

D-Link DWC-1000
Wireless Controller

ユーザマニュアル





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。

 警告	この表示を無視し、まちがった使いかたをすると、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、まちがった使いかたをすると、傷害または物損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。

警告

-  **分解・改造をしない**
機器が故障したり、異物が混入すると、やけどや火災の原因となります。
分解禁止
-  **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**
故障の原因につながります。
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、煙が出なくなつてから販売店に修理をご依頼してください。
禁止
-  **ぬれた手でさわらない**
感電のおそれがあります。
ぬれ手禁止
-  **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、または故障のおそれがあります。
水ぬれ禁止
-  **油煙、湯気、湿気、ほこりの多い場所、振動の激しいところでは使わない**
火災、感電、または故障のおそれがあります。
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、または故障のおそれがあります。
禁止
-  **表示以外の電圧で使用しない**
火災、感電、または故障のおそれがあります。
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。
禁止
-  **設置、移動のときは電源プラグを抜く**
火災、感電、または故障のおそれがあります。
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**
感電のおそれがあります。
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、または故障につながります。
禁止
-  **正しい電源ケーブル、コンセントを使用する**
火災、感電、または故障の原因となります。
禁止
-  **乳幼児の手の届く場所では使わない**
やけど、ケガ、または感電の原因になります。
禁止
-  **次のような場所では保管、使用をしない**
 - ・直射日光のあたる場所
 - ・高温になる場所
 - ・動作環境範囲外
禁止
-  **光源をのぞかない**
光ファイバケーブルの断面、コネクタ、および製品のコネクタ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

注意

-  **静電気注意**
コネクタや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。
-  **コードを持って抜かない**
コードを無理に曲げたり、引っ張りますと、コードや機器の破損の原因となります。
-  **振動が発生する場所では使用しない**
接触不良や動作不良の原因となります。
-  **付属品の使用は取扱説明書にしたがう**
付属品は取扱説明書にしたがい、他の製品には使用しないでください。機器の破損の原因になります。
禁止

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。

- 保守マーク表示を守ってください。また、ドキュメント類に説明されている以外の方法でのご使用はやめてください。三角形の中に稲妻マークがついたカバー類をあけたり外したりすると、感電の危険性を招きます。筐体の内部は、訓練を受けた保守技術員が取り扱うようにしてください。
- 以下のような状況に陥った場合は、電源ケーブルをコンセントから抜いて、部品の交換をするかサービス会社に連絡してください。
 - 電源ケーブル、延長ケーブル、またはプラグが破損した。
 - 製品の中に異物が入った。
 - 製品に水がかかった。
 - 製品が落下した、または損傷を受けた。
 - 操作方法に従って運用しているのに正しく動作しない。
- 本製品をラジエータや熱源の近くに置かないでください。また冷却用通気孔を塞がないようにしてください。
- 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。万一製品が濡れてしまった場合は、トラブルシューティングガイドの該当する文をお読みになるか、サービス会社に連絡してください。
- 本システムの開口部に物を差し込まないでください。内部コンポーネントのショートによる火事や感電を引き起こすことがあります。
- 本製品と一緒にその他のデバイスを使用する場合は、弊社の認定を受けたデバイスを使用してください。
- カバーを外す際、あるいは内部コンポーネントに触れる際は、製品の温度が十分に下がってから行ってください。
- 電気定格ラベル標記と合致したタイプの外部電源を使用してください。正しい外部電源タイプがわからない場合は、サービス会社、あるいはお近くの電力会社にお問い合わせください。
- システムの損傷を防ぐために、電源装置の電圧選択スイッチ（装備されている場合のみ）がご利用の地域の設定と合致しているか確認してください。
 - 東日本では 100V/50Hz、西日本では 100V/60Hz
- また、付属するデバイスが、ご使用になる地域の電気定格に合致しているか確認してください。
- 付属の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、本システムと周辺装置の電源ケーブルは、正しく接地された電気コンセントに接続してください。このケーブルには、正しく接地されるように、3 ピンプラグが取り付けられています。アダプタプラグを使用したり、ケーブルから接地ピンを取り外したりしないでください。延長コードを使用する必要がある場合は、正しく接地されたプラグが付いている 3 線式コードを使用してください。
- 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システムコンポーネントを保護するには、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。踏みつけられたりつまず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。
- 電源ケーブルやプラグを改造しないでください。設置場所の変更をする場合は、資格を持った電気技術者または電力会社にお問い合わせください。国または地方自治体の配線規則に必ず従ってください。
- 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ください。
- 製品の移動は気をつけて行ってください。キャストやスタビライザがしっかり装着されているか確認してください。急停止や、凹凸面上の移動は避けてください。

静電気障害を防止するために

静電気は、システム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、マイクロプロセッサなどの電子部品に触れる前に、身体から静電気を逃がしてください。シャーシの塗装されていない金属面に定期的に触れることにより、身体の静電気を逃がすことができます。

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. 静電気に敏感なコンポーネントを箱から取り出す時は、コンポーネントをシステムに取り付ける準備が完了するまで、コンポーネント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してください。
2. 静電気に敏感な部品を運ぶ場合、最初に静電気防止容器またはパッケージに入れてください。
3. 静電気に敏感なコンポーネントの取り扱い、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。

- 弊社製品を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、ご使用前にご確認ください。
<http://www.dlink-jp.com/>

目次

安全にお使いいただくために.....	2
ご使用上の注意.....	3
静電気障害を防止するために.....	4
電源の異常.....	4
はじめに.....	9
本マニュアルの対象者.....	10
表記規則について.....	10
第 1 章 本製品のご利用にあたって.....	11
はじめに.....	11
特長と利点.....	12
ポートについて.....	12
前面パネル.....	13
LED 表示.....	14
背面パネル.....	14
第 2 章 製品の設置.....	15
パッケージの内容.....	15
ネットワーク接続前の準備.....	15
設置位置の選択.....	15
設置時の注意.....	15
19 インチラックへの取り付け.....	16
ブラケットの取り付け.....	16
19 インチラックに本製品を取り付ける.....	16
無線コントローラの接続.....	17
電源の投入.....	17
第 3 章 Web ベース設定ユーティリティ.....	18
Web 管理インタフェースへのログイン.....	18
システム要件.....	18
ログイン前の準備.....	18
ログイン方法.....	18
Web 管理インタフェースの画面構成.....	21
標準の Web 管理インタフェース機能.....	22
第 4 章 主な基本設定.....	23
主な基本設定について.....	23
① DHCP サーバの有効化 (オプション).....	23
② 国コードの指定.....	24
③ 管理するアクセスポイントの選択と設定.....	25
④ SSID の変更とセキュリティの設定.....	27
⑤ MAC 認証の設定.....	32
⑥ 設定した AP プロファイルの確認.....	34
⑦ キャプティブポータルの設定.....	34
⑧ RADIUS サーバを持つ SSID をオーセンティケータ (認証 SSID) として使用する.....	42
⑨ ゲスト管理の設定.....	43
⑩ BYOD 環境の設定.....	50
ここから遷移すべき場所.....	57
第 5 章 高度な無線 LAN 設定.....	58
WLAN の一般的な設定.....	59
WLAN の基本設定.....	59
チャンネル計画と送信電力.....	61
チャンネル計画の設定.....	61
送信電力設定.....	63
WIDS 設定.....	64
AP WIDS の設定.....	64
クライアントの WIDS 設定.....	66
Distributed トンネル.....	68
Distributed トンネルの設定.....	68
WLAN 視覚化.....	69
画像のアップロード.....	69
起動.....	70

AP ディスカバリ方式	71
L2/VLAN ディスカバリ	71
L3/IP ディスカバリ	73
管理対象のアクセスポイント	74
Valid AP の追加	74
Discovered AP List からアクセスポイントを追加する	77
管理対象アクセスポイントのチャンネルと送信電力の手動変更	78
AP デバッグモードの設定	79
AP プロビジョニングの設定	80
AP プロファイル	82
AP プロファイルの設定	82
AP プロファイルの無線電波の設定	83
AP プロファイル SSID の設定	87
AP プロファイル QoS の設定	88
SSID プロファイル	90
SSID プロファイルの設定	90
WDS 設定	93
WDS Managed AP の設定	94
WDS Managed AP の設定	95
WDS AP リンクの設定	96
ピアグループ	97
ピアグループの設定	97
ピアグループの同期	98
AP ファームウェアのアップグレード	99
AP ファームウェアのダウンロード	99
AP ファームウェアの状態	101
第 6 章 高度なネットワーク設定	103
LAN 設定	103
IP モード設定	103
IPv4 LAN 設定	104
IPv6 LAN 設定	107
IPv6 アドレスプール	108
IPv6 ルータ通知	110
IPv6 通知のプレフィックス	111
LAN DHCP の予約 IP	112
IP/MAC バインディング	113
IGMP 設定	114
UPnP 設定	115
ジャンボフレームの設定	116
インターネット設定	117
Option1 設定	117
Option2/DMZ 設定	119
IPv6 ネットワークにおける Option 設定	120
Option Mode	121
ルーティング設定	125
IP エイリアス	126
DMZ LAN DHCP Reserved IPs (DMZ DHCP の予約 IP)	127
ダイナミック DNS の設定	128
VLAN 設定	129
VLAN の作成、設定	129
ポート VLAN	132
Advanced VLAN (高度な VLAN 設定)	134
ルーティング設定	139
IPv4 スタティックルーティングの設定	139
IPv6 スタティックルーティングの設定	140
ダイナミックルーティング (RIP)	141
OSPF 設定	142
OSPFv3 設定 (IPv6)	144
6to4 トンネル設定	145
ISATAP トンネル (IPv6)	146
プロトコルバインディング	147
QoS 設定	148
QoS 優先度	148
QoS モードの有効化	148
QoS ポリシー設定	153
CoS と DSCP マーキングの設定	157
トラフィックシェーピング (Option QoS)	158

第7章 ネットワークのセキュリティ設定	160
認証 (Authentication)	160
クライアントの管理 (User Database)	160
グループの管理	162
ユーザ管理	168
ゲストアカウントの使用の管理	171
ビリングプロファイル	172
ログインプロファイル	175
外部認証	180
Facebook Wi-Fi	188
Web コンテンツフィルタリング	189
スタティックフィルタリング	189
ファイアウォールの設定 (Firewall)	192
ファイアウォールルールの設定	192
ファイアウォールスケジュール設定	194
クライアントのブロック	195
カスタムサービスにおけるセキュリティ	196
ALG サポート	198
ファイアウォールのための VPN バススルー	200
ダイナミックポートフォワーディング	200
インターネット攻撃から保護する	202
第8章 VPN 設定	203
IPSec VPN (IPSec VPAN の設定)	203
Policies (IPSec VPN ポリシーの設定)	203
Tunnel Mode (トンネルモード)	207
DHCP Range (IP アドレス範囲の設定)	209
Certificate (認証証明書)	210
Easy VPN Setup (VPN セットアップ)	213
PPTP VPN (PPTP VPN 設定)	214
Server (PPTP VPN サーバ設定)	214
Client (PPTP クライアント)	215
L2TP VPN (L2TP VPN 設定)	216
Server (L2TP VPN サーバ設定)	216
SSL VPN (SSL VPN 設定)	218
SSL VPN Server Policy (SSL VPN ポリシー設定)	218
ポータルレイアウトの作成	220
ネットワークリソース	221
SSL VPN クライアント設定	224
OpenVPN サポート	226
OpenVPN 設定	226
Local Networks 設定	227
Remote Networks 設定	228
Authentication 設定	229
第8章 ステータスおよび統計情報	230
統計情報と利用率の参照	231
ダッシュボードの管理	232
システム状態の参照	235
機器状態の参照	235
USB 情報の参照	236
ネットワーク情報の参照	237
DHCP クライアントの参照	237
キャプティブポータルセッションの参照	238
アクティブセッションの参照	238
VPN セッションの参照	239
インタフェースのトラフィックの参照	240
無線情報の参照	241
コントローラの状態と統計情報の参照	241
アクセスポイント情報の参照	245
接続クライアントの参照	266
クラスタ情報の参照	278
WDS グループ状態	279
WDS グループのアクセスポイントの状態	280

第9章 メンテナンス	284
システム設定 (Administration)	284
システム名の設定	284
システムの日付と時間の設定	285
ログインセッションタイムアウトの設定	286
USB 共有ポートの設定	286
ライセンスのアクティブ化	287
管理設定 (Management)	288
リモート管理	288
省エネ設定	289
SNMP の使用	290
ファームウェア (Firmware)	298
コンフィグレーションの保存と復元	298
コンフィグレーションの復元	299
工場出荷時設定の復元	300
無線コントローラの再起動	301
ファームウェアのアップグレード	302
コマンドラインインタフェースの使用	304
第10章 トラブルシューティング	305
LED トラブルシューティング	305
Power LED が消灯	305
LAN ポート LED が消灯	305
Web 管理インタフェース	305
リセットボタンを使用した、工場出荷時設定の復元	306
日付と時間に関する問題	306
アクセスポイントに関するディスカバリ問題	306
接続問題	306
ネットワークの性能と不正アクセスポイントの検出	307
無線コントローラにおける診断ツールの使用	307
IP アドレスの Ping	307
Traceroute の使用	308
DNS 検索の実行	309
ログパケットのキャプチャ	310
システムチェックの実施	312
ログ設定	313
ログ出力の定義	313
トラフィックの追跡 / ルーティングログ	314
Syslog ログ	314
リモートログ	315
Syslog サーバ構成	316
イベントログ	317
現在のログ	318
WLAN ログ	318
Firewall ログ	319
IPSec VPN ログ	319
SSL VPN ログ	320
WCF ログ	320
Captive Portal ログ	321
付録 A 基本計画のワークシート	322
付録 B 工場出荷時設定	324
付録 C 用語解説	324

はじめに

本ユーザマニュアルは、本製品のインストールおよび操作方法を例題と共に記述しています。

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 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

- 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 VPN 設定

- リモートクライアント間の安全な通信のための VPN 機能について説明します。

第9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10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11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

字体・記号	解説	例
「」	メニュータイトル、ページ名、ボタン名。	「Submit」 ボタンをクリックして設定を確定してください。
青字	参照先。	" ご使用になる前に " (13 ページ) をご参照ください。
courier フォント	CLI 出力文字、ファイル名。	(switch-prompt)#
courier 太字	コマンド、ユーザによるコマンドライン入力。	show network
courier 斜体	コマンド項目 (可変または固定)。	value
< >	可変項目。< > にあたる箇所に値または文字を入力します。	<value>
[]	任意の固定項目。	[value]
[< >]	任意の可変項目。	[<value>]
{ }	{ } 内の選択肢から 1 つ選択して入力する項目。	{choice1 choice2}
(垂直線)	相互排他的な項目。	choice1 choice2
Menu Name > Menu Option	メニュー構造を示します。	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。

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

D-Link 無線コントローラ (D-Link Wireless Controller: DWC) DWC-1000 は、小規模のネットワーク環境用に設計された機能をフルに搭載した無線 LAN コントローラです。集中制御機能には、自動チャンネル、および電力調整など様々なアクセスポイント管理機能があります。高度な無線セキュリティ機能は、不正 AP 検知、キャプティブポータル、無線侵入検知システム (Wireless Intrusion Detection System : WIDS) を含んでおり、ハッカーから攻撃を回避する強力な無線ネットワーク保護を提供します。ライセンスのアップグレードを行うと、VPN (Virtual Private Network) トンネル、IPSec (IP Security)、PPTP (Point-to-Point Tunneling Protocol)、L2TP (Layer 2 Tunneling Protocol)、および SSL (Secure Sockets Layer) などの機能を通じて最適なネットワークセキュリティを提供します。SSL VPN トンネルを使用して、いつでもどこでもクライアントレスリモートアクセスにより Road Warrior (モバイル接続) を行うことができます。

DWC に増強された機能性をアクティブ化するのに利用可能なライセンスには 3 つのタイプがあります。これらのライセンスは初期値ではアクティブ化されていません。

- 1. VPN ライセンス** - アップグレードにより、以下の機能が有効となります。:
ISP 接続タイプ (PPPoE、PPTP、L2TP、NAT/ 透過モード)、オプション 2/DMZ ポート、IP エイリアシング、ダイナミックルーティング (RIP)、VPN (PPTP/L2TP/SSL VPN)、ダイナミック DNS、URL フィルタ、アプリケーションルール、ファイアウォールルール、および ALG/SMTP-ALG
- 2. AP ライセンス** - 本ライセンスにより、管理可能な AP コントローラ数が増えます。
初期値では DWC-1000 は最大 6 台の AP を管理できます。AP ライセンスアップグレードごとに 6 台まで増やすことができ、最大 24 台まで管理できます。
- 3. WCF ライセンス** - 本ライセンスにより、ダイナミックでパワフルな Web フィルタリング機能を、様々な場面で使用することが可能です。これらは従業員のオンライン閲覧状況を確認する企業や、生徒の好ましくないコンテンツ閲覧の制限を行う学校、特定の場所からのアクセスを制限したい小企業や個人商店などにとって有効な機能です。性的なサイトやギャンブル、オンラインショッピングなど 32 カテゴリの Web サイトを制限することが可能です。そして数クリックでカテゴリのブロック/ブロック解除を実行することができます。ダイナミック WCF はまたログ機能でもあり、ユーザによるブロックされているサイトへのアクセスや、ログイン/ログアウトの日時など、対応するイベントがログとして保存されます。

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検出と設定
- 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

コンフィグレーションプロファイルを使用して設定を行います。コンフィグレーションプロファイルにより、無線コントローラは、そのプロファイルに関連するアクセスポイントに無線電波、SSID、QoS パラメータを配布します。

無線コントローラは、1 つの定義済みプロファイルを持ちます。このプロファイルをそのまま使用するか、要求に合うようにそれを編集するか、または必要に応じて新しいコンフィグレーションプロファイルを作成することができます。

例:

- あるオフィスビルでは、(一般的な作業エリアなどの) ファシリティのあるエリアに位置するアクセスポイントに 1 つのコンフィグレーションプロファイル、またそのファシリティの別のエリア (例: 人事部) にあるアクセスポイントに、それとは別のプロファイルを持つことができます。
- 複数のビジネスが WLAN を共有するが、各ビジネスは自身のネットワークを持つ場合、ショッピングモールには複数のコンフィグレーションプロファイルが必要となります。
- ビルや部署ごとに異なるポリシーを必要とする大規模ネットワークでは、ビルや部署のセキュリティポリシー用に設定されたアクセスポイントを持つことができます。(例: ゲスト用、管理用、販売用など)

特長と利点

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が可能です。

基本スペック

- ・追加ライセンスなしで、1つの無線コントローラは最大6個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24個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-1000-AP6-LIC) があります。
- ・IEEE 802.11a、802.11b、802.11g、802.11n、および 802.11ac 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、クラス分け。
- ・キャプティブポータル認証、ゲスト管理。
- ・ライセンスパック「DWC-1000-VPN」を購入すると、「VPN」「ルータ」「ファイアウォール」が二つのギガビットオプションポートでご使用になれます。
- ・ライセンスパック「DWC-1000-WCF」を購入すると、安全で安定のネットワークと学習環境が維持できる「ダイナミック Web コンテンツフィルタ」が一年間有効になります。本ライセンスの適用前に、VPN ライセンス「DWC-1000-VPN」を購入、適用する必要があります。

サイトの調査が完了した後に、収集したデータを使用して、[322 ページの「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。

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-1000
10BASE-T/100BASE-TX/1000BASE-T ポート	WAN x 2、LAN x 4 (10/100/1000 Mbps)
RJ-45 コンソールポート	1
USB ポート	2

前面パネル

本製品の前面パネルには、ステータスを表示する Power/ ステータス LED、USB ポート / LED、および LAN/Option ポート / LED が配置されています。

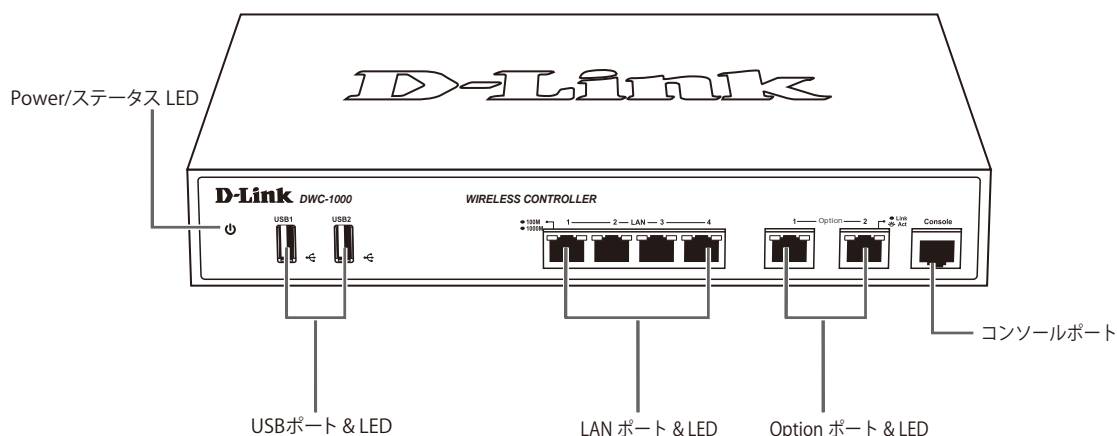


図 1-1 前面パネル図

前面パネルの各機能は以下の通りです。

機能	説明
Power/ ステータス LED	本無線コントローラの状態を示します。製品の電源をオンにした場合、電源が起動中、Power / ステータス LED は橙色に点灯します。起動には 1 分ほどかかり、起動が完了すると機能 LED は緑色の点灯に変わります。電源をオフにして再度オンにする場合には、オフの後に数秒待ってからオンにすることをお勧めします。
USB ポート / LED	以下の様々な USB2.0 のデバイスをサポートすることができます。USB デバイスを接続し、認識されると緑色に点灯します。: <ul style="list-style-type: none"> ネットワーク共有のためのフラッシュディスク、またはハードディスク プリンタ
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。
Option ポート (1-2)	バックボーンなどに接続 (別途 DWC-1000-VPN ライセンスが必要) するためのギガビットイーサネットポートです。各ポートに動作 LED (左) とリンク LED (右) があります。
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) にアクセスするのに使用します。

LED 表示

本製品は、Power / ステータス、および Option / LAN ポートについて LED をサポートしています。Option / LAN ポートの LED は以下の通り、リンクスピードと TX/RX ステータスがあります。

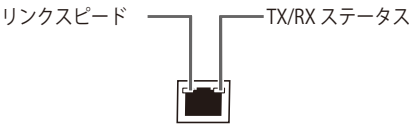


図 1-2 Option/LAN LED 図

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	製品の電源を立ち上げ中です。
	点滅	橙	デバイスはクラッシュして、リカバリモード中です。
	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	システムに欠陥があり、ファームウェアのアップグレードに失敗しました。
	消灯	—	製品に電源が供給されていません。
Option / 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	—	ポートは 10Mbps で動作中です。
Option / 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	—	リンクが確立していません。
USB	点灯	緑	USB デバイスが接続しています。
	点滅		データを送受信しています。
	消灯	—	USB デバイスが接続していません。

背面パネル

本製品の背面パネルには、リセットボタン、電源スイッチ、および電源コネクタが配置されています。

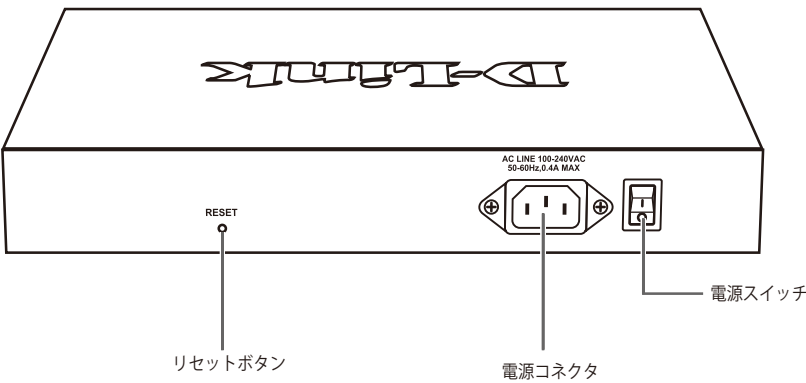


図 1-3 背面パネル図

背面パネル機能

部位	機能
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。
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。

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
- ・ PL シート
- ・ 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

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、弊社ホームページにてユーザ登録を行い、サポート窓口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。
- ・ アクセスポイントからクライアントへの接続性テストを実行して、クライアントで達成可能な最大スループットを決定します。

サイトの調査が完了した後に、収集したデータを使用して、[322 ページの「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、無線コントローラ的位置を選択します。以下のガイドラインに従って本製品を設置してください。

- ・ 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は少なくとも 91.4cm を以上の空間を保つようにする。
- ・ 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をつくの防止します。

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

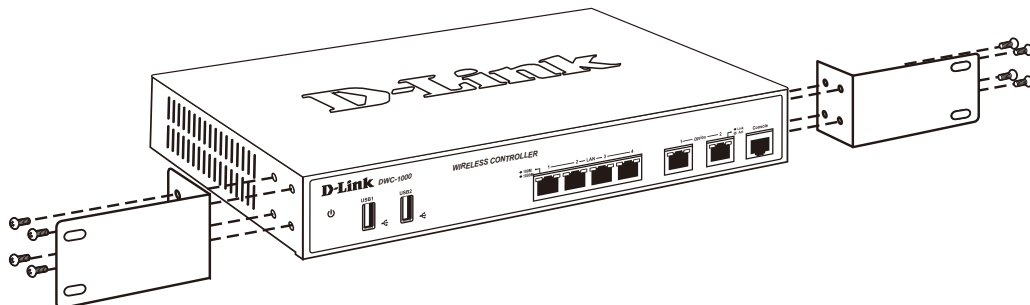


図 2-1 ブラケットの取り付け

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ずに製品を設置すると、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。

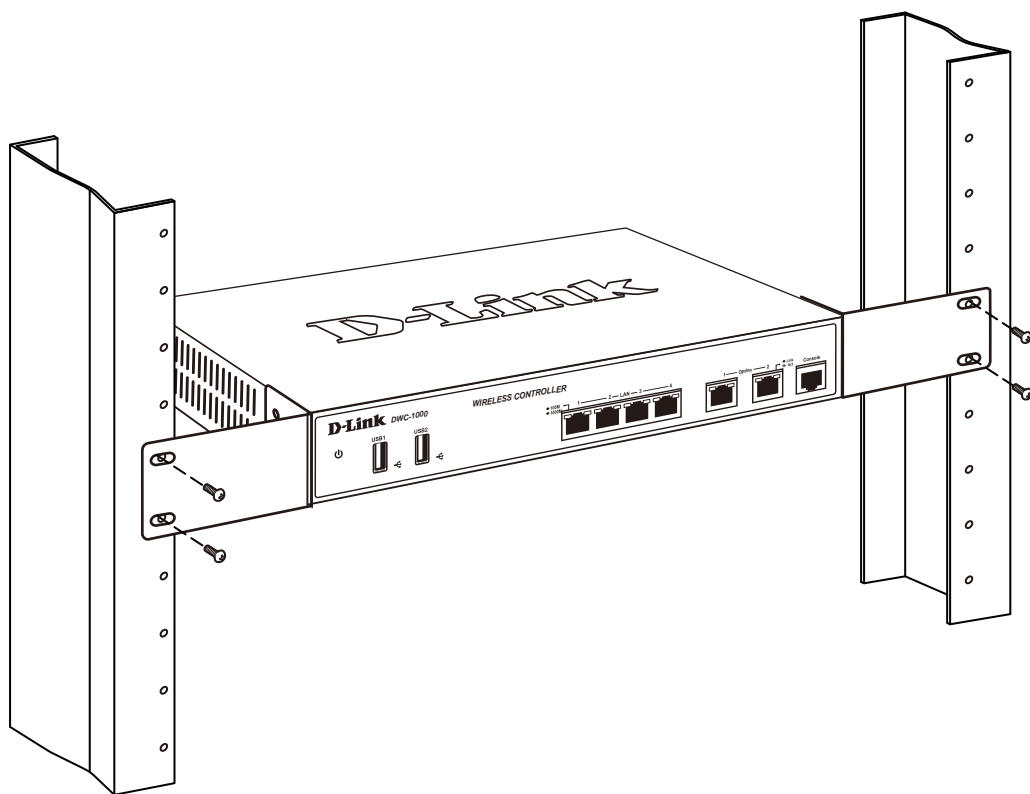


図 2-2 製品のラックへの設置

無線コントローラの接続

1. コントローラ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。

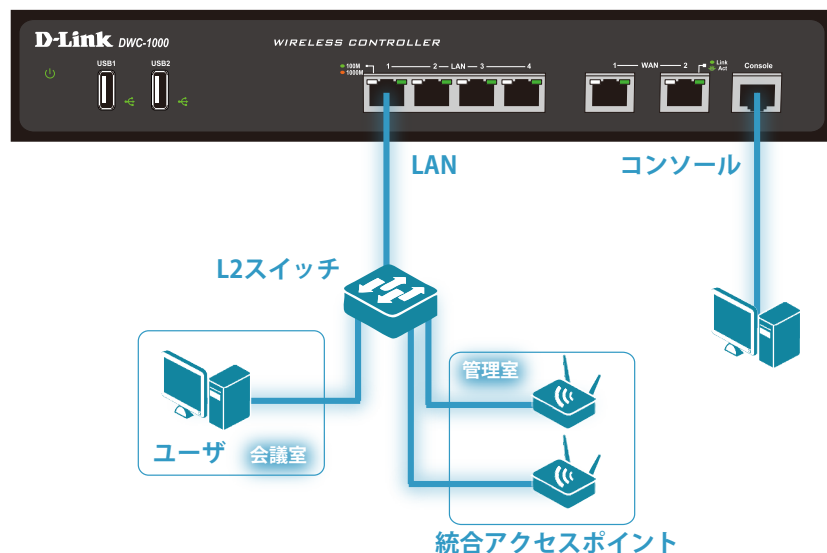


図 2-4 製品接続図

4. 「VPN/ ファイアウォール/ルータ」ライセンスパックを購入済みの場合、以下の内容に従い、「Option1」「Option2」ポートを使用します。:
 - Option1 = ケーブル /DSL モデムに接続する WAN ポート
 - Option2 = デュアル WAN 接続や内部サーバ専用の「WAN」または「DMZ」ポート
5. 「DMZ ポート」として使用する場合、ポートの IP アドレスは無線コントローラの IP アドレスとは違うものにする必要があります。

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
- 標準の Web 管理インタフェース機能

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。

本セクションの情報を使用すると、短い時間で基本情報の実行や無線コントローラの起動が行えます。

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 9.0 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

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。(99 ページの「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。ここでは、Windows 7 で動作する画面で説明します。手順と画面は、他の Windows OS についても同じです。

1. 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を注意してください。

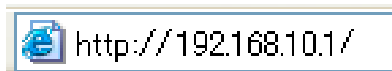
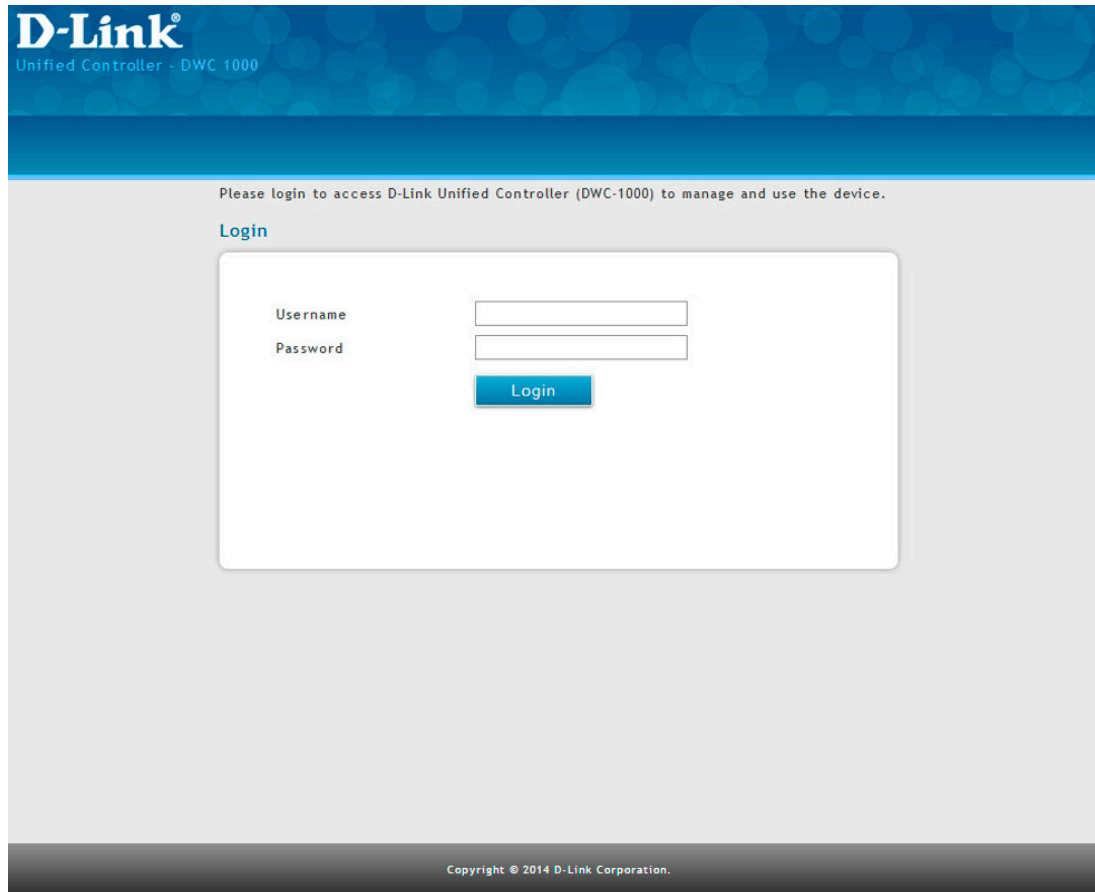


図 3-1 アドレス入力画面

注意 ログインプロンプトが表示されない場合、305 ページの「第 10 章 トラブルシューティング」の「Web 管理インタフェース」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。



The image shows the login interface of the D-Link Unified Controller (DWC-1000). At the top, there is a blue header with the D-Link logo and the text 'Unified Controller - DWC 1000'. Below the header, a message reads: 'Please login to access D-Link Unified Controller (DWC-1000) to manage and use the device.' Underneath this message is the word 'Login' in blue. The main part of the screen is a light gray area containing a white login box. Inside this box, there are two input fields: 'Username' and 'Password'. Below these fields is a blue 'Login' button. At the bottom of the page, there is a dark gray footer with the text 'Copyright © 2014 D-Link Corporation.'

図 3-2 Login 画面

6. 「Username」および「Password」に「admin」と入力して、「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。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（[150 ページの「ユーザの編集」](#)参照）、[322 ページの「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。

- 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. ログインに成功すると以下の画面が表示されます。

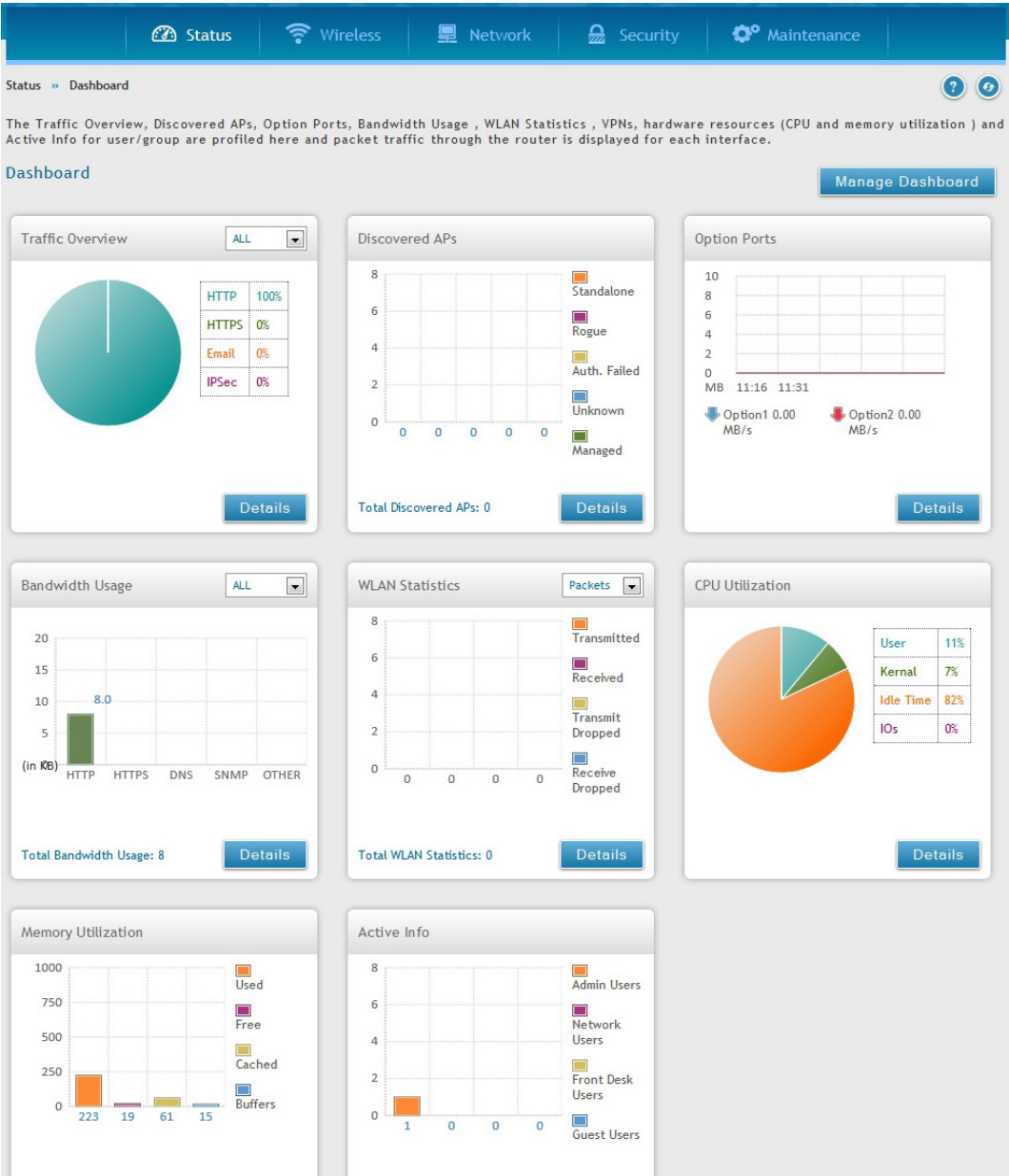


図 3-3 Dashboard 画面

ここでは、一般的な状態情報、LAN/WLAN の状態情報を表示します。**Status > Dashboard** をクリックすることで、本画面を表示できます。

8. 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。
9. Web 管理インター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。

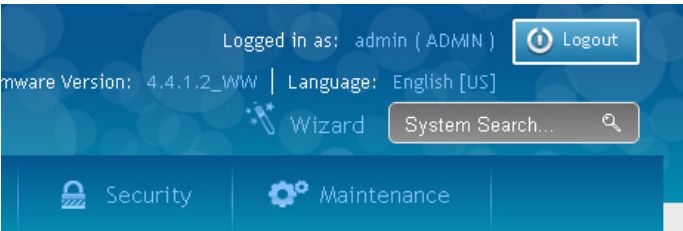


図 3-4 Logout アイコン

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、以下のコンポーネントがあります。

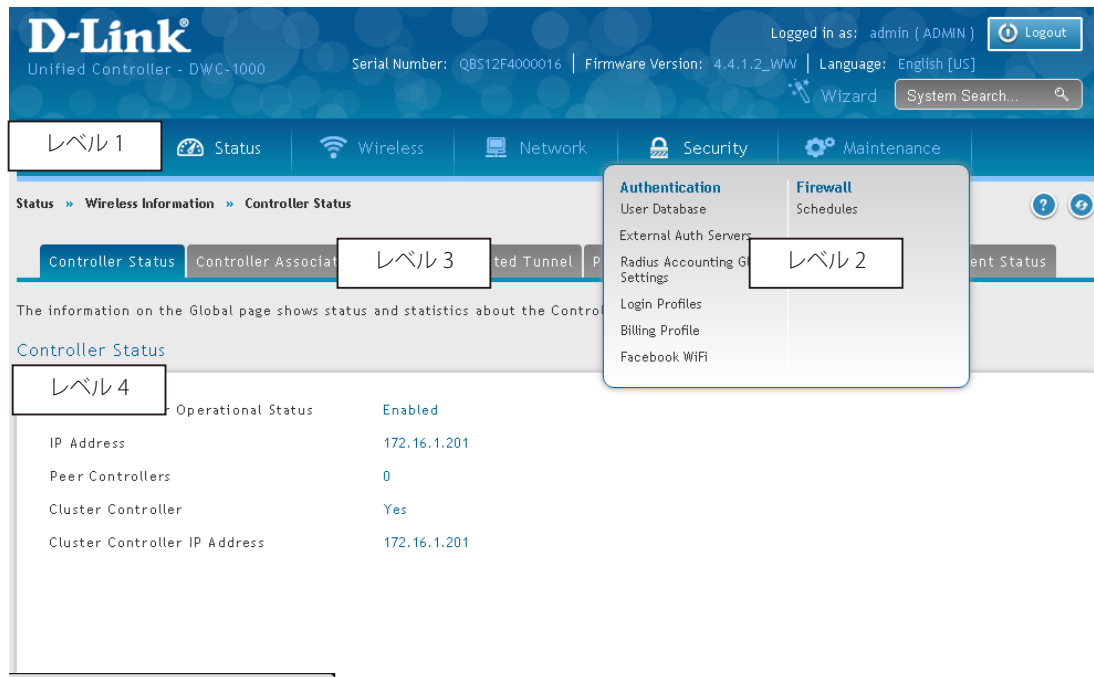


図 3-5 メニュー構成

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にマウスを移動すると、プルダウンメニューに現れます。
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。

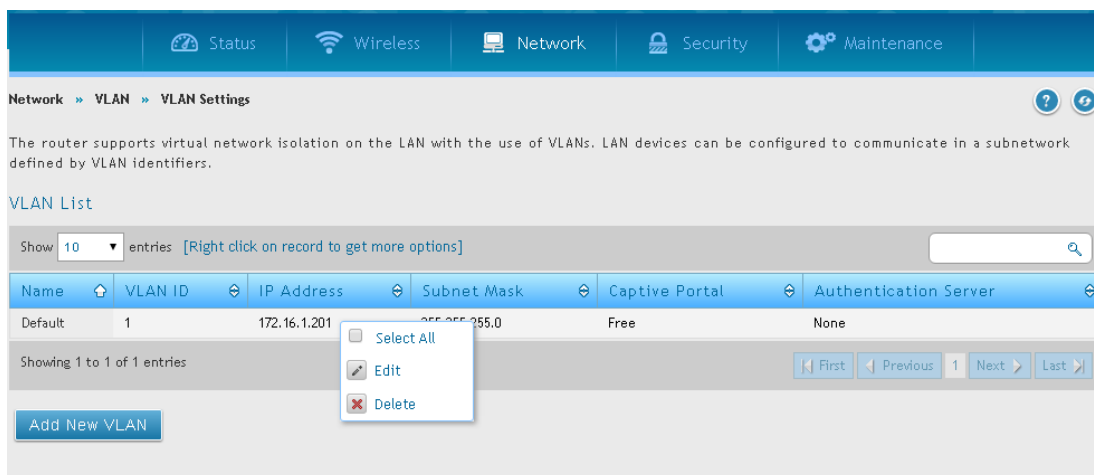



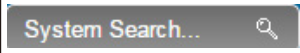
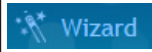


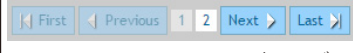


図 3-6 アクションボタンの例

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により、既存の項目に加え、さらに多くのアクションを可能にします。 <ul style="list-style-type: none">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 - 発見したアクセスポイントを管理します。View Information - 項目によって各種の情報がります。

標準の Web 管理インタフェース機能

Web 管理インタフェースにはいくつかの標準的な機能があります。

項目	説明
 ヘルプ機能	様々な機能やインタフェースの設定のための説明があります。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。これは画面の右上隅にあります。
	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。
 Wizard 機能	デバイスの設定、インターネットへの接続、有線 / 無線ネットワークの設定、セキュリティオプションの設定、新規ユーザの作成など、一般的なコンフィグレーションタスクに非常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。
Status » System Information » Device 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。
Show 10 entries	ページ内のテーブルの項目数を表示します。システムは 1 ページに 10、25、50、100 のエントリを表示できます。
 First/ Previous/ Next/Last (テーブル上)	情報は複数のページの場合に表示されます。First/ Previous/ Next/ Last 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、テーブルの右上隅にあります。
 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。

第4章 主な基本設定

本セクションでは、コントローラをインストール後に実行する主な基本設定について説明します。

主な基本設定について

以下に一般的な基本設定について記載します。番号順に従って設定していくと、本コントローラの基本的な設定は完了します。その他、各セクションの詳細設定については、各セクションの説明を参照ください。

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

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て、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** の順にメニューをクリックし、以下の画面を表示します。

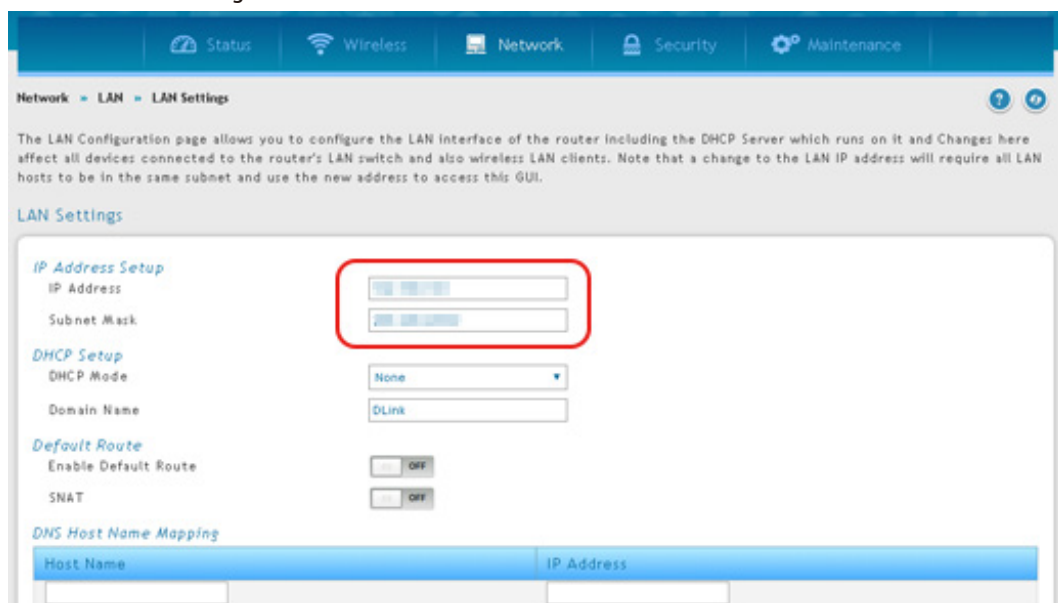


図 4-1 LAN Settings 画面

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。
3. 「Save」ボタンをクリックして、設定を保存します。
4. 一旦 WebGUI 画面が消えます。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** 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。以下「DHCP Setup」内を指定し、DHCP サーバとしての概要を設定します。

項目	説明
DHCP Setup	
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	割り当てられる 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。

② 国コードの指定

各国には、無線電波を使用するための規則があります。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。

③ 管理するアクセスポイントの選択と設定

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発見します。以下の手順を使用して、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 > Discovered AP 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。

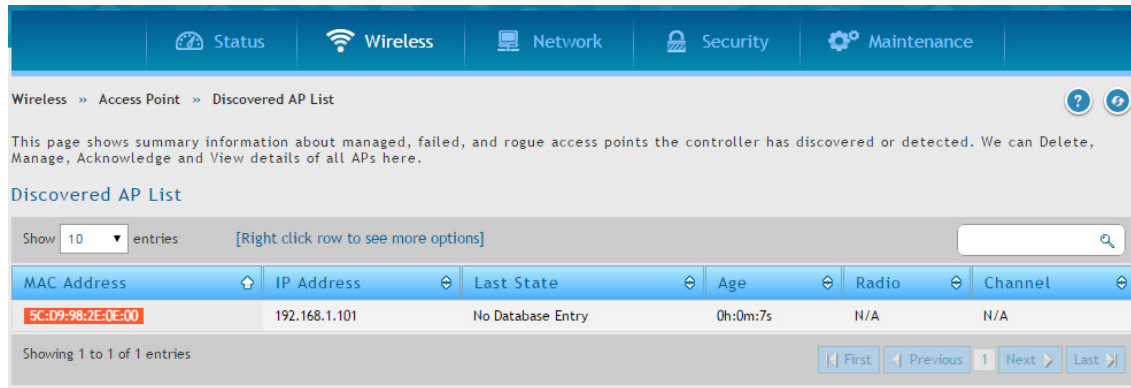


図 4-3 Discovered AP List 画面

無線コントローラが発見したアクセスポイントのリストを表示します。

2. 「Discovered 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。

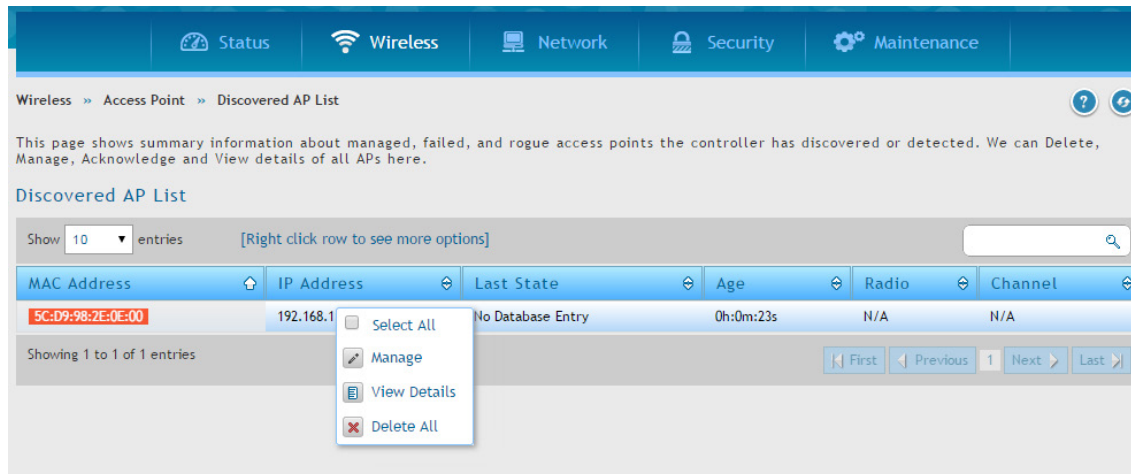


図 4-4 Discovered AP List 画面（右クリックメニュー）

以下の画面が表示されます。

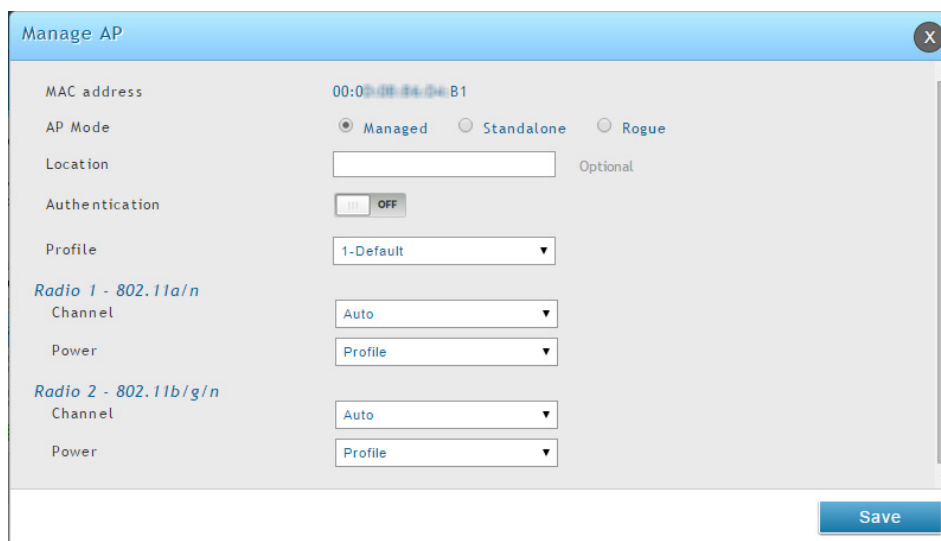


図 4-5 Manage AP 画面

主な基本設定

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。
AP Mode	「Managed」、「Standalone」、または「Rogue」を選択します。 <ul style="list-style-type: none">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。Standalone - これを選択すると、続く「Location」から「Expected Wired Network Mode」までのフィールドを入力する必要があります。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。
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「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。
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 を表示します。(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表示します。(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 のモードを表示します。(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表示します。(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表示します。(参照用)

4. 無線コントローラに管理させる追加のアクセスポイントのそれぞれに対して手順 2 と 3 を繰り返します。

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。

Wireless > Access Point > AP Profiles > AP Profile SSID

AP Profiles | AP Profile Radio | **AP Profile SSID** | AP Profile QoS

This page displays the virtual access point (VAP) settings associated with the selected AP profile. Each VAP is identified by its network number and Service Set Identifier (SSID). We can configure and enable up to 16 VAPs per radio on each physical access point.

Access Point Profiles SSID List

AP Profile: 1-Default

Radio Mode: ☒ 802.11a/n/ac ☐ 802.11b/g/n

Show 10 entries [Right click on record to get more options]

SSID Name	SSID Status	VLAN	Hide SSID	Security	Redirect	Captive Portal
1-dlink1	Enabled	1-Default	Disabled	None	None	Free
2-dlink2	Disabled	1-Default	Disabled	None	None	Free
3-dlink3	Disabled	1-Default	Disabled	None	None	Free
4-dlink4	Disabled	1-Default	Disabled	None	None	Free
5-dlink5	Disabled	1-Default	Disabled	None	None	Free
6-dlink6	Disabled	1-Default	Disabled	None	None	Free
7-dlink7	Disabled	1-Default	Disabled	None	None	Free
8-dlink8	Disabled	1-Default	Disabled	None	None	Free
9-dlink9	Disabled	1-Default	Disabled	None	None	Free
10-dlink10	Disabled	1-Default	Disabled	None	None	Free

Showing 1 to 10 of 16 entries

First Previous 1 2 Next Last

図 4-6 AP Profile SSID 画面

無線コントローラに設定済みの無線ネットワークのリストと共に表示されます。

2. 編集する「SSID Name」の横のパラメータを右クリックして、「Edit」を選択し、以下の画面を表示します。

The screenshot shows the 'SSID Configuration' window. The 'SSID' field contains 'dlink1'. The 'VLAN' field contains '1'. The 'Security' field is set to 'None'. The 'Save' button is at the bottom right.

図 4-7 SSID Configuration 画面

3. 「SSID Configuration」画面で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全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 設定に作成済みであることを確認してください。（ 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。 <ul style="list-style-type: none">• None - どのセキュリティメカニズムも使用しません。• WEP - WEP セキュリティを有効にします。表示されるオプションも指定します。• WPA/WPA2 - WPA/WPA2 セキュリティを有効にします。表示されるオプションも指定します。

注意 本項目では AP プロファイルに適用する SSID プロファイルのセキュリティ設定について説明しています。各 SSID プロファイルの詳細設定につきましては「[SSID プロファイル](#)」を参照ください。

SSID 設定 (WEP)

The screenshot shows the 'SSID Configuration' window with the 'Security' field set to 'WEP'. The 'Authentication' section is expanded, showing options for 'Open System', 'Shared Key', 'WEP Key Type' (ASCII, HEX), 'WEP Key Length' (64, 128), and 'WEP Keys' (1, 2, 3, 4). The 'Save' button is at the bottom right.

