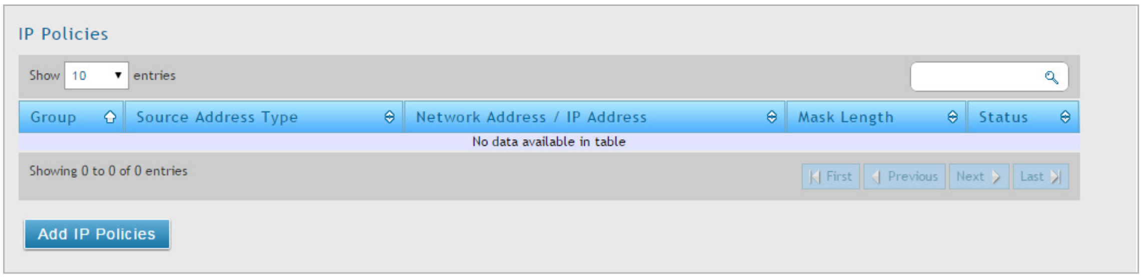


図 7-9　IP Policies 画面

2. 「Add IP Policies」ボタンをクリックし、以下の画面を表示します。

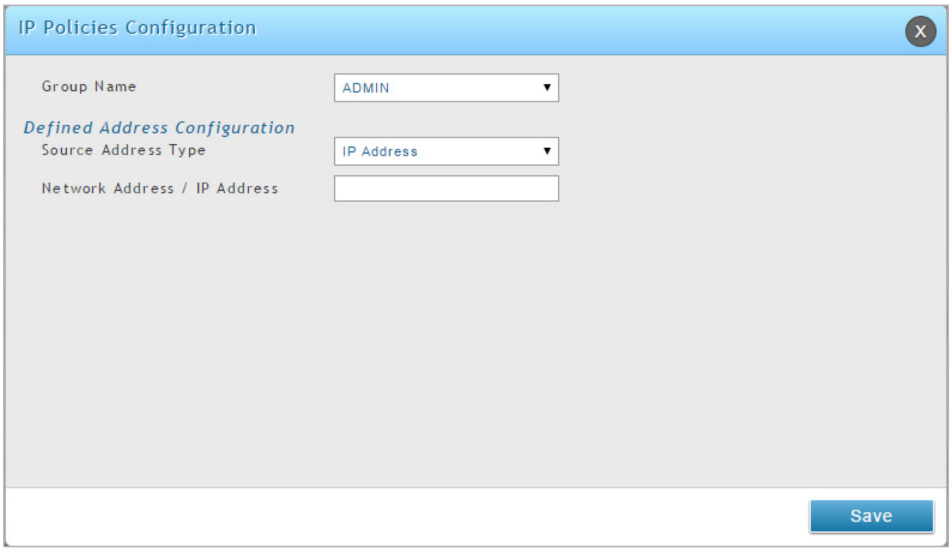


図 7-10　IP Policies Configuration 画面

3. フィールドにデータを入力し、「Save」ボタンをクリックします。定義したアドレスがリストに表示されます。

項目	説明
Group Name	プルダウンメニューからグループ名を選択します。
Source Address Type	ソースアドレスのタイプを選択します。 • IP Address - 特定の IP アドレスを指定します。 • IP Network - IP ネットワークを指定します。
Network Address / IP Address	ネットワークまたは IP アドレスを入力します。
Mask Length	サブネットマスク長を入力します。

IP ポリシーには、以下のメニューがあります。IP ポリシーリストで右クリックして、選択することができます。

項目	説明
Select All	すべてのグループを選択します。
Allow	IP ポリシーを許可します。
Deny	IP ポリシーを拒否します。
Delete IP Policies	IP ポリシーを削除します。
Add IP Policy	IP ポリシーに IP アドレス / ネットワークを追加します。

ユーザ管理

ユーザグループの追加後に、ユーザをユーザグループに追加できます。個別にユーザを追加するほか、CSV（comma-separated values）フォーマットのファイルからインポートすることもできます。
ユーザの追加後に、変更が必要とされる場合は、編集することもできます。また、不要なユーザを削除できます。

手動によるユーザの追加

Security > Authentication > User Database > Users メニュー

ユーザを追加する方法の 1 つがユーザを個別に追加する方法です。

1. **Security > Authentication > User Database > Users** の順にメニューをクリックし、以下の画面を表示します。

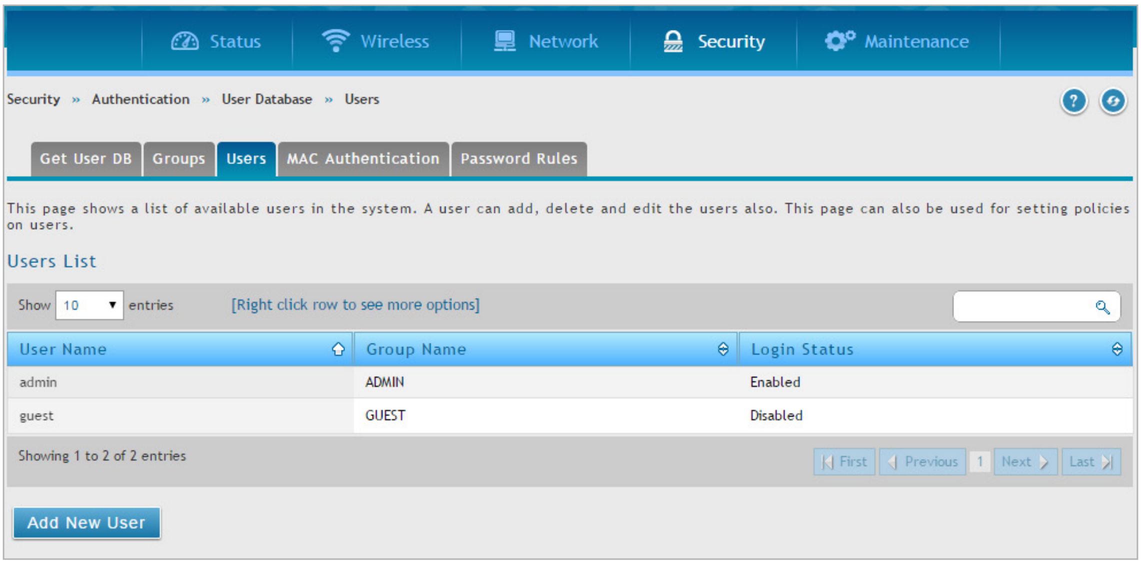


図 7-11　Users List 画面

2. 「Add New User」ボタンをクリックすると、以下の画面が表示されます。

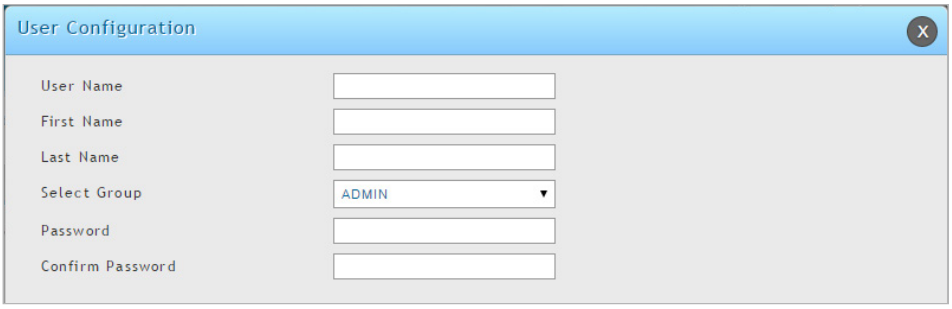


図 7-12　User Configuration 画面

3. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
User Name	本ユーザの固有の名称を入力します。名前は、追加する可能性のある他のユーザとこのユーザを簡単に識別できるようにする必要があります。
First Name	ユーザの名前を入力します。
Last Name	ユーザの名字を入力します。
Select Group	本ユーザが所属するキャプティブポータルグループを選択します。
Enable Password Change	本項目は「Select Group」で Captive Portal グループを選択した場合にのみ表示されます。「ON」を選択すると、ユーザがパスワードの変更を行うことができるようになります。
Password	ユーザが Web 管理インタフェースにアクセスするためにログインプロンプトで指定するべきログインパスワード（大文字、小文字の区別あり）を入力します。セキュリティのために、入力したパスワード文字は、ドット「.」でマスクされます。
Confirm Password	確認のために上記「Password」フィールドに入力したものと同じパスワード（大文字、小文字の区別あり）を入力します。セキュリティのために、入力したパスワード文字は、ドット「.」でマスクされます。
Type of Login	本項目は「Select Group」で Captive Portal グループを選択した場合にのみ表示されます。「Multi Login」を選択すると、ユーザが同一のユーザ名 / パスワードを使用して、複数のデバイスから同時にログインすることができます。
Forced Login	本項目は「Select Group」で Captive Portal グループを選択し、「Single Login」を選択した場合にのみ表示されます。「ON」にすると強制ログインが有効になります。
Max Login Users	本項目は「Select Group」で Captive Portal グループを選択し、「Multi Login」を選択した場合にのみ表示されます。同時にログインできるユーザの最大数を設定します。

項目	説明

ユーザのインポート

Security > Authentication > User Database > Get User DB メニュー

CSV 形式のファイルからユーザをインポートすることで、ユーザを個別に追加するよりも速く登録できます。

1. **Security > Authentication > User Database > Get User DB** の順にメニューをクリックし、以下の画面を表示します。

図 7-13　Get User DB 画面

2. 「ファイルを選択」ボタンをクリックします。

3. CSV ファイルの場所に移動して、ファイルを選択し、「開く」ボタンをクリックします。

4. 「Upload」ボタンをクリックします。

ユーザの編集

Security > Authentication > User Database > Users メニュー

ユーザのログインパスワードやアイドルタイムアウトの変更など、ユーザ設定を編集します。

ユーザの編集

1. **Security > Authentication > User Database > Users** の順にメニューをクリックし、「Users List」画面を表示します。

2. 編集するユーザを右クリックし、「Edit」を選択して、以下の画面を表示します。

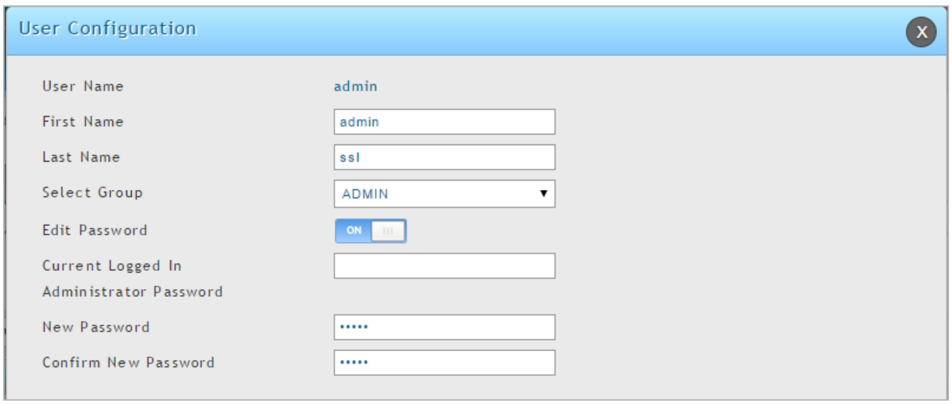


図 7-14　User Configuration 画面

3. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
User Name	本ユーザの固有の名称を表示します。
First Name	ユーザの名前を入力します。
Last Name	ユーザの名字を入力します。
Select Group	本ユーザが所属するグループを選択します。
Edit Password	Web 管理インタフェースにログインするためにユーザが使用するパスワードを変更するには、「ON」を選択します。
Current Logged In Administrator Password	現在のログインパスワード（大文字、小文字の区別あり）を入力します。セキュリティのために、入力したパスワード文字はドット「.」でマスクされます。

項目	説明
New Password	に新しいログインパスワード（大文字、小文字の区別あり）を入力します。セキュリティのために、入力したパスワード文字はドット「.」でマスクされます。新しいパスワードを「付録 A 基本計画のワークシート」に記録します。
Confirm Password	確認のために、再度新しいパスワードを入力します。

ユーザの削除

Security > Authentication > User Database > Users メニュー

不要なユーザを削除します。

注意 ユーザを削除する前に、注意のメッセージは表示されません。そのため、削除する前に、ユーザが不要であることを必ず確認してください。

ユーザの削除

1. **Security > Authentication > User Database > Users** の順にメニューをクリックし、「Users List」画面を表示します。
2. 削除するユーザを右クリックし、「Delete」を選択します。すべてのユーザを削除するために、「Select All」をチェックして、「Delete」を選択します。

パスワードのルール

Security > Authentication > User Database > Password Rules メニュー

パスワードの 長さと文字をルール化して、Captive Portal ユーザ認証のセキュリティを強化します。

1. **Security > Authentication > User Database > Password Rules** の順にメニューをクリックし、以下の画面を表示します。

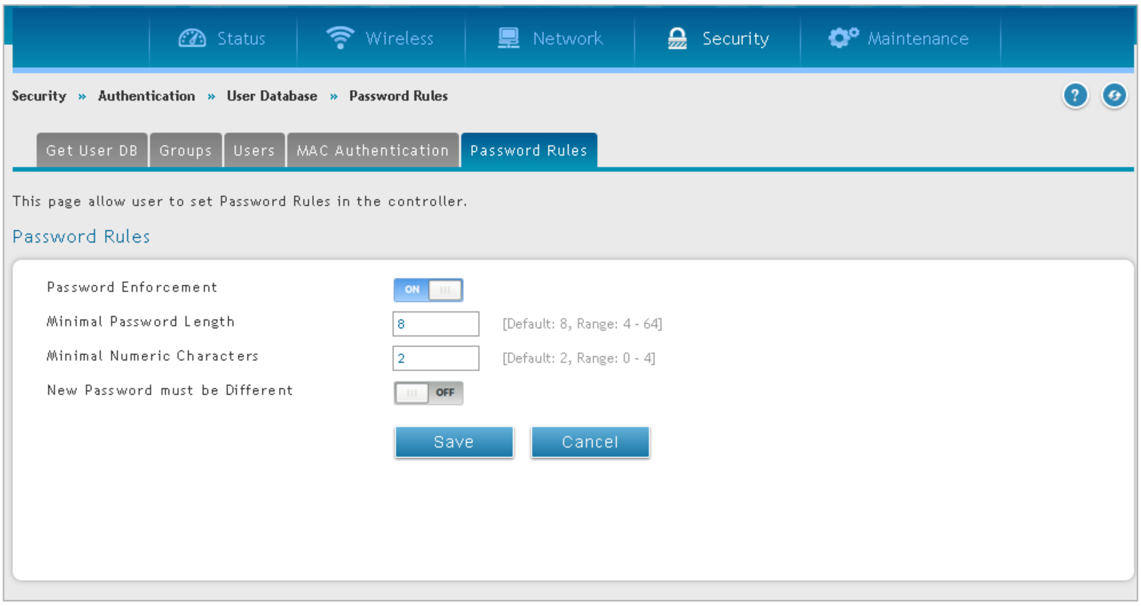


図 7-15　Password Rules 画面

2. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
Password Enforcement	「ON」に切り替えて、続くパスワードのルールを有効にします。
Minimal Password Length	必要とする最小の文字数を入力します。
Minimal Numeric Characters	ユーザがパスワードに使用しなければならない数字の最小の数を入力します。
New Password must be Different	設定した新しいパスワードが、元のパスワードと異なる必要があるかどうか指定します。

ゲストアカウントの使用の管理

ゲストアカウントは無線コントローラによって生成されます。ゲストのインターネット使用を制御するためには、相対的なビリングプロファイルを設定します。

ビリングプロファイル設定には、以下の通り 4 つの手順があります。

図 7-16

- アカウントの作成 : 一時的なアカウントは、ローカルのデータベースのフロントアカウントによって生成されます。
- アカウントのアクティブ化 : 一時的なアカウントがアクティブ化され、有効になります。
- アカウントの喪失 : 一時的なアカウントは、利用期間または従量の期限に到達します。
- アカウントの終了 : 一時的なアカウントは、利用期間 / 従量に到達するかどうかにかかわらず終了し、ローカルのデータベースから削除されます。

設定する値により、ビリングプロファイルにも様々なタイプがあります。最も一般的なビリングプロファイルには、以下の 5 つのタイプがあります。

1. 一時的なアカウントの利用時間は、持続時間によって制限されます。アカウントには期限があり、アカウントが存在している間は有効です。

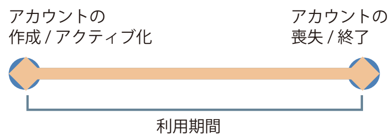
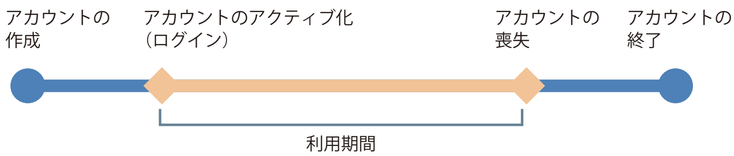


図 7-17

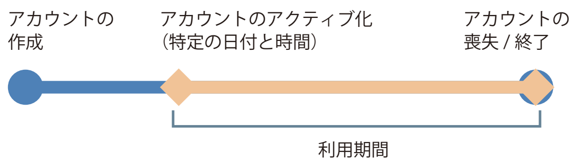
このビリングプロファイルは、ホテルで使用するというシナリオに適しています。一時的なアカウントがカスタマのチェックイン時に作成され、有効になります。

2. 一時的なアカウントの利用時間は、アカウントの存続時間によって制限されます。アカウントには期限があり、最初のログインの間、有効になります。



このビリングプロファイルは、カフェや空港などで使用するというシナリオに適しています。カスタマは、最初のログインから計算した時間内で、無線インターネットサービスを使用できます。

3. 一時的なアカウントは特定の日時に有効です。アカウントには期限があります。



このビリングプロファイルは、プレスカンファレンスで使用するというシナリオに適しています。必要に応じて、主催者がイベント前にアカウントを生成し、 事前に関係者に情報を引き渡します。一時的なアカウントは特定の日時から有効になります。

4. 一時的なアカウントは使用時間が制限されます。アカウントには、利用終了までの期限はありません。

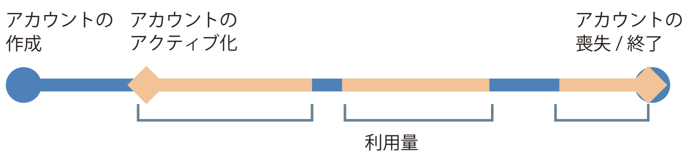


図 7-18

このビリングプロファイルは、ホットスポットで使用するというシナリオに適しています。サービスプロバイダは、利用時間に基づいて無線サービスに課金します。このアカウントでは、複数のデバイスが同時にログインすることができます。

5.　一時的なアカウントは使用トラフィックも制限されます。アカウントには、利用終了までの期限はありません。

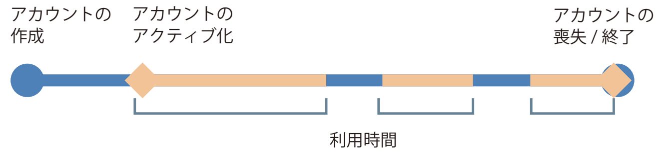


図 7-19

このビリングプロファイルは、ホットスポットで使用するというシナリオに適しています。サービスプロバイダは、使用量に基づいて無線サービスに課金をします。

ビリングプロファイル

Security > Authentication > Billing Profile メニュー

1.　Security > Authentication > Billing Profile の順にメニューをクリックし、以下の画面を表示します。

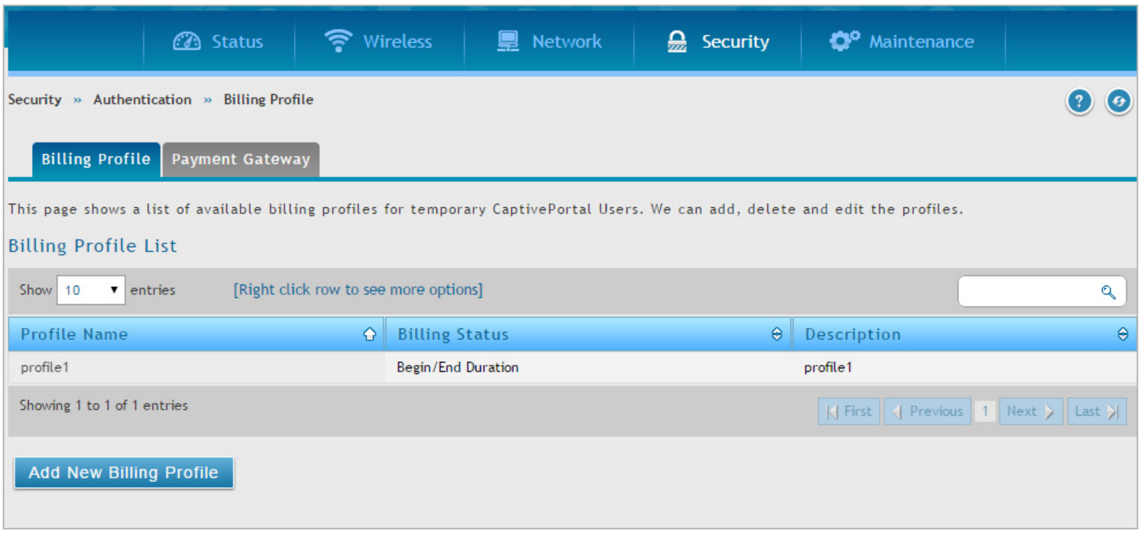


図 7-20　Billing Profile List 画面

2.　「Add New Billing Profile」ボタンをクリックし、以下の画面を表示します。

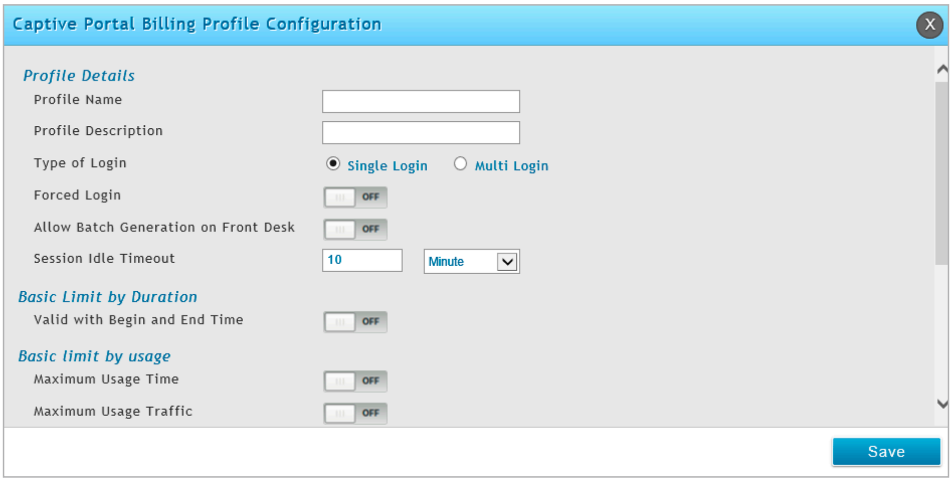


図 7-21　Captive Portal Billing Profile Configuration 画面

3.　フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
Profile Details	
Profile Name	各プロファイルは、識別用のプロファイル名を持ちます。
Profile Description	プロファイルの説明文です。
Type of Login	ログインのタイプを以下から選択します。 ・Single Login - 複数のユーザがこのプロファイルで生成される同じキャプティブポータルのログイン証明書を使用して、同時にログインすることはできません。 ・Multi Login - 複数のユーザがこのプロファイルで生成される同じキャプティブポータルのログイン証明書を使用して、同時にログインできるようになります。
Forced Login	「Single Login」を選択した場合に、強制ログインを「ON」または「OFF」にします。
Max Login Users	「Multi Login」を選択した場合に、同時にログインできるユーザの最大数を設定します。
Allow Batch Generation on Front Desk	本オプションを有効にすると、フロントデスクユーザは、ワンクリックで、一時的なキャプティブポータルユーザを一括して生成できます。
Session Idle Timeout	このプロファイルに生成された CP ユーザのアイドルタイムを指定します。
Basic Limit by Duration	
Valid with Begin and End time	Duration ベースの制限を有効または無効にします。
Valid Begin	「Valid with Begin and End Time」を有効にすると、ユーザのアクセスを期間によって制限する以下の 3 つタイプのいずれかを指定することができます。 ・Start while Account Created - ユーザが作成済みである場合にアカウントをアクティブにします。 ・Start While Account Login - 証明書を使用して、ユーザの最初のログイン時にアカウントをアクティブ化します。 ・Begin From - この日付からアカウントをアクティブ化します。
Start while Account Created	「Start while Account Created」を選択した場合、フィールドに値を入力し、単位（Hours または Days）を選択し、利用時間を設定します。
Start While Account Login	「Start While Account Login」を選択した場合、フィールドに値を入力し、単位（Hours または Days）を選択し、利用時間を設定します。
Begin From	「Begin From」を選択した場合、アカウントが有効になる日時を選択します。
Allow Front Desk to Modify Duration	「Valid with Begin and End time」を有効にする場合、このオプションを「ON」にすることで、フロントデスクユーザは持続時間の制限を編集できます。
Basic Limit by usage	
Maximum Usage Time	アカウントの期限が切れる前に、ユーザがログインを維持できる最大時間を有効または無効にします。「ON」を指定した場合、フィールドに値を入力し、単位（Hours または Days）を選択し、利用時間を設定します。
Maximum Usage Traffic	アカウントの期限が切れる前に、ユーザが使用できる最大トラフィックを有効または無効にします。「ON」を指定した場合、フィールドに値を入力し、単位（MB または GB）を選択します。内向きトラフィックだけが帯域幅の利用について考慮されるものとします。
Show Alert Message on Login Page while Rest of Usage Time / Traffic under	利用時間 / トラフィック量が希望した制限に到達した時に、警告メッセージを取得するために、Hours/MB に値を入力します。「0」は、警告メッセージが必要でないことを意味します。
Allow Front Desk to Modify Usage	「Maximum Usage Time」または「Maximum Usage Traffic」を有効にする場合、このオプションを「ON」にすることで、フロントデスクユーザは利用制限を編集できます。
Ticket Printing Options	
Header	「ON」にしてヘッダを指定します。
Customized Note	「ON」にしてカスタム項目を指定します。
Time Stamp	「ON」にしてタイムスタンプを指定します。
Footer	「ON」にしてフッターを指定します。
Ticket Logo	「ON」にしてチケットロゴを指定します。「Add」をクリックすると画像を追加できます。
Unit Price	
Set Price	値段を指定します。「ON」にして値段を指定します。
Price	「Set Price」を有効にすると表示されます。値段を指定します。
Monetary Unit	金銭の単位を指定します。

ペイメントゲートウェイ

Security > Authentication > Billing Profile > Payment Gateway メニュー

ペイメントゲートウェイは、支払いと振替がインターネット経由で行われることを承認する電子商取引アプリケーションサービスプロバイダのサービスです。ペイメントゲートウェイ設定を行うと、ユーザは「Captive Portal」から無線サービスをオンラインで購入できます。

1. **Security > Authentication > Billing Profile > Payment Gateway** の順にメニューをクリックし、以下の画面を表示します。

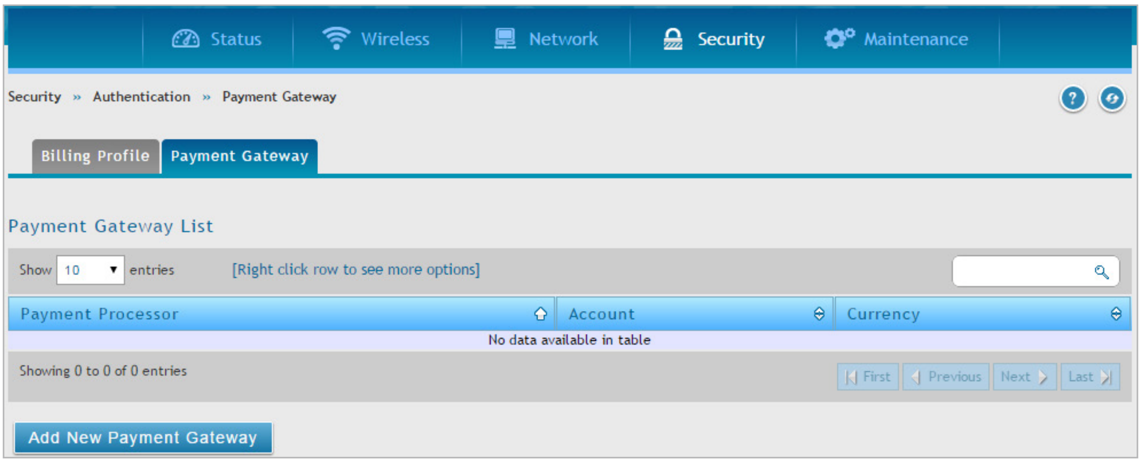


図 7-22　Payment Gateway List 画面

2. 「Add New Payment Gateway」ボタンをクリックし、以下の画面を表示します。

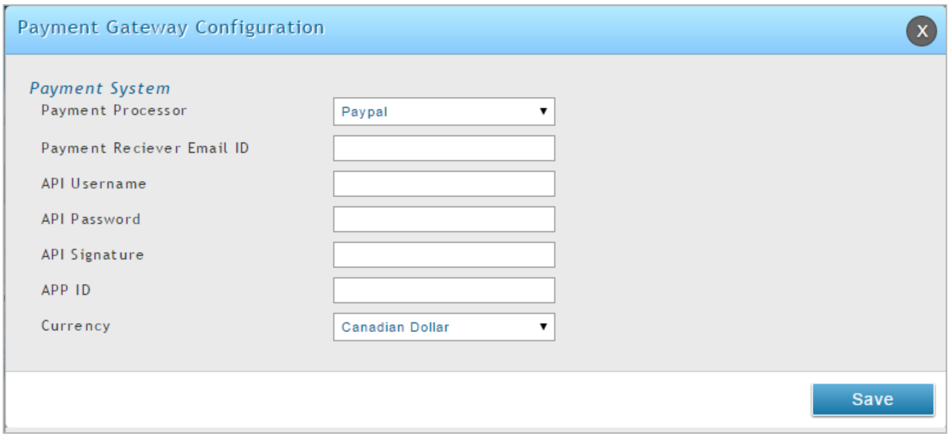


図 7-23　Payment Gateway Configuration 画面

3. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
Authorize.net を選択した場合：	
Login ID	ログイン ID を指定します。
Transaction Key	決済鍵を指定します。
SHA2 Hash	SHA2 Hash を指定します。
Transaction Server	決済サーバを「Live」「Test」から指定します。
Transaction Mode	決済モードを「Live」「Test」から指定します。
Currency	支払い画面の単位を選択します。
Paypal または Paypal Test を選択した場合：	
Payment Receiver Email ID	ペイパルの受信する支払いに使用されるメールアカウントを指定します。
API Username	ペイパルプレミア / ビジネス /Web サイトペイメントプロアカウントの API ユーザ名を指定します。
API Password	ペイパルアカウントの API パスワードを指定します。
API Signature	ペイパルプレミア / ビジネス /Web サイトペイメントプロアカウントの API 署名を指定します。
APP ID	ペイパルが提供する APP ID を指定します。
Currency	支払い画面の単位を選択します。
SecurePay を選択した場合：	
Merchant ID	SecurePay から提供される Merchant ID を 5-7 文字で入力します。
AVS Mode	このゲートウェイアカウントに適用する AVS ルールの種類を指定します。
Use Tokenization	トークナイゼーションを有効 / 無効に設定します。トークナイゼーションはカード番号を保存する方式で、マーチャントがカードの機密データを取り扱えないようにします。カード番号はストレージ参照（トークン）に置き換えられます。

項目	説明
Gateway Alias	ゲートウェイに割り当てるゲートウェイ名を入力します。CRM 内の複数のゲートウェイアカウントを識別する際に役に立ちます。
Currency	支払い画面の単位を選択します。
WorldPay を選択した場合：	
Installation ID	WorldPay ペイメントサービスからマーチャントに対し一意に割り当てられた参照番号を入力します。
Authorization Password	WorldPay インストール ID と一緒に受領したパスワードを入力します。
Currency	支払い画面の単位を選択します。

今後エージェントにより表示、設定項目が変わることもあります。詳しくはエージェントのサポートをご確認ください。

ログインプロファイル

無線クライアントがアクセスポイントの SSID または VLAN に接続する場合、ユーザはログイン画面を参照します。「Login Profile and SLA」画面では、特定の文字や画像で画面のカスタマイズをすることができます。 無線コントローラは、複数のログインおよび SLA ページをサポートします。SSID または VLAN に対して個別にログインページまたは SLA を関連付けます。

キャプティブポータルのログインページのカスタマイズ

Security> Authentication> Login Profiles> Login Profiles メニュー

1. **Security > Authentication > Login Profiles > Login Profiles** の順にメニューをクリックし、以下の画面を表示します。

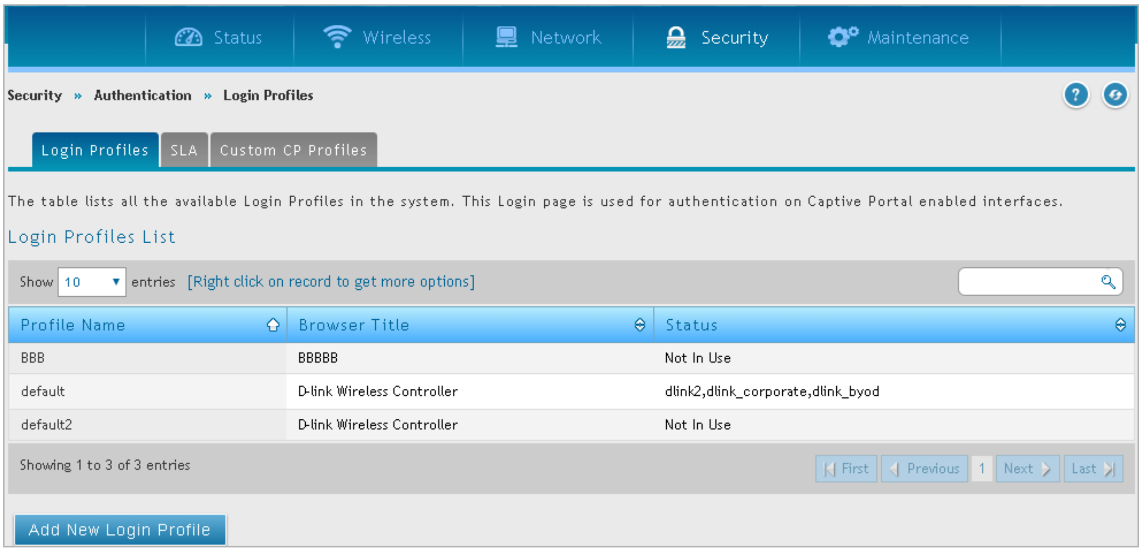


図 7-24　 Login Profiles List 画面

2. 「Add New Login Profile」ボタンをクリックし、以下の画面を表示します。

図 7-25　Login Profile Configuration 画面

3. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
General Details	
Profile Name	キャプティブポータルプロファイルの名前を入力します。名前は、追加する可能性のある他のプロファイルとこのプロファイルを簡単に識別できるようにする必要があります。
Browser Title	キャプティブポータルセッション中にブラウザのタイトルに表示される文字列を入力します。
Background	キャプティブポータルセッション中に表示されたログインページが、画像またはカラーを表示するかどうかを選択します。 • Image - ページの背景として画像を表示します。 • Color - ページの背景色を設定します。
Page Background Image	「Background」で「Image」を設定した場合、**Add > ファイル選択**の順にクリックして、画像ファイルをアップロードします。画像を選択して「開く」をクリックし、「Upload」ボタンをクリックします。画像の最大サイズは 50KBytes です。
Background Image settings	「Background」で「Image」を設定した場合、画像の表示方法を指定します。 • Default - 画像を垂直・水平方向に繰り返して、ログイン画面全体に表示します。 • Simple - 画像をログイン画面にそのまま表示します。 • Strech - 画像をログイン画面全体に引き延ばして表示します。 • Vertical repeat - 画像を垂直方向に繰り返して、ログイン画面に表示します。 • Horizontal repeat - 画像を水平方向に繰り返して、ログイン画面に表示します。
Page Background Color	「Background」で「Color」を設定した場合、キャプティブポータルセッション中に表示されるページの背景色をプルダウンメニューから選択します。
Custom Color	「Page Background Color」で「Custom」を選択した場合、HTML のカラーコードを入力します。
Minimal Page for Mobile Devices	「ON」にするとページをモバイルデバイス用（必要最小表示）に設定します。
Header Details	
Background	キャプティブポータルセッション中に表示されたログインページが、画像またはカラーを表示するかどうかを選択します。 • Image - ページのヘッダとして画像を表示します。 • Color - ヘッダの背景色を設定します。

項目	説明
Header Background Image	「Background」で「Image」を設定した場合、**Add > ファイル選択**の順にクリックして、画像ファイルをアップロードします。画像を選択して「開く」をクリックし、「Upload」ボタンをクリックします。画像の最大サイズは 50KBytes です。
Header Background Color	「Background」で「Color」を設定した場合、ヘッダのカラーをプルダウンメニューから選択します。 「Header Background Color」で「Custom」を選択した場合、「Custom Color」に HTML のカラーコードを入力します。
Custom Color	「Header Background Color」に「Custom」を選択した場合、HTML のカラーコードを入力します。
Header Caption	キャプティブポータルセッション中にログインページのヘッダに表示されるテキストを入力します。
Caption Font	ヘッダテキストのフォントを選択します。
Font Size	ヘッダテキストのフォントサイズを選択します。
Font Color	ヘッダテキストのフォント色を選択します。
Login Details	
Login Section Title	（オプション）キャプティブポータルセッションへのログイン時に表示されるログインボックスのタイトルに表示されるテキストを入力します。
Welcome Message	（オプション）キャプティブセッションへのログインに成功した場合に表示されるウエルカムメッセージを入力します。
Error Message	（オプション）キャプティブセッションへのログインに失敗した場合に表示されるエラーメッセージを入力します。
Footer Details	
Change Footer Content	ログインページのフッターコンテンツへの変更を有効または無効にします。
Footer Content	「Change Footer Content」をチェックした場合、フッターに表示されるテキストを入力します。
Footer Font Color	「Change Footer Content」がチェックした場合、フッターに表示される色を入力します。
External Payment Gateway	
Enable External Payment Gateway	外部のペイメントゲートウェイおよびログインページからのオンライン無線サービスの購入を有効または無効にします。
Session Title 1	ユーザがキャプティブポータルセッションへのログイン時に、オンライン購入のログインボックスのタイトルに表示されるテキストを入力します。
Message	ユーザがキャプティブポータルセッションへのログイン時に、オンライン購入ログインボックスに表示されるテキストを入力します。
Session Title2	オンライン購入が完了した時に、メッセージボックスのタイトルに表示されるテキストを入力します。
Success Message	オンライン購入が完了した時に、メッセージボックスに表示されるテキストを入力します
Session Title3	オンライン購入に失敗した時に、メッセージボックスのタイトルに表示されるテキストを入力します。
Failure Message	オンライン購入が失敗した時に、メッセージボックスに表示されるテキストを入力します。
Enable Billing Profile	
ログインページに表示されるビリングプロファイルを選択します。テーブルには「Unit Price」を設定したビリングプロファイルのみ表示されます。状態を「ON」に切り替えて、ビリングプロファイルを有効にします。	
Service Disclaimer Text	無線サービスを選択および購入する前に表示されるサービスに関する免責事項のテキストを入力します。
Payment Server	支払いアカウントおよびその支払い代行サーバを選択します。

キャプティブポータルの SLA のカスタマイズ

Security > Authentication > Login Profiles > SLA メニュー

1. **Security > Authentication > Login Profiles > SLA** の順にメニューをクリックし、以下の画面を表示します。

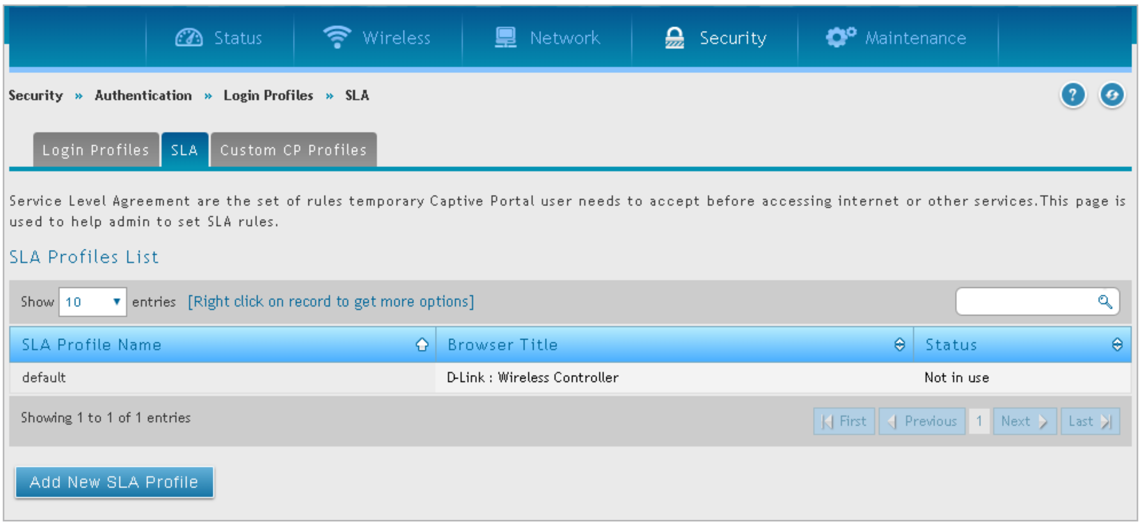


図 7-26　SLA Profiles List 画面

2. 「Add New SLA Profile」ボタンをクリックし、以下の画面を表示します。

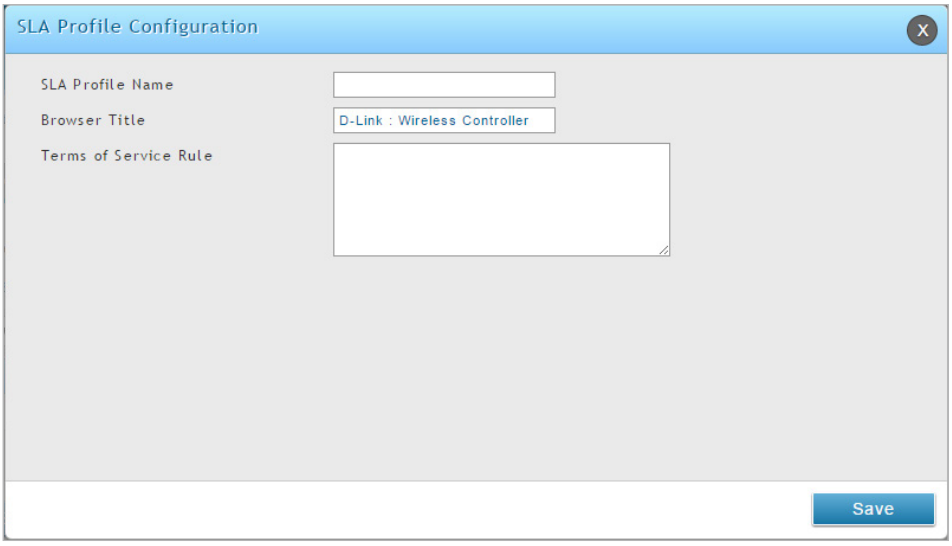


図 7-27　SLA Profile Configuration 画面

3. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
SLA Profile Name	SLA プロファイルの名称を入力します。名前は、追加する可能性のある他の SLA プロファイルとこのプロファイルを簡単に識別できるようにする必要があります。
Browser Title	キャプティブポータルセッション中にブラウザのタイトルに表示される文字列を入力します。
Terms of Service Rule	インターネットへのアクセス前に、一時または SLA タイプのキャプティブポータルユーザが受け入れる必要のあるルールセットを指定します。

カスタムキャプティブポータルプロファイルのアップロード

Security > Authentication > Login Profiles > Custom CP Profiles メニュー

1. **Security > Authentication > Login Profiles > Custom CP Profiles** の順にメニューをクリックし、以下の画面を表示します。

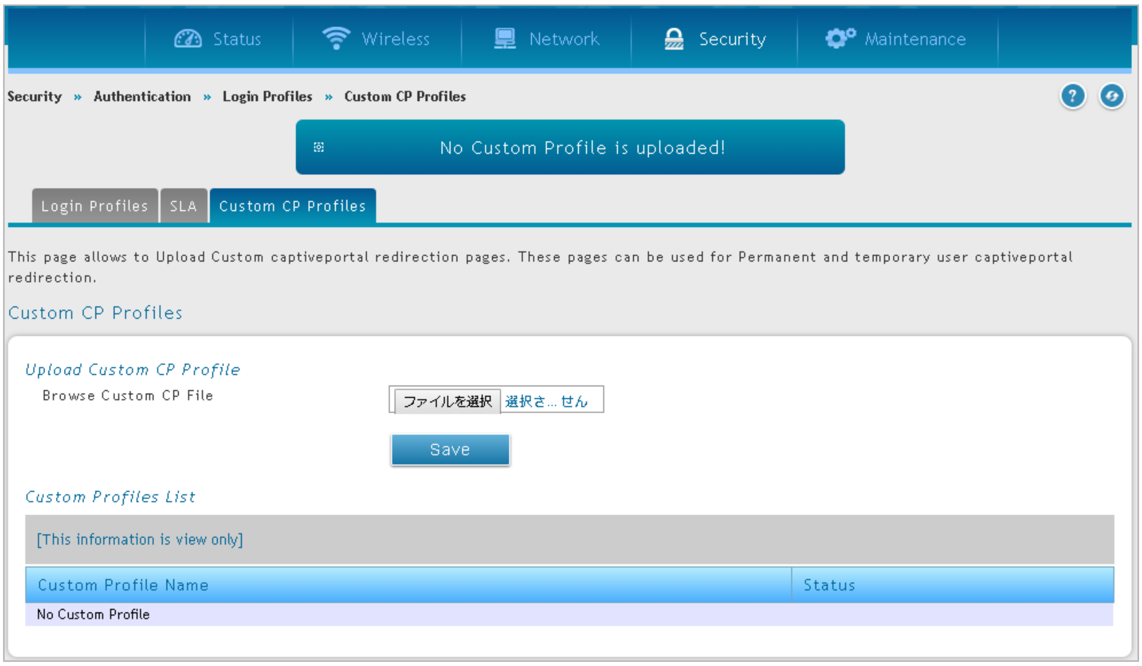


図 7-28　Custom CP Profiles 画面

2. 「Browse Custom CP File」でカスタムプロファイルページの「.tgz」ファイルを参照し、アップロードします。

3. 「Save」ボタンをクリックします。

外部認証

コントローラ上のローカルユーザデータベースは、通常、GUI または CLI への管理アクセスを許可するために使用されます。外部認証サーバは、一般的により安全であり、無線アクセスポイントの接続の許可、IPSec エンドポイントの認証、さらに VLAN 上のキャプティブポータルを通じたアクセスの許可を行うために使用されます。

本セクションでは、コントローラで利用可能な認証サーバと設定の必要条件について説明します。すべての場合において、設定したサーバへの接続性を検証するために「Server Checking」ボタンが使用されます。

RADIUS サーバの設定

Security > Authentication > External Auth Server > RADIUS Server メニュー

無線セキュリティのエンタープライズモードは、WPA、WPA2、WPA3 セキュリティに RADIUS サーバを使用します。RADIUS サーバは、RADIUS 認証を使用するプロファイルで有効なアクセスポイントに対して、無線クライアントの接続を認証するために、コントローラによって設定され、アクセスされる必要があります。

- Authentication Server IP Address がサーバを識別するために必要です。コントローラがプライマリサーバに到達できない場合に必要に応じてセカンダリ RADIUS サーバが冗長性を提供します。
- Authentication Port - RADIUS サーバ接続のためのポートです 。
- Secret - このコントローラが、指定した RADIUS サーバへのログインを許可される共有秘密を入力します。このキーは RADIUS サーバの秘密鍵に一致する必要があります。
- 「Timeout」および「Retries」フィールドはプライマリに到達できない場合にセカンダリに移動するため、またはサーバとの通信が不能である場合に RADIUS 認証の試行を停止するために使用されます。

RADIUS サーバの設定

1. **Security > Authentication > External Auth Server > RADIUS Server** の順にメニューをクリックし、以下の画面を表示します。

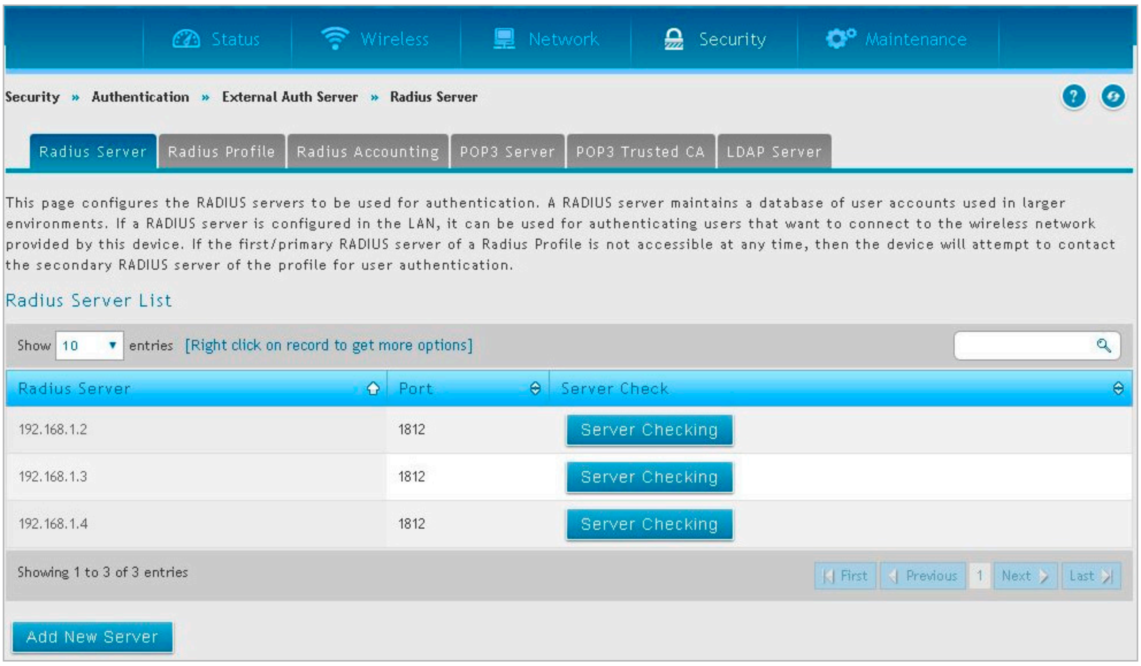


図 7-29　Radius Server 画面

2. 「Radius Server List」で、Radius サーバを右クリックし、「Edit」を選択します。

3. 設定を変更し、「Save」ボタンをクリックします。

項目	説明
Radius Server	RADIUS 認証サーバの IP アドレスを指定します。
Port	RADIUS 認証サーバのポートを指定します。
Secret	デバイスが定義済みの RADIUS サーバにログインするための秘密鍵を指定します。これは RADIUS アカウンティングサーバの秘密鍵に一致する必要があります。

RADIUS プロファイルの設定

Security > Authentication > External Auth Server > RADIUS Profile メニュー

RADIUS プロファイルの設定を行います。

1. **Security > Authentication > External Auth Server > RADIUS Profile** の順にメニューをクリックし、以下の画面を表示します。

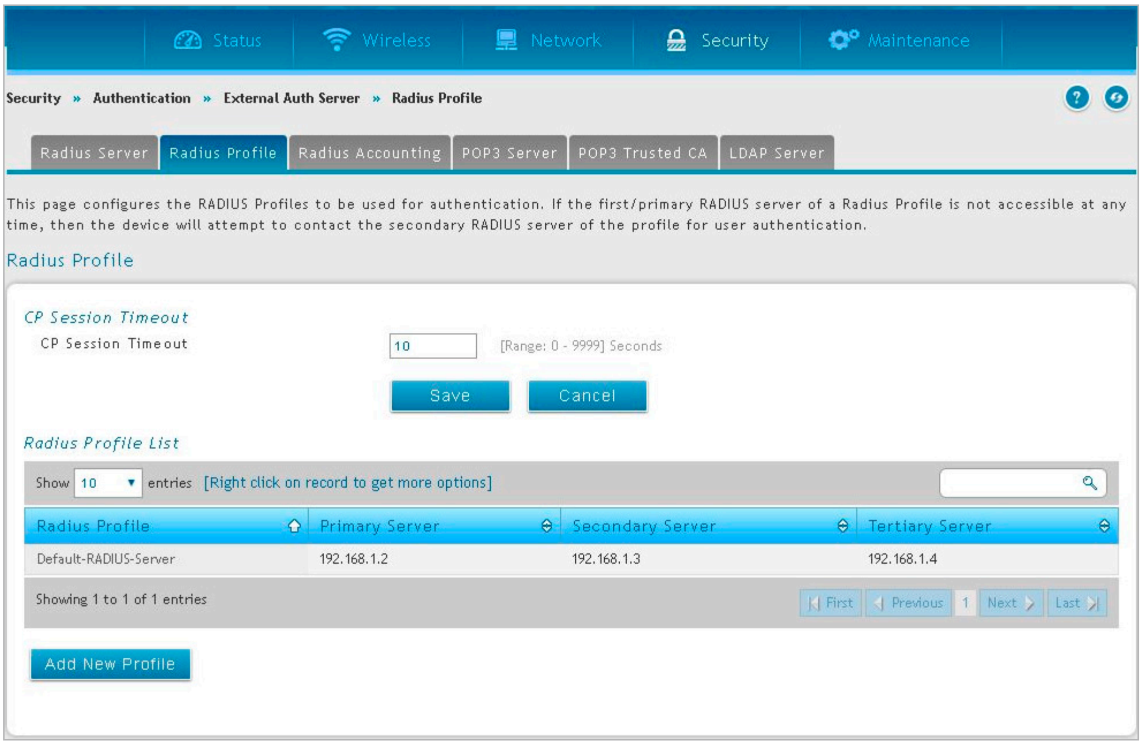


図 7-30　Radius Profile 画面

2. 「Add New Profile」ボタンをクリックし、以下の画面を表示します。

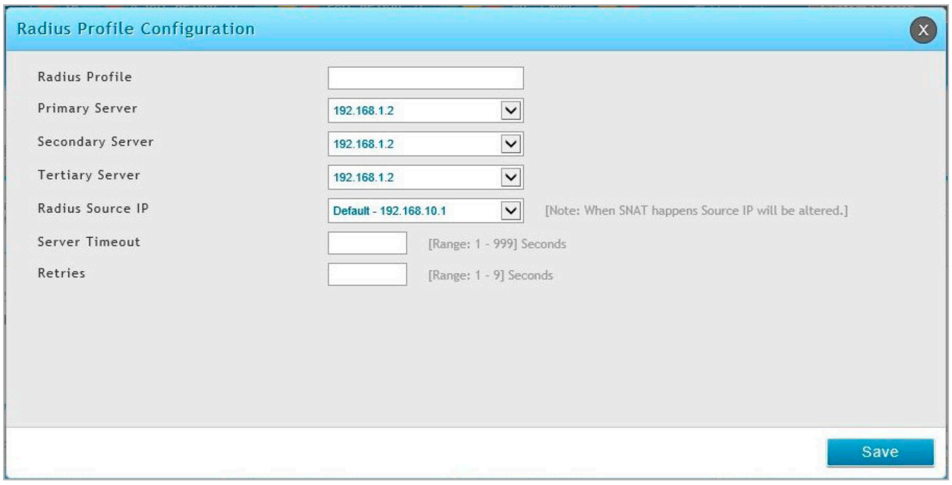


図 7-31　Add New Account 画面

3. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
Radius Profile	Radius プロファイルの名前を入力します。
Primary Server	プライマリ RADIUS 認証サーバの IP アドレスを選択します。
Secondary Server	セカンダリ RADIUS 認証サーバの IP アドレスを選択します。
Tertiary Server	ターシャリ RADIUS 認証サーバの IP アドレスを選択します。
Radius Source IP	Radius パケットの送信元アドレスとして使用される IP アドレスを指定します。 注意　パケットが Source NAT される場合、Radius パケットの送信元 IP アドレスは変更されます。
Server Timeout	コントローラが RADIUS サーバからの応答を待つ時間（秒）を指定します。
Retries	RADIUS サーバへの接続の試行回数を指定します。

RADIUS アカウンティングサーバの設定

Security > Authentication > External Auth Server > RADIUS Accounting メニュー

RADIUS アカウンティングサーバの設定を行います。本項目で設定したアカウンティングサーバは SSID ページでの RADIUS アカウンティングの有効 / 無効設定時に表示されます。

1. **Security > Authentication > External Auth Server > RADIUS Accounting** の順にメニューをクリックし、以下の画面を表示します。

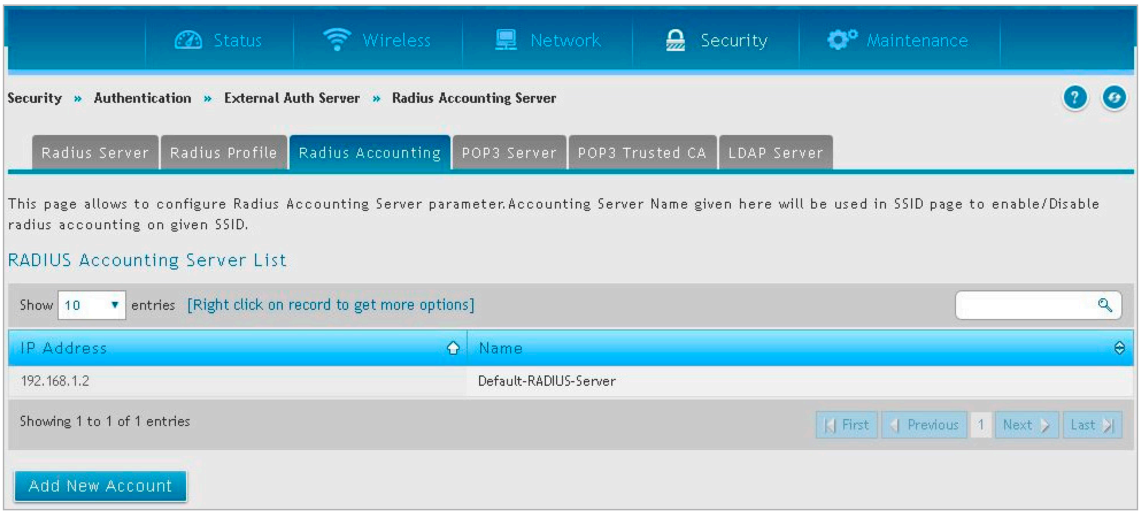


図 7-32　Radius Accounting Server List 画面

2. 「Add New Account」ボタンをクリックし、以下の画面を表示します。

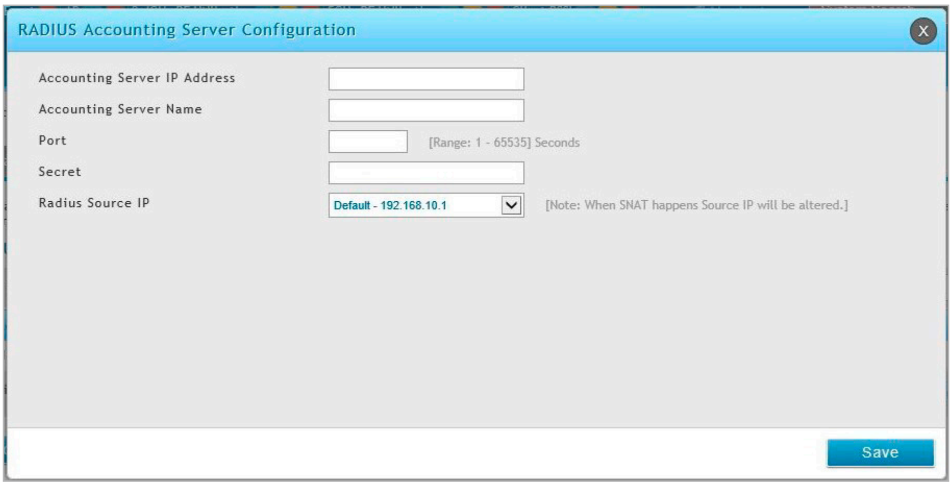


図 7-33　Radius Accounting Server Configuration 画面

3. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
Accounting Server IP Address	RADIUS アカウンティングサーバの IP アドレスを指定します。
Accounting Server Name	RADIUS メッセージを送信する RADIUS 認証サーバの名前を指定します。
Port	RADIUS アカウンティングサーバのポートを指定します。
Secret	デバイスが設定済みの RADIUS アカウンティングサーバにログインするための秘密鍵を指定します。 これは RADIUS アカウンティングサーバの秘密鍵に一致する必要があります。
Radius Source IP	Radius パケットの送信元アドレスとして使用される IP アドレスを指定します。 注意　パケットが Source NAT される場合、Radius パケットの送信元 IP アドレスは変更されます。

POP3 サーバの設定

Security > Authentication > External Auth Server > POP3 Server メニュー

POP3 は、TCP/IP 接続上でメールに最も一般的に使用されるアプリケーションレイヤのプロトコルです。暗号化トラフィックを POP3 サーバに送信するために、ポート 995 経由で SSL 暗号化と共に認証サーバを使用します。POP3 サーバの証明書は、ユーザがアップロードした CA 証明書によって検証されます。SSL 暗号化が使用されない場合、ポート 110 が POP3 認証トラフィックに使用されます。

無線コントローラは、単に POP3 クライアントとして機能し、外部 POP3 サーバに接続することでユーザを認証します。この認証オプションは IPSec、PPTP/L2TP サーバ、およびキャプティブポータルユーザで利用可能です。PPTP / L2TP サーバ用の POP3 は、PAP でのみサポートしており、CHAP/ MSCHAP / MSCHAPv2 暗号化ではサポートしていないことにご注意ください。

POP3 サーバの設定

1. **Security > Authentication > External Auth Server > POP3 Server** の順にメニューをクリックし、以下の画面を表示します。

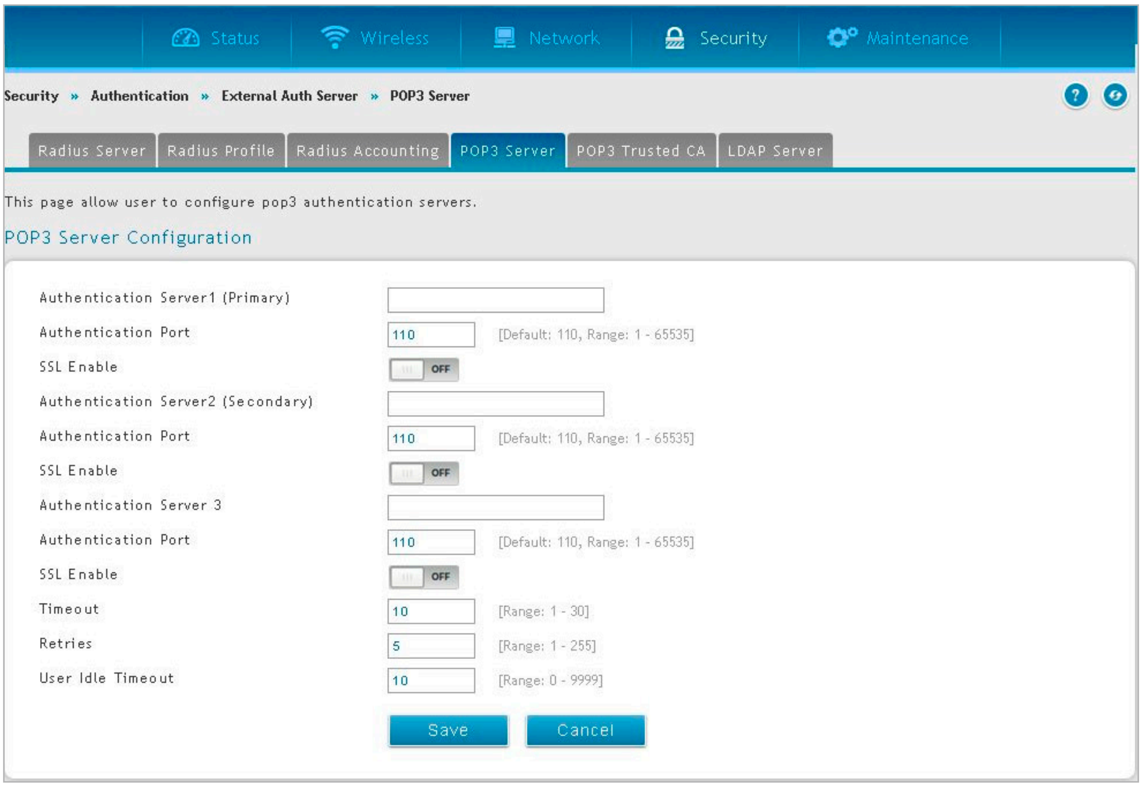


図 7-34　POP3 Server Configuration 画面

2. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
Authentication Server1-3	POP3 認証サーバ 1-3 の IP アドレスを指定します。
Authentication Port	POP3 メッセージを送信する認証サーバのポートを指定します。
SSL Enable	POP3 の SSL サポートを有効にします。本オプションが有効な場合、CA（認証局）を選択する必要があります。
CA File	POP3 サーバの証明書を検証する CA（認証局）を指定します。
Timeout	POP3 サーバからの応答に対するコントローラの待ち時間（秒）を設定します。
Retries	POP3 サーバへの接続試行回数を指定します。
User Idle Timeout	ユーザがアイドル状態になってからタイムアウトするまでの時間を指定します。

POP3 のトラスト CA の設定

Security > Authentication > External Auth Server > POP3 Trusted CA メニュー

CA ファイルは、設定した認証サーバの ID を検証するために、POP3 ネゴシエーションの一部として使用されます。3 つの設定サーバのそれぞれが、認証に使用する固有の CA を持つことができます。

1. **Security > Authentication > External Auth Server > POP3 Trusted CA** の順にメニューをクリックし、以下の画面を表示します。

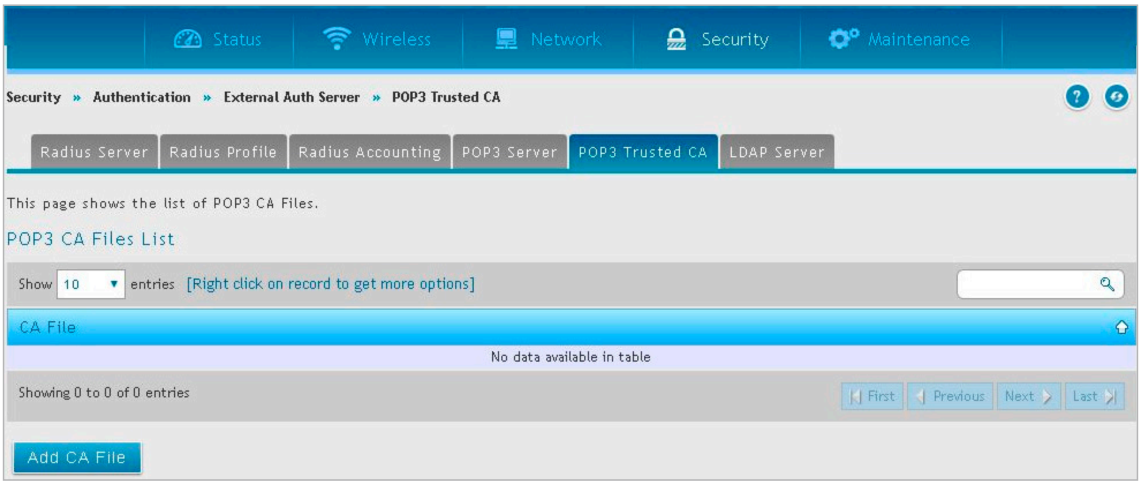


図 7-35　POP3 CA Files List 画面

2. 「Add CA File」ボタンをクリックして、CA ファイルを追加します。

図 7-36　CA File Configuration 画面

3. 「ファイルの選択」をクリックして、CA ファイルを参照します。選択後、「Save」ボタンをクリックします。

LDAP サーバの設定

Security > Authentication > External Auth Server > LDAP Server メニュー

LDAP 認証方式では、コントローラと外部のサーバ間で認証証明書を交換するために LDAP を使用します。LDAP サーバは、ディレクトリ構造内に大容量のユーザデータベースを保持します。ユーザ情報が階層的に保存されるため、同じユーザ名で異なるグループに所属するユーザを認証することができます。なお、Windows や Linux サーバにおける LDAP サーバの設定は、ユーザ認証用の NT ドメインや Active Directory サーバの設定よりも格段に簡単になっています。

コントローラに設定された情報は、コントローラとそのホストの認証を通過します。LDAP 属性、ドメイン名（DN）、および管理者アカウント＆パスワードは、LDAP サーバにコントローラの認証を許可するキーフィールドです。

LDAP サーバの設定

1. **Security > Authentication > External Auth Server > LDAP Server** の順にメニューをクリックし、以下の画面を表示します。

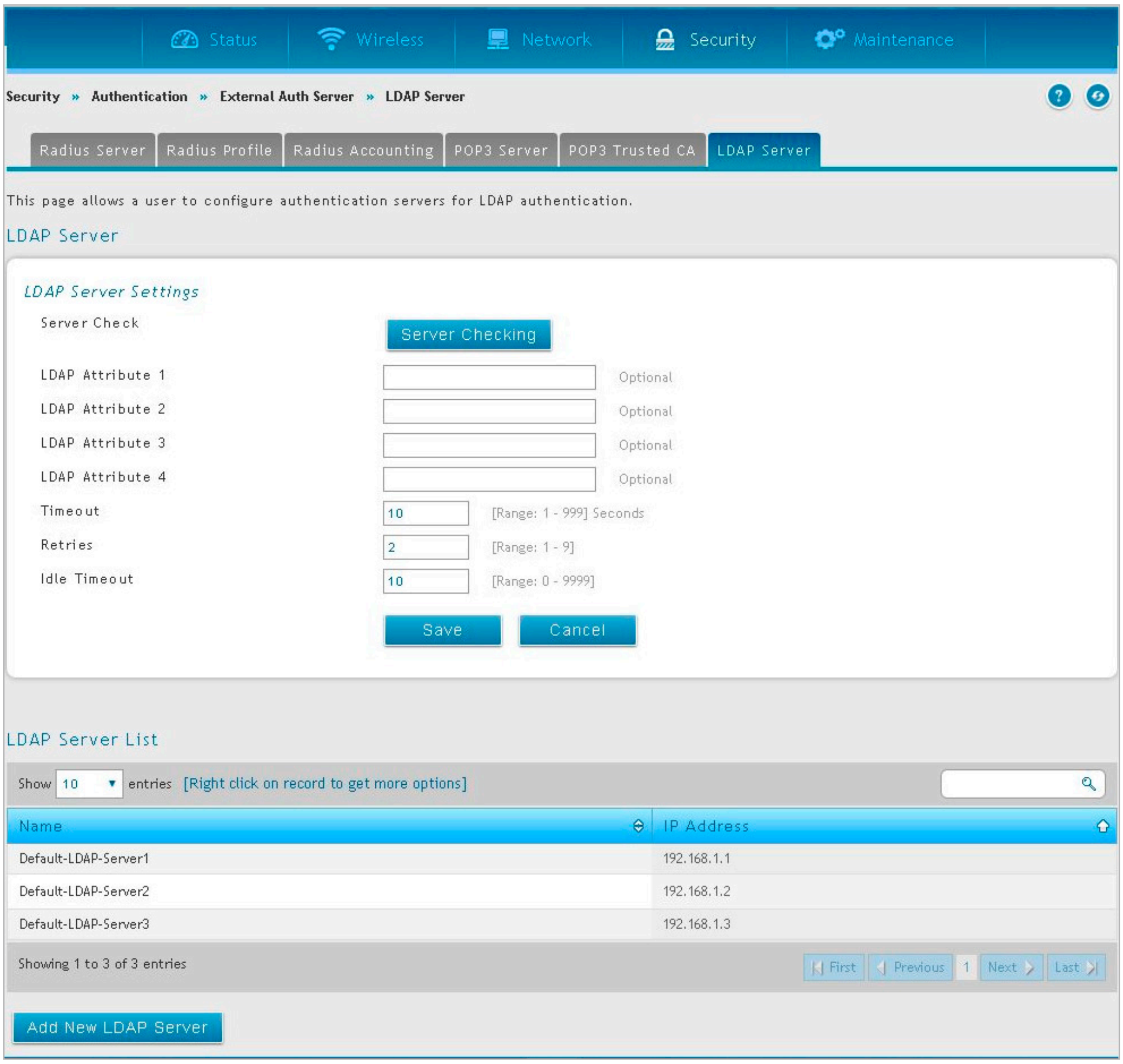


図 7-37　LDAP Server Configuration 画面

2. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
LDAP Attribute (1-4)	LDAP サーバで設定された LDAP ユーザに関連する属性を指定します。これらは、SAM アカウント名、Associated ドメイン名などの属性を含みます。同じユーザ名を持っていて異なるユーザを見分けるためにこれらを使用できます。
Timeout	LDAP サーバからの応答をコントローラが待つ時間（秒）を設定します。
Retries	LDAP サーバへの接続試行回数を指定します。
Idle Timeout	アイドル状態になってからタイムアウトするまでの時間を指定します。

3.　新しい LDAP サーバを追加する場合は、「Add New LDAP Server」ボタンをクリックし、以下の画面を表示します。

図 7-38　Add New LDAP Server 画面

4.　フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
Profile Name	LDAP 認証サーバのプロファイル名を指定します。
Authentication Server	LDAP 認証サーバの IP アドレスを指定します。
LDAP Base DN	LDAP 認証におけるベースドメイン名を指定します。このドメインで LDAP 認証を使用するベース DN については管理者に問い合わせてください。
Administrator Account	PPTP/L2TP 接続に LDAP 認証が必要な時に使用される LDAP サーバの管理アカウントを指定します。
Password	管理パスワードを入力します。

RADIUS アカウンティンググローバル設定

Security > Authentication > Radius Accounting Global Configuration メニュー

本項目では RADIUS アカウンティングサーバのグローバル設定、表示を行います。設定 SSID においてアカウンティングをグローバルに有効 / 無効に指定するために、「Accounting Mode」を使用します。

1.　**Security > Authentication > Radius Accounting Global Configuration** の順にメニューをクリックし、以下の画面を表示します。

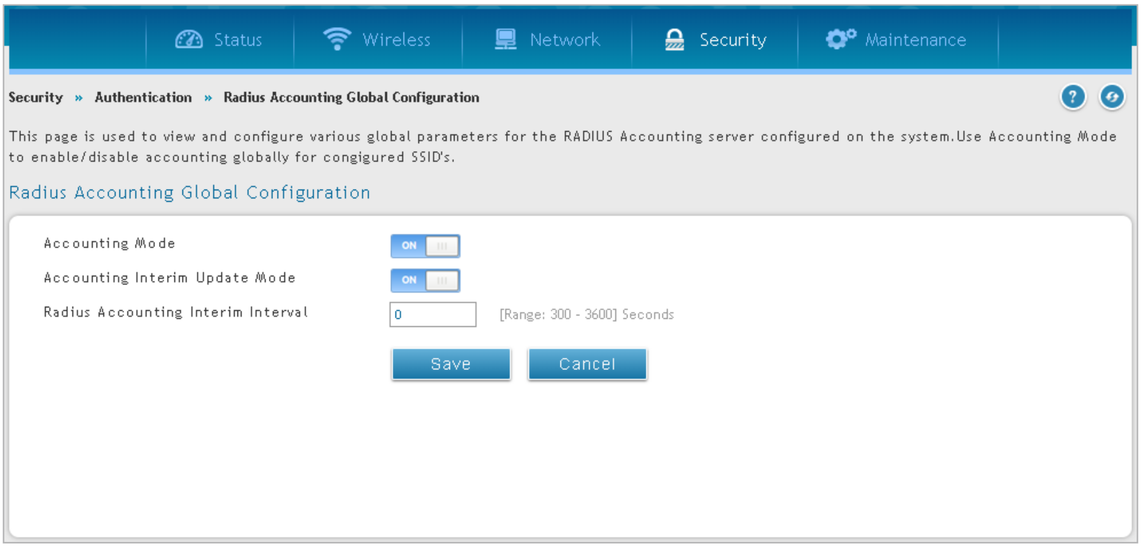


図 7-39　Radius Accounting Global Configuration 画面

2.　フィールドにデータを入力、設定し「Save」ボタンをクリックします。

項目	説明
Accounting Mode	RADIUS アカウンティングモードを有効 / 無効にします。
Accounting Interim Update Mode	RADIUS アカウンティングの 中間報告（Interim-Update）モードを有効 / 無効に指定します。
Radius Accounting Interim Interval	RADIUS アカウンティングの 中間報告（Interim-Update）モード有効時に、中間報告の間隔を指定します。300 - 3600（秒）で指定できます。

Facebook Wi-Fi 設定

Security > Authentication > Facebook Wifi メニュー

Facebook WiFi は「facebook.com」を使用した認証用キャプティブポータルメカニズムです。Facebook WiFi 認証を使用するには Facebook にゲートウェイデバイスとして登録する必要があります。

1. **Security > Authentication > Facebook Wifi** の順にメニューをクリックし、以下の画面を表示します。

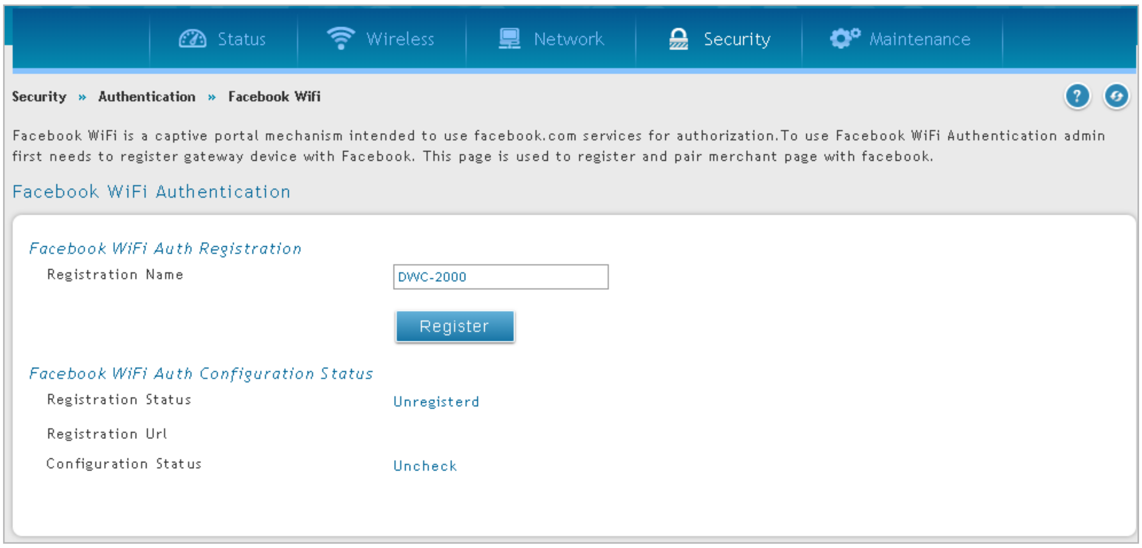


図 7-40　Facebook WiFi Authentication 画面

2. フィールドにデータを入力、設定し「Register」ボタンをクリックします。

項目	説明
Facebook WiFi Auth Registration	
Registration Name	登録名を指定し、「Register」をクリックします。
Facebook WiFi Auth Configuration Status	
Registration Status	登録ステータスを表示します。
Registration Url	登録された URL を表示します。
Configuration Status	設定ステータスを表示します。

E-mail 設定

Security > Authentication > Email Configuration メニュー
本項目ではコントローラからキャプティブポータルユーザへ E メールを送信する SMTP サーバの設定を行います。

1. **Security > Authentication > Email Configuration** の順にメニューをクリックし、以下の画面を表示します。

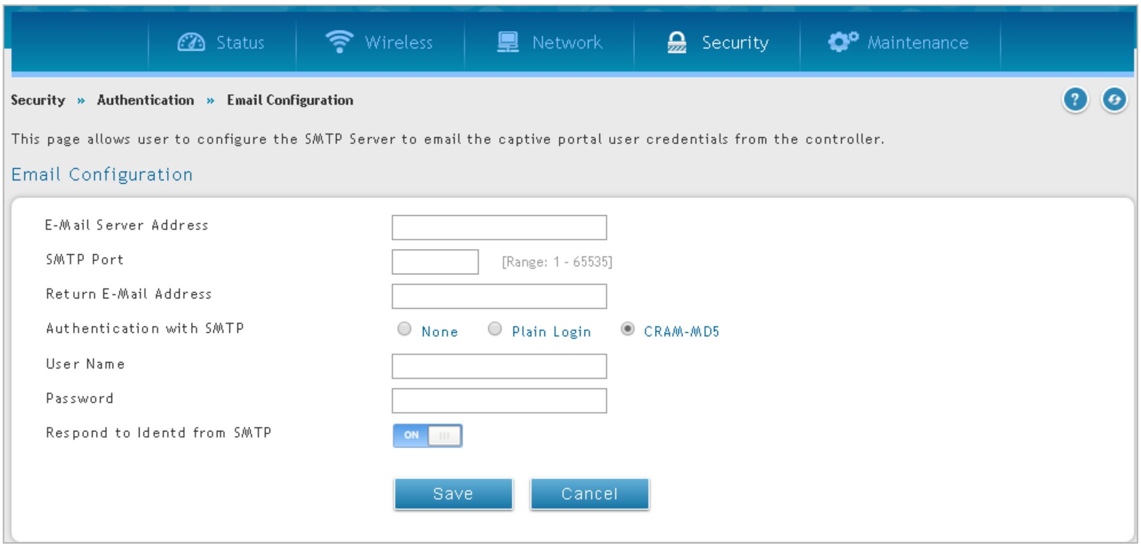


図 7-41　Email Configuration 画面

2. フィールドにデータを入力、設定し「Register」ボタンをクリックします。

項目	説明
E-Mail Server Address	キャプティブポータルユーザに E メール送信するための SMTP サーバアドレスを指定します。
SMTP Port	E メールサーバの SMTP ポートを指定します。
Return E-Mail Address	SMTP サーバからの E メールを受信する E メールアドレスを指定します。送信失敗時に必要です。
Authentication with SMTP	接続前に SMTP サーバによる認証が必要な場合、「Plain Login」「CRAM-MD5」でユーザ名、パスワードの認証を設定します。「None」を選択すると認証は行われません。
User Name	認証時のユーザ名を指定します。
Password	認証時のパスワードを指定します。
Respond to Identd from SMTP	SMTP サーバからの「IDENT」リクエストに、コントローラから応答を行うかどうかを設定します。

証明書設定

CA 証明書や自己署名証明書の追加を行います。

信頼済み証明書

Security > Authentication > Certificates メニュー

信頼済み証明書（CA 証明書）は、CA によって署名された証明書の有効性を検証するために使用されます。証明書生成時に、認証局（CA）と呼ばれる信頼される組織や機関によって署名が行われます。本画面のテーブルには、各 CA の証明書が表示されます。リモート VPN ゲートウェイまたはクライアントがデジタル証明書を提示した場合、認証処理の中でその証明書が信頼済み組織のいずれかによって発行されているかどうかが検証されます。

1. **Security > Authentication > Certificates Trusted Certificates** の順にメニューをクリックし、以下の画面を表示します。

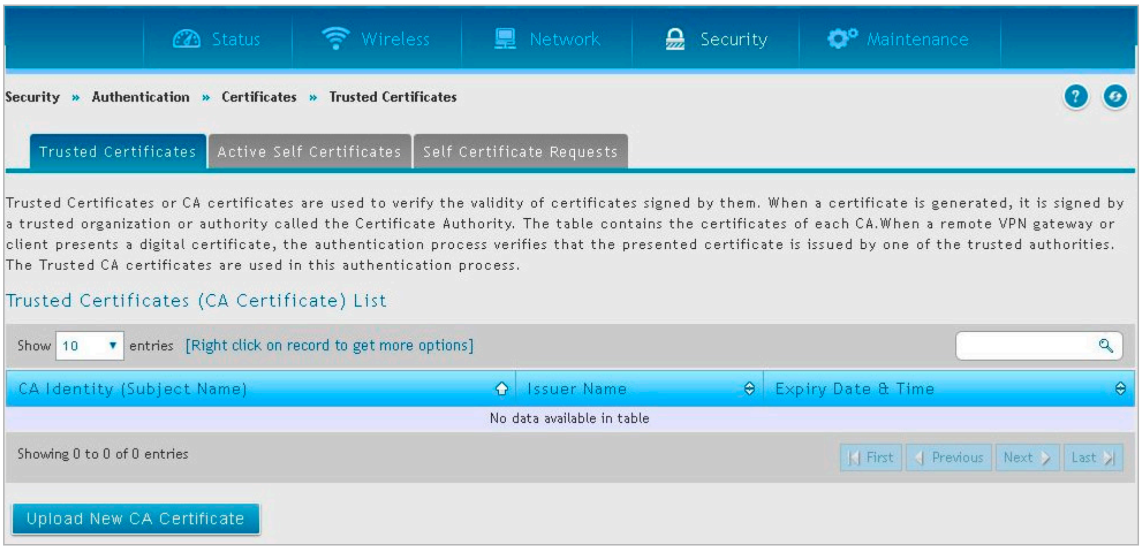


図 7-42　Trusted Certificates (CA Certificate) List 画面

2. 「Add New CA Cert」ボタンをクリックして、証明書を追加します。

図 7-43　CA File Configuration 画面

3. 「ファイルの選択」をクリックして、CA ファイルを参照します。選択後、「Save」ボタンをクリックします。

アクティブな自己署名証明書

Security > Authentication > Certificates メニュー

このテーブルには、信頼済み認証局（CA）によって発行された証明書の一覧が表示されます。リモート IKE サーバは、これらの証明書を使用してこのルータを検証します。

1. **Security > Authentication > Active Self Certificates** の順にメニューをクリックし、以下の画面を表示します。

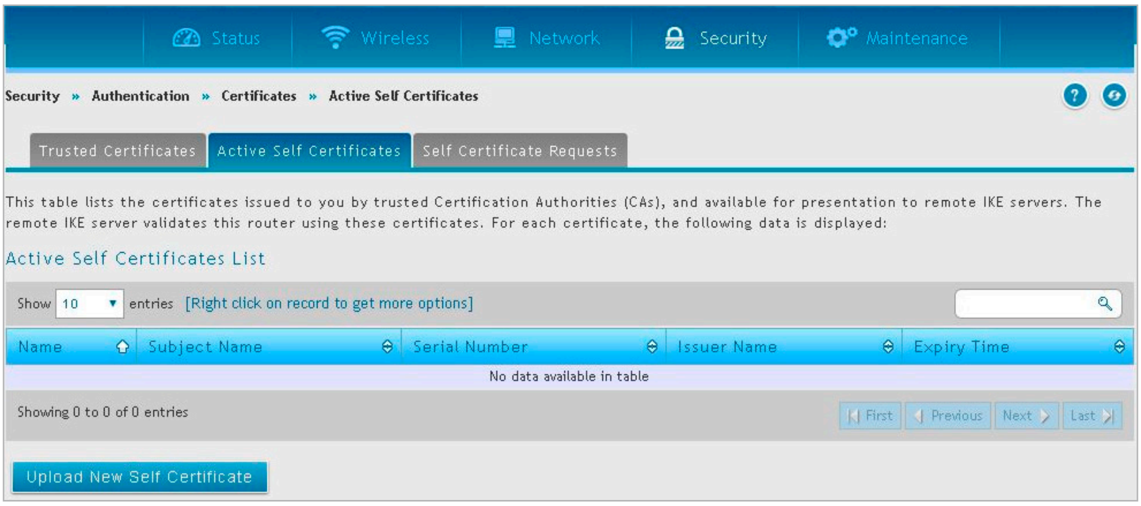


図 7-44　Active Self Certificates List 画面

2. 「Upload New Self Certificate」ボタンをクリックして、証明書を追加します。

図 7-45　Upload Active Self Certificate 画面

3. 「ファイルの選択」をクリックして、ファイルを参照します。選択後、「Upload」ボタンをクリックします。

自己署名証明書のリクエスト

Security > Authentication > Certificates メニュー -

本画面には、生成されたすべての証明書リクエストが表示されます。

1. **Security > Authentication > Self Certificate Requests** の順にメニューをクリックし、以下の画面を表示します。

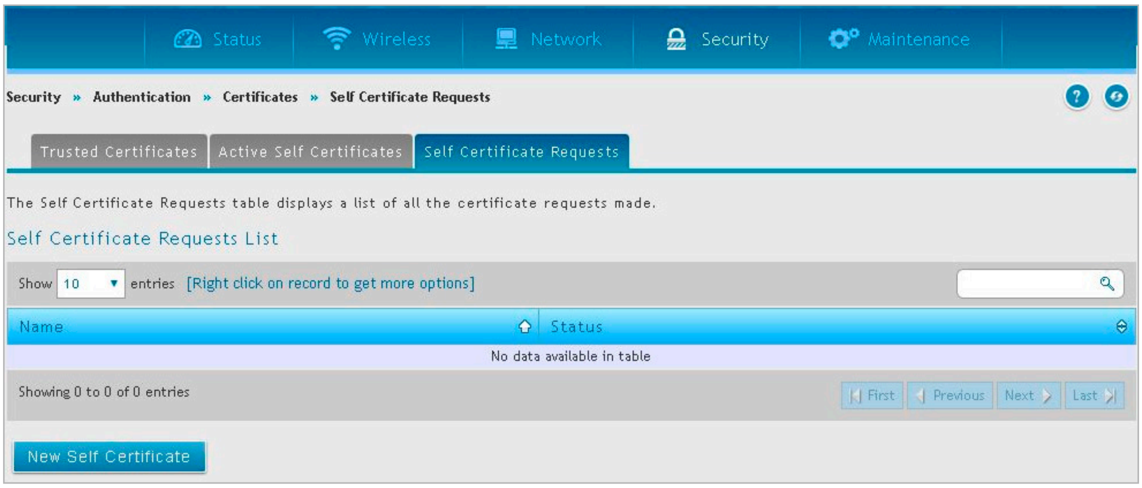


図 7-46　Self Certificate Request List 画面

2. 「New Self Certificate」ボタンをクリックして、証明書を追加します。

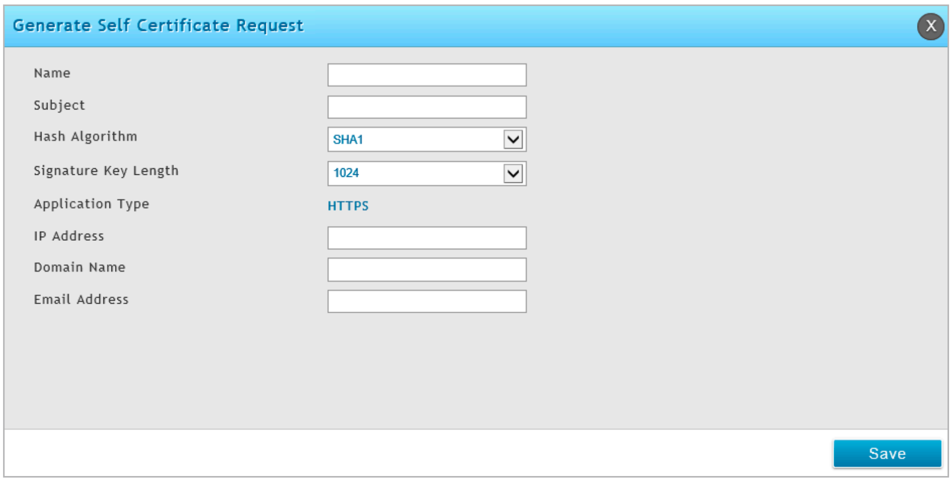


図 7-47　Generate Self Certificate Request 画面

3. フィールドにデータを入力、設定し「Save」ボタンをクリックします。

項目	説明
Name	証明書に固有の名前を指定します。
Subject	証明書の CN（Common Name）を入力します。一般的には以下のフォーマットで定義されます。 CN=<device name>, OU=<department>, O=<organization>, L=<city>, ST=<state>, C=<country>. For example: CN=router1, OU=my_company, O=mydept, L=SFO, C=US
Hash Algorithm	ハッシュアルゴリズムを MD5 または SHA1 から指定します。
Signature Key Length	シグネチャの長さを 1024、2048 から指定します。 1024bit の RSA 鍵は安全性が低いと考えられています。 セキュリティのため、一部のブラウザではこれらの設定が制限されており、使用を避けることを推奨します。
Application Type	アプリケーションタイプが表示されます。
IP Address	オプションとして IP アドレスを入力します。
Domain Name	オプションとしてドメイン名を入力します。
Email Address	オプションとして Email アドレスを入力します。

MAC バイパス設定

Security > Authentication > MAC Bypass メニュー

MAC バイパスは、登録した MAC アドレスを持つユーザがキャプティブポータルへのログインをせずにインターネットを閲覧できるようにする機能です。

1. **Security > Authentication > MAC Bypass** の順にメニューをクリックし、以下の画面を表示します。

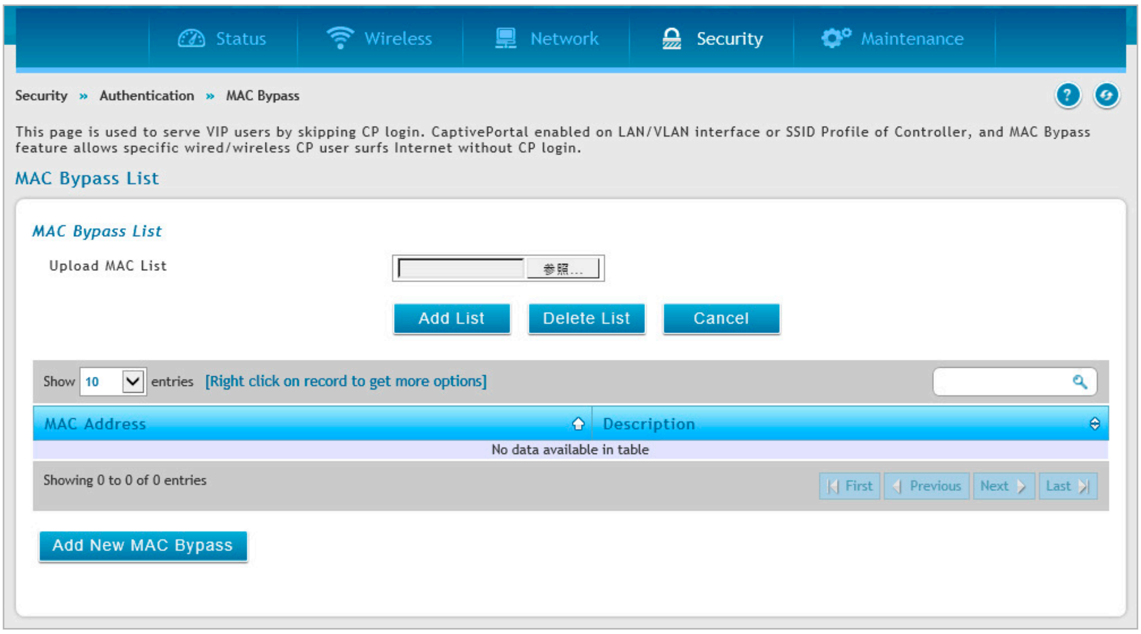


図 7-48　MAC Bypass List 画面

■ MAC リストを登録する場合：

「参照」をクリックし、csv 形式のファイルを選択　→　「Add List」をクリックします。

■ MAC リストを削除する場合：

「Delete List」をクリックします。

■ MAC アドレスを追加する場合：

1. 「Add New MAC Bypass」をクリックします。

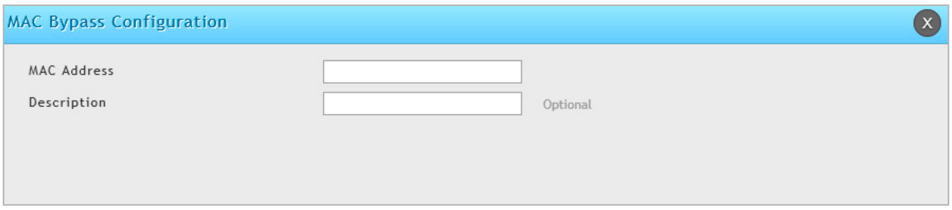


図 7-49　MAC Bypass Configuration 画面

2. 以下の項目を設定します。
    - MAC Address - MAC アドレスを入力します。
    - Description - 説明を入力します。

3. 「Save」をクリックします。

OAuth サーバ設定

Security > Authentication > oAuth Server メニュー

OAuth サーバの設定を行います。

OAuth サーバは、キャプティブポータルで LAN および WLAN クライアントを認証するために使用できる外部認証サーバです。

注意　本機能は現在サポートしているアクセスポイントでは使用できません。

1. **Security > Authentication > Security > Authentication > oAuth Server** の順にメニューをクリックし、以下の画面を表示します。

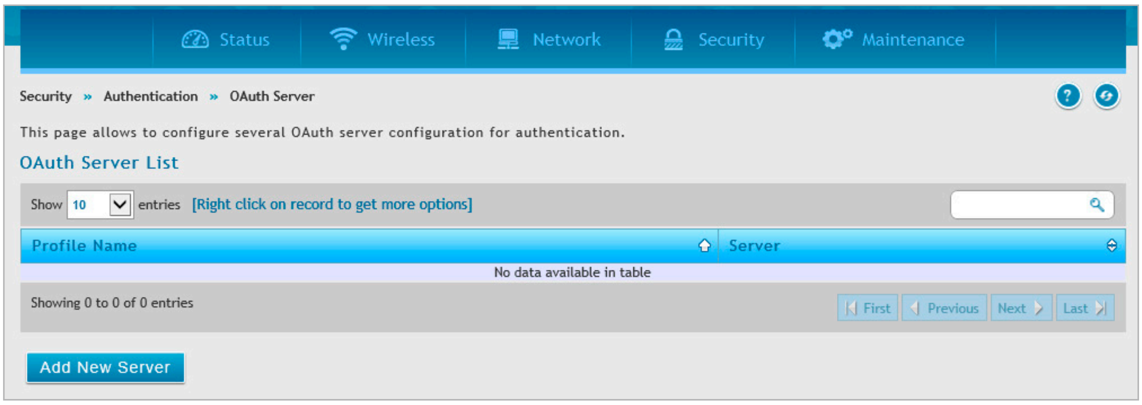


図 7-50　OAuth Server List 画面

2. 「Add New Server」をクリックし、以下の画面を表示します。

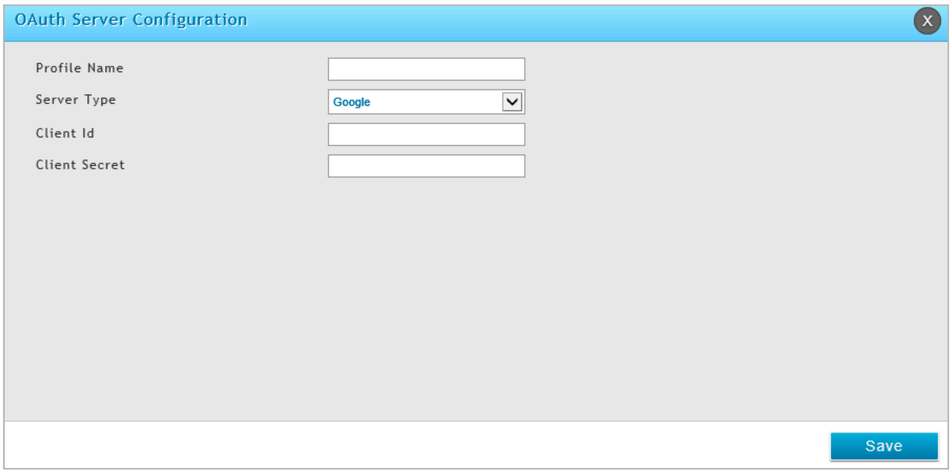


図 7-51　OAuth Server Configuration 画面

3. フィールドにデータを入力、設定し「Save」ボタンをクリックします。

項目	説明
Profile Name	プロファイル名を入力します。
Server Type	サーバタイプを「Google」「Facebook」「Line」「Weibo」から選択します。
Client Id	クライアント ID を入力します。
Client Secret	クライアントシークレットを入力します。

■ エントリの編集

エントリ上で右クリックし、「Edit」をクリックします。

■ エントリの削除

エントリ上で右クリックし、「Delete」をクリックします。

クライアントのブロック

Security > Firewall > Blocked Clients メニュー

トラフィックが直接本製品を通過すると、コントローラはブロッククライアント（MAC アドレス）からのトラフィックをブロックします。

ブロックするクライアントの追加

1. **Security > Firewall > Blocked Clients** の順にメニューをクリックし、以下の画面を表示します。

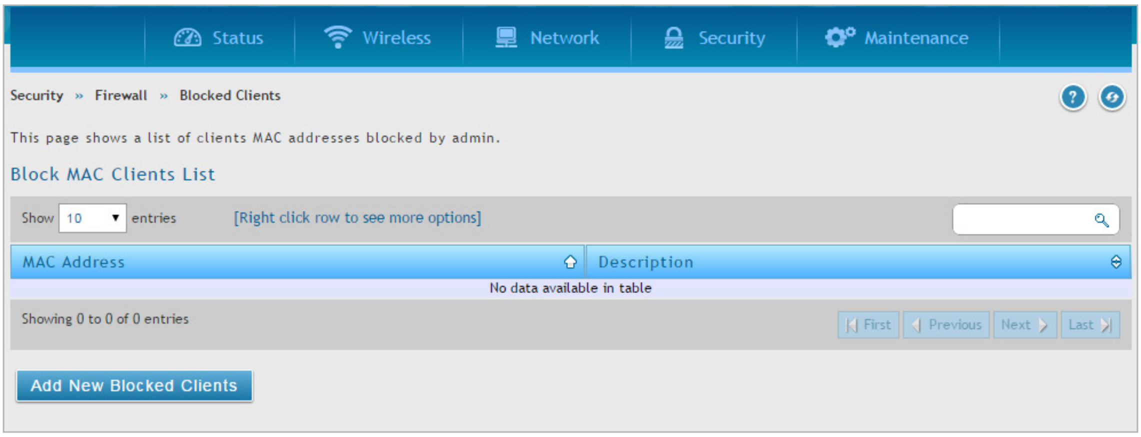


図 7-52　Block MAC Clients List 画面

2. 「Add New Blocked Clients」ボタンをクリックし、以下の画面を表示します。

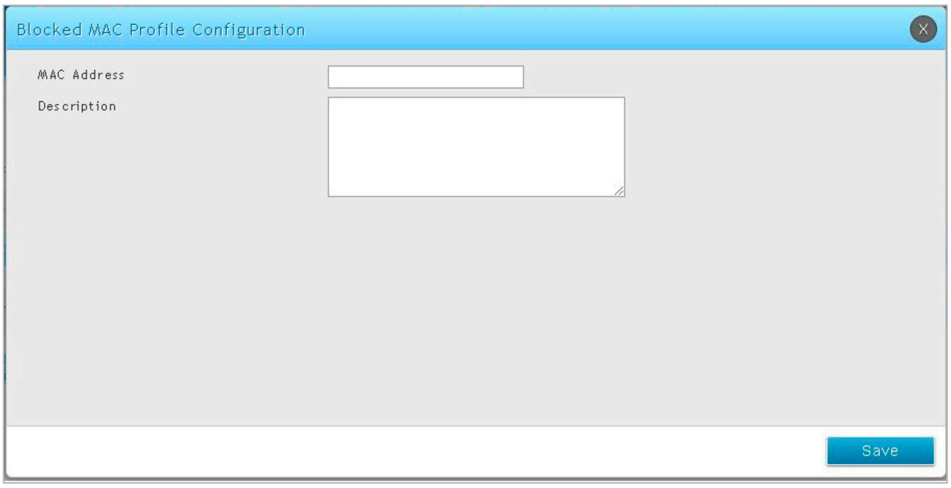


図 7-53　Blocked MAC Profile Configuration 画面

3. クライアントの MAC アドレスと説明文を入力して、「Save」ボタンをクリックします。

第 8 章　ステータスおよび統計情報

本章では、無線コントローラとアクセスポイントのステータス情報と統計情報を表示する以下の機能について説明します。

設定項目	説明
統計情報と利用率の参照	デバイスの状態、無線 / 有線トラフィックの統計情報、トンネル、接続するクライアント、および利用率を表示します。また、ダッシュボードのカスタマイズを行います。
システム状態の参照	コントローラの基本情報、ログ、USB デバイスに関する情報を表示します。
ネットワーク情報の参照	DHCP クライアント、キャプティブポータルセッション、送受信統計情報、リンクアグリゲーションの状態を表示します。
コントローラの参照	コントローラの無線設定、Radius アカウンティングサーバなどの情報を表示します。
アクセスポイント情報の参照	アクセスポイントの統計情報を表示します。

統計情報と利用率の参照

Status > Dashboard メニュー

無線コントローラは、システムが使用しているリソースについて表示するダッシュボードを提供します。ダッシュボードページは以下のセクションでまとめられています。

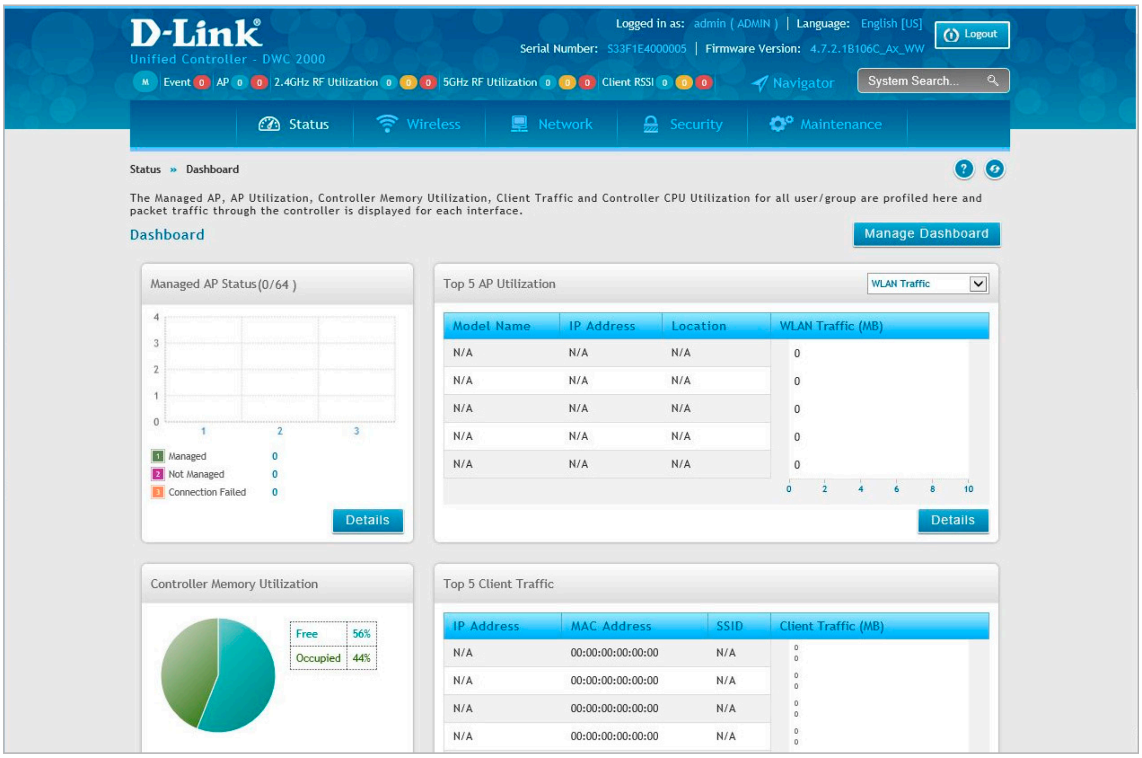


図 8-1　　Dashboard 画面

セクション	説明
Managed AP Status	検出した現在の状態ごとに管理アクセスポイントのチャートを表示します。
Controller Memory Utilization	コントローラが消費しているメモリ使用率（%）を表示します。
Controller CPU Utilization	コントローラが消費している CPU 使用率（%）を表示します。
Top 5 AP Utilization	AP の各使用率 / トラフィック統計と無線 LAN トラフィック消費上位 5 個を表示します。
Top 5 Client Traffic	クライアントのトラフィック統計とトラフィック消費上位 5 個を表示します。
Monthly Active Users	接続ユーザの履歴を表示します。

ダッシュボードの管理

以下の手順で、ダッシュボードをカスタマイズすることができます。

1. 「Manage Dashboard」ボタンをクリックします。

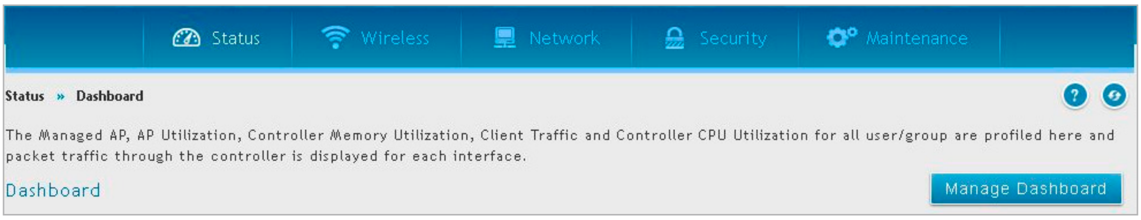


図 8-2　Dashboard 画面

2. 以下の画面が表示されます。

図 8-3　Managed Dashboard 画面

ダッシュボードに表示される概要パネルを有効または無効にすることができます。また、「Dashboard Auto Refresh」でダッシュボードの更新間隔を設定することができます。

3. パネルを「ON」または「OFF」に切り替えて、「Save」ボタンをクリックします。

詳細情報

各ダイアログで「Details」ボタンをクリックすることで、詳細情報または統計情報をレビューすることができます。

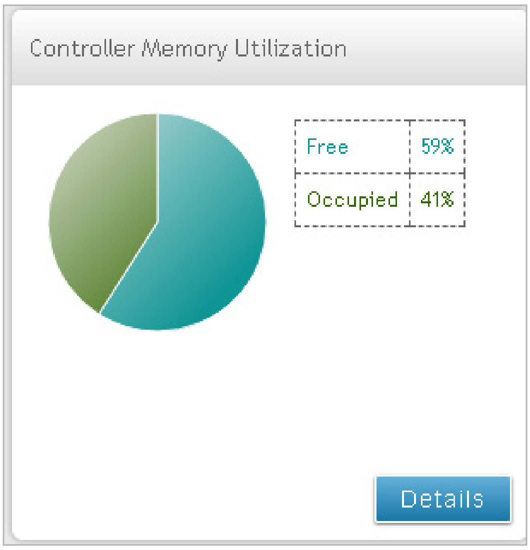


図 8-4　Controller Memory Utilization 画面

Memory Utilization Details

Total Memory	1827 MB
Used Memory	448 MB
Free Memory	1380 MB
Cached Memory	86 MB
Buffer Memory	19 MB

図 8-5　　Controller Memory Utilization Details 画面

Managed AP Status Details

Model Name	Firmware	MAC Address	IP Address	Location	Status	System Uptime
DWL-7620AP	4.7.2.9	[redacted]	192.168.10.8		Managed	00:01:55:38

図 8-6　　Managed AP Status Details 画面

CPU Utilization Details

CPU usage by user	1 %
CPU usage by kernel	0 %
CPU idle	99 %
CPU waiting for IO	0 %

図 8-7　　CPU Utilization Details 画面

AP Utilization Details

Model Name	IP Address	Location	MAC Address	Firmware	AP Up Time	Auth. Clients	WLAN Traffic	RF Utilization 5G	RF Utilization 2.4G
DWL-7620AP	192.168.10.8		[redacted]	4.7.2.9	00:01:58:58	1	1	9	5

図 8-8　　AP Utilization Details 画面

Client Traffic Details

Client IP Address	Client MAC Address	SSID	AP MAC Address	AP Location	Channel	NetBIOS	Rx(MB) from STA	Tx(MB) to STA
No data available in table								

図 8-9　　Client Traffic Details 画面

「Traffic Information」テーブルでは、以下の各物理ポートの詳しい送受信統計情報を表示します。

- 各インタフェース（LAN、VLAN）のポートにおけるパケットレベルの情報
- 送受信パケット
- 各インタフェースの送受信方向の合計（バイト / 秒）

有線ポートで何らかの問題が発生していることが疑われる場合、このテーブルを使用して、ポートの稼働時間や送信レベルでの問題を診断します。統計情報テーブルには、各ページの更新時に最新のポートレベルデータの表示を可能にする自動更新機能があります。「Manage Dashboard」から更新間隔を設定します。トラフィック情報をリセットするには、「Clear Statistics」ボタンをクリックします。

Traffic Information

Traffic	WLAN [Packets]	WLAN [Bytes]	LAN
Incoming	0	0	86213
Outgoing	0	0	251281
Dropped Incoming	0	0	0
Dropped Outgoing	0	0	0

Clear Statistics

図 8-10　　Traffic Information 画面

システム状態の参照

コントローラのシステム情報を参照します。

デバイス状態の参照

Status > System Information > Device メニュー

無線コントローラのコンフィグレーション設定の要約を表示します。ここでは以下のセクションにまとめています。

- General - システム名、ファームウェアバージョン、WLAN モジュールバージョン、シリアル番号などを表示します。
- Port Information - 管理者設定パラメータに基づいて情報を表示します。LAN1 にはコントローラのローカルインタフェースが表示されます。LAN ポートを「Standalone」に設定すると、対応する LAN の下に情報が表示されます。

Status > System Information > Device の順にメニューをクリックし、以下の画面を表示します。

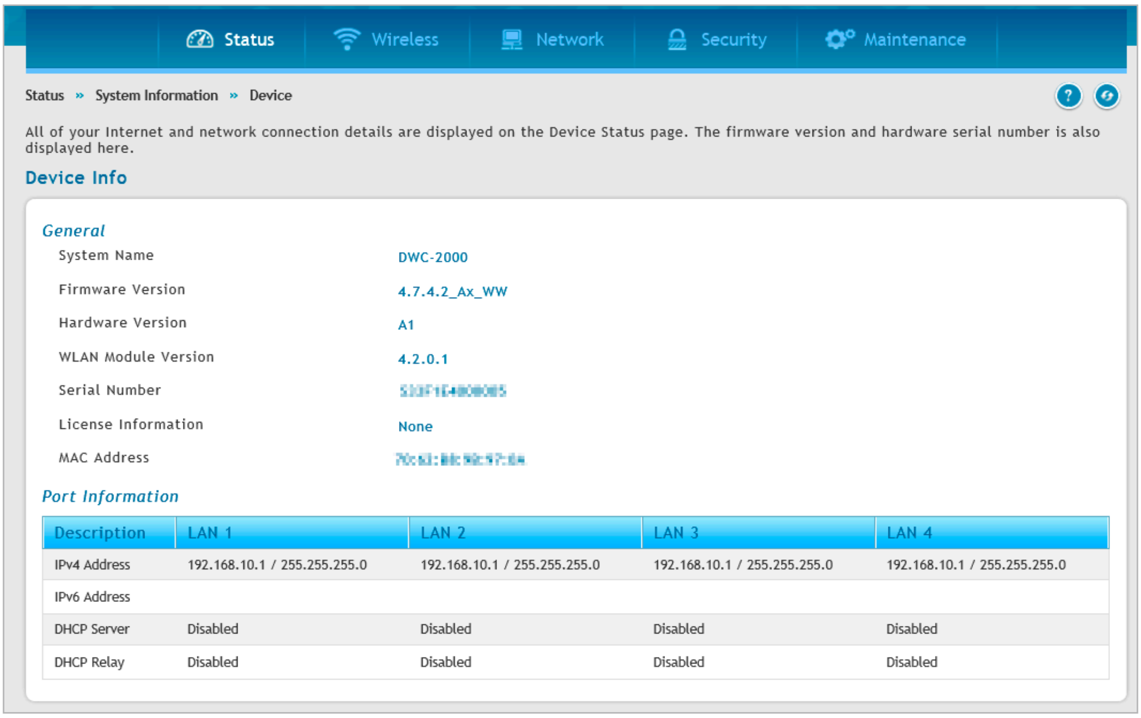


図 8-11　Device Info 画面

以下の項目があります。

項目	説明
General	
System Name	コントローラのユニット名が表示されます。
Firmware Version	コントローラが現在使用しているファームウェアのバージョンが表示されます。
Hardware Version	コントローラのハードウェアバージョンが表示されます。
WLAN Module Version	現在コントローラで動作している無線コントローラモジュールのバージョンが表示されます。
Serial Number	コントローラのメーカのシリアル番号が表示されます。
License Information	コントローラで有効なライセンスのタイプのリストが表示されます。
MAC Address	LAN ポートの MAC アドレスが表示されます。
Port Information	
IPv4 Address	LAN ポートの IPv4 アドレスが表示されます。
IPv6 Address	LAN ポートの IPv6 アドレスが表示されます。
DHCP Server	コントローラの DHCP サーバが有効または無効であるかを示します。「Enabled」の場合、LAN ポートに接続する DHCP クライアントのマシンは、ダイナミックにそれらの IP アドレスを受信します。
DHCP Relay	コントローラが DHCP リレーとして機能しているかどうかを示します。「Enabled」の場合、セキュリティアプライアンスは DHCP リレーとして動作します。

USB 情報の参照

Status > System Information > USB Status メニュー

無線コントローラに接続する USB デバイスの情報について表示します。無線コントローラには、直接、USB プリンタや USB ディスク（ファームウェアアップグレードの用途のみ）を接続できる 2 つの USB ポートがあります。

Status > System Information > USB Status の順にメニューをクリックし、以下の画面を表示します。

図 8-12　USB (s) Status 画面

以下の項目があります。

項目	説明
USB Port1/USB Port 2	
Status	接続 / 切断されたデバイスの状態を表示します。
Vendor	コントローラに接続する USB デバイスのベンダ名を表示します。
Model	コントローラに接続する USB デバイスのモデル名を表示します。
Type	コントローラは、USB ディスクドライブ（メモリスティック）デバイス、3G USB モデム（アダプタ）または USB プリンタに接続するインタフェースをサポートしています。
Mount Status	コントローラに接続する USB デバイスのマウント状態を表示します。

ネットワーク情報の参照

コントローラのネットワーク情報を参照します。

DHCP クライアントの参照

Status > Network Information > DHCP Clients メニュー
無線コントローラから IP がリースされているクライアントの一覧を表示します。

LAN のリースクライアント
Status > Network Information > DHCP Clients > LAN Leased Clients の順にメニューをクリックし、以下の画面を表示します。

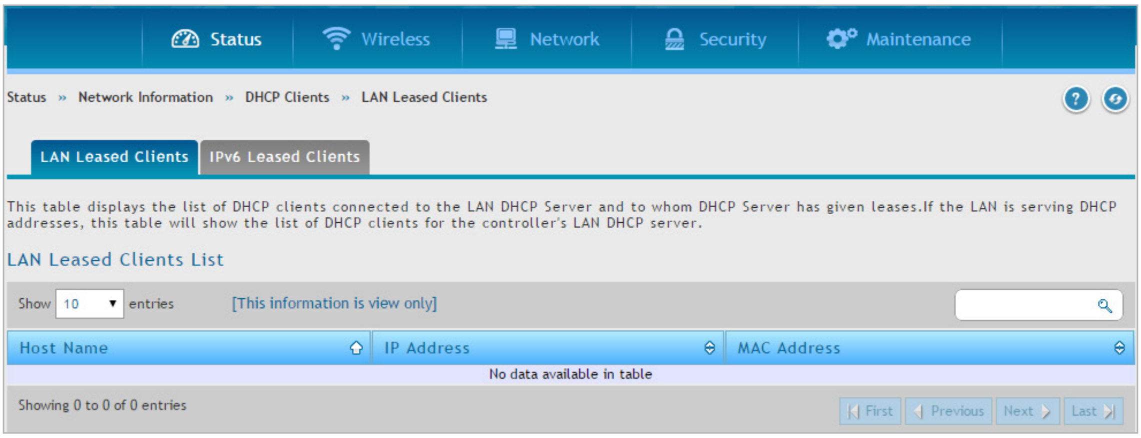


図 8-13　LAN Leased Clients List 画面

以下の項目があります。

項目	説明
Host Name	接続するクライアントのホスト名が表示されます。
IP Address	予約 IP リストに一致するホストの LAN IP アドレスが表示されます。
MAC Addresses	設定済みの IP アドレス予約を持つ LAN ホストの MAC アドレスが表示されます。