図 4-8 SSID Configuration 画面 (WEP)

表 4-1 WEP の設定オプション

項目	説明
Security	<ul style="list-style-type: none"> 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	<p>認証タイプを選択します。</p> <ul style="list-style-type: none"> Open System - どの無線ステーションも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どう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	<p>キータイプを選択します。</p> <ul style="list-style-type: none"> 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)	<p>WEP キーの長さを選択します。</p> <ul style="list-style-type: none"> 64 - 64 ビット 128 - 128 ビット
WEP Keys	<p>Tx: 送信キーのインデックスです。</p> <p>AP がどの WEP キーを使用してデータを送信するのかを示しています。</p> <p>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、キーを入力するところのキー番号のラジオボタンをクリックします。</p> <p>続いて、WEP キーを入力します。</p>
WEP キーの入力	<p>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。</p> <ul style="list-style-type: none"> 64 bit - ASCII: 5 文字、Hex: 10 文字 128 bit - ASCII: 13 文字、Hex: 26 文字 <p>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 キーから 1 つを使用するように設定されます。</p>

SSID 設定 (WPA/WPA2)

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

表 4-2 WPA/WPA2 設定オプション

項目	説明
Security	<p>「Security」に「WPA」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。</p> <ul style="list-style-type: none"> 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。

項目	説明
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。 <ul style="list-style-type: none"> 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 標準で最も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行えます。ただし、WPA2 サポートのクライアントに対しては、多少セキュリティは高くなります。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。 <ul style="list-style-type: none"> 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のに、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。
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。
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ことを想定して、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。
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 > SSID 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。

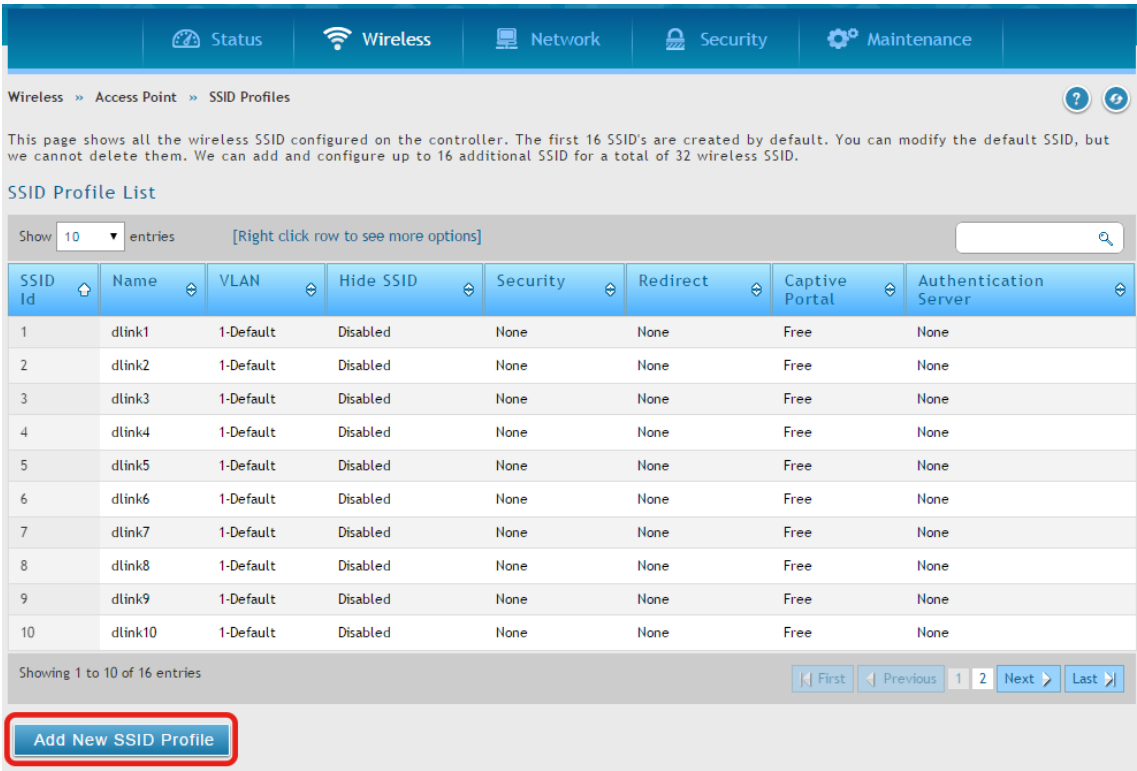
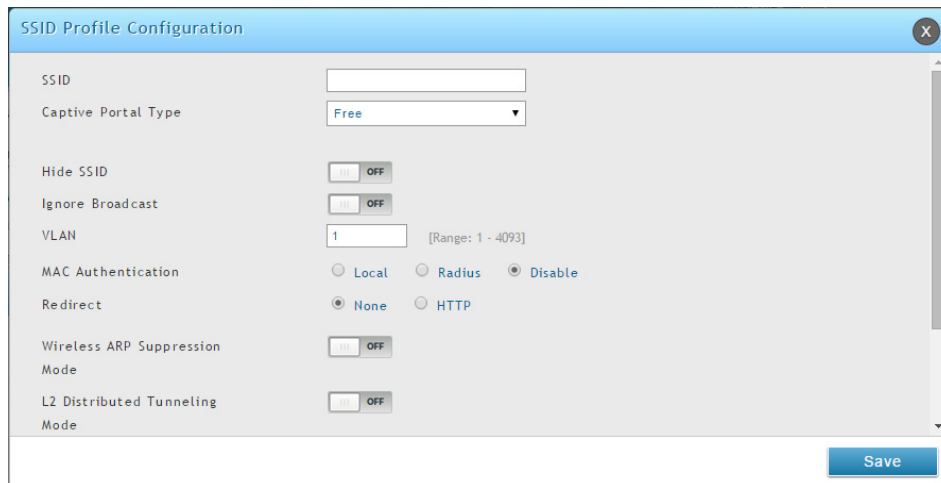


図 4-10 SSID Profile List 画面

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。



SSID Profile Configuration dialog box showing various settings:

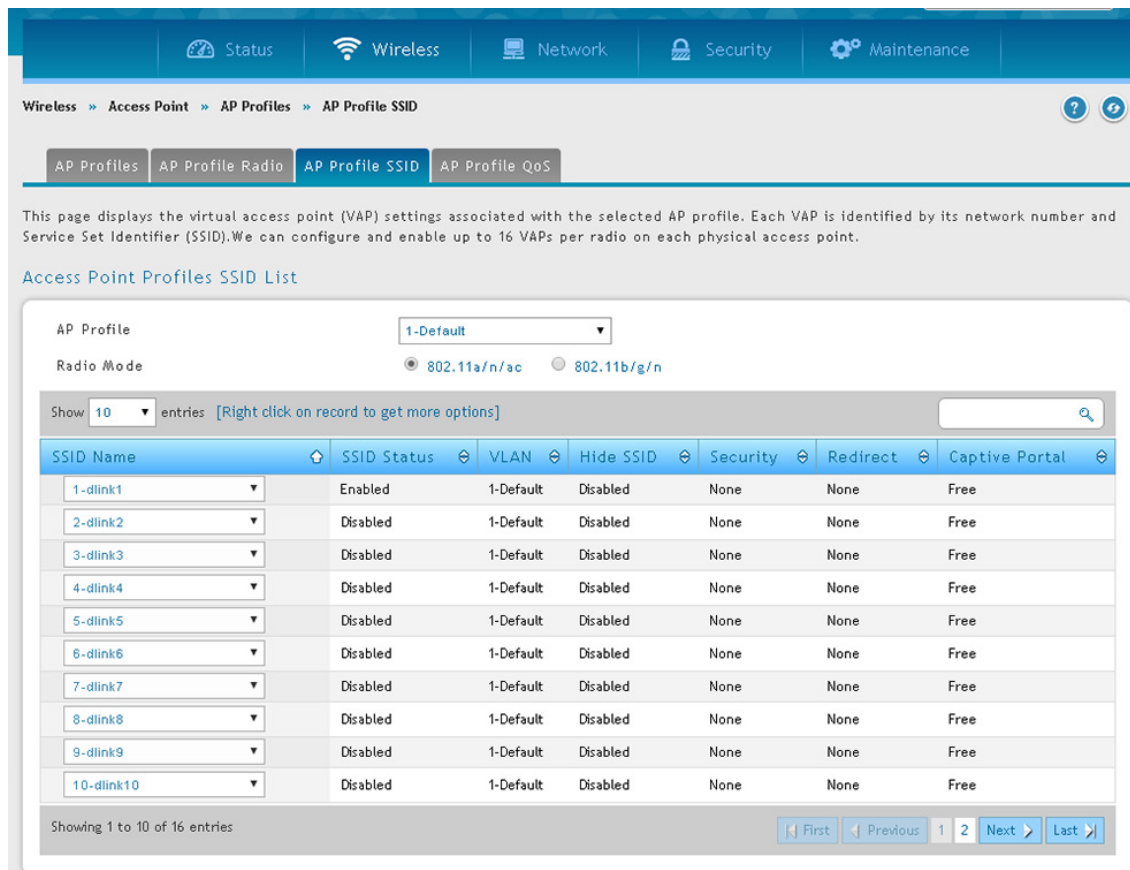
- SSID: [Empty text box]
- Captive Portal Type: Free (dropdown)
- Hide SSID: OFF (checkbox)
- Ignore Broadcast: OFF (checkbox)
- VLAN: 1 (text box, Range: 1 - 4093)
- MAC Authentication: Local (radio), Radius (radio), Disable (radio, selected)
- Redirect: None (radio, selected), HTTP (radio)
- Wireless ARP Suppression Mode: OFF (checkbox)
- L2 Distributed Tunneling Mode: OFF (checkbox)
- Save button

図 4-11 SSID Profile Configuration 画面

6. フィールドを入力後、「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。

注意 各 SSID プロファイルの詳細設定につきましては「[SSID プロファイル](#)」を参照ください。

7. Wireless > Access Point > AP Profiles > 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。



AP Profile SSID configuration page showing the following elements:

- Navigation tabs: AP Profiles, AP Profile Radio, **AP Profile SSID**, AP Profile QoS
- Text: This page displays the virtual access point (VAP) settings associated with the selected AP profile. Each VAP is identified by its network number and Service Set Identifier (SSID). We can configure and enable up to 16 VAPs per radio on each physical access point.
- Section: Access Point Profiles SSID List
- AP Profile: 1-Default (dropdown)
- Radio Mode: 802.11a/n/ac (radio, selected), 802.11b/g/n (radio)
- Show: 10 entries [Right click on record to get more options]
- Table with columns: SSID Name, SSID Status, VLAN, Hide SSID, Security, Redirect, Captive Portal
- Table data (10 rows):

SSID Name	SSID Status	VLAN	Hide SSID	Security	Redirect	Captive Portal
1-dlink1	Enabled	1-Default	Disabled	None	None	Free
2-dlink2	Disabled	1-Default	Disabled	None	None	Free
3-dlink3	Disabled	1-Default	Disabled	None	None	Free
4-dlink4	Disabled	1-Default	Disabled	None	None	Free
5-dlink5	Disabled	1-Default	Disabled	None	None	Free
6-dlink6	Disabled	1-Default	Disabled	None	None	Free
7-dlink7	Disabled	1-Default	Disabled	None	None	Free
8-dlink8	Disabled	1-Default	Disabled	None	None	Free
9-dlink9	Disabled	1-Default	Disabled	None	None	Free
10-dlink10	Disabled	1-Default	Disabled	None	None	Free
- Showing 1 to 10 of 16 entries
- Navigation buttons: First, Previous, 1, 2, Next, Last

図 4-12 AP Profile SSID 画面

8. 「AP Profile」プルダウンメニューから編集する「SSID」を選択します。
9. 希望する「Radio Mode」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。「SSID ID1」を有効にしない場合、新しい SSID を作成し「SSID ID1」として登録する必要があります。

⑤ MAC 認証の設定

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に有益です。また、802.1X セキュリティ方式にも関連付けて使用できます。その場合、802.1X 認証より前に行われます。MAC 認証を有効にすると、無線クライアントがネットワークに接続するためには、はじめに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 サーバに記載されている 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 アドレスがないと、アクセスポイントはクライアントへのアクセスを拒否されます。
- Black-list:
「MAC Authentication」データベースまたは RADIUS サーバに記載されている 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 アドレスがないと、アクセスポイントはクライアントへのアクセスを許可されます。

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。

Wireless >> General

This page will guide you through common and easy steps to configure your DWC-1000 router WLAN global settings. Make sure that WLAN controller is being enabled for working of wireless functionality.

General Setting

WLAN Global Setup

WLAN Controller Operational Status: ☒ ON ☐ OFF

IP Address: 192.168.10.1

Peer Group ID: 1 [Default: 1, Range: 1 - 255]

Client Roam Timeout: 30 [Range: 1 - 120] Seconds

Ad Hoc Client Status Timeout: 24 [Range: 0 - 168] Hours

AP Failure Status Timeout: 24 [Range: 0 - 168] Hours

Client MAC Authentication Mode: ☒ White-list ☐ Black-list

RF Scan Status Timeout: 24 [Range: 0 - 168] Hours

Detected Clients Status Timeout: 24 [Range: 0 - 168] Hours

Tunnel IP MTU Size: ☒ 1500 ☐ 1520

Cluster Priority: 1 [Range: 0 - 255]

AP Client QoS: ☐ ON ☒ OFF

Radius Authentication Server: Default-RADIUS-Server

Radius Authentication Server Status: Configured

Radius Accounting Server: Default-RADIUS-Server

Radius Accounting Server Status: Configured

Global Accounting Mode: ☐ ON ☒ OFF

AP Validation

AP MAC Validation: ☒ Local ☐ Radius

Require Authentication Passphrase: ☐ ON ☒ OFF

Manage AP with Previous Release Code: ☐ ON ☒ OFF

Country Configuration

Country Code: US - United States

Save Cancel

図 4-13 General Setting 画面

2. 「Client MAC Authentication Mode」で、「Black-list」または「White-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。

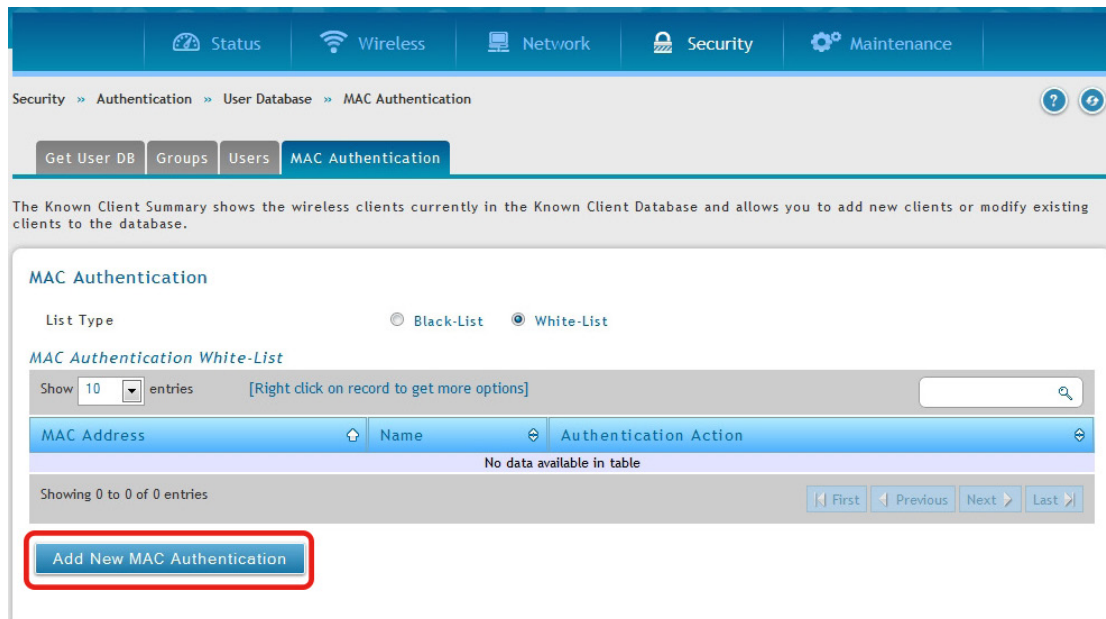


図 4-14 MAC Authentication 画面

手順 2 で選択したリストタイプ (Black-list または White-list) に従って画面を表示します。

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。

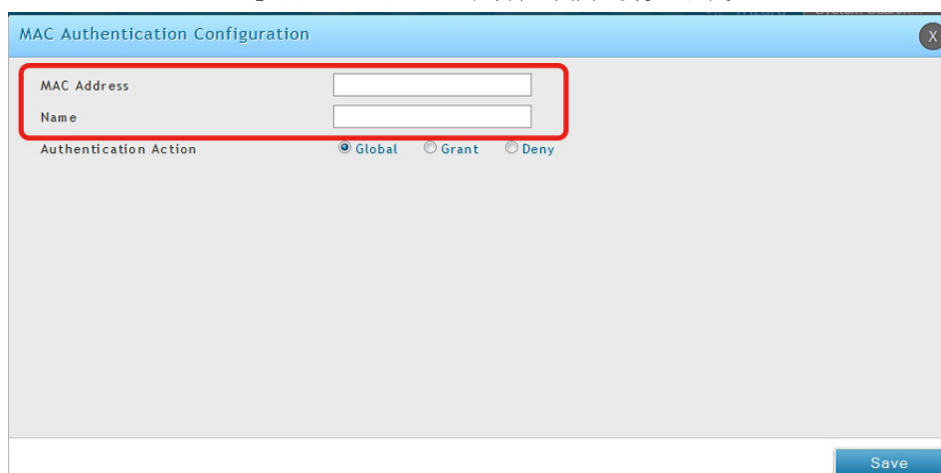


図 4-15 MAC Authentication Configuration 画面

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

6. Wireless > Access Point > SSID Profiles の順にメニューをクリックします。
7. 「SSID」 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。

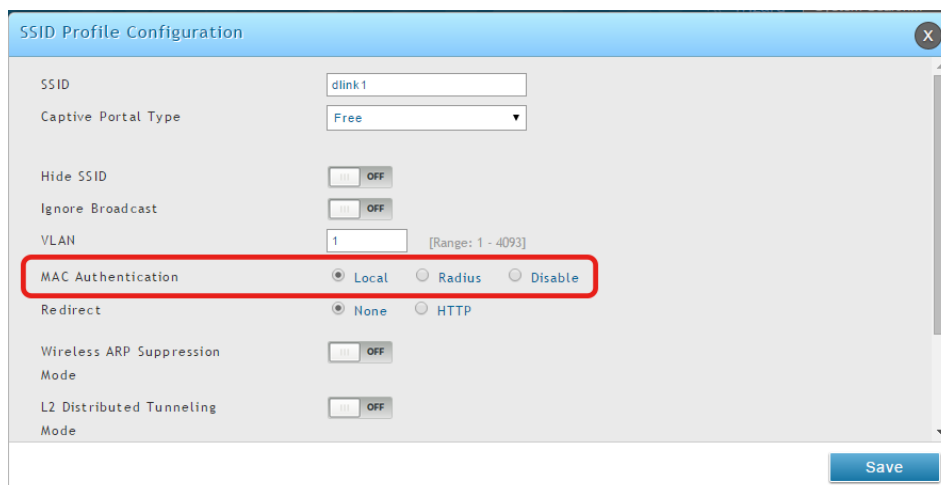


図 4-16 SSID Profile Configuration 画面

8. 「Local」 を選択し、「Save」 ボタンをクリックします。

⑥ 設定した 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を確認します。

注意 コンフィグレーション設定を変更するたびに、本手順を実行する必要があります。

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。

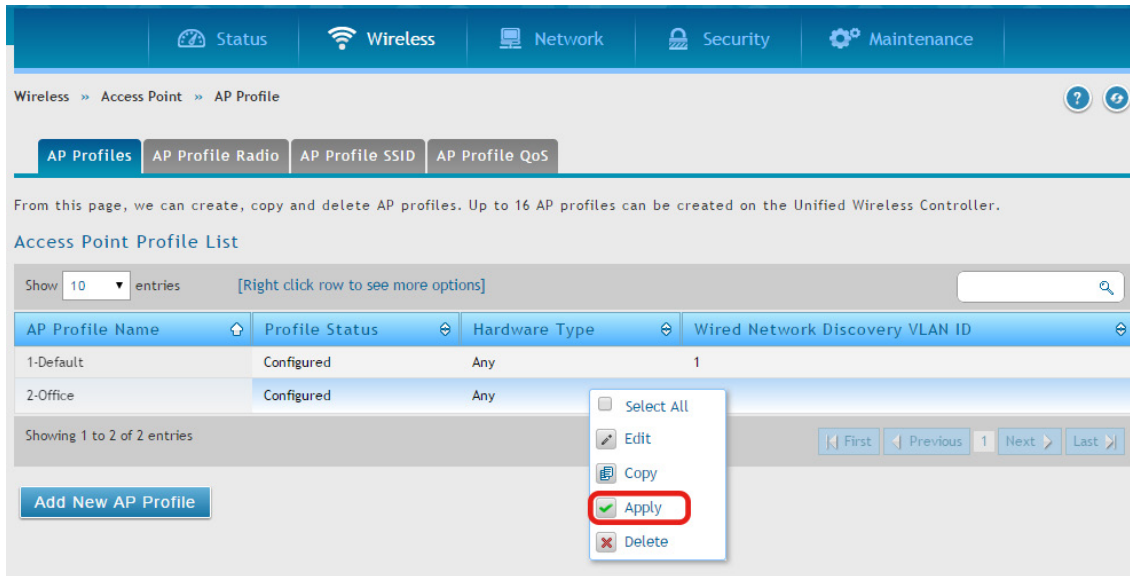



図 4-17 AP Profile List 画面

2. 「Access Point Profile List」の下で、更新する AP プロファイルで右クリックし、「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。

⑦ キャプティブポータルの設定

ローカルデータベースを持つ無線コントローラのキャプティブポータル設定には、以下の4つの手順があります。

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。

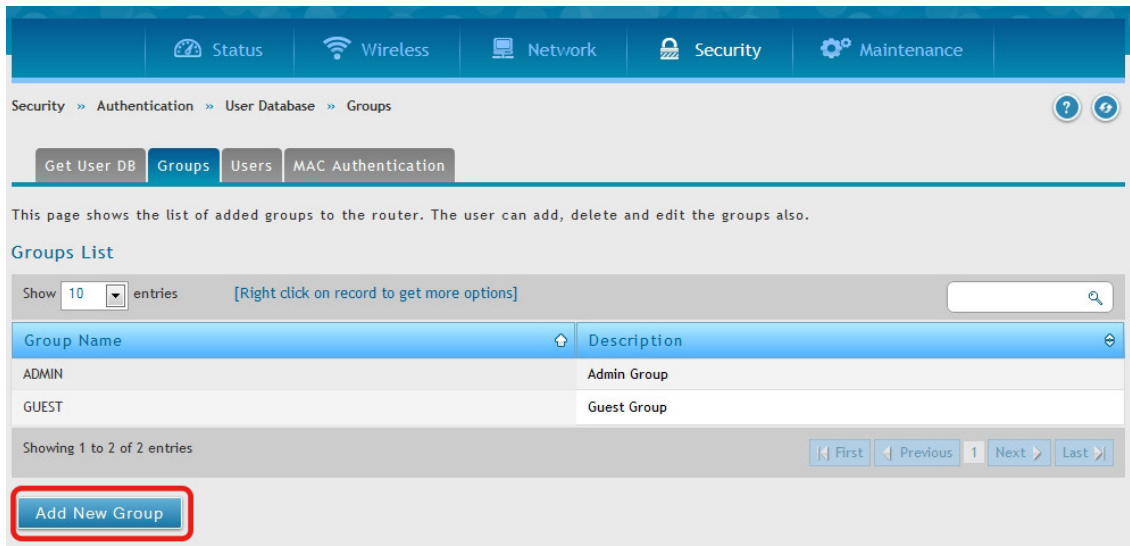
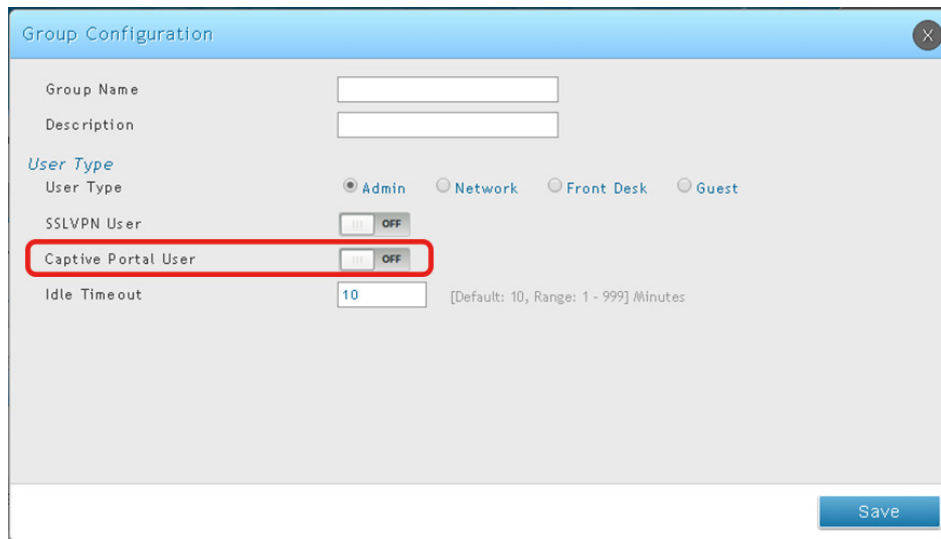


図 4-18 Group List 画面

- 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。



The image shows a 'Group Configuration' dialog box with the following fields and options:

- Group Name: Text input field
- Description: Text input field
- User Type: Radio buttons for Admin (selected), Network, Front Desk, and Guest.
- SSLVPN User: Toggle switch set to OFF.
- Captive Portal User: Toggle switch set to OFF, highlighted with a red rectangle.
- Idle Timeout: Text input field with '10' entered, and a note '[Default: 10, Range: 1 - 999] Minutes'.
- Save: Button at the bottom right.

図 4-19 Group Configuration 画面

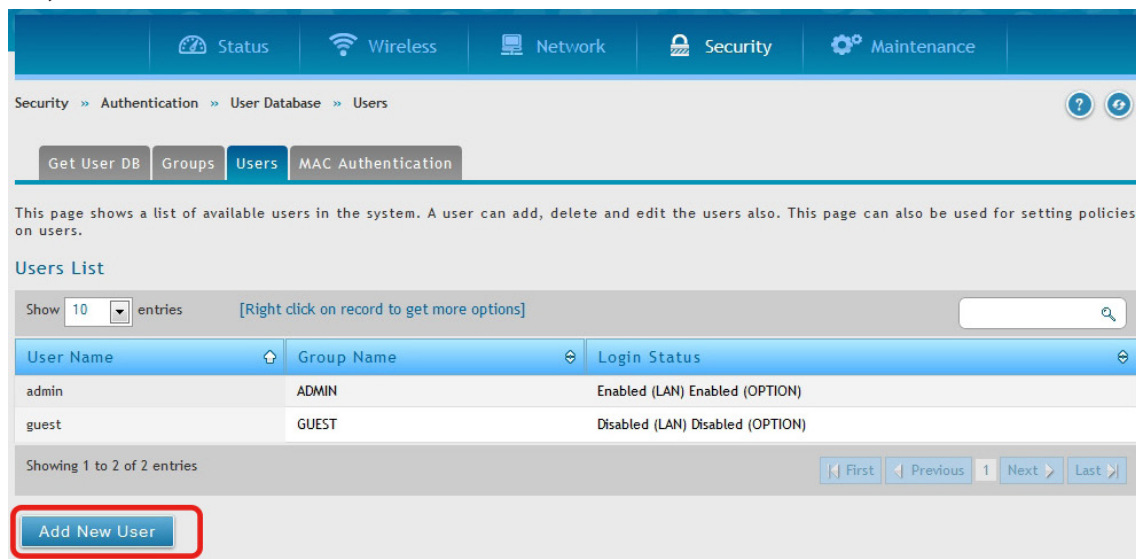
以下の項目があります。

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。



The image shows the 'User List' screen in the Security > Authentication > User Database > Users menu. It includes a navigation bar with tabs for Get User DB, Groups, Users (selected), and MAC Authentication. Below the tabs, there is a description of the page and a 'Users List' table. The table has columns for User Name, Group Name, and Login Status. Two users are listed: 'admin' (ADMIN group, Enabled) and 'guest' (GUEST group, Disabled). At the bottom, there is a red-bordered button labeled 'Add New User'.

図 4-20 User 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。

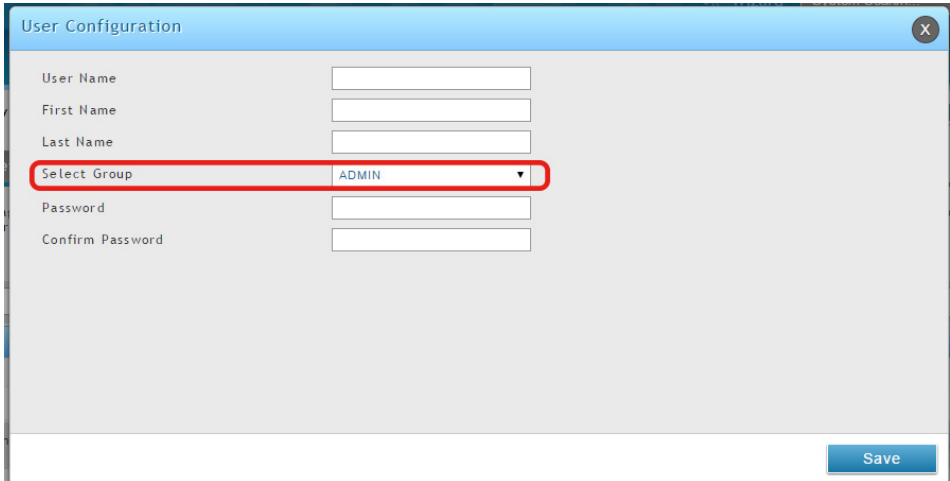


図 4-21 User Configuration 画面

以下の項目があります。

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。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	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。
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 プロファイルに関連付ける

- a. **Wireless > Access Point > SSID 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。

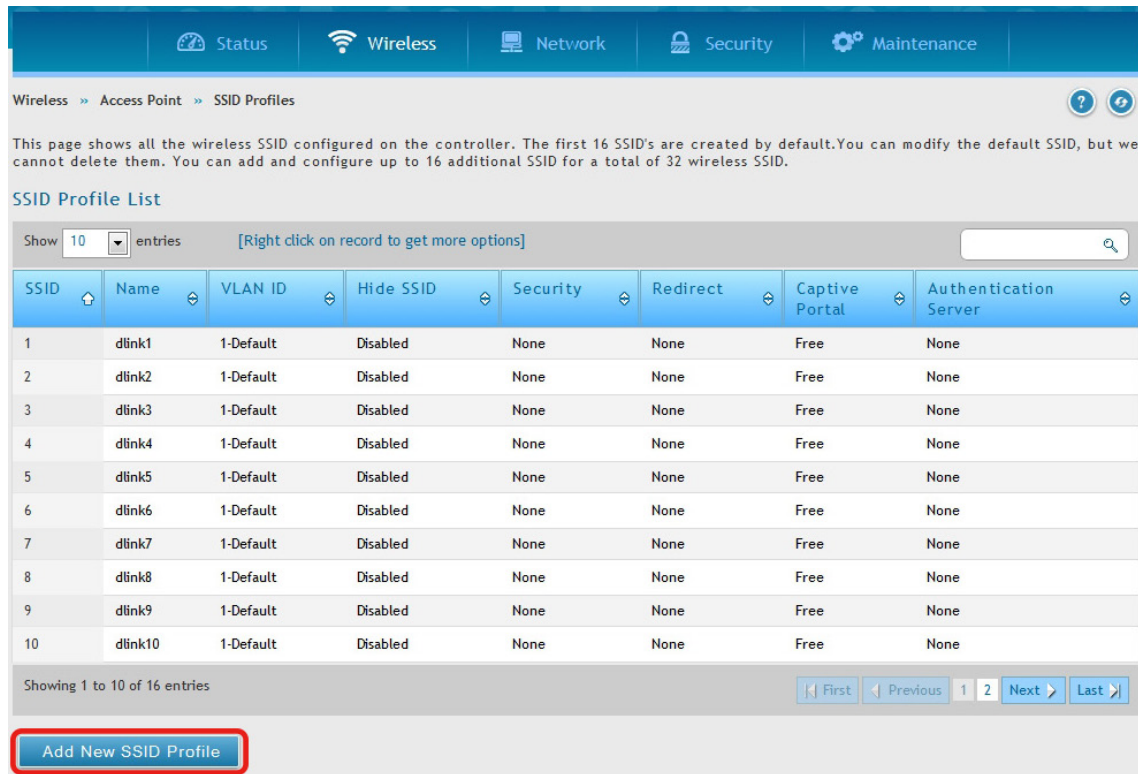


図 4-22 AP Profile SSID 画面

- b. 「SSID Status」で、キャプティブポータル機能を使用する「SSID」を右クリックして、「Edit」を選択すると、以下の画面が表示されます。

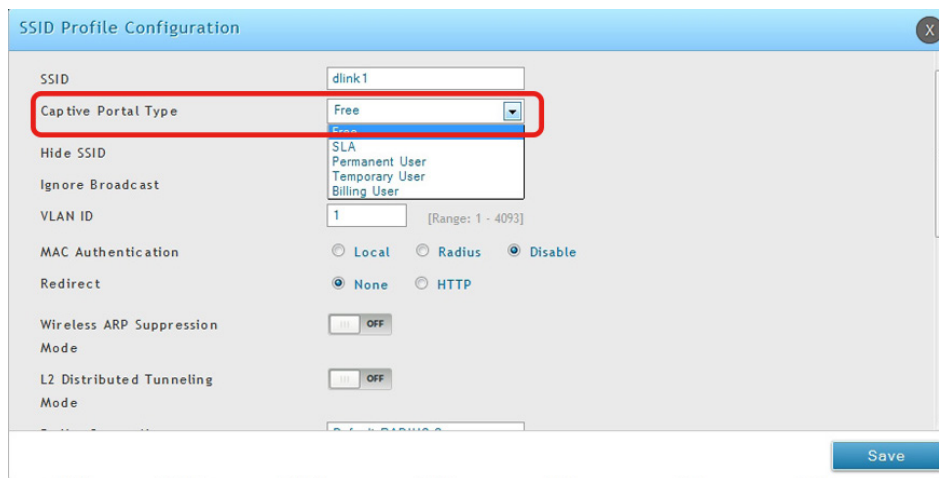
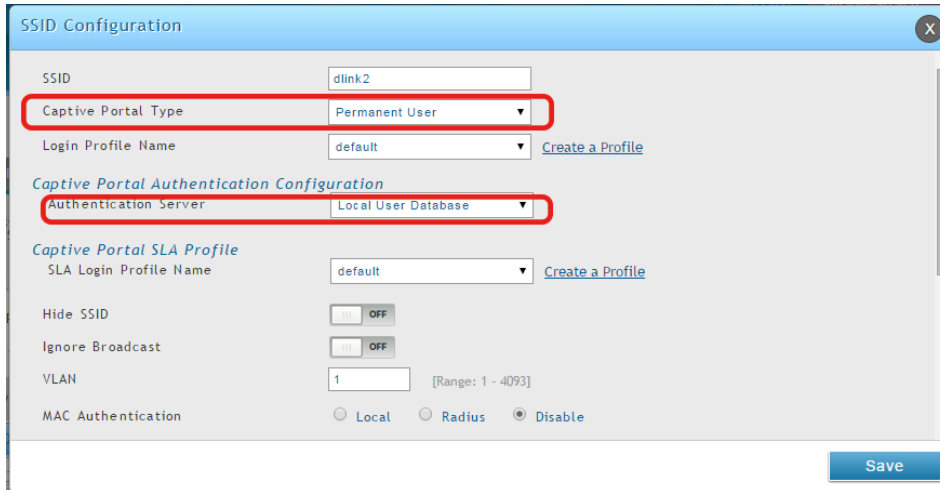


図 4-23 SSID Configuration 画面

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」- 認証方式はローカルユーザデータベースとなります。

この場合、ローカルなデータベースのユーザアカウントはパーマネントユーザのアカウントです。「Captive Portal Type」で「Permanent User」を選択し、「Authentication Server」で「Local User Database」を選択します。



The image shows the 'SSID Configuration' window. The 'SSID' field contains 'dlink2'. The 'Captive Portal Type' dropdown menu is set to 'Permanent User'. The 'Login Profile Name' dropdown is set to 'default'. The 'Captive Portal Authentication Configuration' section shows the 'Authentication Server' dropdown set to 'Local User Database'. The 'Captive Portal SLA Profile' section shows the 'SLA Login Profile Name' dropdown set to 'default'. The 'Hide SSID' and 'Ignore Broadcast' checkboxes are both set to 'OFF'. The 'VLAN' field contains '1'. The 'MAC Authentication' section has three radio buttons: 'Local', 'Radius', and 'Disable', with 'Local' selected. A 'Save' button is at the bottom right.

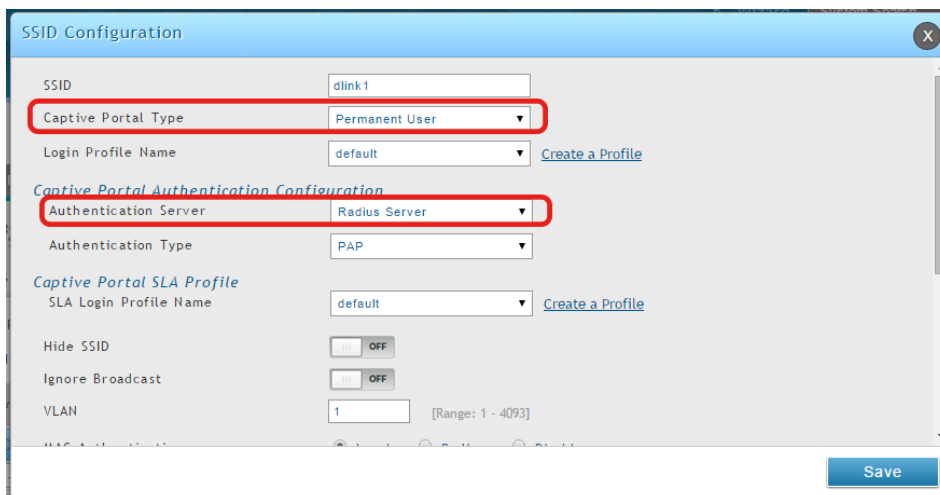
図 4-24 SSID Configuration 画面

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された SSID と関連付けされます。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、キャプティブポータルページへコントロールがリダイレクトします。

認証データベースが 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。



The image shows the 'SSID Configuration' window. The 'SSID' field contains 'dlink1'. The 'Captive Portal Type' dropdown menu is set to 'Permanent User'. The 'Login Profile Name' dropdown is set to 'default'. The 'Captive Portal Authentication Configuration' section shows the 'Authentication Server' dropdown set to 'Radius Server' and the 'Authentication Type' dropdown set to 'PAP'. The 'Captive Portal SLA Profile' section shows the 'SLA Login Profile Name' dropdown set to 'default'. The 'Hide SSID' and 'Ignore Broadcast' checkboxes are both set to 'OFF'. The 'VLAN' field contains '1'. The 'MAC Authentication' section has three radio buttons: 'Local', 'Radius', and 'Disable', with 'Local' selected. A 'Save' button is at the bottom right.

図 4-25 SSID Configuration 画面

4. キャプティブポータル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。

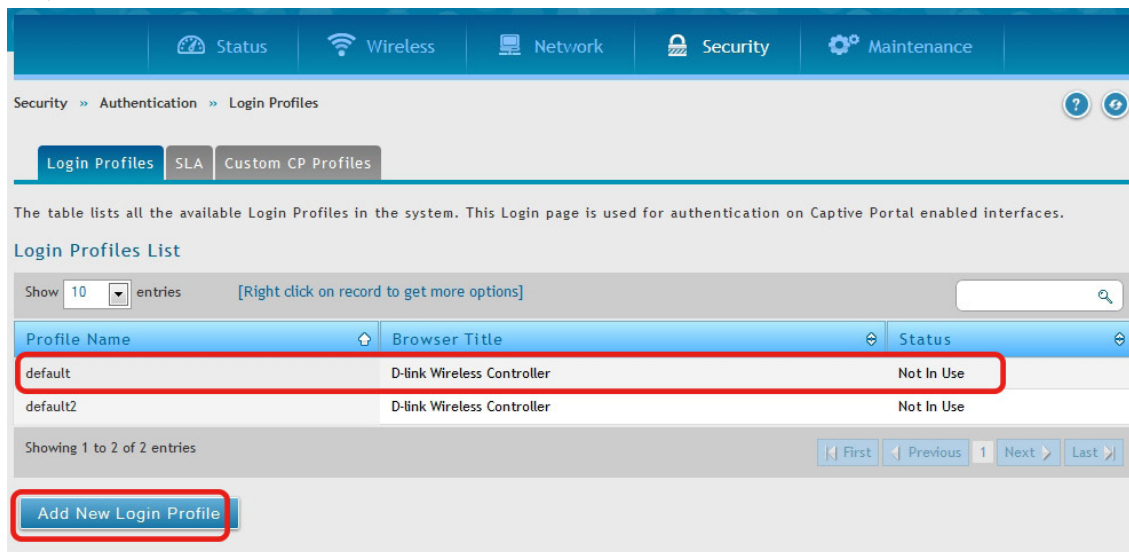


図 4-26 Login Profiles List 画面

- b. 「Add New Login Profile」 ボタンをクリックして、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、プロファイル編集します。以下の画面が表示されます。

Login Profile Configuration

General Details

Profile Name

Browser Title

Background

Image

Color

Page Background Image

Default

Add

Add

Add

Add

Add

Minimal Page for Mobile Devices

ON

OFF

Header Details

Background

Image

Color

Header Background Image

Default

Add

Add

Add

Add

Add

Add

Add

Add

Add

Add

Add

Header Caption

Caption Font

Tahoma

Font Size

Small

Font Color

Red

Login Details

Login Section Title

Portal Login

Welcome Message

Please Login!

Error Message

Invalid UserName/Password

Footer Details

Change Footer Content

ON

OFF

Footer Content

Footer Font Color

White

External Payment Gateway

Enable External Payment Gateway

ON

OFF

Session Title1

Message

Session Title2

Success Message

Session Title 3

Failure Message

Enable Billing Profiles

Profile Name	Billing Status	Description	Status
No data available in table			

Service Disclaimer Text

Service Disclaimer Text

Payment Server

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（表示）します。キャプティブプロファイル固有の名称の指定を推奨します。
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。 <ul style="list-style-type: none"> 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 100k バイトです。
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。
Minimal Page for Mobile Devices	「ON」にするとモバイルデバイス対応のページを表示します。
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が、画像またはカラーを表示するかどうかを選択します。 <ul style="list-style-type: none"> Image - ページで画像を表示します。「Header Background Color」フィールドを使用して、背景画像を選択します。画像の最大サイズは 100k バイトです。 Color - ページで背景色を表示します。ラジオボタンを使用して、色を選択します。
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。画像の最大サイズは 100k バイトです。
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。「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。
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。
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。
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ェ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「ON」にした場合、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」を「ON」にした場合、フッターに表示されるカラーを入力します。
External Payment Gateway	
Enable External Payment Gateway	外部ペイメントゲートウェイを有効にします。
Session Title 1 - 3	セッションのタイトルを 1-3 まで指定します。
Message	セッション 1 に表示されるメッセージを指定します。
Success Message	セッション成功時に表示されるメッセージを指定します。
Failure Message	セッション失敗時に表示されるメッセージを指定します。
Enable Billing Profiles	
Service Disclaimer Text	表示されるサービス概要を指定します。
Payment Server	ペイメントサーバを指定します。

- 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が設定内容に沿っていることを確認します。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。

⑧ RADIUS サーバを持つ SSID をオーセンティケータ（認証 SSID）として使用する

RADIUS 認証を持つ 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 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。

StatusWirelessNetworkSecurityMaintenance

Security >> Authentication >> External Auth Server >> RADIUS Server

RADIUS Server

RADIUS Accounting

RADIUS Accounting Global Setting

POP3 Server

POP3 Trusted CA

LDAP Server

AD Server

NT Domain

This page configures the RADIUS servers to be used for authentication. A RADIUS server maintains a database of user accounts used in larger environments. If a RADIUS server is configured in the LAN, it can be used for authenticating users that want to connect to the wireless network provided by this device. If the first/primary RADIUS server is not accessible at any time, then the device will attempt to contact the secondary RADIUS server for user authentication.

RADIUS Server Configuration

Server Check

Server Checking

Authentication Server 1 IP Address

192.168.1.2

Authentication Port

1812

[Range: 0 - 65535]

Secret

.....

Timeout

1

[Range: 1 - 999] Seconds

Retries

2

[Range: 1 - 9] Seconds

Authentication Server 2 IP Address

192.168.1.3

Authentication Port

1812

[Range: 0 - 65535]

Secret

.....

Timeout

1

[Range: 1 - 999]

Retries

2

[Range: 1 - 9]

Authentication Server 3 IP Address

192.168.1.4

Authentication Port

1812

[Range: 0 - 65535]

Secret

.....

Timeout

1

[Range: 1 - 999]

Retries

2

[Range: 1 - 9]

Save

Cancel

図 4-28 RADIUS Server Configuration 画面

以下の項目があります。

項目	説明
Server Checking	クリックして、コントローラと RADIUS サーバ間の接続をテストします。Authentication Server 名と接続状況が表示されます。
Authentication Server 1-3 IP Address	RADIUS 認証サーバの IP アドレスを指定します。
Authentication 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。
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	コントローラが処理をやめる前に RADIUS サーバに行う再試行回数を指定します。

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。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。
3. 「Server Checking」ボタンをクリックして、DWC-1000 と RADIUS サーバ間の接続をテストします。

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。

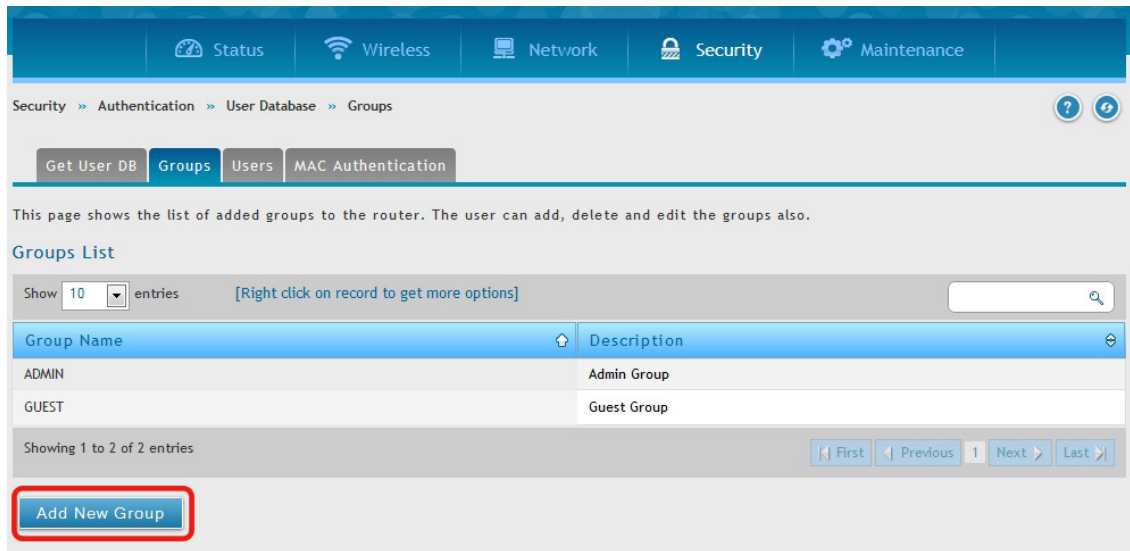


図 4-29 Group List 画面

- 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。

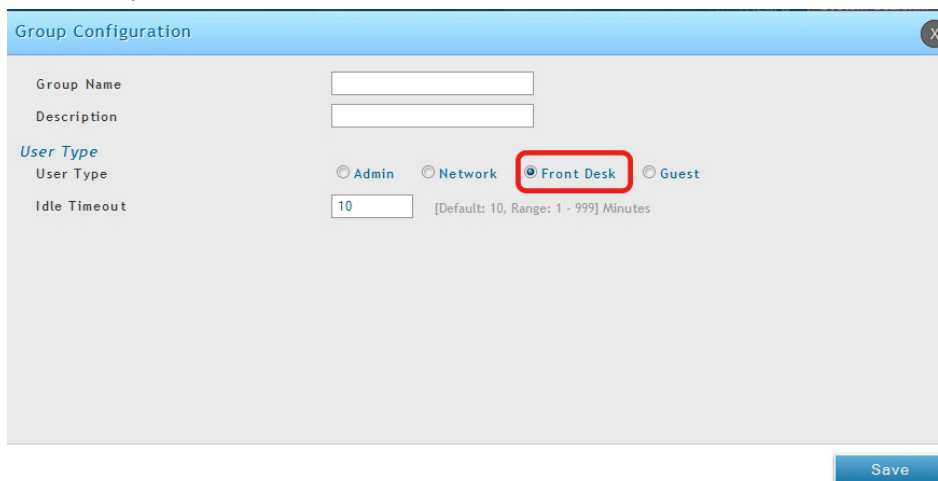


図 4-30 Group Configuration 画面

- 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。

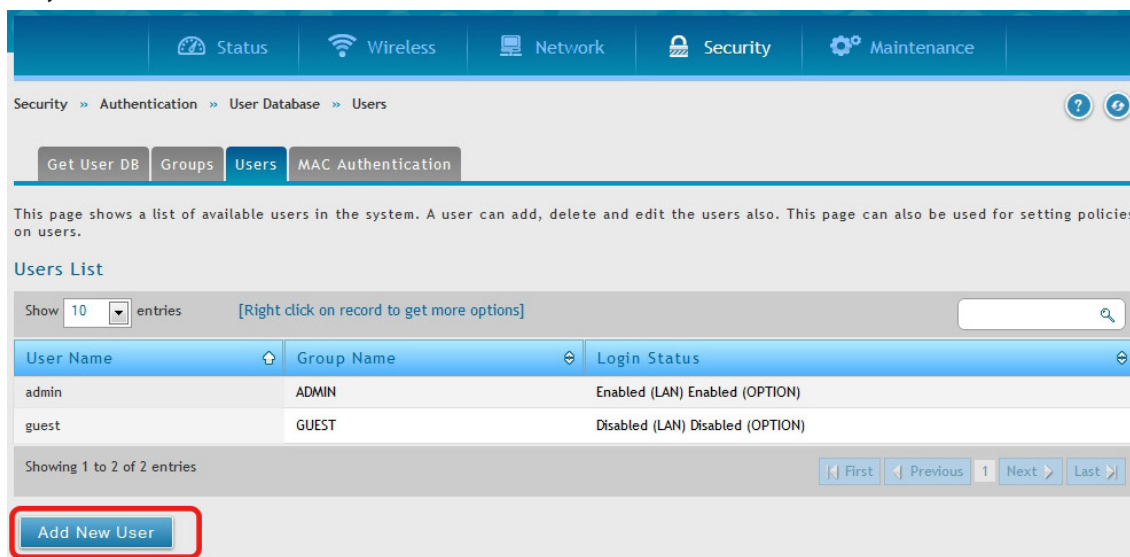
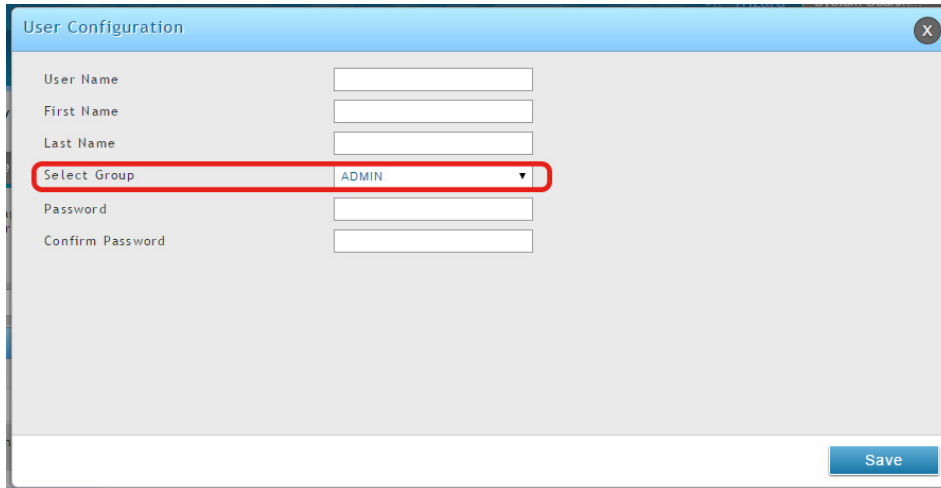


図 4-31 User List 画面

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



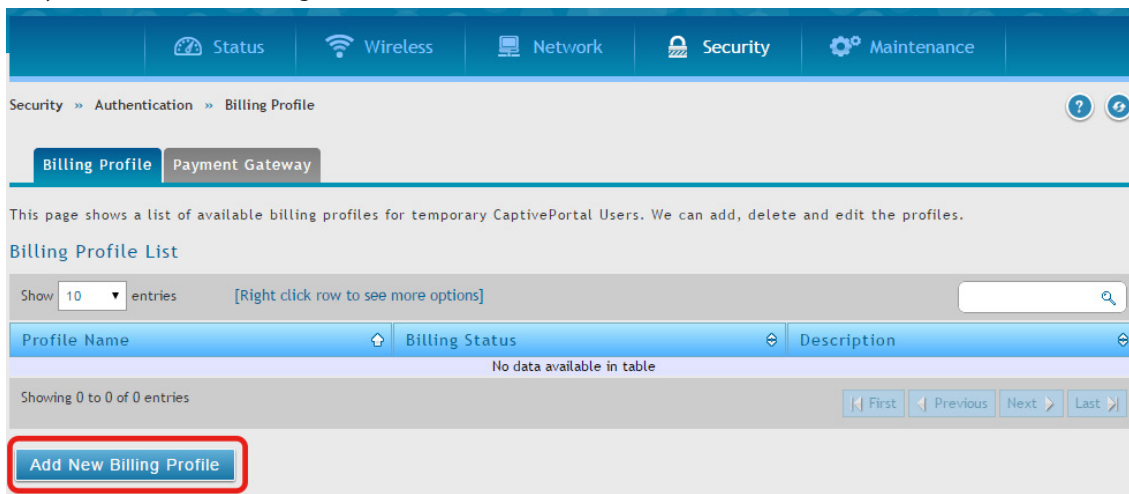
The image shows a 'User Configuration' dialog box with the following fields: User Name, First Name, Last Name, Select Group (a dropdown menu currently showing 'ADMIN'), Password, and Confirm Password. A red rectangle highlights the 'Select Group' dropdown. A 'Save' button is located at the bottom right of the dialog.

図 4-32 User Configuration 画面

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

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、以下の画面を表示します。



The image shows the 'Billing Profile List' screen in a web interface. The breadcrumb trail is 'Security > Authentication > Billing Profile'. There are tabs for 'Billing Profile' and 'Payment Gateway'. A message states: 'This page shows a list of available billing profiles for temporary CaptivePortal Users. We can add, delete and edit the profiles.' Below this is a table with columns 'Profile Name', 'Billing Status', and 'Description'. The table is currently empty, showing 'No data available in table'. At the bottom, there is a button labeled 'Add New Billing Profile' which is highlighted with a red rectangle.

図 4-33 Billing Profile List 画面

「Add New Billing Profile」 ボタンをクリックします。

- b. ビリングプロファイル設定には、スケジュールごとに 4 個の手順があります。



- ・ 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。

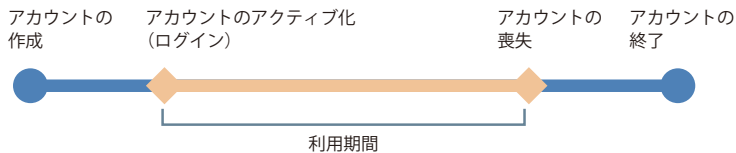
最も一般的なビリングプロファイルのタイプには以下の5つがあります。:

- I. 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、アカウントは作成されると有効になります。



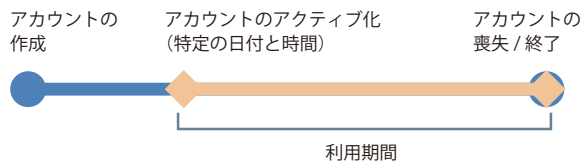
このビリングプロファイルは、ホテルで使用するというシナリオに適しています。一時的なアカウントは、カスタマのチェックイン時に、作成されて有効になります。

- II. 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、アカウントは最初にログインすると、有効になります。



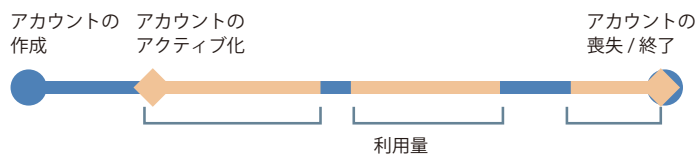
このビリングプロファイルは、カフェや空港などで使用するというシナリオに適しています。カスタマは、最初のログインから計算した時間内で、無線インターネットサービスを使用できます。

- 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。



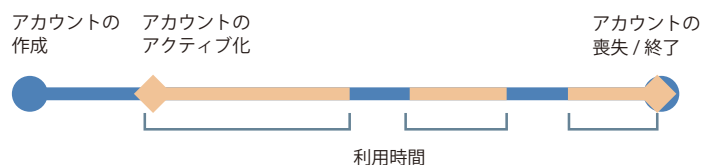
このビリングプロファイルは、プレスカンファレンスで使用するというシナリオに適しています。必要であれば、前もってイベントとデリバリの情報を関係者に説明する前に、主催者はアカウントを生成します。一時的なアカウントは特定の日時から有効にされます。

- 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。

Captive Portal Billing Profile Configuration

Profile Details

Profile Name

Profile Description

Allow Multiple Login

OFF

Allow Customized account on Front Desk

OFF

Allow batch generation on Front Desk

OFF

Session Idle Timeout

[Default: 10, Range: 1 - 60] Minutes

Show alert message on login page while rest of usage time/traffic under

Hour

Basic Limit by Duration

Valid with Begin and End time

OFF

Basic limit by usage

Maximum Usage Time

OFF

Maximum Usage Traffic

OFF

Unit Price

Set Price

OFF

Save

図 4-34 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	自身を識別するプロファイル名を指定します。
Profile Description	プロファイルの説明文を指定します。
Allow Multiple Login	「ON」にすると、複数のユーザは、同時にログインできるように、このプロファイルに作成済みである同じキャプティブポータルのログイン証明書を使用できます。
Allow Customized account on Front Desk	「ON」にすると、フロントデスクユーザは、このプロファイルに作成済みであるキャプティブポータルユーザにカスタマイズしたアカウント名を付与できます。
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。
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。
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/Days/MB/GB 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。
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」を有効にした場合に、所要時間までユーザのアクセスを制限するタイプを選択します。: <ul style="list-style-type: none">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。

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制限を編集できます。

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 > SSID Profiles** の順にクリックし、「SSID Profile 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. プルダウンメニューから「Captive Portal Type」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>) 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。

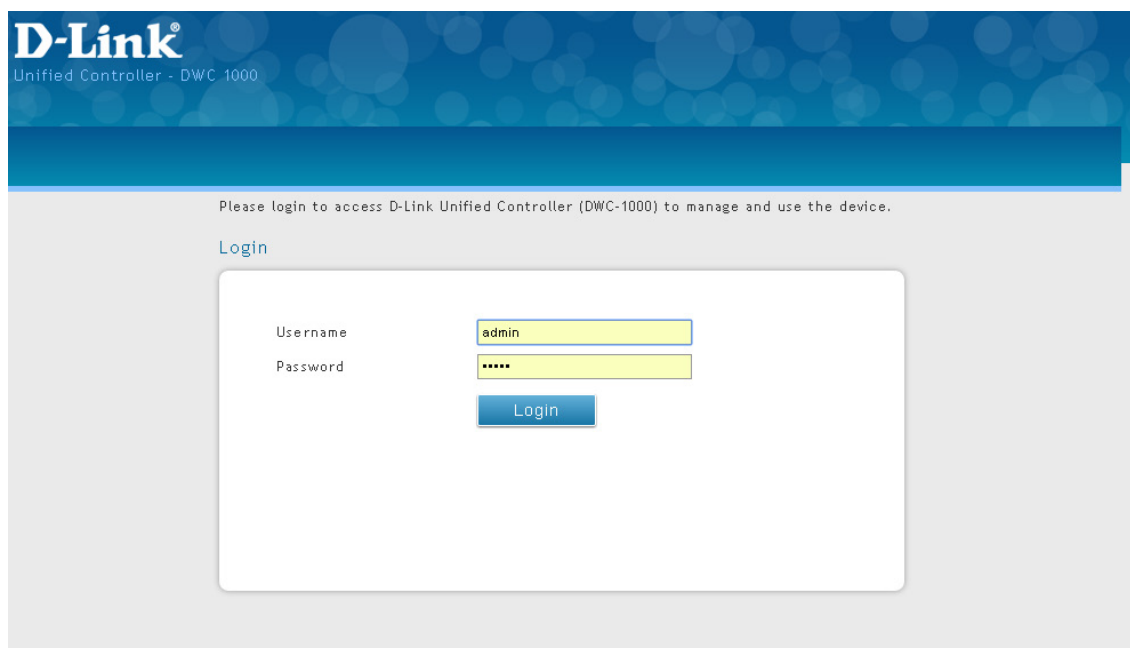


図 4-35 ゲストキャプティブポータル画面

- b. ビリングプロファイルを選択します。必要に応じて、使用法を修正します。「Generate」ボタンをクリックします。

Home

This page shows information about Front Desk profile and generated users.