LAN IPv6 のリースクライアント
Status > Network Information > DHCP Clients > IPv6 Leased Clients の順にメニューをクリックし、以下の画面を表示します。

図 8-14　IPv6 Leased Clients List 画面

以下の項目があります。

項目	説明
Host Name	接続するクライアントのホスト名が表示されます。
IP Address	DHCP IPv6 サーバが予約する LAN IPv6 アドレスが表示されます。
MAC Address	DHCP IPv6 サーバ上にある場合には、予約された IP アドレスが割り当てられる MAC アドレスが表示されます。

キャプティブポータルセッションの参照

Status > Network Information > Captive Portal Sessions メニュー

コントローラが管理するアクセスポイントを通じて取得したアクティブなインターネットセッションがテーブルに表示されます。これらのユーザは、ローカルまたは外部ユーザデータベースに存在していて、インターネットアクセスを許可されたログイン証明書を持っています。

Status > Network Information > Captive Portal Sessions の順にメニューをクリックし、以下の画面を表示します。

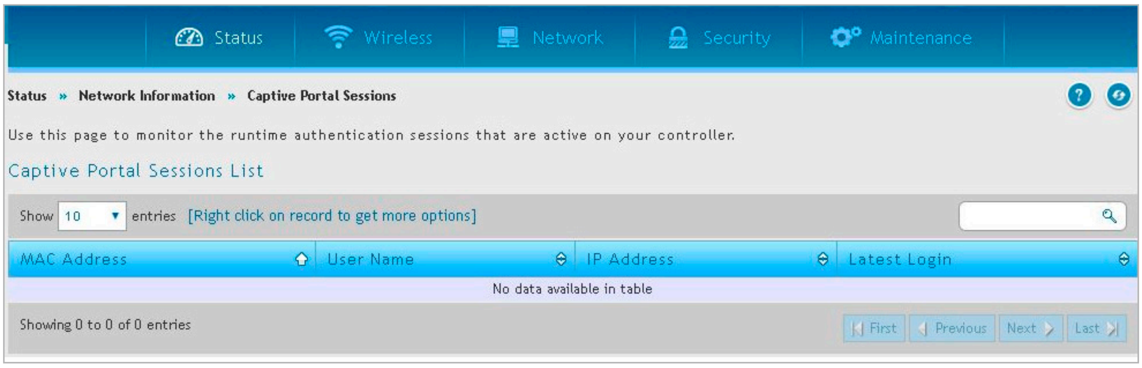


図 8-15　Captive Portal Sessions List 画面

インターネットセッションのパススルーが有効である場合、セッションで右クリックし、「Disconnect」を選択すると、管理者は認証ユーザを個別に切断できます。

セッションを選択し、右クリックメニューから「Block Device」を選択します。「Block Device」ボタンをクリックすると、クライアントはブロックリスト（**Security > Firewall > Blocked Clients**）に追加され、このクライアントによる現在および今後のセッションがブロックされます。

以下の項目があります。

項目	説明
MAC Address	ユーザの MAC アドレスが表示されます。
User Name	ユーザ名が表示されます。
IP Address	ログインユーザの IP アドレスが表示されます。
Latest Login	最新のログイン日時が表示されます。

インタフェースのトラフィックの参照

Status > Network Information > Interfaces メニュー

各インタフェースにおける内向き / 外向きパケットを表示します。

Status > Network Information > Interfaces の順にメニューをクリックし、以下の画面を表示します。

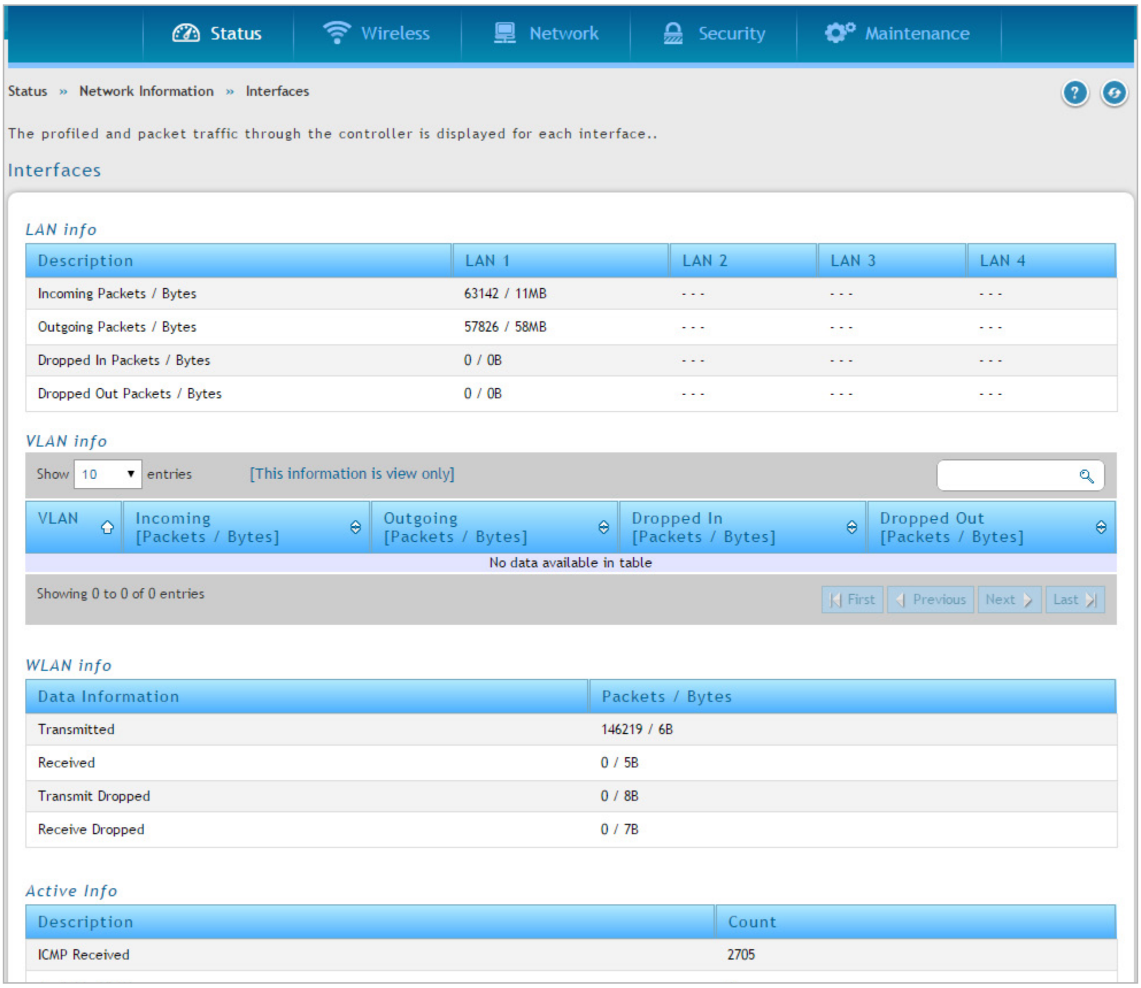


図 8-16　Interfaces 画面

以下の項目があります。

項目	説明
LAN Info (LAN 1-4)	
Incoming Packets / Bytes	ポートに入力する IP パケット（数 /bytes）が表示されます。
Outgoing Packets / Bytes	ポートから出力するパケット（数 /bytes）が表示されます。
Dropped In Packets / Bytes	インタフェースの内向き方向で破棄されたパケット（数 /bytes）が表示されます。
Dropped Out Packets / Bytes	インタフェースの外向き方向で破棄されたパケット（数 /bytes）が表示されます。
VLAN Info	
VLAN	VLAN ID が表示されます。
Incoming[Packets / Bytes]	ポートに入力する IP パケット（数 /bytes）が表示されます。
Outgoing [Packets / Bytes]	ポートから出力するパケット（数 /bytes）が表示されます。
Dropped In [Packets / Bytes]	インタフェースの内向き方向で破棄されたパケット（数 /bytes）が表示されます。
Dropped Out [Packets / Bytes]	インタフェースの外向き方向で破棄されたパケット（数 /bytes）が表示されます。
WLAN Info	
Transmitted	コントローラの管理下にあるすべてのアクセスポイントが送信したパケット数が表示されます。
Received	コントローラの管理下にあるすべてのアクセスポイントが受信したパケット数が表示されます。
Transmit Dropped	コントローラの管理下にあるすべてのアクセスポイントが送信し、破棄された総パケット数が表示されます。
Receive Dropped	インタフェースの内向き方向で破棄されたパケットが表示されます。
Active Info	
ICMP Received	インタフェースに受信した ICMP パケットの総数が表示されます。
Available VLAN	有効とされたアクティブな VLAN インタフェースが表示されます。
Active Interfaces	有効なインタフェースの数が表示されます。

リンクアグリゲーションの参照

Status > Network Information > Link Aggregation メニュー

リンクアグリゲーションの状態を表示します。

Status > Network Information > Link Aggregation の順にメニューをクリックし、以下の画面を表示します。

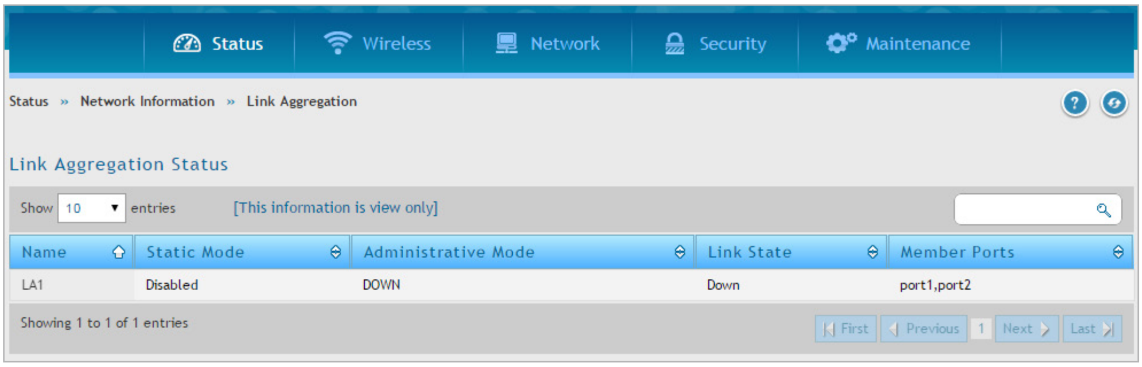


図 8-17　 Link Aggregation Status 画面

以下の項目があります。

項目	説明
Name	リンクアグリゲーショングループ（LAG）名を表示します。
Static Mode	リンクアグリゲーショングループ（LAG）のスタティックモードの状態を表示します。
Administrative Mode	管理モードの状態（有効 / 無効）を表示します。管理モードが無効な場合、トラフィックはフローをせず、LACPDU は破棄されますが、リンクアグリゲーションを形成するリンクは解放されません。初期値は有効です。
Link State	リンクが「Up」（アクティブ）または「Down」（ダウン）しているかを表示します。
Member Ports	リンクアグリゲーションの作成後、本フィールドは、文字列形式で LAG のメンバを表示します。

コントローラの参照

コントローラの無線情報を表示します。

コントローラの状態と統計情報の参照

Status > Wireless Information > Controller Status メニュー
コントローラの状態と情報を表示します。

Status > Wireless Information > Controller Status の順にメニューをクリックし、以下の画面を表示します。

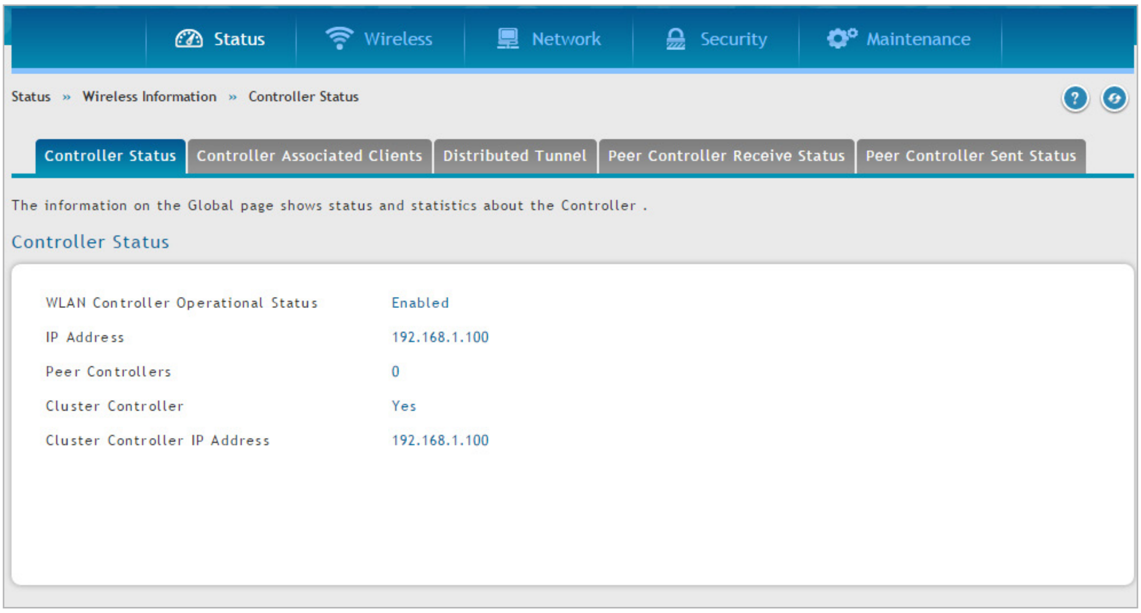


図 8-18　Controller Status 画面

以下の項目があります。

項目	説明
WLAN Controller Operational Status	WLAN コントローラの動作状態が表示されます。
IP Address	無線コントローラの IP アドレスが表示されます。
Peer Controllers	ネットワーク上で検出されたピア WLAN コントローラの数が表示されます。
Cluster Controller	このコントローラがクラスタにおけるクラスタコントローラかどうかを表示します。ピアコントローラのグループでは、コントローラの 1 つが、自動的に選出されるか、またはクラスタコントローラになるように設定されます。クラスタコントローラは、ピアグループ内のすべてのアクセスポイントとクライアントに関するステータスと統計情報を収集します。 注意　クラスタコントローラだけが、全クラスタの管理対象アクセスポイント、クライアント、統計情報および RF スキャンデータベースを表示できます。クラスタコントローラではないコントローラは、ローカルに接続するデバイスに関する情報だけを表示します。
Cluster Controller IP Address	クラスタコントローラであるピアコントローラの IP アドレスが表示されます。

関連クライアント

Status > Wireless Information > Controller Status > Controller Associated Clients メニュー

コントローラと、関連クライアントを表示します。このコントローラがクラスタコントローラである場合、他のピアコントローラで管理される関連クライアントも表示します。

Status > Network Information > Controller Status > Controller Associated Clients の順にメニューをクリックし、以下の画面を表示します。

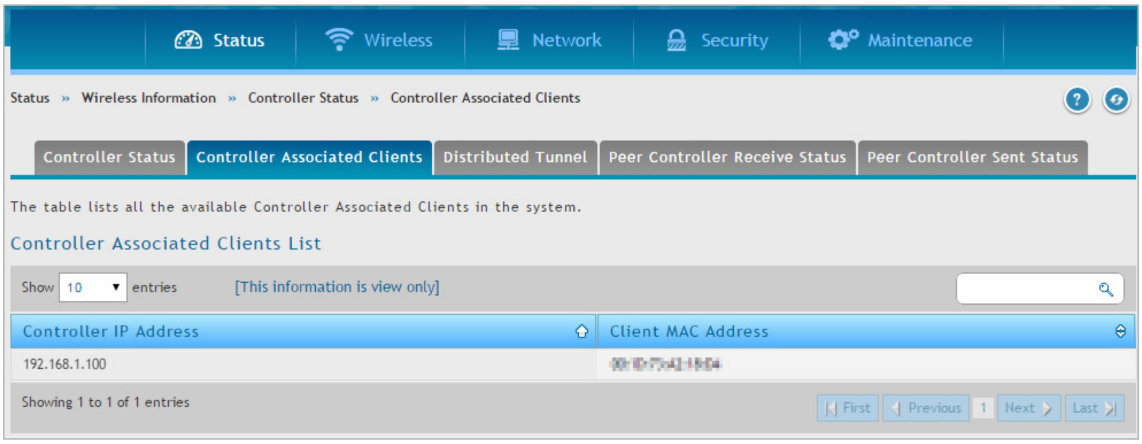


図 8-19　Controller Associated Clients List 画面

以下の項目があります。

項目	説明
Controller IP Address	無線クライアントが接続するアクセスポイントを管理するコントローラの IP アドレスを表示します。
Client MAC Address	接続する無線クライアントの MAC アドレスを表示します。

分散型トンネル

Status > Wireless Information > Controller Status > Distributed Tunnel メニュー

AP-AP トンネルモードは、無線コントローラにデータトラフィックを送信せずに無線クライアントの L3 ローミングをサポートするために使用されます。

AP-AP トンネルモードで、クライアントが最初に無線システムにおいてアクセスポイントに接続する場合、アクセスポイントは、VLAN フォワーディングモードを使用することで無線クライアントのデータを転送します。クライアントが最初に接続するアクセスポイントを「ホーム AP」と呼びます。クライアントがローミングするアクセスポイントを「アソシエーション AP」と呼びます。

Status > Network Information > Controller Status > Distributed Tunnel の順にメニューをクリックし、以下の画面を表示します。

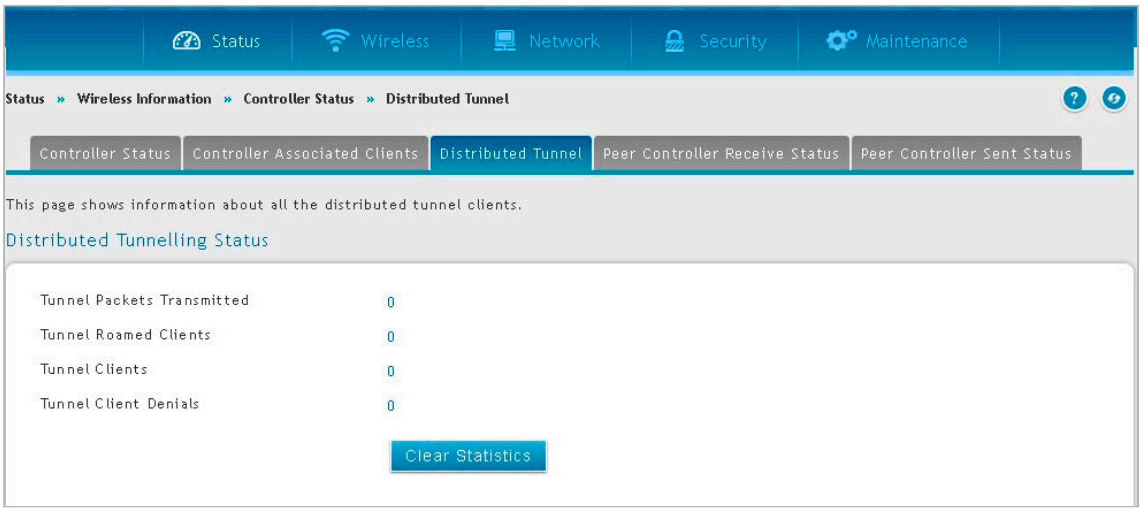


図 8-20　Distributed Tunneling Status 画面

以下の項目があります。

項目	説明
Tunnel Packets Transmitted	すべてのアクセスポイントが分散型トンネル経由で送信したパケットの総数が表示されます。
Tunnel Roamed Clients	分散型トンネルを使用してホーム AP からローミングに成功したクライアントの数が表示されます。
Tunnel Clients	分散型トンネルを使用してアクセスポイントに接続するクライアントの総数が表示されます。
Tunnel Client Denials	クライアントがローミングする際に、システムが分散型トンネルを設定できなかったクライアントの総数が表示されます。

統計情報をリセットするには、「Clear Statistics」ボタンをクリックします。

ピアコントローラの受信状態

Status > Wireless Information > Controller Status > Peer Controller Receive Status メニュー

ピアコントローラ設定機能では、1 つの無線コントローラから他のすべてのコントローラに無線設定を送信します。この機能では、コントローラが同期され、1 つのコントローラからクラスタ内のすべての無線コントローラを管理することができます。「Peer Controller Receive Status」画面では、コントローラがピアの 1 つから受信した設定に関する情報を表示します。

Status > Wireless Information > Controller Status > Peer Controller Receive Status の順にメニューをクリックし、以下の画面を表示します。

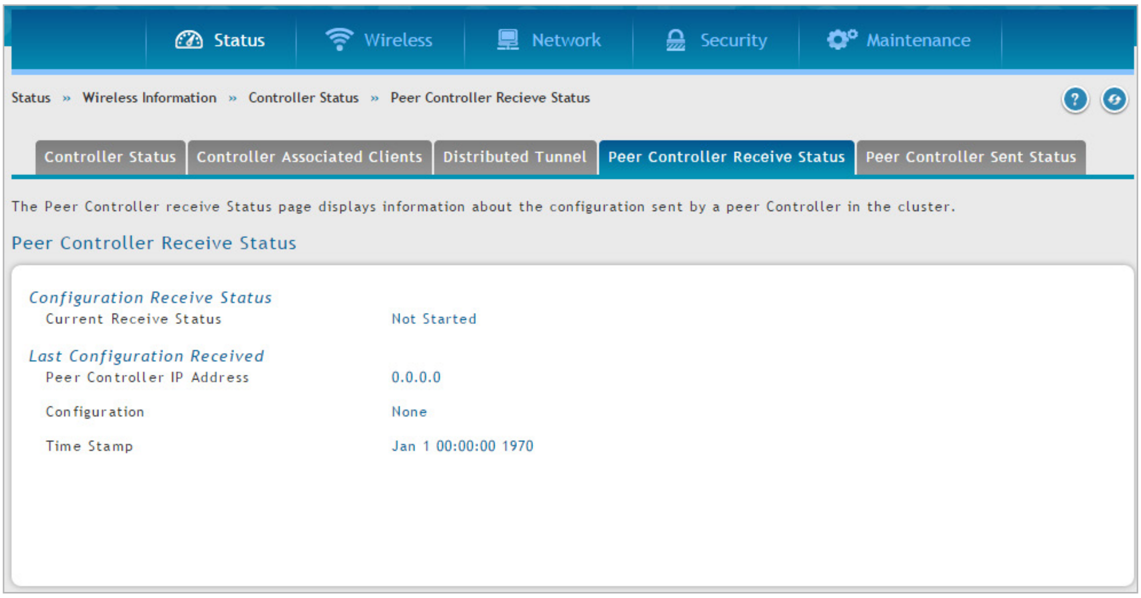


図 8-21　Peer Controller Received Status 画面

以下の項目があります。

項目	説明
Current Receive Status	
Current Receive Status	ピアコントローラから無線設定を受信する場合のグローバルなステータスを表示します。 • Not Started - 開始していません。 • Receiving Configuration - 設定を受信中です。 • Saving Configuration - コンフィグレーションを保存中です。 • Applying AP Profile Configuration - AP プロファイルの設定を適用中です。 • Success - 成功 • Failure - Invalid Code Version - 不正なコードバージョン • Failure-Invalid Hardware Version - 不正なハードウェアバージョン • Failure-Invalid Configuration - 不正なコンフィグレーション
Last Configuration Received	
Peer Controller IP Address	本コントローラが何らかの無線コンフィグレーションデータを受信した際に、データを送信したピアコントローラの IP アドレスを表示します。
Configuration	ピアコントローラから最後に受信したコンフィグレーションの種類を表示します。 • Global • Discovery • Channel/Power • AP Database • AP Profiles • Known Client • Captive Portal • RADIUS Client • QoS ACL • QoS DiffServ • None - 無線コントローラは他のコントローラのコンフィグレーションを何も受信していません。
Time Stamp	この無線コントローラがピアコントローラからコンフィグレーションデータを受信した最後の時間を表示します。

ピアコントローラの送信状態

Status > Wireless Information > Controller Status > Peer Controller Sent Status メニュー

クラスタ内の 1 つのコントローラから別のコントローラに対して、コンフィグレーションを送信することができます。「Peer Controller Sent Status」画面では、クラスタ内でピアコントローラによって送信されたコンフィグレーションの情報を表示します。また、コンフィグレーションを受信した各ピアコントローラの IP アドレスを表示します。

Status > Wireless Information > Controller Status > Peer Controller Sent Status の順にメニューをクリックし、以下の画面を表示します。

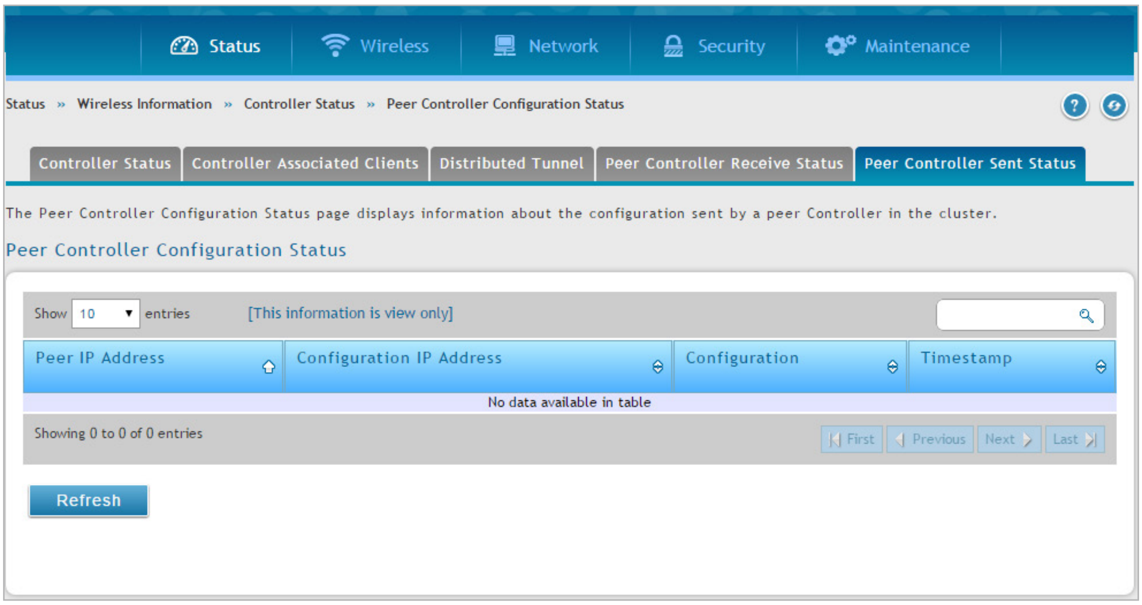


図 8-22　Peer Controller Sent Status 画面

以下の項目があります。

項目	説明
Peer IP Address	コンフィグレーション情報を受信したクラスタ内の各ピアコントローラの IP アドレスを表示します。
Configuration Controller IP Address	コンフィグレーション情報を送信したクラスタ内のコントローラの IP アドレスを表示します。
Configuration	コントローラがピアコントローラから受信したコンフィグレーションの種類を表示します。
Timestamp	コンフィグレーションがコントローラに適用された日時を表示します。時間は UTC で表示されるため、各ピアコントローラが NTP を使用している場合にのみ、本機能を使用できます。

「Refresh」ボタンをクリックすると、情報を更新します。

RADIUS アカウンティング統計

Status > Wireless Information > Radius Accounting Staststics メニュー

RADIUS アカウンティングサーバの統計情報を表示します。

Status > Wireless Information > Radius Accounting Staststics の順にメニューをクリックし、以下の画面を表示します。

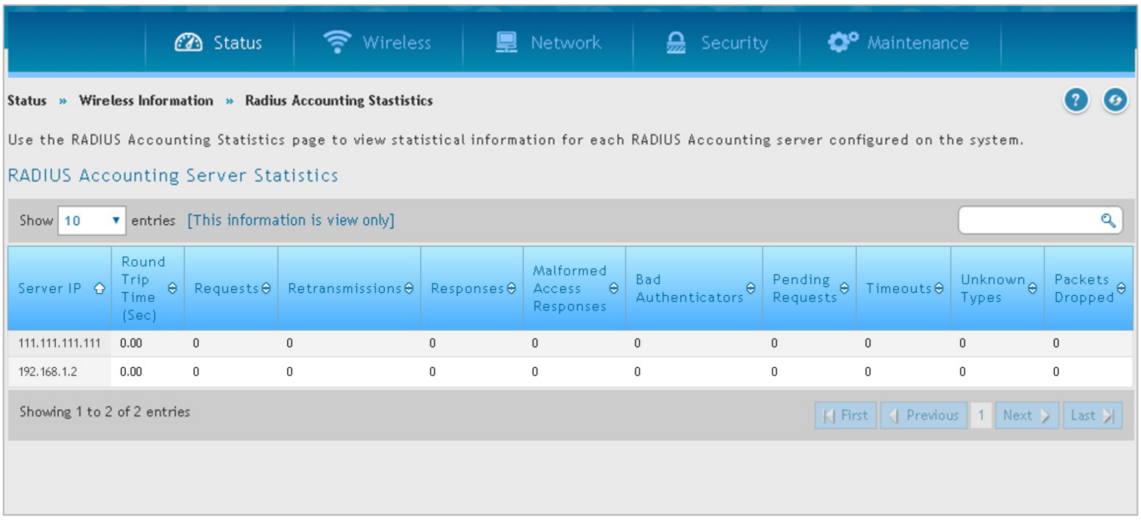


図 8-23　RADIUS Accounting Server Statistics 画面

以下の項目があります。

項目	説明
Server IP	RADIUS アカウンティングサーバの IP アドレスです。
Round Trip Time (Secs)	RADIUS アカウンティングサーバから送信された、一致した最新の Accounting-Response と Accounting-Request の間隔を表示します。（秒）
Requests	サーバに送信された RADIUS アカウンティングリクエストパケット数を表示します。再送信は数に含まれません。
Retransmissions	サーバに再送信された RADIUS アカウンティングリクエストパケット数を表示します。
Responses	サーバから送信されアカウンティングポートで受信した RADIUS アカウンティングパケット数を表示します。
Malformed Access Responses	サーバからの不正な RADIUS Accounting-Response パケットの数を表示します。不正パケットには無効なパケット長が含まれます。不正認証や不明なタイプは不正アカウンティングパケットとしてカウントされません。
Bad Authenticators	サーバから送信された、無効な認証を含む RADIUS Accounting-Response の受信パケット数を表示します。
Pending Requests	タイムアウトしていない、または応答を受信した、サーバ宛の RADIUS Accounting-Request パケット数を表示します。
Timeouts	サーバのタイムアウト回数を表示します。
Unknown Types	サーバから送信されアカウンティングポートで受信した不明な種類の RADIUS パケットの数を表示します。
Packets Dropped	サーバから送信されアカウンティングポートで受信し、破棄された RADIUS パケットの数を表示します。

「Refresh」ボタンをクリックすると、情報を更新します。

アクセスポイント情報の参照

アクセスポイントの統計情報を表示します。

Global Status

Status > Wireless Information > Access Point > Global Status メニュー

無線コントローラが検出したアクセスポイント に関するサマリ情報を表示します。

Status > Wireless Information > Access Point > Global Status の順にメニューをクリックし、以下の画面を表示します。

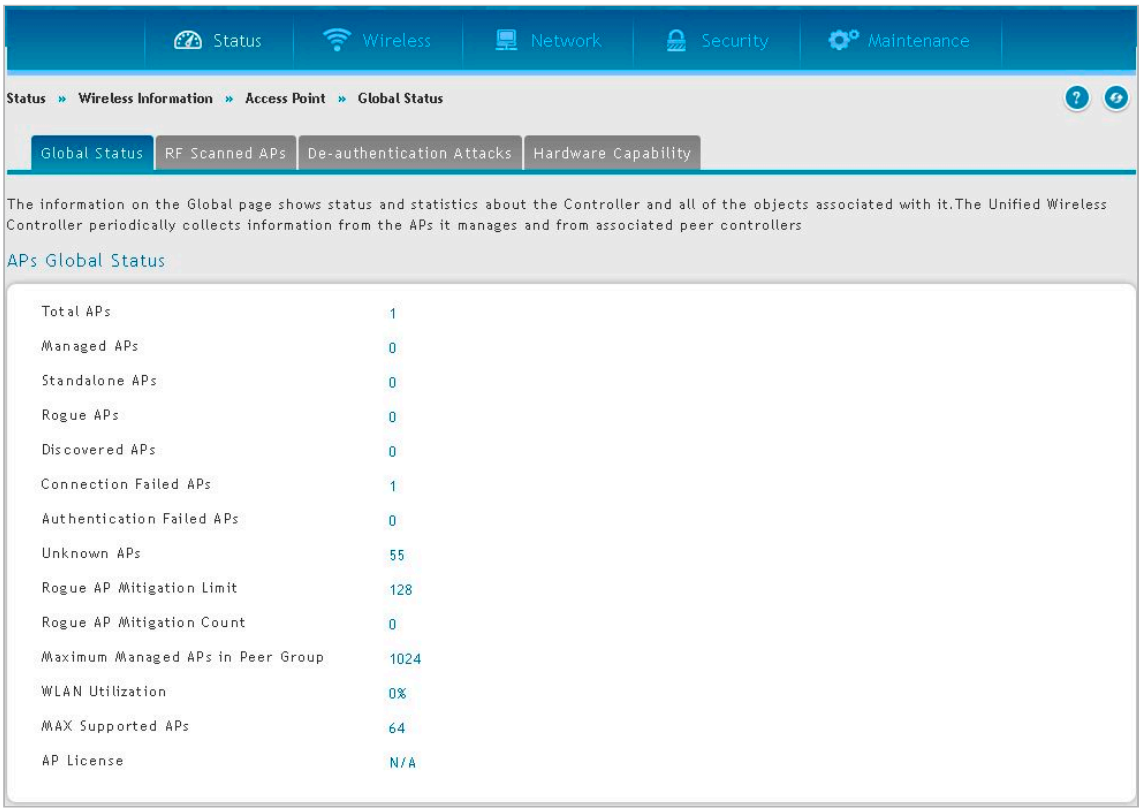


図 8-24　APs Global Status 画面

以下の項目があります。

項目	説明
Total APs	データベース内の管理対象アクセスポイントの総数を表示します。この値は常に「Managed APs」、「Connection Failed APs」、「Discovered APs」の値の合計と等しくなります。
Managed APs	管理対象 AP データベース内のアクセスポイント数を表示します。これらは、認証、設定が完了しており、無線コントローラとアクティブな接続が確立されているアクセスポイントです。
Standalone APs	Standalone モードの信頼済みアクセスポイント数を表示します。コントローラは、Standalone モードのアクセスポイントを管理しません。
Rogue APs	現在 WLAN 上で検出されている不正アクセスポイントの数を表示します。アクセスポイントが RF スキャンを実行する際、認知されていないアクセスポイントを検出する場合があります。このようなアクセスポイントを「Rogue」（不正）として報告します。
Discovered APs	コントローラと接続し、完全には設定が完了していないアクセスポイントを表示します。これには「Discovered」（検出）または「Authenticated」（認証）状態のすべての管理アクセスポイントが含まれます。
Connection Failed APs	以前に認証され、スイッチの管理下にあったものの、現在は無線コントローラとの間に接続が確立されていないアクセスポイントの数を表示します。
Authentication Failed APs	ファストパス無線統合コントローラとの通信の確立に失敗したアクセスポイント数を表示します。
Unknown APs	現在 WLAN 上に検出されている「Unknown」（未知）のアクセスポイントの数を表示します。無線コントローラが管理するように設定済みのアクセスポイントが、アクティブに管理されていない時に RF スキャンを通じて検出されると、「Unknown」（未知）のアクセスポイントとして分類されます。
Rogue AP Mitigation Limit	システムが認証解除フレームを送信できるアクセスポイントの最大数を表示します。
Rogue AP Mitigation Count	不正なアクセスポイントを減らすために、現在、無線システムが認証解除メッセージを送信しているアクセスポイントの数を表示します。0 の値は、軽減が行われていないことを示します。
Maximum Managed APs in Peer Group	クラスタが管理するアクセスポイントの最大数を表示します。

項目	説明
WLAN Utilization	本コントローラの管理下にあるすべてのアクセスポイントのネットワーク使用率を表示します。本値はグローバル統計値を基にしています。
MAX Supported APs	本コントローラがサポートするアクセスポイントの数です。
AP License	本コントローラがサポートできるライセンスが有効なアクセスポイントの数です。

RF スキャンで検出されたアクセスポイント

Status > Wireless Information > Access Point > RF Scanned APs メニュー

アクセスポイントの無線帯域では、定期的に無線周波数をスキャンすることで、範囲内の他のアクセスポイントや無線クライアントの情報を収集します。通常の動作モードでは、アクセスポイントは、常に無線帯域で動作可能なチャンネルのスキャンをします。本ページでは、無線コントローラが検出した他のアクセスポイントおよび無線クライアントに関する情報を表示します。

Status > Wireless Information > Access Point > RF Scanned APs の順にメニューをクリックし、以下の画面を表示します。

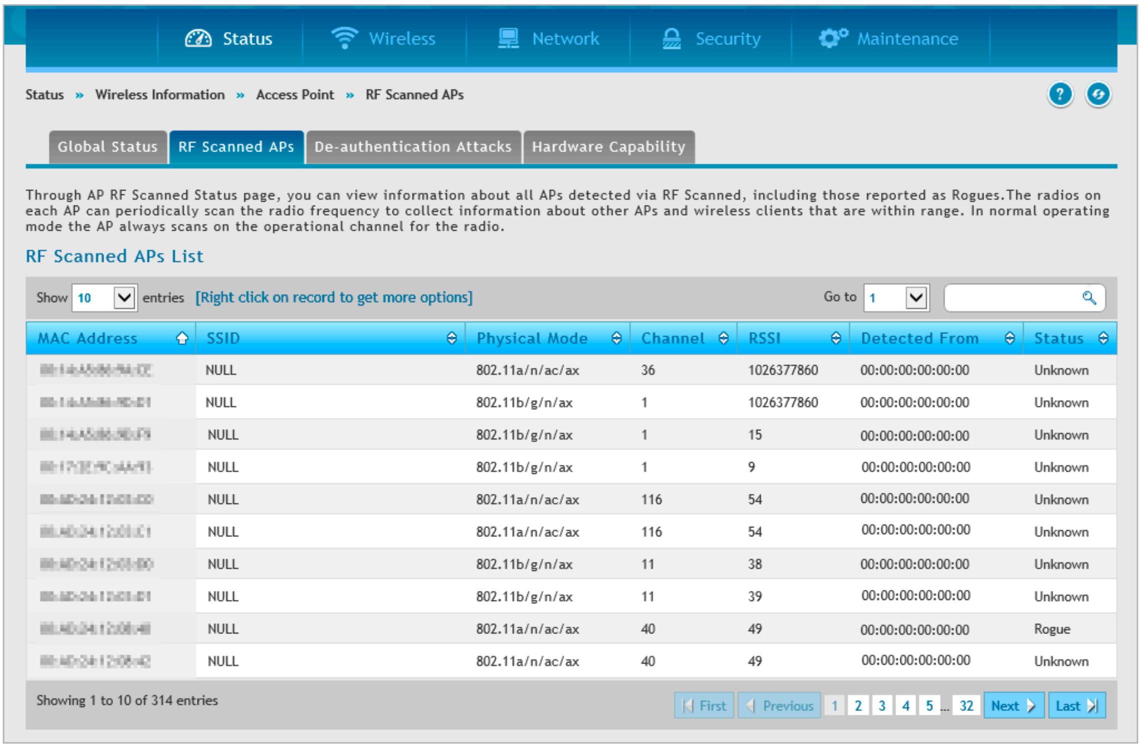


図 8-25　RF Scanned APs List 画面

以下の項目があります。

項目	説明
MAC Address	検出したアクセスポイントのイーサネット MAC アドレスを表示します。これは、物理的な無線インタフェースまたは VAP の MAC アドレスです。
SSID	ネットワークの無線名（SSID）で、ブロードキャストされたビーコンフレームから検出します。
Physical Mode	アクセスポイントで使用している 802.11 のモードを表示します。
Channel	アクセスポイントの送信チャンネルを表示します。
RSSI	受信信号の強さの指標となる数値が表示されます。1-100 の範囲で示され、1 が最も小さい信号の強さとなります。
Detected From	どの AP 上で RF スキャンにより検出されたかを示します。
Status	アクセスポイントの管理状態を表示します。 • Managed - Neighbour アクセスポイントは、無線システムにより管理されています。 • Standalone - アクセスポイントは、スタンドアロンモードで管理され、Valid AP エントリ（ローカルまたは RADIUS）として設定されています。 • Rogue - アクセスポイントは、脅威検出アルゴリズムの 1 つによって脅威として分類されています。 • Unknown - アクセスポイントは、ネットワークで検出されますが、脅威検出アルゴリズムは脅威として分類しません。

アクセスポイントまたはクライアントを右クリックして、オプションを起動します。

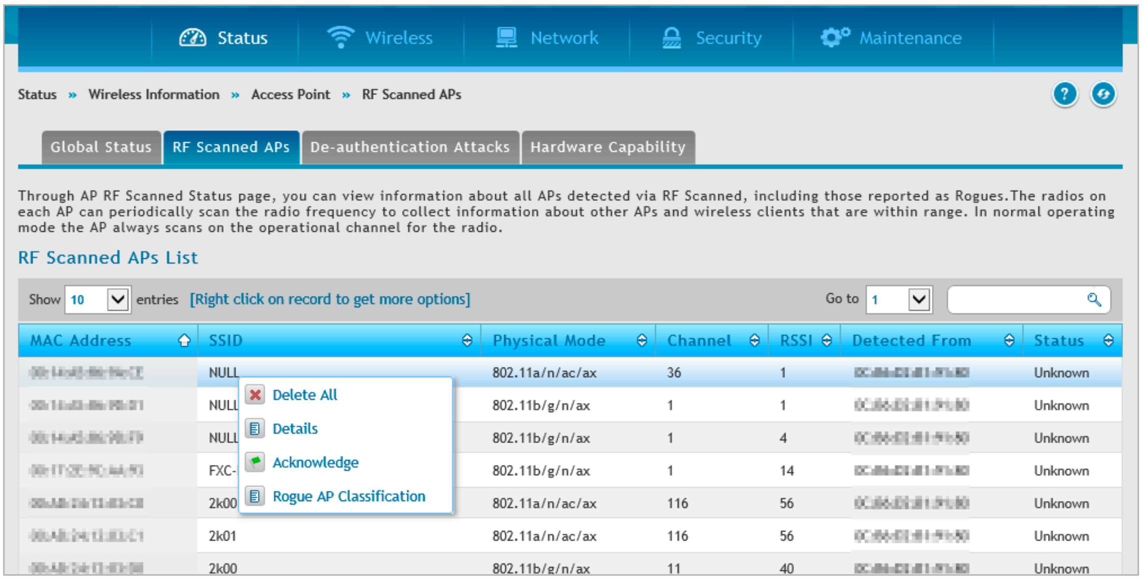


図 8-26　RF Scan APs List 画面 - オプションメニュー

以下のオプションメニューがあります。

項目	説明
Delete All	すべてのエントリを削除します。
Details	「Rogue」（不正）として報告されたものを含む RF スキャンで検出されたすべてのアクセスポイントに関する情報を表示します。
Acknowledge	アクセスポイントの不正状態をクリアします。
Rogue AP Classification	脅威検出テストのリストを表示します。

アクセスポイントを右クリックして、「Details」を選択すると、以下の画面が表示されます。

図 8-27　AP RF Scan Detailed Status 画面

以下の項目があります。

項目	説明
MAC Address	検出されたアクセスポイントの MAC アドレスを表示します。これは、物理的な無線インタフェースまたは VAP の MAC アドレスです。D-Link アクセスポイントの場合は常に VAP の MAC アドレスとなります。
BSSID	ビーコンフレーム内の BSSID（Basic Service Set Identifier）を表示します。
SSID	ネットワークの SSID を表示します。ブロードキャストされたビーコンフレームから検出します。
Physical Mode	アクセスポイントで使用している 802.11 のモードを表示します。
Channel	アクセスポイントの通信チャンネルを表示します。
Security Mode	アクセスポイントが使用するセキュリティモードを表示します。

項目	説明
Status	Neighbour アクセスポイントの管理状況を示します。スイッチに認識されている有効なアクセスポイントであるか、または Rogue（不正）と見なされるかなどの情報を取得できます。 ・Managed - Neighbour アクセスポイントは、無線システムにより管理されています。 ・Standalone - アクセスポイントは、スタンドアロンモードで管理され、Valid AP エントリ（ローカルまたは RADIUS）として設定されています。 ・Rogue - 不正なアクセスポイントは脅威検出アルゴリズムの 1 つによって脅威として分類されています。 ・Unknown - アクセスポイントは、ネットワークで検出されますが、脅威検出アルゴリズムは脅威として分類しません。
802.11n Mode	本アクセスポイントが IEEE 802.11n モードをサポートするかどうかを表示します。
Initial Status	アクセスポイントが不正でない場合、初期ステータスは Status（「Managed」、「Standalone」、または「Unknown」）と同じです。不正アクセスポイントについては、初期ステータスは Rogue になる前の分類となります。
Beacon Interval	Neighbour アクセスポイントのネットワークへのビーコン間隔を表示します。
Transmit Rate	アクセスポイントの現在の送信速度を表示します。
Highest Supported Rate	ビーコンフレームの中で本アクセスポイントが通知した最も高いサポートレートを表示しますト。レートは、Mbps 単位で表示されます。
WIDS Rogue AP Mitigation	Rogue アクセスポイントの移行がこのアクセスポイントで進行しているかどうかを示す状況を表示します。
Peer Managed AP	ピア管理の AP かどうかを表示します。
Age	起動時間を表示します。
Ad HOC Network	アドホックネットワークかどうかを表示します。
Discovered Age	検出からの時間を表示します。
OUI Description	OUI の概要を表示します。

アクセスポイントを右クリックして、「Rogue AP Classification」を選択すると、以下の画面が表示されます。

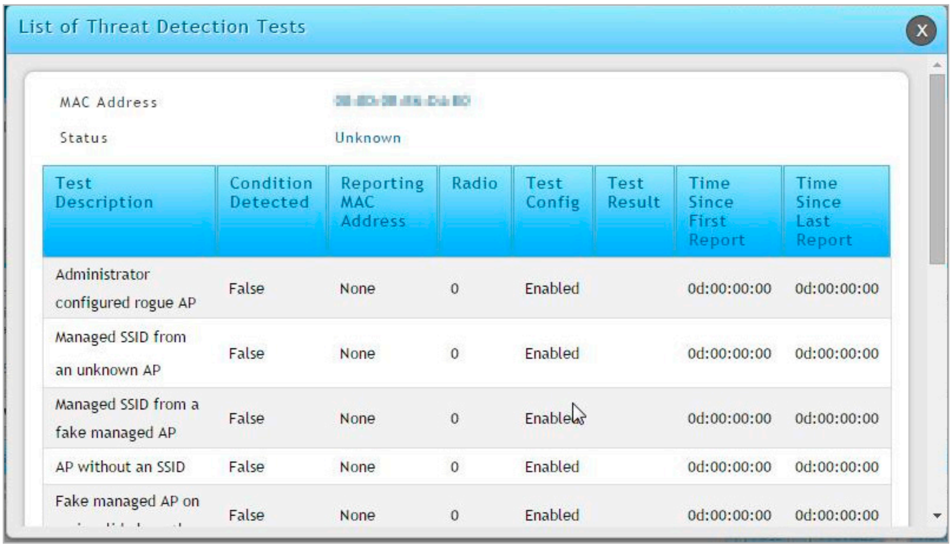


図 8-28　 List of Threat Detection Tests 画面

De-Authentication Attacks

Status > Wireless Information > Access Point > De-authentication Attacks メニュー

認証解除攻撃の画面では、クラスタコントローラが攻撃を行った不正なアクセスポイントに関する情報を表示します。無線コントローラは、認証解除メッセージを不正なアクセスポイントに送信することで、不正なアクセスポイントから防御できます。無線システムが本機能を動作させるためには、認証解除攻撃機能をグローバルに有効にする必要があります。攻撃機能を有効にする前に、正当なアクセスポイントが「Rogue」（不正）として分類されていないことをご確認ください。本機能は初期値では無効になっています。

無線システムは、同時に 16 個のアクセスポイントに対して認証解除攻撃を行うことができます。この攻撃の目的は、不正なアクセスポイントが検出され、無効になるまでの一時的な方法として動作することです。

認証解除攻撃は、すべての不正なタイプに有効なものではないため、検出された不正なアクセスポイントのすべてには使用されません。以下の不正なアクセスポイントには攻撃を行うことはできません。

- 検出された不正アクセスポイントが有効な管理アクセスポイントの BSSID を偽造している場合、その攻撃が正しいアクセスポイントへのサービスを拒否し、ハッカーがシステムを攻撃するように別の手段を提供する可能性があるため、無線システムは攻撃を行いません。
- Ad hoc ネットワークにおける認証解除攻撃は、これらが認証を使用しないため有効ではありません。
- カントリードメインが認可するチャンネル以外で動作するアクセスポイントは、不正チャンネルにおけるどんなトラフィックの送信も法律に反しているため、攻撃されません。

無線コントローラは、認証解除攻撃を行っている BSSID のリストを保持します。コントローラは、あらゆる管理アクセスポイントに対して、不正なアクセスポイントが動作している BSSID とチャンネルのリストを送信します。

Status > Wireless Information > Access Point > De-authentication Attacks の順にメニューをクリックし、以下の画面を表示します。

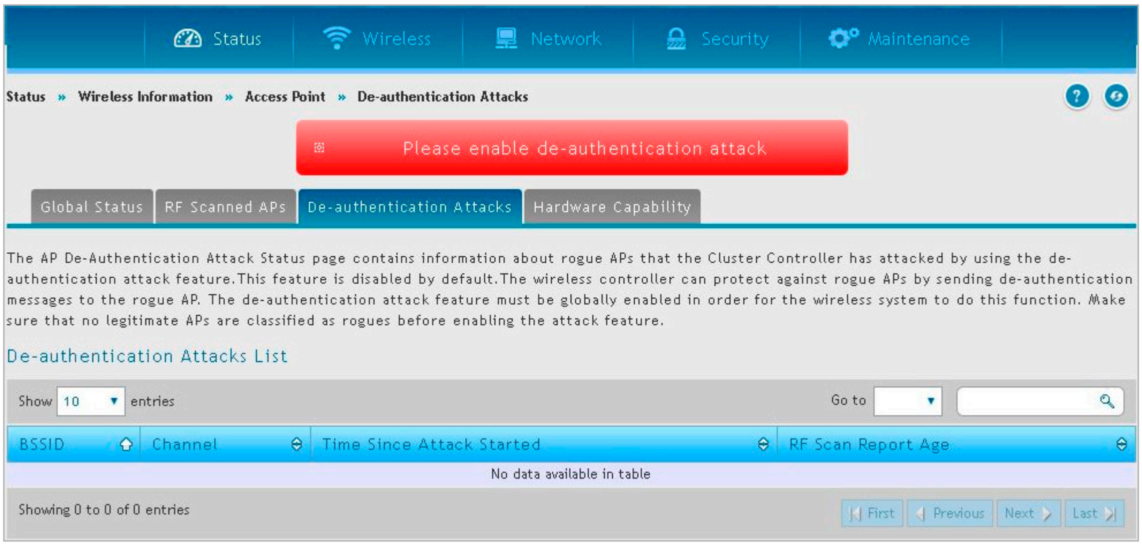


図 8-29　De-Authentication Attacks List 画面

以下の項目があります。

項目	説明
BSSID	攻撃を開始するアクセスポイントの BSSID を参照します。BSSID は MAC アドレスです。
Channel	不正なアクセスポイントが動作しているチャンネルを表示します。
Time Since Attack Started	アクセスポイントが起動してから経過した時間を表示します。
RF Scan Report Age	RF スキャンがこのアクセスポイントを報告してから経過した時間を表示します。

Hardware Capability

Status > Wireless Information > Access Point > Hardware Capability メニュー

無線コントローラは、無線帯域、サポートする IEEE 802.11 モード、およびソフトウェアイメージなど異なるハードウェア機能を持つアクセスポイントをサポートしています。ここでは、アクセスポイントにダウンロードできるソフトウェアイメージをはじめ、アクセスポイントがサポートする無線ハードウェアや IEEE モードに関する情報を表示します。

Status > Wireless Information > Access Point > Hardware Capability の順にメニューをクリックし、以下の画面を表示します。

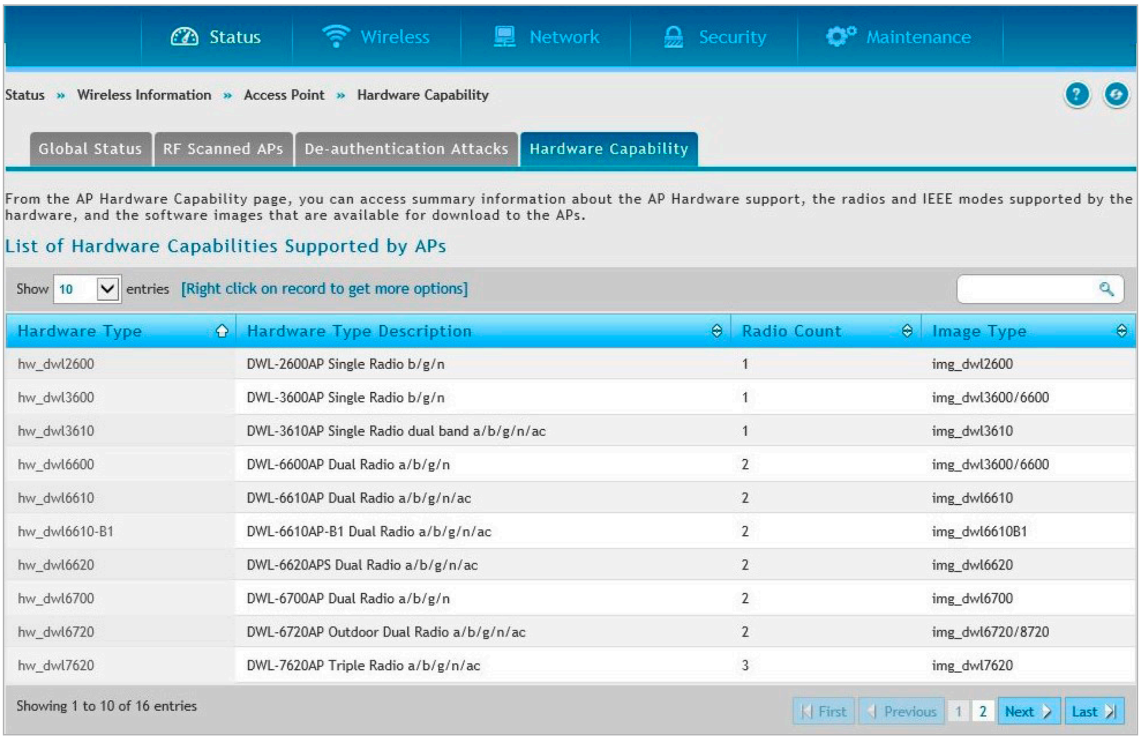


図 8-30　List of Hardware Capabilities Supported by APs 画面

以下の項目があります。

項目	説明
Hardware Type	各アクセスポイントのハードウェアタイプに割り当てられた識別名を表示します。
Hardware Type Description	プラットフォームとサポートしている IEEE 802.11 モードを表示します。
Radio Count	ハードウェアがサポートする無線インタフェースの個数（1、2、または 3）を表示します。
Image Type	ハードウェアが要求するソフトウェアのタイプを表示します。

右クリックオプションで「Radio Information」を選択し、指定したハードウェアタイプについて無線インタフェースの情報を表示します。

図 8-31　AP Hardware Radio Capability 画面

管理アクセスポイント

Wireless > Access Point > AP List > Managed メニュー

管理されているアクセスポイントに関する詳細を表示します。

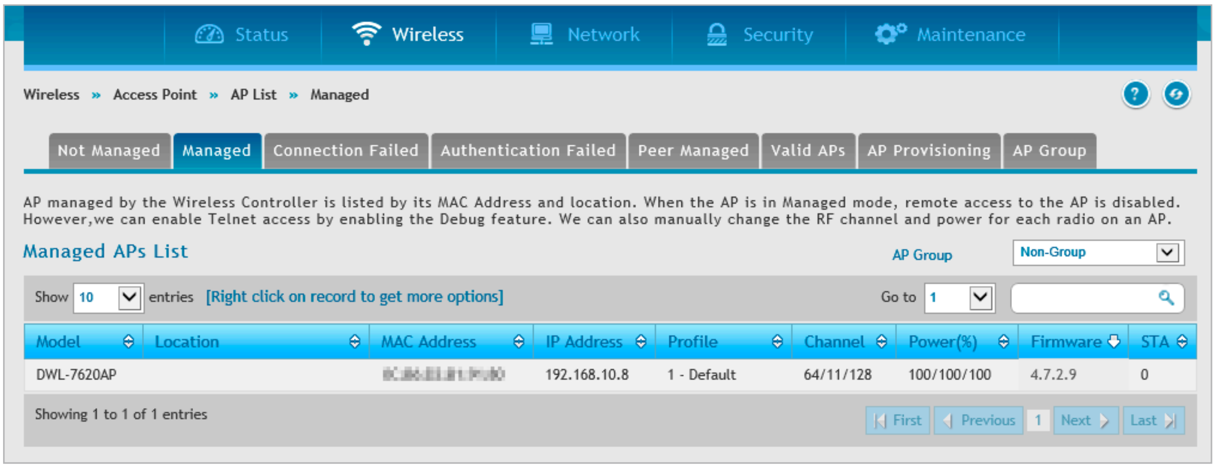


図 8-32　Managed APs List 画面

以下の項目があります。

項目	説明
Model Name	管理対象のアクセスポイントのモデル名を表示します。
Location	アクセスポイントが物理的に位置している場所に関するオプションの説明を表示します。
MAC Address (*)	管理対象のアクセスポイントのイーサネットアドレスを表示します。アスタリスク (*) が MAC アドレスに続く場合、アクセスポイントはピアコントローラに管理されています。
IP Address	管理対象のアクセスポイントの IP アドレスを表示します。
Profile	管理対象のアクセスポイントに対して設定されているプロファイルを表示します。プロファイルは Valid AP データベースに存在するアクセスポイントに対して割り当てられます。
Channel	無線モード及び AP が動作する国に基づく利用可能なチャンネルを表示します。手動によりチャンネルを変更すると AP プロファイルの設定は上書きされますが、AP 再起動やプロファイル再適用時に保持されません。
Power	チャンネルの送信電波出力を表示します。
Firmware	管理対象のアクセスポイントのファームウェアバージョンを表示します。
STA	ステーションを表示します。

管理されているアクセスポイントを右クリックすると、オプションメニューを選択できます。

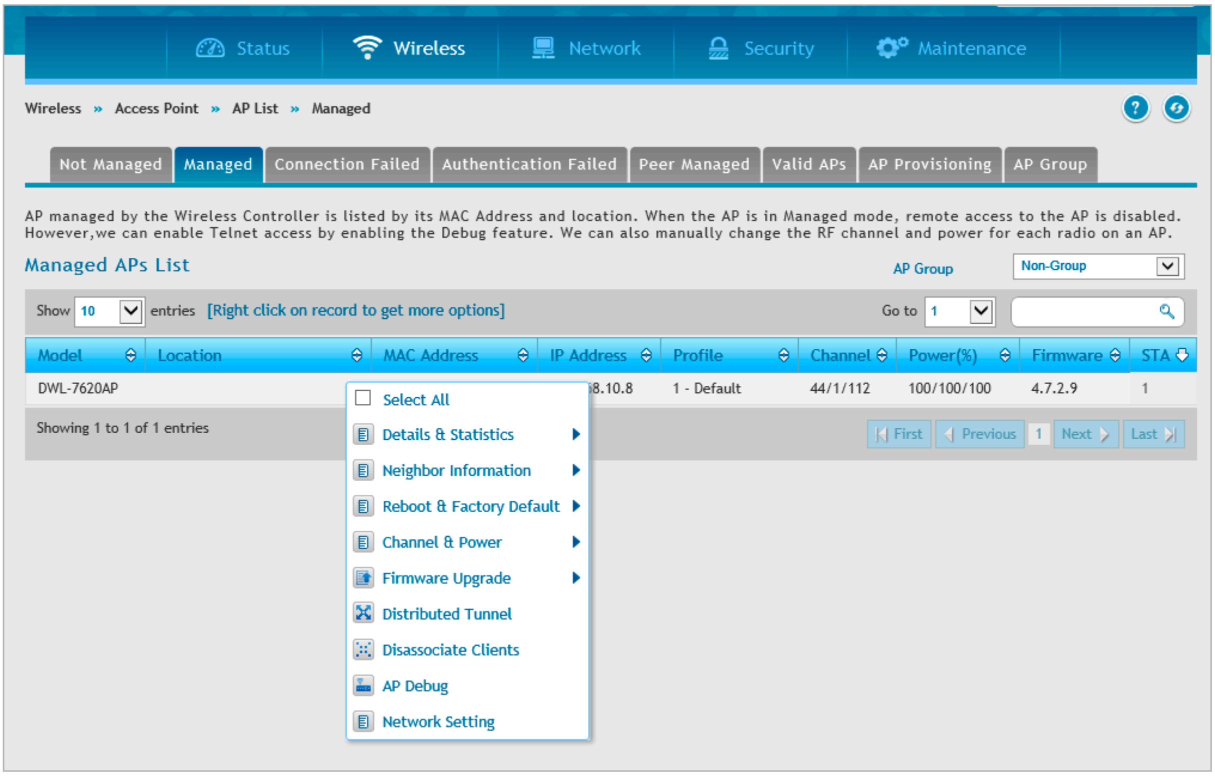


図 8-33　Managed APs List 画面

以下のメニューがあります。

項目	説明
Details & Statistics	以下のメニューが表示されます。 • AP Details - アクセスポイントから収集した詳細なステータス情報を表示します。 • Radio Details - 無線インタフェースの詳細なステータスを表示します。 • VAP Details - 選択したアクセスポイント上の仮想アクセスポイント（VAP）や、無線コントローラが管理するアクセスポイントの無線インタフェースに関するサマリ情報を表示します。 • AP Statistics - アクセスポイントが送受信したパケット数と種類を表示します。 • Radio Statistics - アクセスポイントが送受信したパケット数と種類の情報を無線インタフェースごとに表示します。 • VAP Statistics - アクセスポイントが送受信したパケット数と接続に失敗した無線クライアント数の情報を VAP ごとに表示します。
Neighbor Information	以下のメニューが表示されます。 • Neighbour APs - 指定したアクセスポイントが、選択した無線インタフェース上で周期的な RF スキャンを行って検出した隣接アクセスポイントを表示します。 • Neighbour Clients - アクセスポイントに接続中、またはアクセスポイントの無線インタフェースが検出した無線クライアントの情報を表示します。
Reboot & Factory Default	以下のメニューが表示されます。 • Reboot AP - 管理するアクセスポイントを再起動します。 • Factory Reset - 管理するアクセスポイントを工場出荷時設定に戻します。
Channel & Power	無線モード毎にチャンネルと電力の情報を表示します。
Firmware Upgrade	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。
Distributed Tunnel	現在、アクセスポイントで使用中の L2 トンネルに関する情報を表示します。
Disassociate Clients	選択したアクセスポイントからクライアントを切断します。
AP Debug	デバッグモードを有効化します。 設定内容については「AP デバッグモードの設定」を参照してください。
Network Setting	アクセスポイントのネットワーク設定を行います。

AP Details

「Managed APs List」内のエントリを右クリックして、「Details & Statistics > AP Details」を選択します。

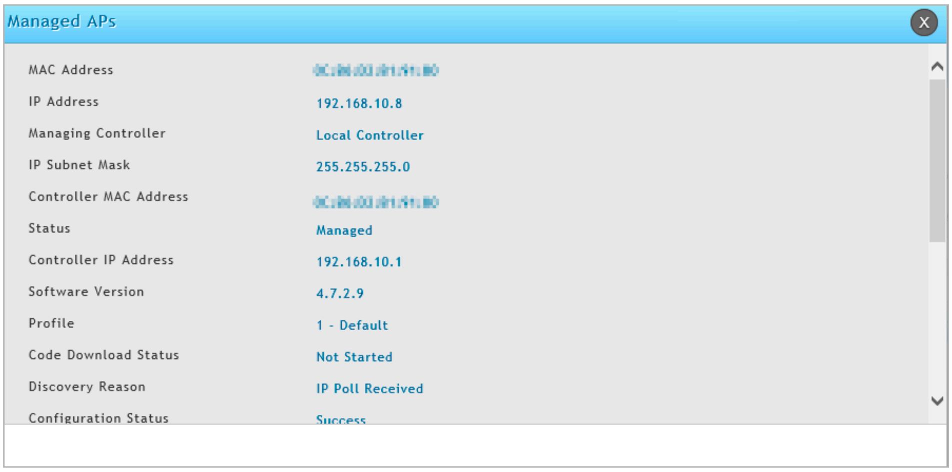


図 8-34　AP Details 画面

以下の項目があります。

項目	説明
MAC Address	統合無線コントローラ管理下にあるアクセスポイントのイーサネットアドレスを表示します。 アクセスポイントの MAC アドレスの後に (*) が続いている場合、ピアコントローラが管理しています。
IP Address	管理対象のアクセスポイントの IP アドレスを表示します。
Managing Controller	アクセスポイントがローカルコントローラまたはピアコントローラによって管理されるかどうかを示します。
IP Subnet Mask	管理対象のアクセスポイントのサブネットマスクを表示します。
Controller MAC Address	アクセスポイントを管理しているコントローラの MAC アドレスを表示します。
Status	アクセスポイントの状態を示します。 • Discovered - コントローラが検出しましたが、まだ認証状態ではありません。 • Authenticated - コントローラが認可および認証しました（認証を有効に設定している場合）が、AP プロファイル設定を適用していません。 • Managed - AP プロファイル設定が適用され、「Managed」モードで動作中です。 • Connection Failed - 統合無線コントローラはアクセスポイントとの接続を喪失しました。エラーのエントリは管理者が削除するまでは管理 AP データベースに残ります。管理下のアクセスポイントは再起動中「Failed」と表示されることがあります。 注意　管理の接続性を喪失している場合、アクセスポイントの両インタフェースはダウンします。アクセスポイントに接続するすべてのクライアントの接続が解除されます。コントローラによって再度管理されると、アクセスポイントの無線インタフェースは動作状態になります。
Controller IP Address	アクセスポイントを管理しているコントローラの IP アドレスを表示します。
Software Version	アクセスポイントのソフトウェアバージョンを表示します。アクセスポイントの検出時に取得される情報です。
Profile	管理下のアクセスポイントに現在適用されている AP プロファイルを表示します。プロファイルは Valid AP データベース内のアクセスポイントに適用されています。 注意　アクセスポイントが検出されて統合無線コントローラの管理下に入ると、その後プロファイルが Valid AP データベース内（ローカルまたは RADIUS サーバ）で変更され、新しいプロファイルが適用される場合、そのアクセスポイントは自動的に再起動します。
Code Download Status	アクセスポイントに対するソフトウェアのダウンロードリクエストの状態を示します。 • Not Started - ダウンロードを開始していません。 • Requested - このアクセスポイントにダウンロードが計画されていますが、現在のダウンロードグループにアクセスポイントがないため、ダウンロードの開始がまだ伝えられていません。 • Code-Transfer-In-Progress - アクセスポイントはソフトウェアのダウンロードを通知しました。 • Failure - アクセスポイントはソフトウェアのダウンロードの失敗を報告しました。 • Aborted - アクセスポイントが TFTP サーバよりソフトウェアのロードを行う前にダウンロードは中止されました。 • Waiting-For-APs-To-Download - ダウンロードはこのアクセスポイントで終了し、他のアクセスポイントのダウンロード終了を待っています。この状態では Reset コマンドはアクセスポイントに送信されません。 • NVRAM-Update-In-Progress - ダウンロードに成功しました。Reset コマンドがアクセスポイントに送信されました。 • Timed-Out - アクセスポイントは設定時間内に無線コントローラに再接続しませんでした。

項目	説明
Discovery Reason	アクセスポイントを検出した方法を表示します。 • IP Poll Received - 無線コントローラから実施した IP ポーリングによりアクセスポイントを検出しました。IP アドレスは IP ポーリングリストに設定されます。 • Peer Redirect - アクセスポイントはピアコントローラからのリダイレクトにより検出されました。アクセスポイントは他のピアコントローラへの接続を試みて、そのピアコントローラから現在の統合無線コントローラの IP アドレスを学習しました。（アクセスポイントを認可する時、ピアは統合無線コントローラの IP アドレスを RADIUS サーバからの応答により学習しました。） • Controller IP Configured - 管理下のアクセスポイントに無線コントローラの IP アドレスが設定されています。 • Controller IP DHCP - 管理下のアクセスポイントは、DHCP サーバより IP アドレスを取得しました。 • L2 Poll Received - アクセスポイントは、D-Link 無線デバイス検出プロトコルにより検出されました。
Configuration Status	アクセスポイントに割り当てられているプロファイルで設定が成功したかどうかを確認できます。 • Not Configured - アクセスポイントにプロファイルがまだ送信されていません。アクセスポイントは検出された可能性がありますが、まだ認証されていません。 • In Progress - 現在コントローラからアクセスポイントに対して AP プロファイルコンフィグレーションパケットを送信中です。 • Success - すべてのプロファイルがアクセスポイントに送信され、コンフィグレーションエラーは認められませんでした。 • Partial Success - すべてのプロファイルがアクセスポイントに送信され、コンフィグレーションエラーが発生しましたが、アクセスポイントは使用可能です。 • Failure - プロファイルがアクセスポイントに送信されましたが、コンフィグレーションエラーが発生しました。アクセスポイントは使用できません。
Protocol	アクセスポイントのソフトウェアがサポートするプロトコルバージョンを表示します。アクセスポイントの検出の際に学習される情報です。
Vendor ID	アクセスポイントのソフトウェアのベンダを表示します。アクセスポイントの検出時に学習されます。
Authenticated Clients	アクセスポイントに接続し、認証されたクライアントの数を表示します。アクセスポイント上で動作中のすべての VAP に認証されたクライアントの合計です。
Part Number	アクセスポイントのハードウェアパート番号を表示します。アクセスポイントの検出の際に学習されます。
System Uptime	前回のアクセスポイントのパワーオンリセットから経過した時間（秒）を表示します。
Serial Number	アクセスポイントのシステムのシリアル番号を表示します。
Age	統合無線コントローラとアクセスポイント間との最後の通信から経過した時間を表示します。
Hardware Type	アクセスポイントのハードウェアプラットフォームを表示します。アクセスポイントの検出の際に学習されます。
Scheduler Status	割り当てプロファイルの無線スケジューラの状態を表示します。
AP Debug	AP デバッグの状態を表示します。

Radio Details

「Managed APs List」内のエントリを右クリックして、「Details & Statistics > Radio Details」を選択します。

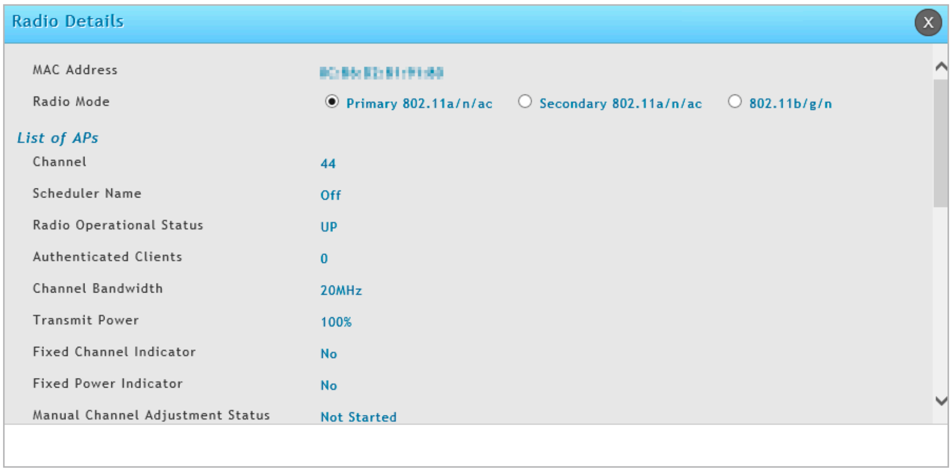


図 8-35　Radio Details 画面

以下の項目があります。

項目	説明
MAC Address	管理アクセスポイントのイーサネットアドレスを表示します。
Radio Mode	無線の接続モードを選択します。
List of APs	
Channel	無線インタフェースが有効な場合、現在動作状態にあるチャンネルを表示します。
Scheduler Name	スケジューラ名を表示します。
Radio Operational Status	無線状況を表示します。
Authenticated Clients	物理無線帯域にあるアクセスポイントが認証したクライアントの合計数を表示します。無線インタフェースで有効な各 VAP に対してアクセスポイントが認証したクライアントの総数です。
Channel Bandwidth	チャンネル帯域幅（20MHz、40MHz、80MHz、80+80 MHz、または 160MHz）を表示します。
Transmit Power	無線帯域の現在の送信出力を表示します。
Fixed Channel Indicator	固定チャンネルが設定され、無線インタフェースに割り当てられているかを示しています。固定チャンネルは Valid AP データベース（ローカルまたは RADIUS サーバ）で設定できます。
Fixed Power Indicator	固定送信出力が設定され、無線インタフェースに割り当てられているかを示しています。固定送信出力は Valid AP データベース（ローカルまたは RADIUS サーバ）で設定できます。
Manual Channel Adjustment Status	チャンネルを変更する手動リクエストの現在の状況を示しています。 • Not Started - チャンネル変更のリクエストが発行されていません。 • Requested - ユーザがチャンネル変更のリクエストを発行しましたが、コントローラはまだ処理をしていません。 • In Progress - コントローラは本無線インタフェースでチャンネル変更リクエストを処理中です。 • Success - チャンネル変更リクエストは完了しました。 • Failure - チャンネル変更リクエストは失敗しました。
Manual Power Adjustment Status	電力調整の手動リクエストの現在の状況を表示します。
WLAN Utilization	物理無線帯域のネットワーク利用量の合計を表示します。本値は無線帯域の統計情報に基づきます。
Total Neighbours	RF エリア内の指定帯域内で隣接するデバイス（アクセスポイントとクライアントの両方）の数を表示します。
Radio Resource Management	無線リソース管理の有効 / 無効を表示します。
Force Roaming	強制ローミングの有効 / 無効を表示します。
Force Roaming Threshold	強制ローミングのしきい値を表示します。
Radar Status	
Supported Channel	トラフィックの送受信に使用される無線チャンネルを表示します。
Radar Detection Enabled	規制範囲によっては、5GHz 帯域のチャンネルで無線モードの検出が必要です。チャンネルで無線モードの検出が必要な場合、アクセスポイントは、他の無線機器の混信を避けるために 802.11h 仕様を使用します。
Radar Detected	他の 802.11 デバイスがそのチャンネルで検出されたかどうかを表示します。
Radar Detected Time	デバイスが最後にチャンネルで検出されてから経過した時間を表示します。

VAP Details

「Managed APs List」内のエントリを右クリックして、「VAP Details」を選択します。

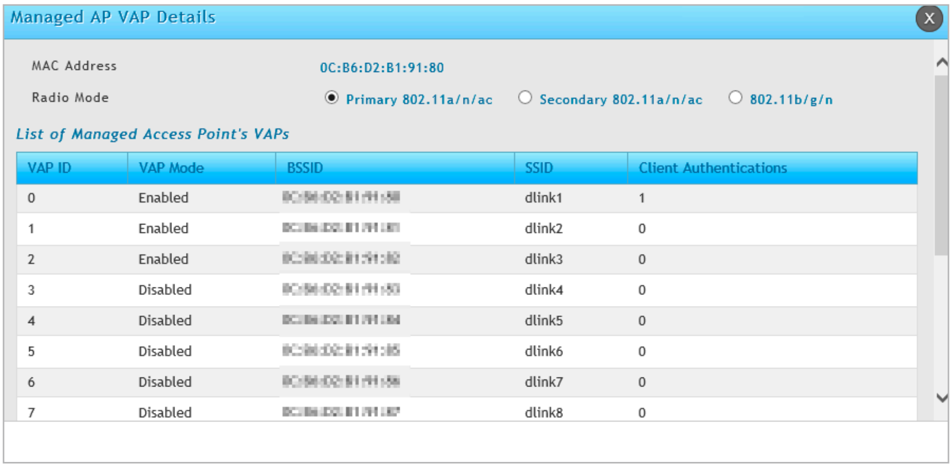


図 8-36　Managed AP VAP Details 画面

以下の項目があります。

項目	説明
MAC Address	管理下のアクセスポイントの MAC アドレスを表示します。
Radio Mode	無線の接続モードを選択します。
List of Managed Access Point's VAPs VAP ID	
VAP ID	VAP を識別するために使用される ID（0-15）で、これは、CLI / SNMP 経由の設定用に VAP を識別するために使用します。
VAP Mode	VAP モード（有効または無効）を表示します。VAP の設定後、有効にした VAP のみが、ビーコンの送信やクライアントと接続できます。
BSSID	VAP のイーサネットアドレスを表示します。
SSID	VAP に割り当てたネットワークを表示します。各 VAP のネットワークは AP プロファイル内で設定され、SSID はネットワークコンフィグレーションに基づいています。
Client Authentications	現在 VAP が認証しているクライアントの合計数を表示します。

AP Statistics

「Managed APs List」内のエントリを右クリックして、「Details & Statistics > AP Statistics」を選択します。

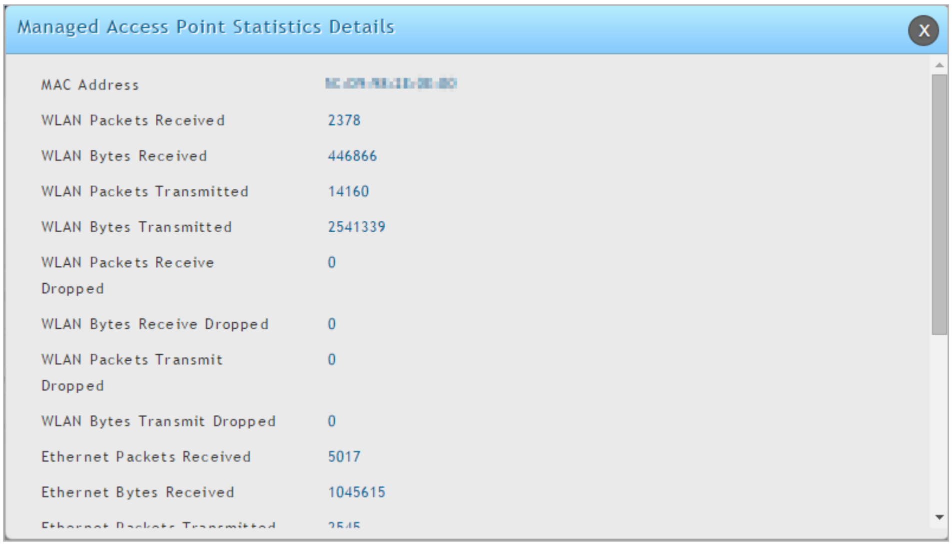


図 8-37　Managed AP Statistics Details 画面

以下の項目があります。

項目	説明
MAC Address	選択したアクセスポイントの MAC アドレスを表示します。
WLAN Packets Received	無線ネットワーク上でアクセスポイントが受信した総パケット数を表示します。
WLAN Bytes Received	無線ネットワーク上でアクセスポイントが受信した総データ量（バイト）を表示します。
WLAN Packets Transmitted	無線ネットワーク上でアクセスポイントが送信した総パケット数を表示します。
WLAN Bytes Transmitted	無線ネットワーク上でアクセスポイントが送信した総データ量（バイト）を表示します。
WLAN Packets Receive Dropped	無線ネットワーク上でアクセスポイントが受信し、破棄された総パケット数を表示します。
WLAN Bytes Receive Dropped	無線ネットワーク上でアクセスポイントが受信し、破棄された総データ量（バイト）を表示します。
WLAN Packets Transmit Dropped	無線ネットワーク上でアクセスポイントが送信し、破棄された総パケット数を表示します。
WLAN Bytes Transmit Dropped	無線ネットワーク上でアクセスポイントが送信し、破棄された総データ量（バイト）を表示します。
Ethernet Packets Received	有線ネットワーク上でアクセスポイントが受信した総パケット数を表示します。
Ethernet Bytes Received	有線ネットワーク上でアクセスポイントが受信した総データ量（バイト）を表示します。
Ethernet Packets Transmitted	有線ネットワーク上でアクセスポイントが送信した総パケット数を表示します。
Ethernet Bytes Transmitted	有線ネットワーク上でアクセスポイントが送信した総データ量（バイト）を表示します。
Multicast Packets Received	有線ネットワーク上でアクセスポイントが受信したマルチキャストパケット数を表示します。
Total Receive Errors	有線ネットワーク上で検知した受信エラーの数を表示します。
Total Transmit Errors	有線ネットワーク上で検知した送信エラーの数を表示します。
ARP Reqs Converted from Bcast to Ucast	アクセスポイントが無線リンクに送信する前にブロードキャストパケットをユニキャストパケットに変換した ARP リクエストの数を表示します。
Filtered ARP Requests	無線リンクで送信する代わりにアクセスポイントが破棄できた ARP リクエストの数を表示します。
Broadcasted ARP Requests	VAP にブロードキャストとして送信された ARP リクエストの数を表示します。このカウンタは WDS リンクを含みません。複数の VAP にブロードキャストされる場合、同じ ARP フレームが複数回カウントされる可能性があります。ARP の抑止が無効にされても、本カウンタは利用可能です。

Radio Statistics

「Managed APs List」内のエントリを右クリックして、「Details & Statistics > Radio Statistics」を選択します。

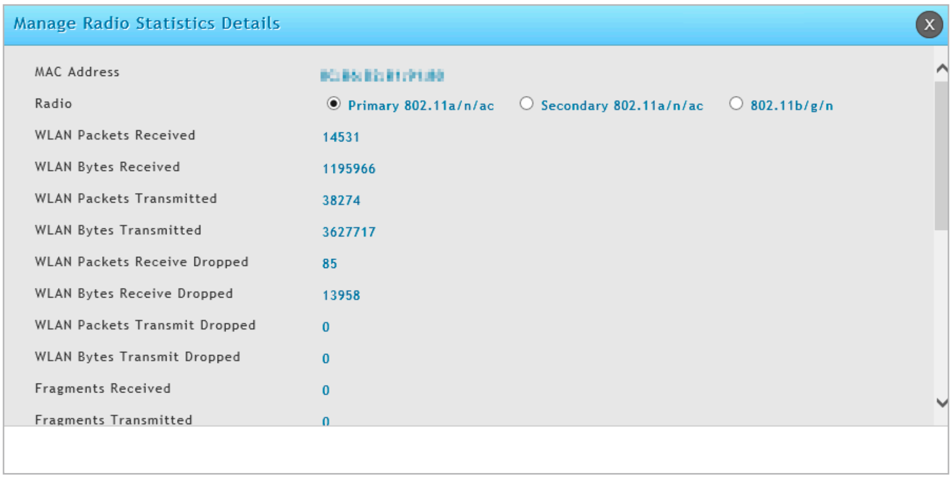


図 8-38　Managed Radio Statistics Details 画面

以下の項目があります。

項目	説明
MAC Address	MAC アドレスを表示します。
Radio	無線の接続モードを選択します。
WLAN Packets Received	無線インタフェース上でアクセスポイントが受信した総パケット数を表示します。
WLAN Bytes Received	無線インタフェース上でアクセスポイントが受信した総データ量（バイト）を表示します。
WLAN Packets Transmitted	無線インタフェース上でアクセスポイントが送信した総パケット数を表示します。
WLAN Bytes Transmitted	無線インタフェース上でアクセスポイントが送信した総データ量（バイト）を表示します。
WLAN Packets Receive Dropped	無線インタフェース上でアクセスポイントが受信し、破棄されたパケット数を表示します。
WLAN Bytes Receive Dropped	無線インタフェース上でアクセスポイントが受信し、破棄されたデータ量（バイト）を表示します。
WLAN Packets Transmit Dropped	無線インタフェース上でアクセスポイントが送信し、破棄されたパケット数を表示します。
WLAN Bytes Transmit Dropped	無線インタフェース上でアクセスポイントが送信し、破棄されたデータ量（バイト）を表示します。
Fragments Received	正しく受信したタイプがデータまたは管理の MPDU フレーム数を表示します。
Fragments Transmitted	送信したタイプがデータまたは管理で、個別アドレスまたはマルチキャストアドレスを含む MPDU フレーム数を表示します。
Multicast Frames Received	受信した宛先 MAC アドレス中にマルチキャストビットが設定されている MSDU フレーム数を表示します。
Multicast Frames Transmitted	正しく送信した宛先 MAC アドレス中にマルチキャストビットが設定されている MSDU 数を表示します。
Duplicate Frame Count	シーケンス制御フィールドで duplicate（冗長）と示されているフレームを受信した回数を表示します。
Failed Transmit Count	Short retry limit/Long retry limit 超過により、MSDU が正しく送信されなかった回数を表示します。
Transmit Retry Count	MSDU が正しく送信された回数を表示します。
Multiple Retry Count	2 度以上のリトライ後に MSDU が正しく送信された回数を表示します。
RTS Success Count	RTS フレームの応答として受信された CTS フレームの数を表示します。
RTS Failure Count	RTS フレームの応答として受信されなかった CTS フレームの数を表示します。
ACK Failure Count	想定していた ACK フレームが受信されなった数を表示します。
FCS Error Count	受信した MPDU により検知した FCS エラー数を表示します。
Frames Transmitted	送信に成功した MSDU の数を表示します。
WEP Undecryptable Count	暗号化されたフレームのうち、暗号化の必要なしと示されているもの、または受信デバイスがプライバシーオプションを使用していないために廃棄されたフレームの数を表示します。

VAP Statistics

「Managed APs List」内のエントリを右クリックして、「Details & Statistics > VAP Statistics」を選択します。

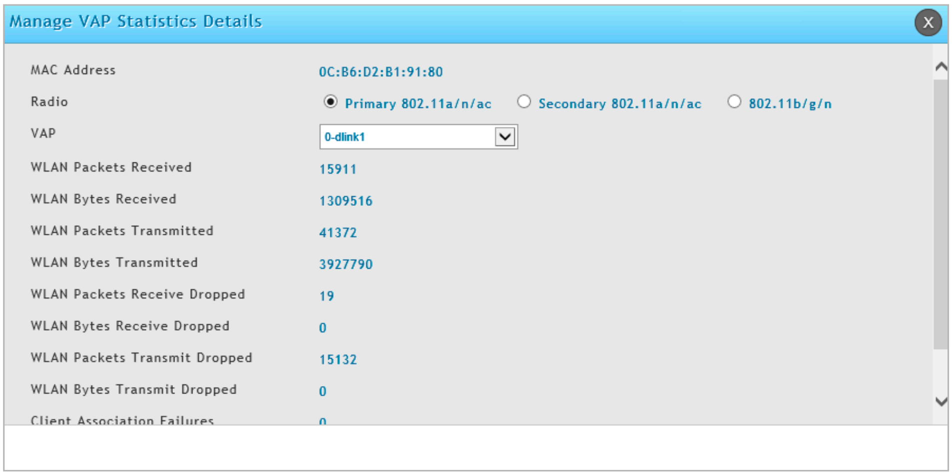


図 8-39　Manage VAP Statistics Details 画面

以下の項目があります。

項目	説明
MAC Address	アクセスポイントの MAC アドレスを表示します。
Radio	無線の接続モードを選択します。
VAP	プルダウンメニューから選択し、希望する VAP 統計情報を取得します。
WLAN Packets Received	指定した VAP が受信した総パケット数を表示します。
WLAN Bytes Received	指定した VAP が受信した総データ量（バイト）を表示します。
WLAN Packets Transmitted	指定した VAP が送信した総パケット数を表示します。
WLAN Bytes Transmitted	指定した VAP が送信した総データ量（バイト）を表示します。
WLAN Packets Receive Dropped	この VAP 上でアクセスポイントが受信し、破棄されたパケット数を表示します。
WLAN Bytes Receive Dropped	この VAP 上でアクセスポイントが受信し、破棄されたデータ量（バイト）を表示します。
WLAN Packets Transmit Dropped	この VAP 上でアクセスポイントが送信し、破棄されたパケット数を表示します。
WLAN Bytes Transmit Dropped	この VAP 上でアクセスポイントが送信し、破棄されたデータ量（バイト）を表示します。
Client Association Failures	VAP により接続を拒否されたクライアント数を表示します。
Client Authentication Failures	VAP への認証に失敗したクライアント数を表示します。

Neighbour APs

「Managed APs List」内のエントリを右クリックして、「Neighbour Information > Neighbour APs」を選択します。

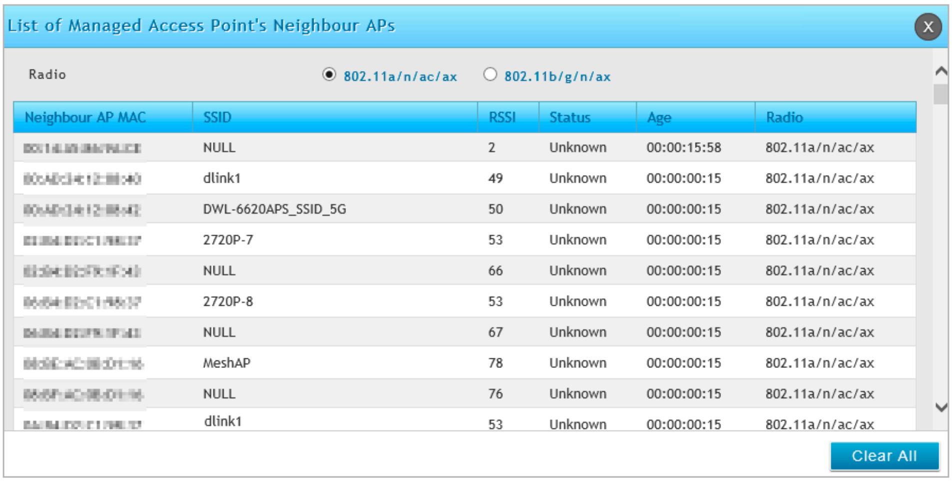


図 8-40　List of Managed Access Point's Neighbour APs 画面

以下の項目があります。

項目	説明
Radio Mode	無線の接続モードを選択します。
Neighbour AP MAC	Neighbour アクセスポイントネットワークの MAC アドレスを表示します。物理的な無線インタフェースまたは VAP の MAC アドレスです。D-Link アクセスポイントの場合は常に VAP の MAC アドレスです。Neighbour アクセスポイントの MAC アドレスは、RF スキャン状態の内容と相互参照できます。
SSID	Neighbour アクセスポイントのネットワークの SSID を表示します。
RSSI	Neighbour アクセスポイントからの信号強度（1-100）を示します。これにより、管理下のアクセスポイントと隣接アクセスポイント間の距離が推測できる場合があります。1 が最も弱い信号強度です。
Status	アクセスポイントの管理状況を示します。これは、ネットワーク上でコントローラに認識されている有効なアクセスポイントであるか、または Rogue（不正）のいずれかです。 • Managed - 無線システムは Neighbour アクセスポイントを管理しています。 • Standalone - アクセスポイントは、スタンドアロンモードで管理され、Valid AP エントリ（ローカルまたは RADIUS）として設定されます。 • Rogue - アクセスポイントは脅威検出アルゴリズムの 1 つにより脅威として分類されています。 • Unknown - アクセスポイントは、ネットワークで検出されましたが、脅威検出アルゴリズムは脅威として分類していません。
Age	無線帯域で、本アクセスポイントが RF スキャンによって最後に報告されてから経過した時間を表示します。
Radio	アクセスポイントの各無線インタフェースが使用している無線モードを表示します。
Clear All	Neighbour アクセスポイントと Neighbour クライアントのリストから、すべてのエントリをクリアします。 現在選択しているアクセスポイントおよび無線インタフェースのみではなく、すべてのアクセスポイントおよび無線インタフェースについて、Neighbour を削除します。 Neighbour が検出されると、リストは再度作成されます。

Neighbour Clients

「Managed APs List」内のエントリを右クリックして、「Neighbour Information > Neighbour Clients」を選択します。

図 8-41　List of Managed Access Point's Neighbour Clients 画面

以下の項目があります。

項目	説明
Neighbour Client MAC	Neighbour アクセスポイントネットワークの MAC アドレスを表示します。物理的な無線インタフェースまたは VAP の MAC アドレスです。D-Link アクセスポイントの場合は常に VAP の MAC アドレスです。Neighbour アクセスポイントの MAC アドレスは、RF スキャン状態の内容と相互参照できます。
RSSI	Neighbour アクセスポイントからの信号強度（1-100）を示します。これにより、管理下のアクセスポイントと Neighbour アクセスポイント間の距離を推測できる場合があります。1 が最も弱い信号強度です。
Discovery Reason	発見された理由を表示します。
Age	無線インタフェースで、本アクセスポイントが RF スキャンにより最後に報告されてから経過した時間を表示します。
Radio	アクセスポイントの各無線インタフェースが使用している無線モードを表示します。
Clear All	Neighbour アクセスポイントと Neighbour クライアントのリストからすべてのエントリをクリアします。 Neighbour が検出されると、リストは再度作成されます。

Channel and Power

「Managed APs List」内のエントリを右クリックして、「Channel & Power > Radio1-3」を選択します。

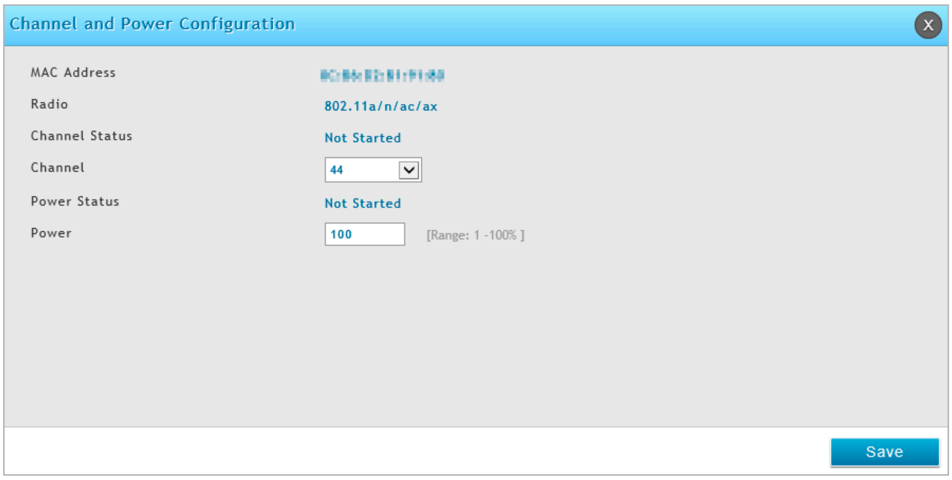


図 8-42　Channel and Power Configuration 画面

以下の項目があります。

項目	説明
MAC Address	アクセスポイントの MAC アドレスを表示します。
Radio	無線の接続モードを表示します。
Channel Status	「Not Started」「Set Requested」「Set Complete」いずれかのステータスが表示されます。
Channel	チャンネルを表示・設定します。チャンネル範囲はインタフェースの無線モードにより決定します。
Power Status	「Not Started」「Set Requested」「Set Complete」いずれかのステータスが表示されます。
Power	電力レベルは、アクセスポイントの RF 信号が遠く範囲に影響します。この値が低すぎる場合、無線クライアントは信号を検出できなかったり、WLAN パフォーマンスが低下したりします。反対に、値が高すぎる場合は、RF 信号は範囲内の他のアクセスポイントに干渉します。
Save	設定を保存します。

Distributed Tunnel

「Managed APs List」内のエントリを右クリックして、「Distributed Tunnel」を選択します。

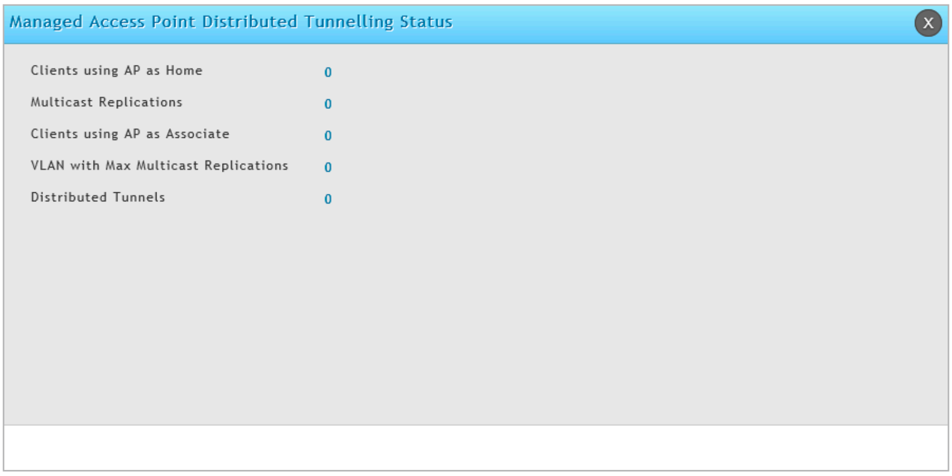


図 8-43　Managed AP Distributed Tunneling Status 画面

以下の項目があります。

項目	説明
Clients using AP as Home	分散型トンネルモードを使用してこのアクセスポイントからローミングし、このアクセスポイントにトンネル経由でデータを送るクライアントの数を表示します。
Multicast Replications	同じ VLAN のメンバであるホーム AP の最大トンネル数を表示します。
Clients using AP as Associate	分散型トンネルモードを使用してこの AP にローミングし、ホーム AP にトンネル経由でデータを送るクライアントの数を表示します。
VLAN with Max Multicast Replications	分散型トンネルにマルチキャストを送信するためにアクセスポイントが最も多くの回数複製を行った VLAN ID を表示します。
Distributed Tunnels	このアクセスポイントとの分散型 L2 トンネルを持っているアクセスポイントの数を表示します。アクセスポイントは、トンネルを使用することで、クライアントに対してホーム AP またはアソシエーション AP として機能します。

Connection Failed（接続失敗アクセスポイント）

Wireless > Access Point > AP List > Connection Failed メニュー

認証され、管理ステータスとなっていたアクセスポイントのうち、現在コントローラと接続していないアクセスポイントの情報を表示します。

Wireless > Access Point > AP List > Connection Failed の順にメニューをクリックし、以下の画面を表示します。

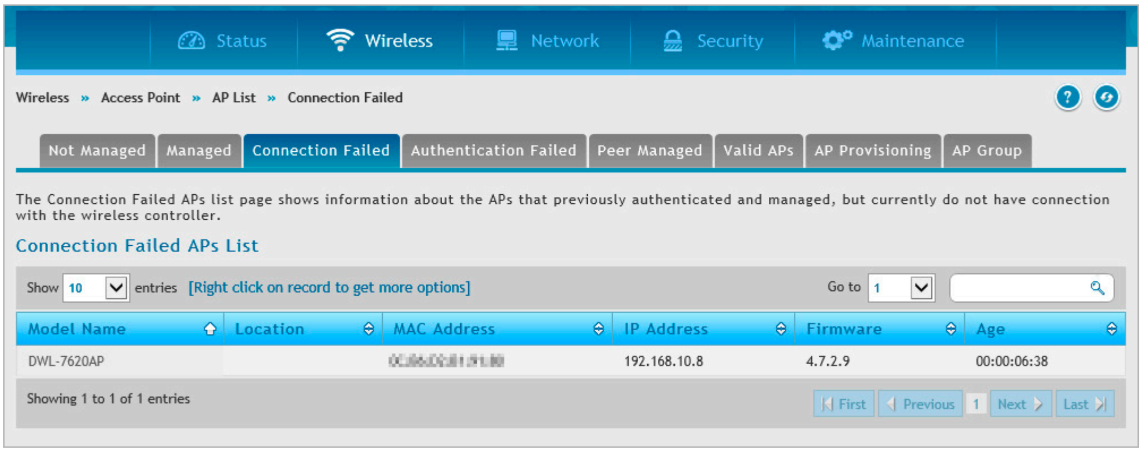


図 8-44　 Connection Failed APs List 画面

以下の項目があります。

項目	説明
Model Name	検出中に学習された、アクセスポイントのハードウェアのパート番号を表示します。
Location	管理アクセスポイントに設定された位置情報を表示します。
MAC Address	アクセスポイントの MAC アドレスを表示します。
IP Address	アクセスポイントの IP アドレスを表示します。
Firmware	アクセスポイントのファームアップバージョンを表示します。
Age	アクセスポイントの最後の検出および情報の更新から経過した時間を表示します。

Authentication Failed（認証エラー）

Wireless > Access Point > AP List > Authentication Failed メニュー

アクセスポイントから無線コントローラへの接続は、不正なパケットフォーマットやベンダ ID などのエラーのため、または Valid AP として正しいローカル /RADIUS 認証情報が設定されていないなどの原因で失敗することがあります。ここでは、無線コントローラとの通信の確立に失敗したアクセスポイントに関する情報を表示します。アクセスポイントで右クリックして、管理または詳細を参照するオプションを起動します。

Wireless > Access Point > AP List > Authentication Failed の順にメニューをクリックし、以下の画面を表示します。

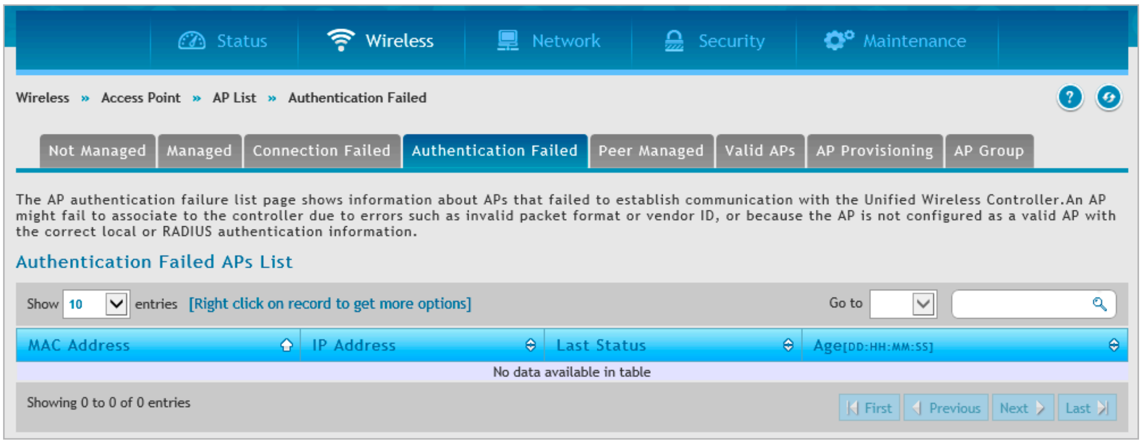


図 8-45　 Authentication Failed APs List 画面

アクセスポイントは以下の原因のいずれかによりエラーになります。

エラー	説明
No Database Entry	アクセスポイントの MAC アドレスがローカル Valid AP データベースまたは外部 RADIUS サーバのデータベース内にないため、アクセスポイントの認可がされません。
Local Authorization	アクセスポイントに設定されている認証用パスワードがローカルデータベースに登録されているものと一致しません。
Not Managed	アクセスポイントは Valid AP データベースにありますが、ローカルのデータベースの AP モードは Managed に設定されません。
RADIUS Authentication	RADIUS サーバの RADIUS クライアントに設定されたパスワードは、サーバによって拒否されました。
RADIUS Challenged	RADIUS サーバは、Challenge-Response 認証モードを使用するように設定されます。これは、アクセスポイントと互換性はありません。
RADIUS Unreachable	アクセスポイントが設定されている RADIUS サーバに未到達です。
Invalid RADIUS Response	アクセスポイントが未承認または不正な RADIUS サーバから応答パケットを受信しました。
Invalid Profile ID	RADIUS データベースに指定されているプロファイル ID はコントローラに存在しない可能性があります。同様の事象が、ピアコントローラから設定を受信した場合にローカルデータベースに起こり得ます。
Profile Mismatch	AP プロファイルに指定されたアクセスポイントのハードウェアタイプは、実際のアクセスポイントのハードウェアと互換性がありません。

以下の項目があります。

項目	説明
MAC Address	アクセスポイントの MAC アドレスを表示します。
IP Address	アクセスポイントの IP アドレスを表示します。
Last Status	最後に発生したエラーの種類を表示します。 • Local Authentication - ローカル認証 • No Database Entry - データベースエントリがありません。 • Not Managed - 管理されていません。 • RADIUS Authentication - RADIUS 認証 • RADIUS Challenged - RADIUS チャレンジ • RADIUS Unreachable - RADIUS 未到達 • Invalid RADIUS Response - 不正な RADIUS 応答 • Invalid Profile ID - 不正なプロファイル ID • Profile Mismatch-Hardware Type - プロファイルが不一致のハードウェアタイプ • 10-AP Image Not Available - コントローラはアクセスポイントに展開する適切なイメージを持っていません。（コントローラで自動 AP イメージアップグレードがサポートされ、有効化されている場合のみ）
Age	エラー発生から経過した時間を表示します。

アクセスポイントを右クリックして、「Managed」を選択すると、以下の画面が表示されます

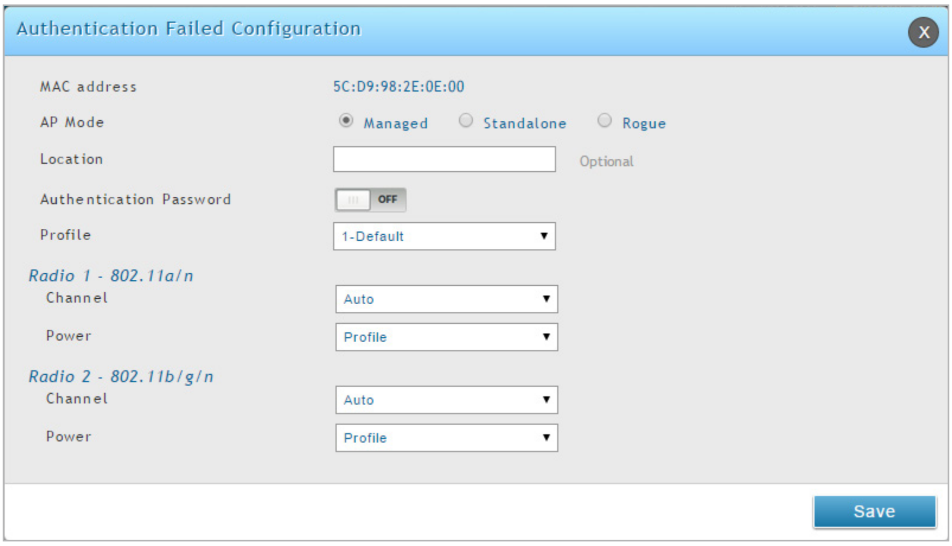


図 8-46　Authentication Failed Configuration 画面

Access Point Failure List から選択したアクセスポイントを Valid AP データベースに追加します。

アクセスポイントを右クリックして、「View Details」を選択すると、以下の画面が表示されます。

図 8-47　Authentication Failed Details 画面

特定の MAC アドレスエントリに関する全情報を表示します。

以下の項目があります。

項目	説明
MAC Address	アクセスポイントの MAC アドレスを表示します。
IP Address	アクセスポイントの IP アドレスを表示します。
Last Failure Type	発生した最後のエラーのタイプを表示します。 • Local Authentication - ローカル認証 • No Database Entry - データベースエントリがありません。 • Not Managed - 管理されていません。 • RADIUS Authentication - RADIUS 認証 • RADIUS Challenged - RADIUS チャレンジ • RADIUS Unreachable - RADIUS 未到達 • Invalid RADIUS Response - 不正な RADIUS 応答 • Invalid Profile ID - 不正なプロファイル ID • Profile Mismatch-Hardware Type - プロファイルが不一致のハードウェアタイプ
Vendor ID	ピアコントローラのソフトウェアのベンダ ID を表示します。
Protocol Version	ピアコントローラのソフトウェアがサポートするプロトコルのバージョンを表示します。
Software Version	特定のピアコントローラのソフトウェアバージョンを表示します。
Hardware Type	アクセスポイントのハードウェアプラットフォームに割り当てられているハードウェア ID を表示します。
Reporting Controller	認証失敗を報告したコントローラを表示します。
Controller MAC Address	コントローラのイーサネットアドレスを表示します。
Controller IP Address	コントローラの IP アドレスを表示します。
Validation Failures	本アクセスポイントが接続（認可）に失敗した回数を表示します。
Authentication Failures	本アクセスポイントに検出された 802.1X 認証エラー数を表示します。
Age	エラー発生から経過した時間を表示します。

Peer Managed

Status > Wireless Information > Access Point > Peer Managed メニュー
クラスタ内のピアコントローラが管理するアクセスポイントに関する情報を表示します。各ピアコントローラは IP アドレスによって特定されます。

Status > Wireless Information > Access Point > Peer Managed の順にメニューをクリックし、以下の画面を表示します。

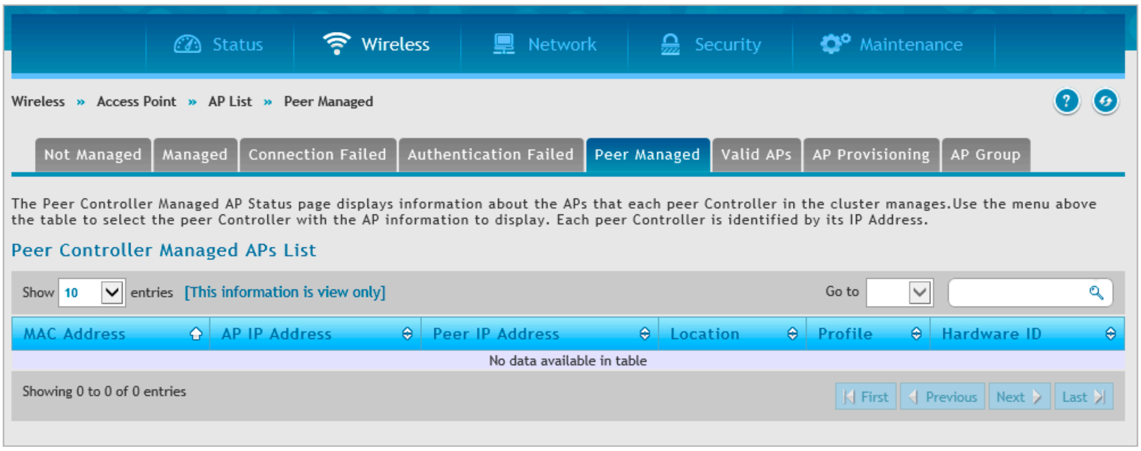


図 8-48　Peer Controller Managed APs List 画面

以下の項目があります。

項目	説明
MAC Address	ピアコントローラが管理する各アクセスポイントの MAC アドレスを表示します。
AP IP Address	アクセスポイントの IP アドレスを表示します。
Peer IP Address	アクセスポイントを管理するピアコントローラの IP アドレスを表示します。プルダウンメニューから「All」を選択すると、本欄が表示されます。
Location	管理するアクセスポイントに設定された場所の記述を表示します。
Profile	無線コントローラがアクセスポイントに適用するアクセスポイントのプロファイルを表示します。
Hardware ID	アクセスポイントのハードウェアプラットフォームに割り当てられているハードウェア ID を表示します。

接続クライアントのグローバル状態

Status > Wireless Information > Associated Clients > Global Status メニュー
管理するアクセスポイントを通じて接続する全クライアントの統計情報を表示します。

Status > Wireless Information > Associated Clients > Global Status の順にメニューをクリックし、以下の画面を表示します。

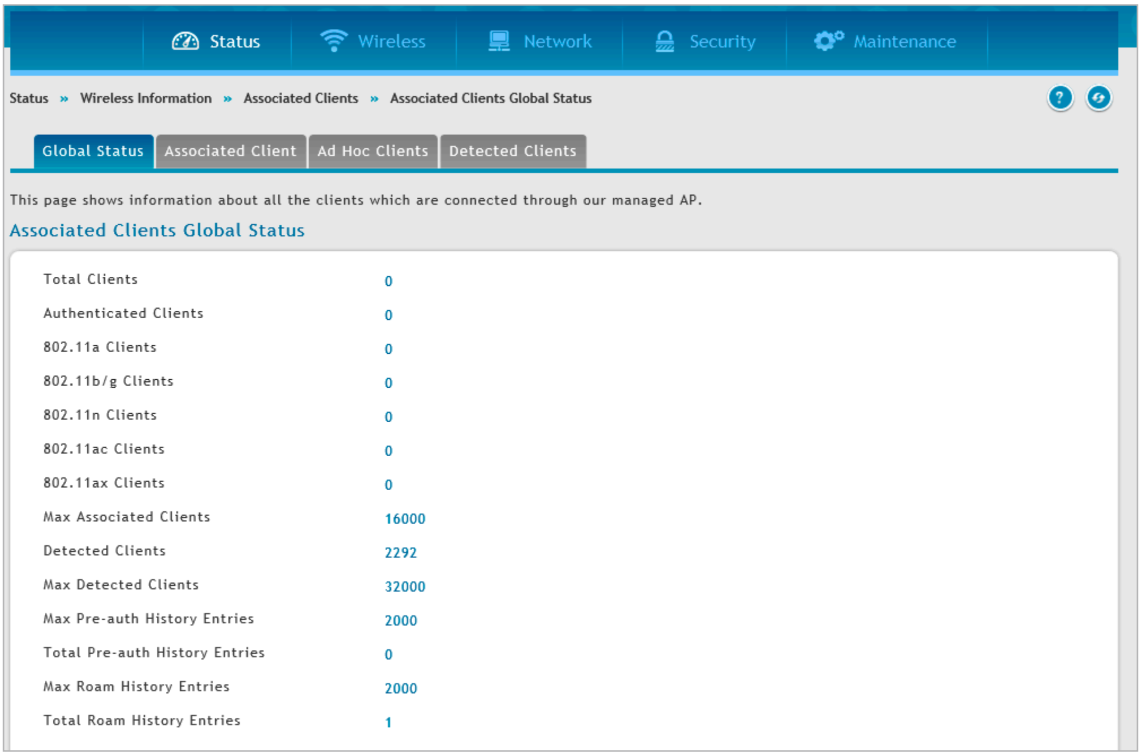


図 8-49　Associated Clients Global Status 画面

以下の項目があります。

項目	説明
Total Clients	データベース中のクライアントの総数を表示します。この値は「Associated」、「Authenticated」、「Disassociated」の状態のクライアントを含みます。
Authenticated Clients	クライアントデータベース中のクライアントで、「Authenticated」状態のクライアントの総数を表示します。
802.11a Clients	認証された IEEE 802.11a クライアントの総数を表示します。
802.11b/g Clients	認証された IEEE 802.11b/g クライアントの総数を表示します。
802.11n Clients	認証された IEEE 802.11n クライアントの総数を表示します。IEEE 802.11a/n、IEEE 802.11b/g/n、5GHz IEEE 802.11n、2.4GHz IEEE 802.11n が含まれます。
802.11ac Clients	認証された IEEE 802.11ac クライアントの総数を表示します。
802.11ax Clients	認証された IEEE 802.11ax クライアントの総数を表示します。
Max Associated Clients	無線システムに接続できるクライアントの最大数を表示します。これは Associated Client データベースで許可されているエントリの最大数です。
Detected Clients	WLAN に検出された無線クライアントの数を表示します。
Max Detected Clients	コントローラが検出できるクライアントの最大数を表示します。この数値は Detected Client データベースのサイズによって制限されます。
Max Pre-auth History Entries	システムが記録できる Client Pre-Authentication イベントの最大数を表示します。
Total Pre-auth History Entries	システムで使用中の事前認証の履歴エントリの現在の数を表示します。
Maximum Roam History Entries	すべての検出クライアントに対してローミング履歴に記録可能なエントリの最大数を表示します。
Total Roam History Entries	システムで使用中の事前認証の履歴エントリの現在の数。

接続するクライアント

Status > Wireless Information > Associated Clients > Associated Clients メニュー

無線コントローラに接続するクライアントに関連するトラフィックを追跡します。

Status > Wireless Information > Associated Clients > Associated Clients の順にメニューをクリックし、以下の画面を表示します。

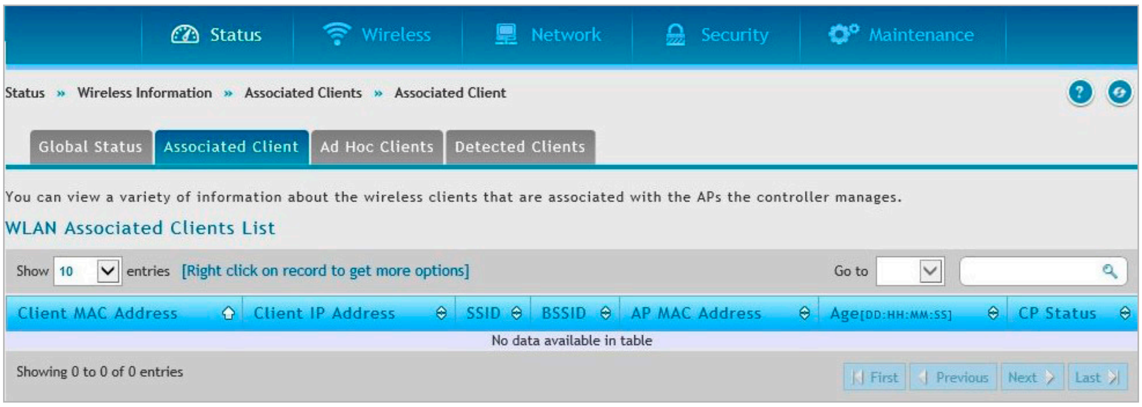


図 8-50　WLAN Associated Clients List 画面

以下の項目があります。

項目	説明
Client MAC Address	クライアントステーションのイーサネット MAC アドレスを表示します。
Client IP Address	クライアントステーションの IP アドレスを表示します。
SSID	クライアントが接続する無線ネットワークの名前を表示します。
BSSID	クライアントが接続する管理対象のアクセスポイント / 仮想アクセスポイントの MAC アドレスを表示します。
AP MAC Address	アクセスポイントのイーサネット MAC アドレスを表示します。
Age	コントローラが新しいステータスを受信、またはこのクライアントの統計情報が更新されてから経過した時間を表示します。
CP Status	クライアントが紐づくキャプティブポータルのステータスを表示します。

クライアントを右クリックすると、オプションメニューを選択できます。

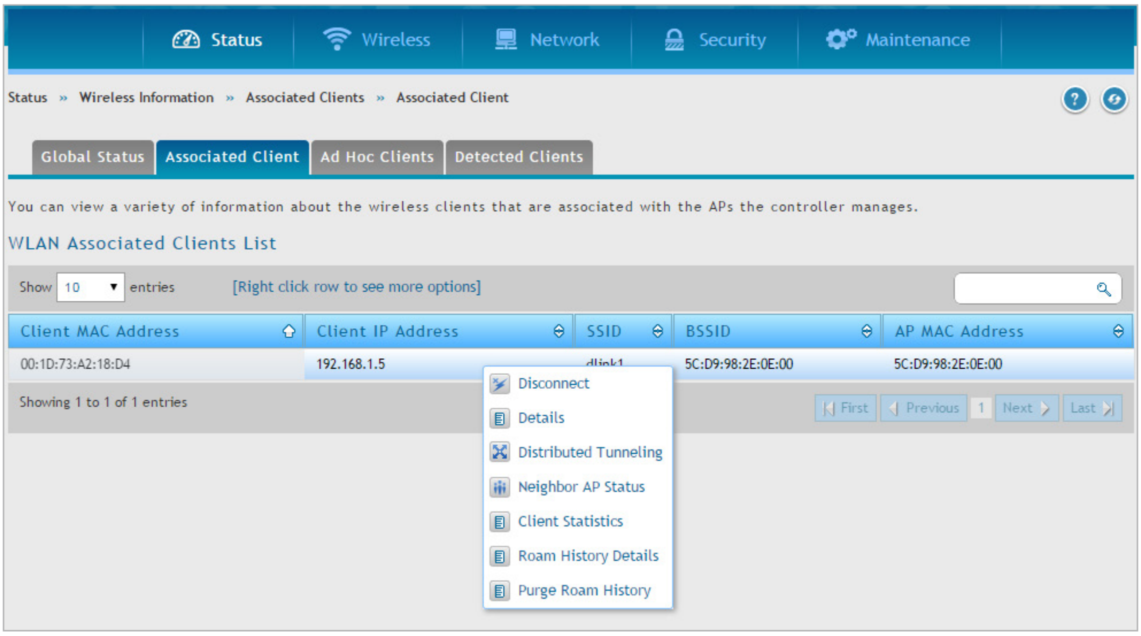


図 8-51　WLAN Associated Clients List 画面 - オプションメニュー

以下のオプションがあります。

項目	説明
Disconnect	接続するクライアントを切断します。
Details	関連付けられているクライアントとそれが接続するアクセスポイントに関する詳細情報を表示します。
Distributed Tunneling	分散型トンネル状態の情報を表示します。
Neighbour AP Status	Neighbour アクセスポイントの状態に関する情報を表示します。
Client Statistics	関連付けられているクライアントとその帯域使用に関する詳細な統計情報を表示します。
Roam History Details	DWC-2000 が管理する、クライアントの接続先の各アクセスポイントの履歴を表示します。
Purge Roam History	選択したクライアントのローミングの履歴をクリアします。