Billing - BillingDesk

Select Billing Profile: dlink

Billing Form | View Accounts

dlink - dlink_billing

Start While Account Created: 1 Hours

Expiration Date and Time: 10/19/2014 11:30 PM (Set time from below)

MM DD YYYY HH MM AM/PM

10 19 2014 11 30 PM

Generate

図 4-36 Billing - Generate 画面

- c. 「Print」をクリックすることで、課金情報を出力します。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。

Billing Profiles Configuration

BP1's User Accounts

Username: HS_8U72f

Password: c13QL9Y

Maximum Usage Time: 1 Hours

Print

図 4-37 Biling 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についてレビューするためには「View Account」タブをクリックし、以下の画面を表示します。

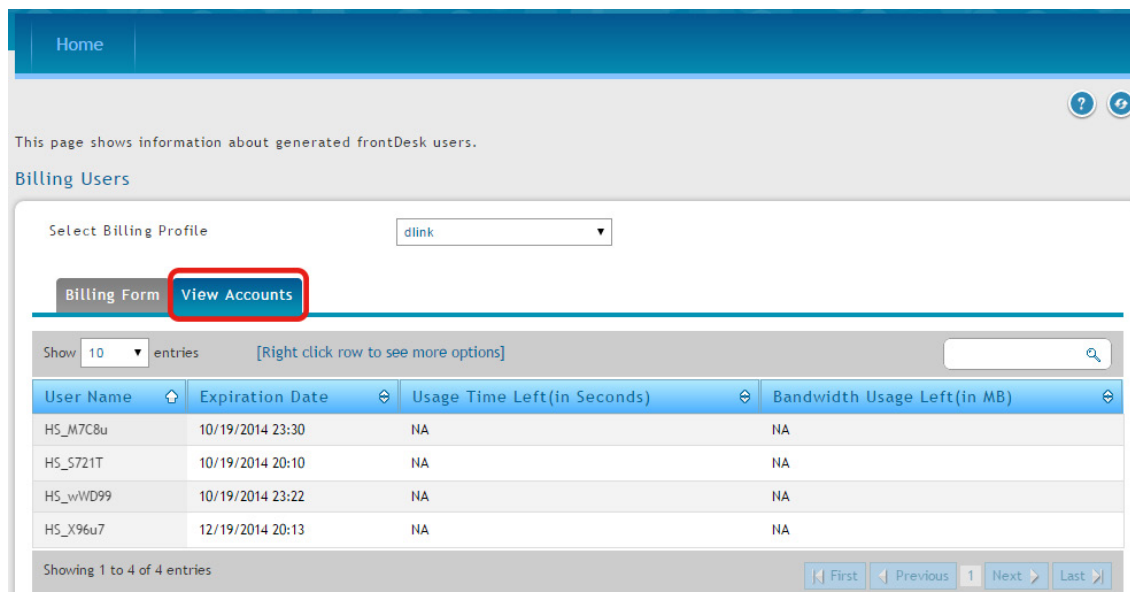


図 4-38 Billing Users 画面

- 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。

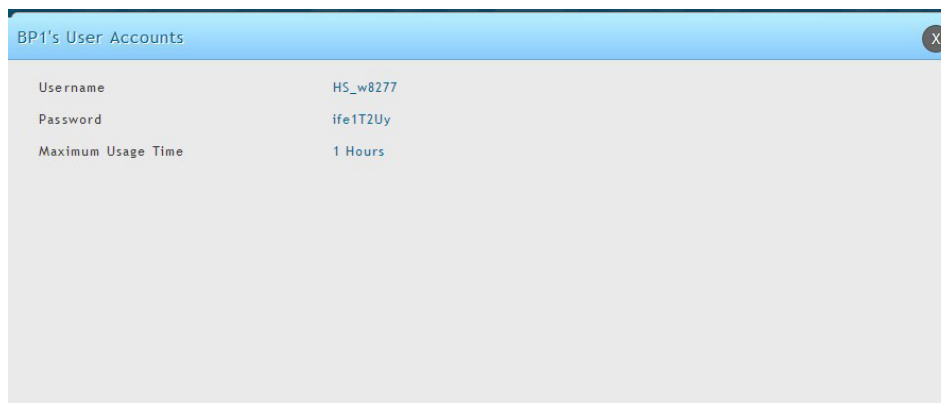


図 4-39 Billing User Account 画面

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。

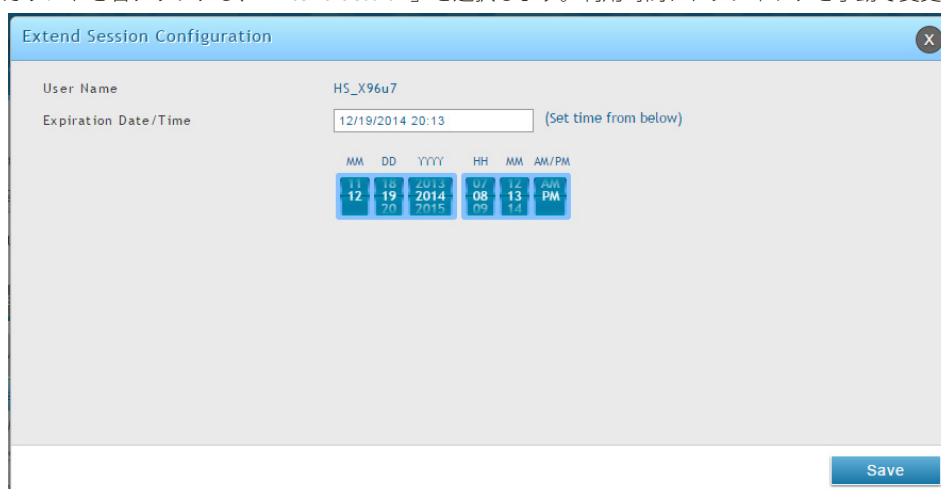


図 4-40 Extend Session Configuration 画面

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。

⑩ BYOD 環境の設定

職場の 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。従業員が仕事に自身のデバイスを使用することを許可する多くの会社では、より高いパフォーマンスと生産性を期待しています。しかし、その反面、個人のデバイスを使用することで、会社もネットワークセキュリティと情報漏洩を検討する必要があります。どのように、会社が提供したデバイスと個人のデバイス (BYOD デバイス) を見分けるかは、IT チームの主なタスクとなります。

デバイスの MAC 認証を使用して、そのデバイスは会社が提供したものか、または個人のものかということに基づき、クライアントに特定の SSID を関連付けます。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。:

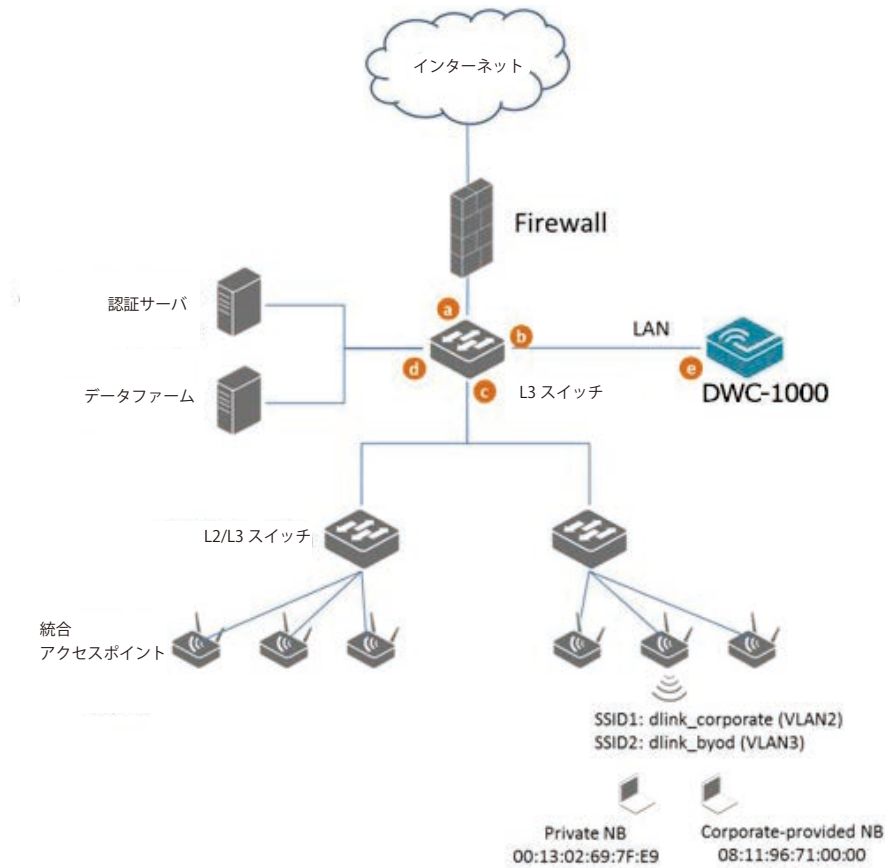


図 4-41 BYOD Configuration 画面

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。

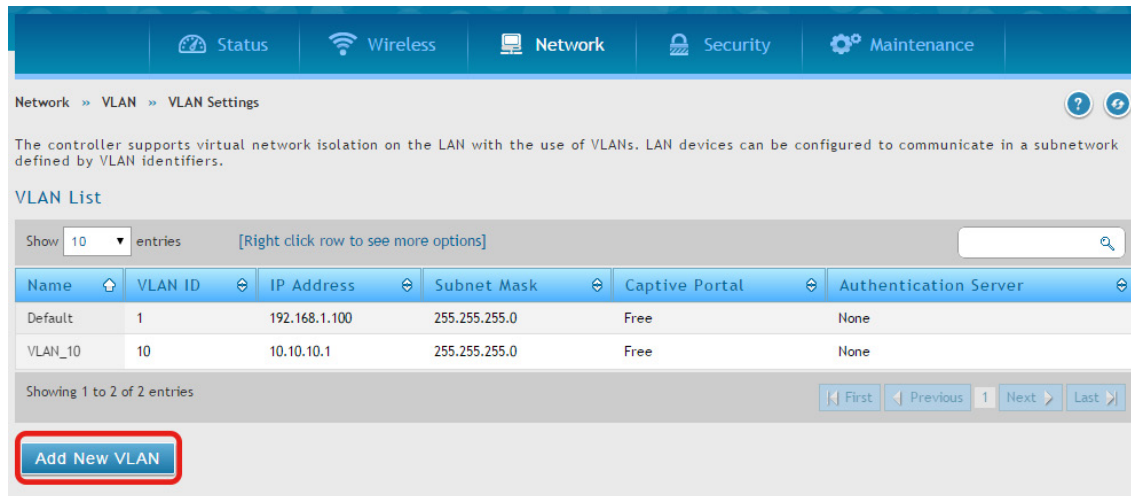


図 4-42 VLAN List 画面

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

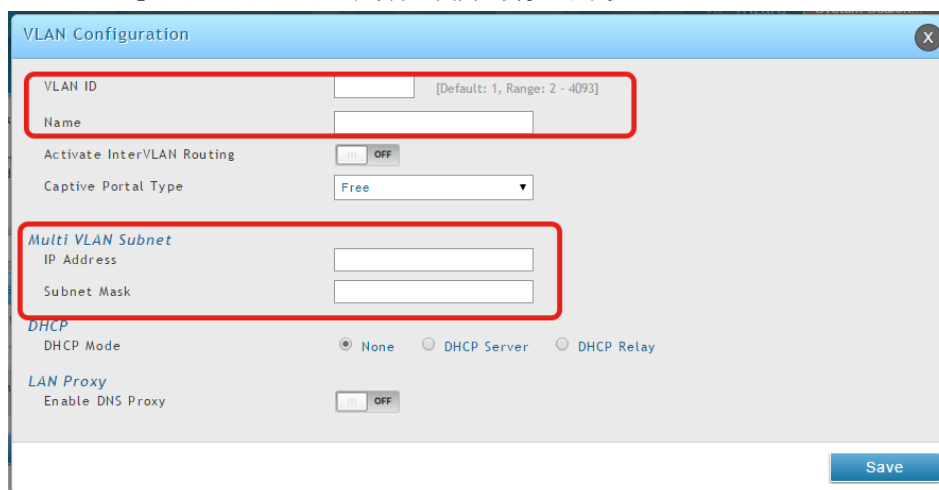


図 4-43 VLAN Configuration 画面

c. VLAN ID と VLAN 名 を入力します。

d. VLAN の IP アドレスを入力します。

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。

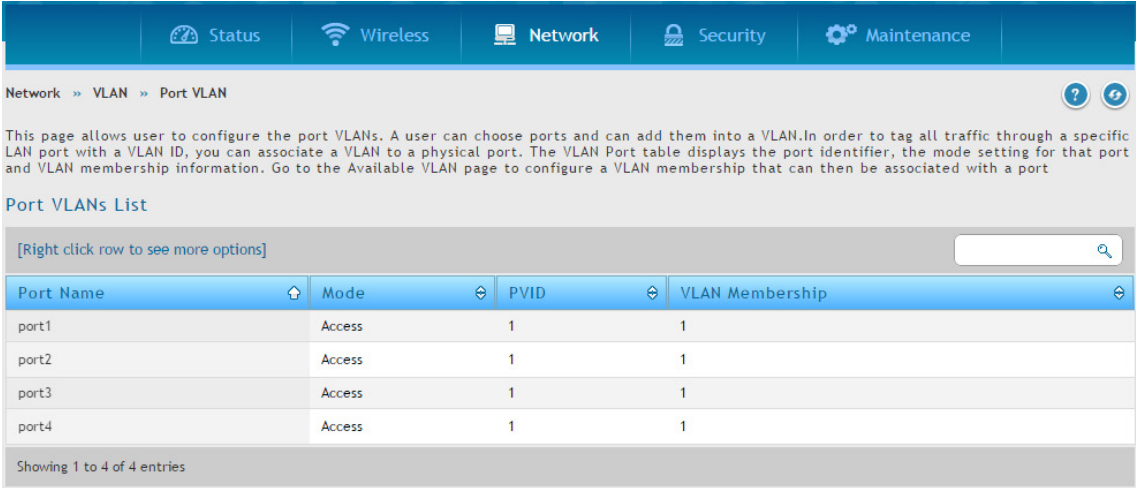


図 4-44 Port VLANs List 画面

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。

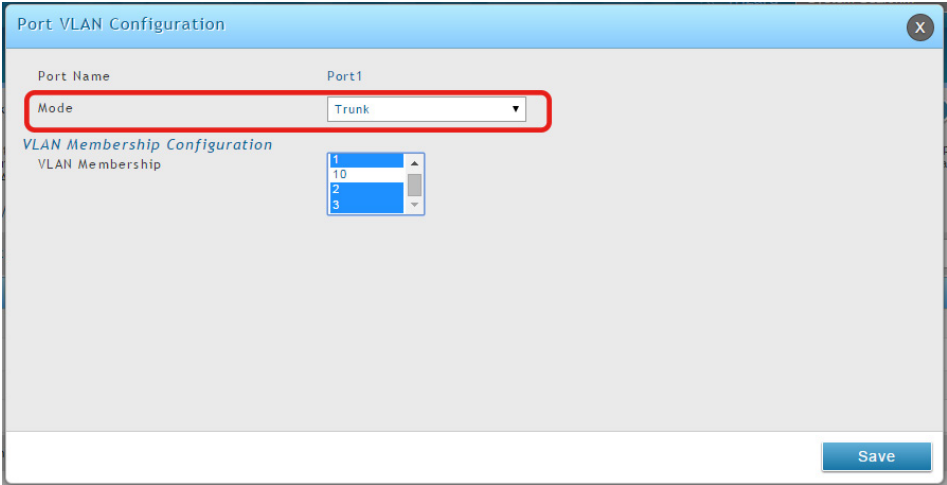


図 4-45 Port VLAN Configuration 画面

「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 > SSID 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。

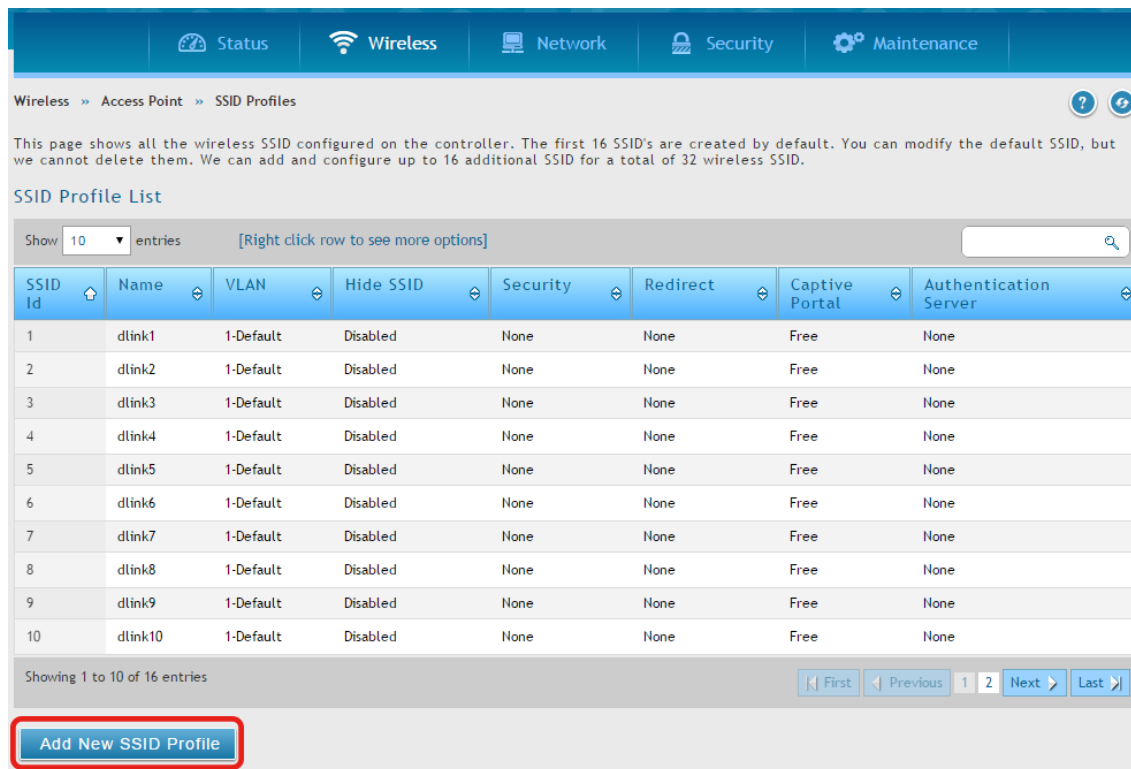


図 4-46 SSID Profile List 画面

- 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。

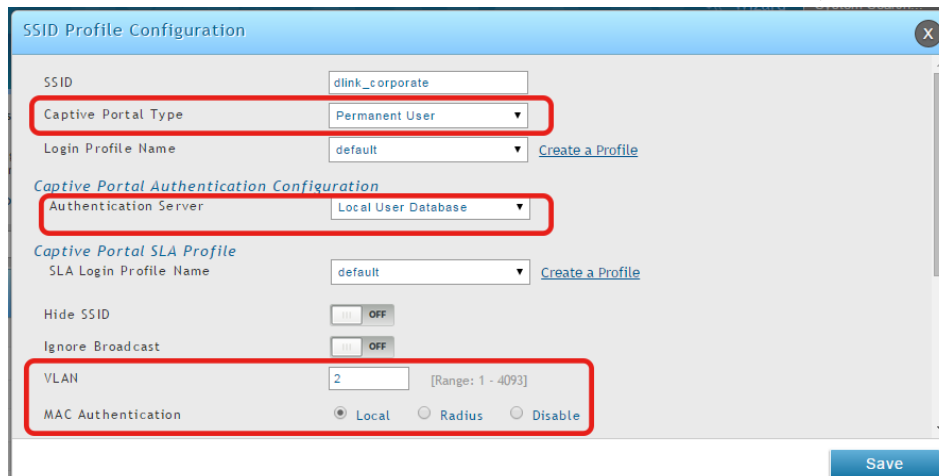


図 4-47 SSID Profile Configuration 画面 - dlink_corporate

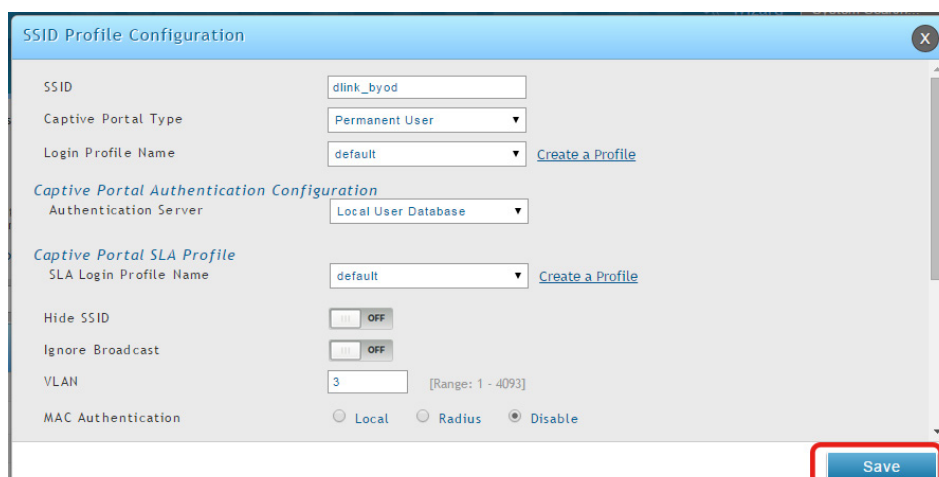


図 4-48 SSID Profile Configuration 画面 - dlink_byod

- 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。

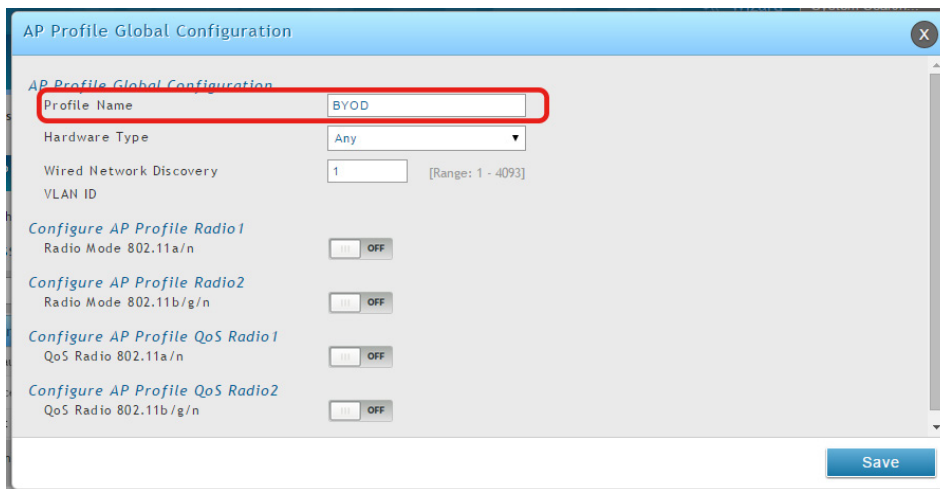


図 4-49 AP Profile Global Configuration 画面

- 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」で「BYOD」を選択します。
- e. 「SSID」リストで「dlink_corporate」列を右クリックして、「Enable」を選択します。
- f. 「dlink_byod」列を右クリックして、「Enable」を選択します。

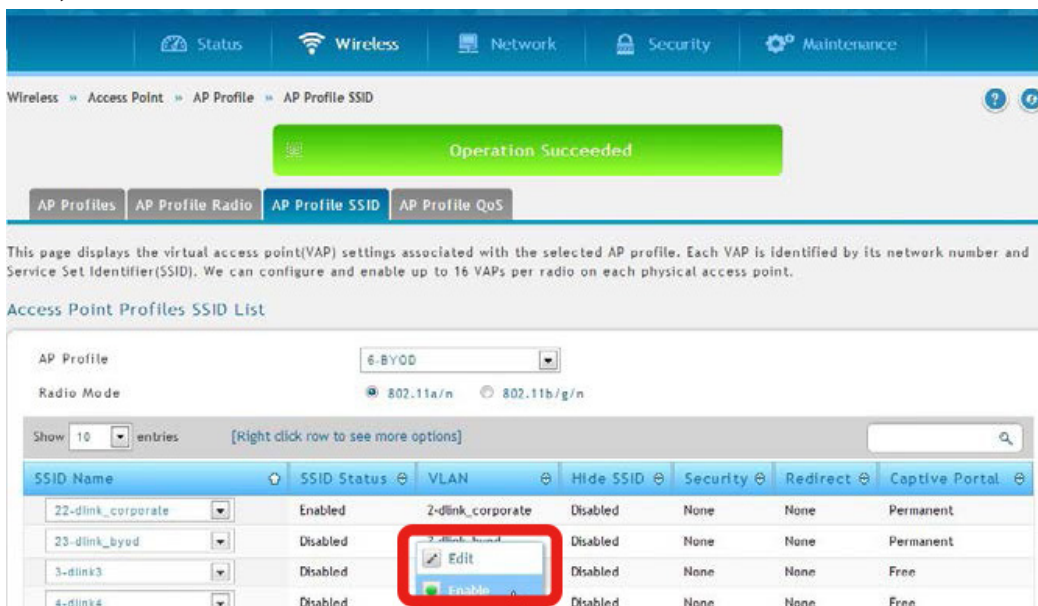
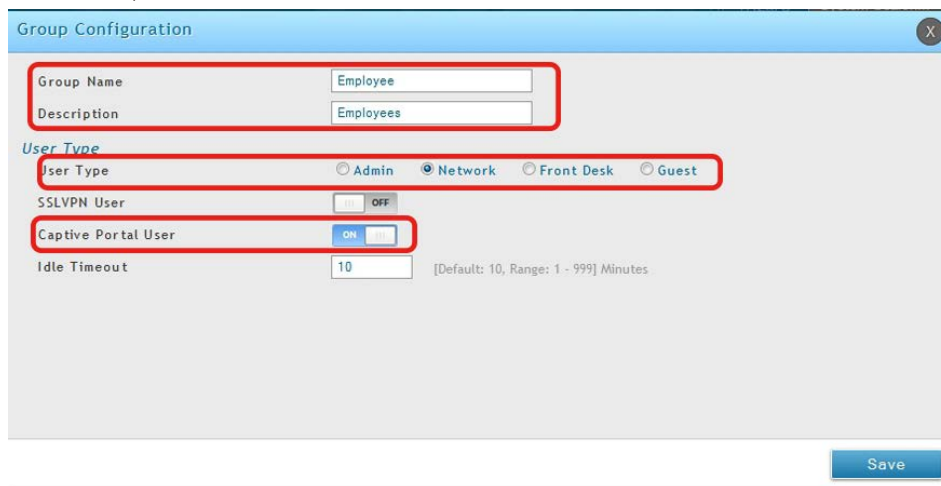


図 4-50 AP Profiles SSID List 画面

- 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. ローカルの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。



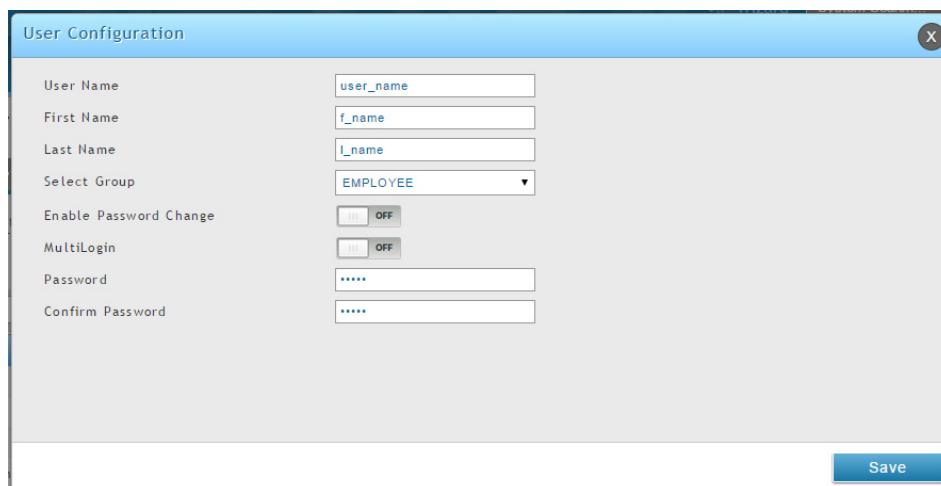
The image shows the 'Group Configuration' dialog box. It has a title bar with a close button (X). The form contains the following fields and controls:

- Group Name:** Text input field with 'Employee' entered.
- Description:** Text input field with 'Employees' entered.
- User Type:** A section with four radio buttons: 'Admin', 'Network' (selected), 'Front Desk', and 'Guest'.
- SSLVPN User:** A toggle switch set to 'OFF'.
- Captive Portal User:** A toggle switch set to 'ON'.
- Idle Timeout:** A text input field with '10' entered. To its right, it says '[Default: 10, Range: 1 - 999] Minutes'.
- Save:** A blue button at the bottom right.

図 4-51 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。



The image shows the 'User Configuration' dialog box. It has a title bar with a close button (X). The form contains the following fields and controls:

- User Name:** Text input field with 'user_name' entered.
- First Name:** Text input field with 'f_name' entered.
- Last Name:** Text input field with 'l_name' entered.
- Select Group:** A dropdown menu with 'EMPLOYEE' selected.
- Enable Password Change:** A toggle switch set to 'OFF'.
- MultiLogin:** A toggle switch set to 'OFF'.
- Password:** Password input field with masked characters '*****'.
- Confirm Password:** Password input field with masked characters '*****'.
- Save:** A blue button at the bottom right.

図 4-52 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** タブの順にメニューをクリックします。
 - b. 「List Type」横に、現在のリストのタイプ (White-List または Black-List) が表示されます。設定を変更するには、[32 ページの「手順 5: MAC 認証モードの選択」](#)を参照してください。

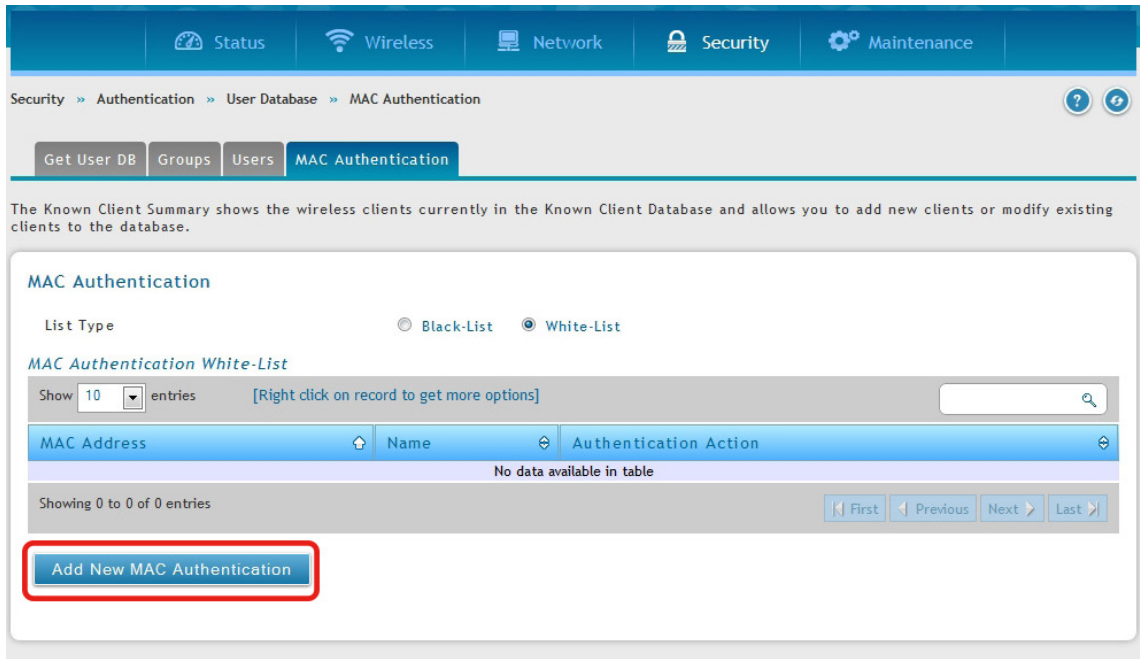


図 4-53 MAC Authentication White-List 画面

- 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。

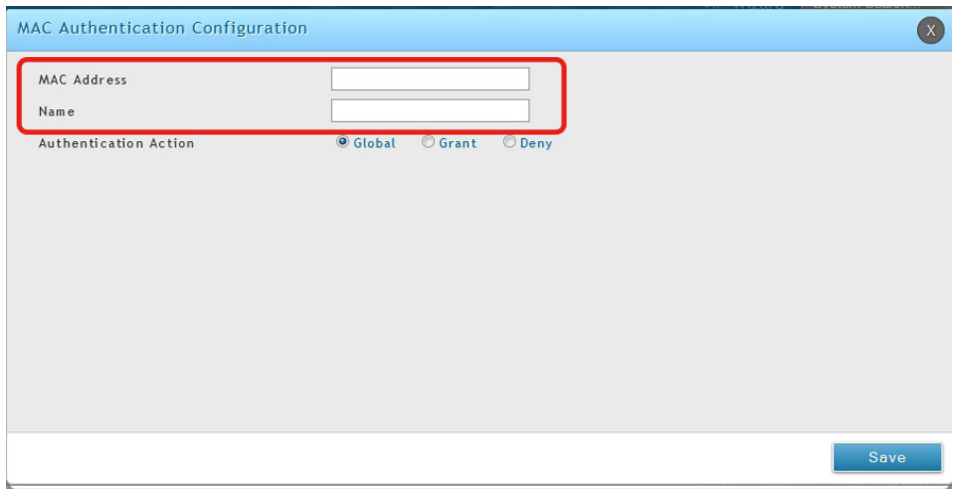


図 4-54 MAC Authentication Configuration 画面

デバイスの MAC アドレスと名称を入力します。

- d. 「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、[42 ページの「手順 8: RADIUS サーバを持つ SSID をオーセンティケーターとして使用する」](#)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発見して、管理します。[25 ページの「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。

ここから遷移すべき場所

番号の順でインストールすると、無線コントローラは、[255 ページの「付録 B 工場出荷時設定」](#)を使用した操作の準備が整います。これらの設定は多くのユーザと多くの状況に適応します。

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	参照ページ
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。	58
チャンネル計画と送信電力	チャンネルアルゴリズムと送信電力を設定します。	60
WIDS 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。	63
Distributed トンネル	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。	67
WLAN 視覚化	無線ネットワークの情報を図式化して表示します。	68
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。	72
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。	75
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。	82
SSID プロファイル	SSID プロファイルを設定します。	90
WDS 設定	WDS の管理グループとそのリンクを設定します。	93
ピアグループ	ピアコントローラの設定を行います。	97
AP ファームウェアダウンロード	アクセスポイントのファームウェアの更新を行います。	99

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による設定を推奨します。

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	
WLAN Controller Operational Status	コントローラの無線 LAN 機能を有効 / 無効にします。
IP Address	無線コントローラの 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）内では、4 台までのコントローラと共に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、この値がこのフィールドで指定した値に到達した時にそのエントリは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表示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そのエントリはリストから削除されます。

項目	説明
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、この値がこのフィールドで指定した値に到達した時にそのエントリは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そのエントリは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そのエントリはリストから削除されます。
Tunnel IP MTU Size	<p>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 サイズを増やすと、トラフィックがフローするポートに対して物理的な MTU を増やす必要があります。</p> <p>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。</p> <ul style="list-style-type: none"> 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。
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。
AP Client QoS	<p>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。</p> <p>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。より詳しく述べると、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。</p>
Radius Authentication Server	RADIUS 認証サーバを指定します。
Radius Authentication Server Status	RADIUS 認証サーバの状態について表示します。
Radius Accounting Server	RADIUS アカウンティングサーバを指定します。
Radius Accounting Server Status	RADIUS アカウンティングサーバの状態について表示します。
Global Accounting Mode	グローバルアカウンティングモードを有効にします。
AP Validation	
AP MAC Validation	<p>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、そのコントローラでローカルに、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で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。</p> <p>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。</p> <ul style="list-style-type: none"> 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	<p>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 Point」画面に移動するか、またはアクセスポイントの CLI にログインして「set managed-ap pass-phrase」コマンドを使用します。</p> <p>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。</p>

項目	説明
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発見して、管理します。
Country Configuration	
Country Code	国コードはご使用のコントローラとアクセスポイントを操作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 システムが運用す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、コントローラを本画面の値に更新します。

チャンネル計画と送信電力

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。

Wireless >> General >> Channel Algorithm >> Channel Algorithm 5 GHz

Channel Setting Manual Channel Plan Channel Plan History

Through this page we can configure AP frequency related parameters for 5 GHz radio channel.

5 GHz 2.4 GHz

RF Channel 5 GHz Settings

Radio: 5 GHz (802.11 a/n/ac)

Channel Plan Mode: ☒ Manual ☐ Interval ☐ Fixed Time

Ignore Unmanaged Aps: ☒ ON ☐ OFF

Channel Change Threshold: [Default: -82, Range: -99 to -1]

Managed AP CH Conflict Threshold: [Default: -56, Range: -99 to -1]

Save Cancel

図 5-2 RF Channel Settings 画面 - Manual

Wireless >> General >> Channel Algorithm >> Channel Algorithm 5 GHz

Channel Setting Manual Channel Plan Channel Plan History

Through this page we can configure AP frequency related parameters for 5 GHz radio channel.

5 GHz 2.4 GHz

RF Channel 5 GHz Settings

Radio: 5 GHz (802.11 a/n/ac)

Channel Plan Mode: ☐ Manual ☒ Interval ☐ Fixed Time

Channel Plan Interval: [Default: 6, Range: 6 - 24] Hours

Ignore Unmanaged Aps: ☒ ON ☐ OFF

Channel Change Threshold: [Default: -82, Range: -99 to -1]

Managed AP CH Conflict Threshold: [Default: -56, Range: -99 to -1]

Save Cancel

図 5-3 RF Channel Settings 画面 - Interval

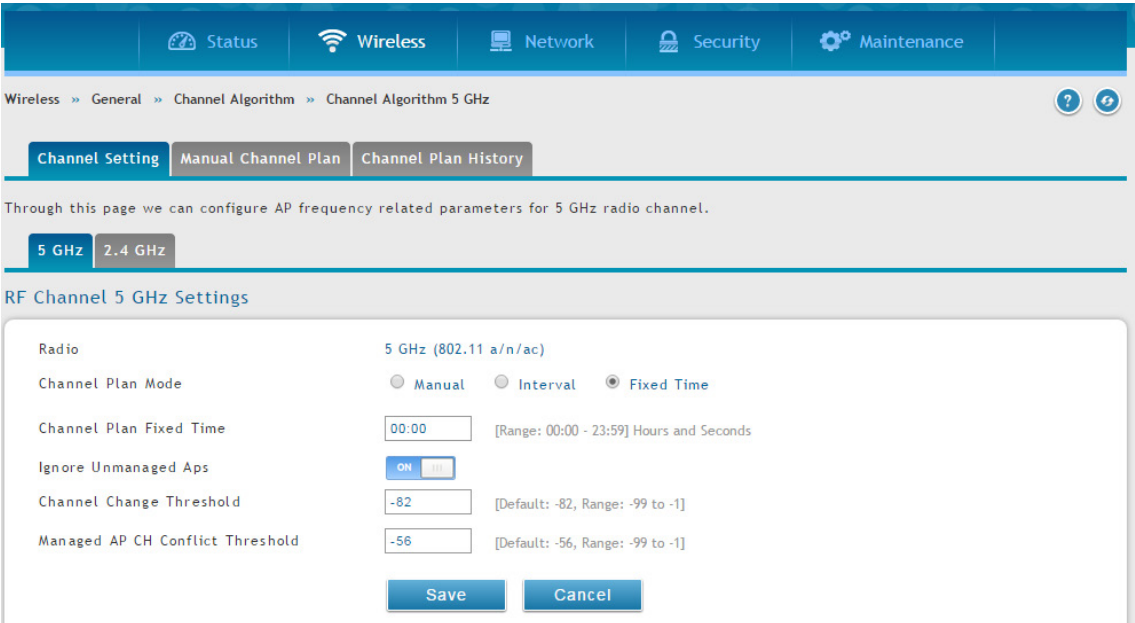


図 5-4 RF Channel Settings 画面 - Fixed Time

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です。802.11a/nおよび802.11b/g/nモードは異なるチャンネルを使用します。チャンネルプランを設定する前に、無線モードを選択します。「5GHz」または「2.4GHz」タブのいずれかをクリックします。
Channel Plan Mode	チャンネルプランのモードを選択します。 <ul style="list-style-type: none">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に、チャンネル計画を再始動する、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は -82dBm です。
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。
Manual Channel Plan	「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	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。

2. 「Save」ボタンをクリックします。

送信電力設定

Wireless > General > Power Algorithm メニュー

アクセスポイントの無線送信電力は、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電力レベルは、アクセスポイントの初期値のレベルであり、送信電力は 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。手動で送信電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電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. 最大送信電力が、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、最大送信電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. 送信電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、送信電力の変更を開始します。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。アクセスポイントがいくつかの作業を行うので、コントローラは、WIDS の操作プロパティを変更するために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。

多くのテストが管理 SSID を通知しているが、本当は管理アクセスポイントではないアクセスポイントを識別することに焦点を合わせています。そのようなアクセスポイントの検出は、ネットワークが誤設定されたか、またはハッカーがパスワードや他のセキュアな情報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。

操作可能なモードの無線電波で、多くの脅威を検出できます。しかし、sentry モードでは特に潜在的に不正なものが、管理対象アクセスポイントの無線モードのいずれとも異なるチャンネルで動作している場合に、より速く脅威を検出できます。ネットワーク内のあらゆる場所において sentry 無線電波を適用可能にできるように、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。

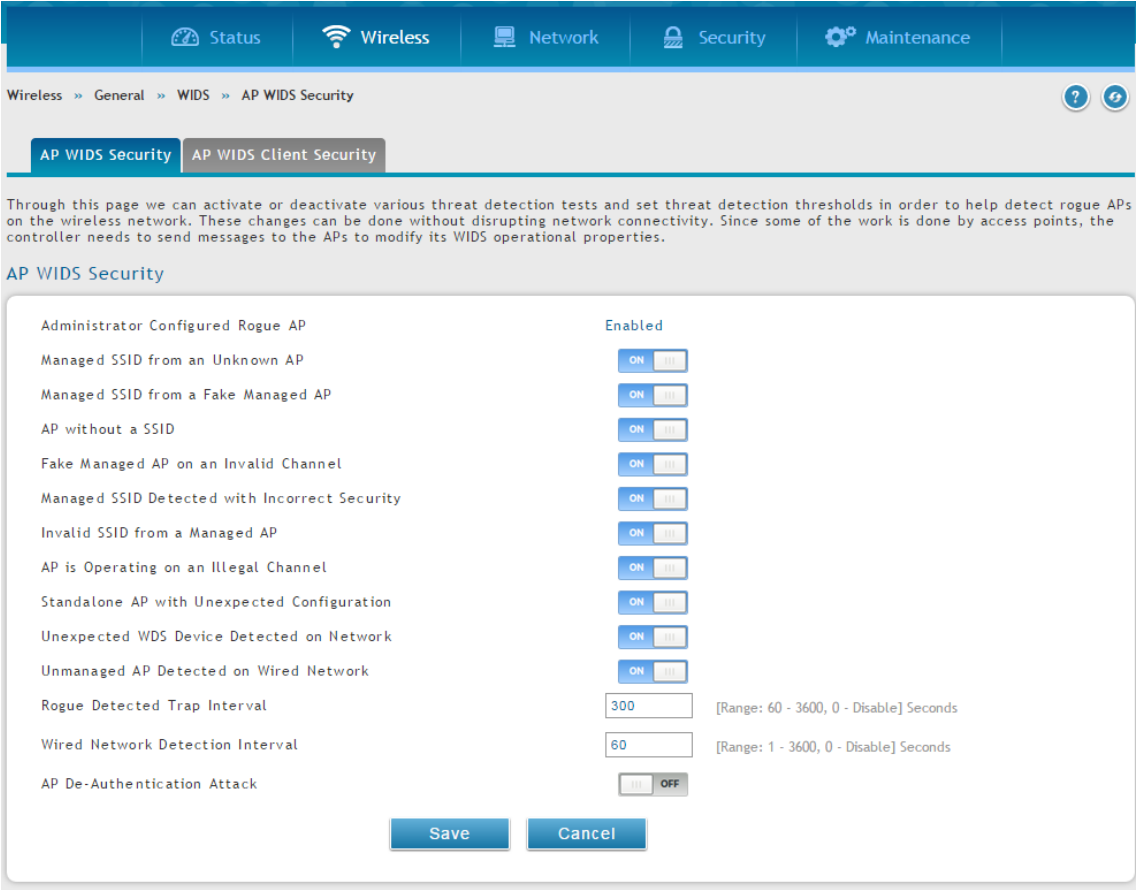


図 5-7 AP WIDS Security 画面

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。

項目	説明
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の接続、パスワードや他のセキュアな情報の開示を行うかもしれません。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、アクセスポイントにはせ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。検出を回避するために、ハッカーは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するかもしれませんが、ビーコンフレームの SSID 伝送を無効にします。アクセスポイントは、まだ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 に対してプロブ要求を送信するクライアントにプロブ応答を送信します。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	管理対象のアクセスポイントのうち、1 つの送信元 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が、アクセスポイントが動作していると思われるチャンネルとは違うチャンネルで検出されます。
Managed SSID Detected 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	<p>ハッカーまたは無線システムが設定される国では合法でないチャンネルで動作する、不正に設定されたデバイスを検出します。</p> <p>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。</p>
Standalone AP with Unexpected Configuration	<p>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予期された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に予期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。</p> <ul style="list-style-type: none"> • 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に検出される場合、アクセスポイントは「Rogue」（不正）と見なされます。WDS モードで明らか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だけが、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に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に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、ネットワークに検出されると、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、認知されないアクセスポイントは「Rogue」として分類され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 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補助します。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に絶えず注意を払います。「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どんなクライアントも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。

The settings we configure on the WIDS Client Configuration page help determine whether a detected client is classified as a rogue. Clients classified as rogues are considered to be a threat to network security.

AP WIDS Client Security

Not Present in OUI Database Test	<input type="button" value="OFF"/>
Not Present in Known Client Database Test	<input type="button" value="OFF"/>
Configured Authentication Rate Test	<input type="button" value="ON"/>
Configured Probe Requests Rate Test	<input type="button" value="ON"/>
Configured De-Authentication Requests Rate Test	<input type="button" value="ON"/>
Maximum Authentication Failures Test	<input type="button" value="ON"/>
Authentication with Unknown AP Test	<input type="button" value="OFF"/>
Client Threat Mitigation	<input type="button" value="OFF"/>
Known Client Database Lookup Method	<input type="button" value="ON"/>
Known Client Database Radius Server Name	<input type="text" value="Default-RADIUS-Server"/>
Rogue Detected Trap Interval	<input type="text" value="300"/> [Range: 60 - 3600, 0 - Disable] Seconds
De-Authentication Requests Threshold Interval	<input type="text" value="60"/> [Range: 1 - 3600] Seconds
De-Authentication Requests Threshold Value	<input type="text" value="10"/> [Range: 1 - 99999]
Authentication Requests Threshold Interval	<input type="text" value="60"/> [Range: 1 - 3600] Seconds
Authentication Requests Threshold Value	<input type="text" value="10"/> [Range: 1 - 99999]
Probe Requests Threshold Interval	<input type="text" value="60"/> [Range: 1 - 3600] Seconds
Probe Requests Threshold Value	<input type="text" value="120"/> [Range: 1 - 99999]
Authentication Failure Threshold Value	<input type="text" value="5"/> [Range: 1 - 99999]

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ー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、または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に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に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に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	クライアントがプローブ要求の送信のために設定レート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	<ul style="list-style-type: none"> ON - Known Clients データベースにあるが、Unknown (未知) のアクセスポイントに接続していないクライアントに認証解除メッセージを送信します。Unknown AP テストを使用する認証を、緩和が行われるために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残ります。
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 であれば、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カウントするのにアクセスポイントが使う時間 (秒) を指定します。
De-Authentication Requests Threshold Value	しきい値の間、コントローラが指定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カウントするのにアクセスポイントが使う時間 (秒) を指定します。
Authentication Requests Threshold Value	しきい値の間、コントローラが指定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カウントするのにアクセスポイントが使う時間 (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は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は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 Tunnel メニュー

1. Wireless > General > 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。

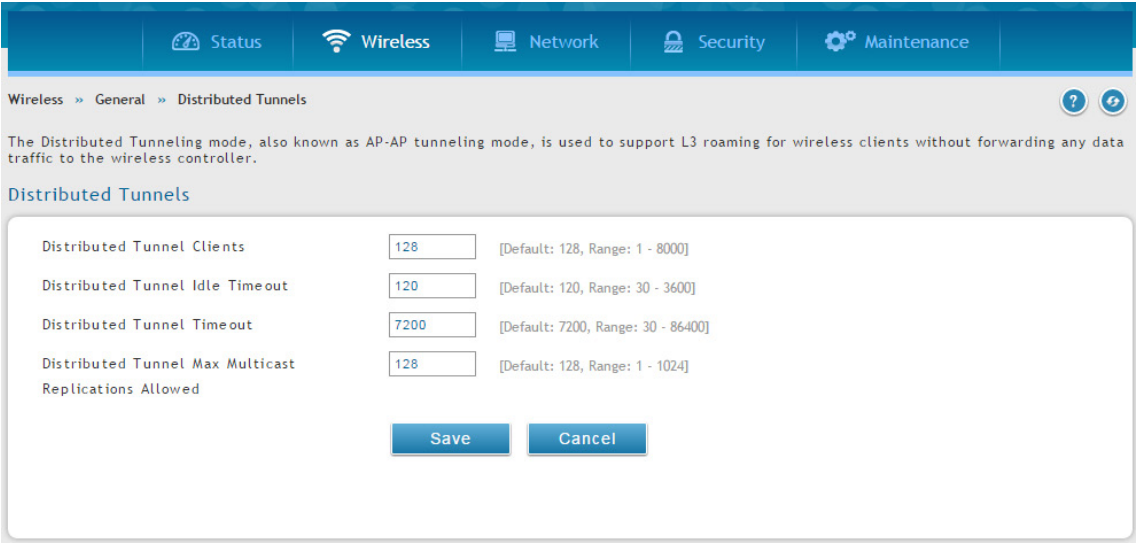


図 5-9 Distributed Tunnels 画面

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 視覚化

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。WLAN Visualization グラフは自身の背景画像を持っておらず、管理者が、ワイヤレスネットワーク内の AP やコントローラのワイヤレストポロジを提供する画像をアップロードすることができます。

画像のアップロード

Wireless > General > WLAN Visualization メニュー

オフィスの見取り図など、1 つ以上の画像をアップロードして、WLAN Visualization 機能にカスタマイズした情報を提供します。

アップロードに推奨される画像ファイルの形式は以下の通りです。

- GIF (Graphics Interchange Format)
- JPG (Joint Photographic Experts Group)
- ファイルサイズが 200KB 以下

WLAN コンポーネントが目立たなくなるため、カラー画像をご使用にならないことをお勧めします。

画像ファイルをアップロードして動作中の設定を保存すると、その画像はコントローラに登録され、WLAN Deployment アプリケーションを使用することで、既存のグラフに割り付けることができます。

画像の登録

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

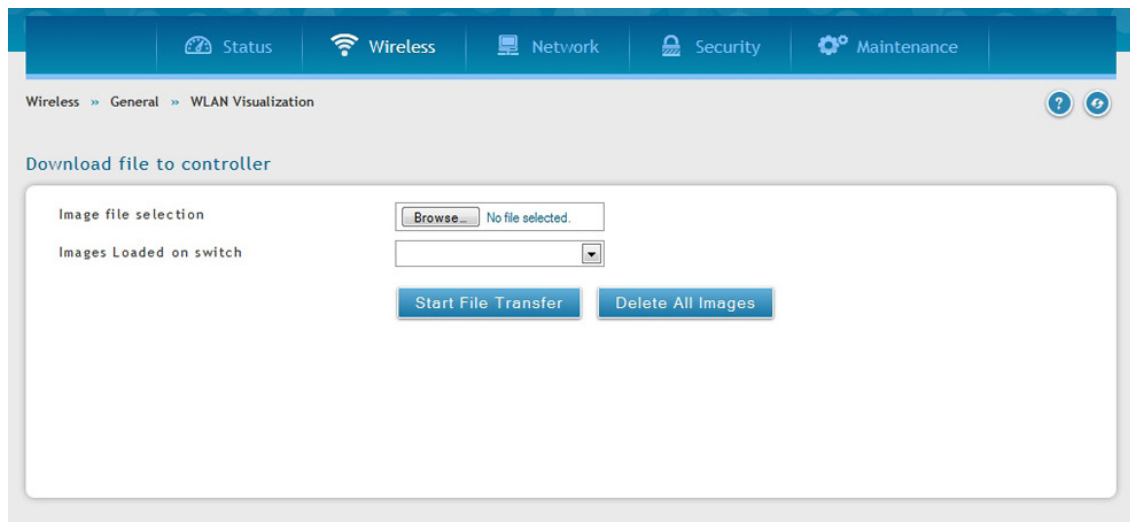


図 5-10 Upload WLAN Visualization 画面

2. 「Image file selection」で「ファイルを選択 (Browse)」をクリックします。
3. ファイルを選択して、「開く (Open)」をクリックします。
4. 「Start File Transfer」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」に表示されます。

画像の削除

画像が既にコントローラにロードされている場合にだけ、本機能は利用可能です。コントローラにロードされているすべてのイメージを削除するには「Delete All Images」をクリックします。背景画像を削除するのは推奨されません。しかし、ユーザの用途により画像を削除しなければならない場合は、画像を削除した後に WLAN Visualization ツールをリフレッシュする必要があります。

起動

Wireless > General > WLAN Visualization メニュー

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

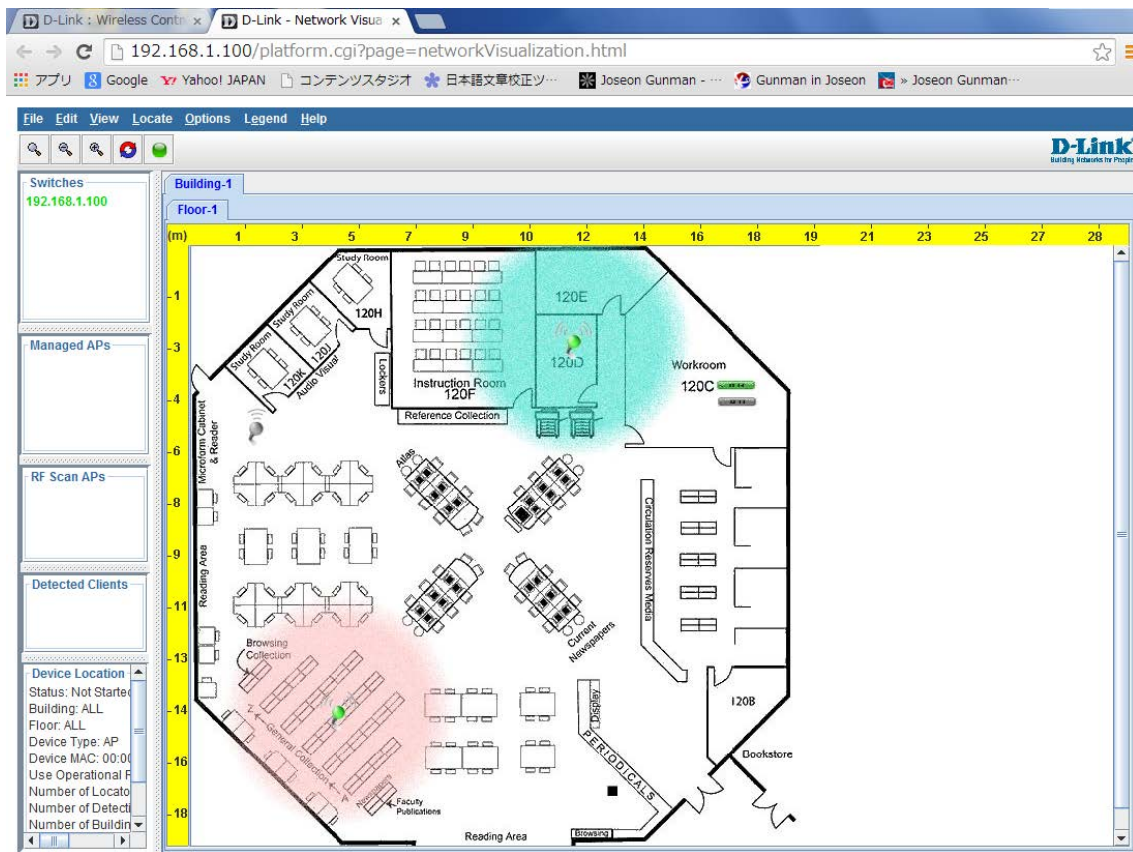


図 5-11 WLAN Visualization 画面

新しいブラウザ画面を開き、(カスタム背景画像のあるなしにかかわらず) アクセスポイントと WLAN コントローラのネットワークをトポロジの図として表示する Java アプレットを起動します。

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 > Discovered 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 > Discovered AP 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。

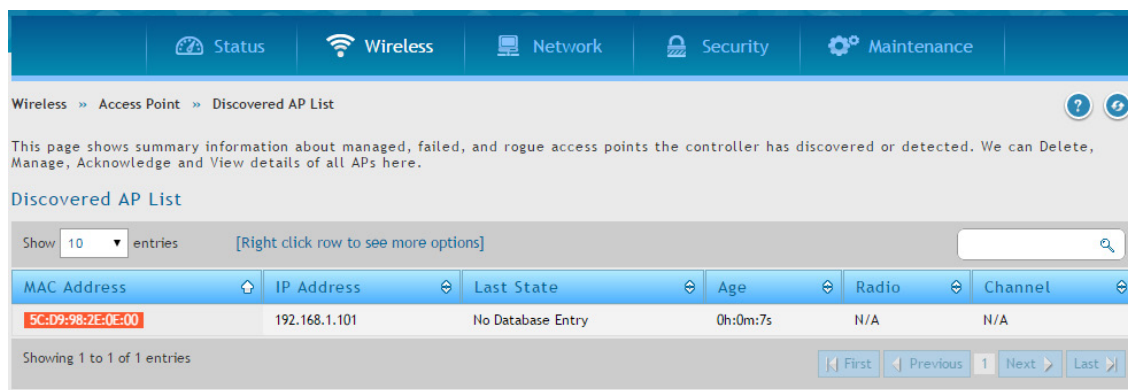


図 5-12 Discovered AP List 画面

コントローラがアクセスポイントを検出したかどうかの情報を表示します。

アクセスポイントを表示する「Discovered AP List」における MAC アドレスのカラーは以下の通りです。

- ・ 緑 - 管理されているアクセスポイント
- ・ 赤 - 接続に失敗したアクセスポイント、またはローカルまたは RADIUS Valid AP データベースにはないアクセスポイント (D-Link UAP)。
- ・ グレー - 未知のアクセスポイント、または不正なアクセスポイント
- ・ 橙 - ピアコントローラに管理されているアクセスポイント

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。

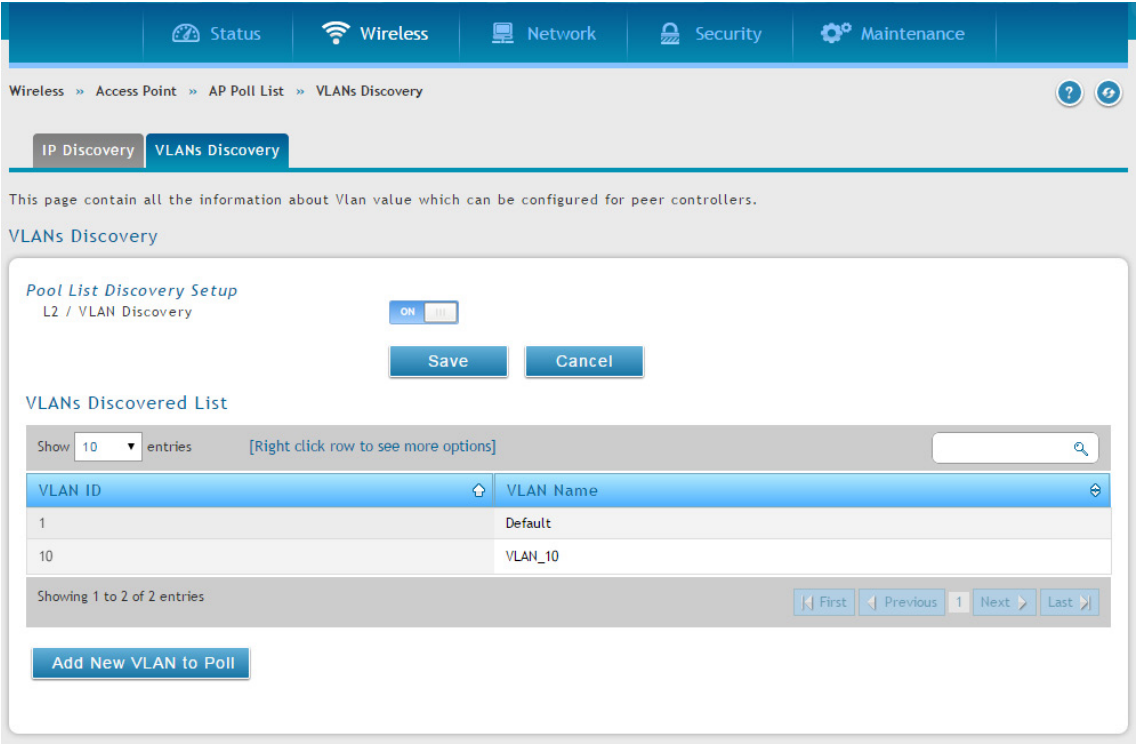


図 5-13 VLANs Discovery 画面

- 2. 「L2/ VLAN Discovery」を「ON」に切り替えて、「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。

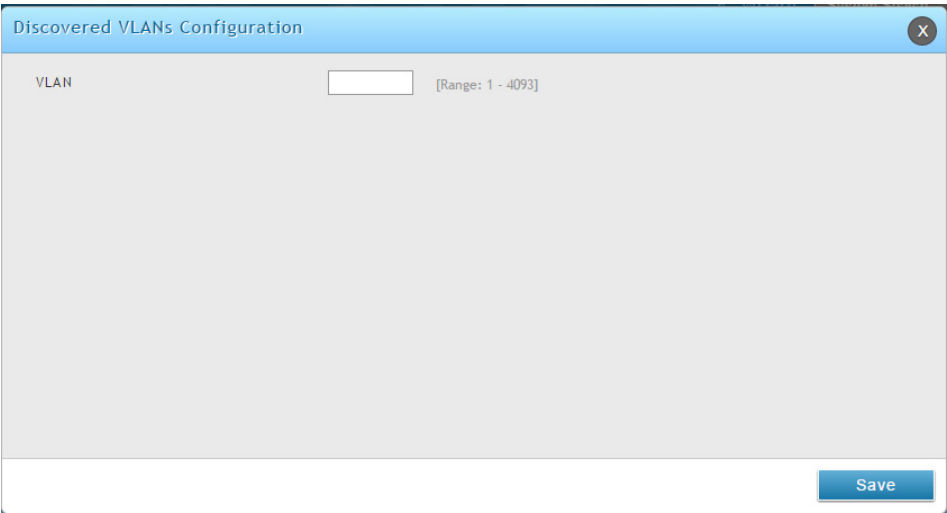


図 5-14 Discovered VLANs Configuration 画面

- 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。

Wireless > Access Point > AP Poll List > IP Discovery

IP Discovery | VLANs Discovery

This page contain all the information about IP Address which can be configured for peer controllers. The IP Discovery list can contain the IP addresses of peer controller and APs for the controller to discover and associate with as part of the WLAN.

IP Discovery

Pool List Discovery Setup
L3 / IP Discovery

ON

Save Cancel

IP Discovered List

Show 10 entries [Right click row to see more options]

IP Address	Status
192.168.1.101	Discovered-Failed
192.168.1.102	Polled
192.168.1.103	Polled
192.168.1.104	Polled
192.168.1.105	Polled

Showing 1 to 5 of 5 entries

First Previous 1 Next Last

Add New IP Addresses to Poll

図 5-15 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。

Discovered IP Addresses Poll Configuration

Start IP Address

End IP Address

Save

図 5-16 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。
5. **Wireless > Access Point > Discovered AP 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。

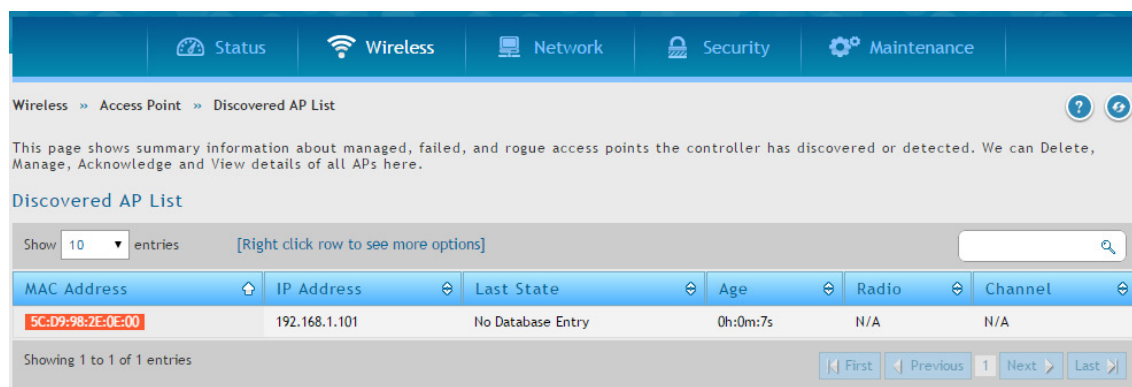


図 5-17 Discovered AP List 画面

L3/IP 検出を通じて発見されたアクセスポイントをチェックします。

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。追加 / 削除、送信電力 / チャンネルの変更、または個別に AP プロファイルを変更が可能です。

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 > Managed APs List > Valid APs メニュー

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

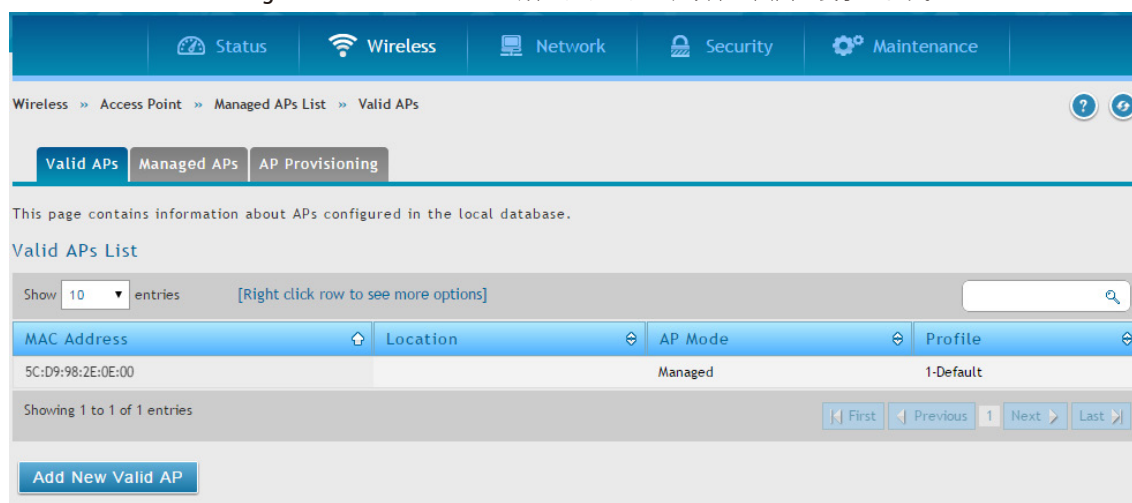


図 5-18 Valid APs List 画面

2. 「Add New Valid AP」ボタンをクリックします。画面は「AP Mode」によって異なります。

The dialog box titled "Valid APs Configuration" has a close button (X) in the top right corner. It contains the following fields and options:

- MAC Address: Text input field.
- AP Mode: Radio buttons for **Managed** (selected), Standalone, and Rogue.
- Location: Text input field, labeled "Optional".
- Authentication Password: Toggle switch set to **OFF**.
- Profile: Dropdown menu showing "1-Default".
- Radio 802.11a/n:
 - Channel: Dropdown menu showing "Auto".
 - Power: Dropdown menu showing "Profile".
- Force Roaming: Toggle switch set to **OFF**.
- Force Roaming Threshold: Text input field showing "20", with a range "[Range: 20 - 50] Seconds".
- Radio 802.11b/g/n:
 - Channel: Dropdown menu showing "Auto".
 - Power: Dropdown menu showing "Profile".
- Force Roaming: Toggle switch set to **OFF**.
- Force Roaming Threshold: Text input field showing "20", with a range "[Range: 20 - 50] Seconds".

A "Save" button is located at the bottom right of the dialog box.

図 5-19 Valid APs Configuration 画面 - Managed モード

The dialog box titled "Valid APs Configuration" has a close button (X) in the top right corner. It contains the following fields and options:

- MAC address: Text input field.
- AP Mode: Radio buttons for Managed, **Standalone** (selected), and Rogue.
- Location: Text input field, labeled "Optional".
- Expected SSID: Text input field.
- Expected Channel: Dropdown menu showing "Any".
- Expected WDS Mode: Radio buttons for **Any** (selected), Normal, and bridge.
- Expected Security Mode: Dropdown menu showing "Any".
- Expected Wired Network Mode: Radio buttons for **Allowed** (selected) and Not Allowed.

A "Save" button is located at the bottom right of the dialog box.

図 5-20 Valid APs Configuration 画面 - Standalone モード

The dialog box titled "Valid APs Configuration" has a close button (X) in the top right corner. It contains the following fields and options:

- MAC address: Text input field.
- AP Mode: Radio buttons for Managed, Standalone, and **Rogue** (selected).
- Location: Text input field, labeled "Optional".

A "Save" button is located at the bottom right of the dialog box.

図 5-21 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。 <ul style="list-style-type: none"> 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 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オンにします。
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。
「Radio 802.11a/n」「Radio 802.11b/g/n」	
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	強制ローミングを有効 / 無効にします。
Force Roaming Threshold	強制ローミングのしきい値を指定します。

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。

注意

Valid AP リストでアクセスポイントを追加、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。

Discovered AP List からアクセスポイントを追加する

Wireless > Access Point > Discovered AP List メニュー

1. Wireless > Access Point > Discovered AP 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。

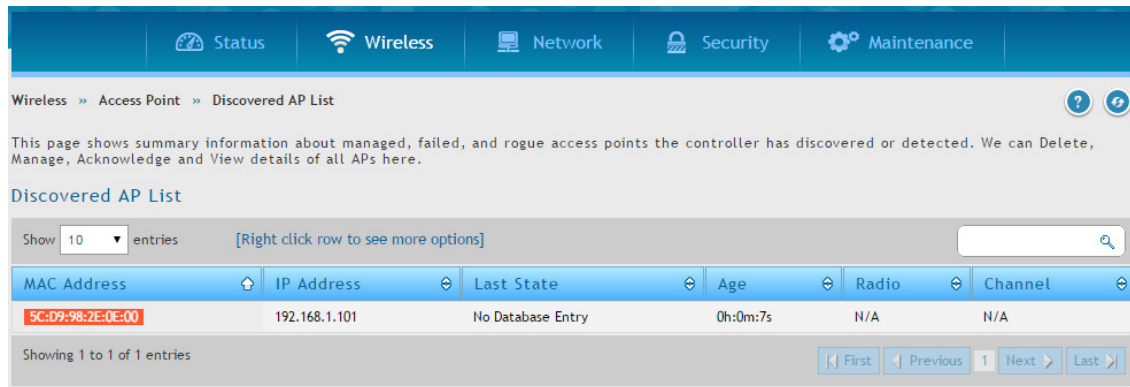


図 5-22 Discovered AP List 画面

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。

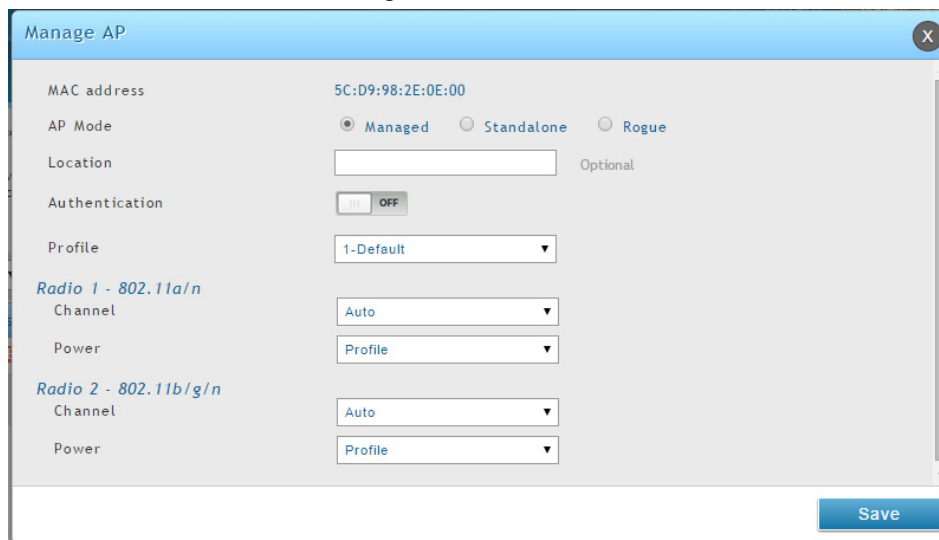


図 5-23 Managed AP 画面

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電力の手動変更

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

「Managed AP」画面から、アクセスポイントの各無線インタフェースに対して、手動で RF チャンネルと送信電力を変更することもできます。手動による電力とチャンネルの変更は、アクセスポイントのプロファイル（自動チャンネル選択を含む）に設定された内容を上書きして、直ちに適用されます。アクセスポイントがコントローラとの接続を解除し、再び接続する場合など、アクセスポイントがリセットされる場合、または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に、手動のチャンネルと電力割り当ては保持されません。

1. Wireless > Access Point > Managed APs List > Managed 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。

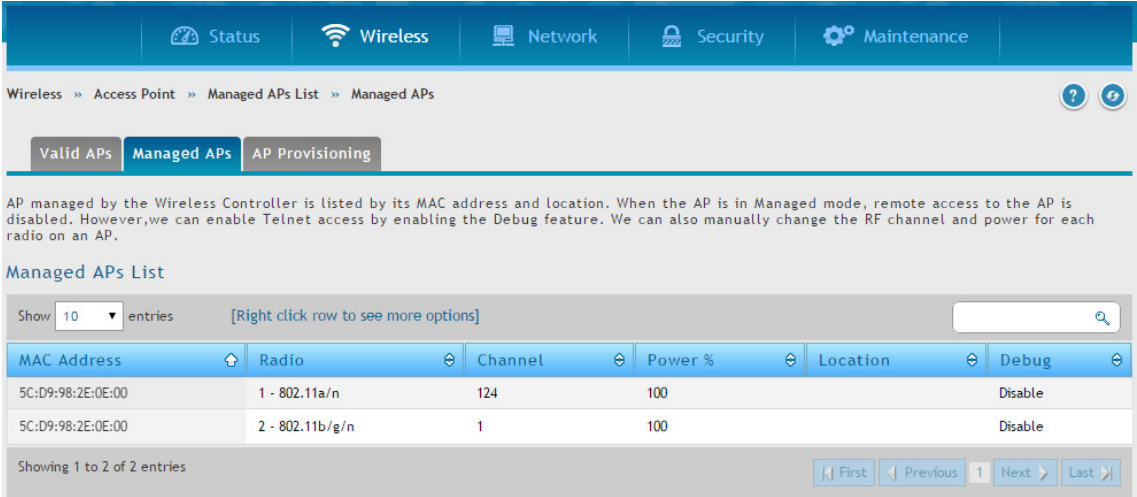


図 5-24 Managed APs List 画面

2. エントリの 1 つで右クリックし、「Channel and Power」を選択すると、以下の画面が表示されます。

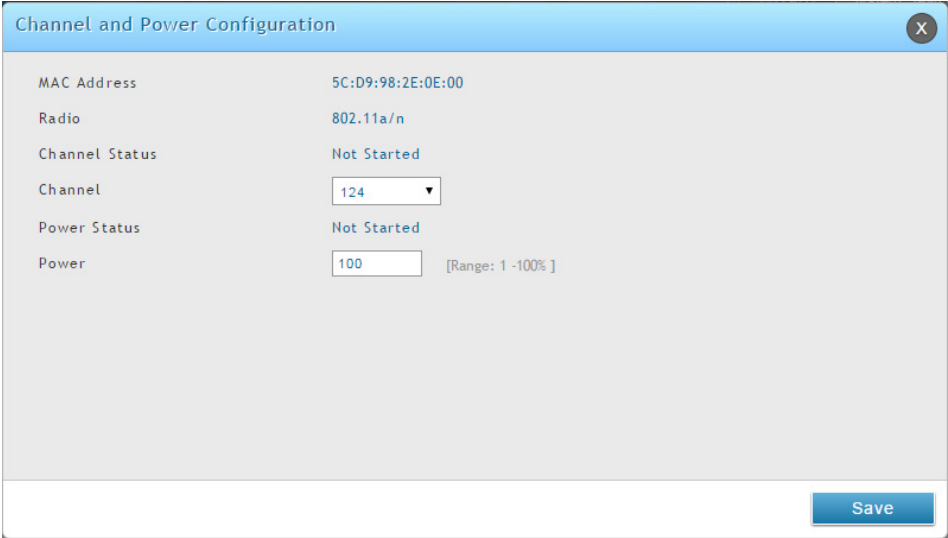


図 5-25 Channel and Power Configuration 画面

3. 希望するチャンネルを選択します。使用できるチャンネルは、無線モードとアクセスポイントを使用する国によって異なります。手動のチャンネル変更は、アクセスポイントのプロファイルに設定されたチャンネルを上書きすると、アクセスポイントの再起動時、またはアクセスポイントのプロファイルが再度使用される場合には保持されません。
4. 希望する送信電力を選択します。アクセスポイントに新しい電力レベルを設定します。手動の電力変更によりアクセスポイントのプロファイルに設定された電力設定を上書きすると、アクセスポイントの再起動時、またはアクセスポイントのプロファイルが再度使用される場合には保持されません。
5. 「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 > Managed APs List > Managed APs 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。しかし、「Managed APs」ページで、デバッグ機能を有効にすることで Telnet によりアクセスすることが可能です。

1. Wireless > Access Point > Managed APs List > Managed 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。

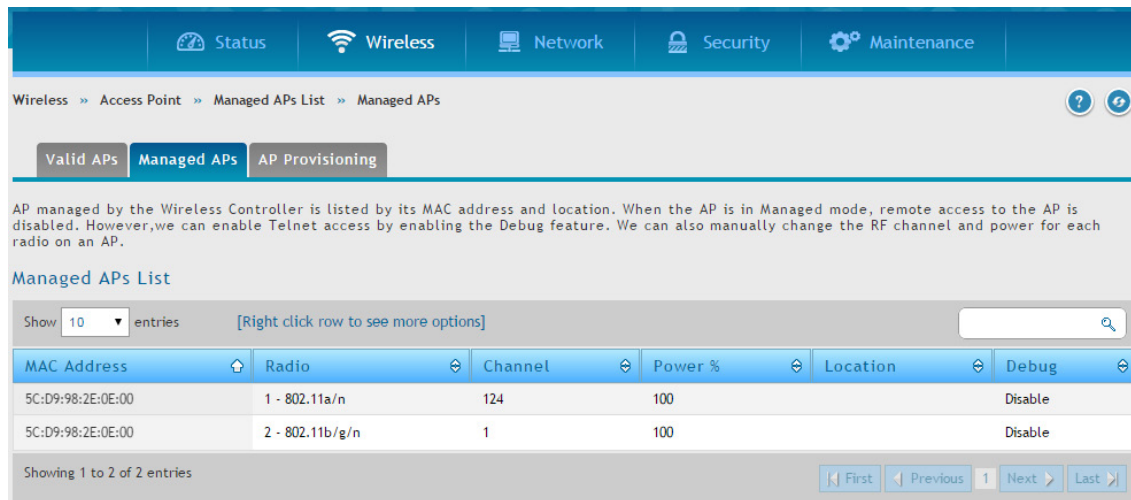


図 5-26 Managed APs List 画面

2. エントリの1つで右クリックし、「AP Debug」を選択します。

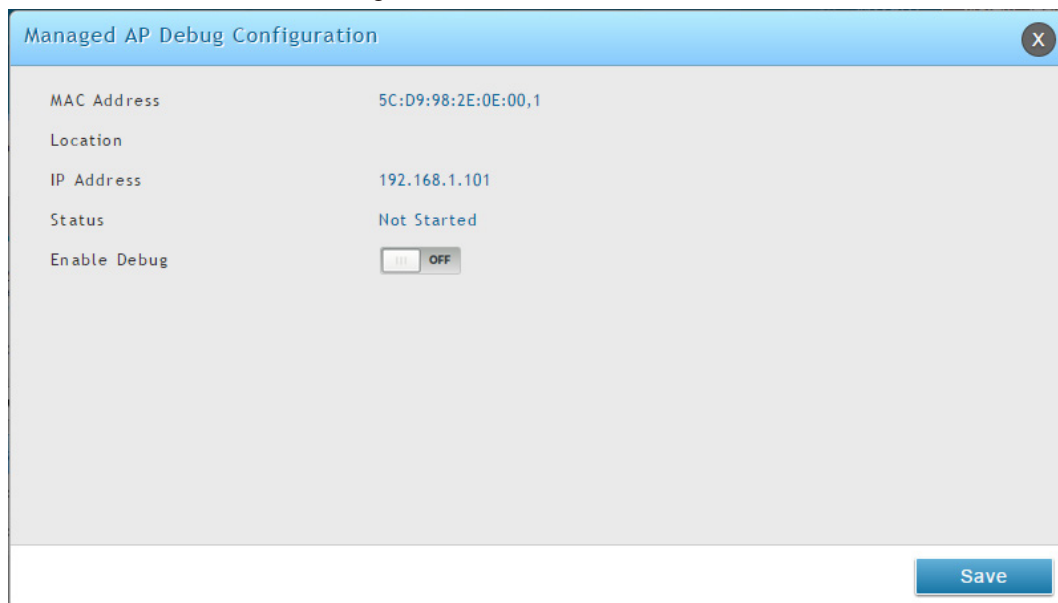


図 5-27 Managed AP Debug Configuration 画面

3. 「Enable Debug」を「ON」に切り替えます。
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 > Managed 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) に対して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、相互認証がクラスタへのアクセスポイント接続を簡素化するために有効でないネットワークにおいて、オプションで使用できます。

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 > Managed 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。

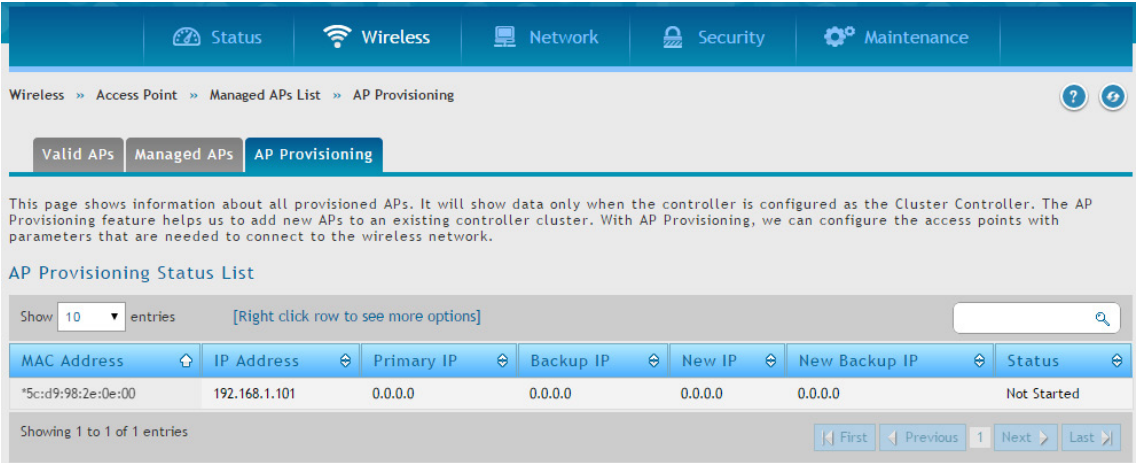


図 5-28 AP Provisioning Status List 画面

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 5-29 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。以下の項目の 1 つです。 <ul style="list-style-type: none">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。

項目	説明
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。 <ul style="list-style-type: none"> • 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のタイムアウト。
AP Certificate and Profile Transmit Status	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。 <ul style="list-style-type: none"> • 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。
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。
Profile	使用する AP プロファイルを選択します。

3. 新しいプライマリアドレス、新しいバックアップアドレス、および AP プロファイルを入力します。

4. 「Save」ボタンをクリックします。

AP プロファイル

アクセスポイントのコンフィグレーションプロファイルは、様々なユーザ層が使用するアクセスポイントを集約する、規模の大きな無線ネットワークに非常に有効な機能です。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、場所、機能または他の要素に基づいてアクセスポイントをカスタマイズできます。プロファイルとはテンプレートのようなもので、一度 AP プロファイルを作成すると、無線コントローラが管理するアクセスポイントにそれを適用できます。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 Profiles > 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。

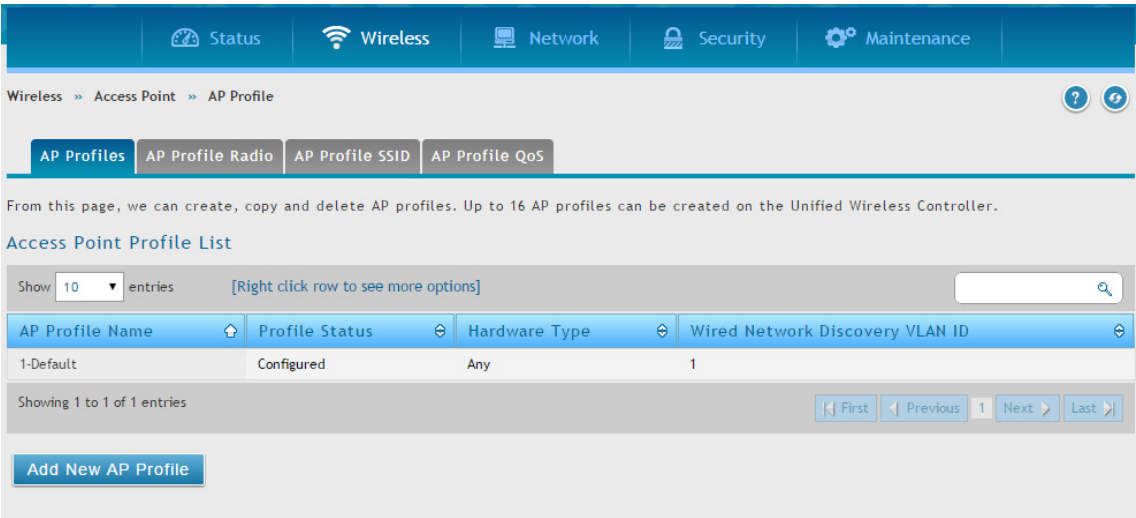


図 5-30 AP Profile List 画面

2. 「Add New AP Profile」 ボタンをクリックします。

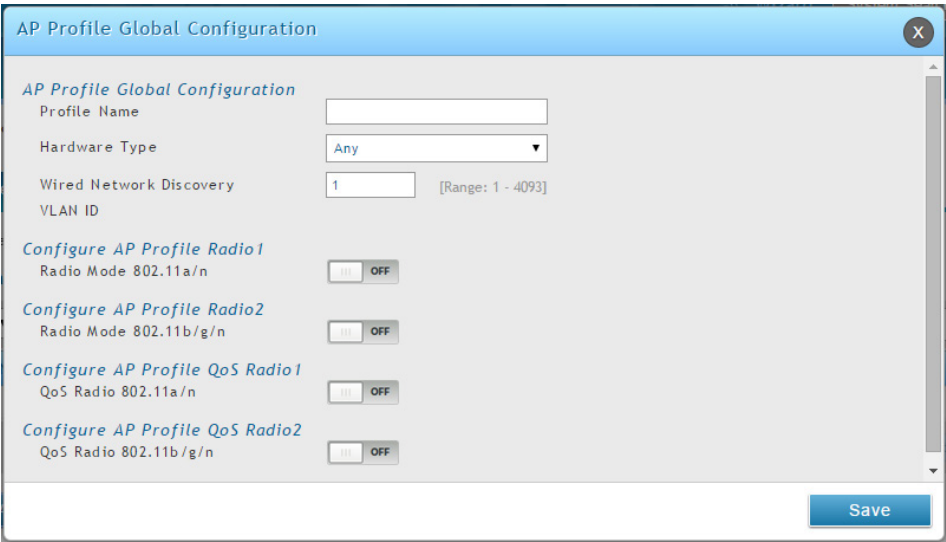


図 5-31 AP Profile Global Configuration 画面

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。

項目	説明
Hardware Type	<p>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（シングルまたはデュアル）と無線インタフェースがサポートする IEEE 802.11 モード（a/b/g/ または a/b/g/n）により決定されます。以下のオプションが利用できます。</p> <ul style="list-style-type: none"> すべて DWL-8600AP Dual Radio a/b/g/n DWL-6600AP Dual Radio a/b/g/n DWL-3600AP Single Radio b/g/n DWL-8610AP Dual Radio a/b/g/n/ac <p>注意 DWL-3600AP はアクセスポイント側のファームウェアが DWC-1000 をサポートしていないため未サポートです。</p>
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。
Configure AP Profile Radio 1	
Radio Mode 802.11a/n	新しい AP プロファイルでは、ここから無線電波 802.11a/n を編集できます。また、「AP Profile Radio」からも編集できます。
Configure AP Profile Radio 2	
Radio Mode 802.11b/g/n	新しい AP プロファイルでは、ここから無線電波 802.11b/g/n を編集できます。また、「AP Profile Radio」からも編集できます。
Configure AP Profile QoS Radio 1	
QoS Radio Mode 802.11a/n	新しい AP プロファイルでは、ここから無線電波 802.11a/n の QoS を編集できます。また、「AP Profile Radio」からも編集できます。
Configure AP Profile QoS Radio 2	
QoS Radio Mode 802.11b/g/n	新しい AP プロファイルでは、ここから無線電波 802.11b/g/n の QoS を編集できます。また、「AP Profile Radio」からも編集できます。

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

広帯域の無線クライアントと無線ネットワーク要求に適應するために、アクセスポイントは 2 個の周波数帯域をサポートしています。初期値では、Radio1 は IEEE 802.11a/n/ac モードで動作し、Radio2 は IEEE 802.11b/g/n モードで動作します。各モードの違いは、運用される周波数帯です。周波数帯域のうち、IEEE 802.11b/g/n は 2.4GHz 帯を使用し、IEEE 802.11a/n/ac は 5GHz 帯を使用します。

1. Wireless > Access Point > AP Profiles > 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。

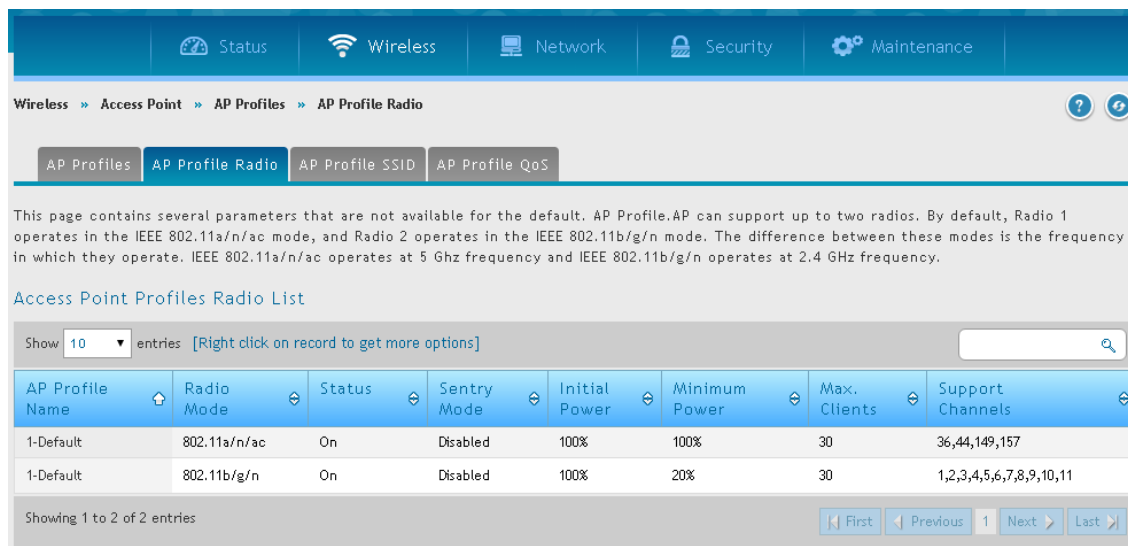


図 5-32 AP Profile Radio List 画面

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。

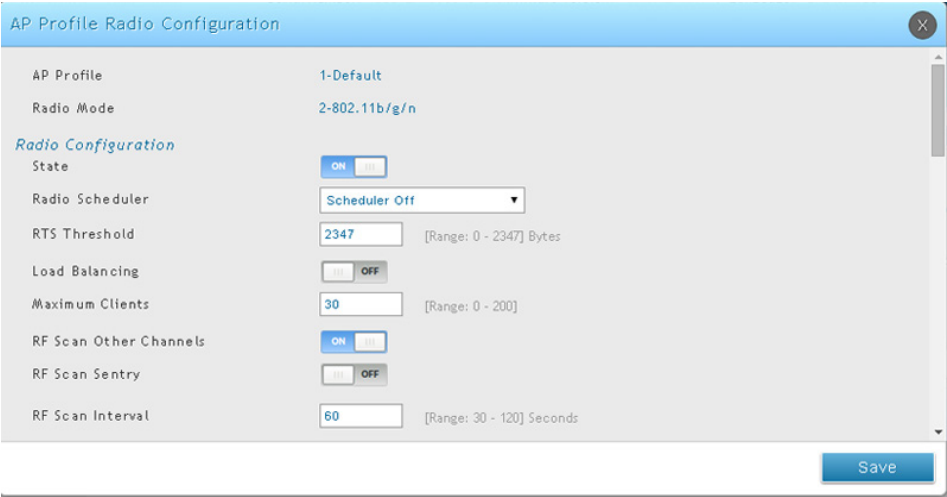


図 5-33 AP Profile Radio Configuration 画面

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	AP 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。: 802.11a/n/c または 802.11b/g/n
Radio Configuration	
State	無線インタフェースを「ON」(有効) または「OFF」(無効) オフにします。 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	設定済みのスケジューラを選択、または「Scheduler Off」でスケジューラを無効にします。
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 ハンドシェイ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、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。 <ul style="list-style-type: none">ON - 無線電波は定期的にオプション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	本オプションを選択すると、無線インタフェースは Sentry モードで動作することができます。「ON」に設定すると、無線インタフェースは、主として専用の 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。
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。
RF Scan Interval	RF スキャン中のチャンネル変更の間隔を制御します。初期値は 10 (ミリ秒) です。
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。

項目	説明
Mode	<p>無線帯域が使用する物理層 (PHY) の標準を定義します。各無線帯域に対して以下のモードから選択します。</p> <ul style="list-style-type: none"> IEEE 802.11a - OFDM 方式を使用して 5GHz 内の U-NII 帯域で動作することを指定する PHY の標準です。また 6-54Mbps の通信速度をサポートします。 IEEE 802.11b/g - 2.4GHz ISM 帯で動作します。IEEE 802.11b は 5.5Mbps と 11Mbps データレートを含む初期の 802.11PHY の拡張です。これは、より高いデータレートを提供するために、相補型符号変調方式 (CCK) 並びに直接シーケンススペクトル拡散 (DSSS) または周波数ホッピング拡散スペクトル (FHSS) を使用します。また、1-11Mbps のデータレート範囲をサポートします。IEEE 802.11g は、802.11b PHY をより速い伝送速度 (最大 54Mbps) に拡張したものです。それは直交波周波数分割多重 (OFDM) を使用します。1-54Mbps の通信速度をサポートします。 IEEE 802.11a/n - 5GHz ISM 帯域で動作し、802.11a と 802.11n デバイスの両方のサポートしています。IEEE 802.11n は、MIMO (multiple-input multiple-output) 技術を含む 802.11 標準の拡張です。IEEE 802.11n は、最大 248Mbps のデータ範囲と、802.11b、802.11g、および 802.11a の屋内範囲の約 2 倍をサポートします。 IEEE 802.11b/g/n - 2.4GHz ISM 帯で動作し、802.11b、802.11g、および 802.11n デバイスのサポートしています。 5GHz IEEE 802.11n - 802.11a または 802.11b/g をサポートする必要がある 5GHz 周波数で動作する 802.11n デバイスを持つネットワークにお勧めのモードです。IEEE 802.11n は、レガシーデバイス (802.11b/g または 802.11a) と互換性が必要ない場合に、より高いスループットを実現できます。 2.4GHz IEEE 802.11n - 802.11a または 802.11b/g をサポートする必要がある 2.4GHz 周波数で動作する 802.11n デバイスを持つネットワークにお勧めのモードです。IEEE 802.11n は、レガシーデバイス (802.11b/g または 802.11a) と互換性が必要ない場合に、より高いスループットを実現できます。 IEEE 802.11n/ac - 5GHz ISM 帯で動作し、11n と 11ac デバイスの両方をサポートします。
DTIM Period	<p>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は、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しています。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。</p> <p>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。</p>
Beacon Interval	<p>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 (m 秒) に 1 度 (1 秒に 10 回) 送信されます。</p>
Automatic Channel	<p>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。</p> <p>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。</p>
Automatic Power	<p>送信電力レベルは、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。自動送信電力調整機能では、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電力を 10% の割合で増減します。</p>
Initial Power	<p>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電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。つまり、自動電力調整を有効にした場合、RF 信号送信電力は増加することがあっても減少しません。単位は RF 信号の最大送信電力に対する割合 (%) です。</p>
Minimum Power	<p>設定した無線インタフェースにおける送信電力の最小値 (1-100%) を指定します。</p>
APSD Mode	<p>「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。</p>
Frag Threshold	<p>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。</p>
Short Retries	<p>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。</p>
Long Retries	<p>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。</p>

項目	説明
Rate Limiting	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> 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 送信から送信リトライを終了までの時間（ミリ秒）を指定します。
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いずれも、常に適合し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	最初に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 再構築のリトライ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	<p>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。</p> <ul style="list-style-type: none"> 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。
Space Time Block Code	<p>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。</p> <ul style="list-style-type: none"> 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	強制ローミングを有効にします。
Force Roaming Threshold	強制ローミングのしきい値を指定します。
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。

AP プロファイル SSID の設定

Wireless > Access Point > AP Profiles > 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 Profiles > 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 5-34 AP 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」(「802.11a/n」または「802.11b/g/n」) を選択します。
4. プルダウンメニューから「SSID Name」を選択します。
5. 「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。

AP プロファイル QoS の設定

Wireless > Access Point > AP Profiles > 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、データ伝送動作をアクセスポイントにだけ適用され、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 Profiles > 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。

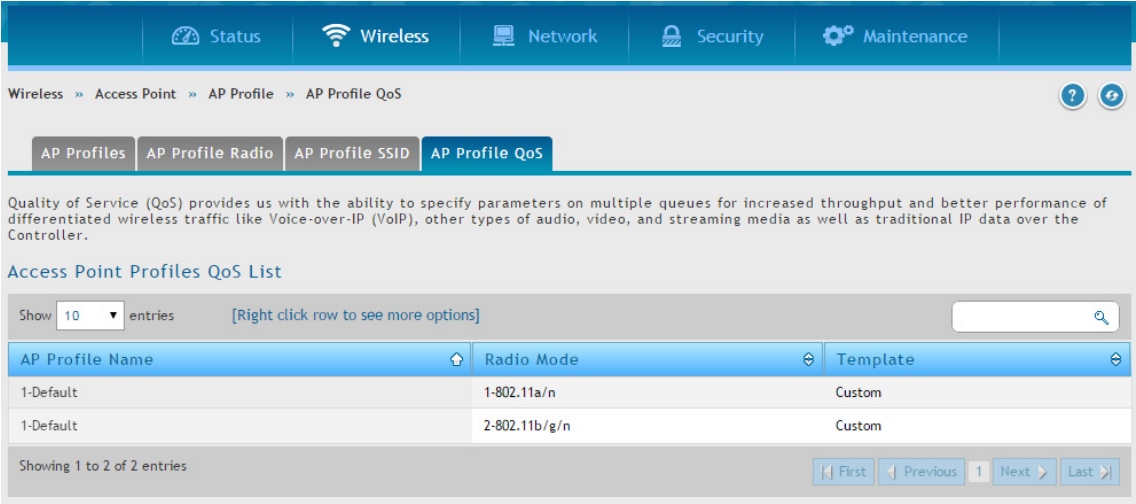


図 5-35 AP Profiles QoS List 画面

2. AP プロファイルを右クリックして、「Edit」を選択します。

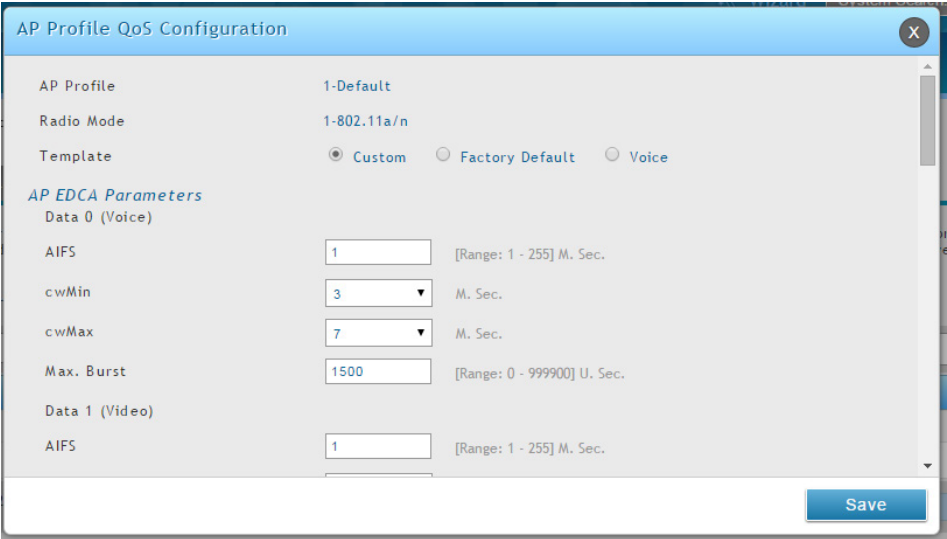


図 5-36 AP Profiles QoS Configuration 画面

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	無線帯域を表示します。: 802.11a/n または 802.b/g/n
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。 <ul style="list-style-type: none">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。

項目	説明
AP EDCA Parameters	
Queue	<p>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。</p> <ul style="list-style-type: none"> • 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 (最小コンテンション画面)	<p>本パラメータは、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。cwmin に対する有効な値は、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。</p>
cwMax (最大コンテンション画面)	<p>本パラメータは、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。</p>
Max. Burst	<p>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。オーバー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。最大バースト長に有効な値は 0 から 999900 です。</p>
WMM Mode	<p>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。</p> <ul style="list-style-type: none"> • 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。
Station EDCA Parameters	
Queue	<p>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。</p> <ul style="list-style-type: none"> • 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 (Inter-Frame Space)	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 (最小コンテンション画面)	<p>本パラメータは、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。</p>
cwMax (最大コンテンション画面)	<p>本パラメータは、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。</p>
TXOP Limit	<p>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。</p>

SSID プロファイル

SSID プロファイルリストでは、コントローラに設定されているすべての無線ネットワークを表示します。初期値では、最初に 16 個のネットワークが作成されます。デフォルトネットワークは変更できますが、削除することはできません。合計 50 個の無線ネットワークに最大 16 個のネットワークを追加および設定できます。マルチネットワークは同じ SSID を持つことができます。

SSID プロファイルの設定

Wireless > Access Point > SSID Profiles メニュー

1. Wireless > Access Point > SSID 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。

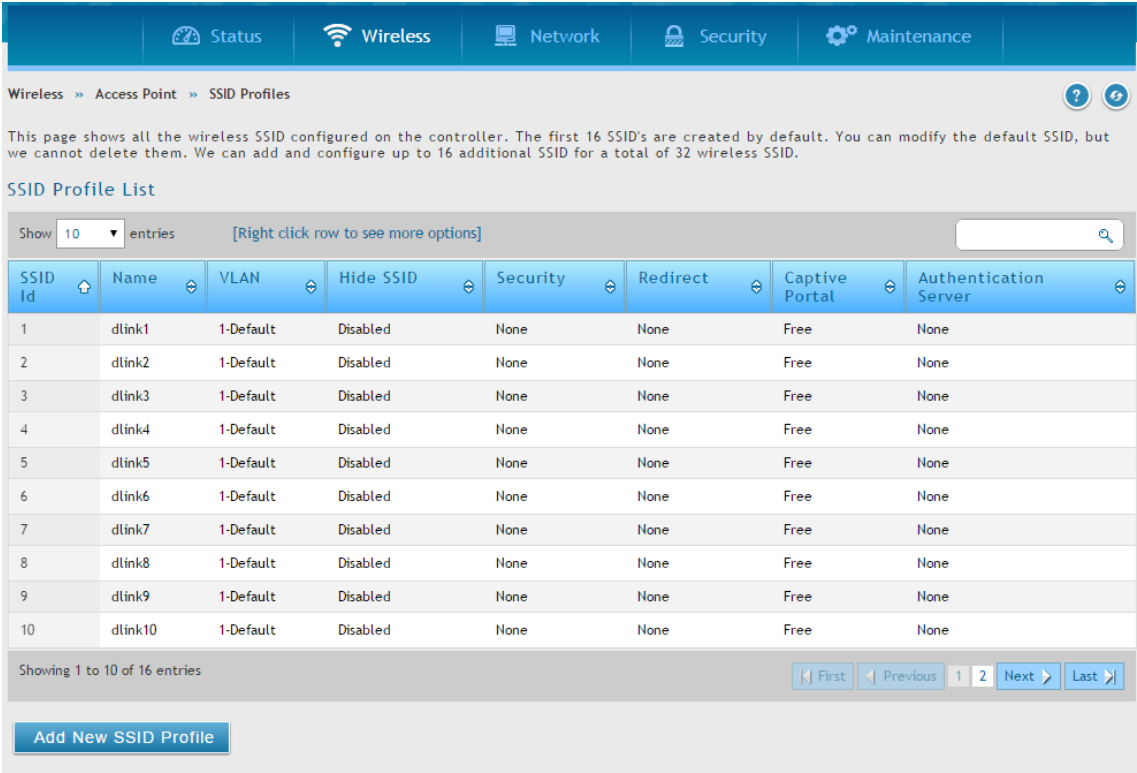


図 5-37 SSID Profile List 画面

2. 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。

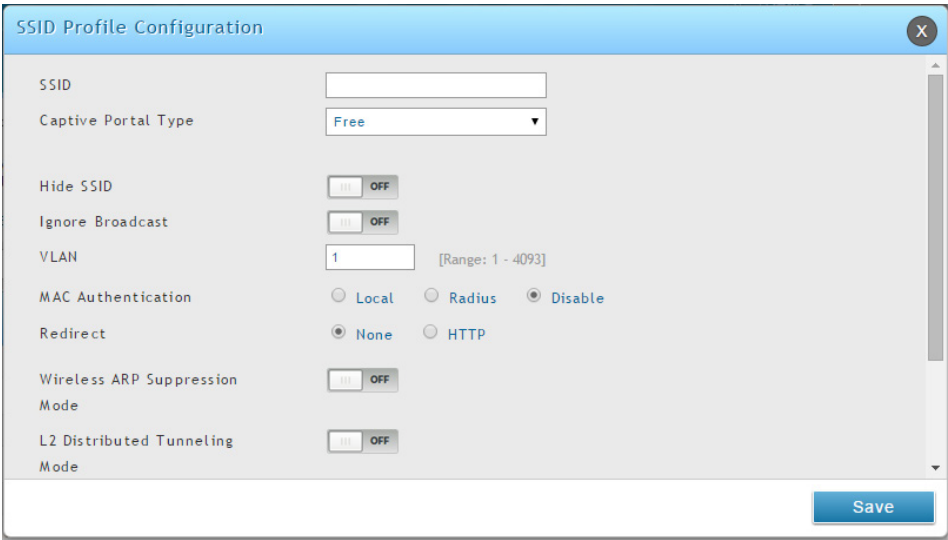


図 5-38 SSID Profile Configuration 画面

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。

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
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。 <ul style="list-style-type: none"> 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。
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
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、サブ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。しかし、ハッカーからの簡単な攻撃を防いだり、暗号化されていないトラフィックを監視するためには十分ではありません。 <ul style="list-style-type: none"> ON - SSID は隠されます。 Off - SSID はブロードキャストされます。
Ignore Broadcast	無線クライアントが利用可能なすべての SSID にプローブ要求をブロードキャストする場合、本オプションは、アクセスポイントがプローブ要求に応答するかどうかを制御します。 <ul style="list-style-type: none"> ON - アクセスポイントがクライアントプローブ要求に応答することを禁止します。 OFF - アクセスポイントがクライアントプローブ要求に応答することを許可します。
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)
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。 <ul style="list-style-type: none"> 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。
Redirect	カスタム Web 画面に無線クライアントをリダイレクトするために、「Redirect」欄の HTTP オプションを選択します。本モードが有効であると、無線クライアントがアクセスポイントに接続し、インターネットにアクセスするために Web ブラウザをオープンした後、指定した URL にリダイレクトされます。カスタム Web 画面は、外部の Web サーバにおかれる必要があります、会社のロゴやネットワーク利用ポリシーなどの情報を含む可能性があります。 <div> 注意 無線クライアントは一度アクセスポイントに接続すると外部の Web サーバにリダイレクトされます。リダイレクト機能では、キャプティブポータル機能を実行できます。キャプティブポータルは、ホットスポットプロバイダのブランディングの提供、および（または）免責事項の表示のために Wi-Fi ホットスポットで使用されます。ユーザはクリックスルーすることによりインターネットに接続できます。 <ul style="list-style-type: none"> HTTP - HTTP リダイレクトは有効です。 None - HTTP リダイレクトは無効です。 </div>
Redirect URL	「Redirect」が「HTTP」である場合、すべての初期の HTTP アクセスがリダイレクトされるべきである URL を入力します。「HTTP」がリダイレクトタイプとして選択されている場合にだけ、本項目は表示されます。

項目	説明
Wireless ARP Suppression Mode	<p>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。</p> <p>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。</p>
L2 Distributed Tunneling Mode	<p>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。</p> <p>注意</p> <ol style="list-style-type: none"> 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、それが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。 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。 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。
RADIUS Authentication Server Status	RADIUS 認証サーバを VAP に設定するかどうかを示します。
Security	<p>デフォルト AP プロファイルは、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によるネットワークへのアクセスを防止することをお勧めします。</p> <ul style="list-style-type: none"> None - どのセキュリティメカニズムも使用されません。 WEP - WEP セキュリティを有効にします。表 4-1 のオプションを入力します。 WPA/WPA2 - WPA/WPA2 セキュリティを有効にします。表 4-2 のオプションを入力します。

WDS 設定

WDS (Wireless Distribution System) は管理対象のアクセスポイントの機能で、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。アクセスポイントは、WDS を使用して、ネットワークへの優先接続ができない屋外やに有線ネットワークを使用したメインキャンパスに接続していない離れたビルにおかれる可能性があります。

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。WDS リンクは、WPA2 Personal 認証と AES 暗号化を使用して守られます。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。
- 1 つのアクセスポイントは 1 つの WDS AP グループだけのメンバとなります。
- 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。

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は、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 1 つを使用します。
 - サテライト AP をスタンドアロンモードに設定する場合には、「Radio」ページを使用して、スタティックなチャンネルを設定します。
 - アクセスポイントを Valid AP データベースに設定する場合は、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。

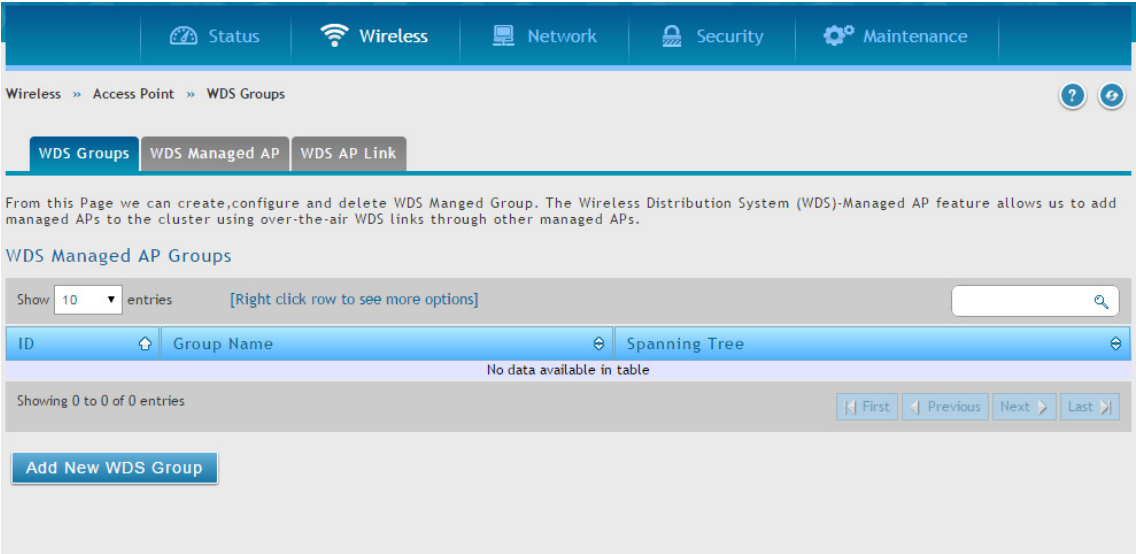


図 5-39 WDS Managed AP Groups 画面

2. 「Add New WDS Group」 ボタンをクリックします。

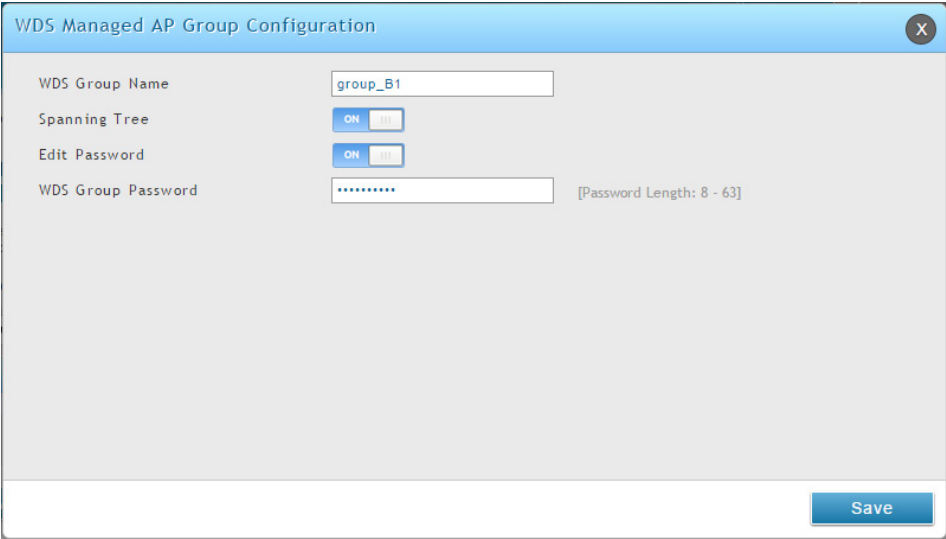


図 5-40 WDS Managed AP Group Configuration 画面

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。

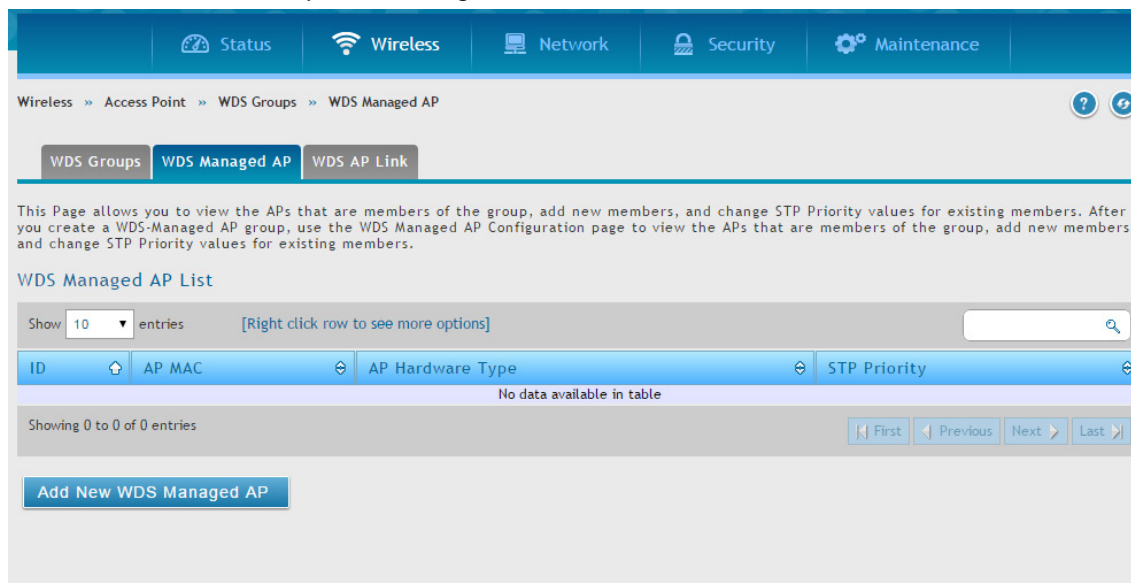


図 5-41 WDS Managed AP List 画面

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 5-42 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	<p>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。</p> <p>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。サテライト AP よりも有線ネットワークに接続するアクセスポイントに低い優先度を割り当てるべきです。</p> <p>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。</p>

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。

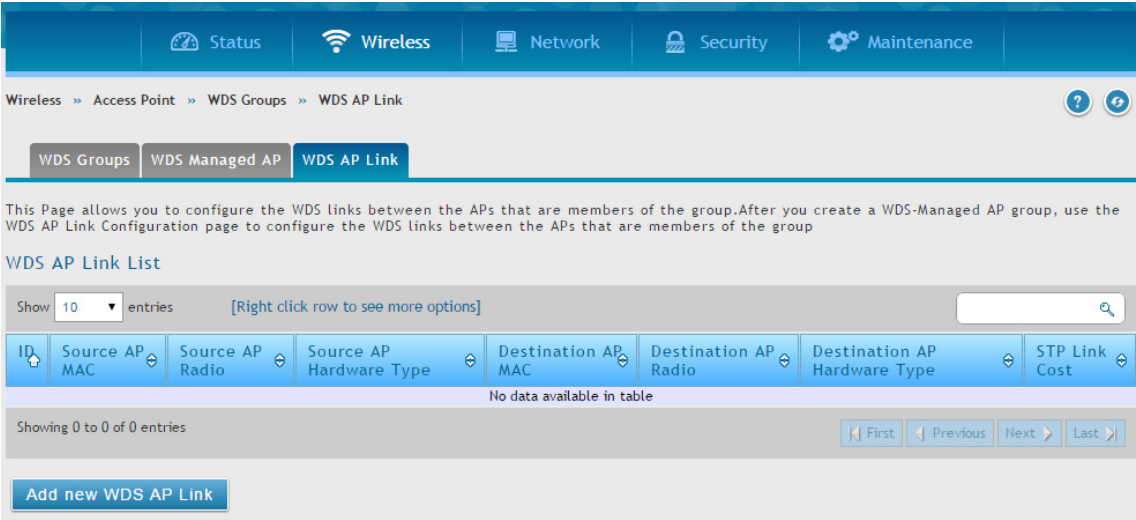


図 5-43 WDS AP Link List 画面

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。

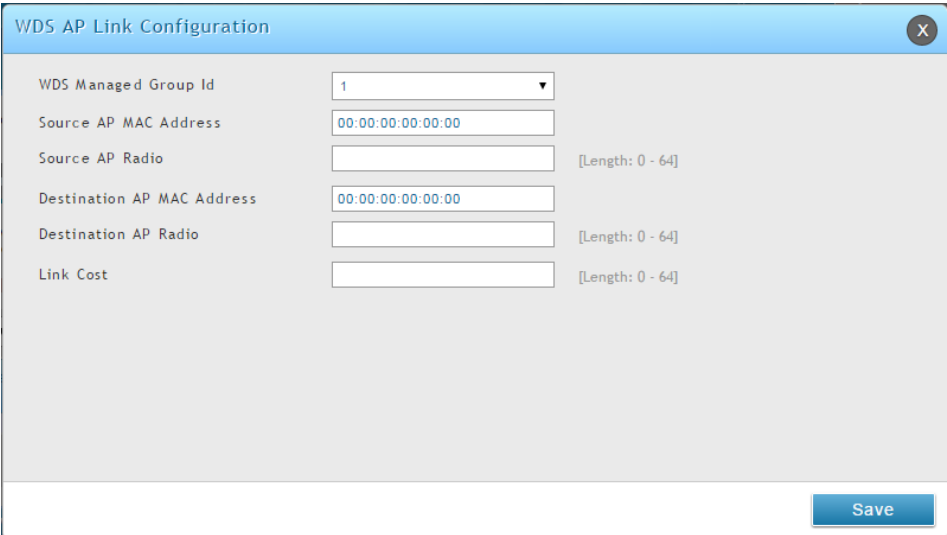


図 5-44 WDS AP Link Configuration 画面

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、WDS リンクの終端の区別を簡単にします。
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の番号を指定します。
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 Radio	送信先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の番号を指定します。
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のに使用されます。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。

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まで、コントローラのコンフィギュレーションの指定部分をコピーできます。本画面では、選択したコンフィギュレーションの部分を、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ことができます。