詳細情報

クライアントを右クリックし、「Details」を選択して、以下の画面を表示します。

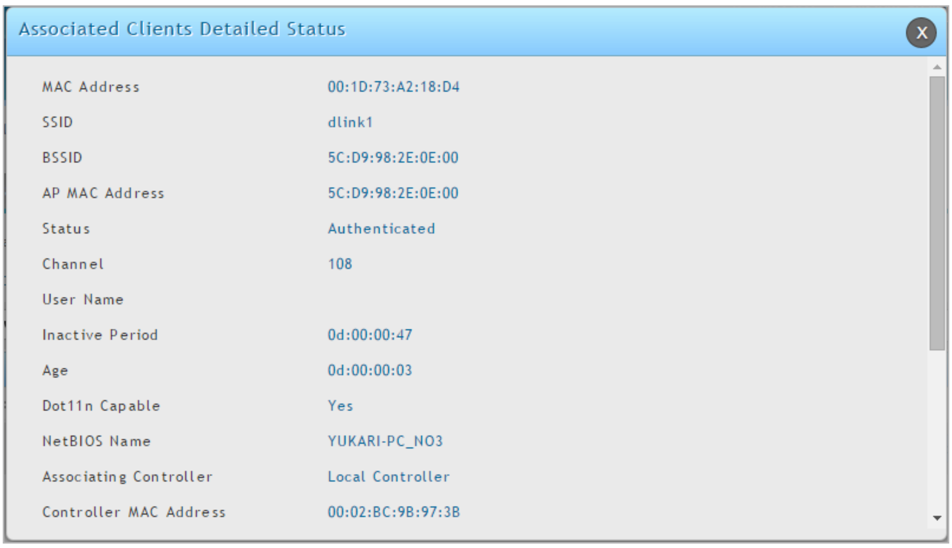


図 8-52　Associated Clients Detailed Status 画面

以下の項目があります。

項目	説明
MAC Address	接続するクライアントの MAC アドレスを表示します。
SSID	クライアントが接続しているネットワークを表示します。
BSSID	クライアントが接続しているアクセスポイントの VAP の MAC アドレスを表示します。
AP MAC Address	管理下にあるアクセスポイントの MAC アドレスを表示します。

項目	説明
Status	クライアントが接続中であるか、認証されているかを表示します。 • Associated - クライアントは現在管理下にあるアクセスポイントと接続中です。 • Authenticated - クライアントは現在接続中で、管理下にあるアクセスポイントに認証されています。 • Disassociated - クライアントは管理下にあるアクセスポイントとは接続していません。タイムアウト時間内に他の管理下にあるアクセスポイントとローミングを開始しないと削除されます。
Channel	クライアントの接続に使用しているチャンネルを表示します。
User Name	802.1X で認証されたクライアントのユーザ名を表示します。他のセキュリティモードを使用したネットワークのクライアントにはユーザ名がありません。
Inactive Period	このクライアントから最後にデータパケットを受信してから経過した時間を表示します。
Age	コントローラが、このクライアントの新しい状態および統計情報の更新を受信してから経過した時間を表示します。
Dot11n Capable	接続するクライアントが IEEE 802.11n 標準をサポートするかどうかを表示します。
NetBIOS Name	無線クライアントの NetBIOS 名を表示します。マイクロソフト Windows ホストにおける NetBIOS 名は、通常ホスト名と同じか、またはホスト名に基づいています。
Associating controller	無線クライアントが接続するアクセスポイントがローカルコントローラまたはピアコントローラのいずれかで管理されているかを表示します。
Controller MAC Address	無線クライアントが接続するアクセスポイントを管理するコントローラの MAC アドレスを表示します。
Controller IP Address	無線クライアントが接続するアクセスポイントを管理するコントローラの IP アドレスを表示します。
Location	管理下にあるアクセスポイントの場所を表示します。
Radio	クライアントが接続中のアクセスポイントの無線インタフェースと無線モードを表示します。
VLAN	クライアントが VAP と接続中で VLAN データ送信モードである時、現在割り当てられている VLAN を表示します。
Transmit Data Rate	クライアントの現在のデータ送信速度を表示します。
Network Time	クライアントがネットワークに認証されてから経過した時間を表示します。
Detected IP Address	必要に応じて、クライアントの IPv4 アドレスを表示します。
Tunnel IP Address	トンネルを使用しないクライアントの場合、何も表示されません。クライアントがトンネルを使用している場合、割り当てられたトンネル IP アドレスが表示されます。

分配型トンネル情報

クライアントを右クリックし、「Distributed Tunneling」をクリックして、以下の画面を表示します。

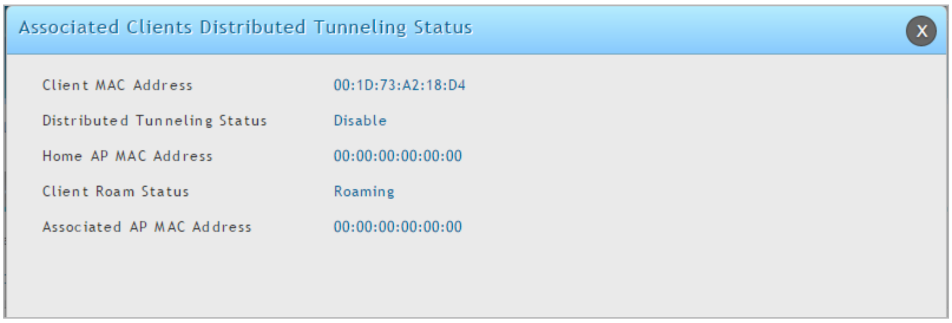


図 8-53　Associated Clients Distributed Tunneling Status 画面

以下の項目があります。

項目	説明
Client MAC Address	接続する無線クライアントの MAC アドレスを表示します。
Distributed Tunneling Status	このクライアントが L2 の分散型トンネルをサポートするネットワークに接続するかどうかを表示します。
Home AP MAC Address	クライアントのホーム AP の MAC アドレスを表示します。分散型トンネルが有効なネットワークに接続するクライアントに対してのみ、この値が意味を持ちます。
Client Roam Status	クライアントがホーム AP 上にあるか、または別のアクセスポイントに移動して、トンネルを使用しているかどうかを表示します。 • Home - クライアントはトンネルを使用していません。 • Roaming - クライアントはトンネルを使用しています。分散型トンネルを無効にすると、フィールドにはローミング状況が「Roaming」として表示されます。
Associated AP MAC Address	クライアントが分散型トンネルプロトコルを通じて接続したアクセスポイントの MAC アドレスを表示します。

Neighbour AP 情報

クライアントを右クリックし、「Neighbour AP Status」をクリックして、以下の画面を表示します。

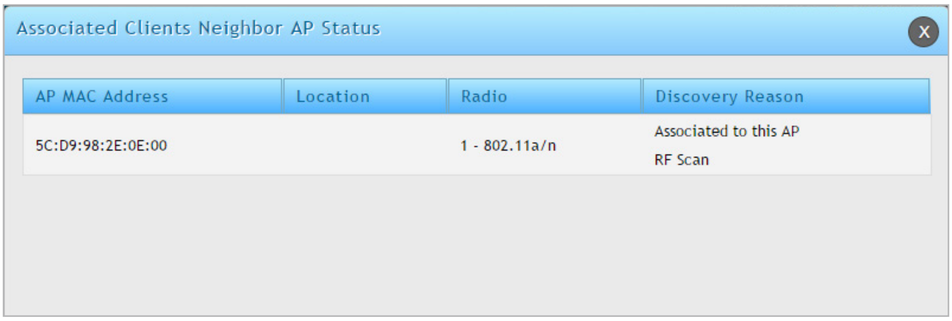


図 8-54　Associated Clients Neighbor AP Status 画面

クライアント統計情報

クライアントを右クリックし、「Client Statistics」をクリックして、以下の画面を表示します。

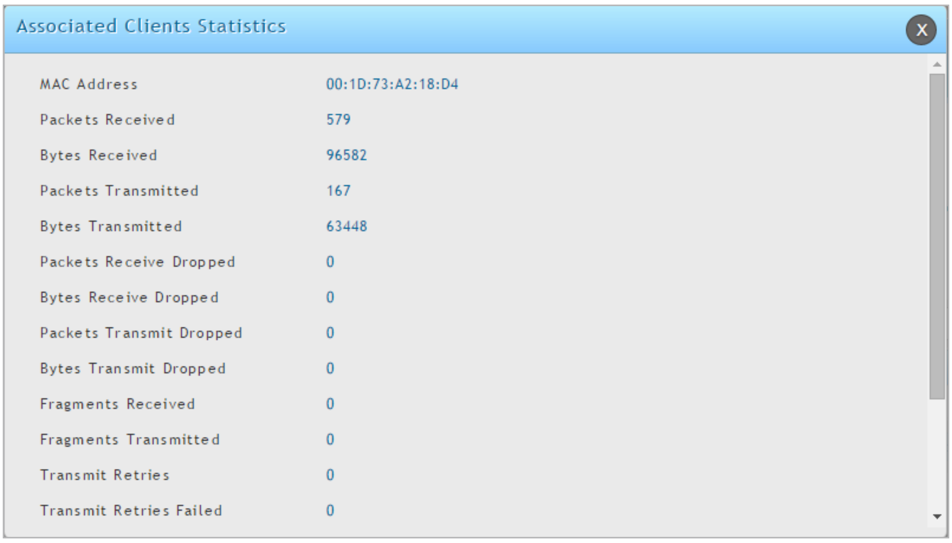


図 8-55　Associated Clients Statistics 画面

無線クライアントが 1 台のアクセスポイントに接続中に送受信したトラフィックの情報を表示します。

以下の項目があります。

項目	説明
MAC Address	クライアントの MAC アドレスを表示します。
Packets Received	クライアントから受信したパケット数の合計を表示します。
Bytes Received	クライアントから受信したバイト数の合計を表示します。
Packets Transmitted	クライアントに送信したパケット数の合計を表示します。
Bytes Transmitted	クライアントに送信したバイト数の合計を表示します。
Packets Receive Dropped	クライアントから受信し、破棄されたパケット数の合計を表示します。
Bytes Receive Dropped	クライアントから受信し、破棄されたバイト数の合計を表示します。
Packets Transmit Dropped	クライアントから送信し、破棄されたパケット数の合計を表示します。
Bytes Transmit Dropped	クライアントから受信し、破棄されたパケット数の合計を表示します。
Fragments Received	クライアントから受信したフラグメント化されたパケット数の合計を表示します。
Fragments Transmitted	クライアントに送信したフラグメント化されたパケット数の合計を表示します。
Transmit Retries	1 回以上のリトライの後、クライアントに送信成功した回数を表示します。
Transmit Retries Failed	1 回以上のリトライの後、クライアントに送信失敗した回数を表示します。
TS Violate Packets Received	指定したアクセスカテゴリの無線クライアントからアクセスポイントが受信したパケット数を表示します。
TS Violate Packets Transmitted	指定したアクセスカテゴリの無線クライアントにアクセスポイントが送信したパケット数を表示します。
Duplicates Received	クライアントから受信した重複パケットの合計数を表示します。

認証済みのクライアントが、セッションの損失および再認証を避けてローミングが行えるようにするために、無線クライアントは、クライアントが接続できる範囲内で他のアクセスポイントに対して認証を試みることができます。事前認証に成功するためには、ターゲットアクセスポイントには、クライアントと一致する SSID およびセキュリティ設定を持つ VAP が必要です。セキュリティ設定は MAC 認証、暗号化方式、事前共有キーまたは RADIUS パラメータを含みます。クライアントが接続するアクセスポイントは、すべての事前認証要求を取得してコントローラに送信します。

ローミングヒストリの詳細

管理されている 1 つのアクセスポイントから別のアクセスポイントへのローミングする場合、無線システムは、クライアントの記録を保持して、「WLAN Associated Detected Clients」の「Roam History List」に本情報を表示します。

クライアントを右クリックし、「Roam History Details」をクリックして、以下の画面を表示します。

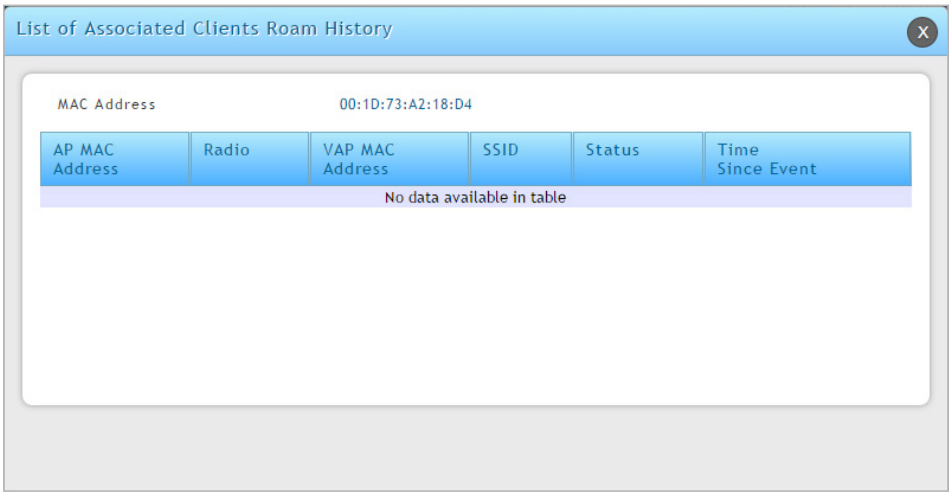


図 8-56　Associated Clients Roam History 画面

以下の項目があります。

項目	説明
MAC Address	検出されたクライアントの MAC アドレスを表示します。
AP MAC Address	クライアントを事前認証した管理アクセスポイントの MAC アドレスを表示します。
Radio	クライアントが認証される無線インタフェースの番号を表示します。
VAP MAC Address	クライアントがローミングを行った VAP の MAC アドレスを表示します。
SSID	VAP が使用される SSID 名を表示します。
Status	履歴エントリが新しい認証またはローミングイベントかどうかを示すフラグを表示します。
Time Since Event	履歴エントリが追加されてから経過した時間を表示します。

アドホッククライアント

Status > Wireless Information > Associated Clients > Ad Hoc Clients メニュー

アドホッククライアントとは、アクセスポイントに接続しているクライアントを経由して WLAN に接続するクライアントです。アドホッククライアントは、直接アクセスポイントと通信を行いません。アドホックネットワークは、RF 帯域を消費し、セキュリティ上のリスクを招く可能性を含んでいるため、特に注意が必要です。

Status > Wireless Information > Associated Clients > Ad Hoc Clients の順にメニューをクリックし、以下の画面を表示します。

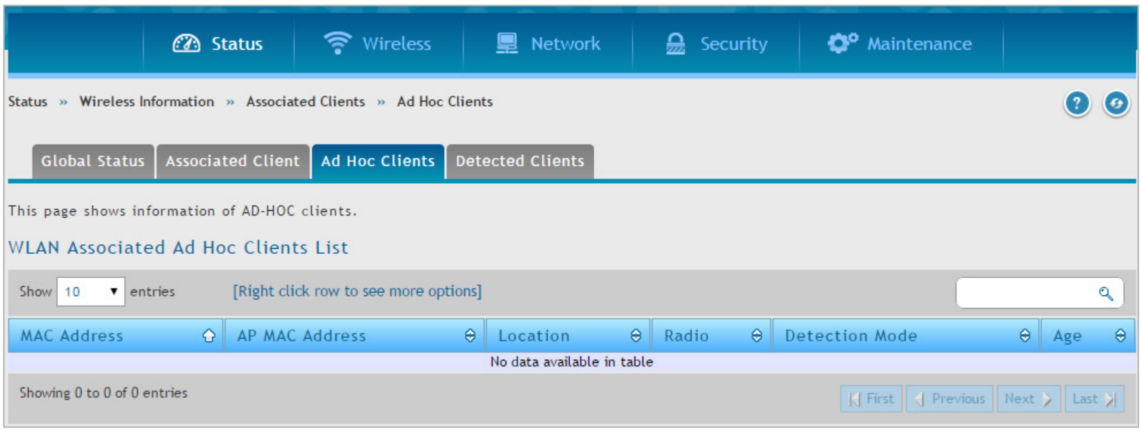


図 8-57　WLAN Associated Ad Hoc Clients List 画面

以下の項目があります。

項目	説明
MAC Address	クライアントの MAC アドレスを表示します。検出モードがビーコンフレームの場合、RF スキャンデータベースや隣接 AP リストには、クライアントはアクセスポイントとして表示されます。検出モードがデータフレームの場合、クライアント情報は隣接クライアントリストに表示されます。
AP MAC Address	クライアントを検出した管理下のアクセスポイントのベースイーサネット MAC アドレスを表示します。
Location	管理下のアクセスポイントに設定された場所の説明を表示します。
Radio	アドホッククライアントが検出された無線帯域とその設定モードを表示します。
Detection Mode	アドホックデバイスの検出方式。「Beacon Frame」または「Data Frame」となります。
Age	アドホックネットワークが最後に検出されてから経過した時間を表示します。

「WLAN Associated Ad Hoc Clients List」の右クリックオプションは以下の通りです。

項目	説明
Delete All	リストからすべてのアドホッククライアントエントリを削除します。リストをクリアしても、アドホッククライアントは切断されません。また、クライアントはアドホックネットワークに残っている場合があります。
Deny	WLAN アクセスからアドホッククライアントをブロックします。この MAC アドレスは、デフォルトアクションが「Deny」（拒否）である「Known Client」データベースに追加されます。
Allow	WLAN へのアドホッククライアントアクセスを許可します。この MAC アドレスは、デフォルトアクションが「Allow」（許可）である「Known Client」データベースに追加されます。

検出クライアント

Status > Wireless Information > Associated Clients > Detected Clients メニュー

クライアントがシステムとの通信を試みた場合、または、システムがクライアントからのトラフィックを検出した場合に、無線システムは無線クライアントを検出します。本画面では、アクセスポイントで認証されたクライアント、および離脱しシステムから切断されたクライアントの情報を表示します。

Status > Wireless Information > Associated Clients > Detected Clients の順にメニューをクリックし、以下の画面を表示します。

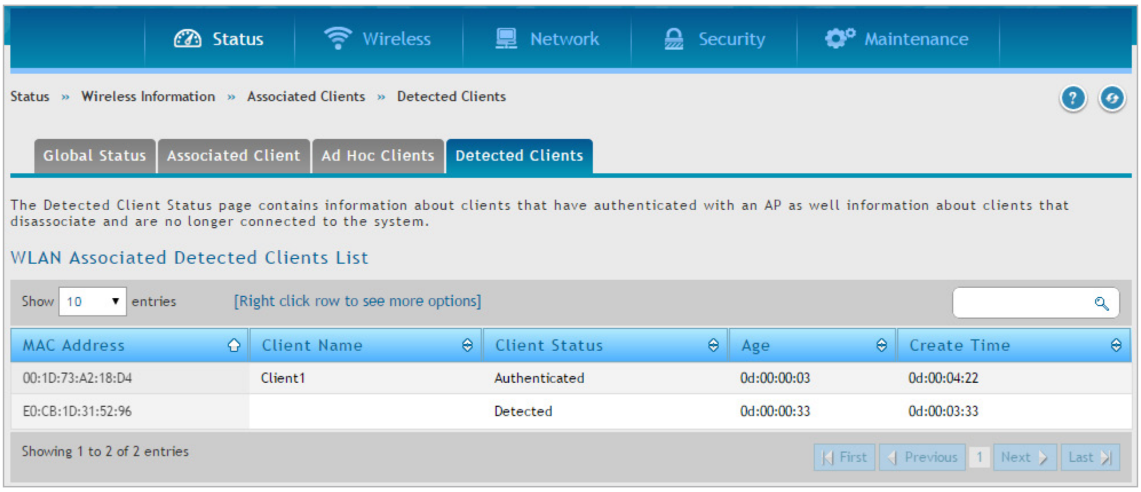


図 8-58　WLAN Associated Detected Clients List 画面

以下の項目があります。

項目	説明
MAC Address	クライアントのイーサネット MAC アドレスを表示します。
Client Name	「Known Client」データベースにあるクライアントの名称を表示します。データベースにクライアントが存在しない場合、このフィールドは空白です。
Client Status	クライアントの状態を表示します。 • Authenticated - 無線クライアントは無線システムで認証されています。 • Detected - 無線クライアントは無線システムで検出されましたが、セキュリティの脅威ではありません。 • Black-Listed - この MAC アドレスを持つクライアントは、MAC 認証経由で明確にアクセスを拒否されます。 • Rogue - クライアントは、脅威検出アルゴリズムの 1 つによって脅威として分類されます。
Age	検出クライアントデータベースエントリを更新したこのクライアントに何らかのイベントが受信されてから経過した時間を表示します。
Create Time	このエントリが検出クライアントデータベースに最初に追加されてから経過した時間を表示します。

「WLAN Detected Clients List」を右クリックするとオプションが表示されます。

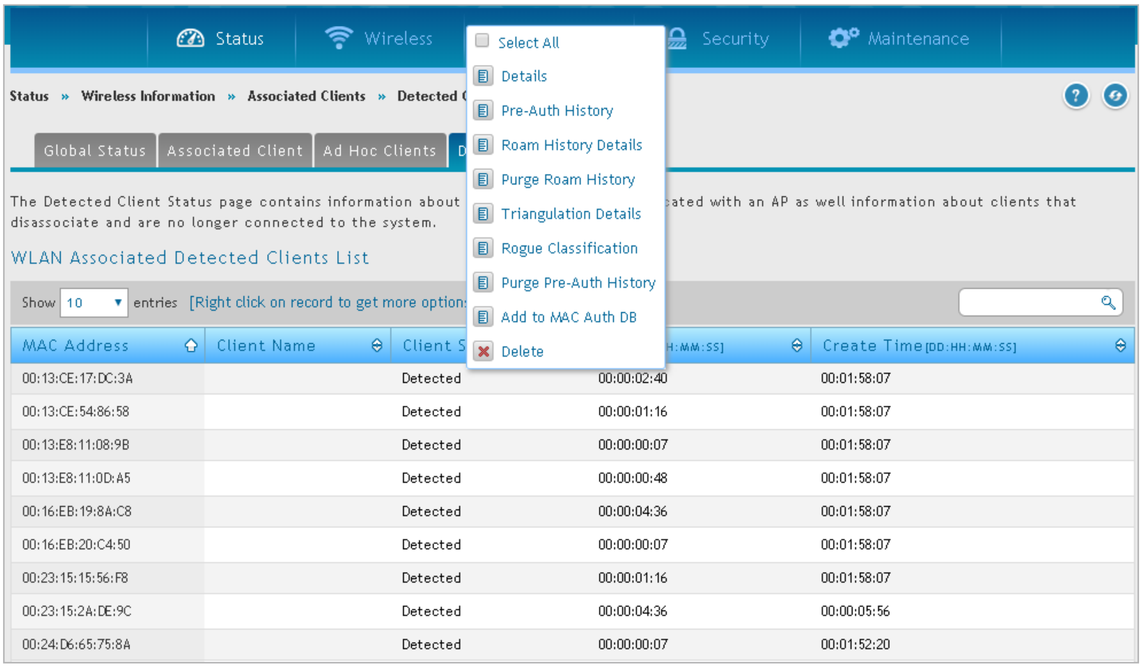


図 8-59　WLAN Associated Detected Clients List 画面 - オプションメニュー

以下のオプションがあります。

項目	説明
Details	選択したクライアントに関する詳細情報を表示します。
Pre-Auth History	検出されたクライアントが行った事前認証要求に関する情報を表示します。
Roam History Details	管理下にある 1 つのアクセスポイントから別のアクセスポイントまでローミングした時の記録を表示します。クライアント毎に最大 10 個のアクセスポイントの履歴が保持されます。
Purge Roam History	「Roam History」セクションから現在のローミングヒストリのデータをクリアします。
Triangulation Detail	クライアントを検出した 3 個までの non-sentry および 3 個までの管理対象のアクセスポイントを表示します。
Rogue Classification	脅威検出テストの結果、クライアントがエラーとなったテストに関する情報を提供します。
Purge Pre-auth History	「Pre-Auth History」から事前認証のデータをクリアします。
Add to MAC Auth DB	MAC 認証データベースへ追加します。

Client Statistics（詳細情報）

クライアントを右クリックし、「Details」を選択して、以下の画面を表示します。

図 8-60　Detected Clients Status 画面

以下の項目があります。

項目	説明
MAC Address	クライアントの MAC アドレスを表示します。
Client Status	クライアントの状態を表示します。 ・Authenticated - 無線クライアントはシステムで認証され、「Rogue」（不正）ではありません。 ・Detected - クライアントは検出されましたが、認証されておらず、「Rogue」ではなく、Known Clients データベースには存在しません。 ・Known - クライアントは Known Clients データベースで検出されましたが、認証されていません。 ・Black Listed - クライアントはシステムに接続しようとしましたが、MAC 認証で拒否されました。 ・Rogue - クライアントは有効な脅威テストでエラーになりました。
Authentication Status	このクライアントが認証されるかどうかを表示します。 注意　クライアントステータスが「Rogue」（不正）であっても、認証ステータスが「Authenticated」であることもあります。
Threat Detection	クライアントに対して脅威検出テストが起動されたかどうかを表示します。テストが無効にされると、クライアントは Rogue としてマークされませんが、脅威が引き起こされた理由を調査することはできます。
Threat Mitigation Status	このクライアントに脅威の軽減を行ったどうかを表示します。
Time Since Entry Last Updated	検出クライアントデータベースのエントリを更新したこのクライアントに何らかのイベントが受信されてから経過した時間を表示します。
Time Since Entry Create	このエントリが検出クライアントデータベースに最初に追加されてから経過した時間を表示します。
Client Name	「Known Client Database」内のクライアント名を表示します。データベースにクライアントが存在しない場合、このフィールドは空白です。
RSSI	クライアントが管理対象のアクセスポイントに認証されると、本フィールドはクライアントを認証するアクセスポイントが報告した最後の RSSI 値（1-100%）を表示します。0 の値は、アクセスポイントが検出されないことを意味します。
Signal	クライアントを認証する管理アクセスポイントが報告した最後の信号強度（-128 ～ 128 dBm）を表示します。
Noise	クライアントを認証する管理アクセスポイントが報告した最後のチャンネルノイズ（-128 ～ 128 dBm）を表示します。
Probe Req Recorded	「Probe Collection Interval」に記録したプローブリクエスト数を表示します。
Probe Collection Interval	各プローブ収集に費やした時間を表示します。プローブ収集は、クライアントが脅威であるかどうかをコントローラが判断するために役立ちます。
Highest Probes Detected	コントローラが「Probe Collection Interval」に検出したプローブの最大数を表示します。
Channel	クライアントが使用しているチャンネルを表示します。
OUI Description	OUI の情報を表示します。
Auth Msgs Recorded	「Auth Collection Interval」（認証収集間隔）に記録した IEEE 802.11 の Authentication メッセージ数を表示します。
Auth Collection Interval	各認証収集に費やした時間を表示します。認証の収集は、クライアントが脅威であるかどうかをコントローラが判断するために役立ちます。
Highest Auth Msgs	コントローラが「Auth Collection Interval」の間に検出した Authentication メッセージの最大数を表示します。
De-Auth Msgs Recorded	認証収集期間に記録した IEEE 802.11 De-Authentication メッセージ数を表示します。
De-Auth Collection Interval	各認証解除の収集に費やした時間を表示します。De-Authentication の収集は、クライアントが脅威であるかどうかをコントローラが判断するために役立ちます。
Highest De-Auth Msgs	コントローラが「De-Auth Collection Interval」に検出した De-Authentication メッセージの最大数を表示します。
Authentication Failures	クライアントで検出された 802.1X 認証エラーの数を表示します。
Probes Detected	最後の RF スキャンで検出したプローブ数を表示します。
Broadcast BSSID Probes	最後の RF スキャンで検出したブロードキャスト BSSID に対するプローブ数を表示します。
Broadcast SSID Probes	最後の RF スキャンで検出したブロードキャスト SSID に対するプローブ数を表示します。
Specific BSSID Probes	最後の RF スキャンで検出した特定の BSSID に対するプローブ数を表示します。
Specific SSID Probes	最後の RF スキャンで検出した特定の SSID に対するプローブ数を表示します。
Last Non-Broadcast BSSID	RF スキャンで最後に検出した非ブロードキャスト BSSID（MAC アドレス）を表示します。
Last Non-Broadcast SSID	RF スキャンで最後に検出した非ブロードキャスト SSID を表示します。
Threat Mitigation Sent	このクライアントに脅威の軽減を行ったどうかを表示します。

Pre-Auth History（事前認証要求に関する情報）

クライアントを右クリックし、「Pre-Auth History」を選択して、以下の画面を表示します。

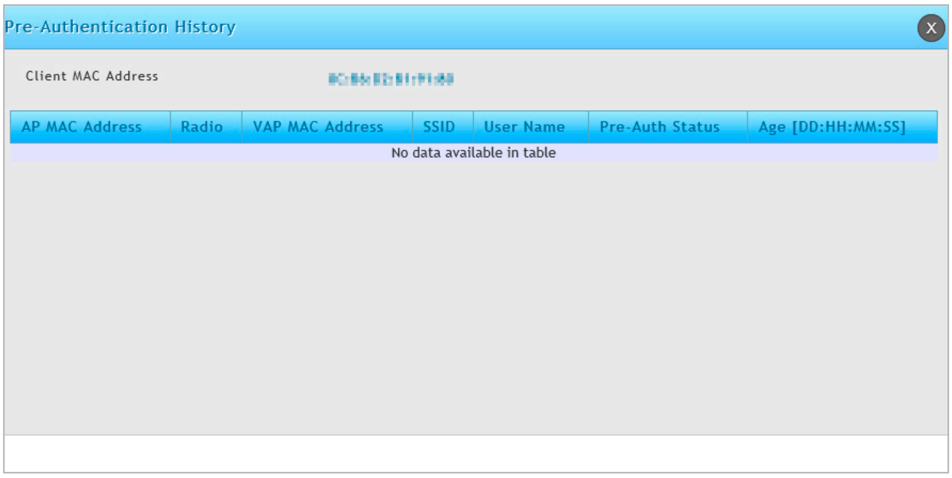


図 8-61　Pre-Authentication History 画面

以下の項目があります。

項目	説明
Client MAC Address	クライアントの MAC アドレスを表示します。
AP MAC Address	クライアントを事前認証する管理アクセスポイントの MAC アドレスを表示します。
Radio	クライアントが認証される無線インタフェースの番号（Radio1 または Radio2）を表示します。
VAP MAC Address	クライアントがローミングを行った VAP の MAC アドレスを表示します。
SSID	VAP が使用される SSID 名を表示します。
User Name	802.1X により認証されているクライアントのユーザ名を表示します。
Pre-Auth Status	クライアントが認証に成功したかどうかを「Success」（成功）または「Failure」（失敗）のステータスで表示します。
Age	ヒストリエントリが追加されてから経過した時間を表示します。

Roam History Details（ローミングの記録）

クライアントを右クリックし、「Roam History Details」を選択して、以下の画面を表示します。

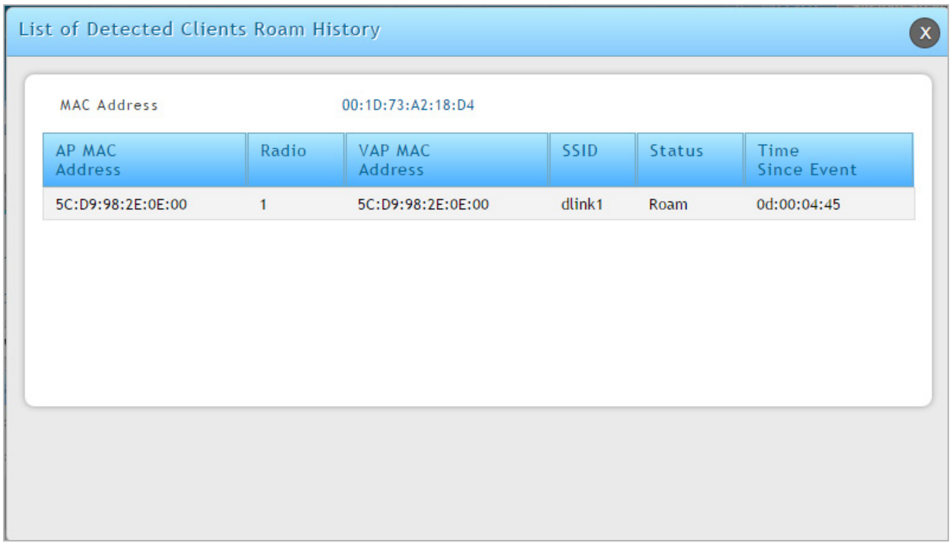


図 8-62　Detailed Clients Roam History 画面

以下の項目があります。

項目	説明
MAC Address	検出されたクライアントの MAC アドレスを表示します。
AP MAC Address	クライアントを認証した管理対象のアクセスポイントの MAC アドレスを表示します。
Radio	クライアントが認証される無線インタフェースの番号を表示します。
VAP MAC Address	クライアントがローミングを行った VAP の MAC アドレスを表示します。
SSID	VAP が使用される SSID 名を表示します。
Status	履歴エントリが新しい認証またはローミングイベントかどうかを示すフラグを表示します。
Time Since Event	履歴エントリが追加されてから経過した時間を表示します。

Triangulation Detail（Triangulation の詳細）

クライアントを右クリックし、「Triangulation Detail」を選択して、以下の画面を表示します。

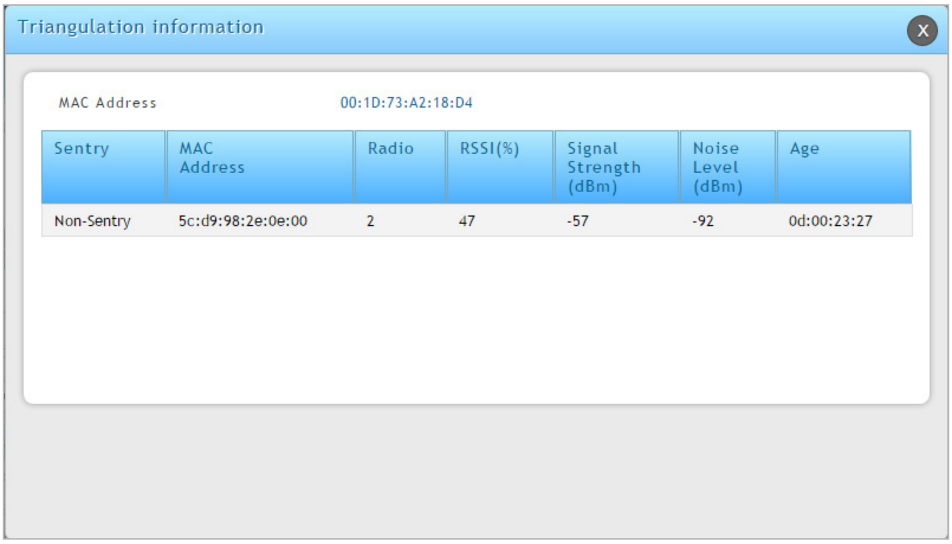


図 8-63　List of Threat Detection Tests 画面

以下の項目があります。

項目	説明
Detected Client MAC Address	クライアントの MAC アドレスを表示します。
Sentry	クライアントを検出した無線インタフェースのモード（Sentry または Non-Sentry）を表示します。 • Non-Sentry - クライアントを検出した無線帯域は、Sentry モードで設定されません。これは、無線インタフェースが、無線クライアントからの接続を受け入れ、トラフィックの送受信を行うことができることを意味します。 • Sentry - クライアントを検出した無線帯域が Sentry モードで設定されます。Sentry AP を配置するネットワークまたは無線インタフェースは、ネットワーク上のデバイスをより迅速に検出して、より徹底的なセキュリティ分析を行うことができます。
MAC Address	クライアントを検出した管理アクセスポイントの MAC アドレスを表示します。
Radio	クライアントが認証される無線インタフェースの番号（Radio1 または Radio2）を表示します。
RSSI	non-sentry AP の受信信号強度（0-100%）を表示します。0 の値は、クライアントが検出されないことを示します。
Signal Strength	受信信号強度（dBm）を表示します。有効な範囲は -127 ～ 127（dBm）ですが、現実的な範囲は -95 ～ -10（dBm）です。
Noise Level	non-sentry AP がチャンネルについて報告したノイズ（-127 ～ 127dBm）を表示します。
Age	このアクセスポイントが信号を検出してから経過した時間を表示します。

Rogue Classification（Rogue の分類）

クライアントを右クリックし、「Rogue Classification」を選択して、以下の画面を表示します。

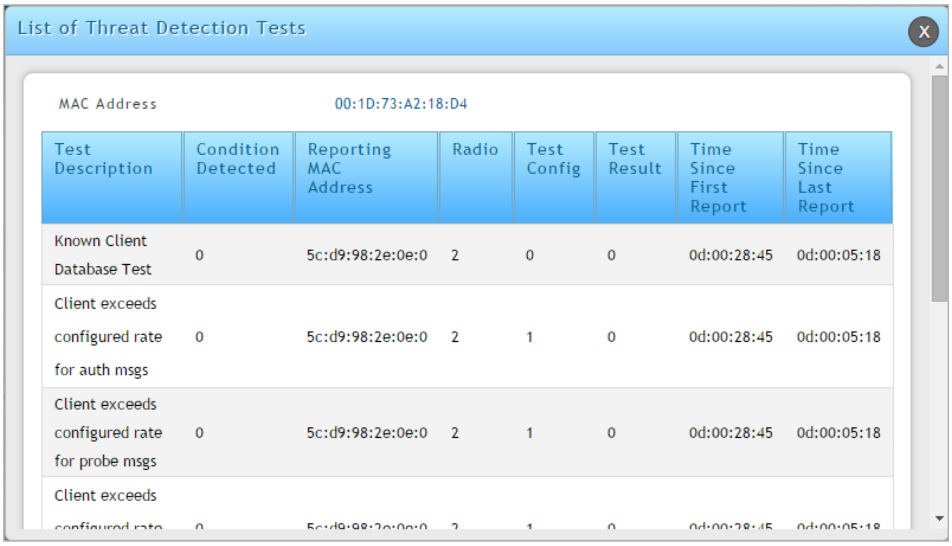


図 8-64　Treat Detection Tests 画面

以下の項目があります。

項目	説明
MAC Address	検出されたアクセスポイントの MAC アドレスを表示します。
Test Description	実行されたテストを表示します。 • Administrator-Configured rogue AP - 管理者が設定した不正アクセスポイント • Managed SSID received from an unknown AP - 不明なアクセスポイントから受信した管理 SSID • Managed SSID from a fake managed AP - 偽の管理対象アクセスポイントから受信した管理 SSID • Fake managed AP on an invalid channel - 不正チャンネルにおける偽の管理対象アクセスポイント • AP without an SSID - SSID を持たないアクセスポイント • Managed SSID detected with incorrect security configuration - 不正なセキュリティ設定を持つことが検出された管理 SSID • Invalid SSID received from managed AP - 管理対象アクセスポイントから受信した不正な SSID • AP is operating on an illegal channel - アクセスポイントが不正なチャンネルで動作中 • Standalone AP is operating with unexpected configuration - スタンドアロンモードのアクセスポイントが予期しない設定を使用して動作中 • Unmanaged AP detected on wired network - 管理対象でないアクセスポイントを有線ネットワークで検出
Condition Detected	テストの結果が正しいかどうかを表示します。
Reporting MAC Address	テスト結果を報告したアクセスポイントの MAC アドレスを表示します。
Radio	報告されたアクセスポイントのどの物理無線帯域がテスト結果の原因となったかを表示します。
Test Config	このテストが不正を報告するように設定されているかどうかを表示します。不正として確実に結果を報告するために、各テストをグローバルに有効 または無効 にします。
Test Result	このテストが、デバイスを不正であると報告したかどうかを表示します。場合によっては、デバイスがこのモードで許可されているため不正ではなく有効であるとして、肯定的なレポートとなる可能性があります。
Time Since First Report	このテストが最初にこの条件を検出した時期を示すタイムスタンプを表示します。
Time Since Last Report	このテストが最後にこの条件を検出した時期を示すタイムスタンプを表示します。

クラスタ情報の参照

Status > Wireless Information > Clustering メニュー

ネットワーク内の他の無線コントローラに関する情報を表示します。同じクラスタ内のピア無線コントローラ同士は、配下のアクセスポイントおよびクライアントのデータを交換します。無線コントローラはこのデータをデータベースに保持するため、IP アドレスやソフトウェアバージョンなどのピアに関する情報を参照できます。コントローラとピア間の接続が失われると、ピアのデータすべてが削除されます。クラスタ内の無線コントローラの 1 つがクラスタコントローラとして選出されます。

クラスタコントローラは、クラスタ内の他のコントローラから状態と統計情報を収集します。これには、アクセスポイントのピアコントローラ、およびアクセスポイントに接続するクライアントに関する情報が含まれます。

Status > Wireless Information > Clustering の順にメニューをクリックし、以下の画面を表示します。

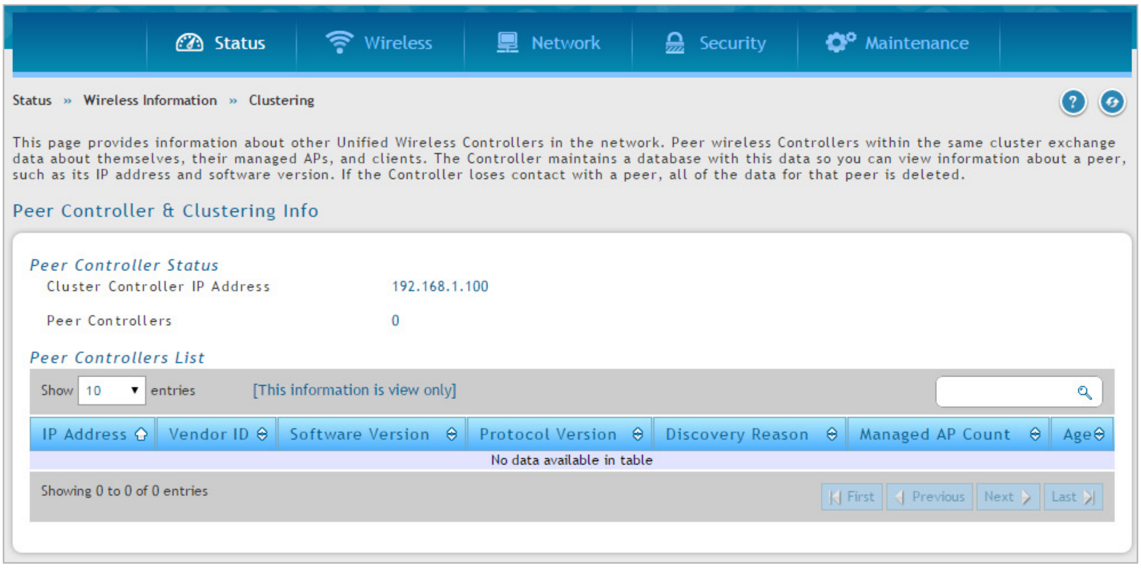


図 8-65　Peer Controller & Clustering Info 画面

以下の項目があります。

項目	説明
Peer Controller Status	
Cluster Controller IP Address	クラスタを制御するコントローラの IP アドレスを表示します。
Peer Controllers	ピアコントローラの数を表示します。
Peer Controllers List	
IP Address	クラスタ内の無線コントローラの IP アドレスを表示します。
Vendor ID	ピアコントローラのソフトウェアのベンダ ID を表示します。
Software Version	特定のピアコントローラのソフトウェアバージョンを表示します。
Protocol Version	ピア無線コントローラのソフトウェアがサポートするプロトコルのバージョンを表示します。
Discovery Reason	L2 ポーリングまたは IP ポーリングを通じた、特定のピア無線コントローラの検出方法を表示します。
Managed AP Count	無線コントローラが現在管理するアクセスポイントの数を表示します。
Age	無線コントローラとの通信から経過した時間（時 : 分 : 秒）を表示します。

WDS グループ状態の参照

Status > Wireless Information > WDS Groups Status > WDS Groups Status メニュー

WDS は、アクセスポイント同士を無線で接続し、相互に通信する機能です。

他の管理対象のアクセスポイントを経由した無線通信の WDS リンクを使用して、クラスタに管理対象のアクセスポイントを追加することができます。

WDS を使用すると、ネットワークへの有線接続ができない屋外などにアクセスポイントを設置することが可能になります。

WDS AP グループは以下の管理対象のアクセスポイントから成ります。

- ルート AP - 無線メディアにおいてブリッジまたはリピータとして機能し、有線リンクを通じてコントローラと通信します 。
- サテライト AP - ルート AP への WDS リンクを通してコントローラと通信します。

本ページでは、設定済みの WDS リンクに関するサマリ情報を表示します。表示するためには、少なくとも 1 つのグループをフィールドに設定する必要があります。WDS AP グループを設定するには、**Wireless > Access Point > WDS Groups** 画面を使用します。

Status > Wireless Information > WDS Groups Status > WDS Groups Status の順にメニューをクリックし、以下の画面を表示します。

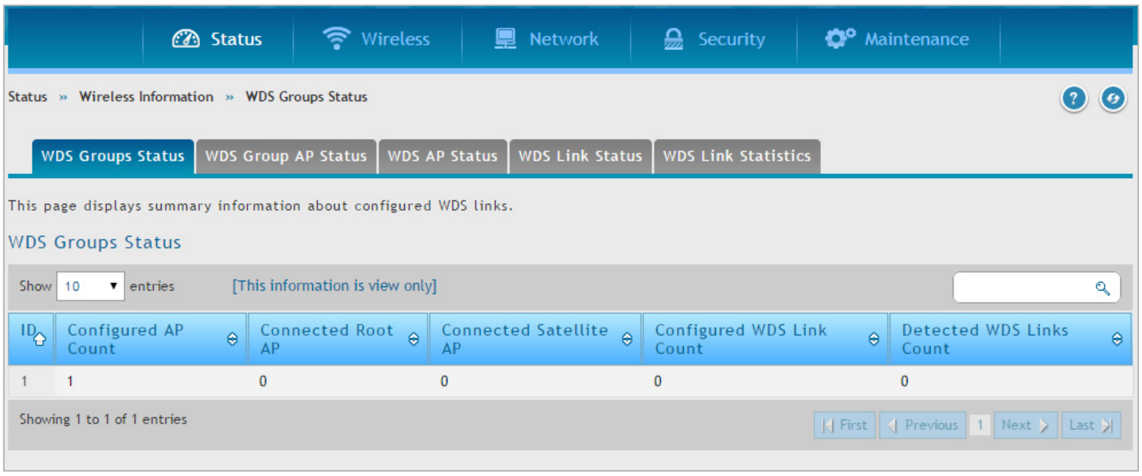


図 8-66　 WDS Groups Status 画面

以下の項目があります。

項目	説明
ID	WDS AP グループを特定する固有の番号を表示します。
Configured AP Count	この WDS AP グループに設定されたアクセスポイントの数を表示します。
Connected Root AP	この WDS AP グループのメンバであるコントローラが現在管理しているルート AP の数を表示します。
Connected Satellite AP	この WDS AP グループのメンバであるコントローラが現在管理しているサテライト AP の数を表示します。
Configured WDS Link Count	WDS AP グループで設定されているリンクの数を表示します。
Detected WDS Links Count	システムに検出された WDS リンクの数を表示します。リンクをカウントするためには、リンクの両端にあるシステム AP 同士で、相互に検出し合う必要があります。

WDS グループのアクセスポイントの状態

Status > Wireless Information > WDS Groups Status > WDS Group AP Status メニュー

WDS グループに設定しているアクセスポイントとリンクに関する詳細情報を表示します。また、このページから、グループのメンバに新しいパスワードを送信することができます。

1. **Status > Wireless Information > WDS Groups Status > WDS Groups AP Status** の順にメニューをクリックし、以下の画面を表示します。

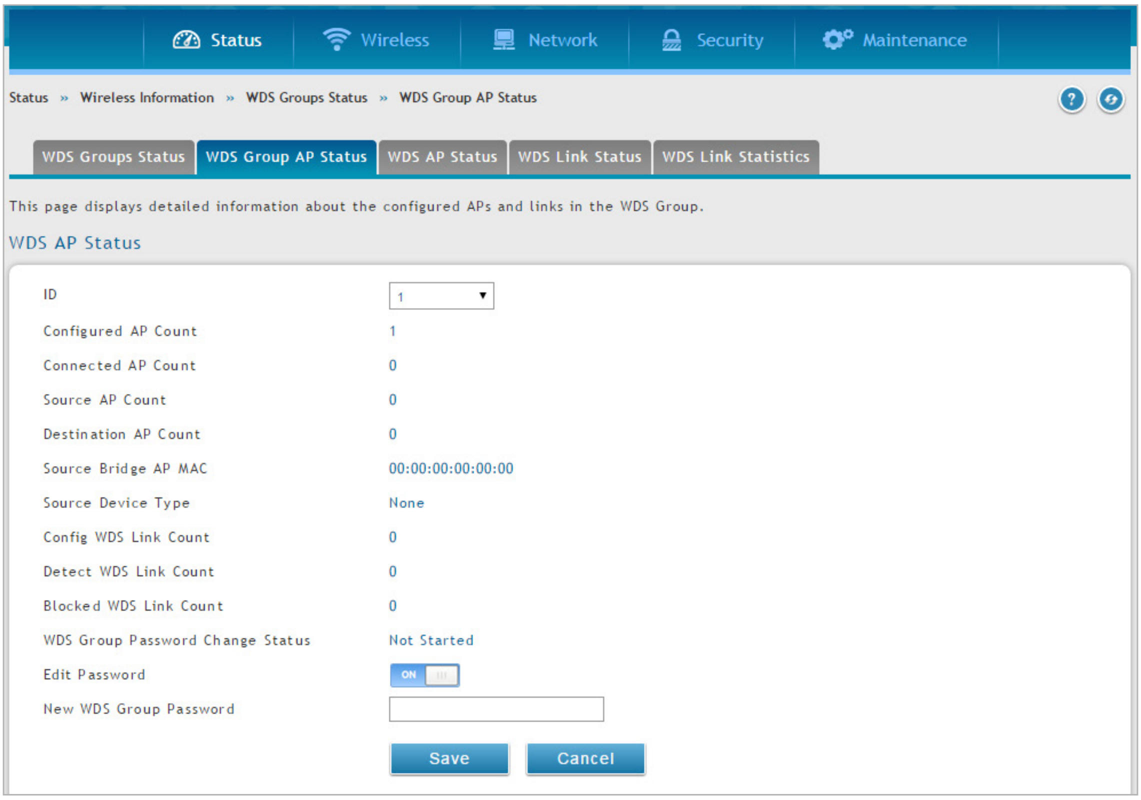


図 8-67　WDS AP Status 画面

2. 以下の項目を入力し、「Save」ボタンをクリックします。

項目	説明
ID	WDS AP グループを特定する固有の番号を表示します。
Configured AP Count	この WDS AP グループに設定されたアクセスポイントの数を表示します。
Connected AP Count	この WDS AP グループのメンバであるコントローラが現在管理しているアクセスポイントの数を表示します。この数は「Connected Root AP」と「Connected Satellite AP」の合計です。
Source AP Count	この WDS AP グループのメンバであるコントローラが現在管理しているルート AP の数を表示します。
Destination AP Count	この WDS AP グループのメンバであるコントローラが現在管理しているサテライト AP の数を表示します。
Source Bridge AP MAC	スパニングツリーのルートブリッジとして選出されたデバイスの MAC アドレスを表示します。スパニングツリーを無効にすると、この値は「00:00:00:00:00:00」となります。
Source Device Type	スパニングツリーのルートブリッジとして選出されたデバイスのタイプを表示します。 ・None（STP は無効） ・Root AP ・Satellite AP ・外部のデバイス（STP Root はアクセスポイントの 1 つではありません。）
Config WDS Link Count	WDS AP グループで設定されているリンクの数を表示します。
Detect WDS Link Count	システムに検出された WDS リンクの数を表示します。リンクをカウントするためには、リンクの両端にあるシステム AP 同士で、相互に検出し合う必要があります。
Blocked WDS Link Count	スパニングツリープロトコルがブロックした WDS リンクの数を表示します。リンクの片方にあるアクセスポイントが、リンクをブロック中として報告すると、このステータスパラメータによってそのリンクがカウントされます。
WDS Group Password Change Status	WDS グループのパスワードの設定を最後に試みた時の状態を表示します。 ・Not Started（未始動） ・Success（成功） ・Invalid Password（無効なパスワード） ・Requested（要求済み） ・Timed Out（タイムアウト）
Edit Password	WDS グループ内のすべてのコントローラおよびアクセスポイントのパスワードを変更するためには、「ON」にします。
New WDS Group Password	「Edit Password」が「ON」の時、新しいパスワード（8-63 文字）を入力します。

WDS アクセスポイント状態の参照

Status > Wireless Information > WDS Groups Status > WDS AP Status メニュー

WDS グループに設定しているアクセスポイントに関するサマリ情報を表示します。

Status > Wireless Information > WDS Groups Status > WDS AP Status の順にメニューをクリックし、以下の画面を表示します。

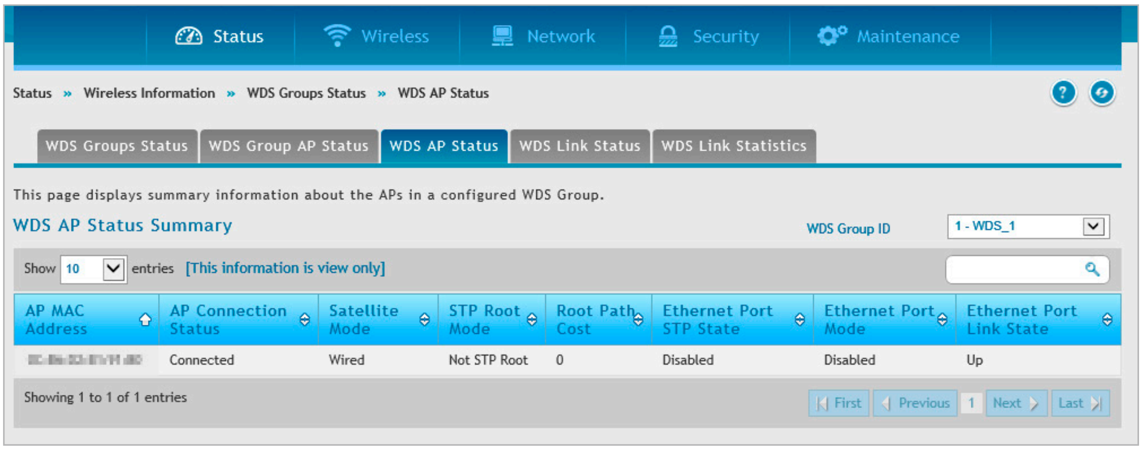


図 8-68　WDS AP Status Summary 画面

以下の項目があります。

項目	説明
WDS Group ID	プルダウンメニューを使用して、設定済みの WDS AP グループを識別するグループ番号を選択します。
AP MAC Address	MAC アドレスによりグループ内のアクセスポイントを識別します。
AP Connection Status	現在、クラスタコントローラの 1 つにアクセスポイントが管理されているか否かを示します。
Satellite Mode	アクセスポイントが WDS リンクでネットワークに接続するサテライト AP か、有線リンクを通じてネットワークに接続するルート AP かを示します。
STP Root Mode	このアクセスポイントがスパニングツリーのルートであるか否かを示します。スパニングツリーを無効にすると、アクセスポイントは「Not STP Root」（STP ルートではない）として常に報告されます。
Root Path Cost	ルートへのスパニングツリーパスコストを示します。ルート AP は常にこの値を 0 として報告します。スパニングツリーを無効にした場合も、値は 0 となります。
Ethernet Port STP State	スパニングツリーが WDS グループ内のアクセスポイントで有効である場合、このステータスパラメータにより、イーサネットポートのスパニングツリーの状態が確認できます。
Ethernet Port Mode	サテライト AP では、イーサネットポートを手動で無効にすることができます。ルート AP では、ポートは常に有効です。
Ethernet Port Link State	イーサネットポートが有効である場合、このステータスにより、ポートのリンクステートが確認できます。

WDS リンク状態の参照

Status > Wireless Information > WDS Groups Status > WDS Link Status メニュー

WDS グループのリンク設定およびリンクステートに関するサマリ情報を表示します。

Status > Wireless Information > WDS Groups Status > WDS Link Status の順にメニューをクリックし、以下の画面を表示します。

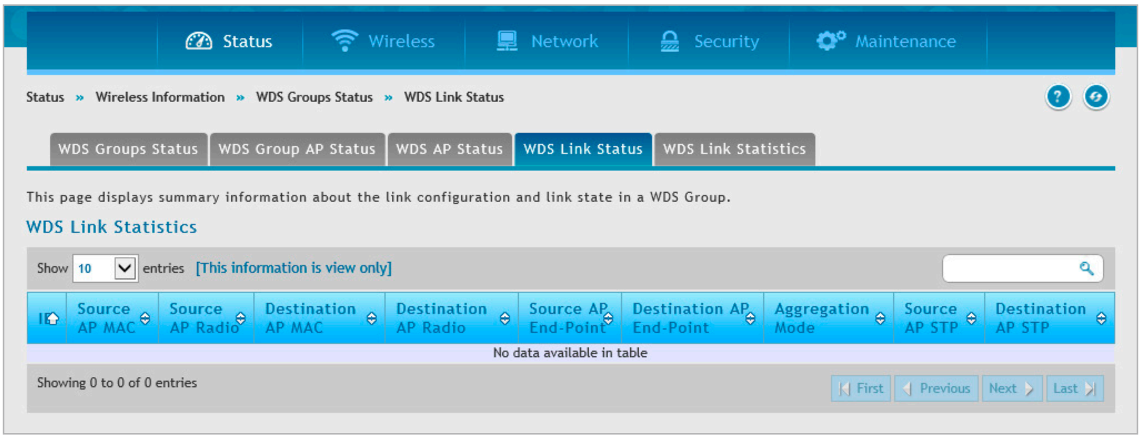


図 8-69　WDS Link Status 画面

以下の項目があります。

項目	説明
ID	定義済みの WDS AP グループを識別するグループ番号を表示します。
Source AP MAC	WDS リンクの片側のエンドポイントの MAC アドレスを表示します。
Source AP Radio	送信元アクセスポイントの WDS リンク終端の無線電波番号を表示します。
Destination AP MAC	グループ内の送信先アクセスポイントの MAC アドレスを表示します。
Destination AP Radio	送信先アクセスポイントの WDS リンク終端の無線電波番号を表示します。
Source AP End-Point	送信先 MAC アドレスで指定されたアクセスポイントが、送信元 MAC アドレスで指定されたアクセスポイントを検出したか否かを表示します。
Destination AP End-Point	送信元 MAC で指定されたアクセスポイントが、送信先 MAC で指定されたアクセスポイントを検出したか否かを表示します。
Aggregation Mode	並列リンクが 2 つのアクセスポイントの間で定義される場合、このフィールドは、このリンクがアグリゲーションリンクのペアの一部であるか否かを示します。
Source AP STP	送信元アクセスポイントへのリンクのスパニングツリーステートを示し、以下の項目のいずれかとなります。 • Disabled（STP が無効またはリンクダウン） • Forwarding • Learning • Listening • Blocking
Destination AP STP	送信先アクセスポイントへのリンクのスパニングツリーステートを示し、以下の項目のいずれかとなります。 • Disabled（STP が無効またはリンクダウン） • Forwarding • Learning • Listening • Blocking