1つ以上のピアコントローラに送信されるコンフィギュレーションを変更することができます。また、ピアコントローラから受信したコンフィギュレーションを変更することもできます。1つのコントローラからクラスタに変更を自動的に伝達することはできません。どのようなコンフィギュレーションも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。

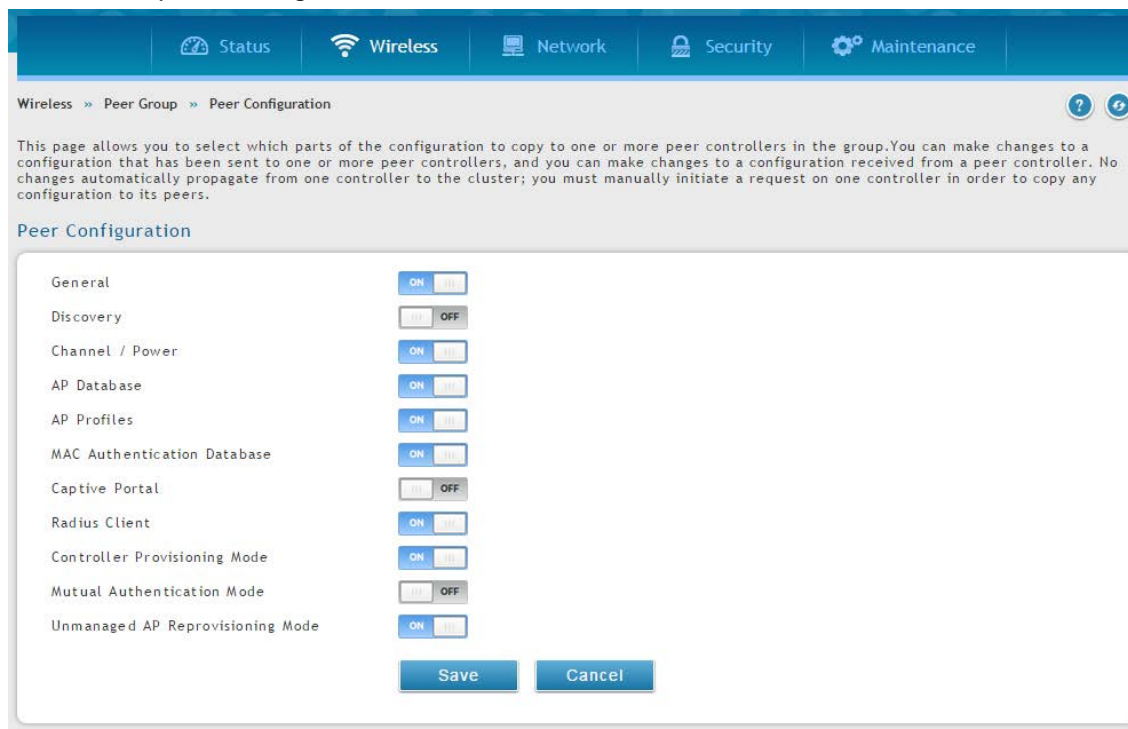


図 5-45 Peer Configuration 画面

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設定するコンフィギュレーションに対して基本および高度なグローバル設定を含めます。固有の設定であるため、そのコンフィギュレーションには、コントローラの IP アドレスを含めません。
Discovery	有効にすると、コントローラがピアに設定するコンフィギュレーションに対して 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設定するコンフィギュレーションに対して 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設定するコンフィギュレーションに対して 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設定するコンフィギュレーションに対してすべての 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設定するコンフィギュレーションに対して 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設定するコンフィギュレーションに対して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設定するコンフィギュレーションに Client RADIUS 情報を含めます。
Controller Provisioning Mode	有効にすると、プロビジョニングメッセージを送受信します。セキュリティ機能として、本オプションを無効にすることができます。

項目	説明
Mutual Authentication Mode	無線ネットワークで相互認証を要求するためには、「ON」を選択します。「OFF」を選択すると、相互認証は要求されません。 1つのコントローラで本パラメータを変更すると、自動的にクラスタ内の他のすべてのコントローラとクラスタ内で管理されるすべてのアクセスポイントのコンフィグレーションが更新されます。 本フィールドが有効である場合、スイッチのプロビジョニングは、新しいコントローラがクラスタに加えられるために有効である必要があります。コントローラのプロビジョニングが無効であると、クラスタは新しいコントローラから証明書を受け付けません。
Unmanaged AP Reprovisioning Mode	有効にすると、アクセスポイントは、コントローラが管理しない場合に、プロビジョニング情報を受け付けることができます。

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。

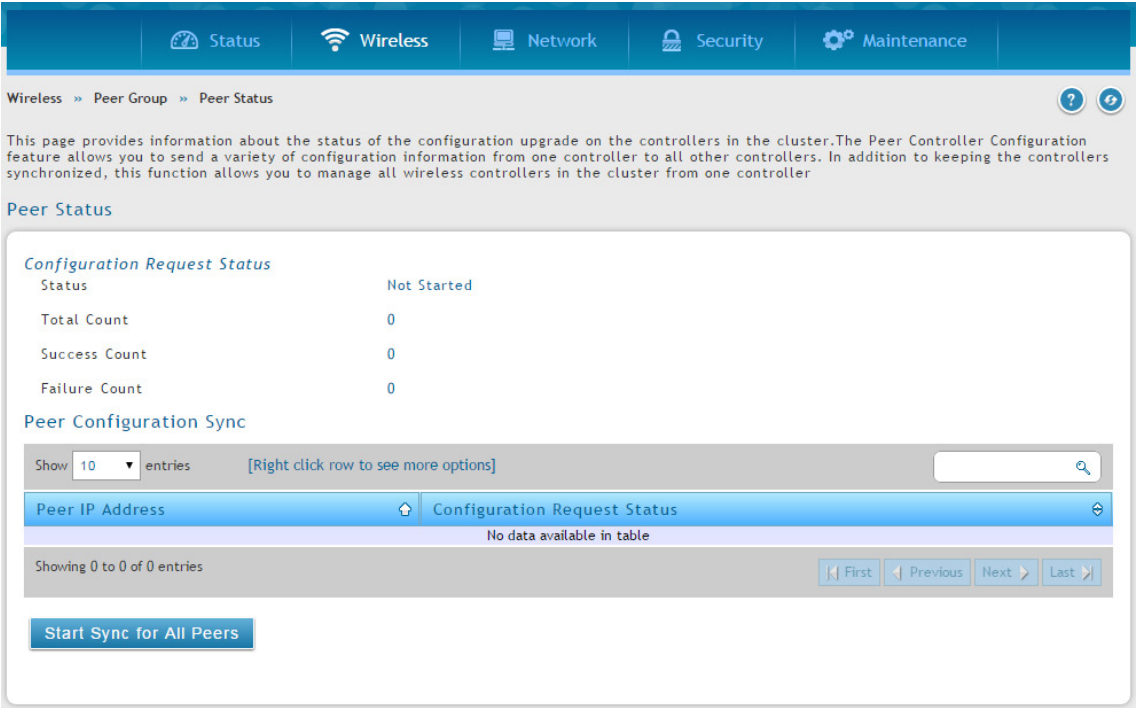


図 5-46 Peer Status 画面

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。

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 5-47 AP Firmware Download 画面

2. フィールドを入力し、更新するアクセスポイントを選択します。「CTRL」を使用しながらクリックすると、複数のアクセスポイントを選択できます。

項目	説明
Server Address	アップグレード用ファイルが格納されているホストの IP アドレスを入力します。ホストには TFTP サーバがインストールされ、起動している必要があります。
File Path	選択ファイルが位置する TFTP サーバのパス (96 文字以内) を指定します。
File Name	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。
Group Size	一度にアップグレードするアクセスポイントの数を指定します。複数のアクセスポイントをアップグレードする場合、各アクセスポイントが TFTP サーバに接続してファイルをダウンロードします。TFTP サーバの過負荷防止のため、一度にアップグレードするアクセスポイント数を制限できます。1 つのグループのアップグレード後に、次のグループのアップグレードが開始されます。

項目	説明
Image Download Type	<p>ダウンロードするイメージタイプを指定します。</p> <ul style="list-style-type: none">• All Images (すべてのイメージ)• DWL-8600AP• DWL-3600AP/ DWL-6600AP• DWL-2600AP• DWL-8610AP <p>注意 すべてのイメージをダウンロードするには、必ず適切な「File Path」および「File Name」欄の両方にファイルパスとファイル名を指定してください。</p>
Managed AP	<p>リスト内にコントローラが管理するすべてのアクセスポイントが表示されます。コントローラがクラスタコントローラである場合、リストにはクラスタ内のすべてのコントローラが管理するアクセスポイントを表示します。</p> <p>各アクセスポイントは MAC アドレス、IP アドレス、およびロケーションの <MAC-IP-Location> 形式により識別されます。1 台のアクセスポイントをアップグレードする場合、プルダウンメニューから目的のアクセスポイントを選択します。すべてのアクセスポイントを対象にする場合は、リストの一番上の「All」を選択します。「All」を選択した場合、「Group Size」フィールドの入力により、同時にアップグレードするアクセスポイントの数を制限して TFTP サーバの過負荷を防止します。アップグレードのために複数のアクセスポイント選択するためには、「CTRL」+ アクセスポイントをクリックすることで行います。</p> <p>注意 管理するアクセスポイントのすべてを同時にアップグレードすることをお勧めします。</p>

3. 「Save」をクリックします。

AP ファームウェアの状態

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

ダウンロードの開始後に、アップグレードに関する情報を表示します。

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。

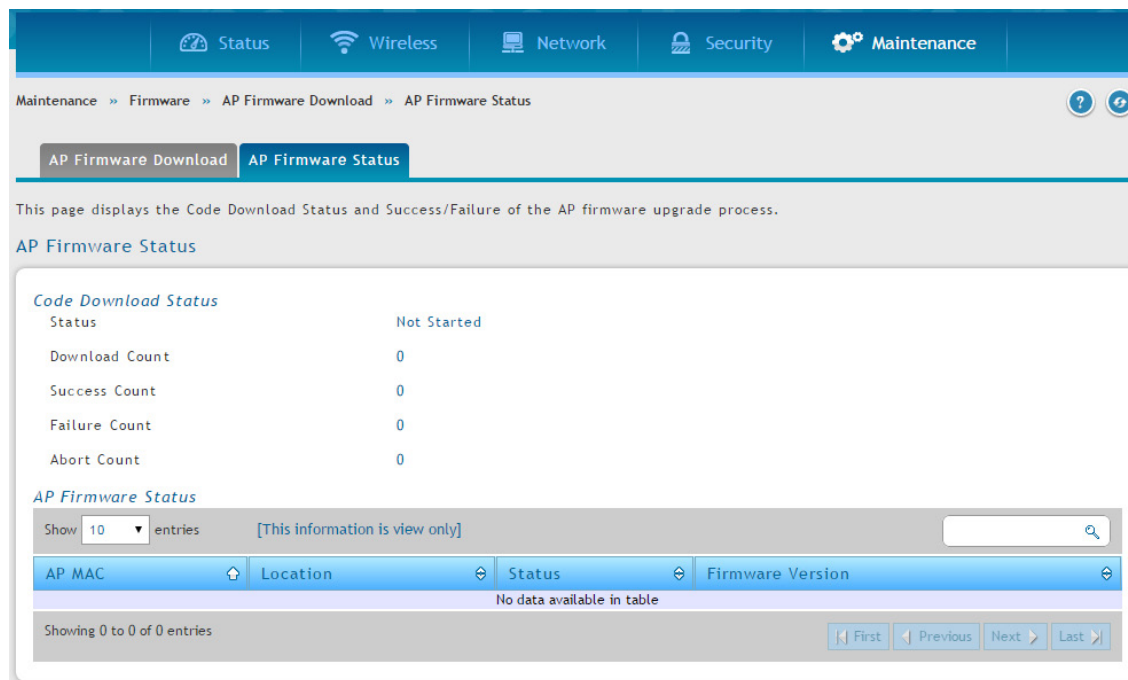


図 5-48 AP Firmware Status 画面

以下の項目を表示します。

項目	説明
Code Download Status	
Status (Global)	<p>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。</p> <ul style="list-style-type: none"> 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を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、WCS 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 台アップグレードしていれば、「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」欄には以下に示す状況の一つが表示されます。 <ul style="list-style-type: none">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廃止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)」参照。
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	参照ページ
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。	103
インターネット設定	Option1/2、DDNS（ダイナミック DNS）の設定などを行います。	117
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。	129
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。	139
QoS 設定	QoS 優先度、ポリシーの設定を行います。	148

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による設定を推奨します。

LAN 設定

Network > LAN メニュー

Network > IPv6 メニュー

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。

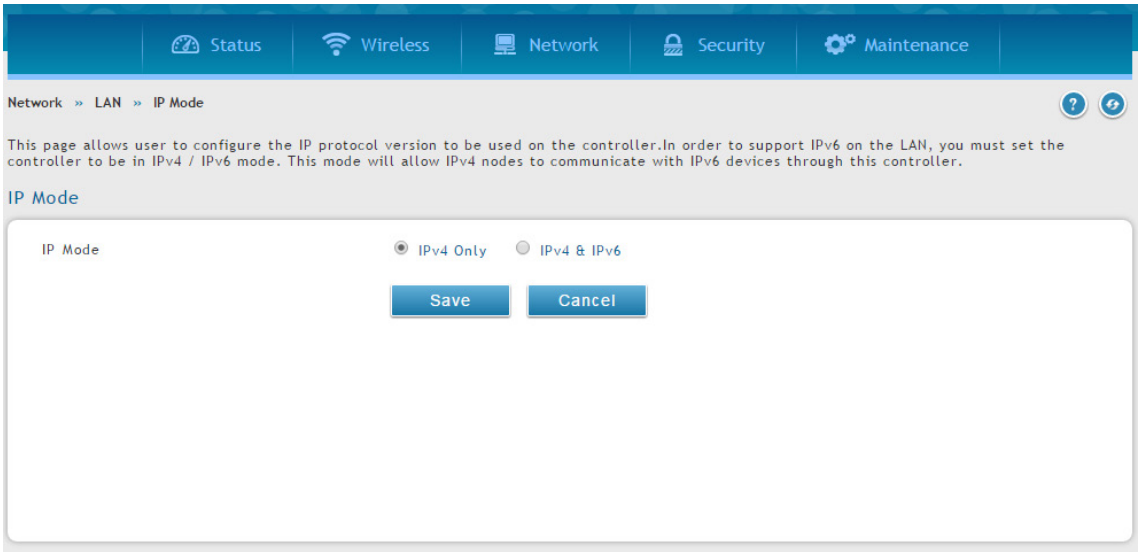


図 6-1 IP Mode 画面

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。

IPv4 LAN 設定

Network > LAN > 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、DHCP のリース情報をネットワークの DHCP サーバである別の LAN デバイスから転送するのに使用されます。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 要求を承諾する場合、コントローラには DHCP 設定内に WINS サーバの IP アドレスがあります。

また、LAN のために 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 の順にメニューをクリックし、以下の画面を表示します。

The screenshot shows the 'LAN Settings' page in a network management interface. The page has a blue header with navigation tabs: Status, Wireless, Network, Security, and Maintenance. Below the header, the breadcrumb 'Network > LAN > LAN Settings' is visible. The main content area is titled 'LAN Settings' and contains several sections:

- IP Address Setup:** Includes fields for 'IP Address' (192.168.10.1) and 'Subnet Mask' (255.255.255.0).
- DHCP Setup:** Includes a 'DHCP Mode' dropdown menu set to 'None', and a 'Domain Name' field with 'DLink' entered.
- Default Route:** Includes checkboxes for 'Enable Default Route' and 'SNAT', both of which are currently turned off.
- DNS Host Name Mapping:** A table with two columns: 'Host Name' and 'IP Address'. The table is empty, showing only the header row.
- LAN Proxy:** Includes a checkbox for 'Activate DNS Proxy' which is currently turned on.

At the bottom of the form, there are 'Save' and 'Cancel' buttons.

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

Status

Wireless

Network

Security

Maintenance

Network » LAN » LAN Settings » IPv4 LAN Settings

IPv4 LAN Settings

IPv6 LAN Settings

IPv6 Address Pools

IPv6 Prefix Length

Router Advertisement

Advertisement Prefixes

The LAN Configuration page allows you to configure the LAN interface of the controller including the DHCP Server which runs on it and Changes here affect all devices connected to the controller's LAN switch and also wireless LAN clients. Note that a change to the LAN IP address will require all LAN hosts to be in the same subnet and use the new address to access this GUI.

LAN Settings

IP Address Setup

IP Address

192.168.1.100

Subnet Mask

255.255.255.0

DHCP Setup

DHCP Mode

DHCP Server

Starting IP Address

192.168.10.100

Ending IP Address

192.168.10.254

Default Gateway

192.168.1.100

Domain Name

DLink

Lease Time

24

[Range: 1 - 262800] Hours

Configure DNS / WINS

ON

Primary DNS Server

Secondary DNS Server

WINS Server

Default Route

Enable Default Route

ON

Gateway

0.0.0.0

DNS Server

0.0.0.0

SNAT

OFF

DNS Host Name Mapping

Host Name	IP Address

LAN Proxy

Activate DNS Proxy

ON

Save

Cancel

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

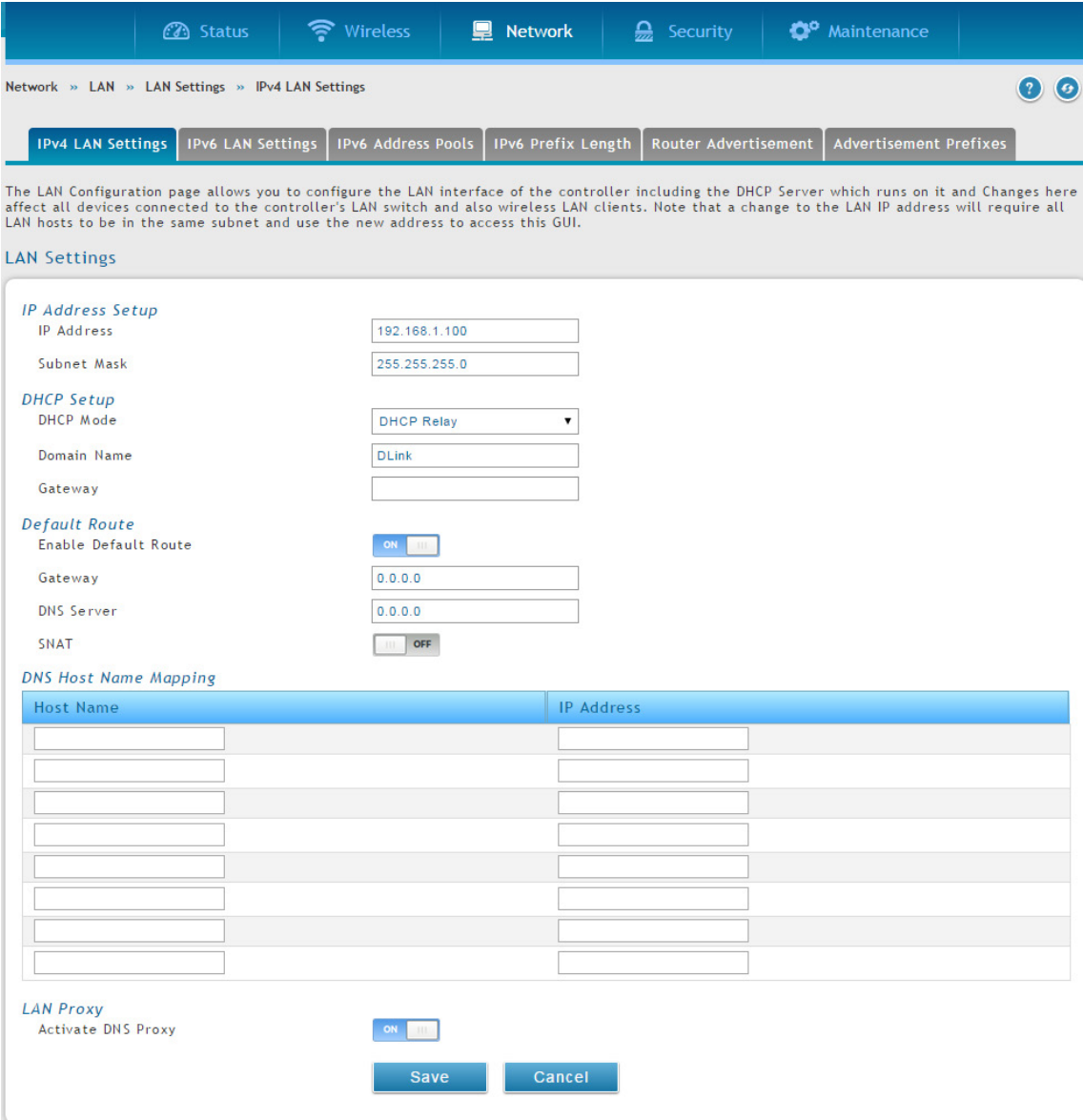


図 6-4 LAN Settings 画面 (DHCP Mode が「DHCP Relay」の場合)

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。 <ul style="list-style-type: none">• 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 デバイスに指定内の IP アドレスに加えて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。
Domain Name	ドメイン名を入力します。
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。
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。
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。

項目	説明
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。
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。
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	
Activate DNS Proxy	<p>この LAN の DNS プロキシを有効または無効にします。</p> <ul style="list-style-type: none"> 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 クライアントが DNS プロキシが動作している IP (つまり、ボックスの LAN IP) に沿ったプライマリ/セカンダリ 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。 <p>本機能は「自動ロールオーバー」モードの場合に特に便利です。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。</p>

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求に基づいて、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には、それらの IPv6 アドレスに共通の開始ビットがあります。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。

The screenshot shows the 'IPv6 LAN Settings' configuration page. At the top, there are navigation tabs: Status, Wireless, Network, Security, and Maintenance. Below these, a breadcrumb trail reads 'Network > IPv6 > LAN Settings > IPv6 LAN Settings'. The main content area has several sub-tabs: 'IPv6 LAN Settings' (selected), 'IPv6 Address Pools', 'Prefixes for Prefix Delegation', 'Router Advertisement', and 'Advertisement Prefixes'. A descriptive text block states: 'This page allows user to IPv6 related LAN configurations. The IPv6 address is 128 bits, with a default 64 bit prefix that defines the network and is common among all LAN hosts. Changes here affect all devices connected to the router's LAN switch. Note that a change to the default LAN IP address will require all LAN hosts to be in the same network prefix and use the new address to access this GUI.' Below this, the 'IPv6 LAN Settings' section contains three main fields: 'LAN TCP/IP Setup' with 'IPv6 Address' set to 'fec0::1', 'IPv6 Prefix Length' set to '64' (with a range of 0-128), and 'DHCPv6 Status' set to 'OFF'. At the bottom of this section are 'Save' and 'Cancel' buttons.

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。

項目	説明
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には、それらの IPv6 アドレスに同じ開始ビットがあります。ネットワークアドレスの一般的な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	ゲートウェイに適切なアドレスを取得する方法を選択します。 <ul style="list-style-type: none">• Stateless - アドレスの割り当てにコントローラの通知を使用します。IPv6 RADVD プロトコルが 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有効にされます。• Stateful - ISP で利用可能などの DHCPv6 サーバからも 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な DHCP によって使用されます。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。
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。 <ul style="list-style-type: none">• 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 DNS from ISP - ISP による LAN DHCP クライアントへの DNS サーバ（プライマリ/セカンダリ）の定義を有効にします。• Use Below - ISP は LAN DHCP クライアントに DNS サーバ（プライマリまたはセカンダリ）を定義することができます。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 サーバは DHCPv6 クライアントに使用されます。
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、割り当てられたプレフィックスに、DHCP 情報の詳細にある LAN 上の他のネットワークデバイスを通知する処理を自動化できます。

1. Network > IPv6 > 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。

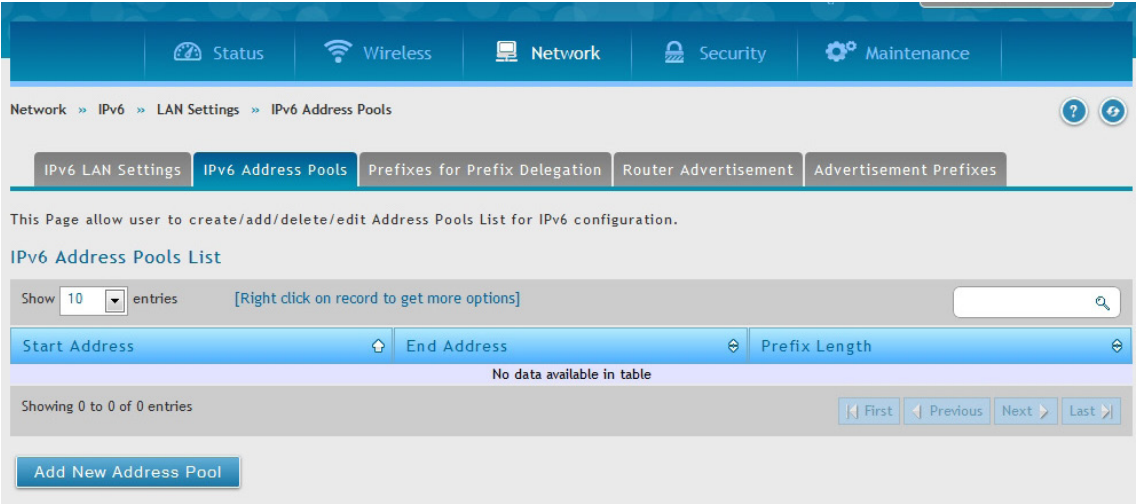
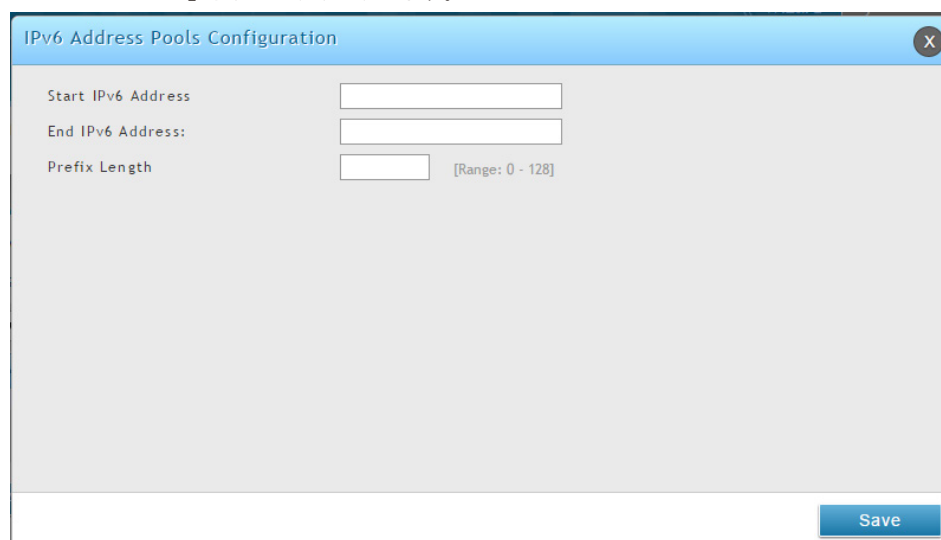


図 6-6 IPv6 Address Pools List 画面

2. 「Add New Address Pool」ボタンをクリックします。



IPv6 Address Pools Configuration

Start IPv6 Address:

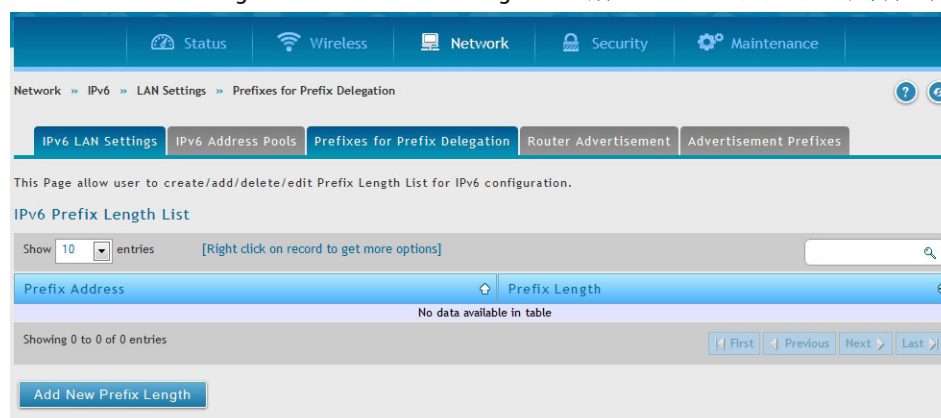
End IPv6 Address:

Prefix Length: [Range: 0 - 128]

Save

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



Network > IPv6 > LAN Settings > Prefixes for Prefix Delegation

IPv6 LAN Settings | IPv6 Address Pools | **Prefixes for Prefix Delegation** | Router Advertisement | Advertisement Prefixes

This Page allow user to create/add/delete/edit Prefix Length List for IPv6 configuration.

IPv6 Prefix Length List

Show 10 entries [Right click on record to get more options]

Prefix Address	Prefix Length
No data available in table	

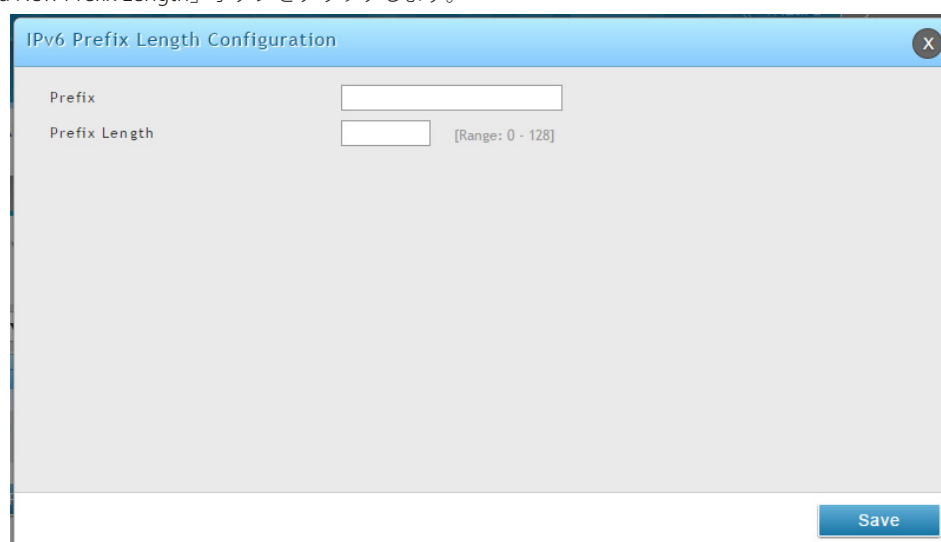
Showing 0 to 0 of 0 entries

First Previous Next Last

Add New Prefix Length

図 6-8 IPv6 Prefix Length List 画面

6. 「Add New Prefix Length」ボタンをクリックします。



IPv6 Prefix Length Configuration

Prefix:

Prefix Length: [Range: 0 - 128]

Save

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 > IPv6 > 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、コントローラはそのような詳細を受け付けるよう設定するデバイスに IP アドレスとサポートするネットワーク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 > IPv6 > 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。

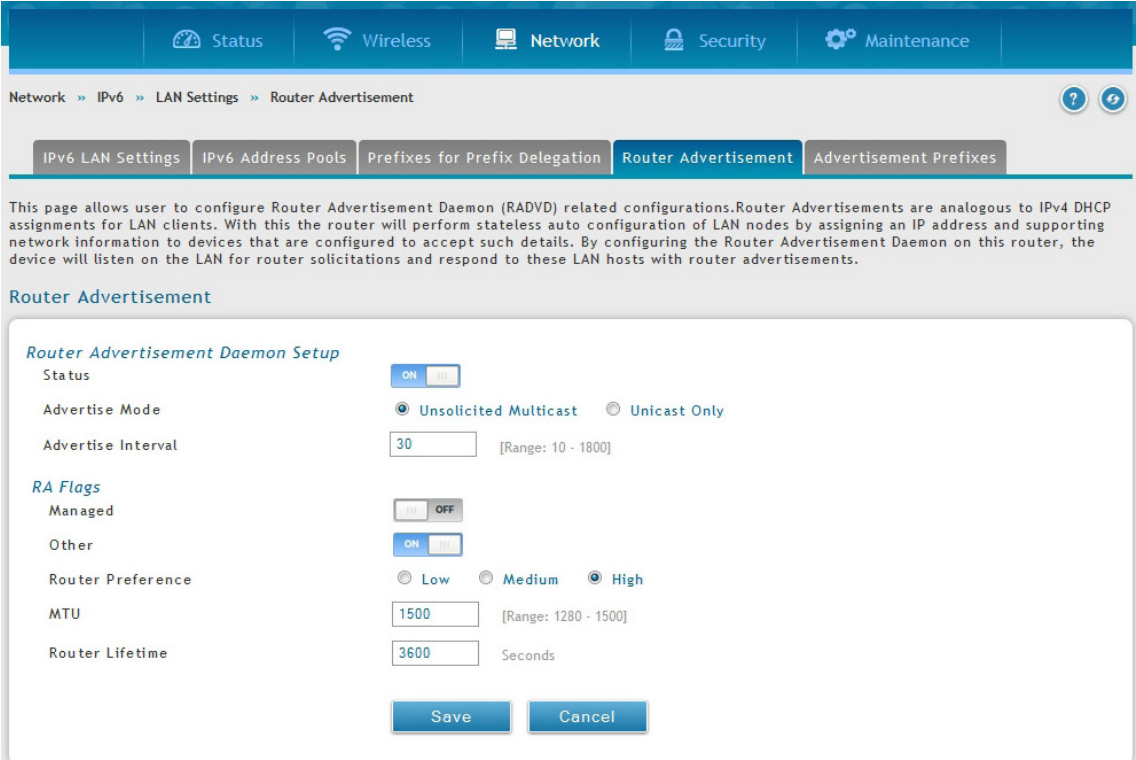


図 6-10 Router Advertisement 画面

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。 <ul style="list-style-type: none">Unsolicted 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、RA は既知のアドレスだけに所属するインタフェースに送信します。
Advertise Interval	「Advertise Mode」が「Unsolicted 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。 <ul style="list-style-type: none">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	ネットワークの全ノードが LAN MTU が既知でない場合と同じ MTU 値を使用するのを保証するために 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 > IPv6 > 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。ルータ通知は、ルータが Neighbor を決定し、コントローラと同じリンク上にホストが存在するかどうかを決定できるサブネットプレフィックスのリストを含んでいます。

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

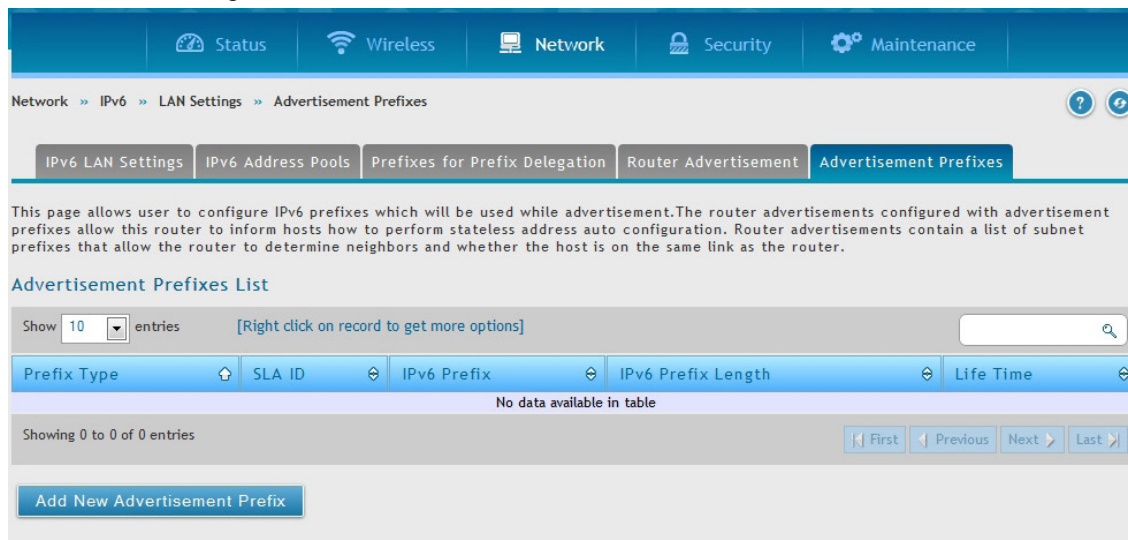


図 6-11 Advertisement Prefixes List 画面

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

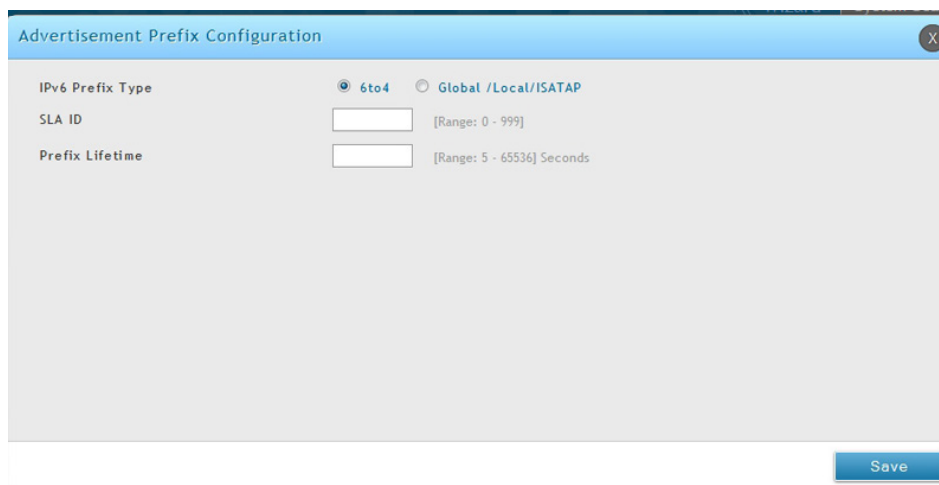


図 6-12 Advertisement Prefixes Configuration 画面

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。
SLA ID	IPv6 プレフィックスタイプが「6to4」の場合、6to4 アドレスプレフィックスの「SLA ID」(Site-Level Aggregation Identifier) はアドバタイズメントが送信されたインタフェースのインタフェース ID に指定されます。
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。

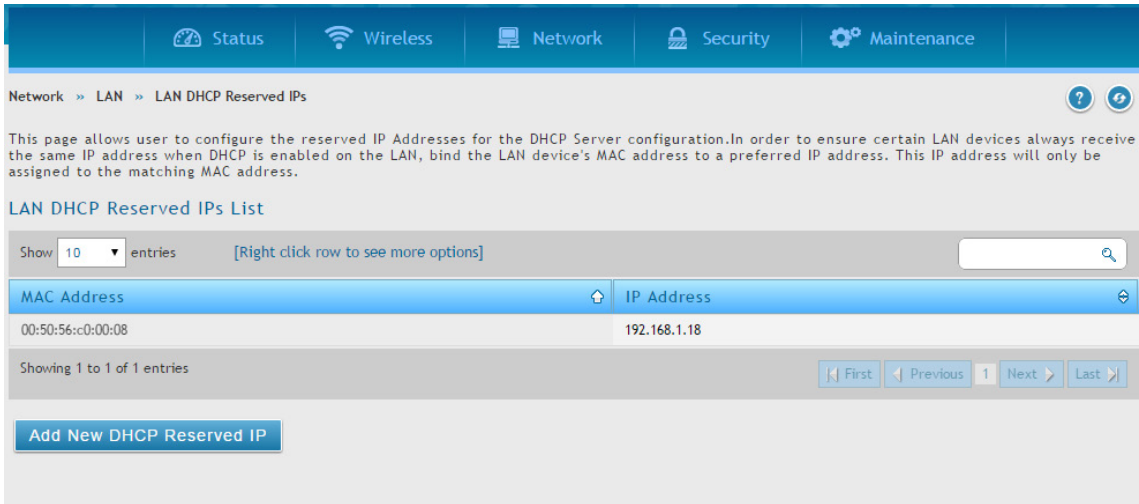


図 6-13 LAN DHCP Reserved IPs List 画面

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

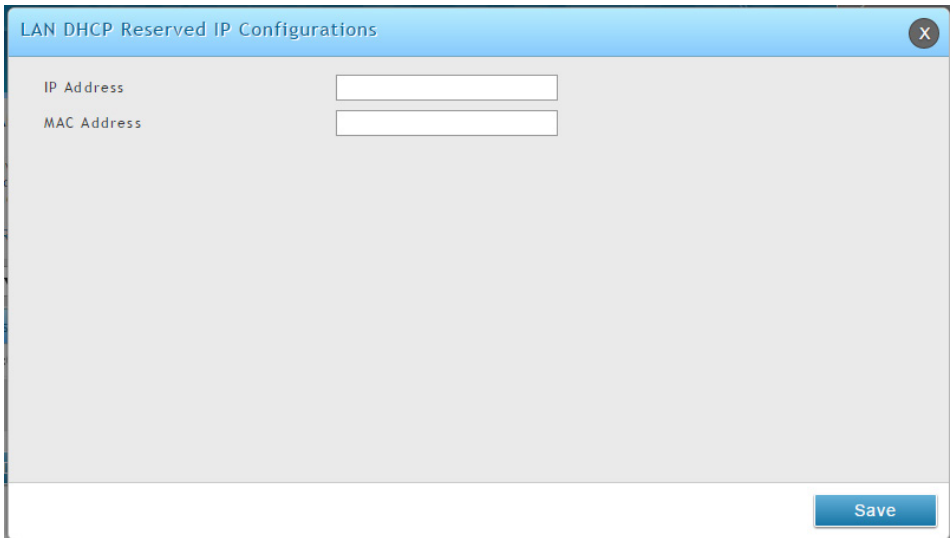


図 6-14 LAN DHCP Reserved IP Configuration 画面

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。

IP/MAC バインディング

Network > LAN > IP/MAC Binding メニュー

LAN ノードがバインドされた MAC アドレスと一致する IP アドレスを持つ場合に、外向きトラフィック（LAN から WAN まで）のみ許可するセキュリティ対策です。これは IP/MAC バインディングで、管理者はゲートウェイが設定済み LAN ノードの固有の MAC アドレスを持つ送信元トラフィックの IP アドレスを確認することで IP アドレスが偽造されないことを保証することができます。違反（すなわち、トラフィックの送信元 IP アドレスが同じ IP アドレスを持っていると思われた MAC アドレスに一致しない）の場合、パケットを破棄して診断のためにログに出力します。

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

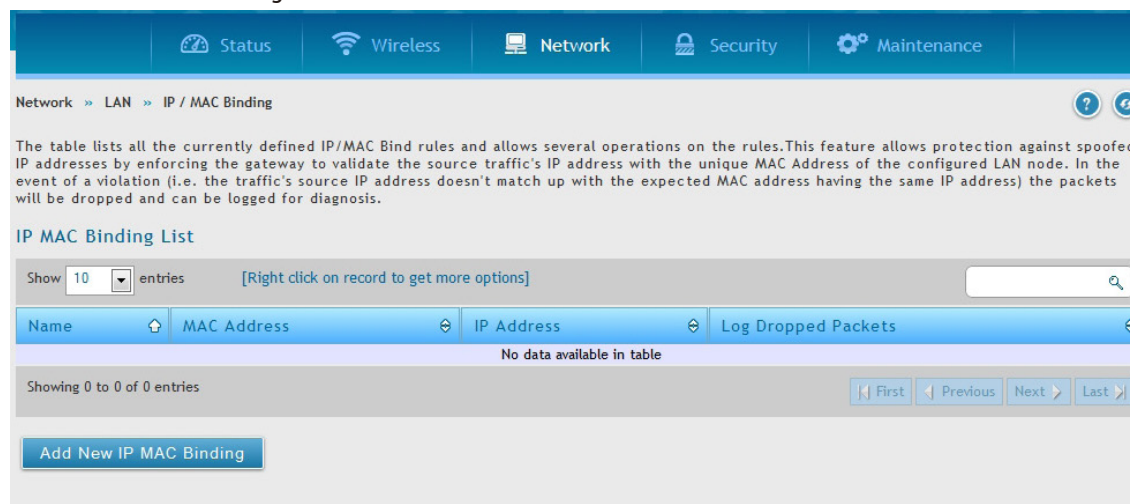


図 6-15 IP/MAC Binding 画面

2. 「Add New IP/MAC Binding」ボタンをクリックします。

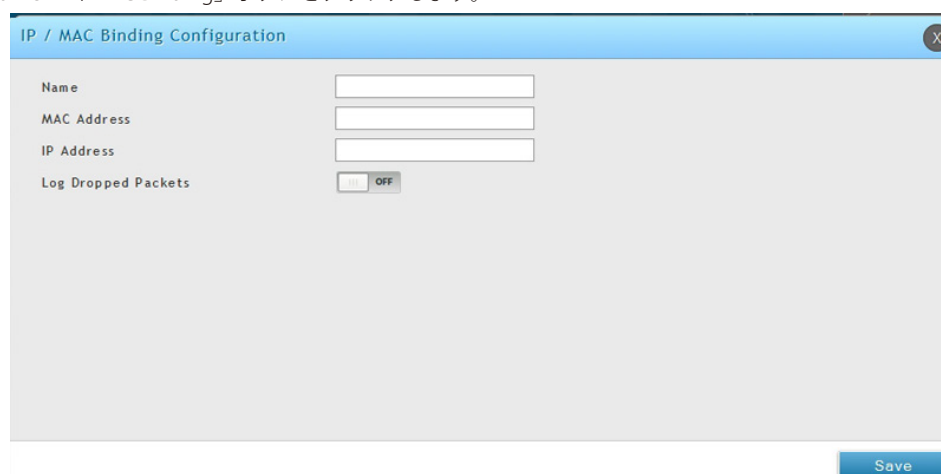


図 6-16 Add New IP/MAC Binding 画面

3. 名前、MAC アドレス、IP アドレスを入力し、「Log Dropped Packets」でドロップしたパケットのログの有効 / 無効を指定します。
4. 「Save」ボタンをクリックします。

IGMP 設定

Network > LAN > IGMP Setup メニュー

注意 本機能は追加ライセンス「DWC-1000-VPN」が有効の場合にのみ利用可能です。

IGMP Snooping (IGMP Proxy) により、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だけに、これを送ります。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大量のマルチキャストトラフィックがあ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。

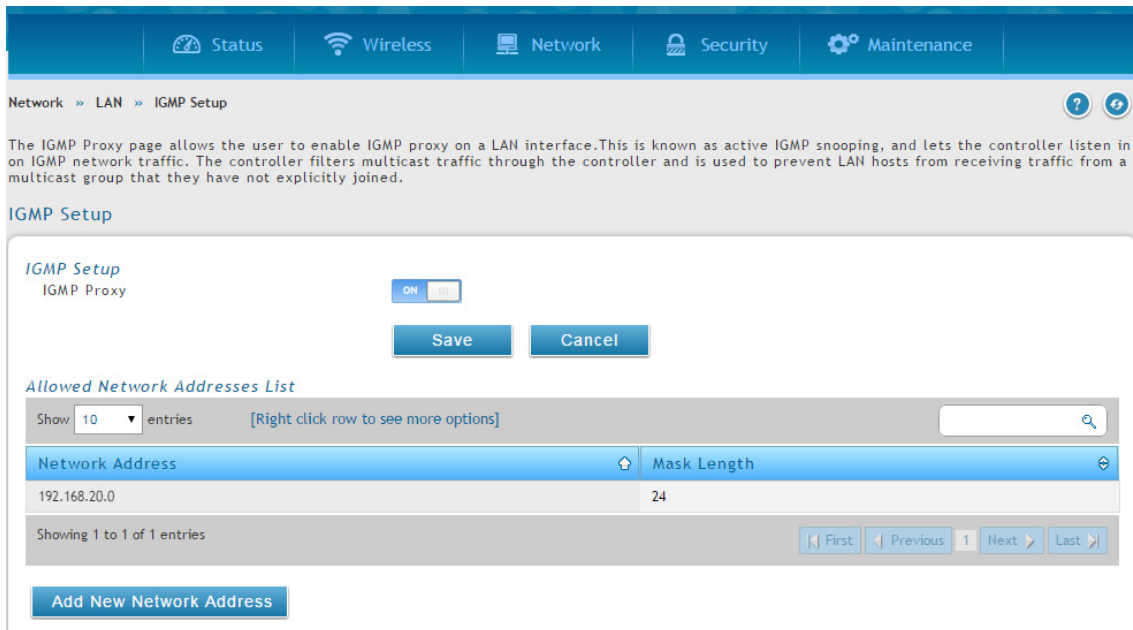


図 6-17 IGMP Setup 画面

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、ネットワークアドレスとマスク長を指定します。

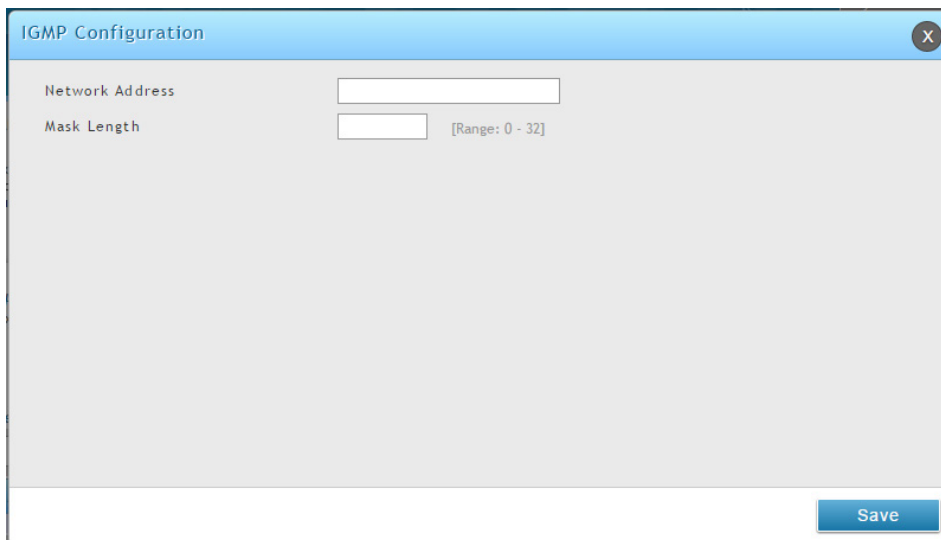


図 6-18 IGMP Configuration 画面

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。

UPnP 設定

Network > LAN > UPnP メニュー

注意 本機能は追加ライセンス「DWC-1000-VPN」が有効の場合にのみ利用可能です。

UPnP（Universal Plug and Play）は、コントローラと通信できるネットワーク上のデバイスを検出し、自動設定を行う機能です。ネットワークデバイスが UPnP によって検出されると、コントローラはネットワークデバイスが要求するトラフィックのプロトコルのために内部または外部ポートをオープンすることができます。

UPnP を有効にすると、LAN（または、定義済み VLAN）にある UPnP をサポートするデバイスを検出するようにコントローラを設定することができます。無効にすると、コントローラはデバイスの自動設定を許可しません。

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

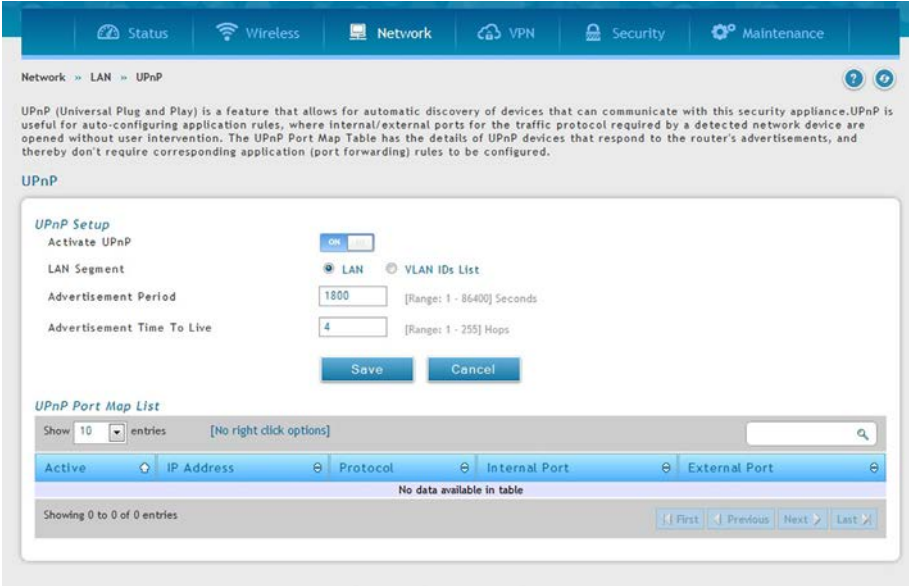


図 6-19 UPnP 設定

2. UPnP を使用するためには以下の設定を行います。

項目	説明
UPnP Setup	
Activate UPnP	UPnP を有効にする場合にチェックします。
LAN Segment	必要に応じて、LAN 全体または指定した VLAN グループで UPnP を有効にします。
Advertisement Period	コントローラがネットワーク上に UPnP 情報をブロードキャストする頻度です。大きい値はネットワークトラフィックを最小限にしますが、新しい UPnP デバイスをネットワークで特定する際に遅延をもたらします。
Advertisement Time to Live	これは各 UPnP パケットのホップで表現されます。また、パケットが破棄される前に伝播できるステップ数です。小さい値は UPnP ブロードキャスト範囲を制限します。初期値の 4 は少ないコントローラを持つネットワークでは一般的な数値です。
UPnP Port Map List	
Active	Yes / No は接続を確立した UPnP デバイスのポートが現在アクティブであるかどうかを示します。
Internal Port	UPnP によってオープンされた内部ポート。
External Port	UPnP によってオープンされた外部ポート。

3. 「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。

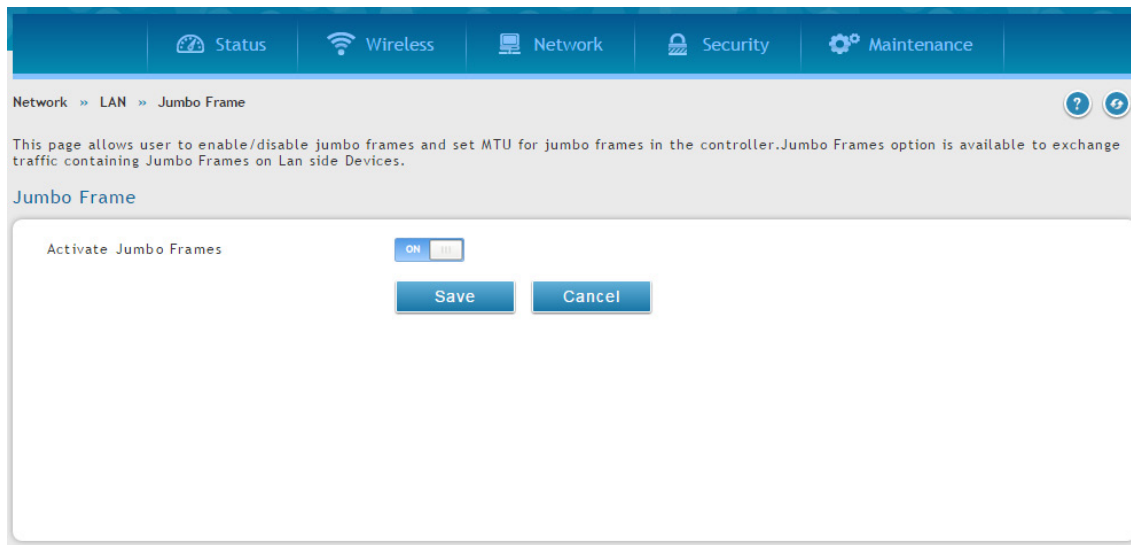


図 6-20 Jumbo Frame 画面

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。

インターネット設定

Network > Internet メニュー

ここではインターネット接続を設定します。

Option1 設定

Network > Internet > Option 1 Settings メニュー

このコントローラには、インターネットへの接続を確立するのに使用する 2 つの Option ポートがあり、インターネットまたは他のネットワークサブネットによる接続をサポートしています。初期値では「Option1」が有効となっており、MAC アドレスとともに LAN インタフェースとして機能しています。「Option2」は無効で、VPN ライセンス「DWC-1000-VPN」を有効にすることにより、コントローラを WAN ポートとして作用させます。ISP 接続タイプと NAT/Transparent を設定します。

1. Network > Internet > Option 1 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。

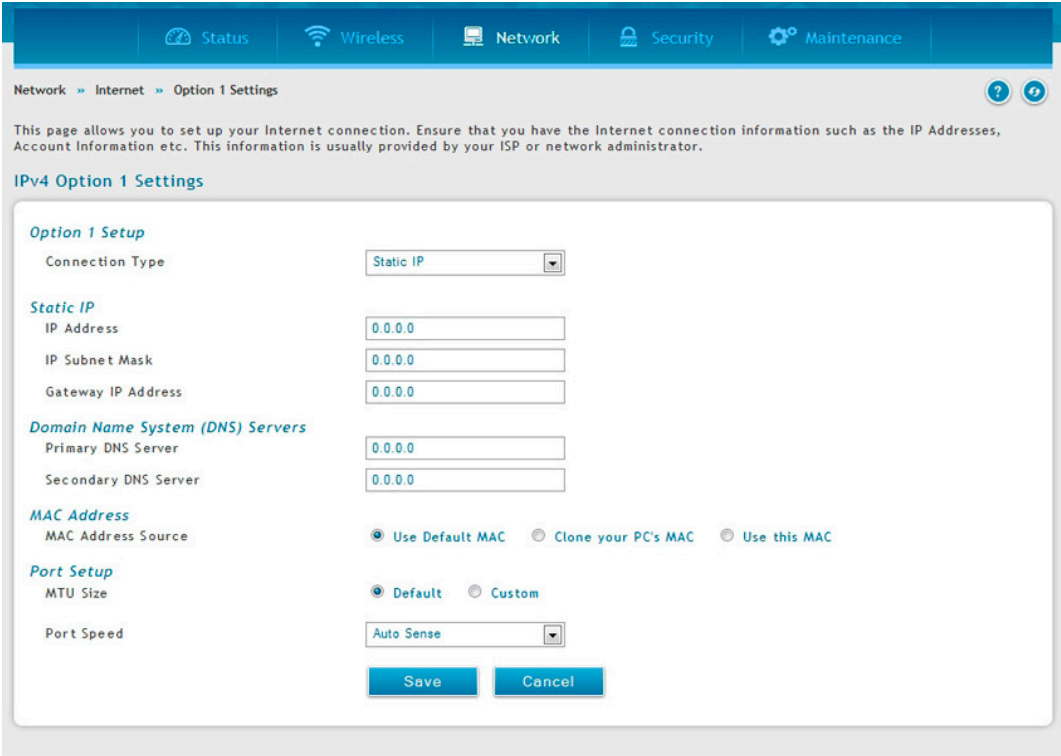


図 6-21 Option1 画面

2. Option1 における設定を行います。

項目	説明
Connection Type	このコントローラのプライマリ Option リンクに設定した ISP に基づいて「Static」「Dynamic」「PPTP/Russian PPTP」(Point-to-Point Tunneling Protocol)、「PPPoE/Japanese PPPoE/Russian PPPoE」(Point-to-Point Protocol over Ethernet)、「L2TP/Russian L2TP」(Layer 2 Tunneling Protocol) を選択します。選択された「Connection Type」により表示されるフィールドが異なります。
Dynamic	
Host Name	DHCP サーバに送信するためにホスト名オプションを指定します。
Static	
IP Address	ご契約の ISP が割り当てたスタティック IP アドレスを入力します。
IP Subnet Mask	サブネットマスクを入力します。通常、これは ISP またはご使用のネットワーク管理者によって提供されます。
Default Gateway	ゲートウェイの IP アドレスを入力します。通常、これは ISP またはご使用のネットワーク管理者によって提供されます。
DNS Server (S)	有効なプライマリ / セカンダリ DNS サーバの IP アドレスを入力します。
PPPoE/Japanese PPPoE/Russian PPPoE	
Address Mode	以下のオプションの 1 つを選択します。 <ul style="list-style-type: none">Dynamic IP - スタティック IP アドレスが割り当てられていない場合にこのオプションを選択します。ISP は DHCP ネットワークプロトコルを使用して IP アドレスを自動的に割り当てます。Static IP - ISP が固定の (スタティックまたはパーマネント) IP アドレスを割り当てた場合にこのオプションを選択します。以下の項目も設定します。
IP Address	ご契約の ISP が割り当てたスタティック IP アドレスを入力します。
Subnet Mask	サブネットマスクを入力します。通常、これは ISP またはご使用のネットワーク管理者によって提供されます。
User Name	ログインに必要なユーザ名を入力します。