WDS リンクの統計情報の参照

Status > Wireless Information > WDS Groups Status > WDS Link Statistics メニュー

WDS リンクで送受信したパケットに関するサマリ情報を表示します。

Status > Wireless Information > WDS Groups Status > WDS Link Statistics の順にメニューをクリックし、以下の画面を表示します。

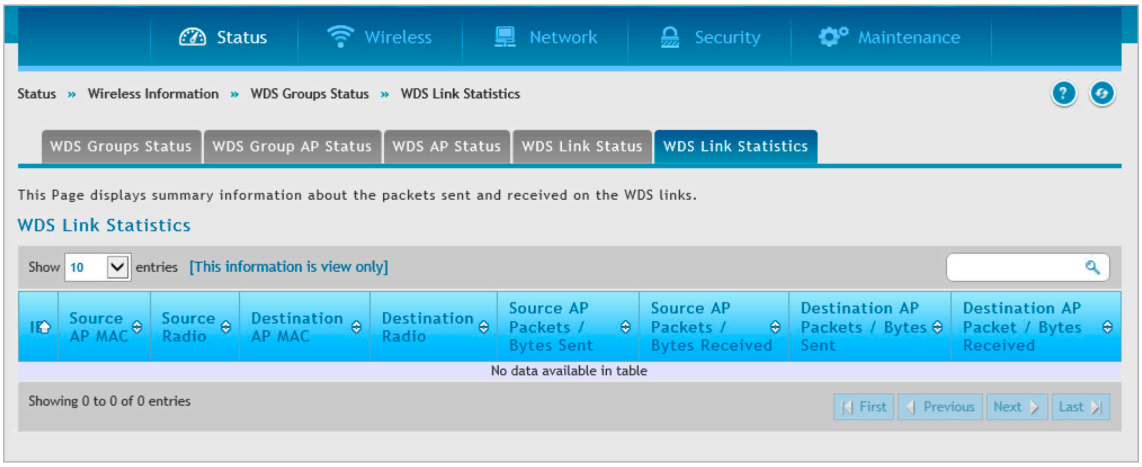


図 8-70　WDS Link Statistics 画面

以下の項目があります。

項目	説明
ID	定義済みの WDS AP グループを識別するグループ番号を表示します。
Source AP MAC	WDS リンクの片側のエンドポイントの MAC アドレスを表示します。
Source Radio	送信元アクセスポイントの WDS リンク終端の無線電波番号を表示します。
Destination AP MAC	グループ内の送信先アクセスポイントの MAC アドレスを表示します。
Destination Radio	送信先アクセスポイントの WDS リンク終端の無線電波番号を表示します。
Source AP Packets / Bytes Sent	送信元アクセスポイントが送信したパケット / バイト数を表示します。
Source AP Packets / Bytes Received	送信元アクセスポイントが受信したパケット / バイト数を表示します。
Destination AP Packets / Bytes Sent	送信先アクセスポイントが送信したパケット / バイト数を表示します。
Destination AP Packets / Bytes Received	送信先アクセスポイントが受信したパケット / バイト数を表示します。

IP ACL 情報の参照

Status > ACL & DiffServ > IP ACL メニュー

IP ACL に関する情報を表示します。

Status > ACL & DiffServ > IP ACL の順にメニューをクリックし、以下の画面を表示します。

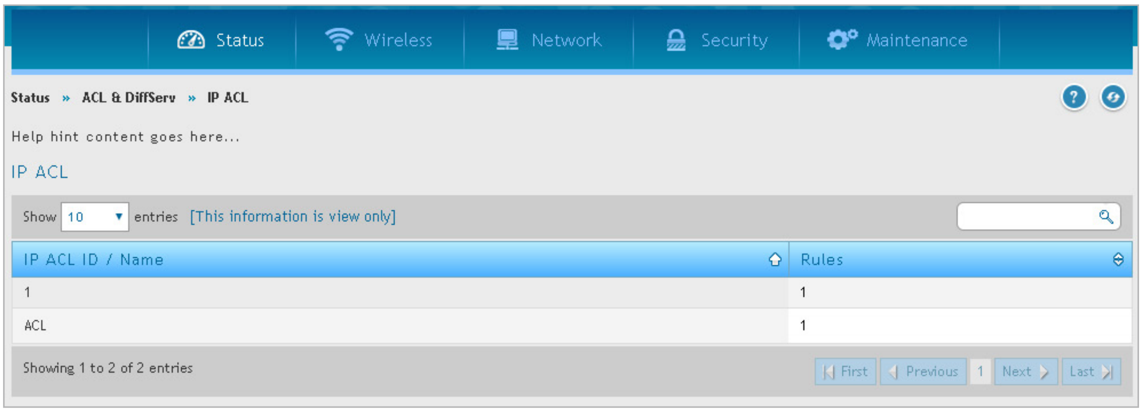


図 8-71　IP ACL 画面

以下の項目があります。

項目	説明
IP ACL ID / Name	IP ACL ID、または IP ACL 名を表示します。
Rules	IP ACL のルール数を表示します。

IP ACL ルール情報の参照

Status > ACL & DiffServ > IP ACL Rules メニュー

IP ACL ルールに関する情報を表示します。

Status > ACL & DiffServ > IP ACL Rules の順にメニューをクリックし、以下の画面を表示します。

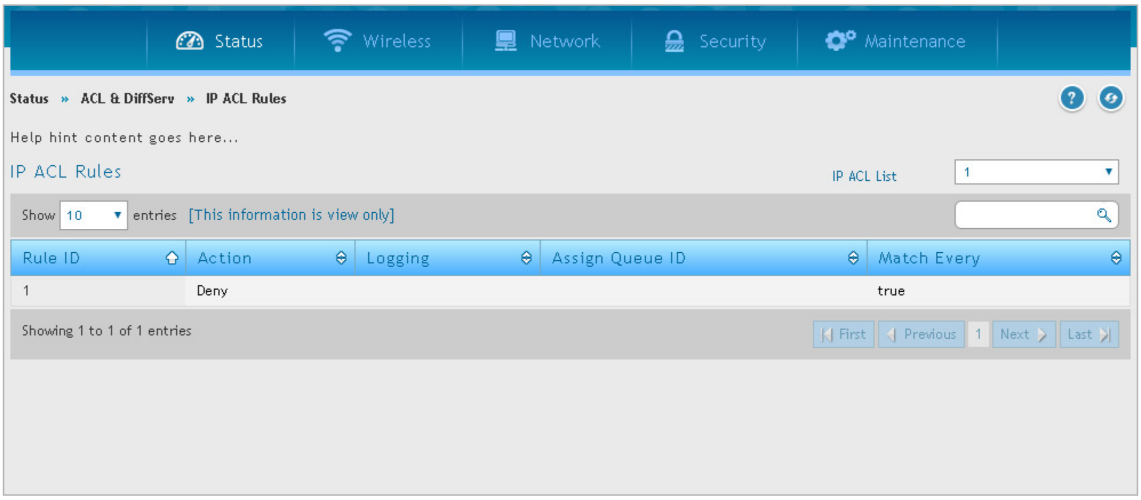


図 8-72　IP ACL Rules 画面

以下の項目があります。

項目	説明
Rule ID	IP ACL ルール ID を表示します。
Action	IP ACL ルールのアクションを表示します。
Logging	IP ACL のロギングの有無を表示します。
Assign Queue ID	割り当てられたキュー ID を表示します。
Match Every	Match Every の有効 / 無効を表示します。

MAC ACL 情報の参照

Status > ACL & DiffServ > MAC ACL メニュー

MAC ACL に関する情報を表示します。

Status > ACL & DiffServ > MAC ACL の順にメニューをクリックし、以下の画面を表示します。

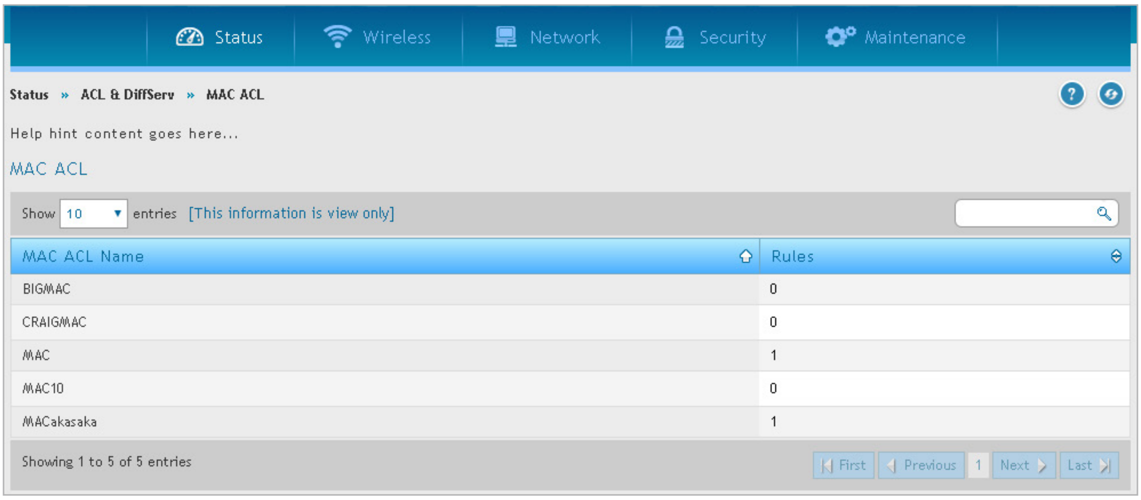


図 8-73　MAC ACL 画面

以下の項目があります。

項目	説明
MAC ACL Name	MAC ACL 名を表示します。
Rules	MAC ACL のルール数を表示します。

MAC ACL ルール情報の参照

Status > ACL & DiffServ > MAC ACL Rules メニュー

MAC ACL ルールに関する情報を表示します。

Status > ACL & DiffServ > MAC ACL Rules の順にメニューをクリックし、以下の画面を表示します。

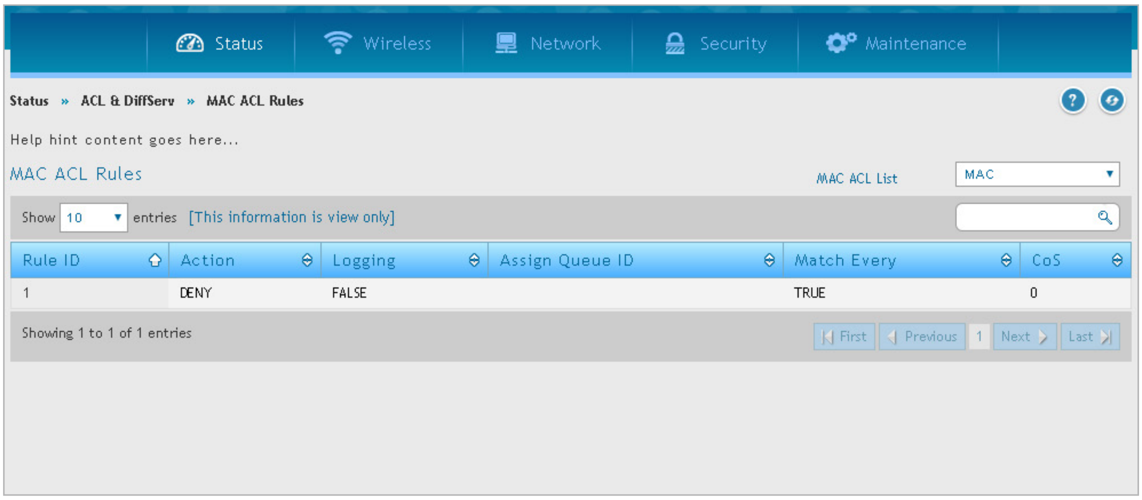


図 8-74　MAC ACL Rules 画面

以下の項目があります。

項目	説明
Rule ID	MAC ACL ルール ID を表示します。
Action	MAC ACL ルールのアクションを表示します。
Logging	MAC ACL のロギングの有無を表示します。
Assign Queue ID	割り当てられたキュー ID を表示します。
Match Every	Match Every の有効 / 無効を表示します。
CoS	CoS 番号を表示します。

DiffServ クラス情報の参照

Status > ACL & DiffServ > DiffServ Class メニュー

DiffServ クラスに関する情報を表示します。

Status > ACL & DiffServ > DiffServ Class の順にメニューをクリックし、以下の画面を表示します。

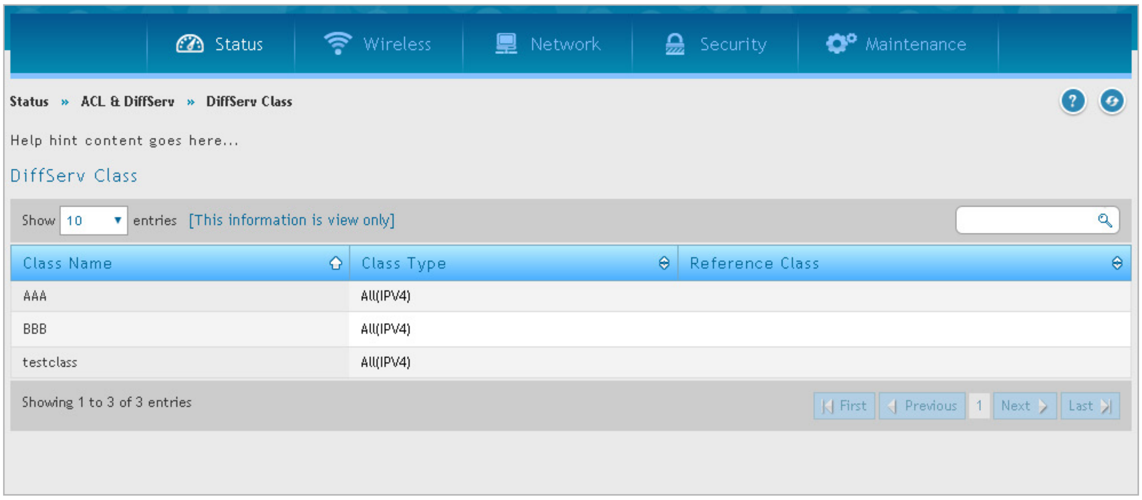


図 8-75　DiffServ Class 画面

以下の項目があります。

項目	説明
Class Name	DiffServ クラス名を表示します。
Class Type	DiffServ クラスタイプを表示します。
Reference Class	参照クラスを表示します。

DiffServ ポリシー情報の参照

Status > ACL & DiffServ > DiffServ Policy メニュー

DiffServ ポリシーに関する情報を表示します。

Status > ACL & DiffServ > DiffServ Policy の順にメニューをクリックし、以下の画面を表示します。

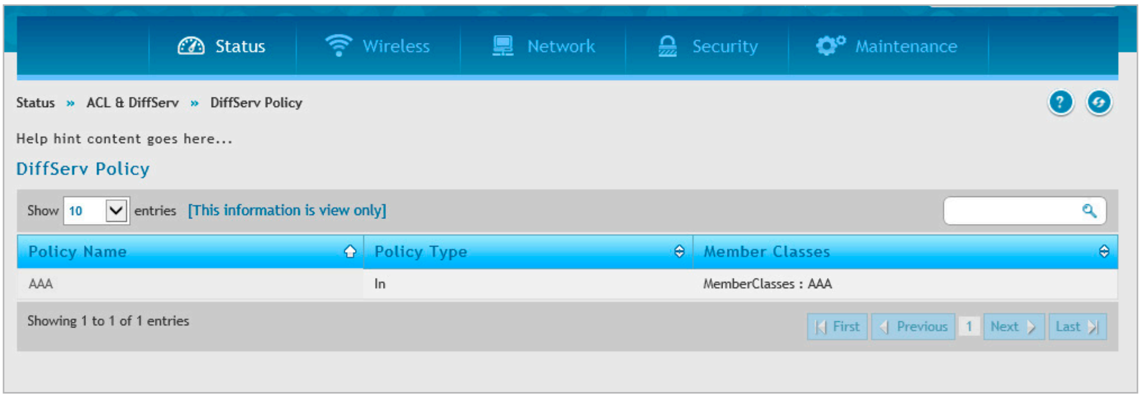


図 8-76　DiffServ Policy 画面

以下の項目があります。

項目	説明
Policy Name	DiffServ ポリシー名を表示します。
Policy Type	DiffServ ポリシータイプを表示します。
Member Classes	DiffServ メンバクラスを表示します。

DiffServ ポリシー属性情報の参照

Status > ACL & DiffServ > DiffServ Policy Attribute メニュー

DiffServ ポリシー属性に関する情報を表示します。

Status > ACL & DiffServ > DiffServ Policy Attribute の順にメニューをクリックし、以下の画面を表示します。

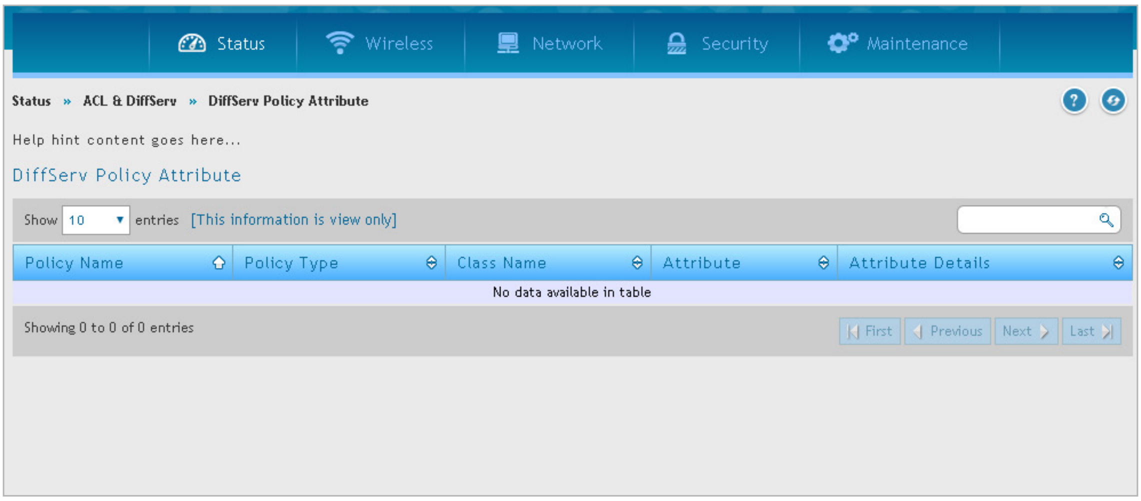


図 8-77　DiffServ Policy Attribute 画面

以下の項目があります。

項目	説明
Policy Name	DiffServ ポリシー名を表示します。
Policy Type	DiffServ ポリシータイプを表示します。
Class Name	DiffServ クラス名を表示します。
Attribute	DiffServ 属性を表示します。
Attribute Details	DiffServ 属性詳細を表示します。

第 9 章　メンテナンス

本章では以下のメンテナンス作業について説明します。

設定項目	説明
システム設定	コントローラの識別名、時刻、セッションタイムアウト、USB 設定などを行います。
ライセンスのアクティブ化	無線コントローラに追加するアクセスポイントのライセンスをアクティブ化します。
UI 管理	ローカルネットワーク外からの無線コントローラの UI 管理を有効にします。
SNMP の使用	SNMP 設定を行います。
ココンフィグレーションの保存と復元	コンフィグレーションの保存と復元を行います。
ファームウェアのアップグレード	無線コントローラのファームウェアをアップグレードします。
コマンドラインインタフェースの使用	VT-100 端末エミュレーションプログラムを使用する CLI インタフェースに接続します。

システム設定

システム名の設定

Maintenance > Administration > System Setting メニュー

コントローラの識別名を入力します。

1. **Maintenance > Administration > System Setting** の順にメニューをクリックし、以下の画面を表示します。

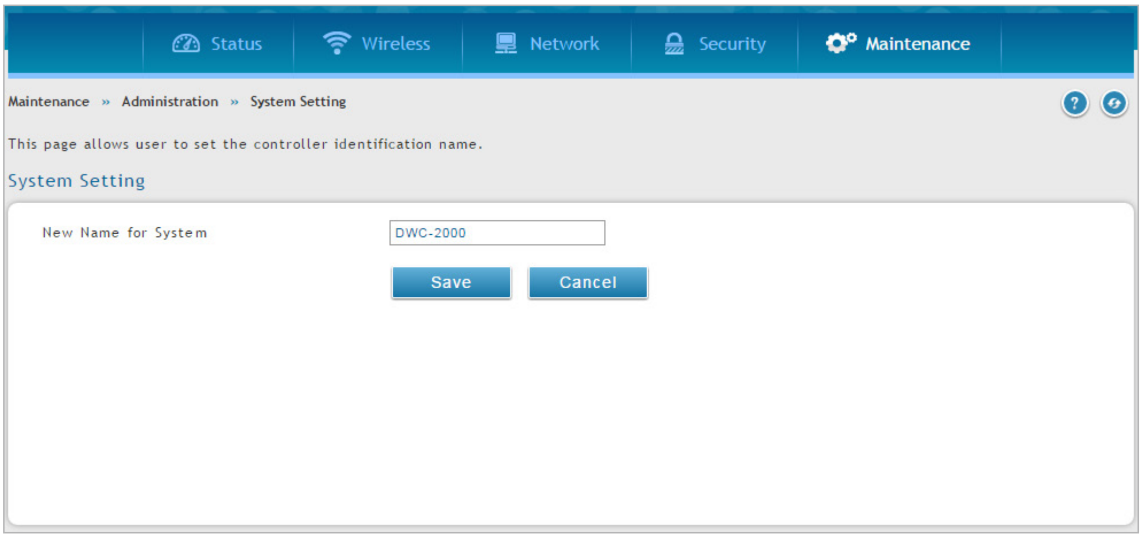


図 9-1　　System Setting 画面

2. システム名を入力して、「Save」ボタンをクリックします。

システムの日付と時間の設定

Maintenance > Administration > Date and Time メニュー

タイムゾーン、サマータイム（Daylight Savings Time）の調整の有無、日時を同期する NTP（Network Time Protocol）サーバの使用について設定することができます。また、手動で「Date and Time」を入力することもできます。これは、コントローラの RTC（Real Time Clock）に情報を保存します。コントローラがインターネットにアクセスする場合、コントローラの時間を設定する最も正確なメカニズムは、NTP サーバ通信を有効にすることです。

以下の手順に従って、日時を設定します。

1. **Maintenance > Administration > Date and Time** の順にメニューをクリックし、以下の画面を表示します。

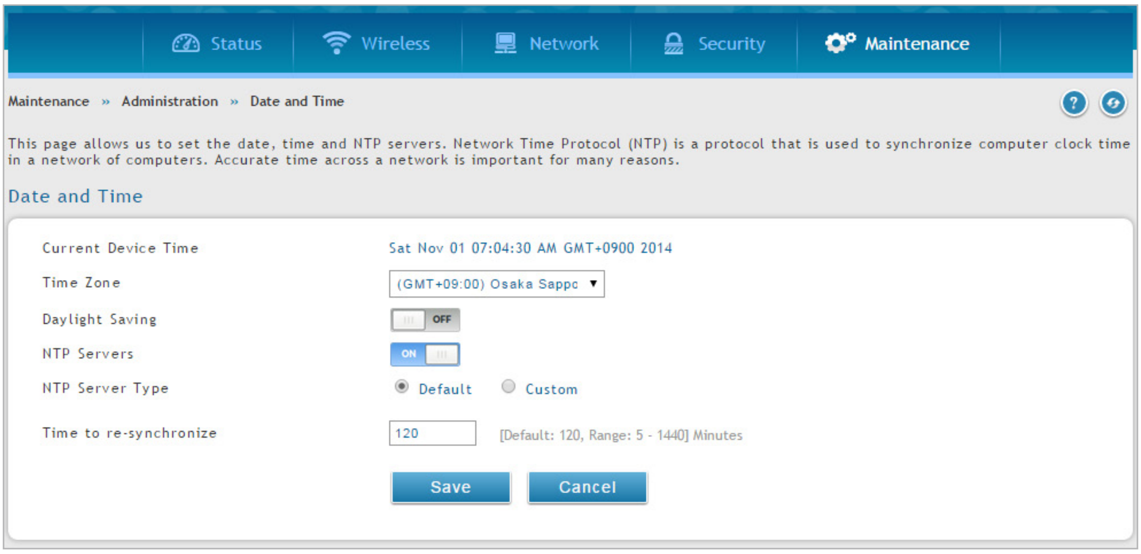


図 9-2　Date and Time 画面（NTP サーバタイプが「Default」）

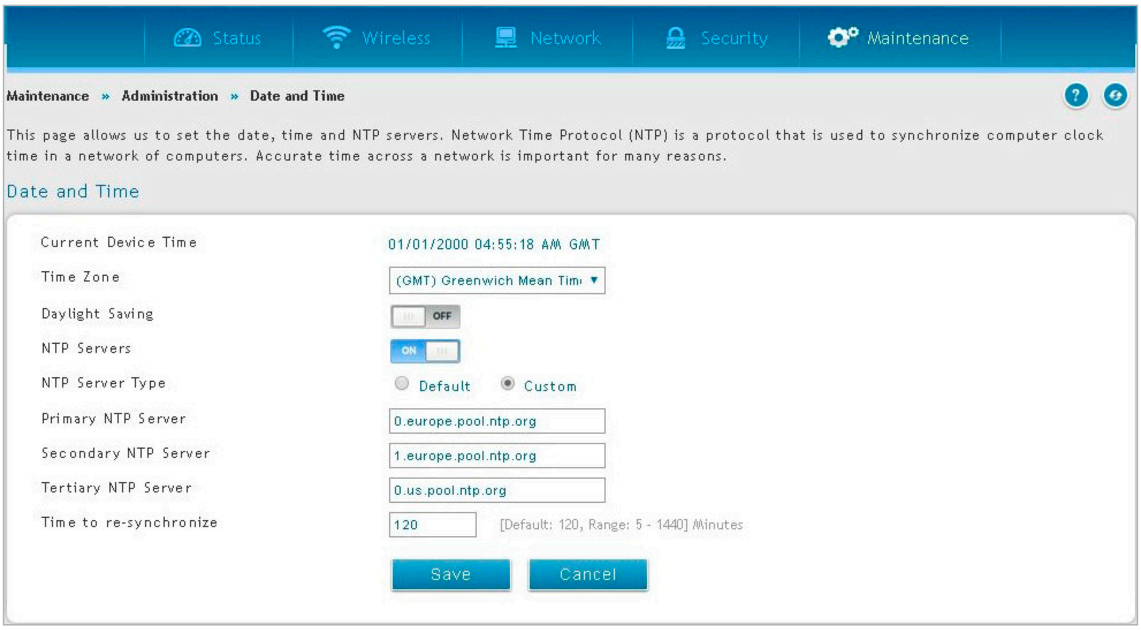


図 9-3　Date and Time 画面（NTP サーバタイプが「Custom」）

2. グリニッジ標準時（GMT）に対するコントローラのタイムゾーンを選択します。

3. サマータイムを有効にする場合は、「Daylight Saving」を「ON」にします。

4. NTP サーバのタイプ（Default または Custom）を選択します。「Custom」の場合、サーバのアドレスまたは FQDN を入力します。また、「Time to re-synchronize」で、NTP サーバと同期する間隔を選択します。（単位：分、初期値：120 分）

5. 「Save」ボタンをクリックします。

ログインセッションタイムアウトの設定

Maintenance > Administration > Session Settings メニュー

システムのセッション設定を行います。

1. **Maintenance > Administration > Session Settings** の順にメニューをクリックし、以下の画面を表示します。

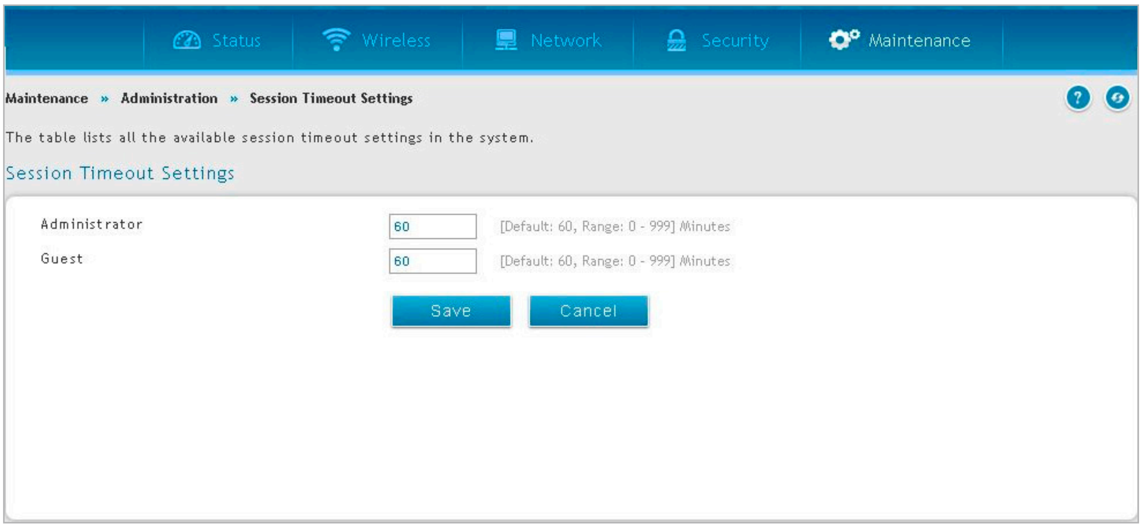


図 9-4　　Session Timeout Settings 画面

以下の項目があります。

項目	説明
Administrator	管理者ユーザのセッションタイムアウト値を入力します。
Guest	ゲストユーザのセッションタイムアウト値を入力します。

2. 管理者とゲストユーザ用のセッションタイムアウトの値を入力し、「Save」ボタンをクリックします。

USB 共有ポートの設定

Maintenance > Administration > USB Share Ports メニュー

デバイスに USB 共有機能を設定します。

1. **Maintenance > Administration > USB Share Ports** の順にメニューをクリックし、以下の画面を表示します。

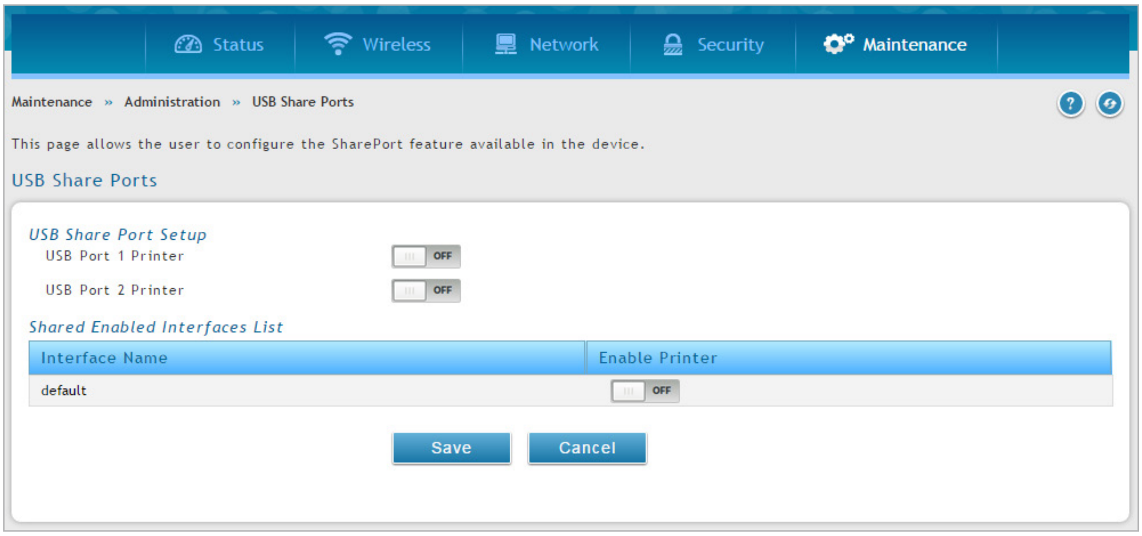


図 9-5　　USB Share Ports 画面

以下の項目があります。

項目	説明
USB Port 1 Printer	「ON」にすると、コントローラに接続する USB プリンタが、ネットワークを経由して共有できるようになります。
USB Port 2 Printer	「ON」にすると、コントローラに接続する USB プリンタが、ネットワークを経由して共有できるようになります。
Enable Printer	「ON」にすると、選択インタフェースのプリンタ共有を有効にします。

2. 共有する USB ポート（USB ポート 1、2、または両方）を有効にして、「Save」ボタンをクリックします。

パッケージマネージャ

Maintenance > Administration > Package Manager メニュー

使用可能なドライバの一覧を表示し、インストール / アンインストールを実行します。

1. **Maintenance > Administration > Package Manager** の順にメニューをクリックし、以下の画面を表示します。

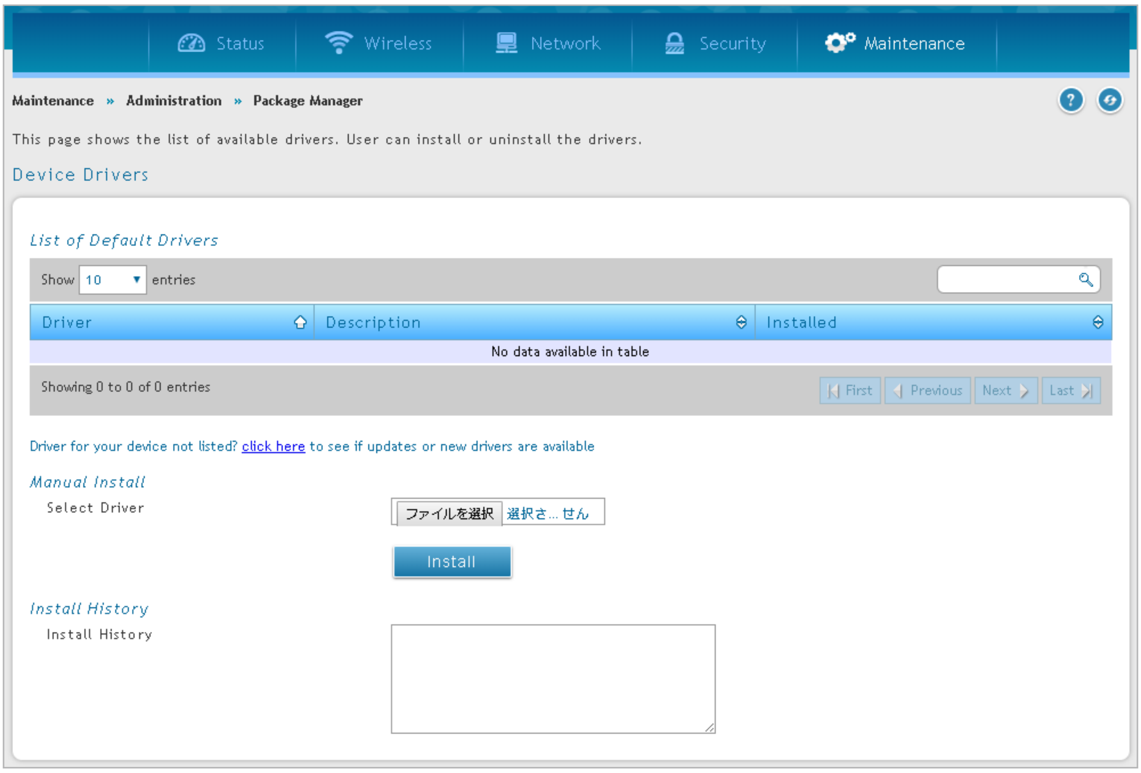


図 9-6　　Device Drivers 画面

以下の項目があります。

項目	説明
List of Default Drivers（デフォルトドライバの一覧）	
Driver	ドライバ名を表示します。
Description	ドライバ概要を表示します。
Installed	ドライバのインストールの有無を表示します。
"Driver for your device not listed? click here to see if updates or new drivers are available"	コントローラで使用可能なドライバを検出します。「click here」をクリックし、ドライバの更新や新しいドライバの有無を確認します。 **注意**　ドライバリストの更新、新しいドライバの検出にはインターネット環境が必要です。
Manual Install	
Select Driver	クリックし、ローカルのドライバファイルを参照します。 「Install」をクリックしインストールを実行します。
Install History	
Install History	インストールの履歴を表示します。

言語設定

Maintenance > Administration > language Settings メニュー

Web GUI の言語選択を行います。

1. **Maintenance > Administration > language Settings** の順にメニューをクリックし、以下の画面を表示します。

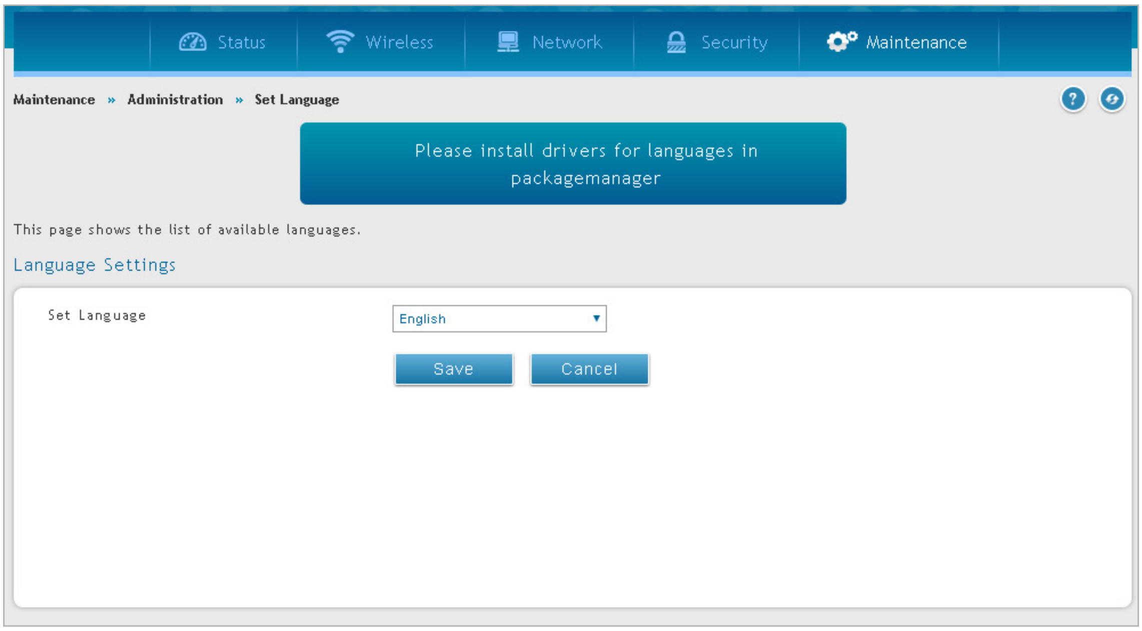


図 9-7　　Language Settings 画面

以下の項目があります。

項目	説明
Language Settings	
Set Language	ドロップダウンメニューから言語を選択し、「Save」をクリックします。 前項目「パッケージマネージャ」でインストールした言語ファイルが表示され、選択が可能になります。

WEB GUI 管理の設定

Maintenance > Administration > Web GUI Management メニュー

VLAN ホスト / ネットワークに対して Web GUI へのアクセス許可を設定します。

1. **Maintenance > Administration > Web GUI Management** の順にメニューをクリックし、以下の画面を表示します。

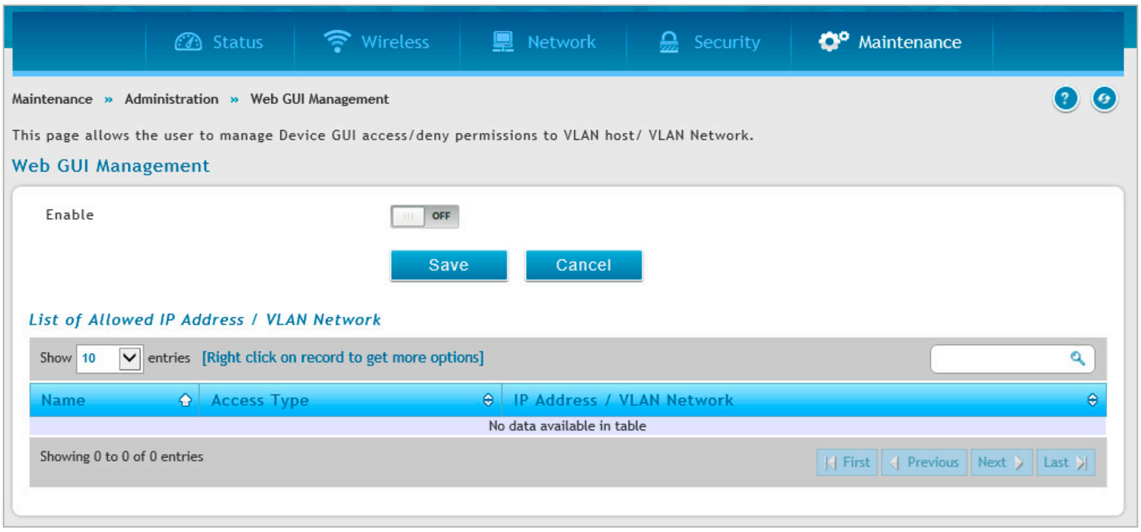


図 9-8　　Web GUI Management 画面

2. 「Enable」を ON にすると、Web GUI 管理を有効化します。

3. 「Add New Configuration」をクリック、または既存のエントリを右クリックして「Edit」を選択し、以下の画面を表示します。

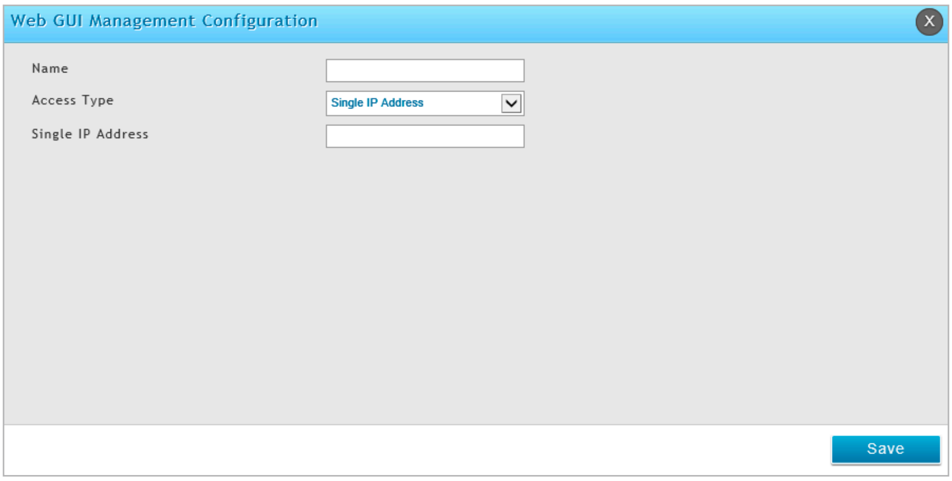


図 9-9　　Web GUI Management Configuration 画面

4. フィールドにデータを入力し、「Save」ボタンをクリックします。

項目	説明
Name	プロファイル名を入力します。
Access Type	プロファイルのアクセスタイプを「Single IP Address」または「VLAN Network」から選択します。
Single IP Address	「Access Type」が「Single IP Address」の場合、VLAN ホストの IP アドレスを入力します。
VLAN Network	「Access Type」が「VLAN Network」の場合、定義済みの VLAN リストから VLAN ネットワークを指定します。

ライセンスのアクティブ化

Maintenance > Administration > License Update メニュー
無線コントローラに追加するアクセスポイントのライセンスをアクティブ化します。

1. D-Link からアクティベーションキーを取得します。
   a. デバイスの底面にある無線コントローラのシリアル番号を確認します。
   b. ライセンスの購入後に、D-Link からライセンスキーを取得します。
   c. Web ブラウザを開き、https://register.dlink.com に遷移して、D-Link のサイトに登録します。
   d. アカウントを持っていない場合、新しいアカウントを登録します。
   e. ユーザ名とパスワードでログインします。
   f. D-Link Global Registration ポータル Web サイトで「ライセンスキーのアクティベーション」をクリックします。
   g. 指示に従って、アクティベーションコードを受信します。

2. アクティベーションキーを取得後、**Maintenance > Administration > License Update** の順にメニューをクリックし、以下の画面を表示します。

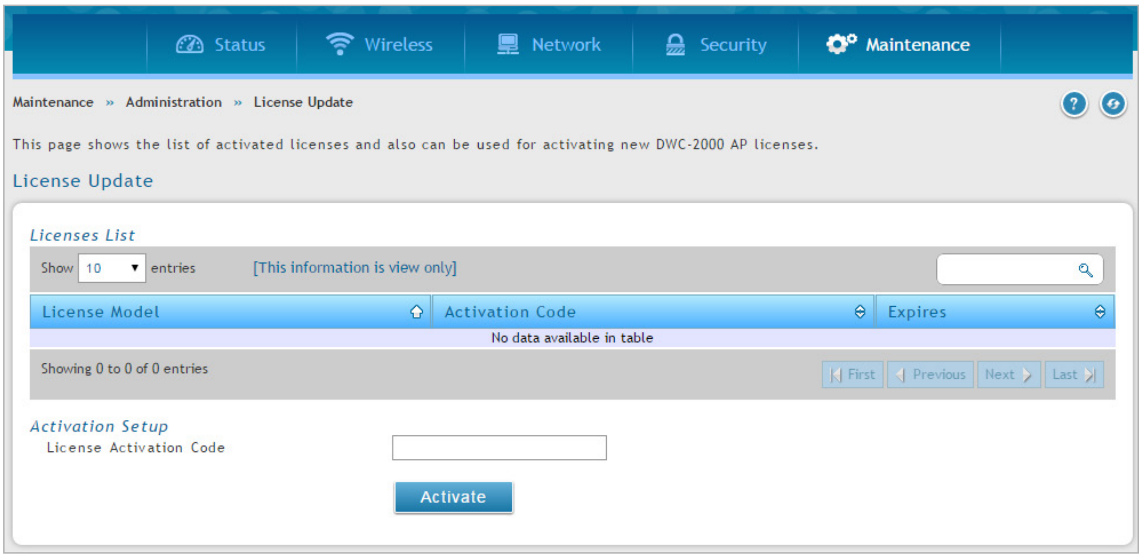


図 9-10　License Update 画面

3. 「Activation Setup」の「License Activation Code」フィールドに、D-Link から提供されたアクティベーションコードを入力します。

4. 「Activate」ボタンをクリックします。アクティベーションコードがリストに表示されます。

5. ライセンスを有効にするには、無線コントローラを再起動します。(「無線コントローラの再起動」参照)

UI 管理

Maintenance > Management > UI Management メニュー
ローカルネットワーク内外からの無線コントローラの UI 管理を設定します。

注意 リモート管理が有効な場合、IP アドレスを知っているユーザは誰でもコントローラにアクセス可能です。操作を続行する前に、管理者とゲストのパスワードの初期値を変更することを強くお勧めします。

1. **Maintenance > Management > UI Management** の順にメニューをクリックし、以下の画面を表示します。

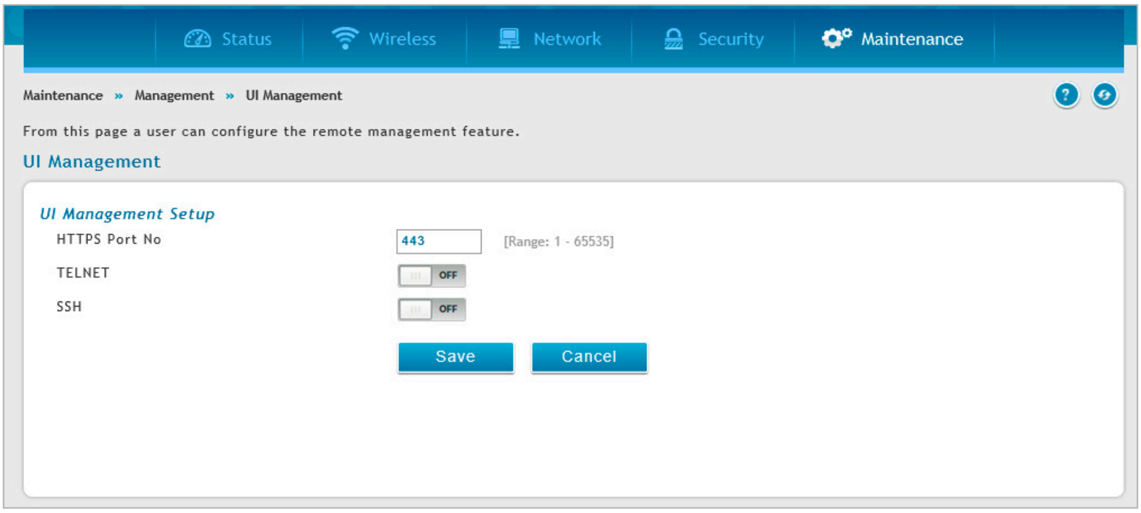


図 9-11　UI Management 画面

以下の項目があります。

項目	説明
HTTPS Port No	HTTPS ポート番号を指定します。初期値：443
TELNET	有効にすると、Telnet によるアクセスが可能になります。
SSH	有効にすると、SSH によるアクセスが可能になります。

2. 「Save」ボタンをクリックします。

SNMP の使用

Maintenance > Management > SNMP メニュー

SNMP は、ネットワーク内の複数のルータが中央のマスタシステムに管理されている場合に便利な追加の管理ツールです。外部の SNMP マネージャにこのコントローラの MIB（Management Information Base）ファイルを提供する場合、マネージャは、構成パラメータの参照または更新のためにコントローラの階層変数を更新できます。管理デバイスとしてのコントローラは、マスタ（SNMP マネージャ）によって MIB 設定変数がアクセスされることを許可する SNMP エージェントを搭載しています。コントローラのアクセスコントロールリストは読み出し用または読み書き用の SNMP 権限を持つネットワーク内のマネージャを識別します。トラップリストでは、コントローラから SNMP コミュニティ（マネージャ）に通知が送信されるポートと、トラップ用の SNMP バージョン（v1、v2c、v3）を設定します。

SNMP v3 ユーザリストの設定

Maintenance > Management > SNMP > SNMP メニュー

SNMP v3 ユーザリストを設定します。

1. **Maintenance > Management > SNMP > SNMP** の順にメニューをクリックし、以下の画面を表示します。

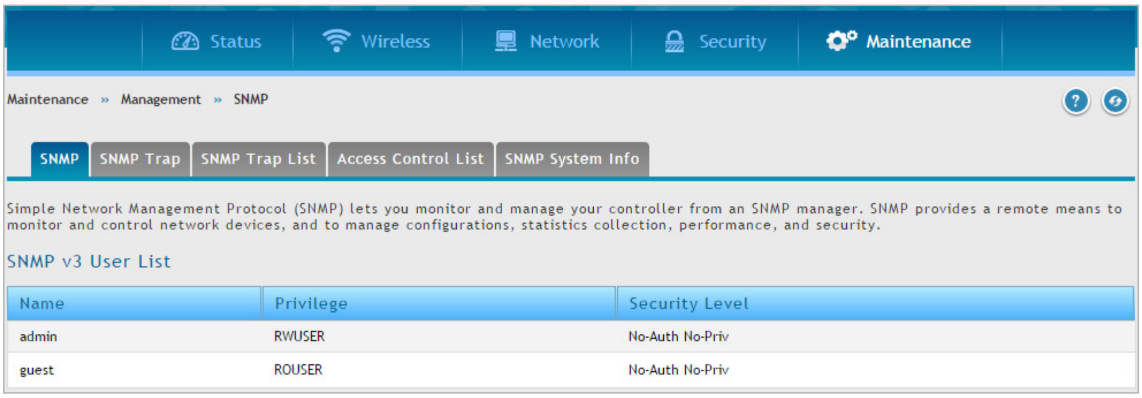


図 9-12　SNMP v3 User List 画面

2. 「admin」または「guest」を右クリックして、「Edit」を選択し、以下の画面を表示します。

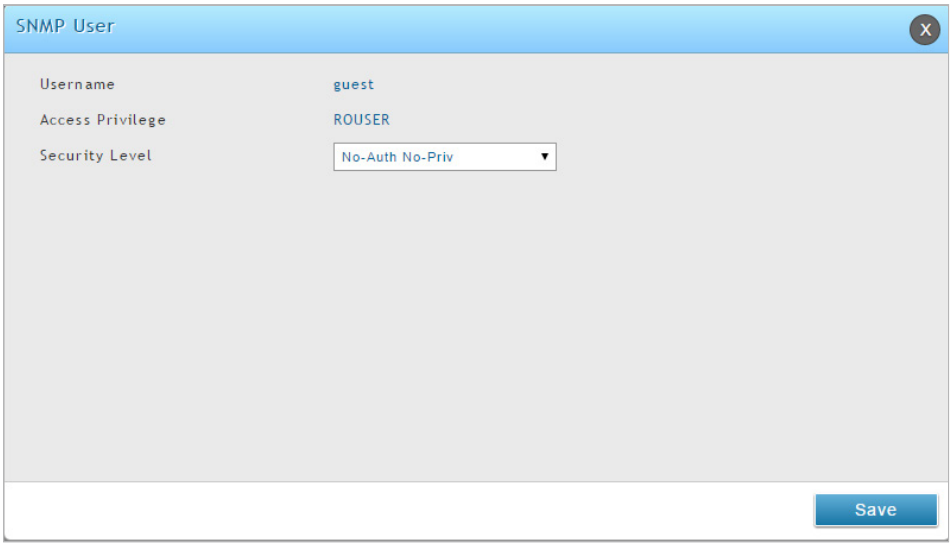


図 9-13　SNMP ユーザ画面（guest）

以下の項目を設定し、「Save」をクリックします。

項目	説明
Security Level	このユーザの認証とプライバシー設定を定義します。 • No-Auth No-Priv - 認証にユーザ名の一致だけを必要とします。 • Auth No-Priv - MD5 または HMAC-SHA アルゴリズムに基づいた認証を提供します。 • AuthPriv - DES-56 ビットを使用した暗号プライバシーと、MD5 または SHA-1 アルゴリズムに基づいた認証を提供します。
Authentication Algorithm	「Auth No-Priv」または「AuthPriv」を選択した場合、MD5 または SHA-1 認証を選択します。
Authentication Password	「Auth No-Priv」または「AuthPriv」を選択した場合、SNMPv3 ユーザと共有される認証パスワードを入力します。
Privacy Algorithm	「AuthPriv」を選択した場合、認証ネゴシエーションに使用されるアルゴリズム（DES または AES）を選択します。
Privacy Password	「AuthPriv」を選択した場合、SNMPv3 ユーザと共有されるプライバシーパスワードを入力します。

SNMP トラップリストの設定

Maintenance > Management > SNMP > SNMP Trap List メニュー

コントローラがトラップメッセージを送信する SNMP エージェントの IP アドレスを設定および表示します。

1. **Maintenance > Management > SNMP > SNMP Trap List** の順にメニューをクリックし、以下の画面を表示します

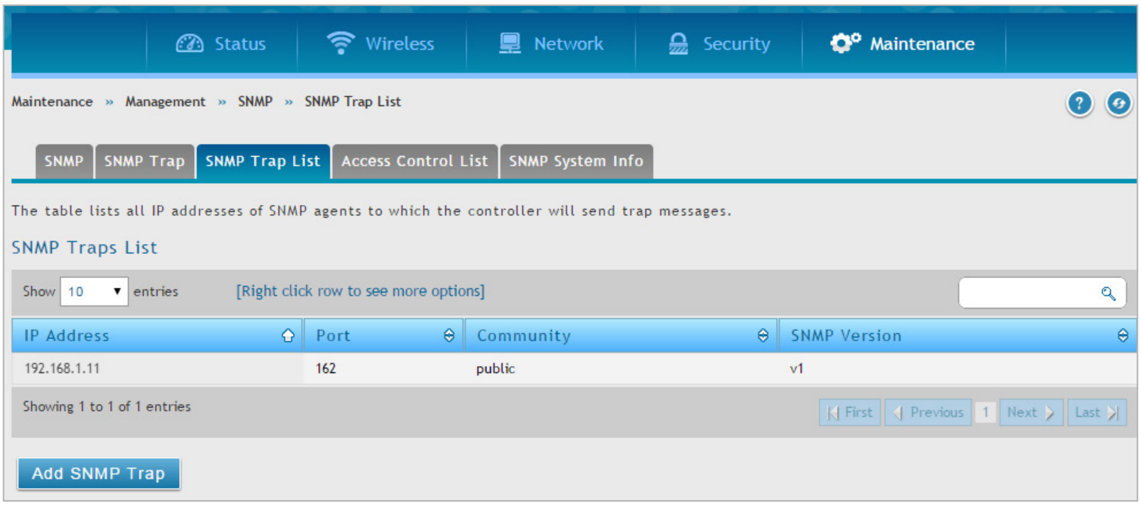


図 9-14　SNMP Traps List 画面

2. 「Add SNMP Trap」ボタンをクリックします。

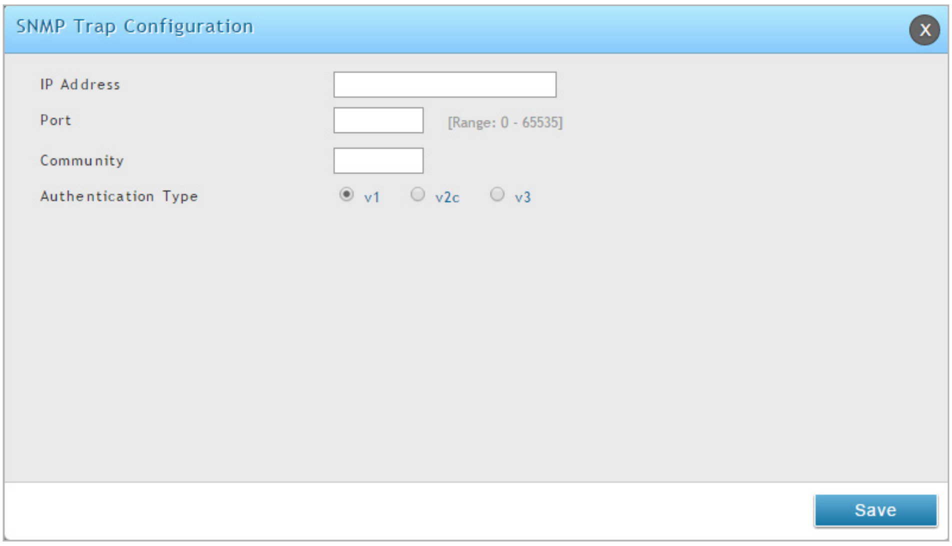


図 9-15　SNMP Trap Configuration 画面

3. フィールドに情報を入力します。

項目	説明
IP Address	SNMP トラップエージェントの IP アドレス。
Port	トラップメッセージの送信先となる IP アドレスの SNMP トラップポート。
Community	エージェントが所属するコミュニティストリング。多くのエージェントは、Public コミュニティでトラップをリッスンするように設定されています。
Authentication Type	トラップエージェントが使用する SNMP バージョン（v1、v2c、または v3）。

4. 「Save」ボタンをクリックします。

エントリの編集

1. 編集するエントリを右クリックし、「Edit」を選択します。

2. 設定変更後、「Save」ボタンをクリックします。

エントリの削除

削除するエントリを右クリックし、「Delete」を選択します。すべてのエントリを削除する場合は、右クリックして「Select All」をチェックし、「Delete」を選択します。

SNMP アクセスコントロールリストの設定

Maintenance > Management > SNMP > Access Control List メニュー

SNMP アクセスコントロールリストを設定します。

1. **Maintenance > Management > SNMP > Access Control List** の順にメニューをクリックし、以下の画面を表示します