高度なネットワーク設定

項目	説明
Password	ログインに必要なパスワードを入力します。
Service	同じユーザ名とパスワードの組合せを使用して 2 つのサーバを識別する必要がある場合にこの欄を使用します。PPP の場合、IP アドレスを使用してサーバを指定できない場合に、この欄を使用して接続する特定のサーバを指定できます。
Authentication Type	プロファイルが使用する認証タイプを指定します。(Auto-negotiate、PAP、CHAP、MS-CHAP、MS-CHAPv2)
Reconnect Mode	以下のオプションの 1 つを選択します。 <ul style="list-style-type: none"> Always On - 接続は通常オンとなります。 On Demand - 指定時間アイドル状態であると、接続は自動的に終了します。「Maximum Idle Time」欄に時間 (分) を入力します。この機能は、ご契約の ISP が接続時間に基づいて課金する場合に便利です。
PPTP/Russian PPTP	
Address Mode	以下のオプションの 1 つを選択します。 <ul style="list-style-type: none"> Dynamic IP - スタティック IP アドレスが割り当てられていない場合にこのオプションを選択します。ISP は DHCP ネットワークプロトコルを使用して IP アドレスを自動的に割り当てます。 Static IP - ISP が固定の (スタティックまたはパーマネント) IP アドレスを割り当てた場合にこのオプションを選択します。以下の項目も設定します。
Server Address	PPTP Server IP アドレスを入力します。
User Name	ISP へのログインに必要なユーザ名を入力します。
Password	ISP へのログインに必要なパスワードを入力します。
MPPE Encryption	PPTP サーバが MPPE 暗号化をサポートする場合にチェックします。
Split Tunnel	このオプションは PPTP および L2TP にだけ有効です。有効にすると、ゲートウェイ IP アドレスの追加をできないようにしますが、代わりに LAN トラフィックを送信するために特定のルートを追加する必要があります。
Reconnect Mode	以下のオプションの 1 つを選択します。 <ul style="list-style-type: none"> Always On - 接続は通常オンとなります。 On Demand - 指定時間アイドル状態であると、接続は自動的に終了します。「Maximum Idle Time」欄に時間 (分) を入力します。この機能は、ご契約の ISP が接続時間に基づいて課金する場合に便利です。
L2TP/Russian L2TP	
Address Mode	以下のオプションの 1 つを選択します。 <ul style="list-style-type: none"> Dynamic IP - スタティック IP アドレスが割り当てられていない場合にこのオプションを選択します。ISP は DHCP ネットワークプロトコルを使用して IP アドレスを自動的に割り当てます。 Static IP - ISP が固定の (スタティックまたはパーマネント) IP アドレスを割り当てた場合にこのオプションを選択します。以下の項目も設定します。
Server Address	L2TP Server IP アドレスを入力します。
User Name	ISP へのログインに必要なユーザ名を入力します。
Password	ISP へのログインに必要なパスワードを入力します。
Secret	シークレットフレーズを入力して、サーバ (L2TP 接続のみ) にログインします。
Split Tunnel	このオプションは PPTP および L2TP にだけ有効です。有効にすると、ゲートウェイ IP アドレスの追加をできないようにしますが、代わりに LAN トラフィックを送信するために特定のルートを追加する必要があります。
Reconnect Mode	以下のオプションの 1 つを選択します。 <ul style="list-style-type: none"> Always On - 接続は通常オンとなります。 On Demand - 指定時間アイドル状態であると、接続は自動的に終了します。「Maximum Idle Time」欄に時間 (分) を入力します。この機能は、ご契約の ISP が接続時間に基づいて課金する場合に便利です。
Domain Name System (DNS) Servers	
DNS Server Source	以下のオプションの 1 つを選択します。 <ul style="list-style-type: none"> Get Dynamically from ISP - ISP がスタティックな DNS IP アドレスを割り当てなかった場合にこのオプションを選択します。 Use These DNS Servers - ISP がスタティックな DNS IP アドレスを割り当てた場合にこのオプションを選択します。以下の欄を入力します。
Primary DNS Server	有効なプライマリ DNS サーバの IP アドレスを入力します。
Secondary DNS Server	有効なセカンダリ DNS サーバの IP アドレスを入力します。
MAC Address	
MAC Address Source	ご契約の ISP が MAC 認証を必要とし、別の MAC アドレスが以前に ISP に登録されていない場合には「Use Default Address」を選択します。 <ul style="list-style-type: none"> Use Default Address - コントローラを設定するために使用しているコンピュータの MAC アドレスを割り当てる場合にこのオプションを選択します。 Clone your PC's MAC Address - コントローラを設定するために使用しているコンピュータの MAC アドレスを割り当てる場合にこのオプションを選択します。 Use this MAC Address - ISP が使用する MAC アドレスを割り当てた場合にこのオプションを選択します。また、以下の欄も入力します。
MAC Address	MAC アドレスを入力します。
Port Settings	

項目	説明
MTU Size	ネットワークに送信可能な最大パケットのサイズを指定します。イーサネットネットワークの通常 MTU 値は 1500Byte、PPPoE/PPTP 接続の場合 1492Byte、L2TP 接続の場合、1460Byte です。初期値は 1500 です。
Custom MTU Size	カスタムの MTU サイズを指定します。
Port Speed	手動でポートスピードを指定します。

3. 「Save」ボタンをクリックします。

Option2/DMZ 設定

Network > Internet > Option2/DMZ Setting メニュー

注意 本機能は追加ライセンス「DWC-1000-VPN」が有効の場合にのみ利用可能です。

本コントローラは、セカンダリのイーサネットポートまたは専用 DMZ ポートとして設定できる物理ポート（Option ポート）の 1 つをサポートしています。DMZ ではビデオ会議などのためにインターネットへの IP アドレスの公開を行うことができます。

「Option2 ポート」をインターネットに接続する場合、「Option」をクリックし、上記「Option1」ポートの設定手順を参照ください。

DMZ 設定には二つの手順があります。

1. 無線コントローラポートを DMZ として設定する。
2. DMZ の設定を対象ポートに行う。

1. Network > Internet > Option2/DMZ 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 6-22 Option 2 / DMZ Setting 画面

2. 「Configurable Port Status」（コントローラの設定可能なポート）を「DMZ」にします。

3. 以下の項目を入力します。

項目	説明
DMZ IP Address	
IP Address	コントローラの DMZ LAN IP アドレスを入力します。
Subnet Mask	上記の IP アドレスのサブネットマスク。
DHCP for DMZ	
DHCP Mode	<ul style="list-style-type: none"> • None - DMZ 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に選択します。 • DHCP Relay - リレーゲートウェイ情報を入力します。 • DHCP Server - DHCP サーバとしてコントローラを使用するために選択して以下の情報を設定します。

4. 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。

IPv6 ネットワークにおける Option 設定

Network > IPv6 > Option 1 Settings / Option 2 Settings メニュー

ここでは IPv6 の関連する Option1 / Option2 設定を行うことができます。

IPv6 Option（WAN）接続のために、DHCPv6 クライアントとして設定する場合、このコントローラはスタティックな IPv6 アドレスを持つか、または接続情報を受信することができます。ISP がインターネットにアクセスするために固定アドレスを割り当てる場合には、スタティックな構成設定を完了する必要があります。ご使用のコントローラに割り当てられた IPv6 アドレスに加えて、ISP で定義された IPv6 プレフィックス長が必要とされます。デフォルト IPv6 ゲートウェイアドレスは、このコントローラがインターネットにアクセスするために接続する ISP のサーバです。インターネットアドレスの解決のために ISP の IPv6 ネットワークにおけるプライマリおよびセカンダリ DNS サーバが使用され、これらはスタティック IP アドレスとプレフィックス長と共に ISP から提供されます。

DHCP を通して ISP が Option IP 設定の取得を許可する場合、ご使用の DHCPv6 クライアント構成の詳細を提供する必要があります。ゲートウェイ上の DHCPv6 クライアントをステートレスまたはステートフルとすることができます。ステートフルクライアントが選択されると、ゲートウェイはアドレスのリースのために ISP の DHCPv6 サーバに接続します。ステートレスの DHCP では、ISP で利用可能な DHCPv6 サーバは必要なくて、ICMPv6 検出メッセージがこのゲートウェイから生成されて、自動設定に使用されます。また、優先される DHCPv6 サーバの IP アドレスとプレフィックス長を指定する 3 番目のオプションがさらに利用可能となります。

1. Network > IPv6 > Option 1 Settings / Option 2 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。

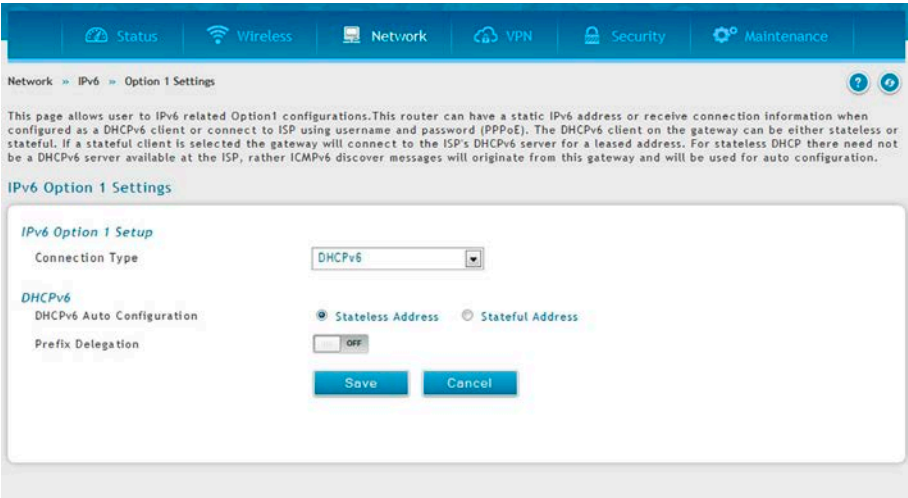


図 6-23 IPv6 Option1

2. 以下の情報を表示または指定します。

項目	説明
Connection Type	IPv6 の接続タイプを「DHCPv6」「Static」「PPPoE」から設定します。
DHCPv6	
DHCPv6 Auto Configuration	<ul style="list-style-type: none">Stateless Address - アドレスの割り当てにコントローラの通知を使用します。IPv6 RADVD プロトコルが 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有効にされます。Stateful Address - ISP で利用可能ななどの DHCPv6 サーバからも IPv6 アドレスを要求します。
Prefix Delegation	このオプションを選択して、ISP で利用可能な DHCPv6 サーバからコントローラに通知プレフィックスを要求し、取得したプレフィックスは LAN 側に通知されたプレフィックスに更新されます。本オプションは DHCPv6 クライアントのステートレスアドレス自動設定モードでのみ選択されます。IPv6 が PPPoE タイプである場合、以下の PPPoE 欄が有効となります。
Static	
IPv6 Address	割り当てられたスタティック IPv6 アドレス。これはご契約の ISP に対してコントローラを特定します。
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には、それらの IPv6 アドレスに同じ開始ビットがあります。ネットワークアドレスの一般的な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。
Default IPv6 Gateway	ISP ゲートウェイの IPv6 アドレス。通常、これは ISP またはご使用のネットワーク管理者によって提供されます。
Primary / Secondary DNS Server	有効なプライマリ / セカンダリ DNS サーバの IP アドレス。
PPPoE	
Username	ISP へのログインに必要なユーザ名を入力します
Password	ISP へのログインに必要なパスワードを入力します
Service	同じユーザ名とパスワードの組合せを使用して 2 つのサーバを識別する必要がある場合にこの欄を使用します。PPP の場合、IP アドレスを使用してサーバを指定できない場合に、この欄を使用して接続する特定のサーバを指定できます。
Authentication Type	プロファイルが使用する認証タイプ : Auto-Negotiate/PAP/CHAP/MS-CHAP/MS-CHAPv2

項目	説明
Dhcpv6 Options	DHCPv6 クライアントのモードはこのモードで始まります。: disable dhcpv6/stateless dhcpv6/stateful dhcpv6/stateless dhcpv6 with prefix delegation
Primary / Secondary DNS Server	有効なプライマリ / セカンダリ DNS サーバの IP アドレス。

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。

Option Mode

Network > Internet > Option Mode メニュー

注意 本機能は追加ライセンス「DWC-1000-VPN」が有効の場合にのみ利用可能です。

インターネット接続用の 2 つの Option (WAN) ポートにポリシーを設定することができます。このコントローラは複数インターネット (WAN) リンクをサポートしています。これは、ポートの 1 つに不安定な WAN 接続がある場合に特定のインターネットに依存するサービスを優先することを保証するフェイルオーバーとロードバランシング機能の長所を利用することができます。

フェイルオーバーまたはロードバランシングを使用するためには、WAN リンク障害検知を設定する必要があります。これは、インターネット上の DNS サーバへのアクセスまたはインターネットアドレスへの ping (ユーザ定義) に関係します。必要であれば、リンクが切断していると思われる場合にリトライ回数を設定することができます。または、Option ポートがダウンしているかどうかを判断する障害のしきい値を設定することができます。

単一オプションポート (Single Option Port)

もし自動フェイルオーバーやロードバランシングを使用しない場合、「Single WAN Port」を「Option Mode」から選択し、設定するオプションポートを指定、「Save」をクリックします。

1. Network > Internet > Option 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。

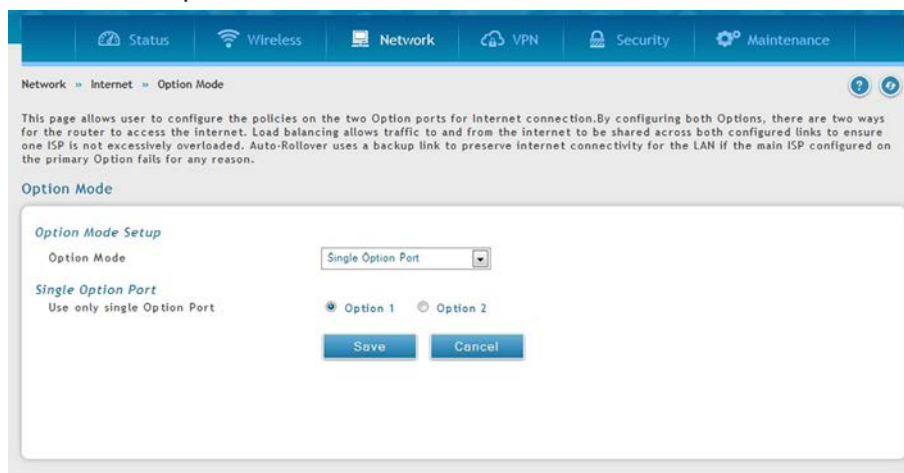


図 6-24 Option MODE 画面

2. 以下の情報を表示または指定します。

項目	説明
Option Mode Setup	単一の Option ポートのみ使用する場合「Single Option Port」を選択します。 • Single Option Port - LAN に 1 つの ISP 接続を設定する場合に選択し、ご契約の ISP に接続する Option ポートを選択します。
Single Option Port	使用するオプションポートを「Option1」「Option2」から指定します。

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。

オプションポートを使用した自動ロールオーバー (Auto-Rollover using Option Port)

この場合、ご使用の Option ポートの 1 つはすべてのインターネットトラフィックに対するプライマリインターネットリンクとして割り当てられます。セカンダリ Option ポートは、プライマリリンクが何らかの理由でダウンした場合に冗長性のために使用されます。この機能を有効にする前に両方の Option ポート (Primary、Secondary) には各 ISP に接続する設定を設定する必要があります。セカンダリ Option ポートは、(いずれかのポートがプライマリとして割り当てられている) プライマリリンク上に障害が検出されるまで、未接続状態のままとなります。プライマリポート上に障害が発生すると、すべてのインターネットトラフィックがバックアップポートに転送されます。「Auto Failover」モードに設定されると、プライマリ Option ポートのリンクステータスは、障害検出設定によって定義された間隔でチェックされます。

以下の項目があります。

1. Network > Internet > Option 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。

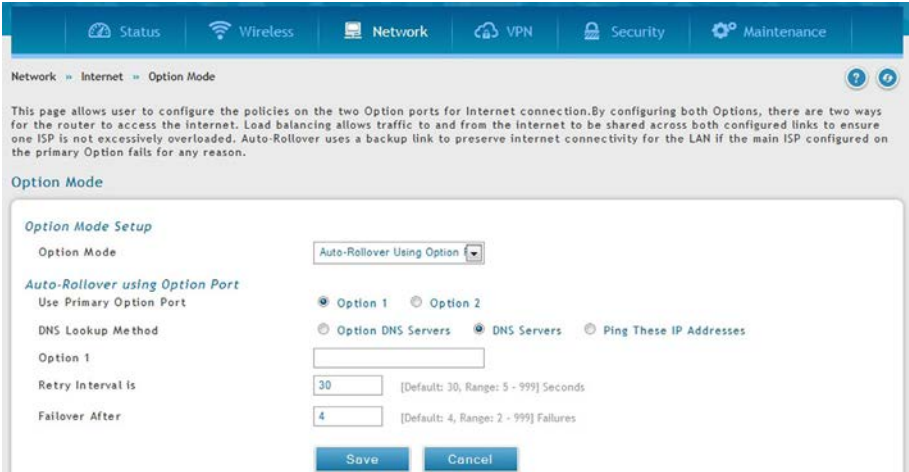


図 6-25 Option MODE (Auto-Rollover using Option Port) 画面

2. 以下の情報を表示または指定します。

項目	説明
Option Mode	<ul style="list-style-type: none">Auto-Rollover using Option port - バックアップの目的で冗長な ISP リンクの使用を希望する場合に選択し、このモードのためのプライマリリンクとして機能する Option ポートを選択します。これを有効にする前にバックアップ Option ポートが設定されていることを確認してください。設定すると、ステータスを検出するために一定間隔でプライマリリンクの接続をチェックします。
Auto-Rollover using Option port	
Use Primary Option Port	プライマリの Option ポートを「Option1」「Option2」から指定します。
Use Secondary Option Port	セカンダリの Option ポートを「Option1」「Option2」から指定します。
DNS lookup Method	<ul style="list-style-type: none">Option DNS Servers - プライマリリンクの DNS サーバの DNS 検索は、プライマリ Option の接続性を検出するのに使用されます。DNS Servers - プライマリリンクの接続性をチェックするためにカスタム DNS サーバの DNS 検索を指定できます。Ping these IP addresses - これらの IP はプライマリリンクの接続性をチェックするために一定の間隔で ping されます。<ul style="list-style-type: none">Option 1/Option 2 : Ping する DNS サーバまたは IP アドレスを入力します。
Retry Interval	上で設定した故障検出方法をコントローラが実行するべき頻度を指定します。
Failover after	これはフェイルオーバーが開始される再試行の数を設定します。

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。

ロードバランシング (Load Balancing)

本機能により、同時に複数の Option リンク（および、おそらく複数の ISP）を使用することができます。1 つ以上の Option ポートを設定後、ロードバランシングオプションは、1 つ以上のリンクにトラフィックを送信できるようになります。プロトコルバインディングは、インターネットフローを管理するために 1 つ以上の Option ポートにサービスを分けて、割り当てるのに使用されます。ロードバランシングモードの場合、定義済み故障検出方式は、すべての設定済み Option ポート上で定期的に使用されます。

DWC-1000 は、現在、ロードバランシングのために 3 つのアルゴリズムをサポートしています。

- Round Robin : このアルゴリズムは、1 つの Option ポートの接続速度が他の速度と大きく異なる場合に特に役に立ちます。この場合、低い待ち時間であるサービス（VOIP など）をより高速なリンクに送信し、低容量のバックグラウンドトラフィック（SMTP など）は低速のリンクに転送するようにプロトコルバインディングを定義できます。プロトコルバインディングは次のセクションで説明します。
- Spill Over : スピルオーバー方式が選択されると、しきい値に達するまで、Option1 は専用リンクとして機能します。この後、Option2 は新しい接続に使用されます。次のオプションを使用することによって、スピルオーバーモードを設定できます。:
 - Load Tolerance : コントローラがセカンダリ Option に切り替わる最大帯域幅 (%) です。
 - Max Bandwidth : この数値にはプライマリ Option で許可される最大の帯域幅を設定します。

リンクの帯域が最大帯域数のロードトレランスを上回ると、コントローラは次の接続をセカンダリ Option に切り替えます。

例えば、プライマリ Option の最大帯域幅が 1Kbps であり、ロードトレランスが 70 に設定される場合です。新しい接続が確立されるたびに、帯域幅は増加します。ある接続数で帯域幅が 1Kbps の 70% に到達すると、新しい接続はセカンダリ Option に切り替えられます。ロードトレランスの最大値は 80 であり、少なくとも 20 とします。

ロードバランシングは、1 つの Option ポートの接続速度が他の速度と大きく異なる場合に特に役に立ちます。この場合、待ち時間が短いサービス（VOIP など）をより高速なリンクに送信し、低容量のバックグラウンドトラフィック（SMTP など）は低速のリンクに転送するようにプロトコルバインディングを定義できます。

Round Robin (ラウンドロビン)

ロードバランシングにおけるアルゴリズムの一つ「Round Robin」について説明します。

1. **Network > Internet > Option 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。

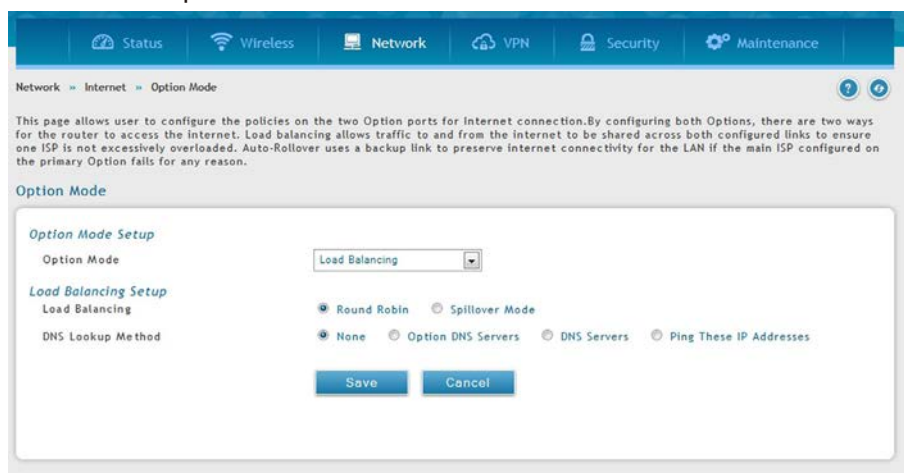


図 6-26 Option MODE (Round Robin) 画面

2. 以下の情報を表示または指定します。

項目	説明
Option Mode	Load Balancing を選択します。
Load Balancing	Round Robin を指定します。
DNS lookup Method	<ul style="list-style-type: none"> • None - DNS Lookup を指定しません。 • Option DNS Servers - DNS サーバの DNS 検索は、プライマリ Option の接続性を検出するのに使用されます。 • DNS Servers - プライマリリンクの接続性をチェックするためにカスタム DNS サーバの DNS 検索を指定できます。 • Ping these IP addresses - これらの IP はプライマリリンクの接続性をチェックするために一定の間隔で ping されます。

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。

Spillover（スピルオーバー）

ロードバランシングにおけるアルゴリズムの一つ「Spillover」について説明します。

1. Network > Internet > Option 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。

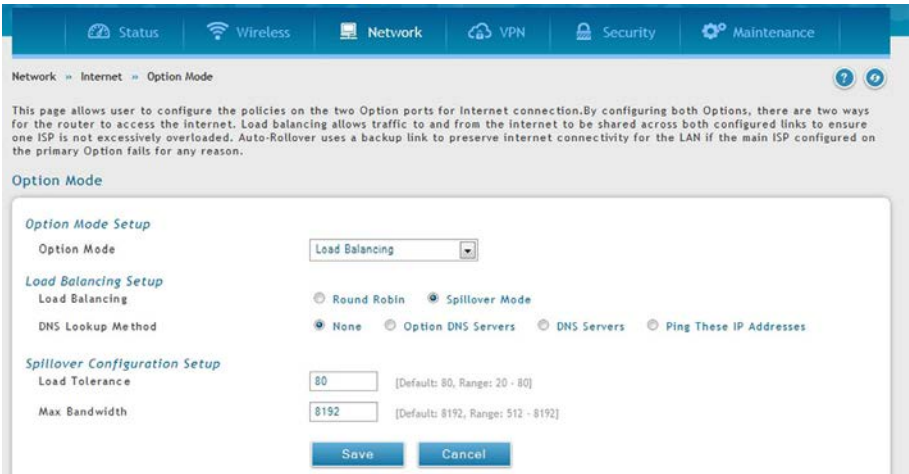


図 6-27 Option MODE（Spillover）画面

2. 以下の情報を表示または指定します。

項目	説明
Option Mode	Load Balancing を選択します。
Load Balancing	Spillover Mode を指定します。
DNS lookup Method	<ul style="list-style-type: none">None - DNS Lookup を指定しません。Option DNS Servers - DNS サーバの DNS 検索は、プライマリ Option の接続性を検出するのに使用されます。DNS Servers - プライマリリンクの接続性をチェックするためにカスタム DNS サーバの DNS 検索を指定できます。Ping these IP addresses - これらの IP はプライマリリンクの接続性をチェックするために一定の間隔で ping されます。
Load Tolerance	コントローラがセカンダリ Option に切り替わる最大帯域幅 (%) です。
Max Bandwidth	この数値にはプライマリ Option で許可される最大の帯域幅を設定します。

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。

ルーティング設定

Network > Internet > Routing メニュー

注意 本機能は追加ライセンス「DWC-1000-VPN」が有効の場合にのみ利用可能です。

LAN と WAN 間のルーティングは、本コントローラが物理インタフェースのいずれに受信されるトラフィックを処理する方法に影響を与えます。ゲートウェイのルーティングモードは安全な LAN とインターネット間のトラフィックフローの動作におけるコアとなります。

NAT or Classical (ルーティングモードの設定)

Network > Internet > Routing メニュー

NAT、クラシカルルーティング、および透過などの異なるルーティングモードを設定します。また、RIP (Routing Information Protocol) を設定することもできます。

このデバイスは従来のルーティング、ネットワークアドレス変換 (NAT)、および転送モードのルーティングをサポートしています。

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

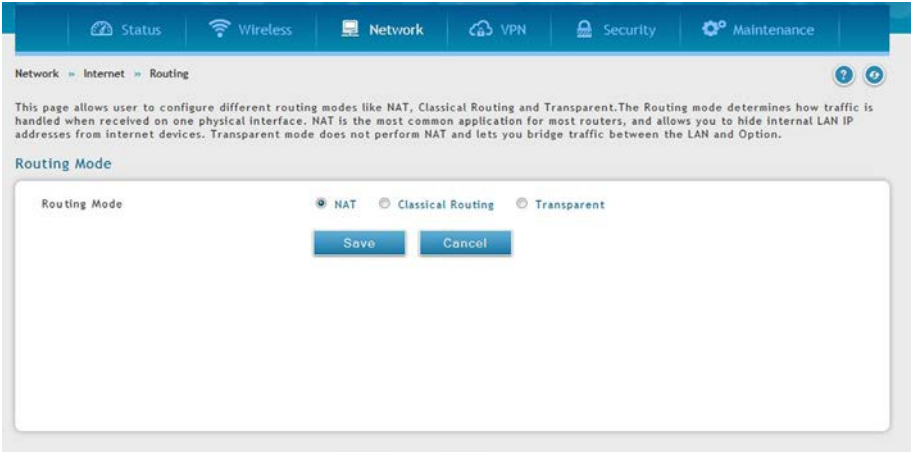


図 6-28 ルーティングモード設定

2. 以下の情報を表示または指定します。

項目	説明
Routing Mode	
NAT	NAT は LAN の複数のコンピュータがインターネット接続を共有できる技術です。LAN 上のコンピュータは「プライベート」の IP アドレス範囲を使用し、一方、コントローラの Option ポートは一つの「パブリック」IP アドレスに設定されます。接続共有と共に、NAT は内部の IP アドレスをインターネット上のコンピュータから隠します。NAT は、ISP が 1 つの IP アドレスだけを割り当てた場合にだけ必要とされます。コントローラ経由で接続するコンピュータは、プライベートサブネットから IP アドレスを割り当てられることが必要です。
Classical Routing	従来のルーティングを使用する場合、LAN 上のデバイスにはそれらのパブリック IP アドレスでインターネットから直接アクセスできます (適切なファイアウォールが設定であると仮定します)。ISP がご使用の各コンピュータに IP アドレスを割り当てた場合には、「Classic Routing」を選択します。
Transparent	LAN と Option 間の透過ルーティングは NAT を実行しません。LAN インタフェースに到着するブロードキャストとマルチキャストパケットは、ファイアウォールまたは VPN ポリシーによってフィルタされない場合、Option に切り換えられます。逆もまた同様です。LAN と Option が同じブロードキャストドメインにある場合に、透過モードを選択します。同じブロードキャストドメインで LAN と Option を維持するためには、「Transparent」モードを選択します。これにより、コントローラを終了するトラフィックおよび他の管理トラフィックを除き、LAN から Option のトラフィック、および Option から LAN のトラフィックをブリッジすることができます。すべての DWC-1000 機能が LAN と Option が同じブロードキャストドメインにあるように設定されるものとする透過モードでサポートされます。

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。

IP エイリアス

Network > Internet > IP Aliasing メニュー

単一の「Option イーサネットポート」はポートにエイリアスを追加することにより、複数の IP アドレスからのアクセスが可能です。IP エイリアスを設定することにより可能になります。既存のエイリアスを追加、または編集する場合右クリックから「Edit」「Delete」を選択し実行します。

注意 本機能は追加ライセンス「DWC-1000-VPN」が有効の場合にのみ利用可能です。

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

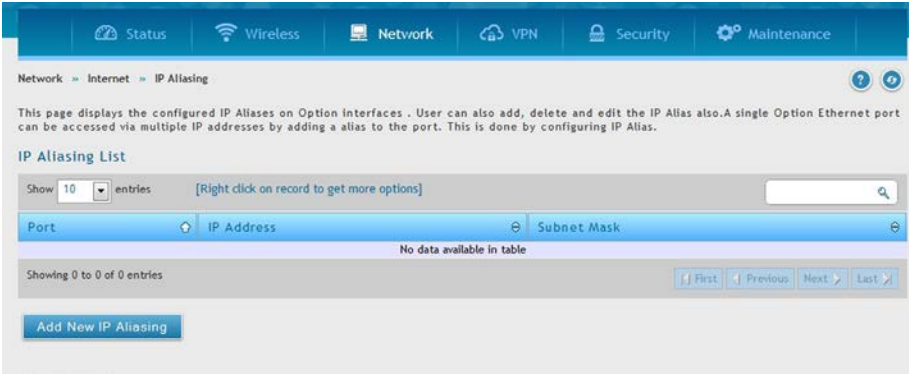


図 6-29 IP Aliases

2. 「Add New IP Aliasing」をクリックし、以下の画面を表示させます。

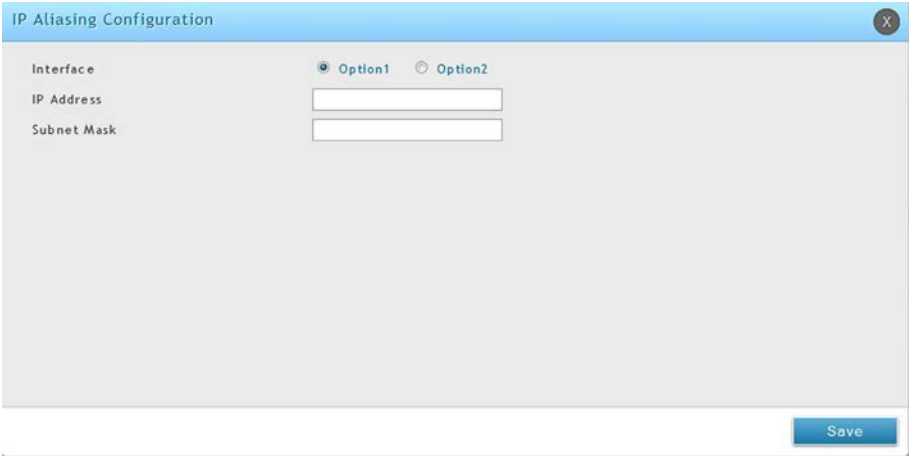


図 6-30 Add New IP Aliasing

項目	説明
Interface	エイリアスが設定するインタフェース。「Option1」「Option2」から選択します。
IP Address	IP エイリアスの IP アドレス
Subnet Mask	IP エイリアスのサブネットマスク

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。

DMZ LAN DHCP Reserved IPs (DMZ DHCP の予約 IP)

Network > Internet > DMZ LAN DHCP Reserved IPs

注意 本機能は追加ライセンス「DWC-1000-VPN」が有効の場合にのみ利用可能です。

DHCP サーバ設定のためにスタティックに予約される IP アドレスを設定します。
コントローラの DHCP サーバは、ネットワーク上の DMZ クライアントに対して IP アドレスと MAC アドレスを追加などの IP 設定を実行することが可能です。クライアントからのリクエストを受けたコントローラは、データベースの MAC アドレスリストとクライアントの MAC アドレスを確認します。もしデータベースのコンピュータ / デバイスに IP アドレスが既にアサインされていた場合、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 DMZ DHCP プールから自動的に IP アドレスがクライアントにアサインされます。

1. Network > Internet > DMZ 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。

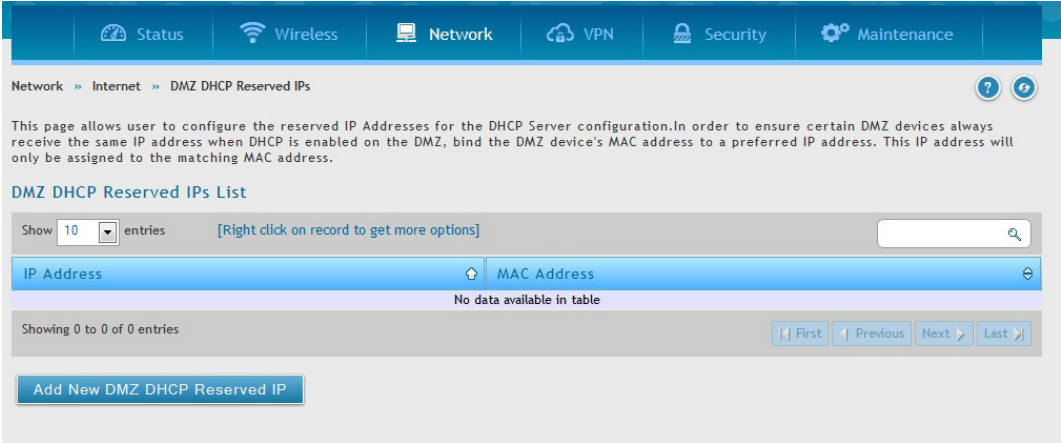


図 6-31 DMZ LAN DHCP Reserved IPs (DMZ)

2. 「Add New DMZ DHCP Reserved IP」 ボタンをクリックして以下の画面を表示します。

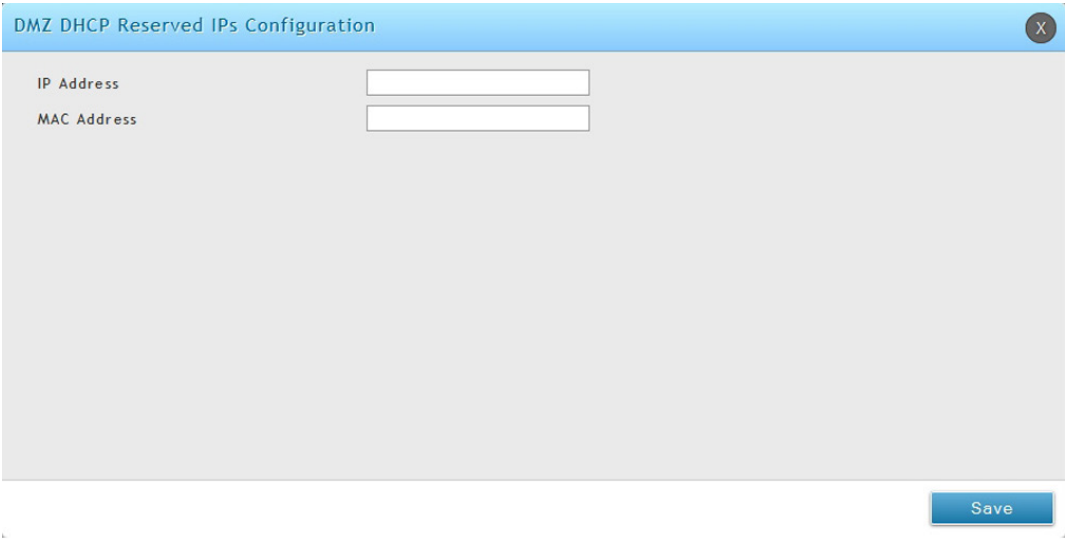


図 6-32 DMZ DHCP 予約 IP アドレスの登録

3. 以下の項目を入力します。

項目	説明
IP Address	DHCP サーバが予約するホストの DMZ IP アドレス。
MAC Address	予約された IP アドレスが割り当てられる MAC アドレス。

4. 「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。

ダイナミック DNS の設定

Network > Internet > Dynamic DNS メニュー

ダイナミック DNS を設定します。

注意 本機能は追加ライセンス「DWC-1000-VPN」が有効の場合にのみ利用可能です。

ダイナミック DNS (DDNS) は、変化するパブリック IP アドレスを持つコントローラがインターネットのドメイン名を使用して設置できるインターネットのサービスです。DDNS を使用するためには、[DynDNS.org](#)、[DlinkDDNS.com](#) または [Oray.net](#) などの DDNS プロバイダでアカウントをセットアップする必要があります。必要であれば、各設定済み Option は異なる DDNS サービスを持つことができます。

設定後、コントローラは、FQDN 経由でコントローラの Option にアクセスするのに依存する機能が正しい IP アドレスに向けられるように、Option IP アドレスにおける DDNS サービスの変更を更新します。DDNS サービス、ホスト、およびドメイン名でアカウントをセットアップする場合、ユーザ名、パスワード、およびワイルドカードのサポートはアカウントプロバイダによって提供されます。

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

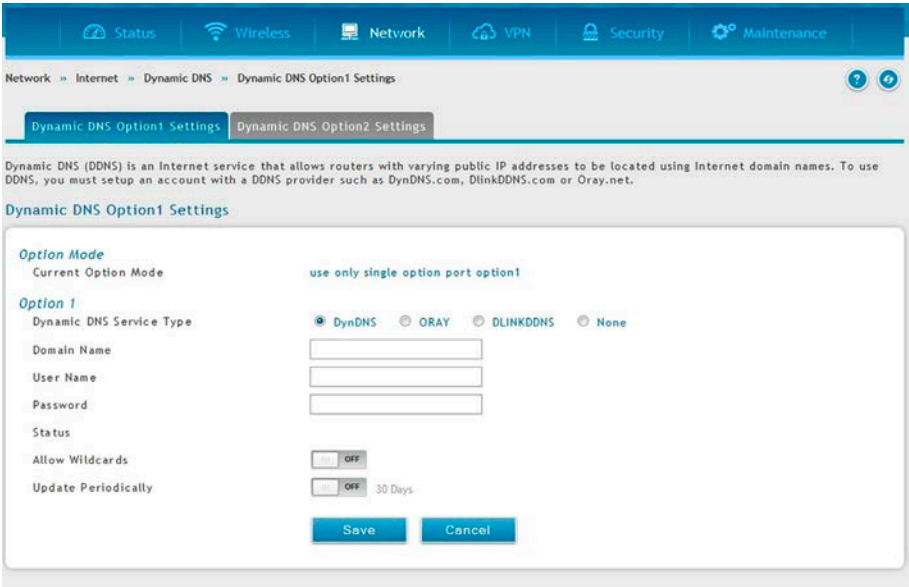


図 6-33 Dynamic DNS 設定

2. 以下の項目を入力します。

項目	説明
User Name	DDNS のユーザ名を入力します。
Domain Name	ドメイン名を入力します。
Password	DDNS パスワードを入力します。
Status	現在の接続状況を表示します。
Allow Wildcards	「ON」にしてワイルドカードを指定します。
Update Periodically	「ON」にし定期的な自動アップデートを指定します。

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。

VLAN 設定

Network > VLAN メニュー

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。独立した論理網は一つの物理ネットワークにだけ作成を許可されます。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、設定

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。

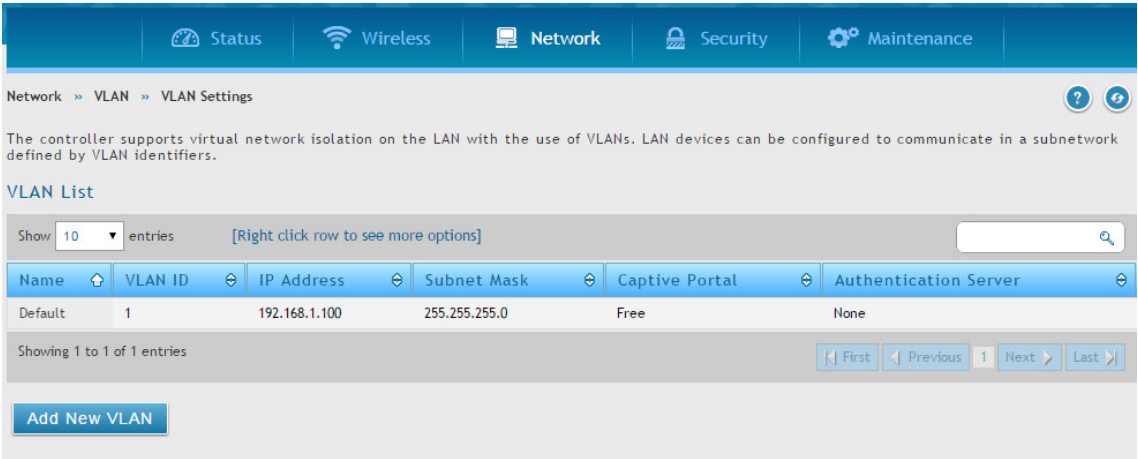


図 6-34 VLAN List 画面

2. 「Add New VLAN」 ボタンをクリックします。

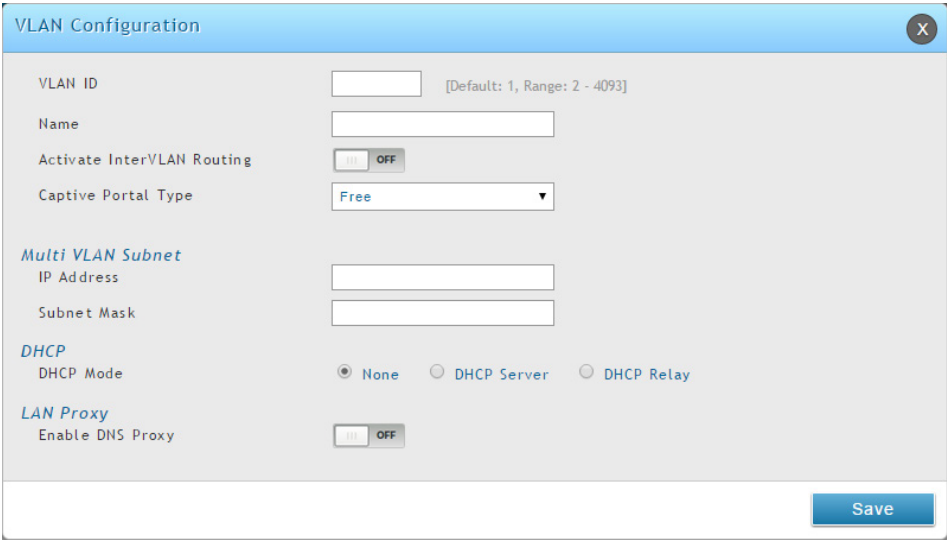


図 6-35 VLAN Configuration 画面

3. 以下の項目を入力します。

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、これから追加する他のものから、この VLAN を容易に特定できるものにすべきです。
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。 <ul style="list-style-type: none">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タイプのタイプ (Free、SLA、Permanent User、Temporary User または Billing User) を選択します。

高度なネットワーク設定

項目	説明
Enable Redirect	リダイレクトを有効にします。表示される「URL」欄にリダイレクト先の URL を入力します。
Authentication Server	「Permanent User」、「Temporary User」または「Billing User」でキャプティブポータルを認証するため、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。
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」「Custome Profile」から選択します。
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	使用する LAN 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。

4. 「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。

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。

The image shows a 'VLAN Configuration' dialog box with a blue header and a close button (X) in the top right corner. The settings are as follows:

- VLAN ID:** 1
- Name:** Default
- Activate InterVLAN Routing:** ON (with a toggle switch)
- Captive Portal Type:** Free (dropdown menu)
- Multi VLAN Subnet:**
 - IP Address:** 192.168.1.100
 - Subnet Mask:** 255.255.255.0
- DHCP:**
 - DHCP Mode:** None (selected with a radio button), DHCP Server, DHCP Relay
- LAN Proxy:**
 - Enable DNS Proxy:** ON (with a toggle switch)

A 'Save' button is located at the bottom right of the dialog box.

図 6-36 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 を必要としない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 サブネットはこの 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を決定します。

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。

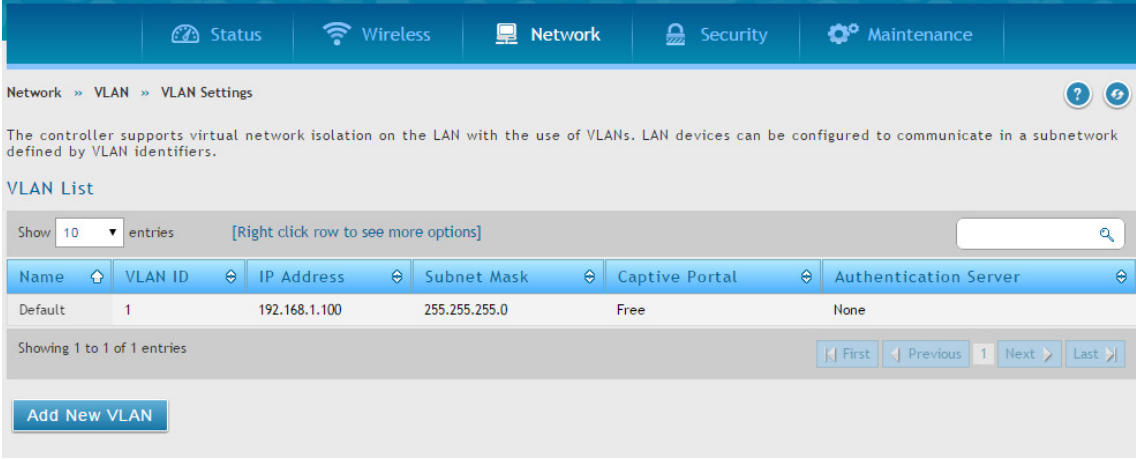


図 6-37 VLAN List 画面

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。

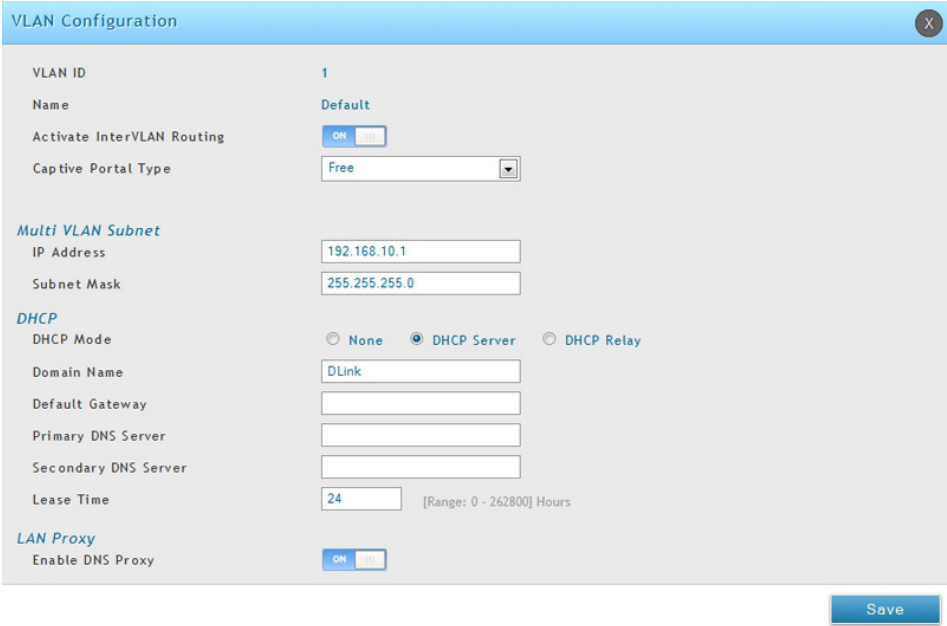


図 6-38 VLAN Configuration 画面

3. 以下の項目を入力します。

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。 <ul style="list-style-type: none">• 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。

項目	説明
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。
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	<p>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「自動ロールオーバー」モードの場合に特に便利です。例えば、各接続用の DNS サーバが異なる場合、リンク障害は DNS サーバへのアクセスを不可能にします。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。</p> <ul style="list-style-type: none">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 クライアントが DNS プロキシが動作している IP (つまり、無線コントローラの LAN IP) に沿ったプライマリ / セカンダリ DNS IP アドレスを受信します。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。

4. 「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。

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。

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。

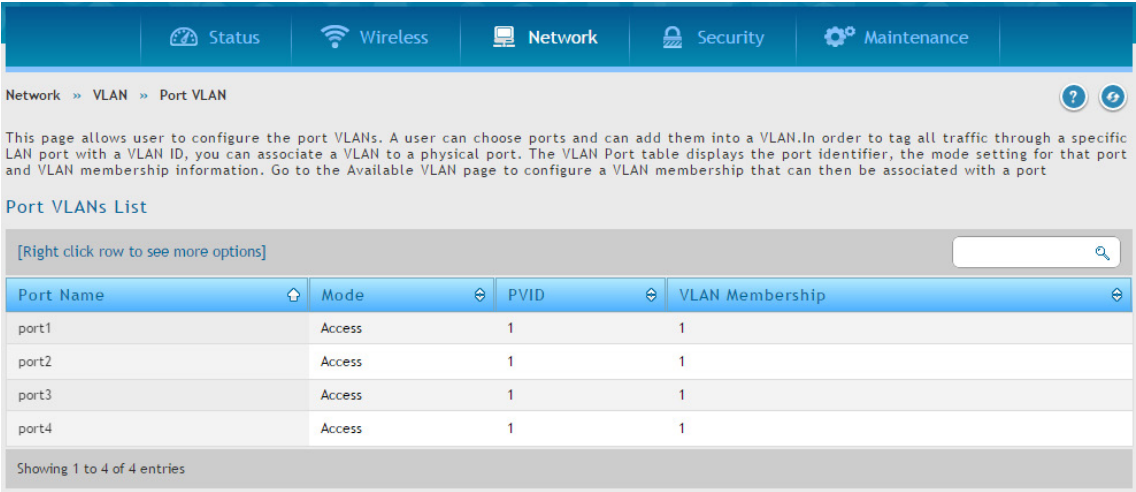


図 6-39 Port VLANs List 画面

2. ポートを右クリックして、「Edit」を選択します。

Port VLAN Configuration

Port Name

Port1

Mode

Access

PVID

1

[Default: 1, Range: 2 - 4093]

Save

図 6-40 Port VLAN Configuration 画面（Access）

Port VLAN Configuration

Port Name

Port1

Mode

Interface

IP Address

Subnet Mask

Gateway

Routing

OFF

Save

図 6-41 Port VLAN Configuration 画面（Interface）

3. 以下の項目を入力します。

項目	説明
Access	他の VLAN からこのポートを分離します。ポートに入力する、また、ポートから出力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 をそれに割り当てます。同じ PVID を持つポートから送信された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。ポートに入力する、またポートから出力され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て設定内容を保存および適用します。

Advanced VLAN（高度な VLAN 設定）

Network > VLAN > Advanced VLAN メニュー

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 分類ルールを受けます。

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 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。

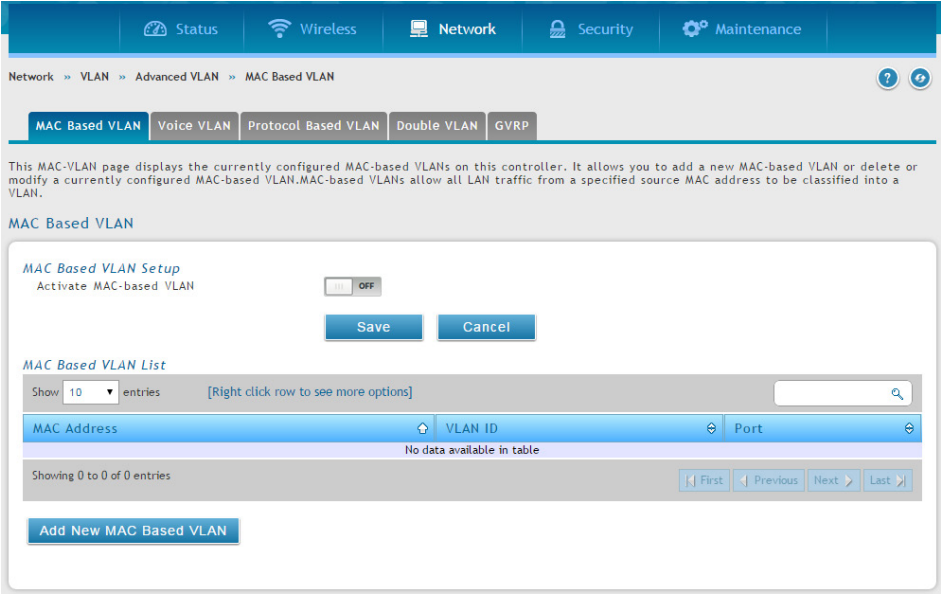


図 6-42 MAC Based VLAN 画面

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。

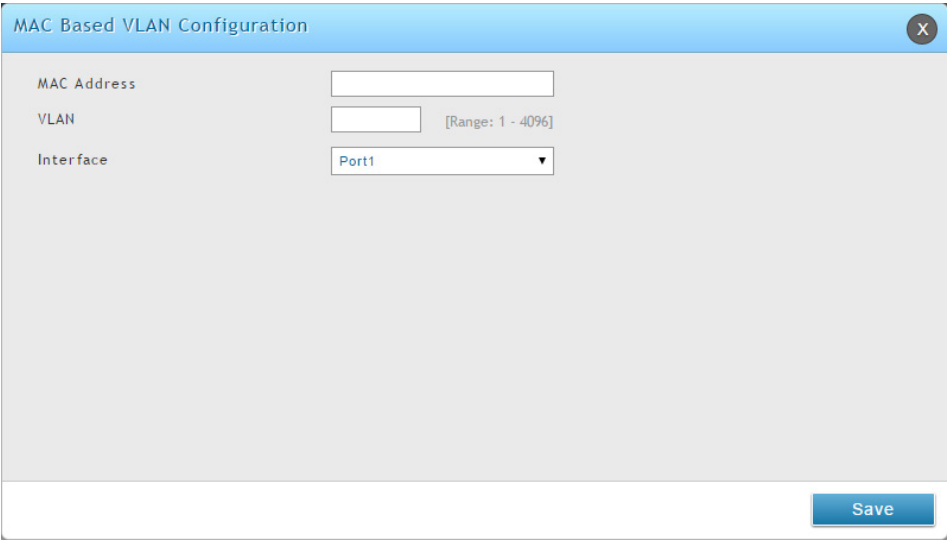


図 6-43 MAC Based VLAN Configuration 画面

4. 以下の項目を入力します。

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。

5. 「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。

音声 VLAN

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

音声 VLAN 機能により、コントローラのポートは、ポートに到着した時に音声とデータトラフィックに分離するように定義した設定を使用して音声トラフィックを送信することができます。音声 VLAN は、ポートのデータトラフィックが高い時に、IP 電話の音声品質の劣化から確実に保護します。

VLAN が提供する固有の隔離機能は、インター VLAN トラフィックを管理制御下におき、ネットワークに付属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 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。

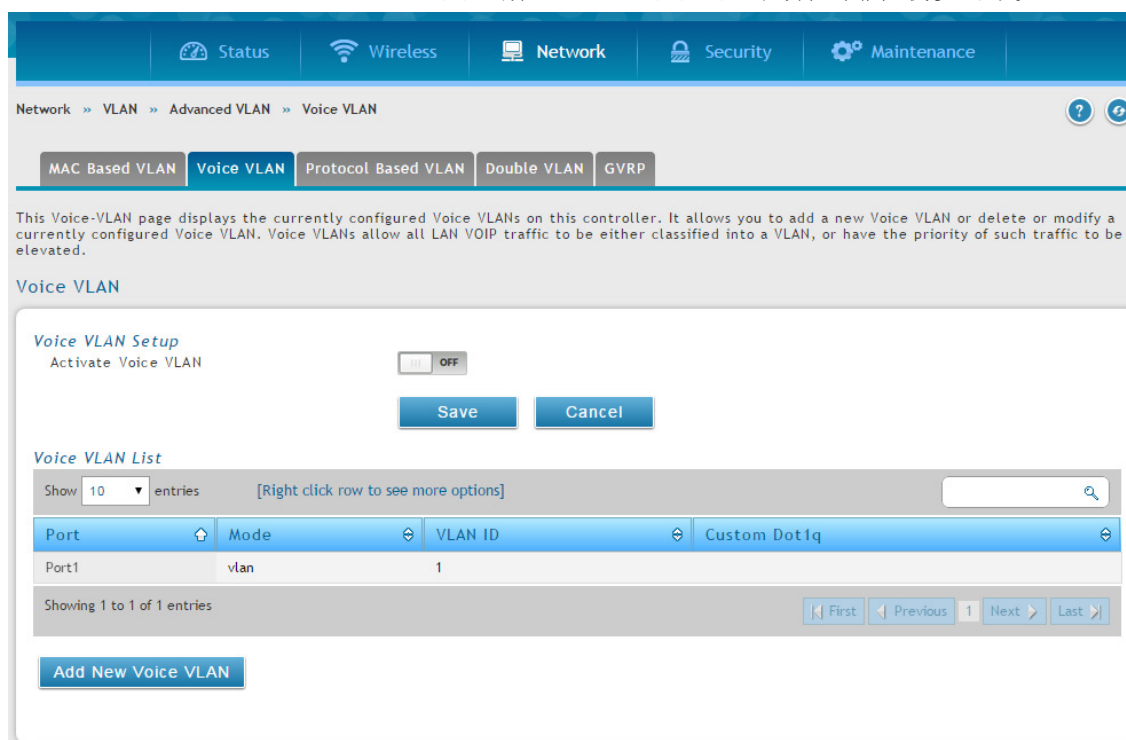


図 6-44 Voice VLAN 画面

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。

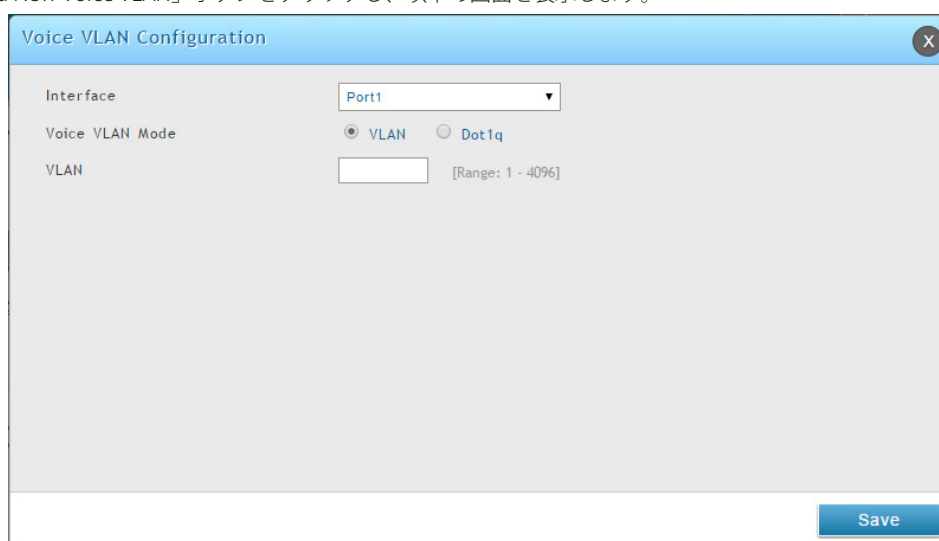


図 6-45 Voice VLAN Configuration 画面

4. 以下の項目を入力します。

項目	説明
VLAN	音声 VLAN パケットは割り当てる番号によってユニークに識別されます。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 に送信します。しかし、音声トラフィックは他のトラフィックと異なり最優先にされません。
Dot1q	VoIP デバイスによってすべての音声トラフィックが他のトラフィックと音声データを区別するように設定されます。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。

5. 「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。

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 packets 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が複数のプロトコルを実行しているホストを含む状況で使用されます。タグなしパケットのフィルタリング基準を定義するの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、この動作を書き換えることができます。タグ付きパケットは、IEEE 802.1Q 標準に従って常に処理されており、プロトコルベースの VLAN には含まれていません。

特定のプロトコルにプロトコルベースの VLAN にポートを割り当てると、そのプロトコルのそのポートに受信したタグなしフレームは、プロトコルベースの VLAN ID に割り当てられます。他のプロトコルのためにポートに受信したタグなしフレームが PVID に割り当てられます。これは、「Port VLAN Configuration」画面を使用してポートに明確に割り当てたデフォルト PVID (1) または PVID のどちらかです。「Protocol-Based VLAN Configuration」画面を使用して、どのプロトコルが、どの VLAN に向かうかを設定し、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 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。

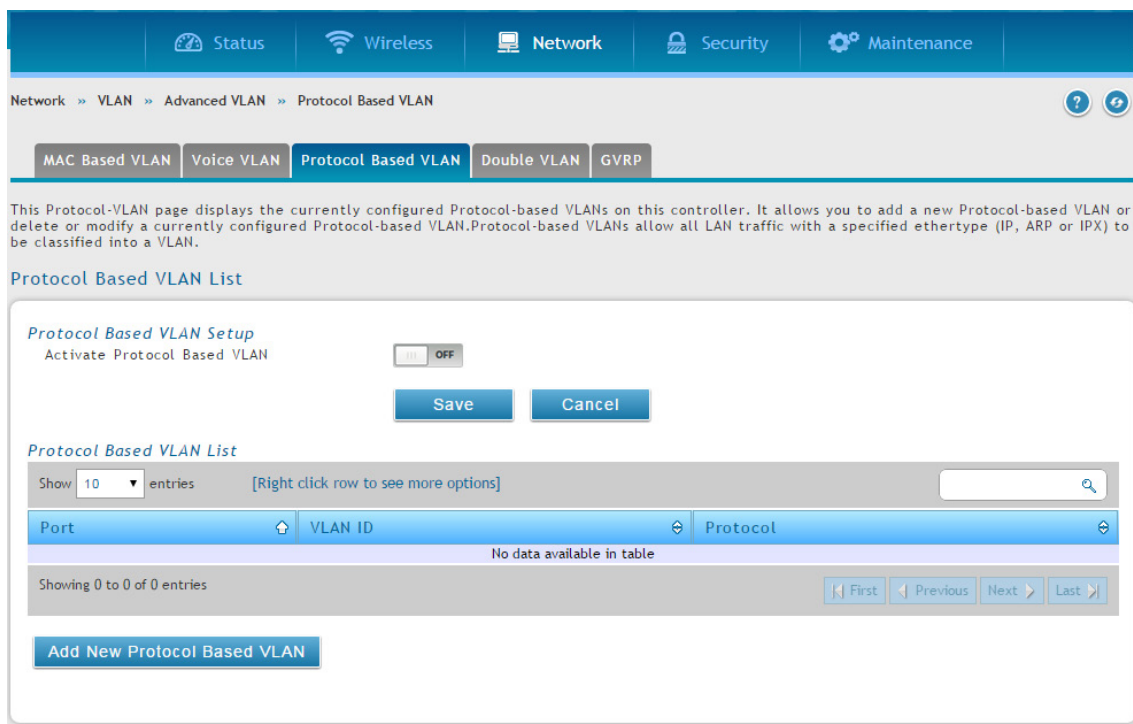


図 6-46 Protocol Based VLAN List 画面

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。

Protocol Based VLAN Configuration

VLAN ID

[Range: 1 - 4096]

Group ID

[Range: 1 - 4096]

Group Name

Interface

Port1

Protocol List

☒ IP ☐ IPX ☐ ARP

Save

図 6-47 Protocol Based VLAN Configuration 画面

4. 以下の項目を入力します。

項目	説明
VLAN ID	このグループに割り当てる VLAN ID (1-3965) 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ー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。

5. 「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。

ダブル VLAN

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

ダブル VLAN トネリングは、ネットワークトラフィックに 2 個目のタグの使用を許可します。追加のタグは、自身の 802.1Q ドメインの入力時に個別のカスタマの VLAN 識別子を保持していると、メトロポリタンネットワーク (MAN) においてカスタマの識別を補助します。

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のに 4k VLAN ID のスペースを分割する必要はありません。ダブル VLAN トネリングが有効な場合、インターフェースから転送されるあらゆるフレームは DVlan タグを割り当て、一方、インターフェースから受信するあらゆるパケットは (1 つ以上のタグが存在すると) タグを削除します。

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

1. Network > VLAN > Advanced VLAN > Double VLAN 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。

StatusWirelessNetworkSecurityMaintenance

Network >> VLAN >> Advanced VLAN >> Double VLAN

MAC Based VLANVoice VLANProtocol Based VLANDouble VLANGVRP

This Double-VLAN page displays the status of Double VLAN Setting on this controller. It allows you to enable or disable the double VLANs.Enabling double VLANs will force all LAN traffic to have two VLAN tags attached to them.

Double VLAN

Show 10 entries [Right click row to see more options]

Interface

Ether Type

Custom Tag

No data available in table

Showing 0 to 0 of 0 entries

FirstPreviousNextLast

Add New Double VLAN

図 6-48 Double VLAN 画面

137

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。

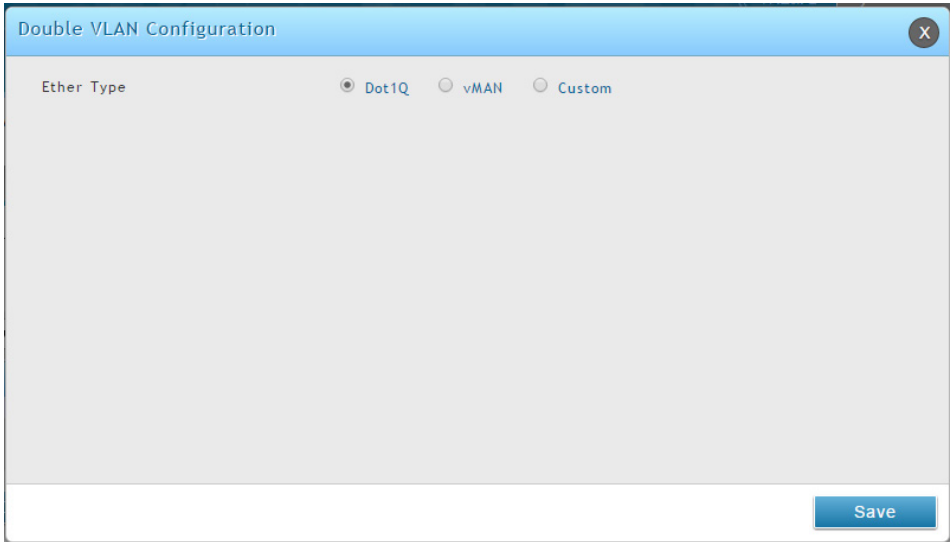


図 6-49 Double VLAN Configuration 画面

3. 「Ether Type」を選択します。(Dot1q、VLAN または Custom)
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を持つ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 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。

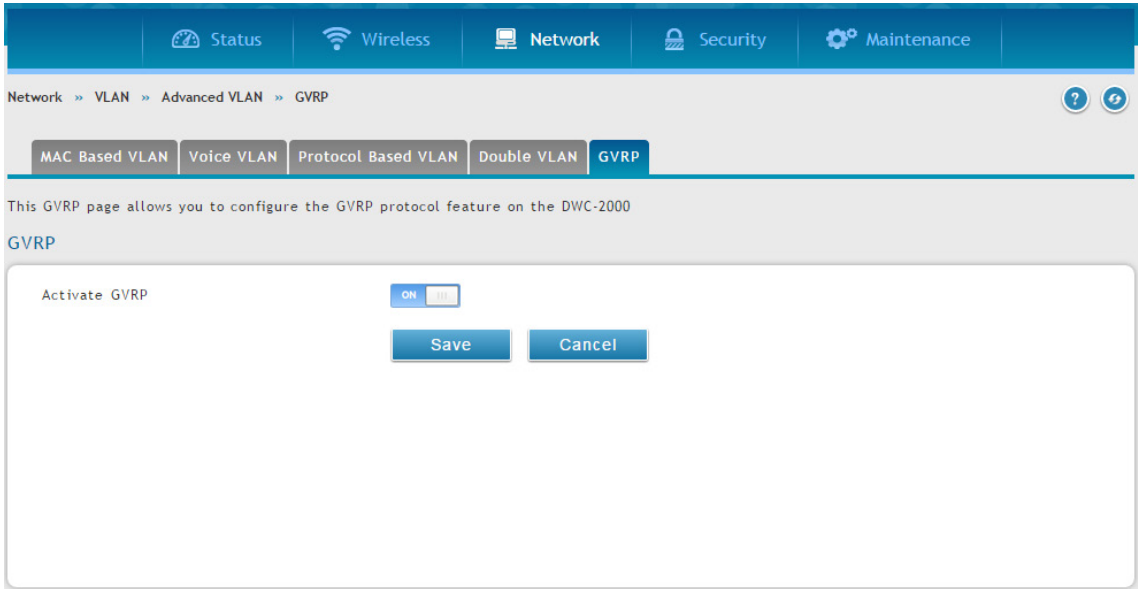


図 6-50 GVRP 画面

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

Network > Routing メニュー

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（変更できない）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うまく動作します。2 種類のスタティックルートがあります。:「Static Route」 および 「Protocol-Binding」

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のに 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 > Static Routes メニュー

スタティックルートの追加

1. Network > Routing > 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。

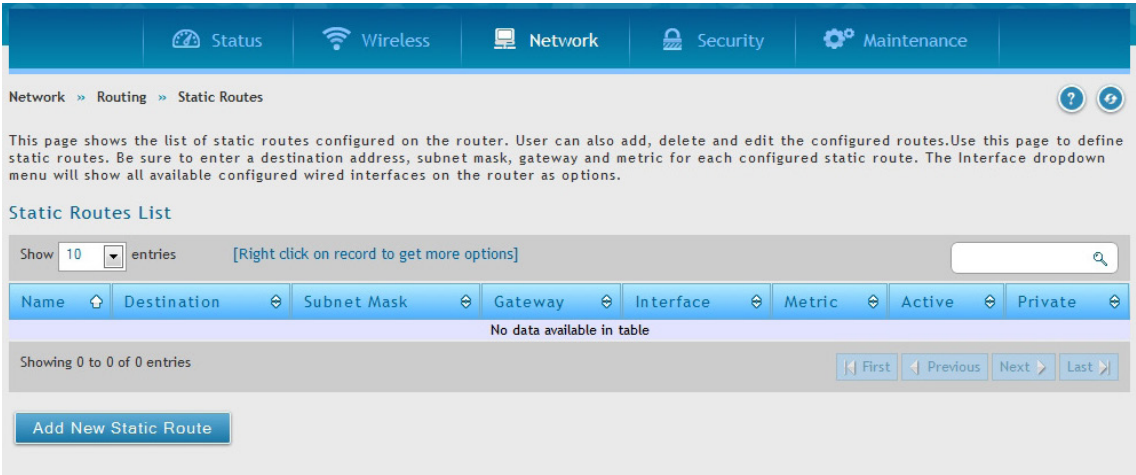


図 6-51 Static Route List 画面

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。

Static Route Configuration

Route Name

Active

☐ OFF

Private

☐ OFF

Destination IP Address

IP Subnet Mask

Interface

LAN > VLAN

Gateway IP Address

Metric

[Range: 2 -15]

Save

図 6-52 Static Route Configuration 画面

3. 以下の項目を入力します。

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、これから追加する他のものから、このスタティックルートを容易に特定できるものにするべきです。
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。 <ul style="list-style-type: none">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。

項目	説明
Private	スタティックルートをプライベートに指定します。 <ul style="list-style-type: none">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	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。 <ul style="list-style-type: none">Option 1/ Option 2 - 無線コントローラの Option ポートがスタティックルートに接続します。LAN > VLAN - 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。DMZ - DMZ として設定されたポートがスタティックルートに接続します。
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。

4. 「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。

IPv6 スタティックルーティングの設定

Network > IPv6 > Static Routing 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。経路に変更を説明するために、このコントローラと他のデバイス間の通信はありません。一度設定されると、ネットワークの変更があるまで、スタティックルートは、アクティブで有効です。

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いくつかの操作を許可します。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同じフィールドを共有します (1つの例外があります)。

IPv6 スタティックルーティングの設定

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

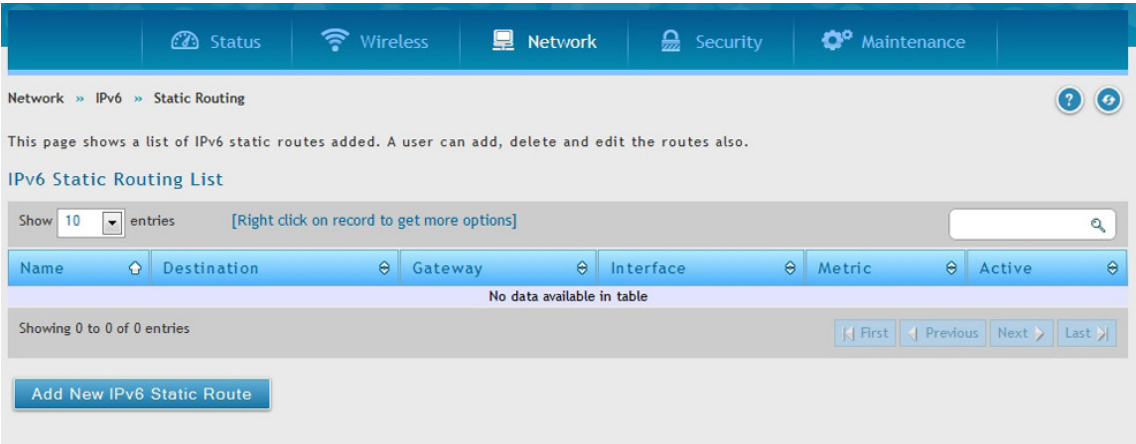


図 6-53 IPv6 Static Routing List 画面

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。

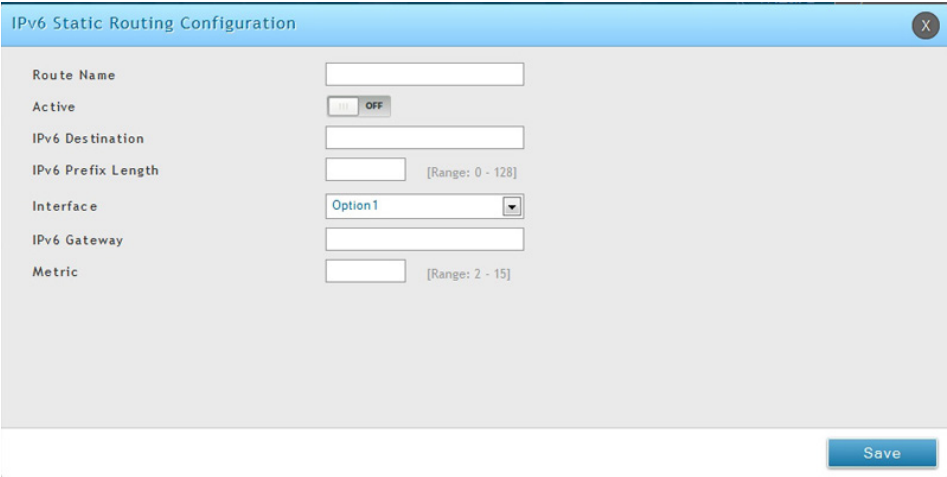


図 6-54 IPv6 Static Routing Configuration 画面

3. 以下の項目を入力します。

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、これから追加する他のものから、このスタティックルートを容易に特定できるものにするべきです。
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。 <ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> 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。

4. 「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。

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。

ダイナミックルーティング (RIP)

Network > Routing > RIP メニュー

RIP (Routing Information Protocol) を使用したダイナミックルーティングは、LAN に一般的に使用される IGP (Interior Gateway Protocol) です。本コントローラは、RIP を使用してトラフィックフローを中断しないで LAN 内の変更を適用するために、LAN 内で他のサポートしているコントローラとルーティング情報を交換して、ルーティングテーブルのダイナミックな調整を行うことができます。

注意 本機能は追加ライセンス「DWC-1000-VPN」が有効の場合にのみ利用可能です。

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

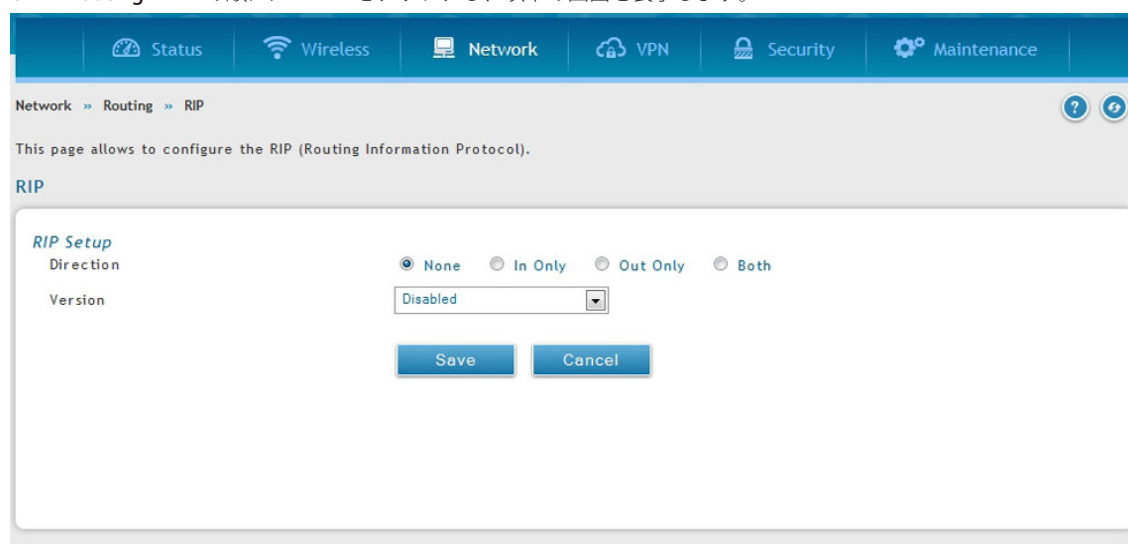


図 6-55 RIP 画面

2. 以下の項目を入力します。

項目	説明
Direction	<p>コントローラが RIP パケットを送受信する方法を定義します。</p> <ul style="list-style-type: none"> Both - コントローラは双方向でルーティングテーブルをブロードキャストし、他のコントローラから受信した RIP 情報を処理します。RIP 機能をフルに活用するためには、この設定をお勧めします。 Out Only - コントローラは定期的にルーティングテーブルをブロードキャストしますが、他のコントローラから RIP 情報を受信しません。 In Only - コントローラは他のコントローラから RIP 情報を受信しますが、ルーティングテーブルをブロードキャストしません。 None - コントローラはルーティングテーブルのブロードキャスト、および他のコントローラから到着する RIP 情報の受信のいずれもしません。事実上、これは RIP を無効にします。
Version	<p>RIP バージョンは LAN 内の他のルーティングデバイスの RIP サポートに依存します。</p> <ul style="list-style-type: none"> Disabled - RIP を無効にする場合に、これを設定します。 RIP-1 - サブネット情報を含んでいないクラスベースのルーティングバージョンです。これは最も一般的にサポートされるバージョンです。 RIP-2 - RIPv1 のすべての機能に加え、サブネット情報をサポートします。データは RIP-2B と RIP-2M の両方に RIP-2 形式で送信されますが、パケットが送信されるモードは異なります。 <ul style="list-style-type: none"> RIP-2B - サブネット全体にデータをブロードキャストします。 RIP-2M - マルチキャストアドレスにデータを送信します。 <p>RIP-2B または RIP-2M が選択されたバージョンであれば、このコントローラと他のコントローラ（同じ RIP バージョンで設定済み）間には認証が必要となります。MD5 認証は第 1 / 第 2 キーの交換処理で使用されます。ルーティング情報の交換が LAN 上で検出された現在の、およびサポートされているコントローラと共に行われることを保証するために、認証キーの有効なライフタイムを設定することができます。</p>

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。

OSPF 設定

Network > Routing > OSPF メニュー

OSPF はシングルルーティングドメイン内のインターネットプロトコル (IP) パケットをルートする内部ゲートウェイプロトコルです。使用可能なコントローラの情報を収集し、ネットワークのトポロジマップを生成します。OSPFv2(バージョン 2) は「RFC2328 - OSPF Version 2」によって定義されたルーティングプロトコルです。(OSPF は「IGP」(Interior Gateway Protocols) です。) OSPF は ISP バックボーンやエンタープライズネットワークなどの巨大ネットワークで広く使用されています。

注意 本機能は追加ライセンス「DWC-1000-VPN」が有効の場合にのみ利用可能です。

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

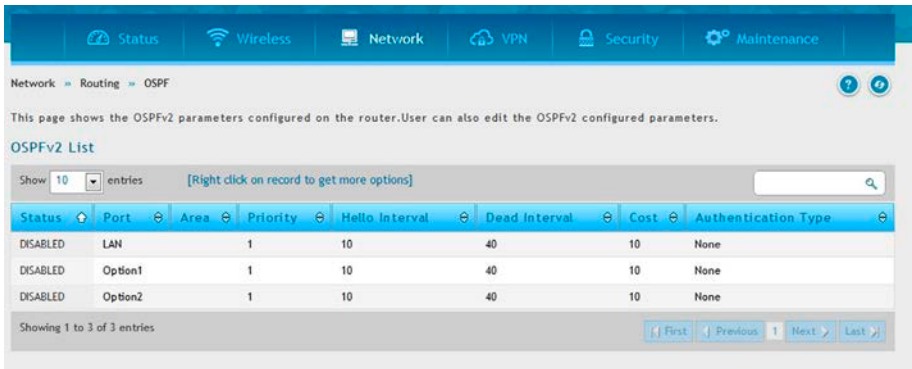


図 6-56 OSPF - IPv4 画面

2. 編集するポート（LAN/Option1/Option2）で右クリック、「Edit」を選択、以下の画面を表示します。

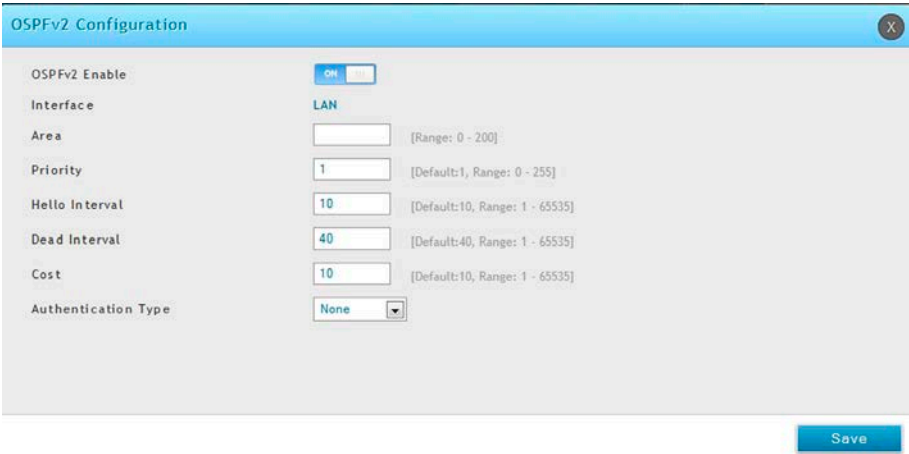


図 6-57 OSPFv2 Configuration 画面

3. 以下の項目を入力します。

項目	説明
OSPFv2 Enable	OSPFv2 を有効 / 無効にします。
Interface	OSPFv2 を有効 / 無効にする物理ネットワークインタフェース。
Area	インタフェースが所属するエリア。1-200の値を入力します。共通セグメントを持つ2つのルータ: それらのインタフェースはセグメントで同じエリアに所属する必要があります。インタフェースは同じサブネットに属し、同一のサブネットマスクを持ちます。
Priority	ネットワークの OSPFv2 代表ルータを決定するのを補助します。高い優先度を持つルータほど代表ルータになる可能性が高くなります。値を 0 に設定すると、ルータはより代表ルータになる可能性が高くなります。初期値は 1 です。低い番号ほど高い優先度を意味します。
Hello Interval	Hello インターバル値（秒）。この値を設定すると、特定のインタフェースに設定時間ごとに Hello パケットが送信されます。本値は共通ネットワークに接続する全ルータで同じである必要があります。初期値は 10（秒）です。
Dead Interval	Hello パケットが受信されなくなってから、Neighbor ルータがその OSPF ルータがダウンしていると判断するまでの時間（秒）。本値は共通ネットワークに接続する全ルータで同じである必要があります。初期値は 40（秒）です。OSPF では、2つの Neighbor 間でこれらのインターバルの値が全く同じである必要があります。異なるインターバル値を持つルータ同士はそのセグメントにおいて Neighbor ルータになることができません
Cost	OSPFv2 インタフェースにパケットを送信するコスト
Authentication Type	この欄では OSPFv2 に使用する認証タイプを表示します。 <ul style="list-style-type: none">• none - インタフェースは OSPF パケットを認証しません。• Simple - インタフェースはシンプルテキストキーを使用して OSPF パケットを認証します。• MD5 - インタフェースは MD5 認証を使用して OSPF パケットを認証します。Md5 を選択した場合、「Md5 Key ID」「Md5 Authentication Key」を指定します。

4. 「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。

OSPFv3 設定 (IPv6)

Network > IPv6 > OSPFv3 メニュー

注意 本機能は追加ライセンス「DWC-1000-VPN」が有効の場合にのみ利用可能です。

OSPF はシングルルーティングドメイン内のインターネットプロトコル (IP) パケットをルートする内部ゲートウェイプロトコルです。使用可能なコントローラの情報を収集し、ネットワークのトポロジマップを生成します。

OSPFv3 は IPv6 をサポートしています。コントローラの OSPFv3 プロセスを有効にするには、OSPFv3 プロセスのグローバルに有効化、コントローラ ID の付与、関連インタフェースの有効化などを行う必要があります。

1. Network > IPv6 > OSPFv3 の順にメニューをクリックし、以下の画面を表示します。

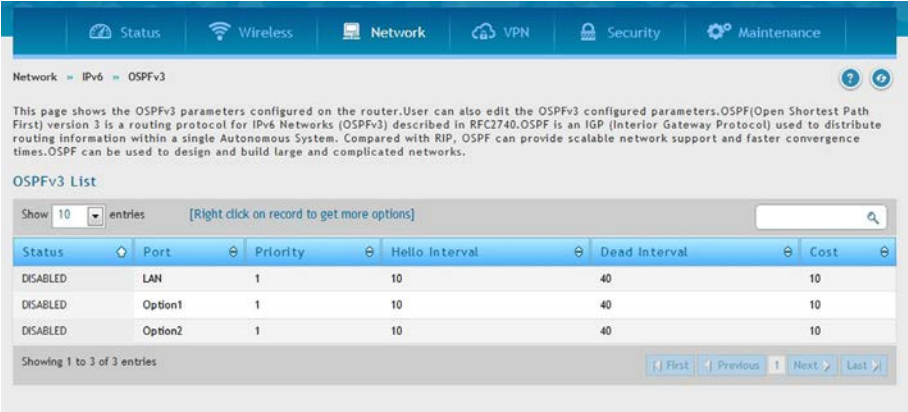


図 6-58 OSPFv3 - IPv6 画面

2. 編集するポート (LAN/Option1/Option2) で右クリック、「Edit」を選択、以下の画面を表示します。

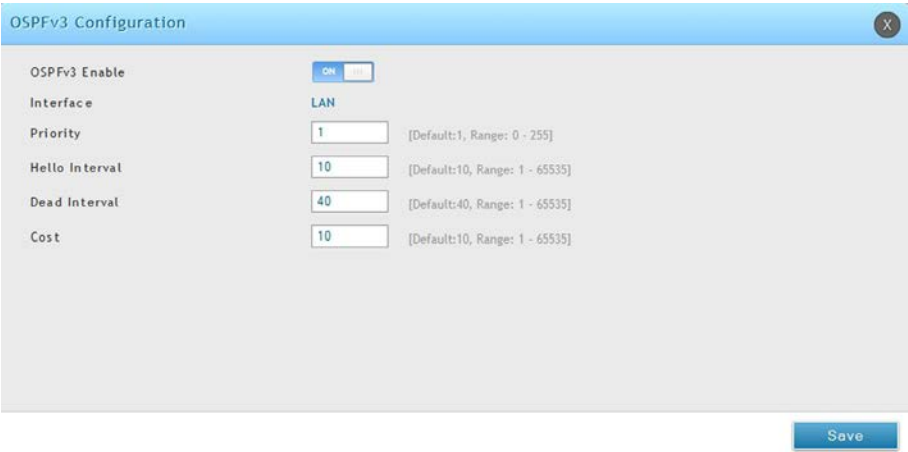


図 6-59 OSPFv2 Configuration 画面

3. 以下の項目を入力します。

項目	説明
OSPFv3 Enable	OSPFv2 を有効 / 無効にします。
Interface	OSPFv3 を有効 / 無効にする物理ネットワークインタフェース。
Priority	ネットワークの OSPFv3 代表ルータを決定するのを補助します。高い優先度を持つルータほど代表ルータになる可能性が高くなります。値を 0 に設定すると、ルータはより代表ルータになる可能性が高くなります。初期値は 1 です。低い番号ほど高い優先度を意味します。
Hello Interval	Hello インターバル値 (秒)。この値を設定すると、特定のインタフェースに設定時間ごとに Hello パケットが送信されます。本値は共通ネットワークに接続する全ルータで同じである必要があります。初期値は 10 (秒) です。
Dead Interval	Hello パケットが受信されなくなってから、Neighbor ルータがその OSPF コントローラがダウンしていると判断するまでの時間 (秒)。本値は共通ネットワークに接続する全ルータで同じである必要があります。初期値は 40 (秒) です。OSPF では、2 つの Neighbor 間でこれらのインターバルの値が全く同じである必要があります。異なるインターバル値を持つルータ同士はそのセグメントにおいて Neighbor ルータになることができません
Cost	OSPFv3 インタフェースにパケットを送信するコスト

4. 「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。

6to4 トンネル設定

Network > IPv6 > 6 to 4 Tunneling メニュー

注意 本機能は追加ライセンス「DWC-1000-VPN」が有効の場合にのみ利用可能です。

6to4 トンネリング機能を有効または無効にします。

6to4はIPv4からIPv6まで移行するためのインターネット遷移メカニズムです。IPv6パケットのIPv4ネットワークへの転送を可能にするシステムです。

1. Network > IPv6 > 6 to 4 Tunneling の順にメニューをクリックし、以下の画面を表示します。

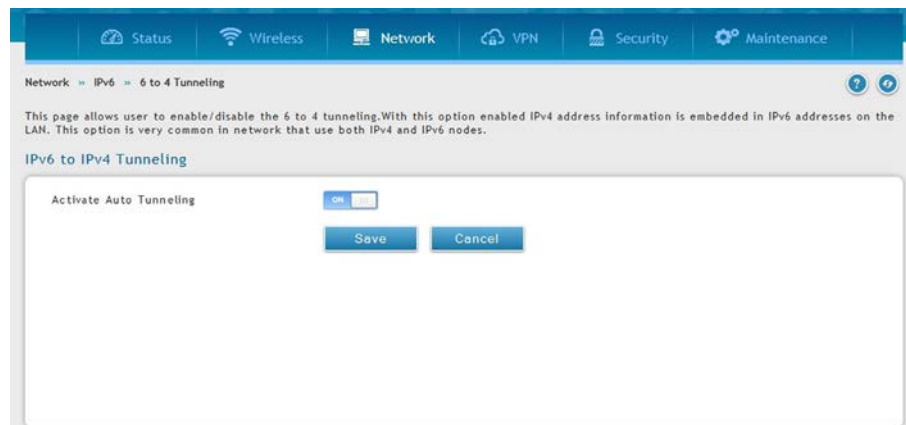


図 6-60 6to4 トンネル設定

2. 6to4 トンネルを有効にするためには、「Activate Auto Tunneling」を「ON」にして「Save」ボタンをクリックします。

ISATAP トンネル (IPv6)

Network > IPv6 > ISATAP Tunnels メニュー

注意 本機能は追加ライセンス「DWC-1000-VPN」が有効の場合にのみ利用可能です。

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) は IPv4 ネットワークのデュアルスタックノード間の IPv6 パケットを送信する、IPv6 送受信メカニズムになります。ISATAP では境界線ルータディスカバリサイトにおける IPv6-IPv4 互換性アドレスフォーマットの使用になります。ISATAP はまた指定リンクレイヤ (IPv4 が IPv6 のリンクレイヤとして起こる) の IPv6 操作においても指定します。

1. Network > IPv6 > ISATAP 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。

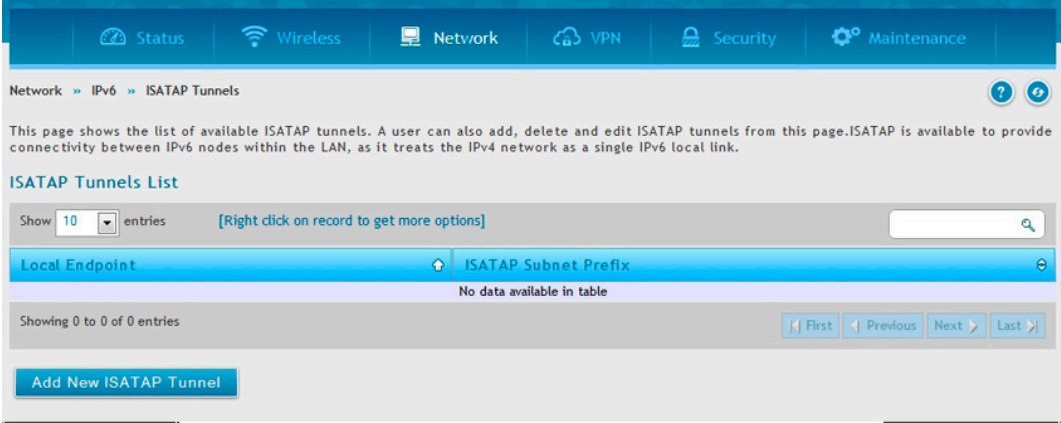


図 6-61 ISATAP Tunnels 画面

2. 「Add New ISATAP Tunnel」 ボタンをクリックして以下の画面を表示します。

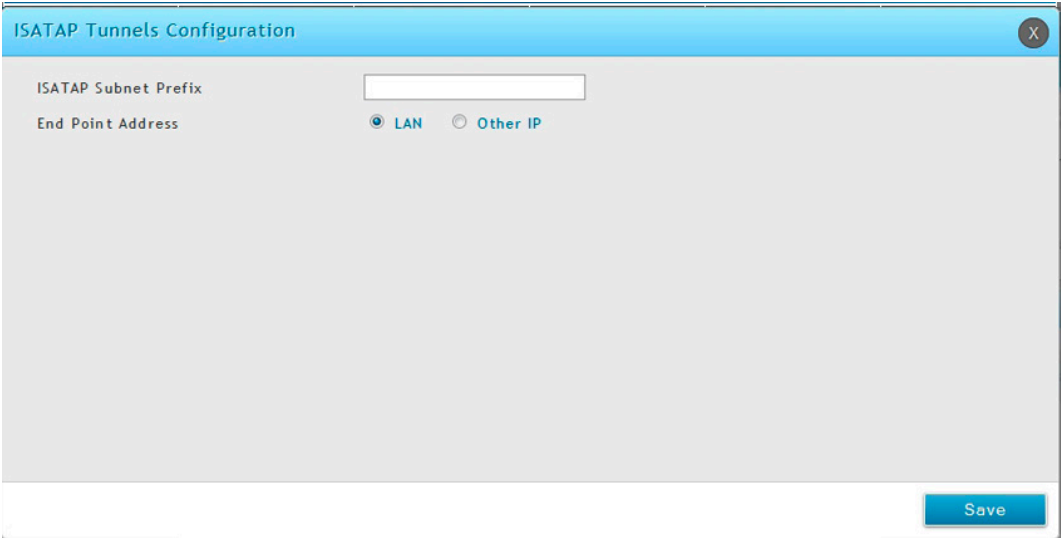


図 6-62 Add New ISATAP Tunnel 画面

コントローラ通知に以下のプレフィックスオプションを設定することができます。:

項目	説明
ISATAP Subnet Prefix	イントラネット用の論理的 ISATAP サブネットにアサインされる 64 ビットのサブネットプリフィクスです。お使いの ISP またはインターネットレジストリから提供され RFC4193 によって定義されています。
End Point Address	コントローラから始まるトンネルのエンドポイントアドレスです。エンドポイントは LAN インタフェース (IPv4 ネットワークを想定) または指定の LAN IPv4 アドレスです。
IPv4 Address	「LAN IPv4 Address」を選択した場合、エンドポイントアドレスを入力します。

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。

プロトコルバインディング

Network > Routing > Protocol Binding メニュー

テーブルに現在定義済みの IP/MAC バインドルールのすべてを表示して、ルールにいくつかの操作を許可します。

注意 本機能は追加ライセンス「DWC-1000-VPN」が有効の場合にのみ利用可能です。

プロトコルバインディングは、ロードバランス機能を使用する場合に必要です。設定したサービスまたはユーザ定義サービスのリストからいずれかを選択すると、利用可能な Option ポートの 1 つだけに送信するようにトラフィックのタイプを割り当てることができます。柔軟性を高めるために、送信先ネットワークまたはマシンと同様に送信元ネットワークまたはマシンを指定できます。例えば、1 セットの LAN IP アドレスに対する VoIP トラフィックを 1 つの Option に割り当てることができます。また、残りの IP アドレスから来るどんな VoIP トラフィックももう一方の Option リンクに割り当てることができます。ロードバランシングモードが有効で、1 つ以上の Option が設定される場合にだけ、プロトコルバインディングは適用されます。

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

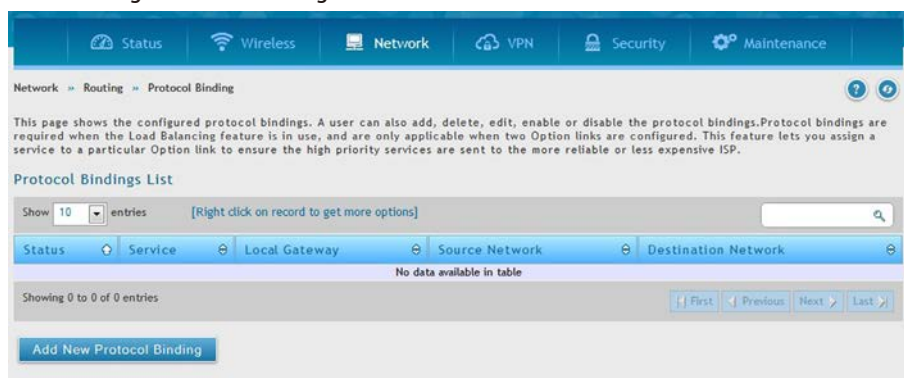


図 6-63 Protocol Binding 画面

2. 対象のエントリで右クリック、「Edit」または「Delete」を指定します。新しいエントリを追加する場合は「Add New Protocol Binding」をクリックし、以下の画面を表示します。

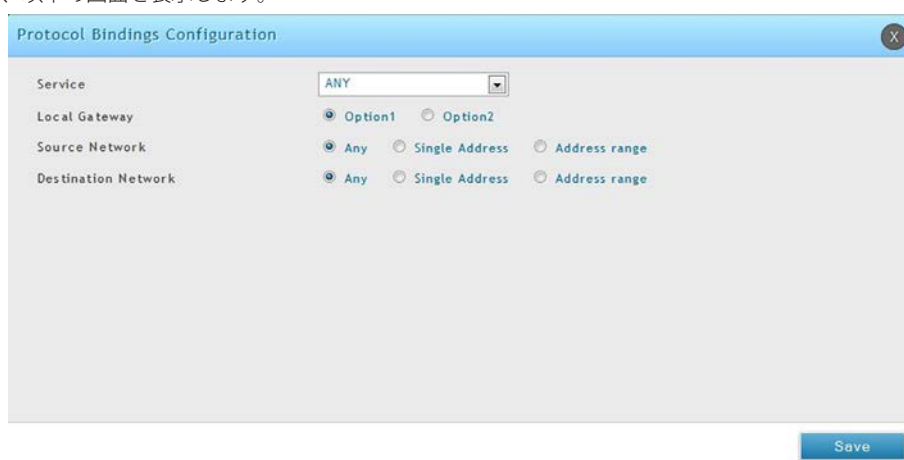


図 6-64 Add New Protocol Binding 画面

3. 以下の情報を表示または指定します。

項目	説明
Service	プロトコルバインディングに利用可能な様々なサービスの 1 つを選択します
Local Gateway	このプロトコルバインディング (Option1 または Option2) にローカルなゲートウェイを設定するポートを選択します。
Source Network	以下の 1 つを選択します。 <ul style="list-style-type: none"> Any - どの指定ネットワークも指定する必要がありません。 Single Address - 1 台のコンピュータに制限します。このプロトコルバインディングの送信元ネットワークの一部であるコンピュータの IP アドレスを必要とします。 Address Range - IP アドレス範囲内のコンピュータが送信元ネットワークの一部であることを許可する場合に選択します。開始アドレスと終了アドレスを必要とします。
Destination Network	以下の 1 つを選択します。 <ul style="list-style-type: none"> Any - どの指定ネットワークも指定する必要がありません。 Single Address - 1 台のコンピュータに制限します。このプロトコルバインディングの送信先ネットワークの一部であるコンピュータの IP アドレスを必要とします。 Address Range - IP アドレス範囲内のコンピュータが送信先ネットワークの一部であることを許可する場合に選択します。開始アドレスと終了アドレスを必要とします。

4. 「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。

QoS 設定

Network > QoS メニュー

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に 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に、これを処理する速度はキューの設定方法、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。遅延が必要な場合は、パケットは、スケジューラが送信のためにそのキューを許可するまで、キューに保持されます。キューが一杯になると、送信のためにパケットを保持する場所がないため、コントローラによって破棄されます。

QoS は、厳しいタイミング要求のパケットを遅延が許容されるパケットと識別することで、一貫性があり予測可能な送信を提供する方法です。タイミング要求の厳しいパケットは、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

Network > QoS > LAN QoS Priority メニュー

QoS 優先度の設定には、次の 3 段階の処理があります。:

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。(151 ページの「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。(153 ページの「DSCP 優先度の設定」または 152 ページの「802.1p 優先度の設定」参照)

QoS モードの有効化

Network > QoS > LAN 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ティ型で運用します。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。輻輳が起ると、すべてのトラフィックのいずれも破棄される可能性があります。

QoS 機能を設定する際、優先処理を提供するためには、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できます。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、帯域幅使用がもっと効果的になります。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 分類をレイヤ 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

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 > LAN 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 > LAN 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。

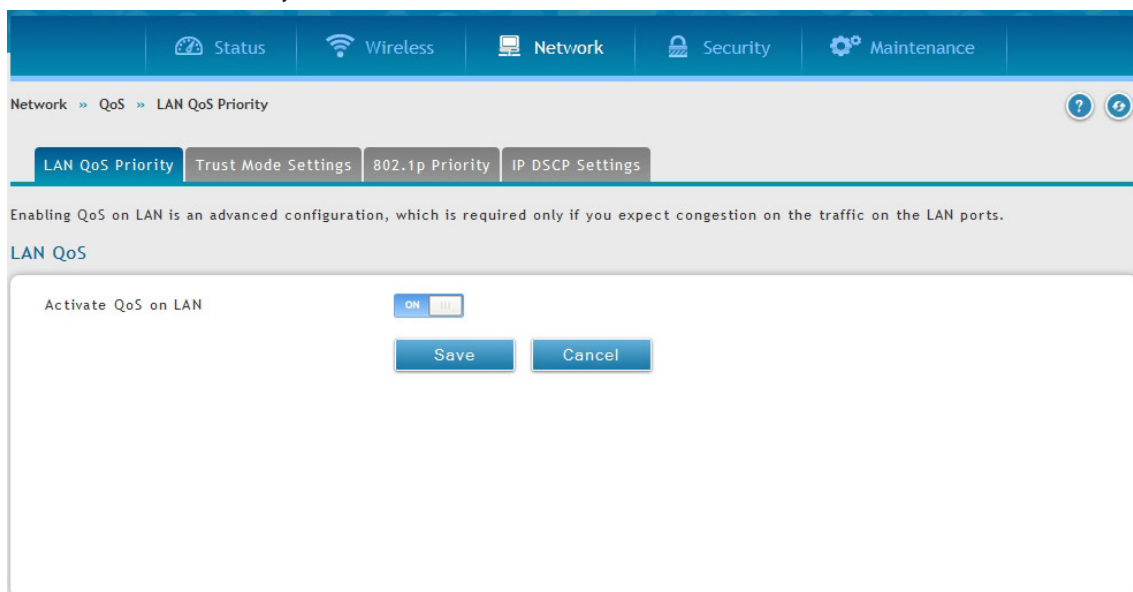


図 6-65 LAN QoS 画面

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。

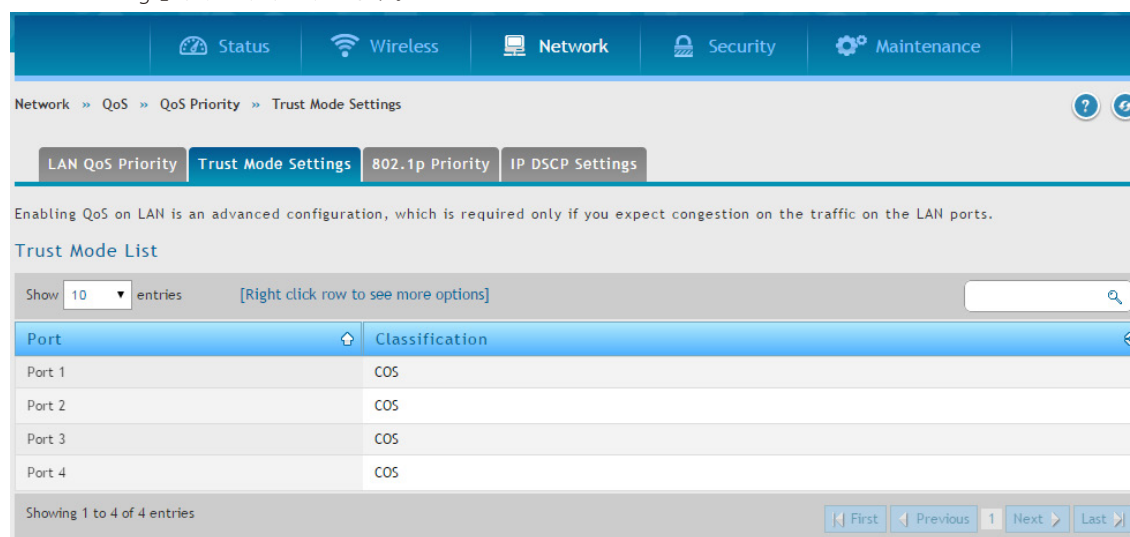


図 6-66 Trust Mode List 画面

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。

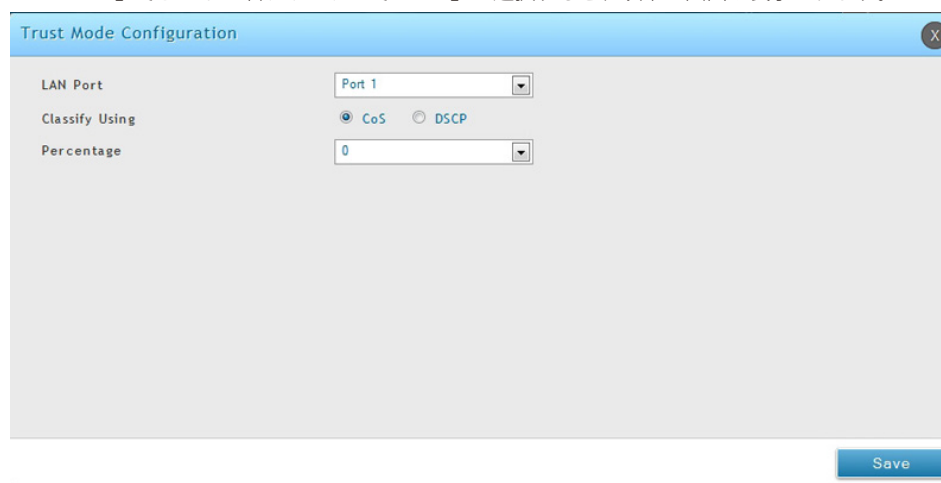


図 6-67 Trust Mode Configuration 画面

5. 「LAN Port」でポート番号を入力し、「Classify Using」で「CoS」または「DSCP」を選択、「Percentage」を指定します。
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ためには、[153 ページの「DSCP 優先度の設定」](#)または、[152 ページの「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 > LAN QoS Priority > Trust Mode Settings メニュー

ポートに CoS、または DSCP を選択します。ポートに輻輳がある場合、LAN ポートは、パケット内のこのフィールドの 1 つ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「P DSCP List」ページで設定されます。

1. Network > QoS > LAN 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。

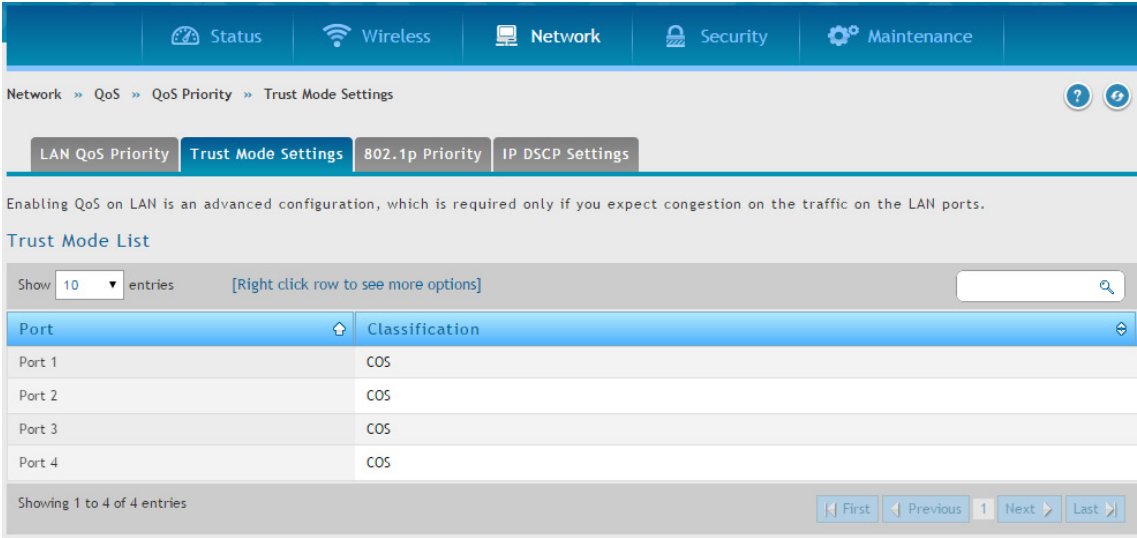


図 6-68 Trust Mode List 画面

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。

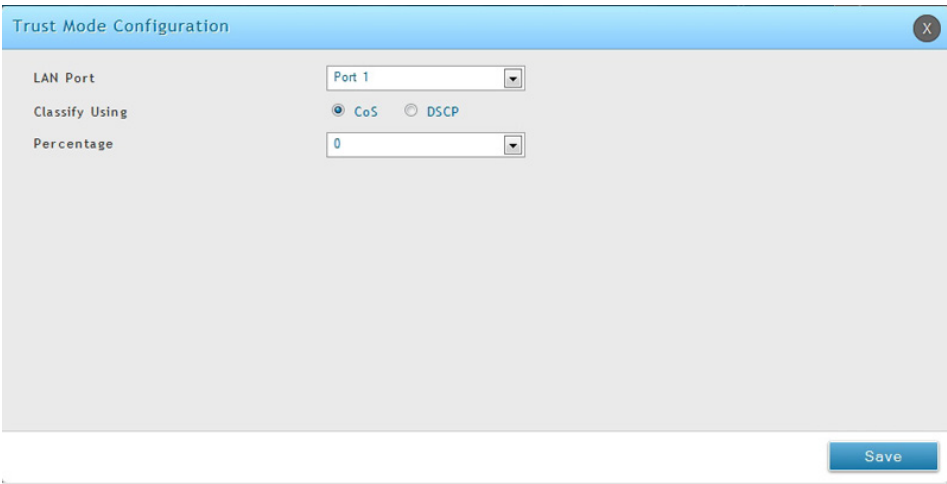


図 6-69 Trust Mode Configuration 画面

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、以下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 > LAN QoS Priority > 802.1p Priority メニュー

CoS を QoS 設定のために選択した場合、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および割り当てます。

1. Network > QoS > LAN 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。

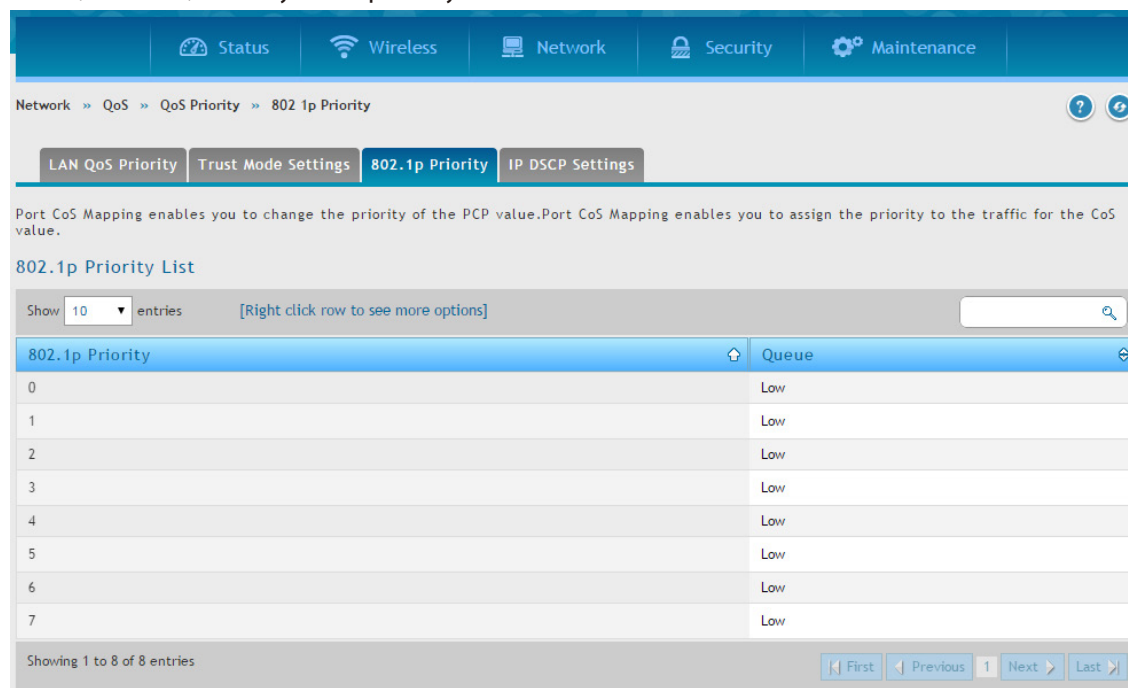


図 6-70 802.1p Priority List 画面

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。

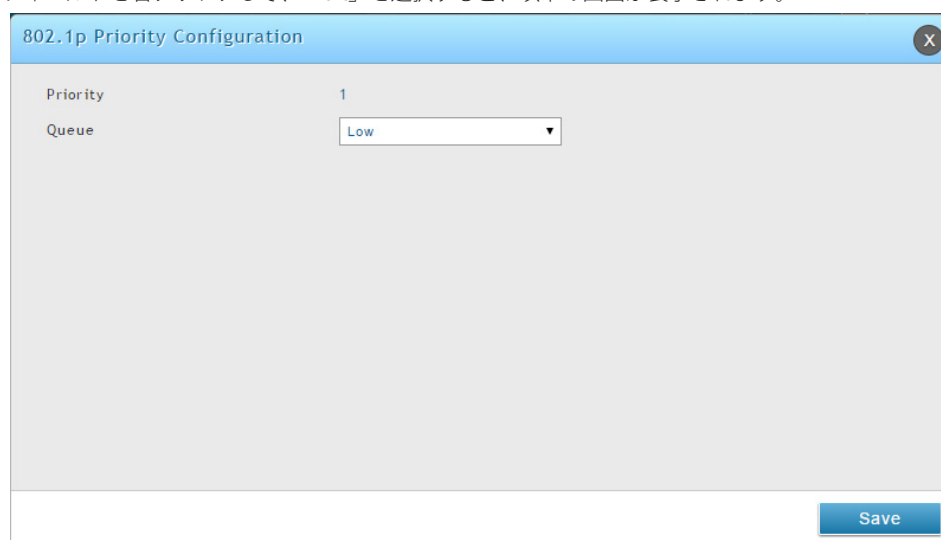


図 6-71 802.1p Priority Configuration 画面

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 > LAN QoS Priority > IP DSCP Settings メニュー

DSCP を QoS 設定のために選択した場合、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および割り当てます。