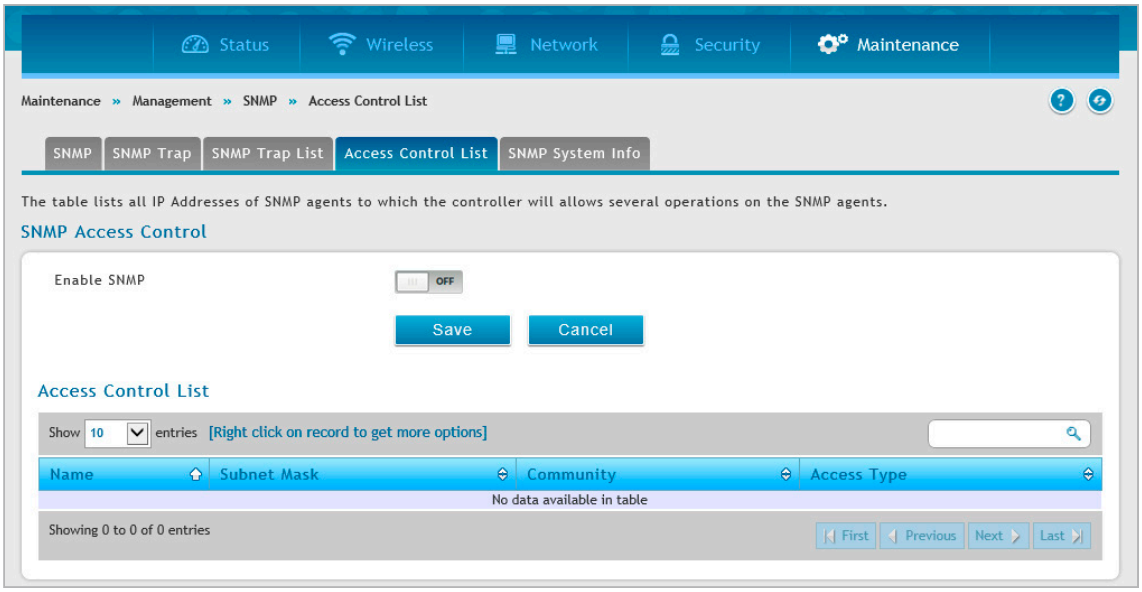


図 9-16　Access Control List 画面

2. 「Enable SNMP」を「ON」にし、「Save」をクリックします。

3. 「Add Access Control」ボタンをクリックし、以下の画面を表示します。

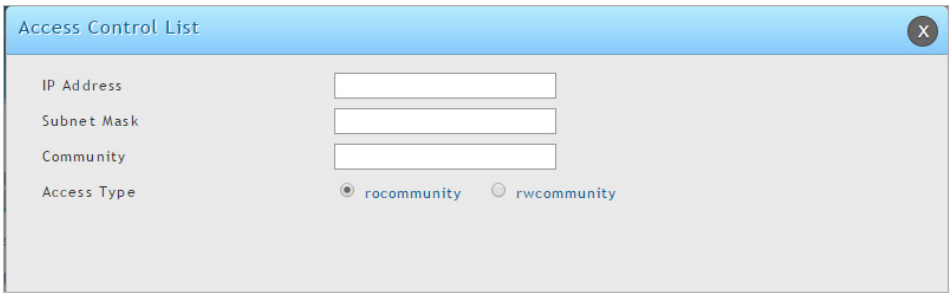


図 9-17　Access Control List 画面

4. フィールドに情報を入力します。

項目	説明
IP Address	SNMP トラップエージェントの IP アドレスを入力します。
Subnet Mask	許可される SNMP マネージャリストを決定するために使用されるネットワークマスクを入力します。
Community	エージェントが所属するコミュニティストリングを入力します。
Access Type	アクセス権限として、読取専用（rocommunity）または読み書き（rwcommunity）のいずれかを選択します。

5. 「Save」ボタンをクリックします。

エントリの編集

1. 編集するエントリを右クリックし、「Edit」を選択します。
2. 設定変更後、「Save」ボタンをクリックします。

エントリの削除

削除するエントリを右クリックし、「Delete」を選択します。

すべてのエントリを削除する場合は、右クリックして「Select All」をチェックし、「Delete」を選択します。

SNMP システム情報の設定

Maintenance > Management > SNMP> SNMP System Info メニュー

コントローラの SNMP システム情報を設定します。

1. **Maintenance > Management > SNMP> SNMP System Info** の順にメニューをクリックし、以下の画面を表示します

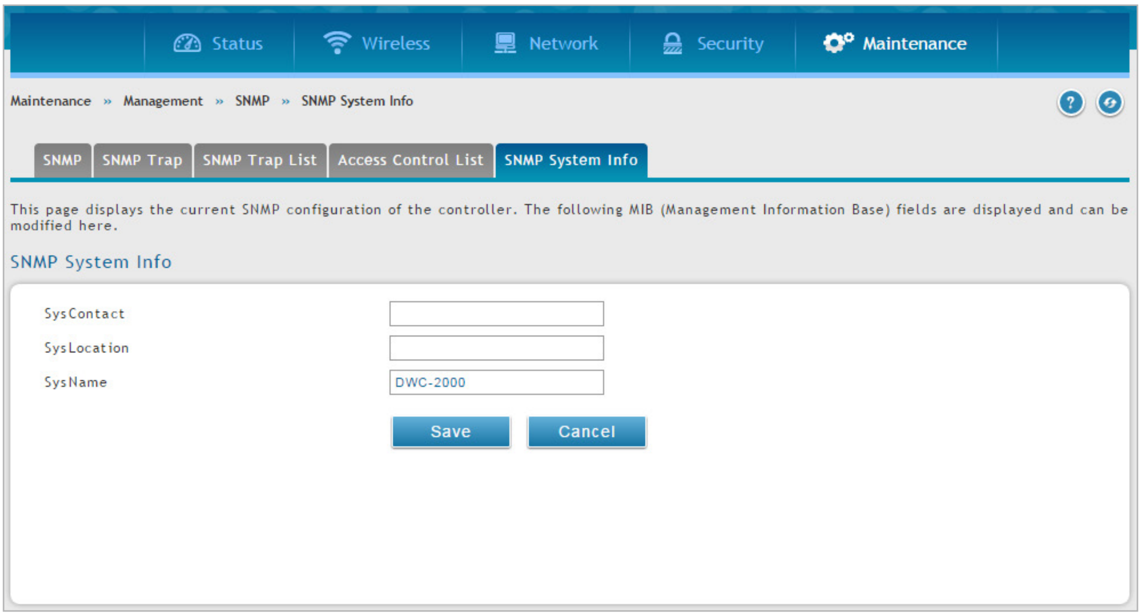


図 9-18　SNMP System Info 画面

2. 必要に応じて情報をフィールドに入力します。

項目	説明
SysContact	本コントローラの連絡窓口の名前を入力します。例 : admin、John Doe
SysLocation	コントローラの物理的な位置を入力します。 例 : Rack#2,4th Floor
SysName	コントローラの簡単な識別名を入力します。

3. 「Save」ボタンをクリックします。

無線 SNMP 情報の設定

Maintenance > Management > SNMP > SNMP Trap メニュー

コントローラの管理に SNMP（Simple Network Management Protocol）を使用する場合、コントローラに SNMP エージェントを設定して、ネットワーク上の SNMP マネージャにトラップを送信するように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に管理されている場合、アクセスポイントはトラップを送信しません。コントローラは自身のイベントと、配下のアクセスポイントからの情報更新から学習したイベントを元に、すべての SNMP トラップを生成します。

すべての無線 SNMP トラップは初期値で無効に設定されています。

1. **Maintenance > Management > SNMP > SNMP Trap** の順にメニューをクリックし、以下の画面を表示します。

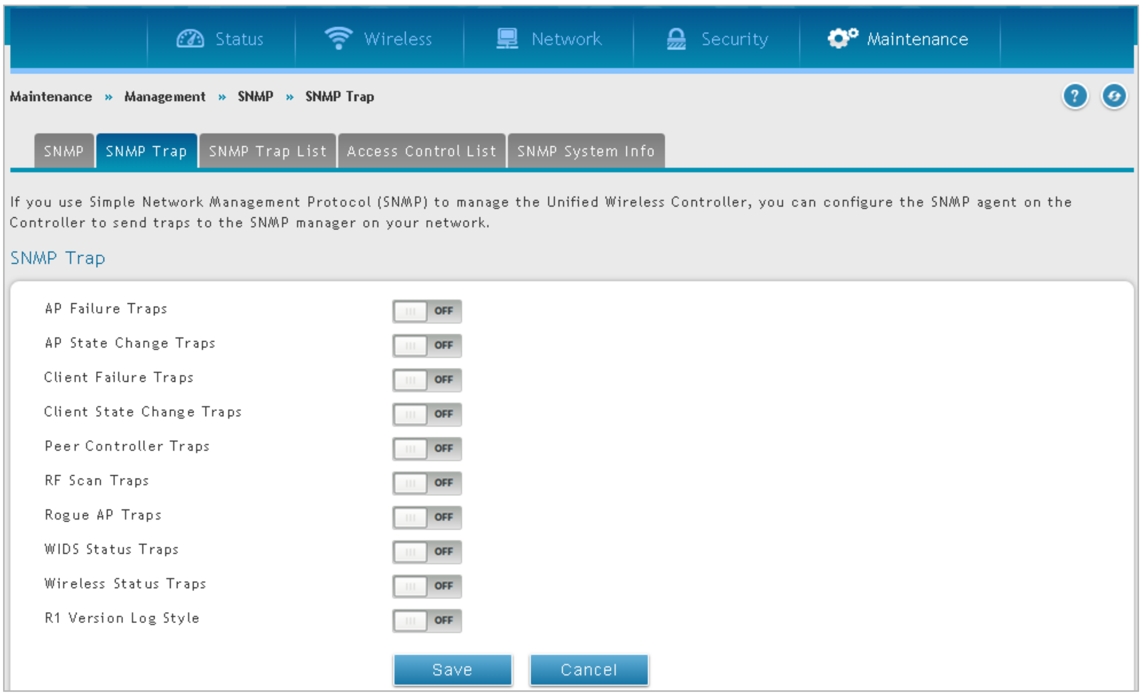


図 9-19　SNMP Trap 画面

2. 必要に応じてトラップを有効にします。

項目	説明
AP Failure Traps	有効にすると、アクセスポイントがコントローラとの接続または認証に失敗した時に、SNMP エージェントがトラップを送信します。
AP State Change Traps	有効にすると、以下のいずれかの原因により SNMP エージェントがトラップを送信します。 • Managed AP Discovered（管理対象のアクセスポイントの検出） • Managed AP Failed（管理対象のアクセスポイントエラー） • Managed AP Unknown Protocol Discovered（管理対象のアクセスポイントから不明なプロトコルを検出） • Managed AP Load Balancing Utilization Exceeded（管理対象のアクセスポイントのロードバランス使用率超過）
Client Failure Traps	有効にすると、クライアントがコントローラが管理するアクセスポイントとの接続または認証に失敗した時に SNMP エージェントがトラップを送信します。
Client State Change Traps	有効にすると、クライアントに関連する以下のいずれかの原因により、SNMP エージェントがトラップを送信します。 • Client Association Detected（クライアントの接続検出） • Client Disassociation Detected（クライアントの切断検出） • Client Roam Detected（クライアントのローミング検出）
Peer Controller Traps	有効にすると、ピアコントローラに関連する以下のいずれかの原因により、SNMP エージェントがトラップを送信します。 • Peer Controller Discovered（ピアコントローラの検出） • Peer Controller Failed（ピアコントローラ異常） • Peer Controller Unknown Protocol Discovered（ピアコントローラから不明なプロトコルを検出） • Configuration command received from peer controller（ピアコントローラからコンフィグレーションコマンドを受信。コントローラは、このトラップを生成するためにクラスタコントローラである必要はありません。）
RF Scan Traps	有効にすると、RF スキャンが新しいアクセスポイント、無線クライアント、またはアドホッククライアントを検出した場合、SNMP エージェントがトラップを送信します。

項目	説明
Rogue AP Traps	有効にすると、コントローラが不正なアクセスポイントを検出した場合、SNMP エージェントがトラップを送信します。また、何らかの不正なアクセスポイントがネットワークに存在していると、エージェントは「Rogue Detected Trap Interval」（秒）ごとにトラップを送信します。
WIDS Status Traps	有効にすると、以下のいずれかの原因により SNMP エージェントがトラップを送信します。 • このコントローラがクラスタスコントローラになりました。 • 不正なクライアントを検出しました。 • 「Rogue Detected Trap Interval」（秒）後も不正なクライアントが存在しています。 • ピアグループにおける管理アクセスポイントの最大数を超過しました。
Wireless Status Traps	有効にすると、コントローラ（このトラップではクラスタコントローラである必要はありません）の動作状態が変更される場合に、SNMP エージェントはトラップを送信します。Channel Algorithm または Power Algorithm が実行されるとトラップを送信します。また、以下のデータベースのリストでエントリ数が最大値を超えた時に SNMP エージェントはトラップを送信します。 • Managed AP database • AP Neighbor List • Client Neighbor List • AP Authentication Failure List • RF Scan AP List • Client Association Database • Ad Hoc Clients List • Detected Clients List
R1 Version Log Style	有効にすると、トラップは「R1 Version Log Style」で表示されます。

3.　「Save」ボタンをクリックします。

DDP クライアントの設定

Maintenance > Management > DDP メニュー

DDP（D-Link Discovery Protocol）クライアントを「ON」または「OFF」にします。

1.　**Maintenance > Management > DDP** の順にメニューをクリックし、以下の画面を表示します。

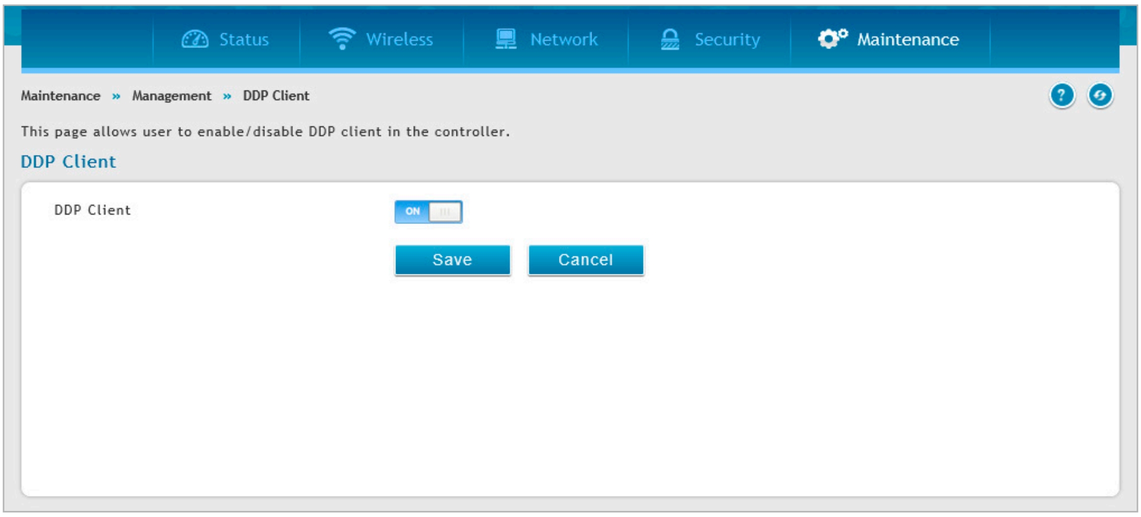


図 9-20　DDP Client 画面

2.　「DDP Client」を「ON」または「OFF」にします。

3.　「Save」をクリックし、設定を保存します。

コンフィグレーションの保存と復元

コンフィグレーションのバックアップ

Maintenance > Firmware > Backup/Restore メニュー

無線コントローラの設定後に、コンフィグレーションのバックアップを行います。設定のバックアップはファイルに保存されます。このバックアップファイルを使用して、何らかの理由で不具合が生じた場合に同じ無線コントローラに設定を復元することができます。また、デバイスの交換時や他の無線コントローラを使用して作業する場合など、別の無線コントローラにも設定を復元することができます。

1. **Maintenance > Firmware > Backup/Restore** の順にメニューをクリックし、以下の画面を表示します。

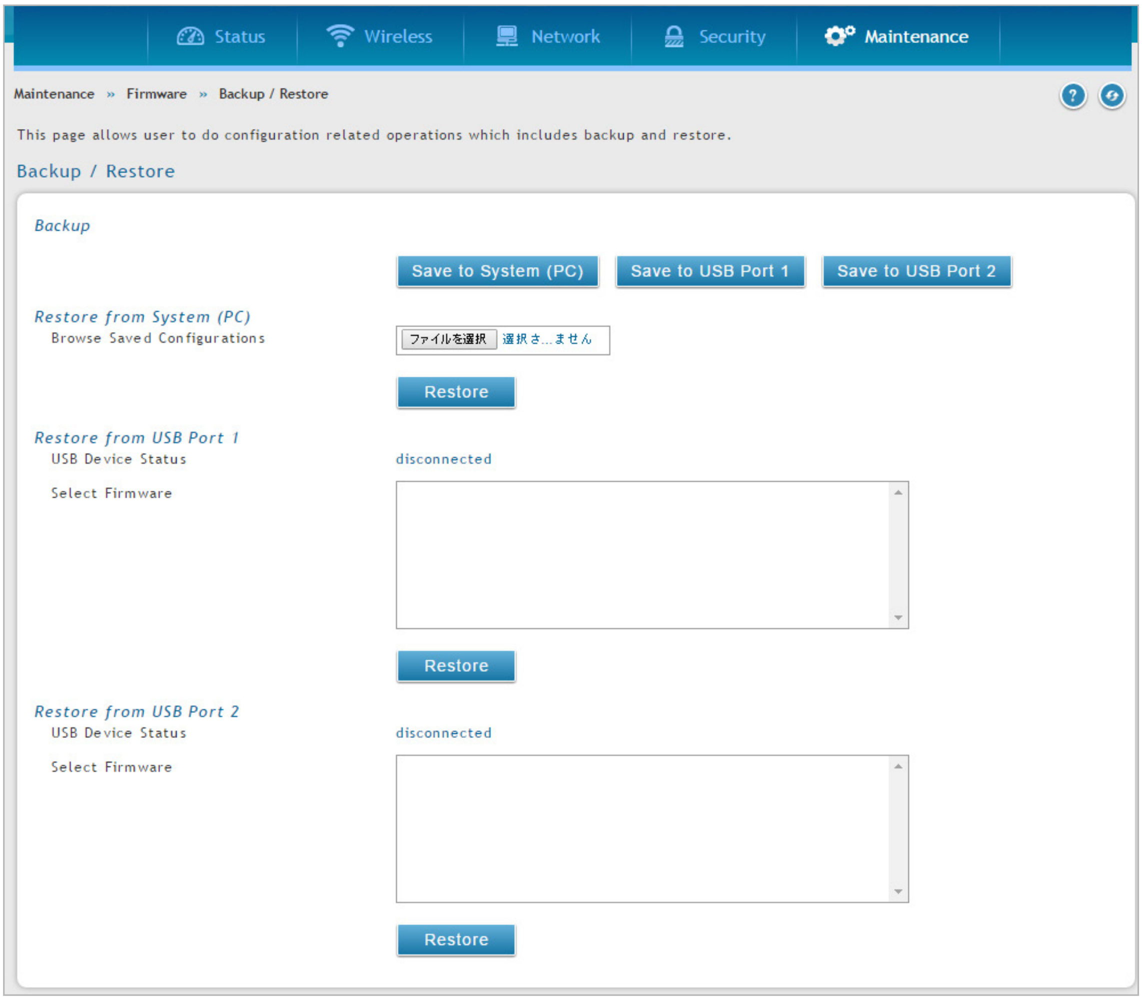


図 9-21　Backup / Restore 画面

2. バックアップを保存する場所によって、「Save to System (PC)」、「Save to USB Port 1」、または「Save to USB Port 2」をクリックします。

PC へのバックアップ

「Save to System (PC)」を選択すると、以下のダイアログメッセージが表示されます。

「OK」ボタンをクリックすると、ブラウザは、自動的にデフォルトのダウンロード場所にダウンロードを始めます。ファイル名には「.tar」という拡張子が付加されます。

USB デバイスへのバックアップ

「Save to USB Port 1」、または「Save to USB Port 2」を選択すると、メッセージを表示せずに、対応する USB フラッシュドライブにファイルをバックアップします。USB メディアが存在しない場合、これらのオプションでは何も実行されません。

コンフィグレーションの復元

Maintenance > Firmware > Backup/Restore メニュー

保存した無線コントローラのコンフィグレーションのバックアップを復元します。

1. **Maintenance > Firmware > Backup/Restore** の順にメニューをクリックし、以下の画面を表示します

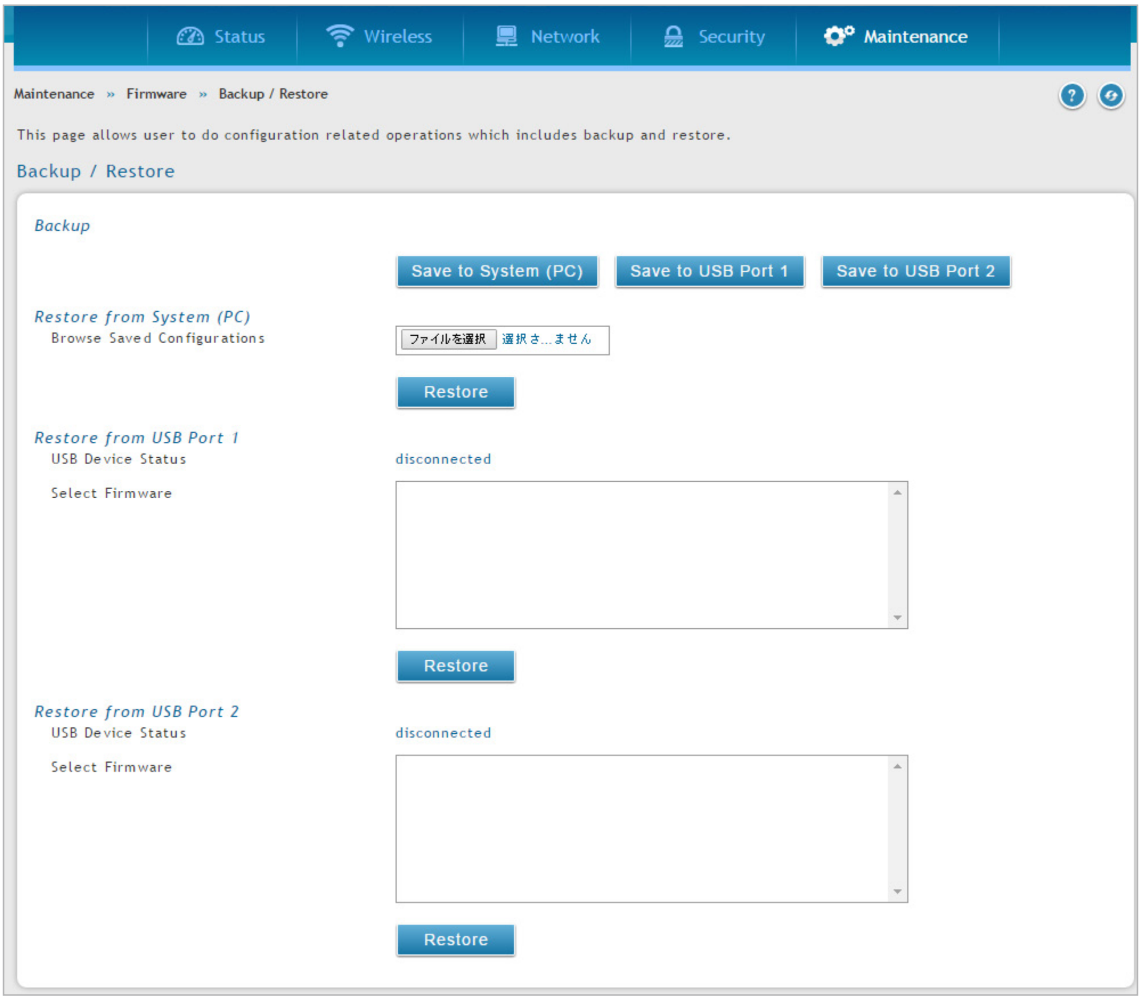
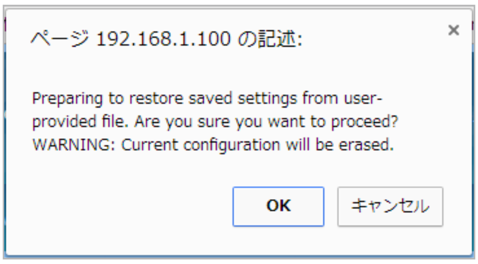


図 9-22　Backup / Restore 画面

2. 「Restore from System (PC)」セクションで、「ファイルを選択」ボタンをクリックします。バックアップファイルを選択して、「開く」をクリックします。

3. 「Restore」ボタンをクリックすると、ダイアログが表示されます。



4. 「OK」をクリックすると、選択したファイルからコンフィグレーションを復元します。

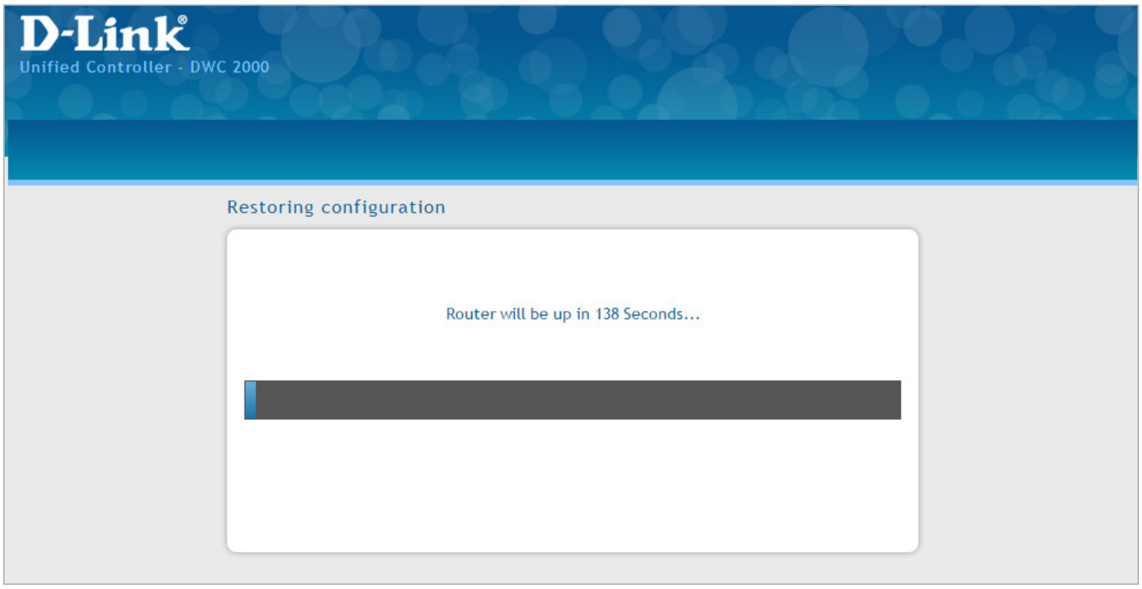


図 9-23　Restoring configuration 画面

終了するまでしばらくお待ちください。終了すると、ログイン画面が表示されます。

工場出荷時設定の復元

Maintenance > Firmware > Reboot / Factory Default メニュー

工場出荷時設定に無線コントローラをリセットすると、購入時の状態に戻り、初期設定に対して行ったすべての変更が失われます。復元される設定には、ログインパスワード、SSID、IP アドレスや無線セキュリティキーなど、オンライン状態とするために必要とされる重要な項目も含まれます。

無線コントローラを元の工場出荷時設定に復元する方法には 2 つあります。

- 無線コントローラの前面にあるリセットボタンを使用する。（「リセットボタンを使用して工場出荷時設定に復元する」参照）
- 以下の Web 管理インタフェースの手順を使用する。

1. **Maintenance > Firmware > Reboot / Factory Default** の順にメニューをクリックし、以下の画面を表示します。

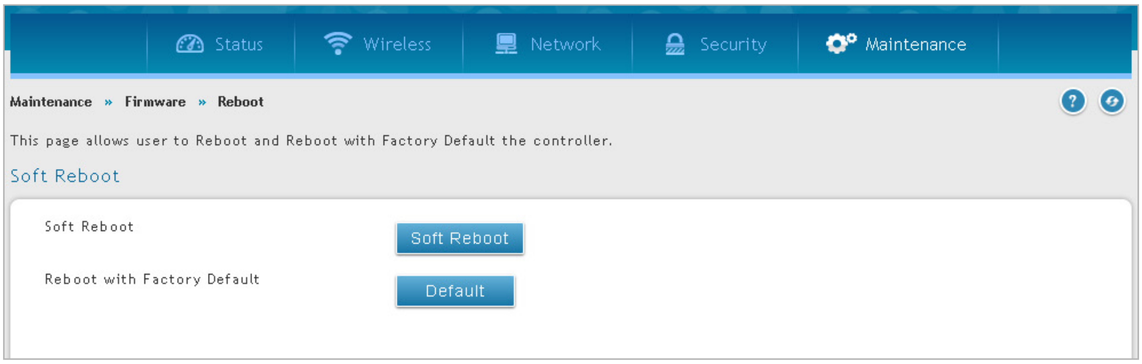
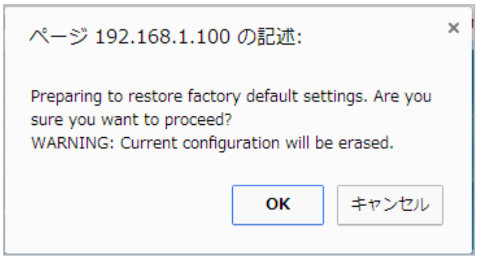


図 9-24　Soft Reboot 画面

2. 「Reboot with Factory Default」の「Default」ボタンをクリックすると、以下のダイアログメッセージが表示されます。



3. 「OK」ボタンをクリックして、工場出荷時設定を復元します。または、「Cancel」ボタンをクリックして、現在の設定を維持します。

注意 工場出荷時設定復元後の無線コントローラの LAN IP アドレスの初期値は「192.168.10.1」で、ログインユーザ名の初期値は「admin」、ログインパスワードの初期値は「admin」です。

無線コントローラの再起動

Maintenance > Firmware > Reboot / Factory Default メニュー

無線コントローラを再起動します。再起動は、電源の切断と投入を実行しますが、初期状態から変更した設定については保持します。

1. **Maintenance > Firmware > Reboot / Factory Default** の順にメニューをクリックし、以下の画面を表示します。

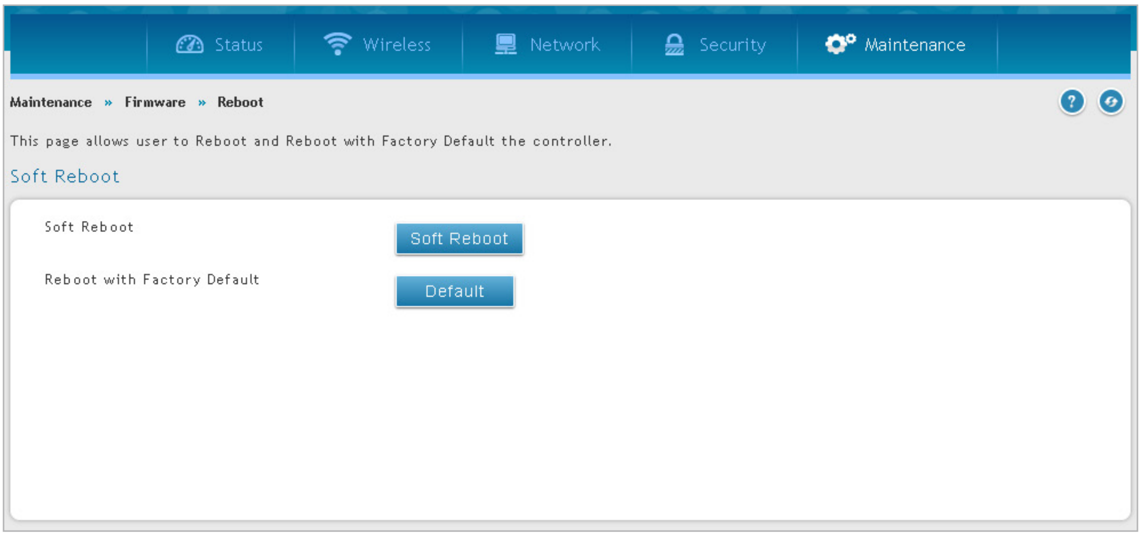
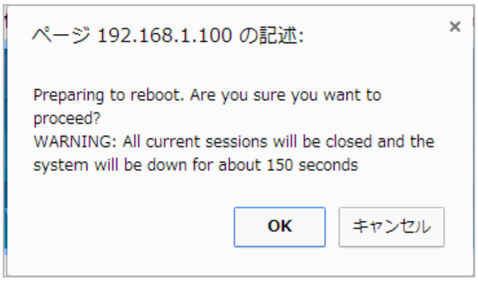


図 9-25　Soft Reboot 画面

2. 「Soft Reboot」の「Soft Reboot」ボタンをクリックすると、以下の確認ダイアログメッセージが表示されます。



3. 「OK」ボタンをクリックして、無線コントローラを再起動します。「Cancel」ボタンをクリックすると、再起動はキャンセルされます。

ファームウェアのアップグレード

無線コントローラのファームウェアのアップグレード

Maintenance > Firmware > Firmware Upgrade > Using System (PC) メニュー

D-Link では、無線コントローラの操作とパフォーマンスの改善を行っています。改良版が利用可能になると、カスタマにファームウェアのアップグレードのリリース版が提供されます。

無線コントローラのインストール後に、システムに最新のファームウェアが適用されていることをチェックします。その後、ファームウェアリリースをチェックし、利用可能になったらインストールします。

■ システム（PC）からのアップグレード

1. 無線コントローラの Web 管理インタフェースで、**Maintenance > Firmware > Firmware Upgrade > Using System (PC)** の順にメニューをクリックし、以下の画面を表示します。

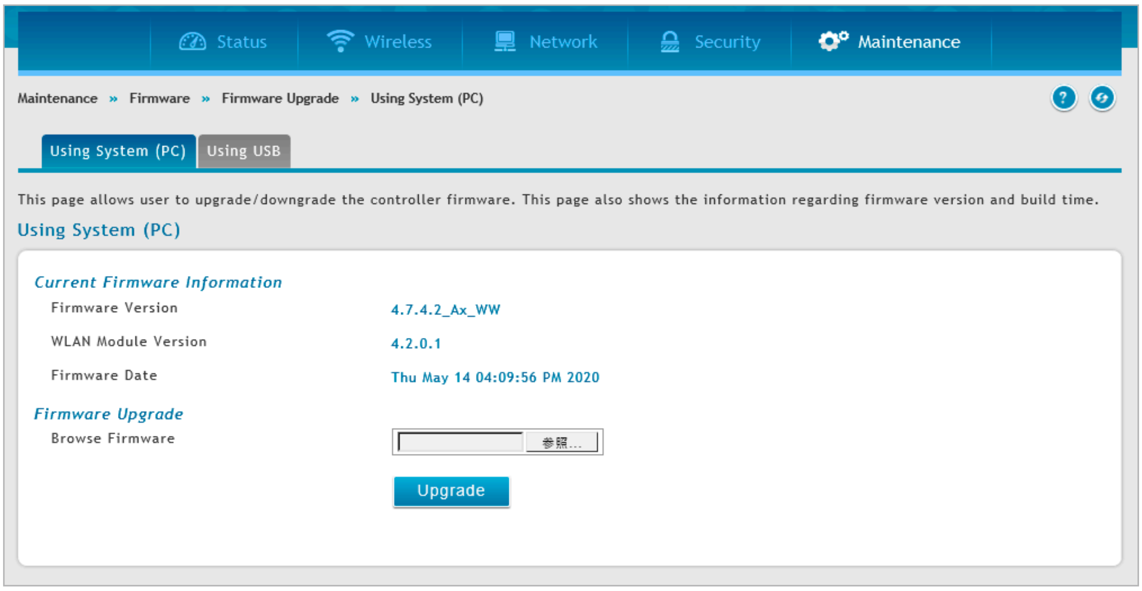
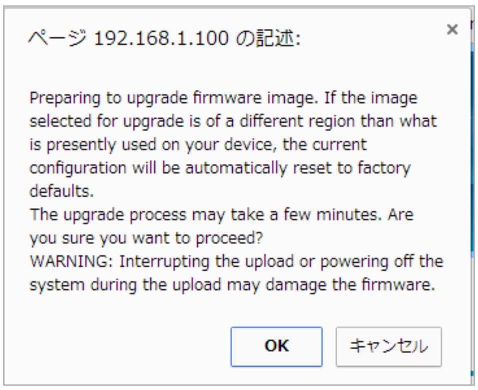


図 9-26　Using System（PC）画面

2. D-Link のサポート Web サイトにあるファームウェアのバージョンが、「Current Firmware Information」の「Firmware Version」より新しい場合、以下の手順に進みます。
3. D-Link Web サイトから新しいファームウェアをダウンロードします。
4. 「Firmware Upgrade」の「ファイルの選択」ボタンをクリックします。
5. ファームウェアファイルを選択後、「開く」ボタンをクリックします。
6. 「Upgrade」ボタンをクリックすると、以下の確認ダイアログメッセージが表示されます。



7. 「OK」ボタンをクリックして、ファームウェアのアップグレードを開始します。プログレスバーによりアップグレードの進捗が表示されます。

注意 アップグレードのプロセスには数分かかります。アップグレードを中断したり、システムの電源を切断したりしないでください。処理が中断された場合、ファームウェアが破損する場合があります。アップグレードが完了するまで、ブラウザからのサイト閲覧も行わないでください。

8. アップグレードが完了したら、無線コントローラの Web 管理インタフェースにログインし、**Maintenance > Firmware > Firmware Upgrade > Using System (PC)** の順にクリックして、新しいファームウェアが「Firmware Version」に表示されることを確認します。

9. ファームウェアのバージョンを「付録 A 基本計画のワークシート」に記録します。

注意 ダウングレードをする場合：
4.7.4.2 系から、4.7.2.1 系を含む旧バージョンへのダウングレードでは設定を引き継ぐことが出来ません。

■ USB ドライブからのアップグレード

1. 無線コントローラの Web 管理インタフェースで、**Maintenance > Firmware > Firmware Upgrade > Using USB** の順にメニューをクリックし、以下の画面を表示します。

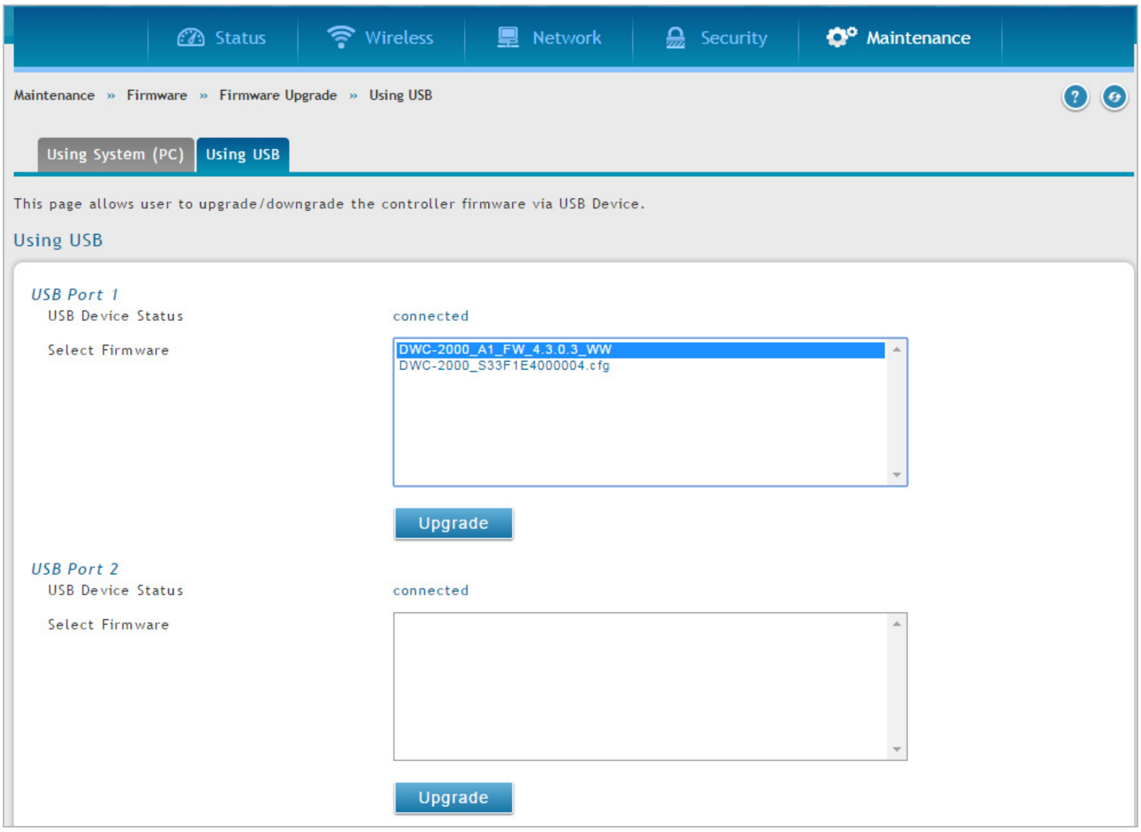


図 9-27　Using USB 画面

2. D-Link のサポート Web サイトにあるファームウェアのバージョンが、「Current Firmware Information」の「Firmware Version」より新しい場合、以下の手順に進みます。

3. D-Link Web サイトから新しいファームウェアを USB ドライブにダウンロードします。

4. 「Select Firmware」でファイルを選択し、「Upgrade」ボタンをクリックすると、以下の確認ダイアログメッセージが表示されます。

5. 「OK」ボタンをクリックして、ファームウェアのアップグレードを開始します。プログレスバーによりアップグレードの進捗が表示されます。

注意 アップグレードのプロセスには数分かかります。アップグレードを中断したり、システムの電源を切断したりしないでください。処理が中断された場合、ファームウェアが破損する場合があります。アップグレードが完了するまで、ブラウザからのサイト閲覧も行わないでください。

6. アップグレードが完了したら、無線コントローラの Web 管理インタフェースにログインし、**Maintenance > Firmware > Firmware Upgrade > Using System (PC)** の順にクリックして、新しいファームウェアが「Firmware Version」に表示されることを確認します。

7. ファームウェアのバージョンを「付録 A 基本計画のワークシート」に記録します。

コマンドラインインタフェースの使用

無線コントローラはコマンドラインインタフェース（CLI）をサポートしています。CLI は、VT-100 端末エミュレーションプログラムを使用して、シンプルなテキストベース・ツリー構造のインタフェースにより、ローカルまたはリモートで無線コントローラと管理対象のアクセスポイントの設定、モニタを行います。無線コントローラは、コマンドラインの対話のために SSH および Telnet をサポートしています。

以下の手順では CLI にアクセスする方法を説明します。

注意 RJ-45/DB9 変換ケーブルは本製品に同梱されています。

1. 無線コントローラの前面パネルのコンソールポートに、VT-100 端末エミュレーションプログラムを持つ PC を接続します。

2. 管理者ユーザ用に、CLI ログイン証明書が GUI で共有されます。CLI にアクセスするためには、SSH またはコンソールのプロンプトで「cli」を入力し、管理者ユーザ権限でログインします。

```
DWC-2000 login:
```

注意 詳しくは、「Wireless Controller CLI Reference Guide DWC-2000」を参照してください。

第 10 章　トラブルシューティング

無線コントローラの使用時に問題に直面した場合、本章のトラブルシューティングを参照し、問題を特定して解決の手がかりとします。

- LED トラブルシューティング
- Web GUI トラブルシューティング
- リセットボタンを使用して工場出荷時設定に復元する
- 日付と時間に関する問題
- アクセスポイントに関するディスカバリ問題
- 接続問題
- ネットワークの性能と不正アクセスポイントの検出
- 無線コントローラにおける診断ツールの使用
- ログ設定

LED トラブルシューティング

無線コントローラの電源をオンにすると、以下のイベントが順番に発生します。

1. 電源をオンにした時に、前面パネルの USB ポート左にある Power LED（緑）が点灯していることを確認します。
2. 約 2 分後に、接続するローカルポート右の LAN ポート LED がすべて点灯していることを確認します。これは、接続するデバイスとのリンクが確立されたことを示します。
3. RJ-45 ポートに 1000Mbps デバイスが接続されている場合は、ポート左側の LED が橙色であることを確認します。ポートに 100Mbps デバイスが接続されている場合は、ポート左側の LED が緑色であることを確認します。ポートに 10Mbps デバイスが接続されている場合は、ポート左側の LED が消灯していることを確認します。
4. SFP ポートに 1000Mbps デバイスが接続する場合は、ポートの LED が橙色であることを確認します。ポートに 100Mbps デバイスが接続する場合は、ポートの LED が緑色であることを確認します。

これらのイベントが発生しない場合、以下の適切なセクションを参照してください。

Power LED が消灯

無線コントローラの電源をオンにしても、Power および他の LED がオフの状態である場合、電源コードが適切に無線コントローラに接続されていること、電源コードが接続するコンセントが壁面スイッチにより制御されずに動作する状態であること確認します。

LAN ポート LED が消灯

イーサネット接続が行われているにもかかわらず、LAN LED が点灯しない場合 :

1. PC と本製品がイーサネットケーブルで正しく接続されていることを確認してください。
2. 接続するスイッチに電源が提供され、スイッチがオンであることを確認します。
3. 正しいケーブル（ストレートまたはクロス）を使用していることを確認します。

Web GUI トラブルシューティング

ご使用の PC から本製品の Web GUI にアクセスできない場合は、以下の手順を参照してください。

1. PC と本製品がイーサネットケーブルで正しく接続されていることを確認してください。
2. ご使用の PC の IP アドレスが本製品と同じサブネットにあることを確認してください。
3. 本製品の現在の IP アドレスが分からない場合、工場出荷時の設定にリセットしてください。（「リセットボタンを使用して工場出荷時設定に復元する」参照）IP アドレスは初期値「192.168.10.1」に戻ります。この場合、IP アドレス以外の設定内容もすべて工場出荷時の状態に戻ります。
4. 設定を工場出荷時設定にリセットしたくない場合は、無線コントローラを再起動し、再起動の間に送信されたパケットをキャプチャするためにスニファを使用してください。ARP パケットを確認し、無線コントローラの LAN インタフェースアドレスを検出します。

リセットボタンを使用して工場出荷時設定に復元する

何らかの理由で無線コントローラの Web GUI にアクセスできない場合、前面パネルのリセットボタンを押して、工場出荷時設定を復元します。

すべての設定をクリアして、工場出荷時の設定値を復元する方法 :

1. リセットボタンを 15 秒以上押し続けます。

2. リセットボタンを放します。再起動処理は数分後に完了します。

注意 IP アドレスの初期値は「192.168.10.1」です。ログインユーザ名の初期値は「admin」、ログインパスワードの初期値は「admin」です。

日付と時間に関する問題

「Date and Time」ページ（**Maintenance > Administration > Date and Time**）では現在の日付と時刻を表示します。無線コントローラは、NTP（Network Time Protocol）を使用して、インターネットにあるネットワークタイムサーバの 1 つから現時刻を取得します。ログ内の各エントリには日付と時刻が出力されます。

日時のスタンプが正確でないことを発見した場合、無線コントローラがインターネットに到達できること確認してください。

アクセスポイントに関するディスカバリ問題

無線コントローラが、すべてまたはいずれかのアクセスポイントを検出しない場合 :

1. 無線コントローラが LAN に接続していることを確認してください。（「LAN ポート LED が消灯」参照）

2. アクセスポイントが異なる VLAN で動作している、ある IP サブネットの後方に配置されている、またはスタンドアロンモードで動作している場合、適切な IP アドレス範囲を入力したことを確認してください。（「手順 1: DHCP サーバの有効化（オプション）」参照）

3. ファイアウォールを使用している場合、ファイアウォールで各アクセスポイント用の UDP ポート番号をブロックしないでください。

4. 各アクセスポイントが固有の IP アドレスを使用していることを確認してください。（「AP ディスカバリ方式」参照）複数のアクセスポイントで同じ IP アドレスが使用されている場合、その中の 1 つデバイスのみが検出されます。このような場合、管理リストにそのアクセスポイントを追加して、その IP アドレスを変更してから、再度ディスカバリを実行して、同じ IP アドレスを持つ次のアクセスポイントを検出してください。（「手順 3: 管理するアクセスポイントの選択」参照）

接続問題

アクセスポイントが「Standalone」モードから「Managed」モードに変更されると、スタティックな IP アドレスは DHCP サーバ（ネットワーク上のサーバまたは無線コントローラで設定されるサーバのいずれか）が発行する IP アドレスに変更されます。これにより、各管理対象のアクセスポイントは固有の IP アドレスを持つことになります。

DHCP サーバが存在しない、またはアクセスポイントが DHCP サーバに到達できない場合、アクセスポイントは、IP アドレスの取得を試みる「Connecting」状態にとどまります。ネットワークに DHCP サーバが存在しない場合は無線コントローラ上に設定してください。（「手順 1: DHCP サーバの有効化（オプション）」参照）DHCP サーバが利用可能になると、アクセスポイントは「Connecting」状態から「Connected」状態に移行します。

新しい SSID を追加したにもかかわらず、その SSID が 5 分以内に Wi-Fi ネットワークに現れない場合、以下の手順で無線コントローラを再起動します。

1. **Maintenance > Firmware > Reboot / Factory Default > Soft Reboot** の順にメニューをクリックします。

2. 「Soft Reboot」ボタンをクリックします。

ネットワークの性能と不正アクセスポイントの検出

不正なアクセスポイントの検出を有効にすると、アクセスポイントは断続的に短期間、チャンネルの使用を停止します。これはネットワーク性能に影響を与える可能性があります。ネットワークのパフォーマンスよりも安全上の配慮が重要であれば、不正なアクセスポイントの検出を有効にすることができます。安全上の配慮よりもネットワークのパフォーマンスが重要であれば、一時的に不正なアクセスポイントの検出を無効にすることができます。

無線コントローラにおける診断ツールの使用

IP アドレスの Ping

Maintenance > Management > Diagnostics > Network Tools メニュー

無線コントローラの診断機能の一部として、IP アドレスを Ping できます。無線コントローラと、無線コントローラに接続するネットワーク上の別のデバイス間の接続性をテストするために本機能を使用できます。

1. **Maintenance > Management > Diagnostics > Network Tools** の順にメニューをクリックし、以下の画面を表示します。

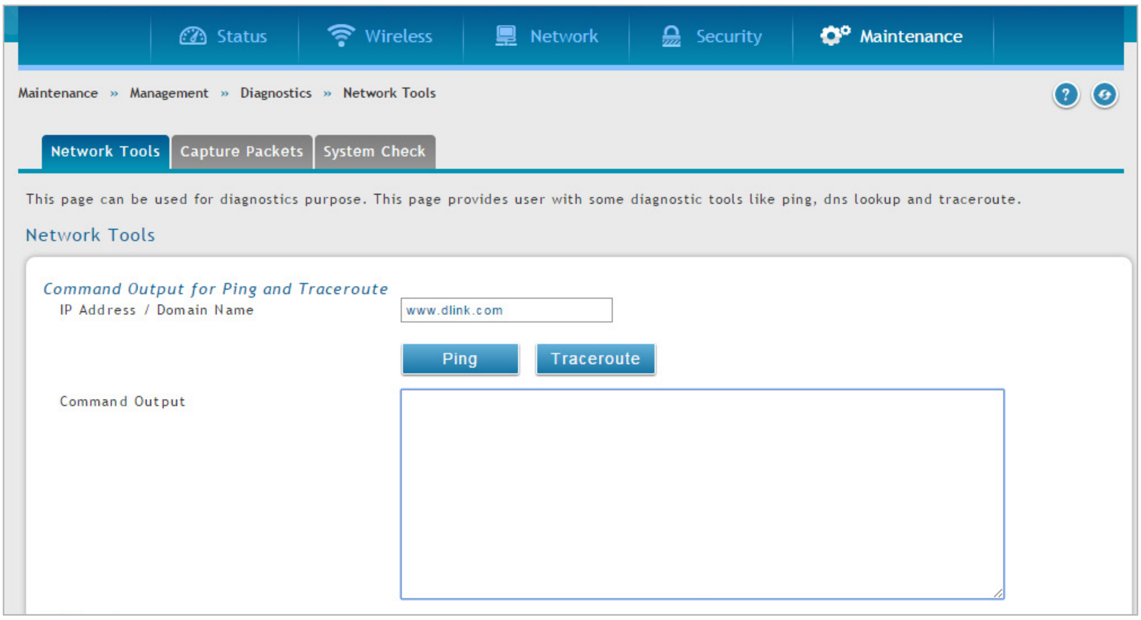


図 10-1　Network Tools 画面

2. 「Command Output for Ping and Traceroute」セクションで「IP Address / Domain Name」に IP アドレスまたはドメイン名を入力します。
3. 「Ping」ボタンをクリックすると、「Command Output」に結果が表示されます。

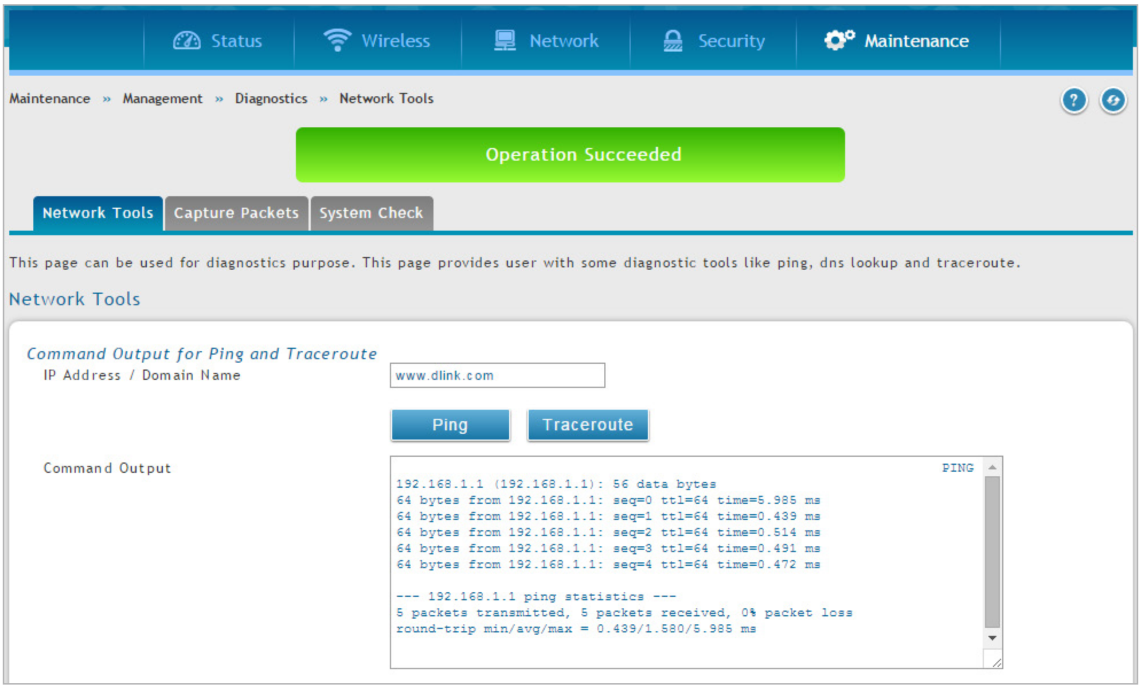


図 10-2　Network Tools 画面

Traceroute の使用

Maintenance > Management > Diagnostics > Network Tools メニュー

無線コントローラは、パブリックホストへのネットワークのパスをマッピングする Traceroute 機能を提供します。本無線コントローラと宛先の間に存在する最大 30 個までのコントローラ（または「ホップ」）が表示されます。

1. **Maintenance > Management > Diagnostics > Network Tools** の順にメニューをクリックし、以下の画面を表示します。

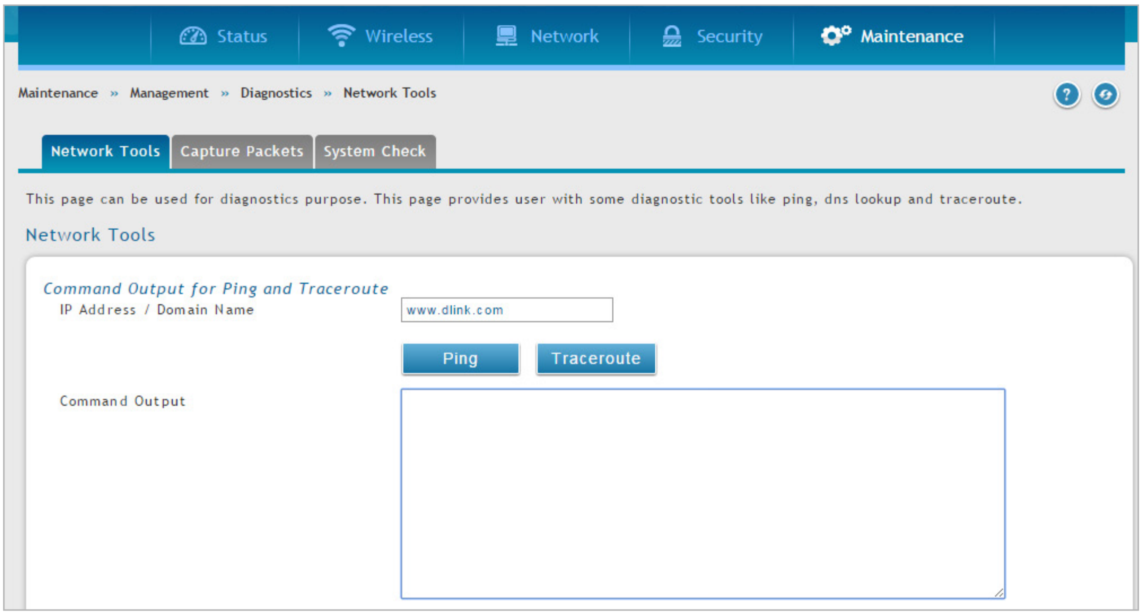


図 10-3　Network Tools 画面

2. 「Command Output for Ping and Traceroute」セクションで「IP Address/Domain Name」に IP アドレスまたはドメイン名を入力します。
3. 「Traceroute」ボタンをクリックすると、「Command Output」に結果が表示されます。

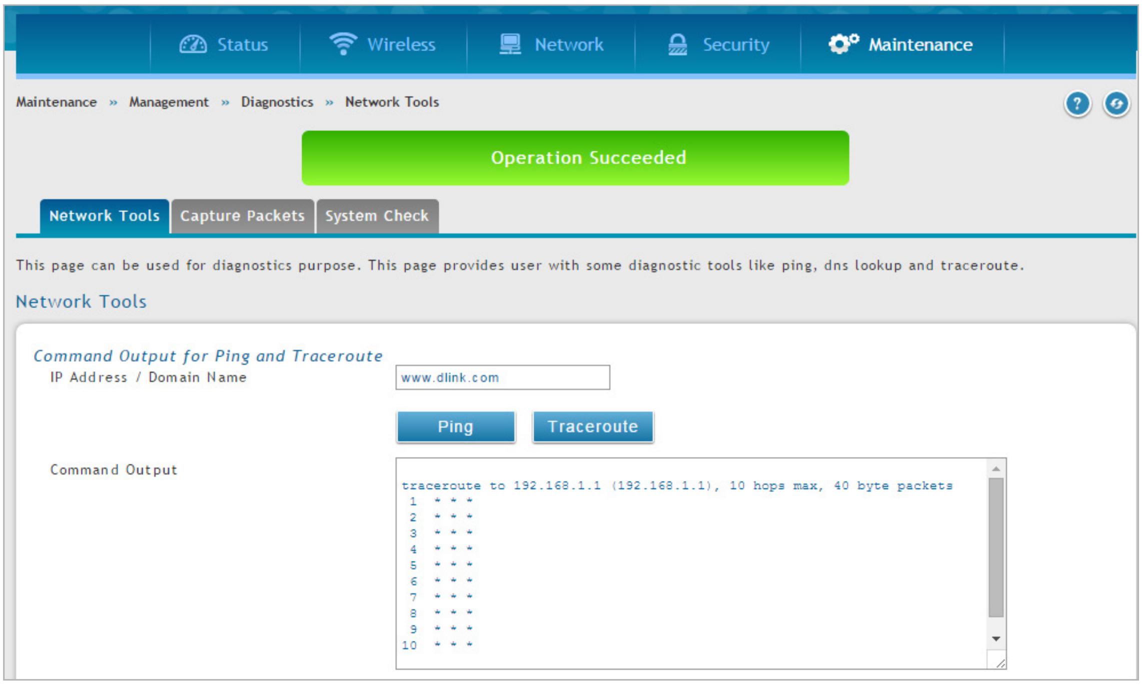


図 10-4　Network Tools 画面

DNS 検索の実行

Maintenance > Management > Diagnostics > Network Tools メニュー

無線コントローラは、インターネット上の Web、FTP、メール、またはその他のサーバの IP アドレスを取得するための DNS 索引機能を提供します。

1. **Maintenance > Management > Diagnostics > Network Tools** の順にメニューをクリックし、以下の画面を表示します。

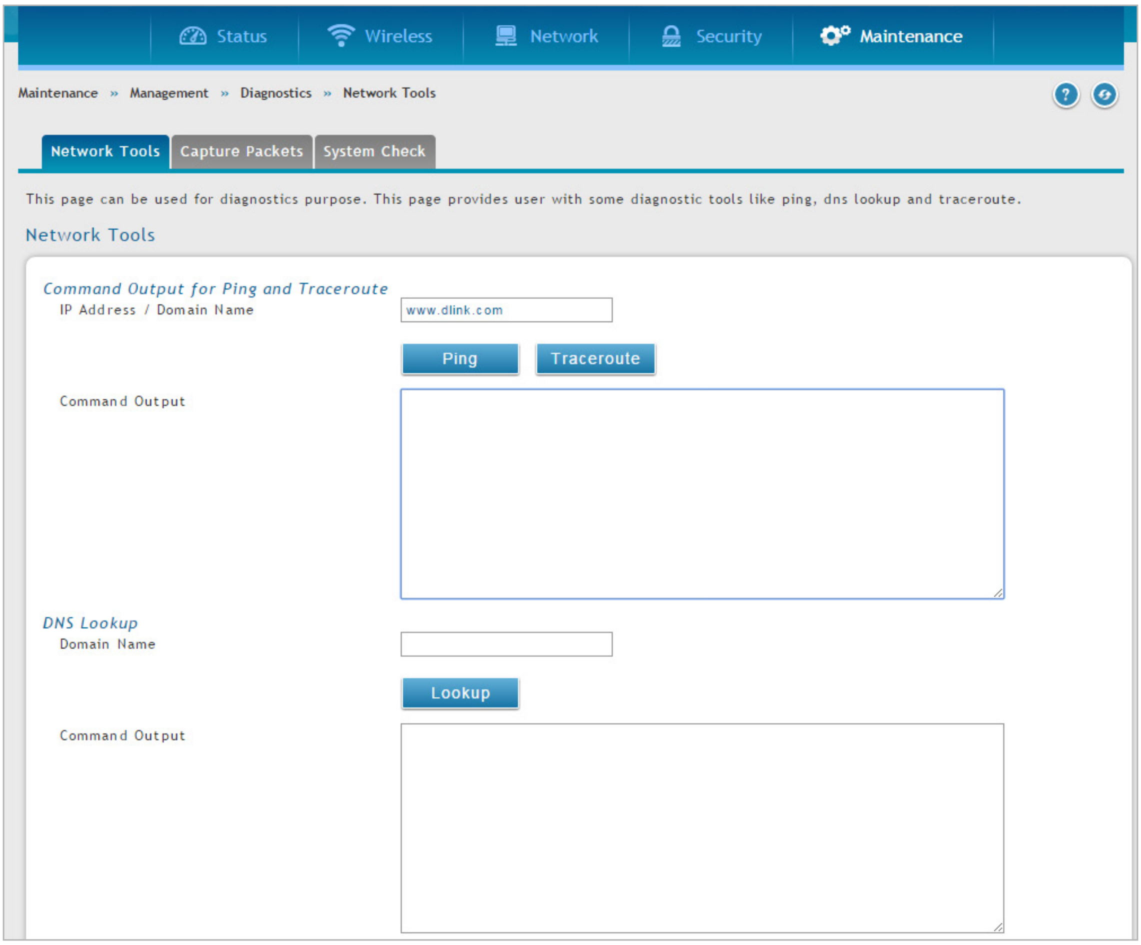


図 10-5　Network Tools 画面

2. 「DNS Lookup」の「Domain Name」フィールドにインターネット名を入力します。

3. 「Lookup」ボタンをクリックすると、「Command Output」に結果が表示されます。ホストまたはドメインエントリが存在する場合、IP アドレスを含む応答が表示されます。「Host Unknown」メッセージ表示された場合、そのインターネット名は存在しません。

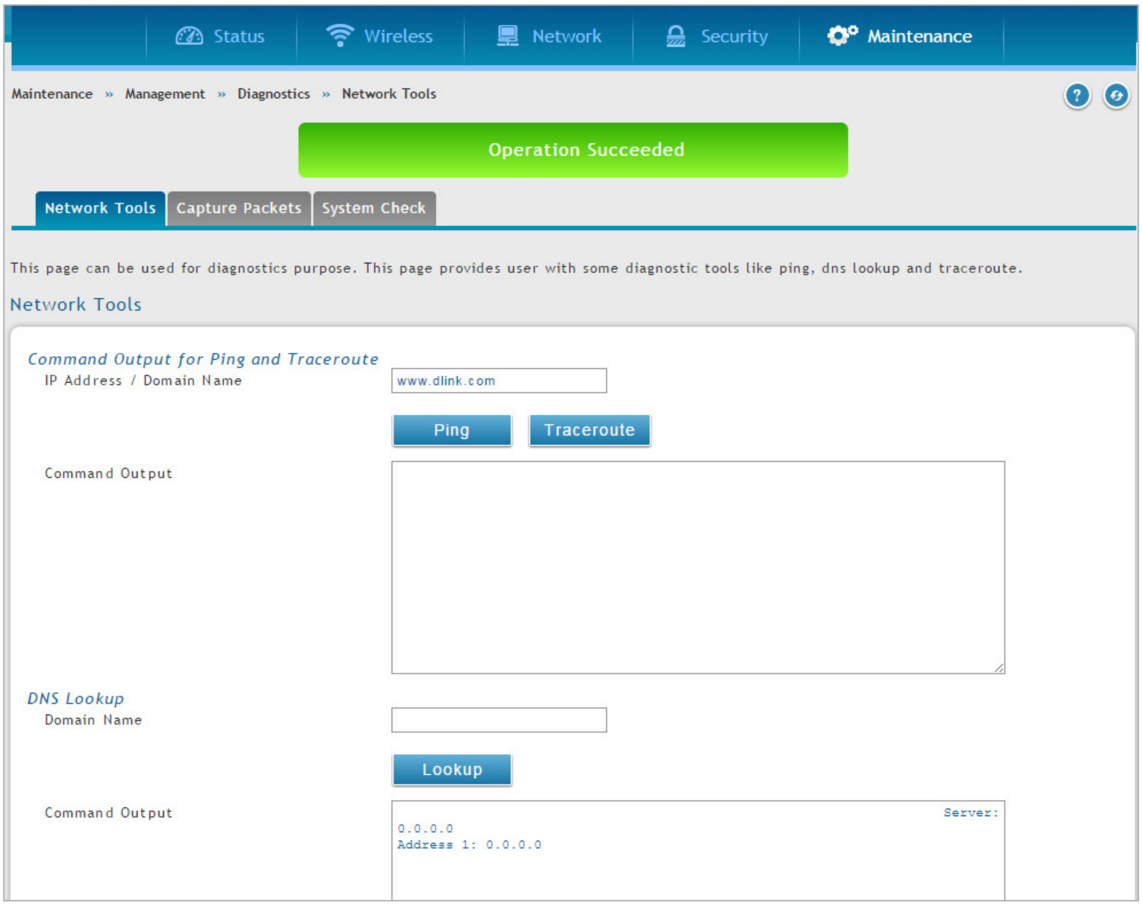


図 10-6　 Network Tools 画面

ログパケットのキャプチャ

Maintenance > Management > Diagnostics > Capture Packets メニュー

無線コントローラにより、LAN インタフェースを通過するすべてのパケットをキャプチャすることができます。パケットのトレースはキャプチャセッションあたり 1MB のデータに制限されます。キャプチャファイルサイズが 1MB を超えると、自動的に削除されて新しいキャプチャファイルが作成されます。

パケットのキャプチャ：

1. **Maintenance > Management > Diagnostics > Capture Packets** の順にメニューをクリックし、以下の画面を表示します。

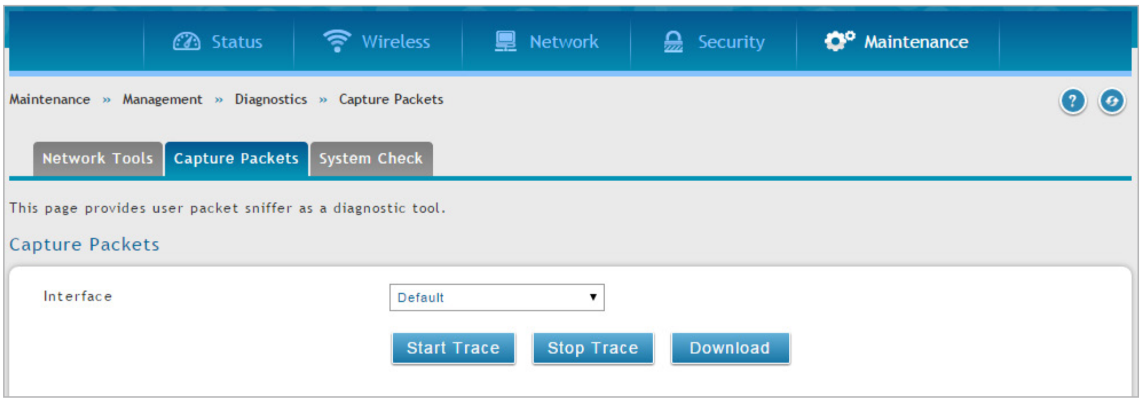


図 10-7　 Capture Packets 画面

2. 「Interface」のプルダウンメニューからインタフェースを選択します。

3. 「Start Trace」ボタンをクリックすると、パケットのキャプチャを開始します。

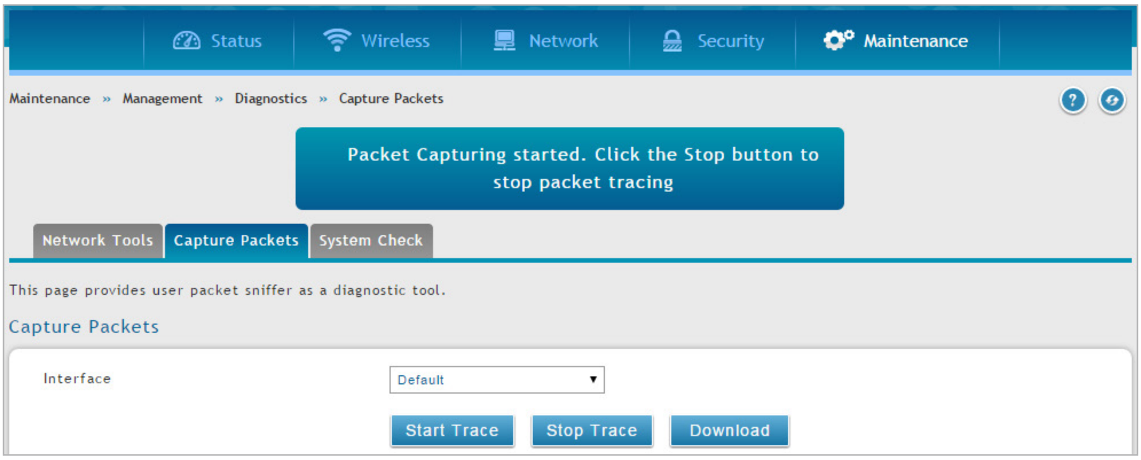


図 10-8　Capture Packets 画面

パケットのキャプチャを停止するには「Stop Trace」ボタンをクリックします。

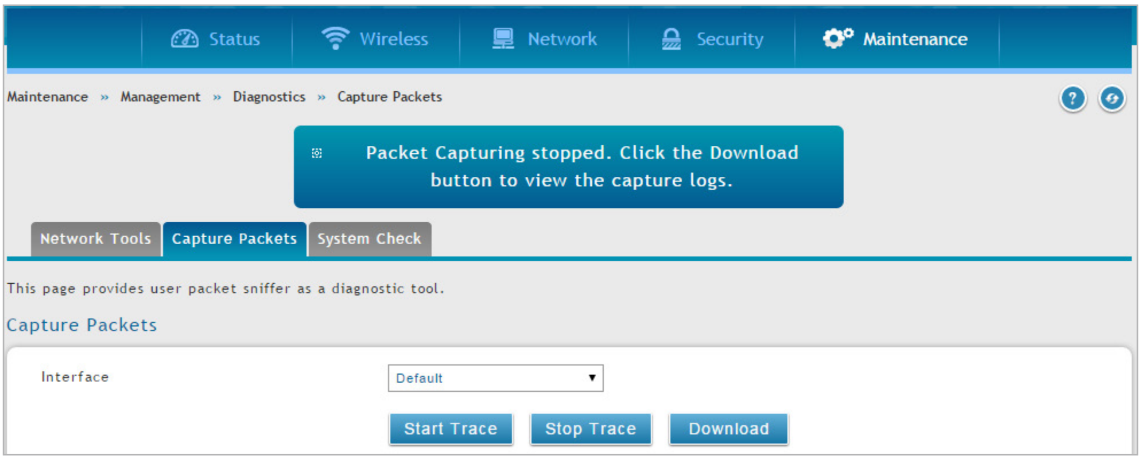


図 10-9　Capture Packets 画面

「Download」ボタンをクリックすると、トレース結果をダウンロードできます。ブラウザのデフォルトのダウンロードフォルダにファイルが保存されます。

システムチェックの実施

Maintenance > Management > Diagnostics > System Check メニュー

無線コントローラのスタティック / ダイナミックルートを表示します。

1. **Maintenance > Management > Diagnostics > System Check** の順にメニューをクリックし、以下の画面を表示します

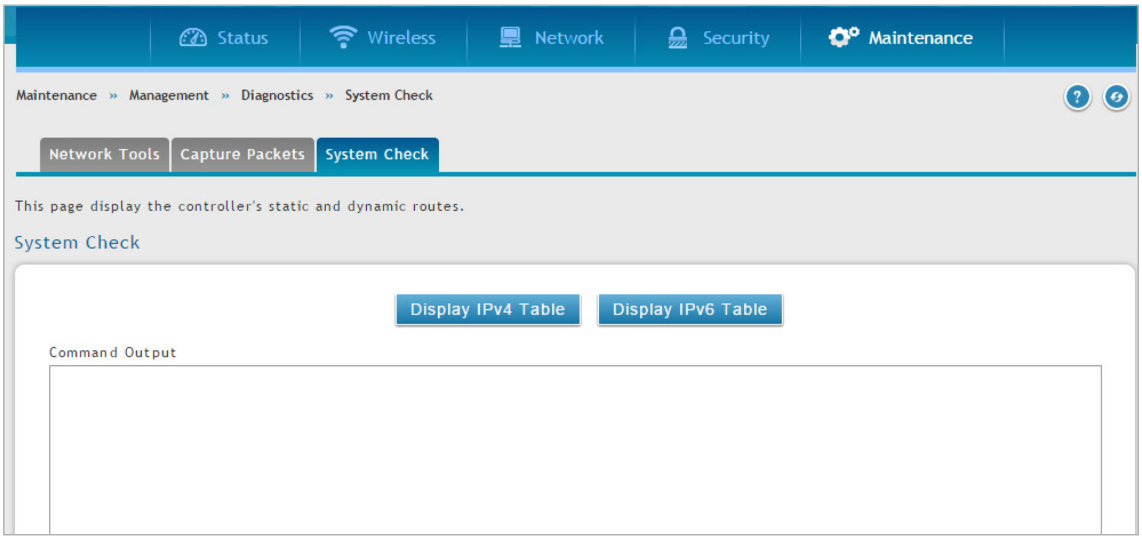


図 10-10　System Check 画面

2. 「Display IPv4 Table」または「Display IPv6 Table」ボタンをクリックすると、「Command Output」に結果が表示されます。

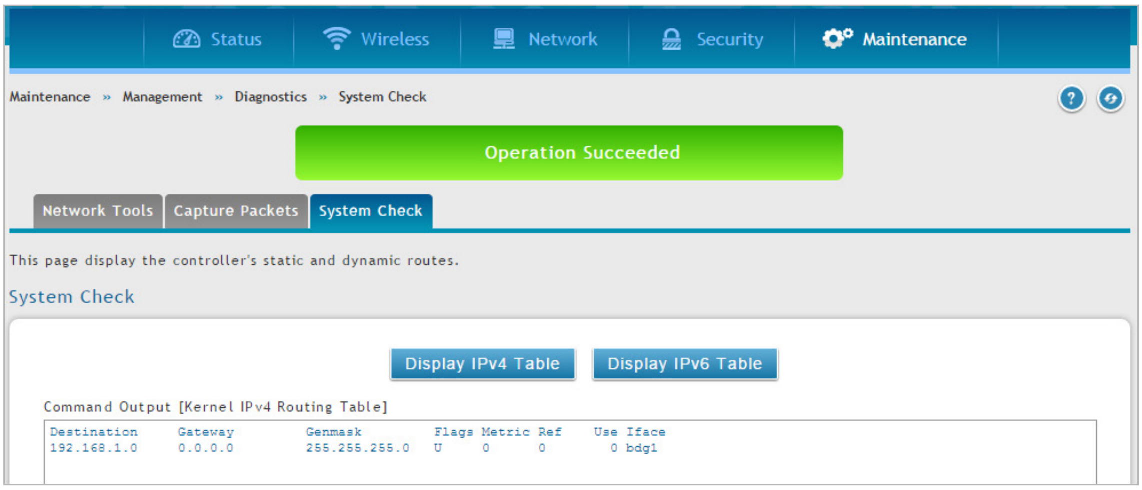


図 10-11　System Check 画面（IPv4）

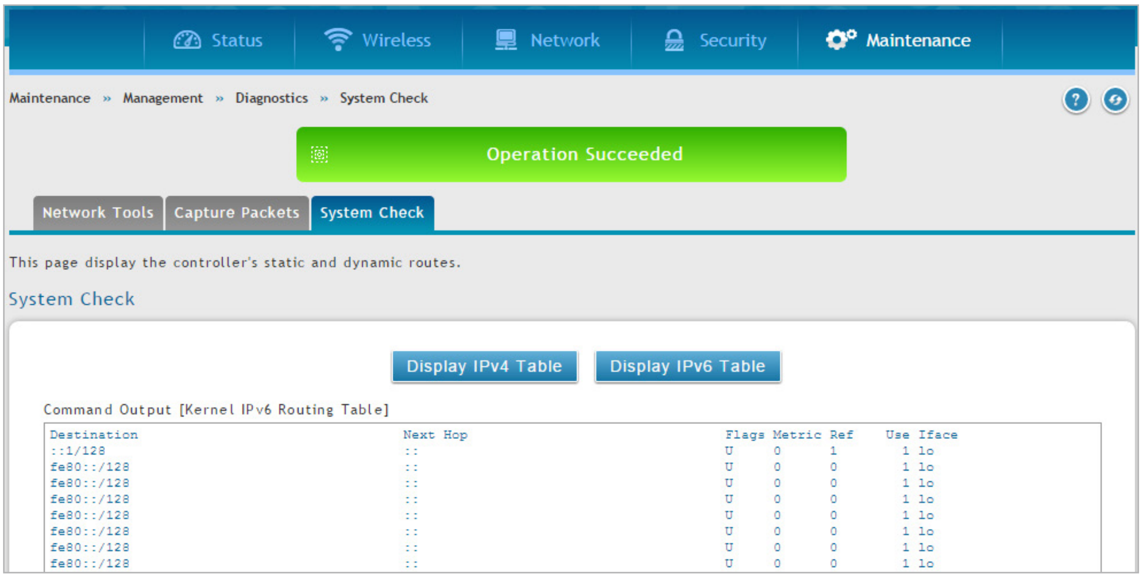


図 10-12　System Check 画面（IPv6）

ログ設定

無線コントローラでは、ログメッセージを取得することができます。無線コントローラを通過するトラフィックタイプをモニタして、潜在的な攻撃またはエラーが検出された際に通知を行うことができます。以下のセクションでは、ログ構成設定とそれらのログにアクセスする方法を説明しています。

ログ出力の定義

Maintenance > Logs Settings > Facility Logs メニュー

「Facility Logs」画面では、無線コントローラから受信するログのレベルを決定することができます。「Select Facility」でファシリティを選択します。

1. **Maintenance > Logs Settings > Facility Logs** の順にメニューをクリックし、以下の画面を表示します。

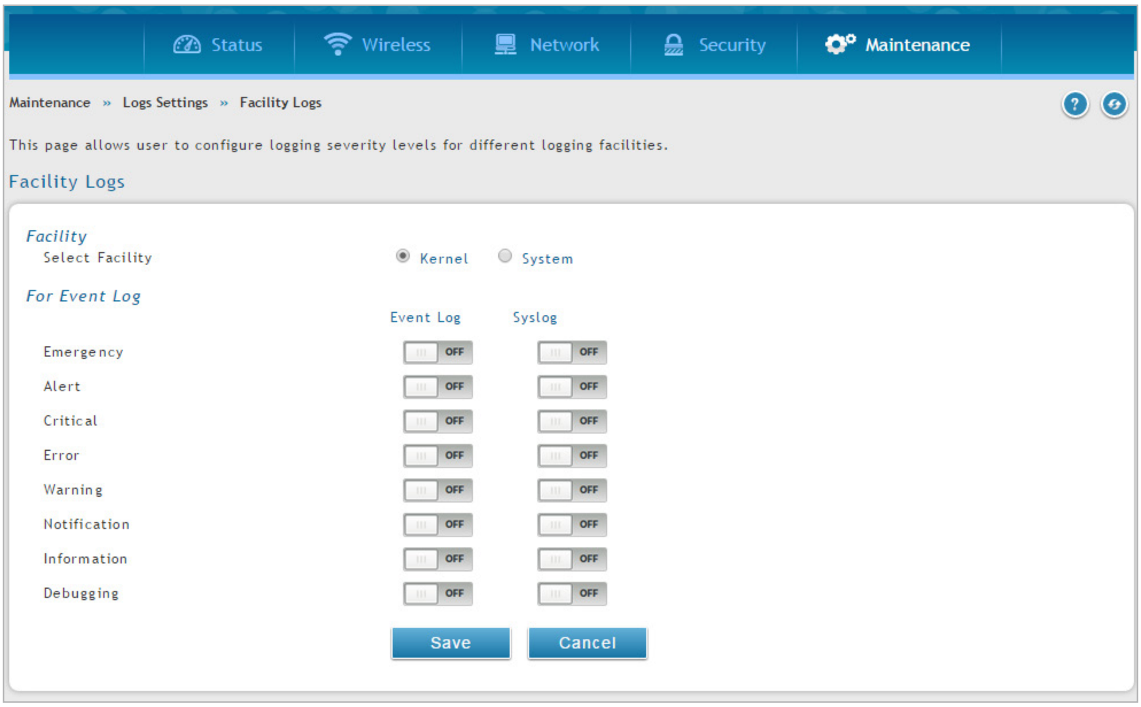


図 10-13　Facility Logs 画面

以下の項目があります。

項目	説明
Facility	
Kernel	Linux カーネル。このファシリティに該当するログメッセージは、ファイアウォールまたはネットワークスタックを通過するトラフィックに対応します。
System	ユニットを管理するための無線コントローラで利用可能なアプリケーションおよび管理レベルの機能。
For Event Log	
Emergency	システムが使用できません。
Alert	直ちに、何らかのアクションを実施する必要があります。
Critical	クリティカルな状態
Error	エラー状態
Warning	注意すべき状態
Notification	標準ではあるが注意すべき状態
Information	情報
Debugging	デバッグレベルのメッセージ

各ファシリティにおいて、上記のイベント（重要度が高い順で記載）がログに出力されます。

2. ファシリティの各セベリティについて「ON」（有効）または「OFF」（無効）にして、「Save」ボタンをクリックします。

ログの表示は、以下のログ送信先に基づいてカスタマイズすることができます。

- Web 管理インタフェースの Event Log ビューア（**Status > System Information > All Logs > Current Logs**）
- リモート Syslog サーバ

別のセクションで説明するメールログについては、Syslog サーバに設定されたログと同じ設定に従います。

トラフィックの追跡 / ルーティングログ

Maintenance > Logs Settings > Routing Logs メニュー

ファイアウォールによりパケットが許可されたか破棄されたかに基づいて、トラフィックを追跡することができます。DoS（Denial of Service）攻撃、一般的な攻撃情報、ログインの試み、破棄されたパケットなどのイベントを、IT 管理者による確認のために取得することができます。

注意 ログオプションを有効にすると、大量のログメッセージを生成する可能性があるため、デバッグ目的だけに使用することをお勧めします。

1. **Maintenance > Logs Settings > Routing Logs** の順にメニューをクリックし、以下の画面を表示します。

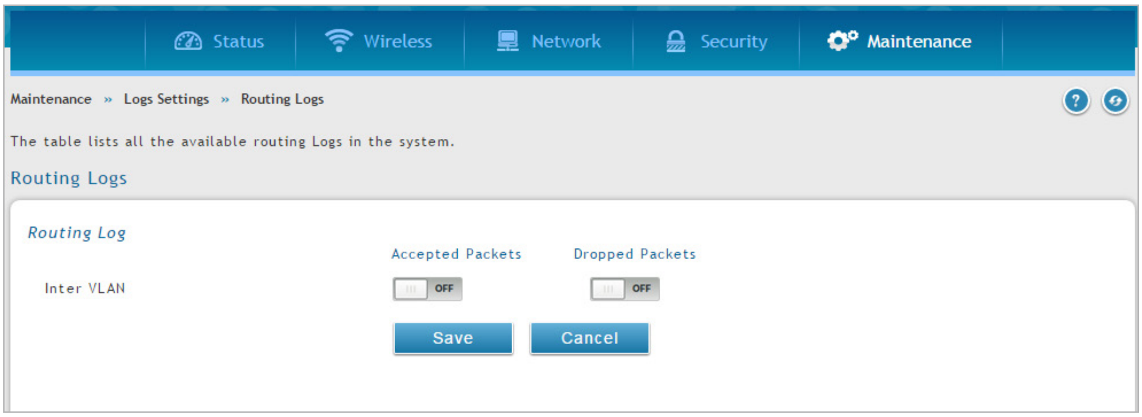


図 10-14　Routing Logs 画面

以下の項目があります。

項目	説明
Routing Log	
Inter VLAN	有効化した場合、インター VLAN ルーティングのログからトラフィックを追跡します。 • Accepted Packets - 有効にすると、セグメントの通過に成功したパケットを追跡します。 • Dropped Packets - 有効にすると、セグメントの通過でブロックされたパケットを追跡します。

2. 設定後、「Save」ボタンをクリックして変更を保存するか、「Cancel」ボタンをクリックして、前の設定に戻ります。

リモートログ

Maintenance > Logs Settings > Remote Logs メニュー

メールアドレスにログを送信するように無線コントローラを設定することができます。メール送信の頻度を選択すると、メールログは定義したスケジュール（1 時間毎、1 日毎、1 週間毎）に基づいて送信されます。
無線コントローラでは、3 つのメール受信先に設定ログを送信することができます。

1. **Maintenance > Logs Settings > Remote Logs** の順にメニューをクリックし、以下の画面を表示します。

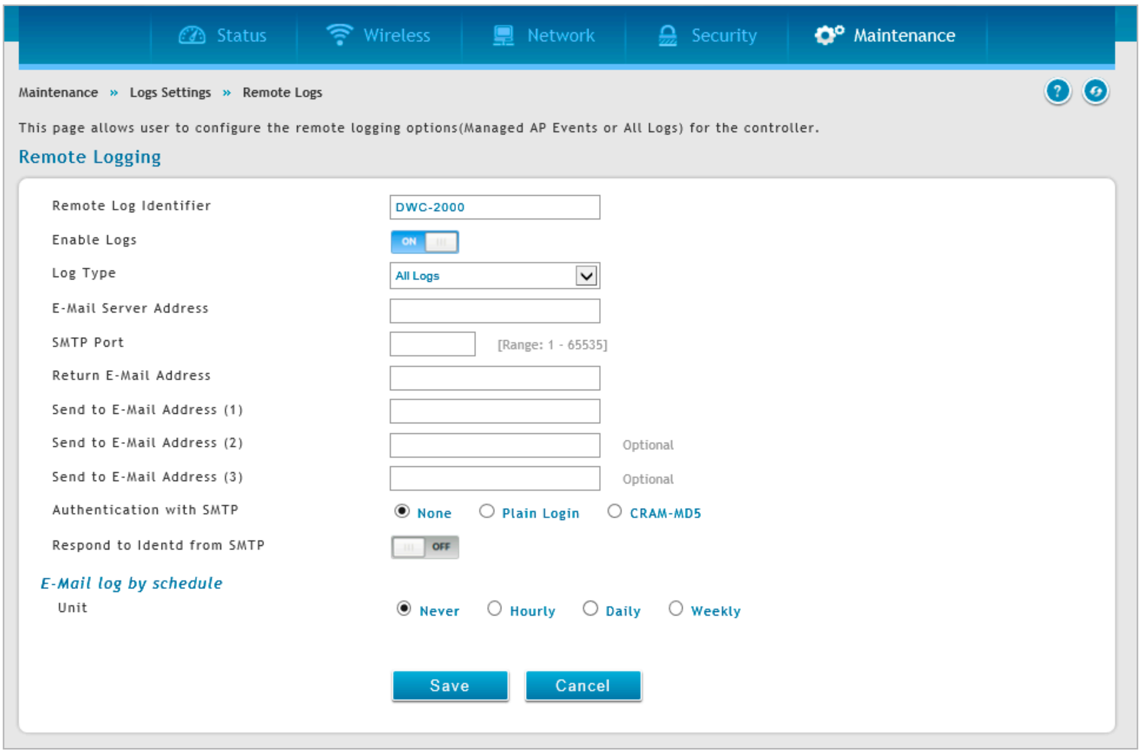


図 10-15　Remote Logging 画面

2. 以下の項目を設定後、「Save」ボタンをクリックして変更を保存します。

項目	説明
Remote Log Identifier	ログ出力メッセージには、メッセージの送信元を識別するためのプレフィックスが含まれます。このログ識別子は、E メールと Syslog ログメッセージの両方の先頭に付けられます。
Enable Logs	メールログを有効、または無効にします。 • ON - メールログを有効にします。本画面で追加のフィールドを入力します。 • OFF - メールログを無効にします。追加のフィールドは表示されません。
Log Type	ログの種類を指定します。 • All logs - 全てのログが対象です。 • Managed AP Event Log - 管理 AP のイベントログのみが対象です。
E-Mail Server Address	SMTP（Simple Mail Transfer Protocol）サーバの IP アドレスまたはインターネット名を入力します。必要に応じて、無線コントローラはこのサーバに接続してメールログを送信します。SMTP サーバは、受信するメール通知に対して操作可能である必要があります。
SMTP Port	メールサーバの SMTP ポートを入力します。
Return E-Mail Address	SMTP サーバからの応答が送信されるメールアドレスを入力します。（失敗メッセージのために必要です。）
Send to E-mail Address (1-3)	ログ、警告が送信されるメールアドレスを最大 3 つまで入力します。
Authentication with SMTP	接続を許可するための SMTP サーバが認証が必要な場合、認証方式を選択します。 • None - 認証は使用されません。「User Name」および「Password」フィールドは表示されません。 • Login Plain - 非暗号化の通信セッション上で Base64 によりコード化されたパスワードを使用してログインするために使用される認証。Base64 でコード化されたパスワードでは、暗号化保護を行わないため安全性が低くなります。 • CRAM-MD5 - RFC 2195 で定義された、HMAC-MD5 MAC アルゴリズムに基づくチャレンジレスポンス認証メカニズム。「CRAM-MD5」は、「Login Plain」よりも高いレベルの認証を提供します。
User Name	「Authentication with SMTP」に「Login Plain」または「CRAM-MD5」を設定した場合、認証に使用するユーザ名を入力します。
Password	「Authentication with SMTP」に「Login Plain」または「CRAM-MD5」を設定した場合、認証に使用するパスワード（大文字、小文字の区別あり）を入力します。
Enable Tls	「Authentication with SMTP」に「Login Plain」または「CRAM-MD5」を設定した場合、認証に使用する TLS を有効にします。

項目	説明
Respond to Identd from SMTP	無線コントローラが SMTP サーバからの IDENT 要求に応答するかどうかを決定します。 • ON - 無線コントローラは SMTP サーバからの IDENT 要求に応答します。 • OFF - 無線コントローラは SMTP サーバからの IDENT 要求を無視します。
E-Mail log by schedule	
Unit	E-Mail ログの送信方法を以下から選択します。Log Type で All Logs を選択した場合に表示されます。 • Never - E-Mail ログを送信しません。 • Hourly - 1 時間ごとに E-Mail ログを送信します。 • Daily - 1 日ごと E-Mail ログを送信します。ログを送信する時刻を設定します。 • Weekly - 1 週間ごとに E-Mail ログを送信します。ログを送信する曜日と時刻を設定します。

Syslog サーバ構成

Maintenance > Logs Settings > Syslog Server メニュー

無線コントローラからログを収集し保存するために、ネットワーク管理者によって外部の Syslog サーバが多く使用されます。このリモートデバイスでは、通常、無線コントローラの Web 管理インタフェース上のローカルなイベントビューアよりもメモリが制限されないため、長期間に渡り多くのログを収集することができます。これは、ネットワーク問題のデバッグや長期間コントローラトラフィックをモニタする場合に役に立ちます。

本無線コントローラは同時に 8 個までの Syslog サーバをサポートします。「Syslog Server」画面上で､各サーバが受信するログファシリティメッセージの種類とセベリティのレベルを設定します。

1. **Maintenance > Logs Settings > Syslog Server** の順にメニューをクリックし、以下の画面を表示します。

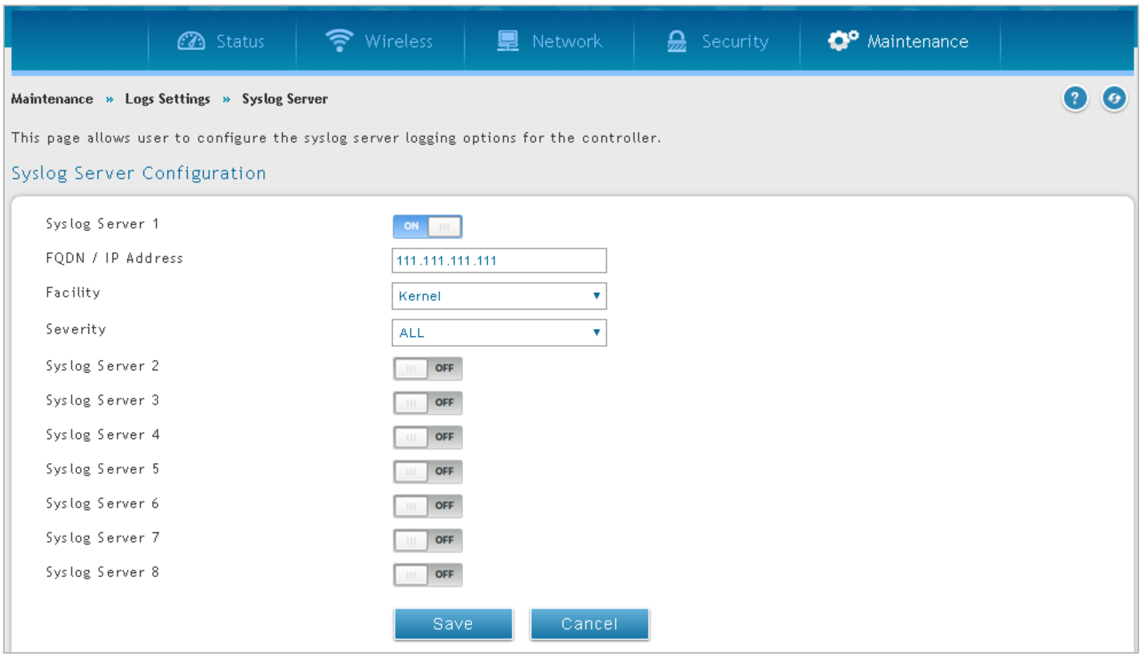


図 10-16　Syslog Server Configuration 画面

2. 以下の項目を設定後、「Save」ボタンをクリックして変更を保存します。

項目	説明
Syslog Server (1-8)	Syslog サーバを有効にするために、Syslog サーバ欄の「ON/OFF」スイッチをクリックし、「Name」欄に IP アドレスまたは FQDN を入力します。本画面の設定を保存した後に、設定した（および有効にした）Syslog サーバに選択されたファシリティとセベリティレベルのメッセージが送信されます。
FQDN / IP Address	Syslog サーバの FQDN/IP アドレスを指定します。
Facility	各 Syslog サーバに、ログ出力用の固有のファシリティ（All、Kernel、System）を選択します。ファシリティ値は RFC 3164 で定義されています。
Syslog Severity	適切な Syslog のセベリティを選択します。セベリティを選択すると、選択されたセベリティ以上のセベリティを持つすべてのイベントが、定義済みの Syslog サーバにログ出力されます。 • All • Log Debug • Log Info • Log Notice • Log Warning • Log Error • Log Critical • Log Alert • Log Emerg

イベントログ

Maintenance > Logs Settings > Event Logs メニュー

Web 管理インタフェースの「Status」メニューでは、設定したログメッセージを閲覧することができます。無線コントローラから（へ）のトラフィックが **Maintenance > Log Settings > Facility Logs** ページ（「ログ設定」参照）、または **Maintenance > Log Settings > Routing Logs** ページ（「トラフィックの追跡 / ルーティングログ」参照）内の設定に一致すると、対応するログメッセージが、タイムスタンプと共に出力されます。

1. **Maintenance > Logs Settings > Event Logs** の順にメニューをクリックし、以下の画面を表示します。

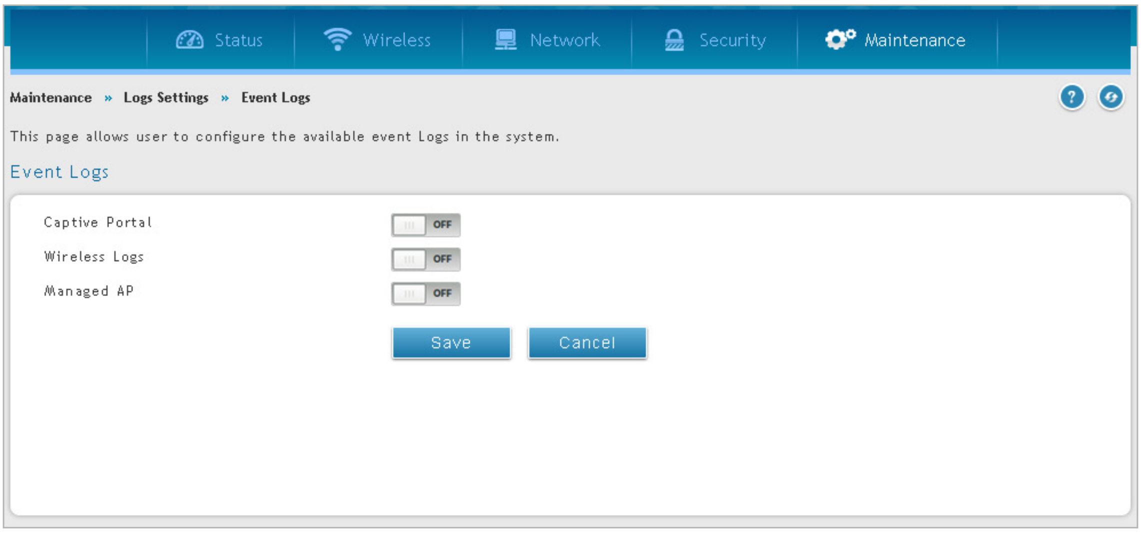


図 10-17　Event Logs 画面

2. 以下の項目を設定後、「Save」ボタンをクリックして変更を保存します。

項目	説明
Captive Portal	有効にすると、コントローラはキャプティブポータルを経由した無線クライアントのログインおよびログアウトに関連する情報をログに出力します。
Wireless Logs	有効にすると、コントローラは無線アクティビティに関連する情報をログに出力します。
Managed AP	有効にすると、コントローラは管理 AP に関連する情報をログに出力します。

注意　ログメッセージを理解するために、手動または NTP サーバにより正確なシステム時間が設定されていることが非常に重要となります。

現在のログ

Status > System Information > All Logs > Current Logs メニュー

コントローラで設定したログメッセージを表示します。各ログは、コントローラに設定された時間に従って決定されるタイムスタンプと共に表示されます。Syslog サーバまたはメールログ出力などのリモートログ出力が設定されている場合、ここで表示されるだけでなく、同じログをリモートインタフェースにも送信します。

Status > System Information > All Logs > Current Logs の順にメニューをクリックし、以下の画面を表示します。

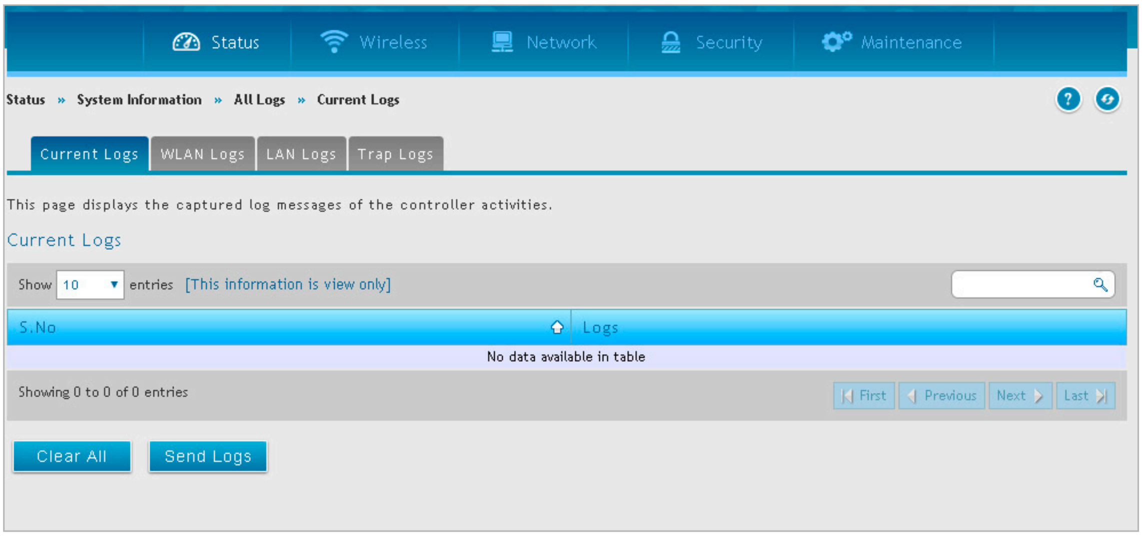


図 10-18　Current Logs 画面

ログの更新またはページのリロードを行うには、（ページの右側）アイコンをクリックします。

「Clear All」ボタンをクリックして、画面内のすべてのエントリをクリアします。

「Send Logs」ボタンをクリックして、画面内のすべてのエントリを設定済みのメール受信者に送信します。

WLAN ログ

Status > System Information > All Logs > WLAN Logs メニュー

WLAN インタフェース上のログメッセージを表示します。各ログは、コントローラに設定された時間に従って決定されるタイムスタンプと共に表示されます。ここに表示される他に、WLAN インタフェースに同じログを送信します。

Status > System Information > All Logs > WLAN Logs の順にメニューをクリックし、以下の画面を表示します。

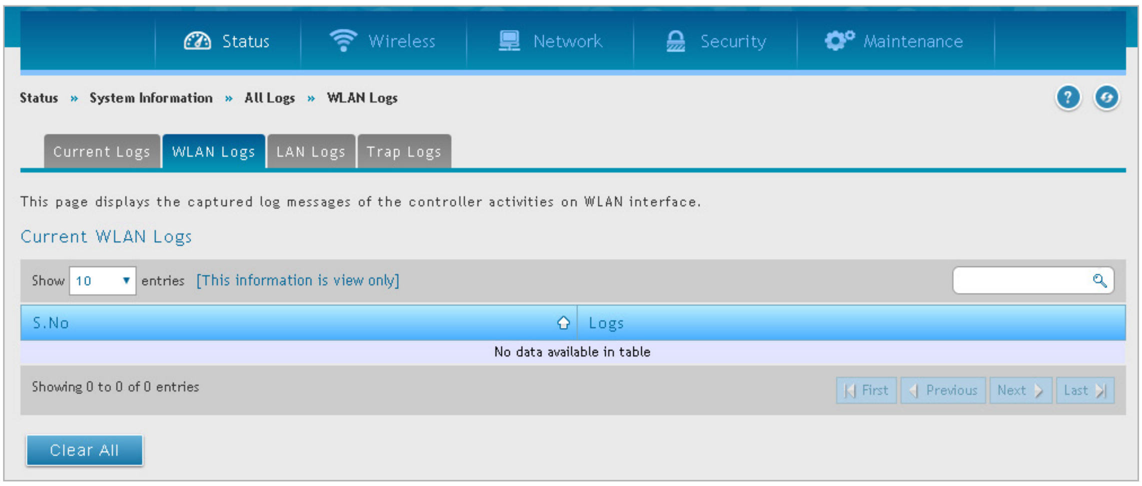


図 10-19　Current WLAN Logs 画面

ログの更新またはページのリロードを行うには、（ページの右側）アイコンをクリックします。

「Clear All」ボタンをクリックして、画面内のすべてのエントリをクリアします。

LAN ログ

Status > System Information > All Logs > LAN Logs メニュー

LAN インタフェース上のログメッセージを表示します。各ログは、コントローラに設定された時間に従って決定されるタイムスタンプと共に表示されます。ここに表示される他に、WLAN インタフェースに同じログを送信します。

Status > System Information > All Logs > LAN Logs の順にメニューをクリックし、以下の画面を表示します。

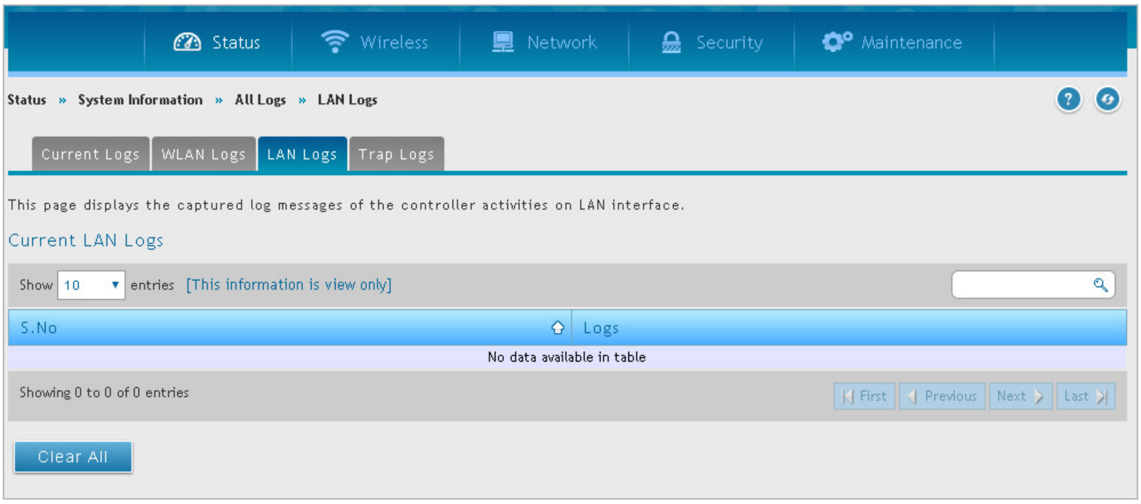


図 10-20　Current LAN Logs 画面

ログの更新またはページのリロードを行うには、（ページの右側）アイコンをクリックします。

「Clear All」ボタンをクリックして、画面内のすべてのエントリをクリアします。

Trap ログ

Status > System Information > All Logs > Trap Logs メニュー

SNMP Trap ログメッセージを表示します。

Status > System Information > All Logs > Trap Logs の順にメニューをクリックし、以下の画面を表示します。

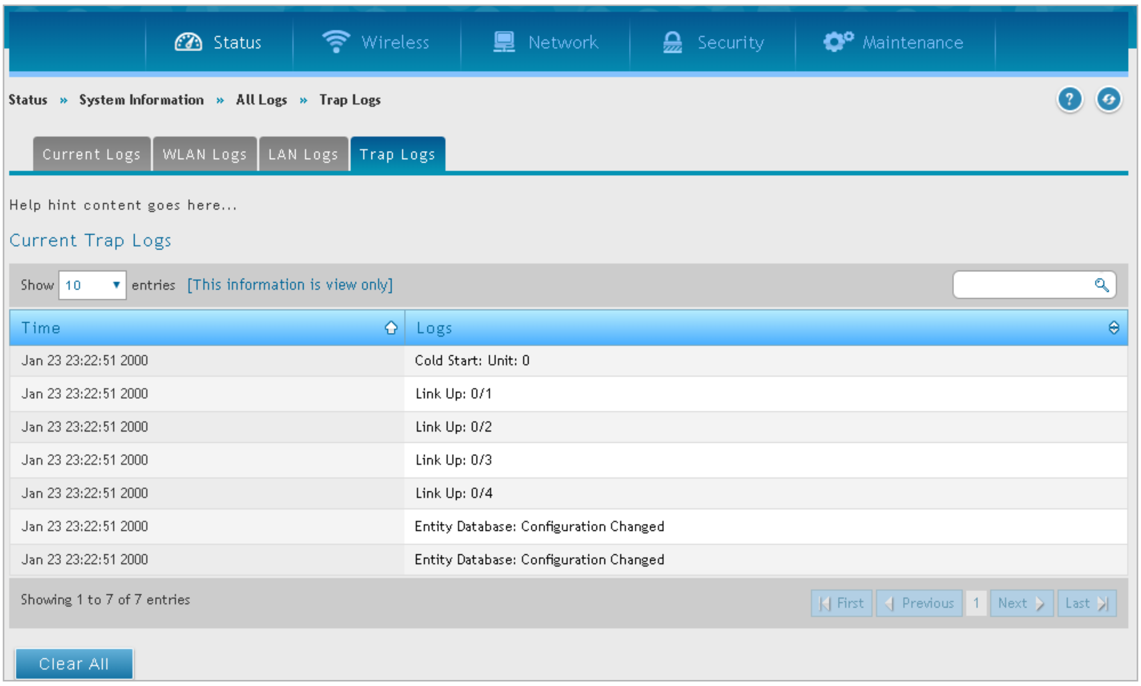


図 10-21　Current Trap Logs 画面

ログの更新またはページのリロードを行うには、（ページの右側）アイコンをクリックします。

「Clear All」ボタンをクリックして、画面内のすべてのエントリをクリアします。

付録

付録 A 基本計画のワークシート

無線周波数(RF)の計画により、提供するWi-Fiカバレッジの範囲を規定します。適切なWi-Fiカバレッジを提供するために、カバレッジマップを規定し、追加のアクセスポイントを必要とする信号が弱い傾向の場所やデッドスポットを確認します。

計画の取り組みを促進させるために、この付録のような基本計画のワークシートを使用して、以下の重要な情報を収集できます。

- ビルの規模
- 無線カバレッジで壁と考えられる障害
- フロア数
- フロア間の距離
- ユーザ総数とアクセスポイントあたりのユーザ数
- 無線電波のタイプ
- 希望のアクセスポイントのデータ速度
- アクセスポイントを配置したいエリア
- アクセスポイントを配置できないエリア
- 適用範囲から外したいエリア

ステップ	タスク	完了有無
サイトの計画		
1	ビルの高さ	
2	ビルの幅	
3	フロア数	
4	フロアの規模	
5	フロア間の距離	
6	目に見える障害物	
7	干渉を引き起こす可能性	
アクセスポイントの計画		
1	周波数帯	
2	予想される信号品質	
3	1 アクセスポイントあたりのクライアント数	
4	1 フロアあたりのクライアント総数	
5	希望のアクセスポイントのデータ速度	
無線コントローラの計画		
1	無線コントローラの初期パスワードを変更し、ここに記録してください。	
2	タイムゾーンを設定し、それをここに記録してください。＿＿＿＿＿＿＿＿＿＿＿＿	
3	無線帯域設定の初期値を使用しますか？ • プロファイル名 : ＿＿＿＿＿＿＿＿＿＿＿＿ • クライアント ＿＿＿＿＿＿＿＿＿＿＿＿ • 利用可能なモード : • 802.11 n: • 802.11 b/g: • 802.11 b/g/n: • 802.11 b/g/n/ax: • 802.11 a : • 802.11 a/n : • 802.11 a/n/ac : • 802.11 a/n/ac /ax :	
4	SSID 情報 • SSID 名 ＿＿＿＿＿＿＿＿＿＿＿＿ • セキュリティ（none、WEP、WPA、WPA2、WPA3）＿＿＿＿＿＿＿＿＿＿＿＿	

ステップ	タスク	完了有無
5	無線コントローラを DHCP サーバとして使用しますか ? • Yes - ホスト名、IP アドレスはダイナミックに割り当てられます。 • No - DHCP リレーを使用するか、またはスタティック IP アドレスを設定して、それらを以下に記録してください。 - IP アドレス : ____________________ - IP サブネットマスク : ____________________ - ゲートウェイ IP アドレス : ____________________ - プライマリ DNS サーバ : ____________________ - セカンダリ DNS サーバ : ____________________	
6	LAN IP アドレス :	
7	サブネットマスク :	
8	IP アドレス範囲 : • 開始の IP アドレス : • 終了の IP アドレス :	
9	デフォルトゲートウェイ(オプション):	
10	DNS サーバ : • プライマリ DNS サーバ : • セカンダリ DNS サーバ :	
11	ドメイン :	
12	WINS サーバ :	
13	インターネットに接続しますか ? • はい • いいえ	
14	無線コントローラとすべてのアクセスポイントのファームウェアレベルを確認して、記録します。: • DWC-2000 無線コントローラ : • DWL-2600AP アクセスポイント : • DWL-3600AP アクセスポイント : • DWL-6620APS アクセスポイント : • DWL-6600AP アクセスポイント : • DWL-7620AP アクセスポイント : • DWL-8600AP アクセスポイント : • DWL-8610AP アクセスポイント :	
15	無線コントローラとすべてのアクセスポイントの MAC アドレスを記録します。: • DWC-2000 無線コントローラ : • DWL-2600AP アクセスポイント : • DWL-3600AP アクセスポイント : • DWL-6620APS アクセスポイント : • DWL-6600AP アクセスポイント : • DWL-7620AP アクセスポイント : • DWL-8600AP アクセスポイント : • DWL-8610AP アクセスポイント :	

付録 B 工場出荷時設定

機能	説明	初期値
デバイスログイン	ユーザログイン	URL http://192.168.10.1
	ユーザ名（大文字小文字区別あり）	admin
	ログインパスワード（大文字小文字区別あり）	admin
ローカルエリアネットワーク（LAN）	IP アドレス	192.168.10.1
	IPv4 サブネットマスク	255.255.255.0
	DHCP サーバ	無効
	DHCP 開始の IP アドレス	192.168.10.100
	DHCP 終了の IP アドレス	192.168.10.254
	Time zone	GMT
	DST のために調整されるタイムゾーン	無効
	SNMP	無効
	リモート管理	無効

付録 C 用語解説

用語	説明
アクセスポイント	ネットワークアクセスを無線デバイスに提供するデバイス。
ARP	Address Resolution Protocol。IP アドレスを MAC アドレスにマップするブロードキャストプロトコル。
CHAP	Challenge-Handshake Authentication Protocol。ISP に対してユーザを認証するためのプロトコル。
DDNS	Dynamic DNS。リアルタイムでドメイン名を更新するシステム。ドメイン名がダイナミック IP アドレスを持つデバイスに割り当てられます。
DHCP	Dynamic Host Configuration Protocol。IP アドレスを動的に割り当てるプロトコル。ホストで IP アドレスが不要となった後にアドレスの再利用が可能です。
DNS	インターネットやプライベートネットワークに接続されたコンピュータ、サービス、その他リソースのための、階層的な分散ネーミングシステム。
FQDN	FQDN（完全修飾ドメイン名）。ホスト部分を含む完全なドメイン名となります。例 : serverA.companyA.com
FTP	File Transfer Protocol。ネットワークノード間でファイルを転送するプロトコル。
HTTP	Hypertext Transfer Protocol。ファイルの転送のために Web ブラウザと Web サーバに使用されるプロトコル。
IKE	Internet Key Exchange。VPN トンネルを構築する際に ISAKMP を使用して安全に暗号化鍵を交換するモード。
IP	Internet Protocol。インターネットプロトコルスイートを使用したインターネットワークを経由して、データグラム（ネットワークパケット）を中継するために使用される主要な通信プロトコル。IP はネットワーク境界を経由したパケットをルーティングする役割を担います。インターネットを確立するプライマリプロトコルです。
IPSec	IP security。データストリームにおける IP パケットの認証、または暗号化によって VPN トンネルを保証するプロトコルセット。IPSec は、「transport」モード（パケットヘッダではなく、ペイロードを暗号化する）または「tunnel」モード（ペイロードとパケットヘッダの両方を暗号化する）のいずれかで動作します。
ISAKMP	Internet Key Exchange Security Protocol。インターネットでセキュリティアソシエーション（SA）と暗号鍵を確立するプロトコル。
ISP	Internet service provider（インターネットサービスプロバイダ）。
MAC Address	Media-access-control address。ネットワークアダプタに割り当てられている固有の物理アドレス識別子。
MTU	Maximum transmission unit。通過可能な最も大きいパケットサイズ（バイト）。イーサネットの MTU は 1500 バイトのパケットです。
NAT	Network Address Translation。パケットがルータまたはファイアウォールを通過する際に IP アドレスを書き換える処理。NAT を使用すると、LAN 上のゲートウェイルータに割り当てられた単一のパブリック IP アドレスを使用して、LAN 上の複数ホストがインターネットにアクセスすることができます。
NetBIOS	ファイル共有、プリンタ共有、メッセージング、認証、および名前解決のためのマイクロソフトの Windows プロトコル。
NTP	Network Time Protocol。コントローラをネットワーク上のクロック（マスタークロック）と同期させるプロトコル。
PAP	Password Authentication Protocol。リモートアクセスサーバまたは ISP に対してユーザを認証するためのプロトコル。
PPPoE	Point-to-Point Protocol over Ethernet。ISP が IP アドレスの割り当てを管理することなくホストのネットワークを ISP に接続するためのプロトコル。
PPTP	Point-to-Point Tunneling Protocol。インターネット上のリモートクライアントからプライベートサーバまでの安全なデータ転送のために VPN を作成するプロトコル。
RADIUS	Remote Authentication Dial-In User Service。リモートユーザ認証とアカウンティングのためのプロトコル。ユーザ名とパスワードの集中管理を提供します。
RSA	Rivest-Shamir-Adleman。公開鍵 暗号化アルゴリズム。
SSID	Service Set Identifier。無線ネットワークに名前をつけるために使用する固有の識別子（英数字 32 文字以内。大文字、小文字の区別あり）。SSID は無線ネットワークを他の無線ネットワークと区別します。特定の無線ネットワークに接続しようとするすべてのアクセスポイントとデバイスは、有効なローミングを可能にするために、同じ SSID を使用する必要があります。
Subnet	一般的なアドレスコンポーネントを共有するネットワークの一部。TCP/IP ネットワークでは、サブネットは IP アドレスに同じプレフィックスを持つすべてのデバイスとして定義されます。例えば、100.100.100 から始まる IP アドレスを持つすべてのデバイスは同じサブネットに所属します。
TCP	Transmission Control Protocol。信頼性と送信順序が保証される、インターネットのデータ送信プロトコル。
UDP	User Data Protocol。信頼性と送信順序が保証されない、インターネットのデータ送信プロトコル。
VPN	Virtual private network。あるネットワークから別のネットワークへのすべてのトラフィックを暗号化することにより、IP トラフィックがパブリックな TCP/IP ネットワークを安全に通過することを可能にするネットワーク。IP レベルで全ての情報を暗号化するためにトンネリングを使用します。
WINS	Windows Internet Name Service。名前解決のためのサービス。異なる IP サブネットのクライアントがブロードキャストを送信せずに、ダイナミックにアドレスの解決、自身の登録、およびネットワークのブラウズを行うことができます。
無線コントローラ	個別に管理されたアクセスポイントを単一・統合されたソリューションに集約することで、無線 LAN のネットワーク管理を集中化および簡素化する D-Link デバイス。