1. Network > QoS > LAN 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。

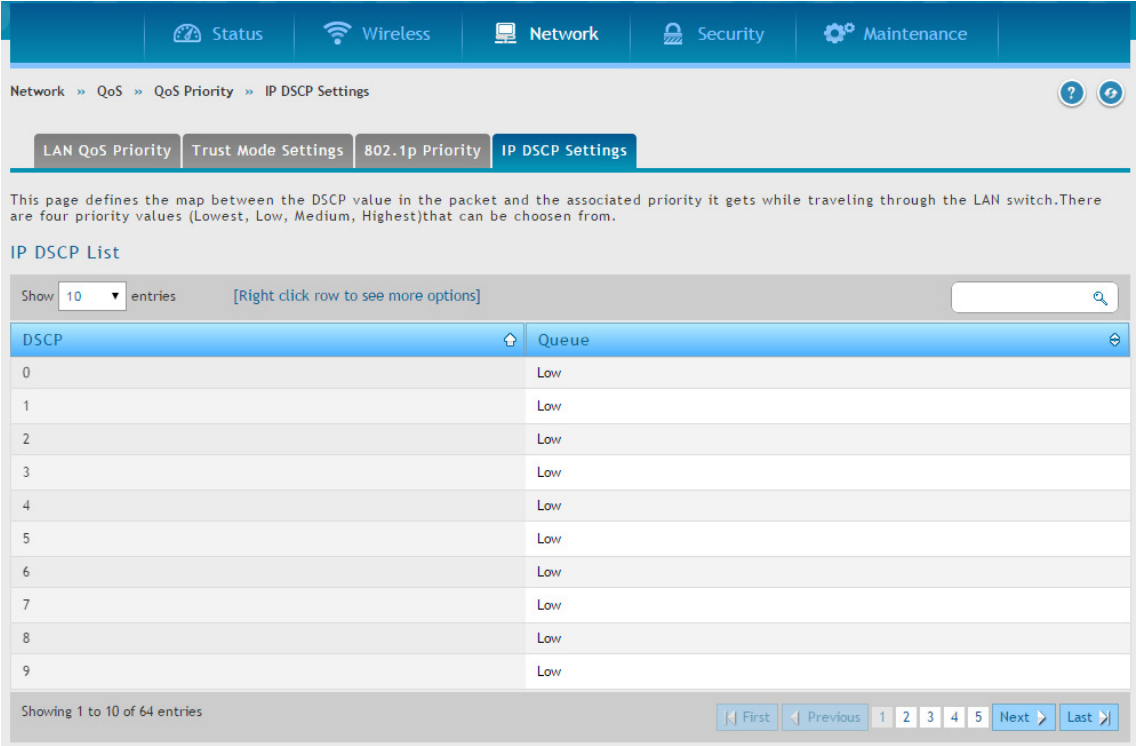


図 6-72 IP DSCP List 画面

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。

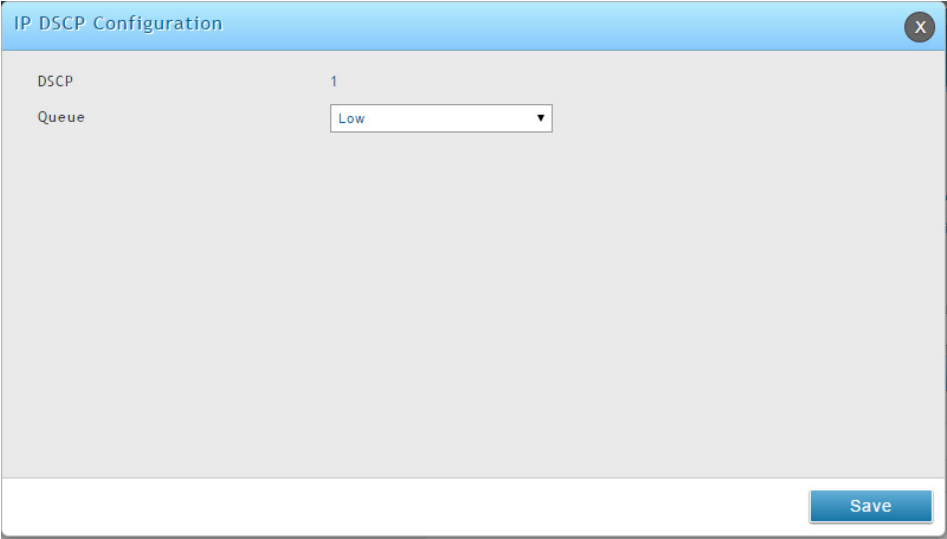


図 6-73 IP DSCP Configuration 画面

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。

QoS ポリシー設定

Network > QoS > LAN QoS Policy メニュー

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 > LAN QoS Policy > Policy Based QoS メニュー

1. Network > QoS > LAN 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。

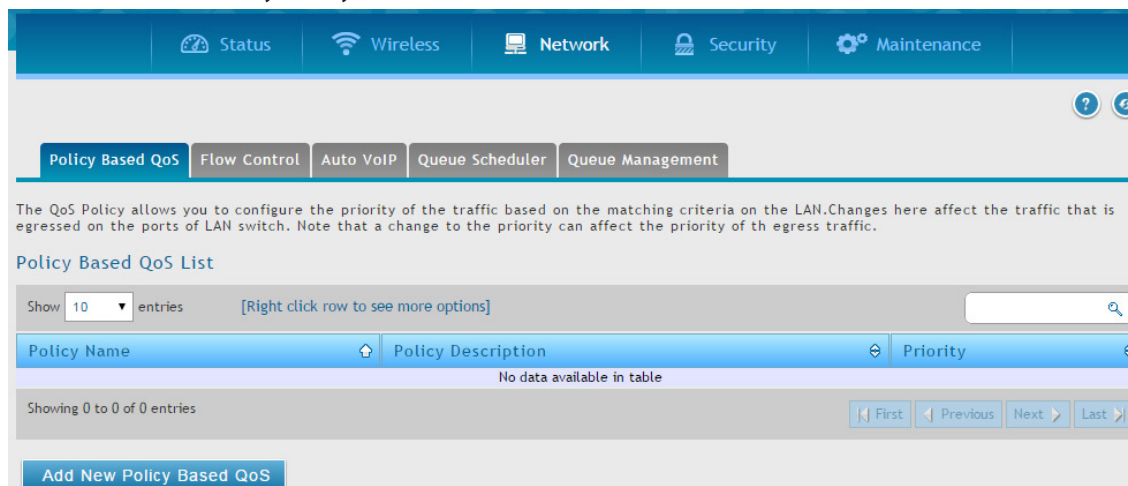


図 6-74 Policy Based QoS List 画面

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 6-75 Policy Based QoS Configuration 画面

3. 以下の情報を表示または指定します。

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します。
Profile Type	本プロファイルの照合基準を選択します。 <ul style="list-style-type: none"> • 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 アドレス) • Source UDP Port (送信元 UDP アドレス)
VLAN	「Profile Type」が「VLAN」の場合、定義済みの VLAN 番号を入力します。

項目	説明
MAC Address	「Profile Type」が「Destination MAC Address」または「Source MAC Address」の場合、定義済みの 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、定義済みの 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 Address」の場合、定義済みの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。 <ul style="list-style-type: none">• Highest (最高)• High (高)• Low (低)• Lowest (最低)

4. 「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。

フローベースコントロールの設定

Network > QoS > LAN 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 > LAN QoS Policy> Flow Control 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。

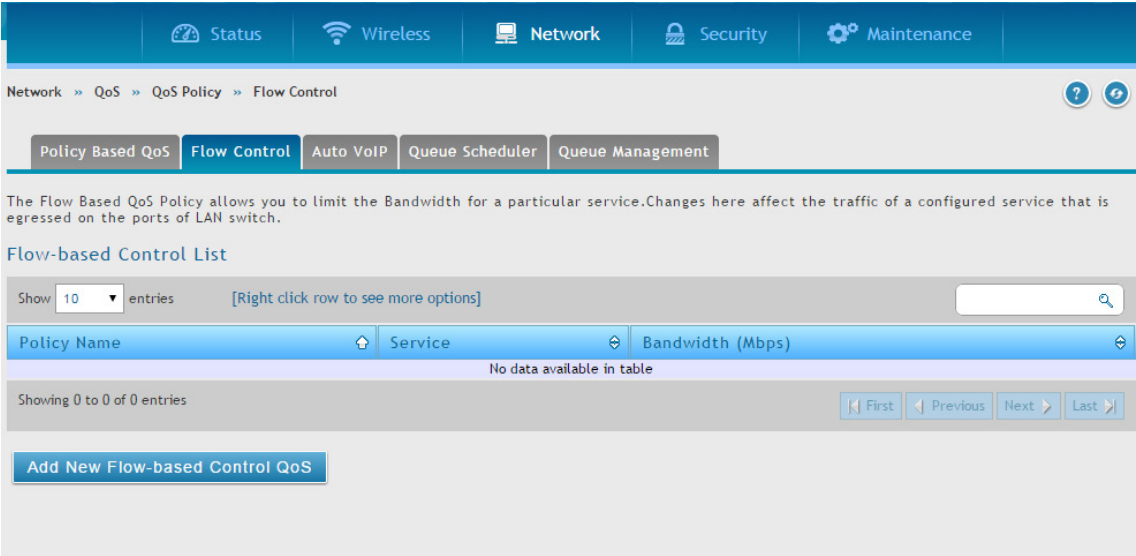


図 6-76 Flow-based Control List 画面

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。

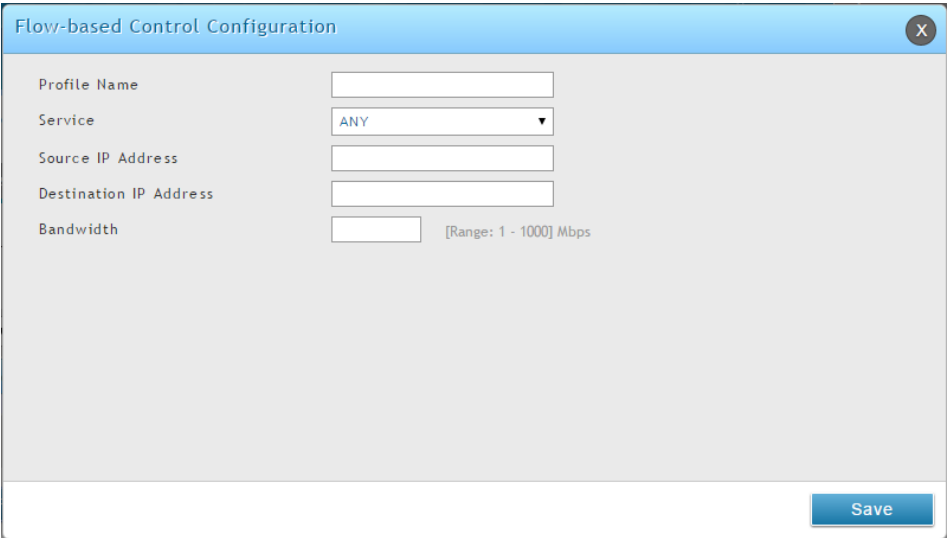


図 6-77 Flow-based Control Configuration 画面

3. 以下の情報を表示または指定します。

項目	説明
Profile Name	プロフィール名を指定します。
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、kie、shhttpd、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。

4. 「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。

自動 VoIP QoS の設定

Network > QoS > LAN 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 > LAN QoS Policy > Auto VoIP 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。

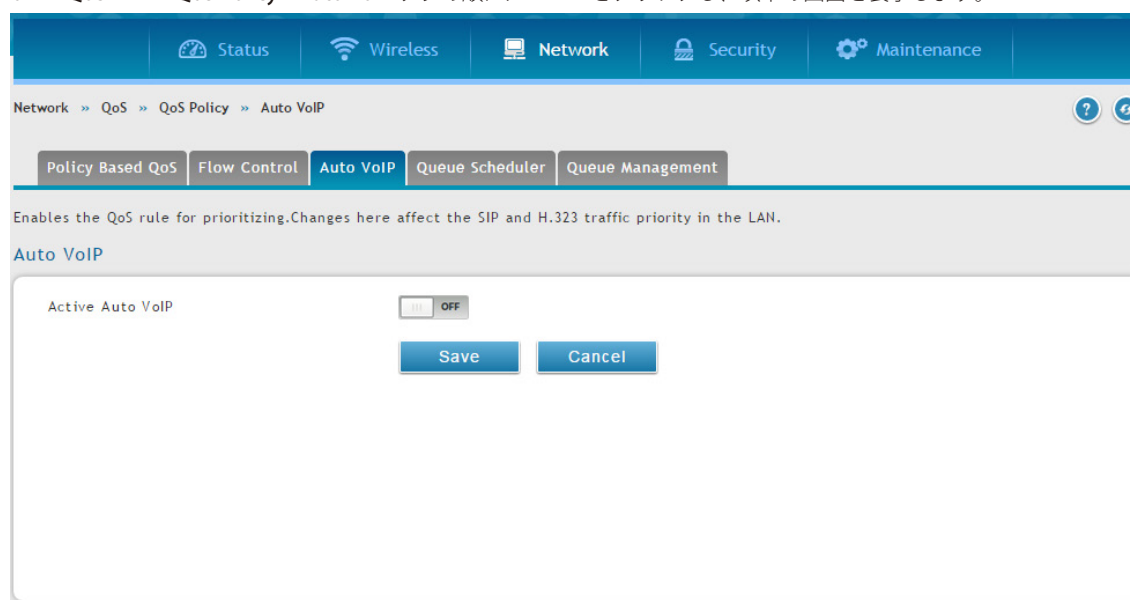


図 6-78 Auto VoIP 画面

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 > LAN 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 > LAN 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。

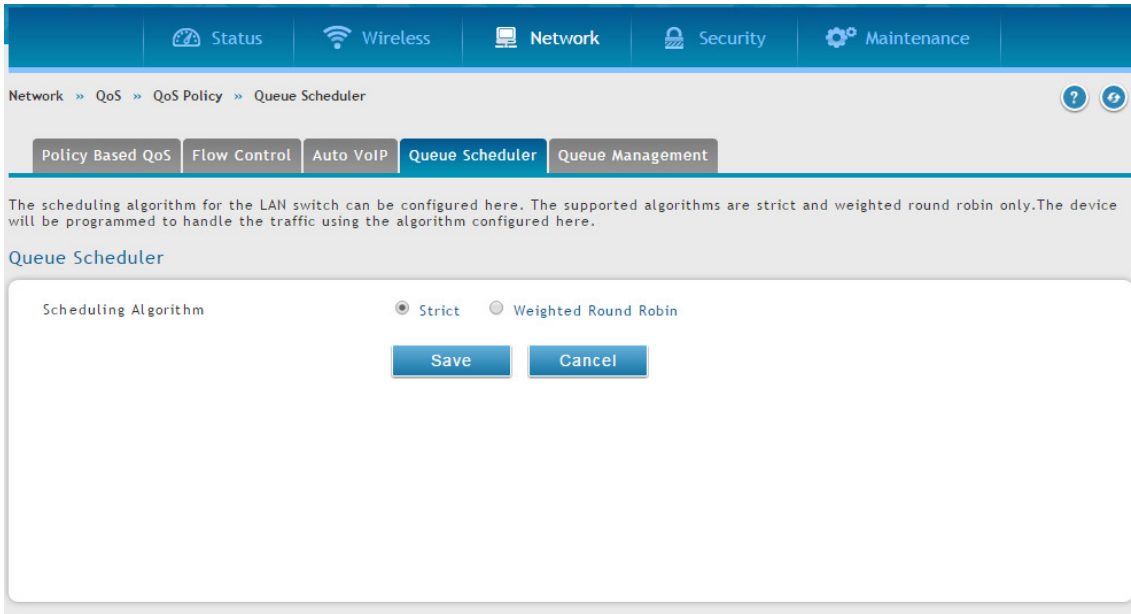


図 6-79 Queue Scheduler 画面

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 > LAN QoS Policy> Queue Management メニュー

無線コントローラで使用する現在のキュー管理アルゴリズムを表示します。

1. Network > QoS > LAN QoS Policy> Queue Management 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。

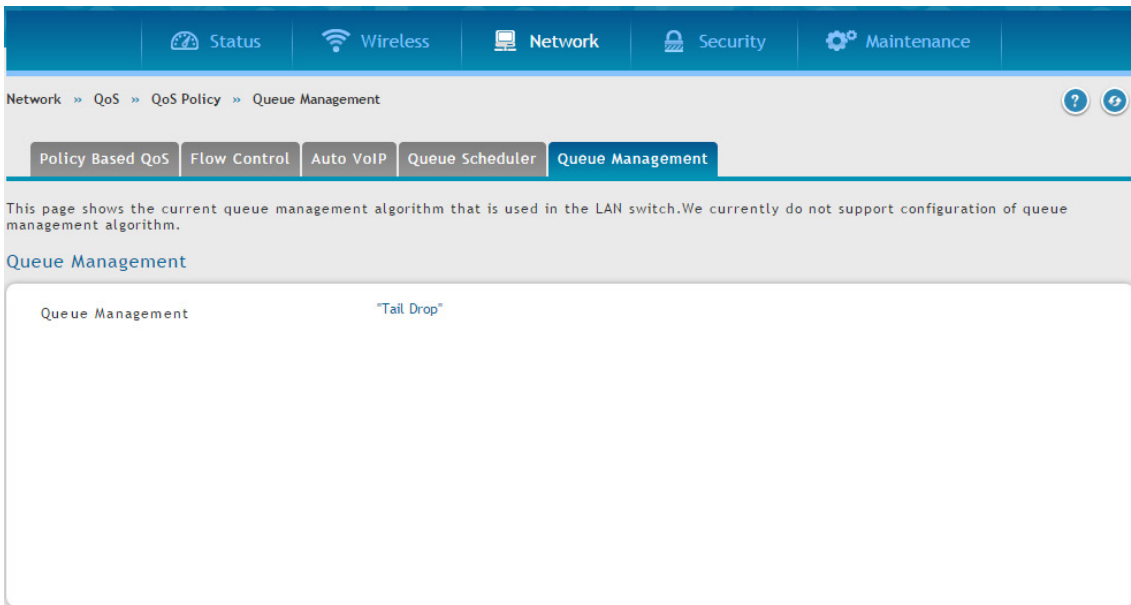


図 6-80 Queue Management 画面

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、上流ルータがパケット内の「DSCP」フィールドに基づいた QoS 決定を行えるように、レイヤ 2 の QoS フィールドは、パケットのレイヤ 3 の QoS フィールドに変換されます。DSCP への CoS リマークが有効になると、特定の CoS 値に対して適切な DSCP 値を選択できます。

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。

Network >> QoS >> CoS DSCP Marking

Remarking CoS to DSCP is an advanced QoS configuration, where the Layer 2 quality of service field is translated to a Layer 3 QoS field in the packet, so that upstream controllers can make a QoS decision based on the DSCP field set in the packet. Once you enable CoS to DSCP marking by choosing the check box, you can choose the appropriate value of the DSCP for a given CoS value.

CoS DSCP Marking List

CoS to DSCP Setup
Enable CoS to DSCP Marking ☒ ON ☐ OFF

CoS DSCP Marking List

Show 10 entries [Right click row to see more options]

CoS	DSCP Value
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

Showing 1 to 8 of 8 entries

1

図 6-81 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。

CoS DSCP Marking Configuration

CoS [Range: 0 - 7]

DSCP

図 6-82 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。

トラフィックシェーピング (Option QoS)

Network > QoS > Option QoS メニュー

帯域管理 (Bandwidth Management) によりインターネットリンクのトラフィックのレートと優先値を制限し、インターネット帯域の最適化を行います。音声などの高い優先値のトラフィックへのクオリティを維持し、低い優先値のトラフィックは制限するなど、インターネットへのトラフィックの優先値とレートを管理、設定します。

1. Network > QoS > Option 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。

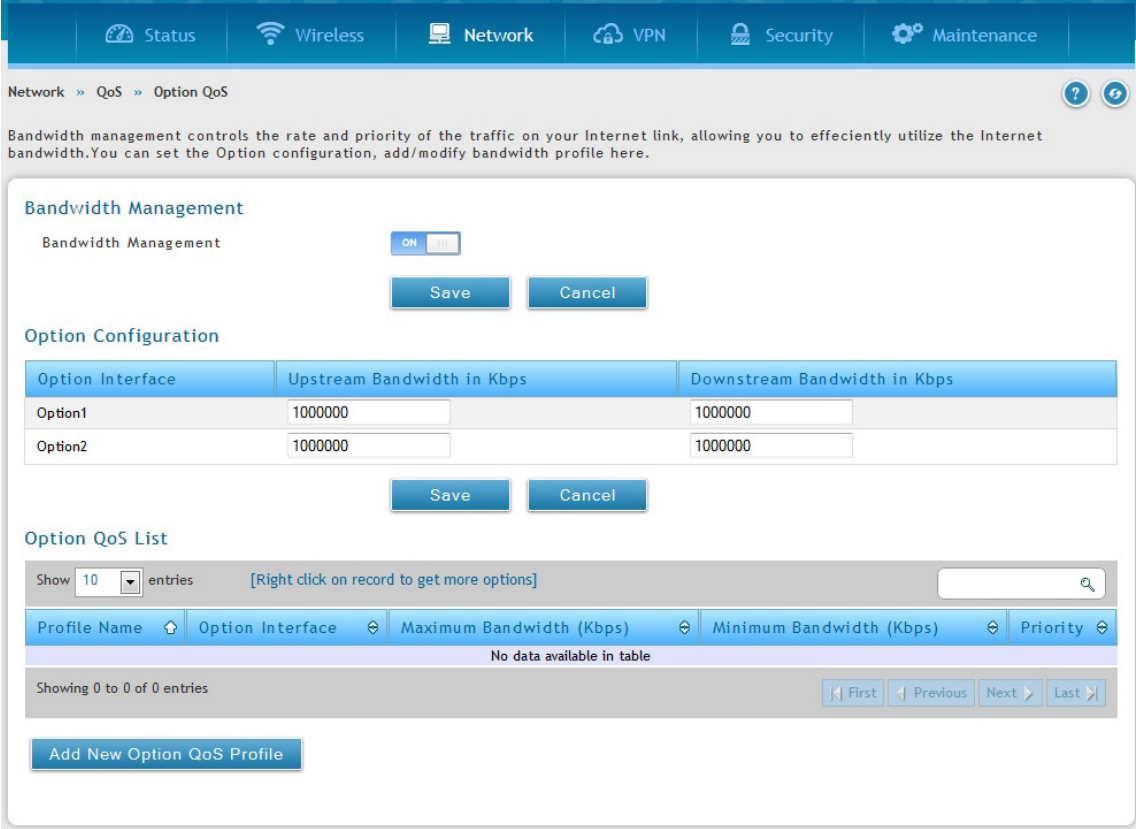


図 6-83 Option QoS 画面

2. 「Bandwidth Management」を「ON」に設定し、「Save」をクリックします。
3. アップストリーム / ダウンストリーム帯域を設定する「Option1」「Option2」インタフェースを定義し、「Save」をクリックします。
4. 新しいプロファイルを作成する場合は、「Add New Option QoS Profile」をクリックし、以下の画面を表示させます。

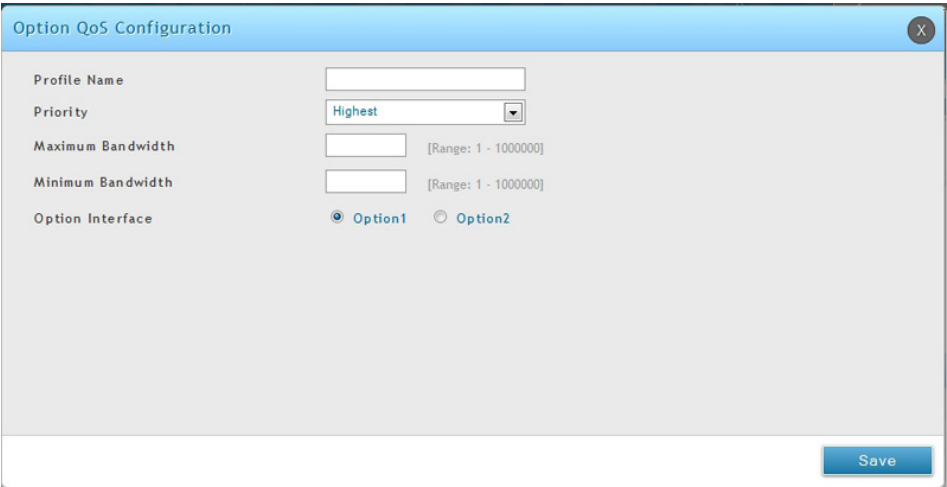


図 6-84 Add New Option QoS Profile 画面

5. 以下の情報を表示または指定します。

項目	説明
Profile Name	プロファイル名を入力します。

項目	説明
Priority	プロファイルの優先度を選択します。 <ul style="list-style-type: none"> • Highest (最高) • High (高) • Low (低) • Lowest (最低)
Maximum Bandwidth	プロファイルの最大帯域値を指定します。
Minimum Bandwidth	プロファイルの最小帯域値を指定します。
Option Interface	プロファイルに適用するオプションインタフェースを指定します。

6. 「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。

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

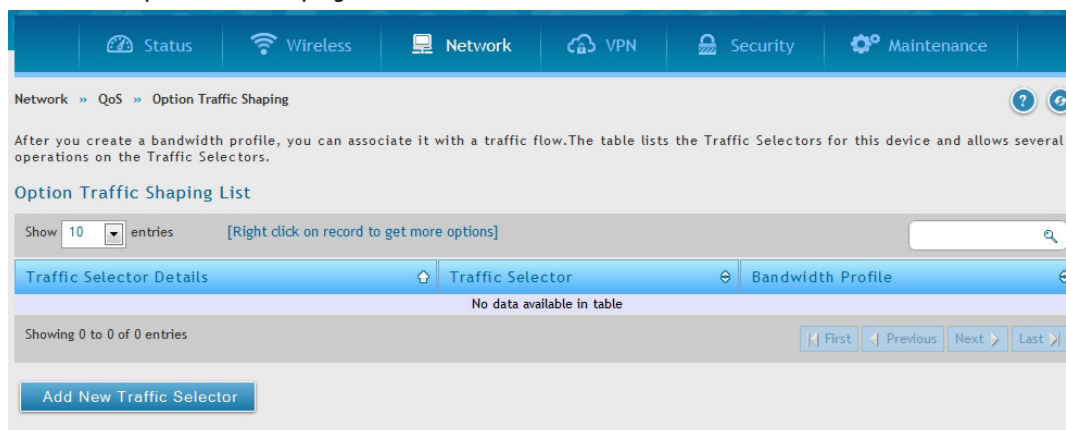


図 6-85 Option Traffic Shaping 画面

8. 「Add New Traffic Selector」をクリックし、以下の画面を表示します。

図 6-86 Option Traffic Shaping 画面

9. 以下の情報を表示または指定します。

項目	説明
Profile Name	作成したプロファイル名を選択します。
Service	ドロップダウンメニューから適用するサービスを選択します。
Traffic Selector Match Type	「Match Type」をドロップダウンメニューから指定します。 「IP Address」「MAC Address」「Port Name」「VLAN」「DSCP value」から指定できます。 以下の項目で選択した「Match Type」の項目を設定します。
IP Address	LAN ホストの IP アドレスを指定します。
MAC Address	MAC アドレスを指定します。
Port Name	ポート番号を指定します。
Available VLANs	VLAN を選択します。
DSCP Value	DSCP 値を指定します。0 から 63 の間で指定できます。

10. 「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。

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	参照ページ
認証 (Authentication)	プロファイル、ユーザデータベースなどを使用してネットワークの認証を行います。	160
Web コンテンツフィルタリング	表示される Web コンテンツについてフィルタをします。	189
ファイアウォールの設定 (Firewall)	コントローラによるファイアウォールの設定を行います。	192

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による設定を推奨します。

認証 (Authentication)

Security > Authentication メニュー

本項目には「User Database」「Billing Profile」「Login Profiles」「External Auth Server」「Facebook Wi-Fi」といった下部項目あります。

クライアントの管理 (User Database)

Security > Authentication > User Database メニュー

「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。

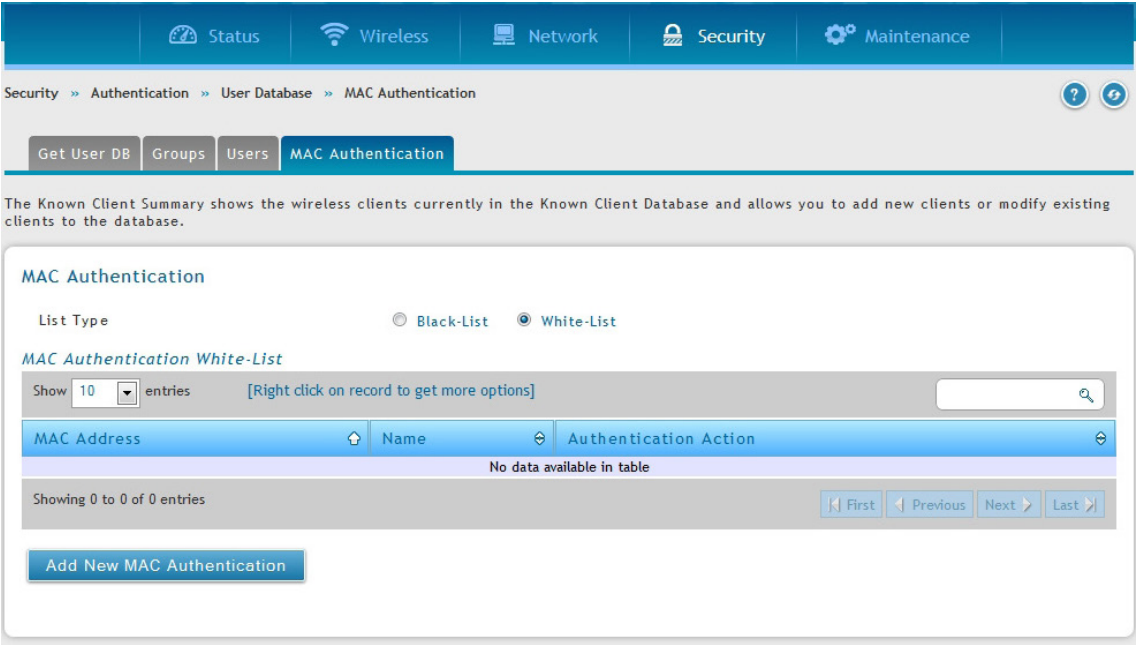


図 7-1 MAC Authentication White-List 画面

「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。

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

図 7-2 MAC Authentication Configuration 画面

3. 以下の情報を表示または指定します。

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。名前は、これから追加する他のものから、この既知のクライアントを容易に特定できるものにするべきです。
Authentication Action	認証アクションを「Global」「Grant」「Deny」から指定します。

4. 「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。

クライアントの編集 / 削除

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

クライアントを追加後、設定を変更する必要がある場合は、編集または削除できます。

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 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、および、もう必要でない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 つの権利（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、ユーザを持つグループを事前設定するためには、[168 ページの「ユーザ管理」](#)の手順を使用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。

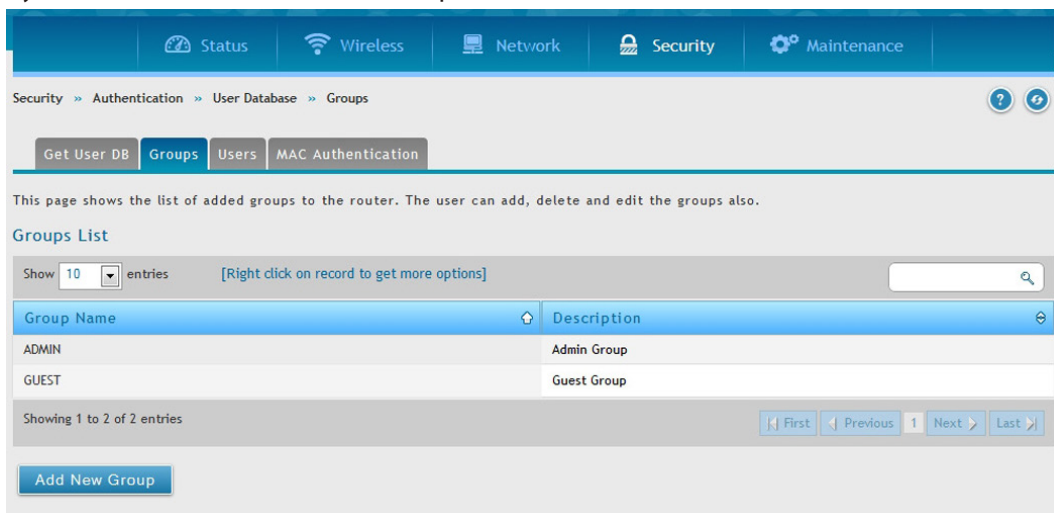


図 7-3 Group List 画面

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。

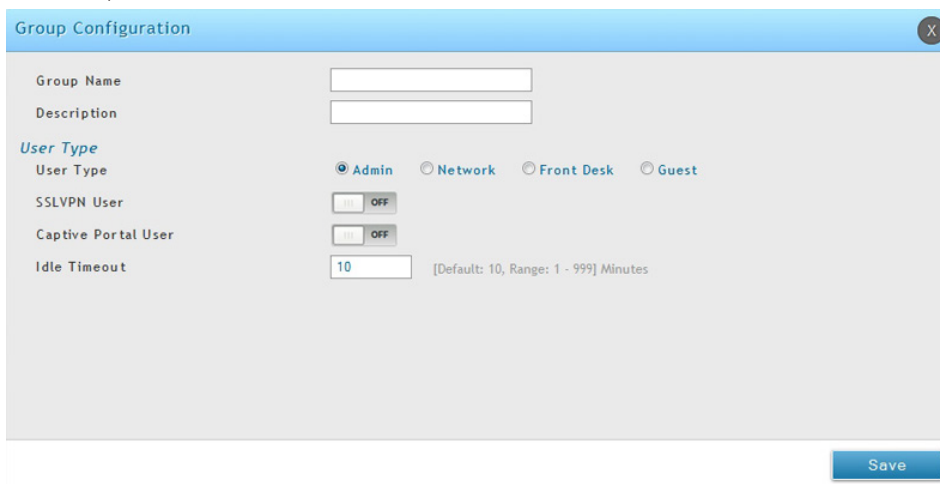


図 7-4 Group Configuration 画面

3. 以下の情報を表示または指定します。

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、これから追加する他のものから、このグループを容易に特定できるものにするべきです。
Description	本ユーザグループの説明文を入力します。
User Type	
User Type	<ul style="list-style-type: none"> Admin - このグループのすべてのユーザにスーパーユーザ権限を付与します。初期値では、1 つの Admin ユーザがあります。 Network - 追加のオプションが有効になります。 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。
SSL VPN User	SSL VPN User を有効 / 無効にします。
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。
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。

4. 「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。

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 7-5 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。(162ページ「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。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、以下の画面を表示します。

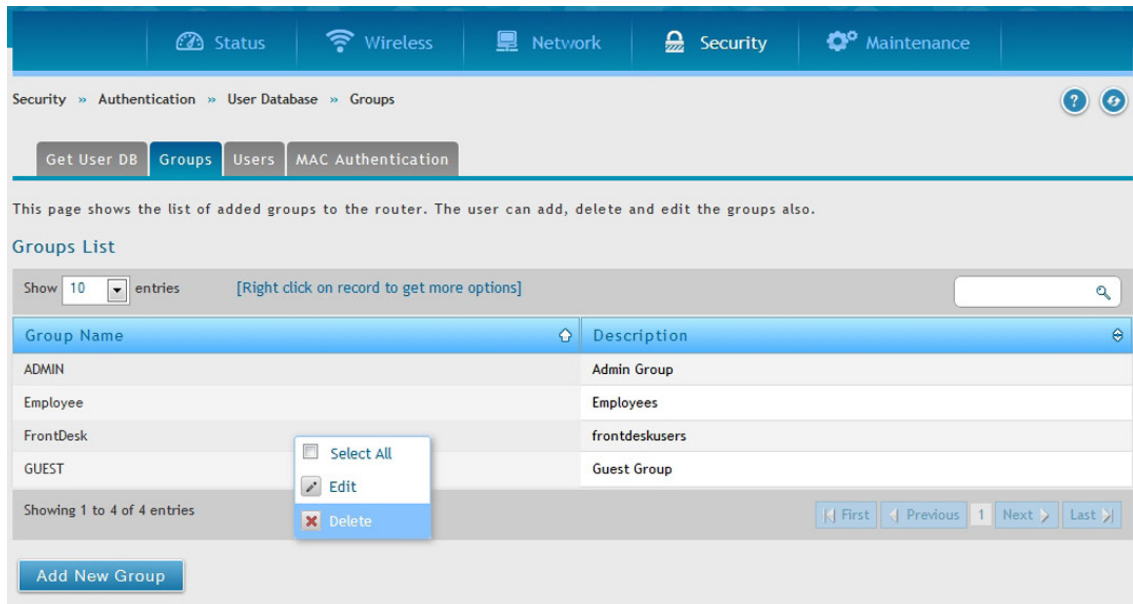


図 7-6 Group List 画面

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ために、「Select All」をチェックし、その後「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。

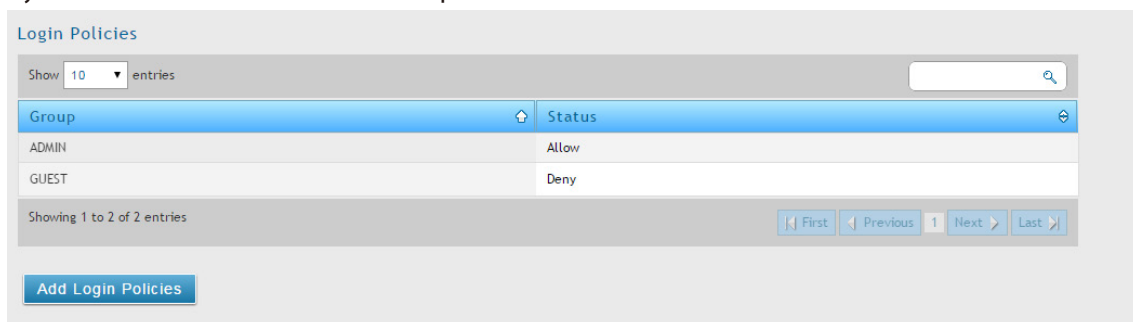


図 7-7 Login Policies 画面

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 7-8 Login Policies Configuration 画面

3. 以下の情報を表示または指定します。

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。 <ul style="list-style-type: none"> 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。
Deny login from Option Interface	選択したグループ内の全ユーザに対して無線コントローラ Option ポートからのログインアクセスを許可または拒否します。 <ul style="list-style-type: none"> 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。

4. 「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。

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。この手順を使用して、特定の Web ブラウザを使用することで、ユーザグループ内のユーザが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 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。

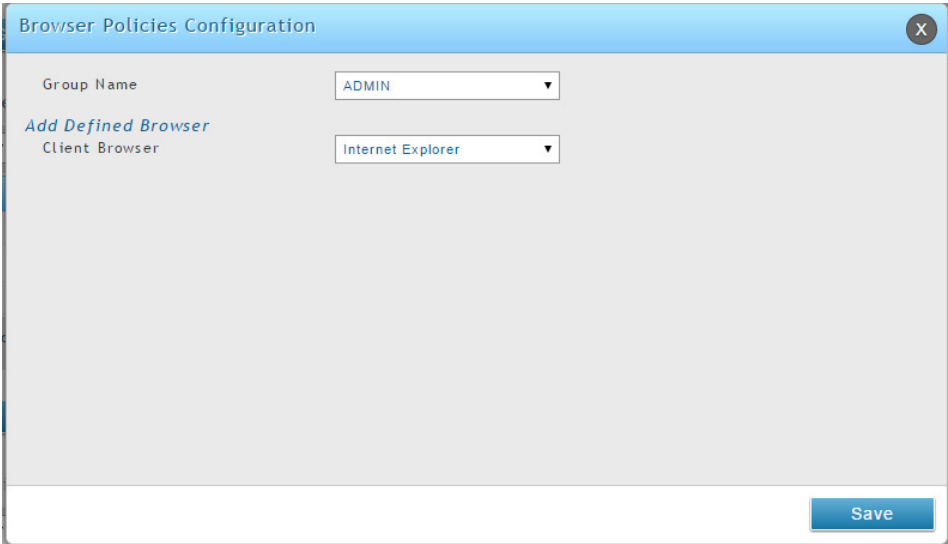


図 7-10 Browser Policies Configuration 画面

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
Allow	ブラウザを許可します。
Deny	ブラウザを拒否します。

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 管理インター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。

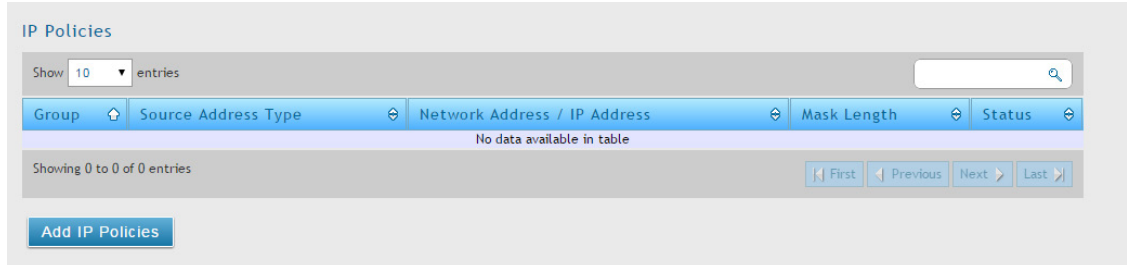


図 7-11 IP Policies 画面

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 7-12 IP Policies Configuration 画面

3. 以下の情報を表示または指定します。

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。 <ul style="list-style-type: none"> • IP Address - 特定の IP アドレスを指定します。 • IP Network - 全体の 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。

4. 「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。

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、必要のない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。

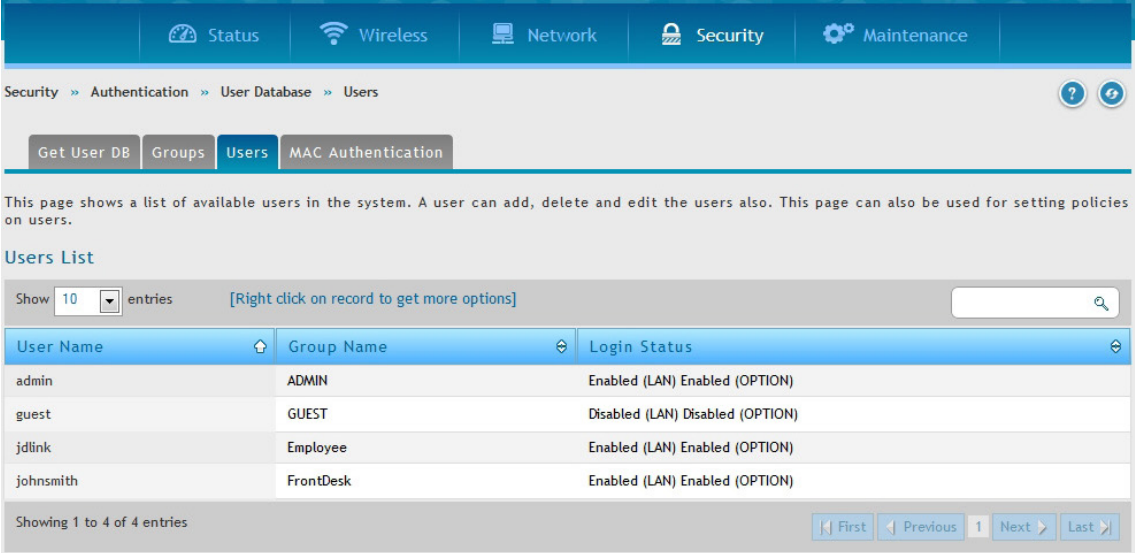


図 7-13 Users List 画面

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。

User Configuration

User Name

First Name

Last Name

Select Group

Password

Confirm Password

ADMIN

Save

図 7-14 User Configuration 画面

3. 以下の情報を表示または指定します。

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。
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。

項目	説明
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一パスワード（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。

- 「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。

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。

- 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。

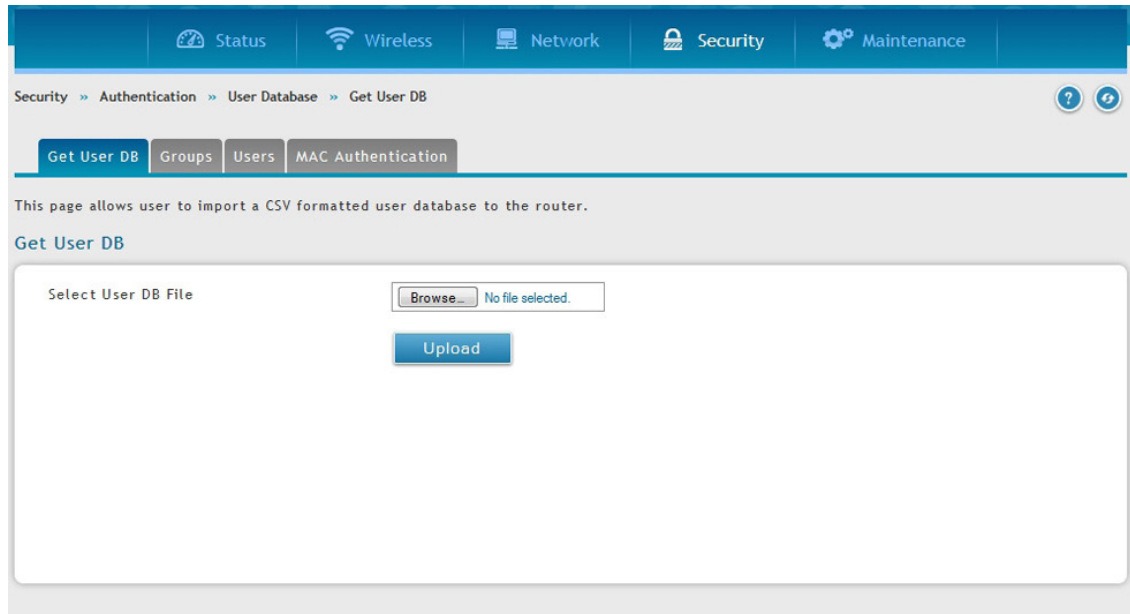


図 7-15 Get User DB 画面

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

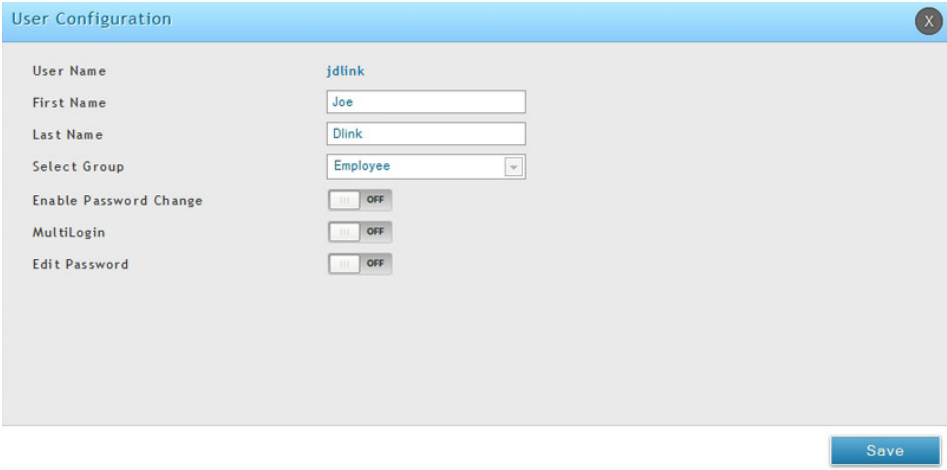


図 7-16 User Configuration 画面

- 3. 以下の情報を表示または指定します。

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。
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 322 ページの「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。

- 4. 「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。

ユーザの削除

Security > Authentication > User Database > Users メニュー

必要としない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、ユーザを必要としない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。

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、スケジュールごとに4個の手順があります。



- 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のタイプには以下の5つがあります。:

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、アカウントは作成されると有効になります。



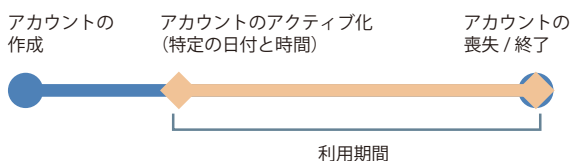
このビリングプロファイルは、ホテルで使用するというシナリオに適しています。一時的なアカウントは、カスタマのチェックイン時に、作成されて有効になります。

2. 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、アカウントは最初にログインすると、有効になります。



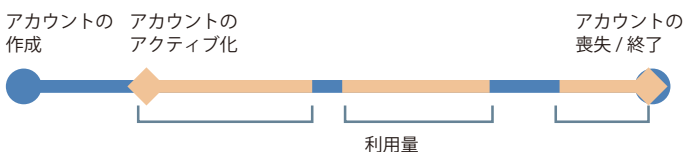
このビリングプロファイルは、カフェや空港などで使用するというシナリオに適しています。カスタマは、最初のログインから計算した時間内で、無線インターネットサービスを使用できます。

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。



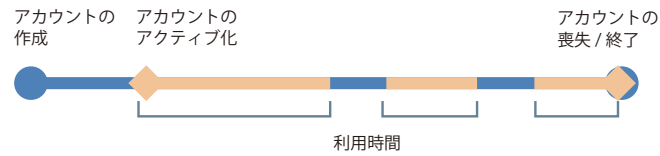
このビリングプロファイルは、プレスカンファレンスで使用するというシナリオに適しています。必要であれば、前もってイベントとデリバリの情報を関係者に説明する前に、主催者はアカウントを生成します。一時的なアカウントは特定の日から有効にされます。

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。



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。



このBilling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。

Billing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。

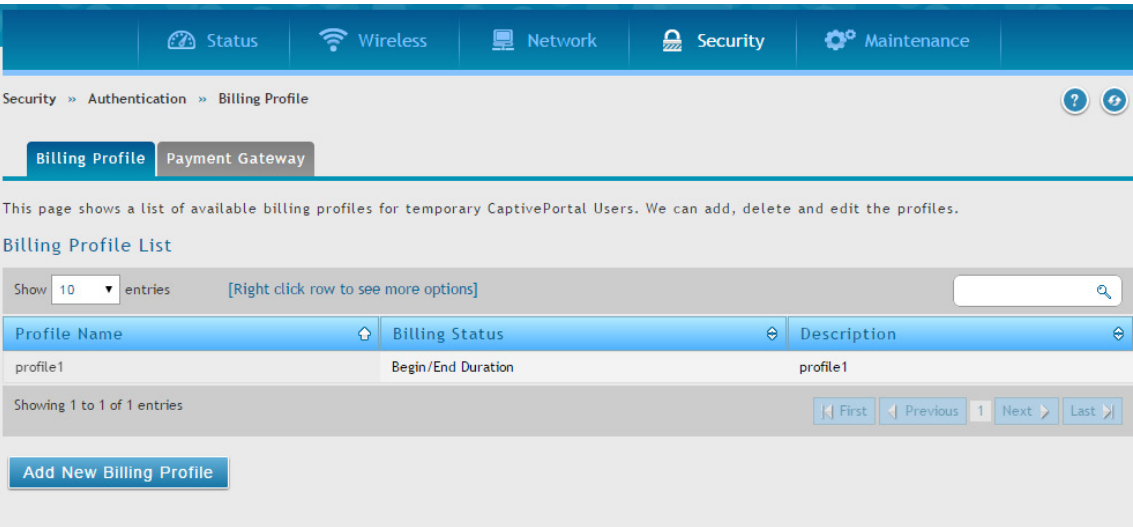


図 7-17 Billing Profile List 画面

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。

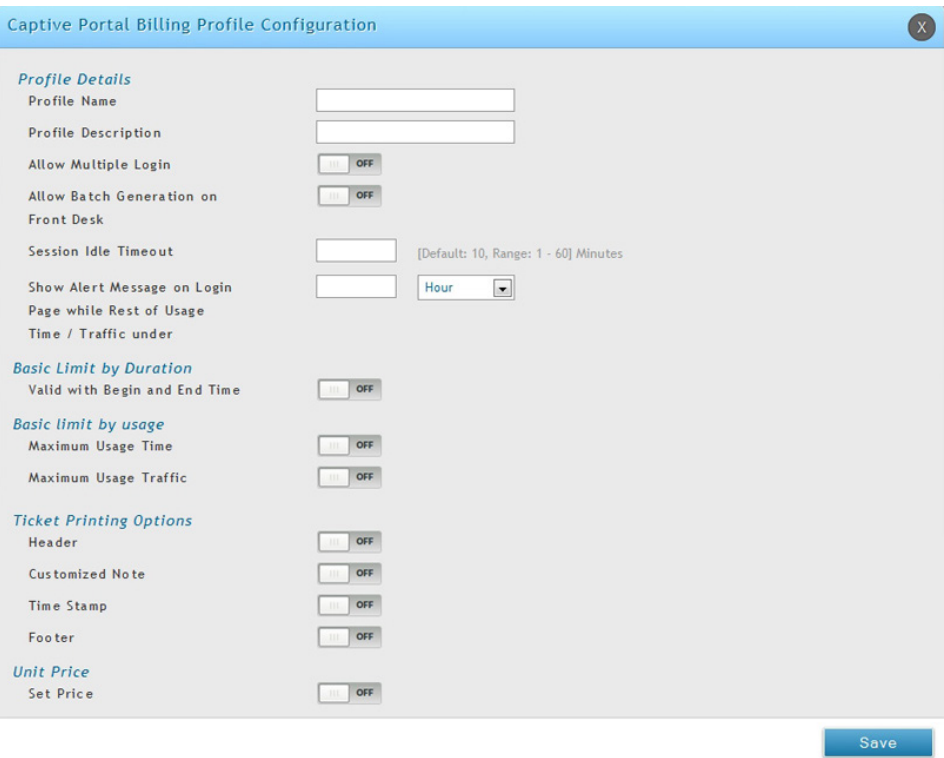


図 7-18 Captive Portal Billing Profile ConfigurationPort 画面

3. 以下の情報を表示または指定します。

項目	説明
Profile Details	
Profile Name	各プロファイルは、自身を識別する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。
Allow Multiple Login	本オプションを有効にすると、複数のユーザは、同時にログインできるように、このプロファイルに作成済みの同じキャプティブポータルログイン証明書を使用できます。
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。
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/Days/MB/GB に値を入力します。「0」を入力すると、警告メッセージが必要でないことを意味します。
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、所要時間までにユーザのアクセスを制限するタイプには以下の 3 つがあります。: <ul style="list-style-type: none"> 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。
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。
Ticket Pricing Options	
Header	チケットにヘッダを付与します。
Customized Note	チケットにロケーションなどのその他の情報を表示させます。
Time Stamp	チケットの現在時刻などを表示します。
Footer	チケットにサービスプロバイダなどフッタを付与します。
Unit Price	
Set Price	ビリングプロファイルに価格を設定します。 キャプティブポータルタイプがビリングユーザに設定されている場合、この価格がキャプティブポータルに表示されます。
Price	価格を指定します。
Monetary Unit	マネタリーユニット (金額の単位) を選択します。

4. 「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。

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 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。

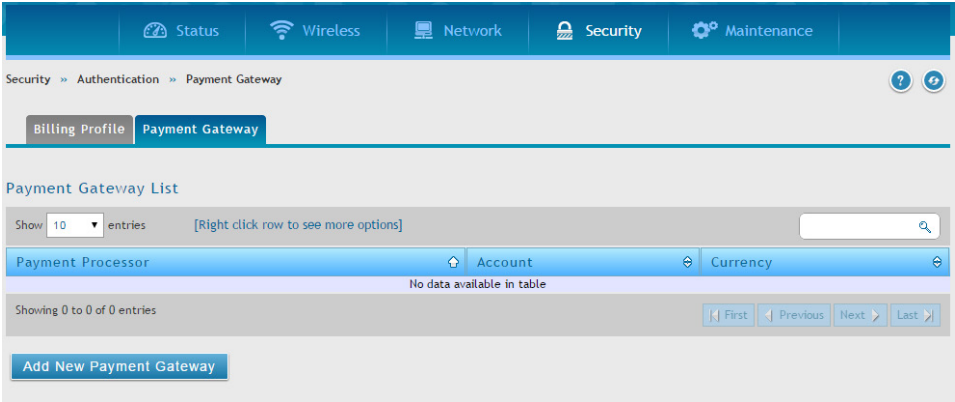


図 7-19 Payment Gateway List 画面

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 7-20 Payment Gateway Configuration 画面

3. 以下の情報を表示または指定します。

項目	説明
Payment Processor	ペイメントエージェントを選択します。(Paypal: PayPal /Authorize.net)
Paypal の場合	
Payment Receiver Email ID	PayPal 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	PayPal 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	PayPal アカウントの API パスワードを指定します。
API Signature	PayPal 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	PayPal 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。
Authorize.net の場合	
Login ID	API アカウント ID を指定します。
Transaction Key	トランザクションキーを指定します。
MD5 Hash	MD5 ハッシュ値を指定します。
Transaction Server	トランザクションサーバを指定します。
Tansaction Mode	トランザクションモードを指定します。
Currency	支払い画面の単位を選択します。

4. 「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。

ログインプロフィール

Security> Authentication> Login Profiles メニュー

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。

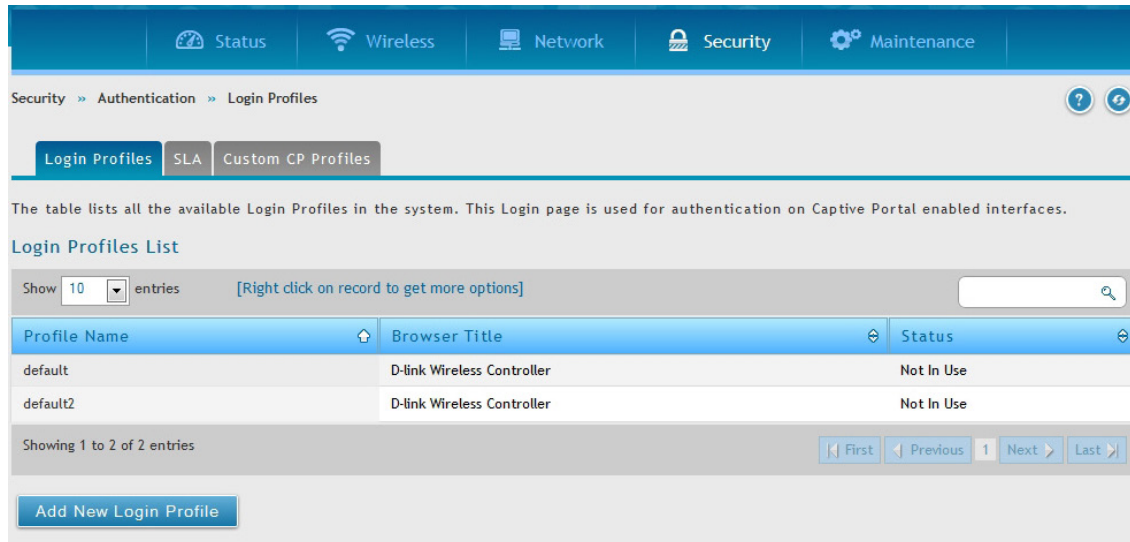


図 7-21 Login Profiles List 画面

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。

Login Profile Configuration

General Details

Profile Name

Browser Title

Background

Page Background Image

Header Details

Header Background Image

Header Caption

Caption Font

Font Size

Font Color

Login Details

Login Section Title

Welcome Message

Error Message

Footer Details

Change Footer Content

Footer Content

Footer Font Color

External Payment Gateway

Enable External Payment Gateway

Session Title 1

Message

Session Title 2

Success Message

Sesssion Title 3

Failure Message

Enable Billing Profiles

Profile Name

Billing Status

Description

Status

No data available in table

Service Disclaimer Text

Payment Server

Save

図 7-22 Login Profile Configuration 画面

3. 以下の情報を表示または指定します。

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称を入力します。名前は、これから追加する他のものから、このキャプティブプロファイルを容易に特定できるものにするべきです。
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。 <ul style="list-style-type: none">Image - ページの背景として画像を表示します。「Page Background Image」フィールドを使用して、背景画像を選択します。Color - ページの背景色を設定します。プルダウンメニューから色を選択します。

項目	説明
Page Background Image	「Background」に「Image」を選択した場合、「Add」リンクをクリックして、画像ファイルをアップロードします。
Page Background Upload	アップロードするファイルを選択します。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 100k バイトです。
Page Background Color	「Background」に「Color」を選択した場合、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」を選択した場合、続くフィールドを入力します。
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 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。 <ul style="list-style-type: none"> Image - ページに画像を表示します。「Header Background Color」フィールドを使用して、背景画像を選択します。画像の最大サイズは 100k バイトです。 Color - ページの背景色を表示します。プルダウンメニューから色を選択します。
Header Background Image	「Background」に「Image」を選択した場合、「Add」リンクをクリックして、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 100k バイトです。
Header Background Upload	アップロードするファイルを選択します。
Header Background Color	「Background」に「Color」を選択した場合、ヘッダの色をプルダウンメニューから選択します。「Custom」を選択した場合、続くフィールドを入力します。
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。
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ェ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	ログインページから外部のペイメントゲートウェイと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	支払いを受けるアカウントおよびその支払い代行サーバを選択します。

4. 「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。

キャプティブポータル SLA のカスタマイズ

Security > Authentication > Login Profiles > SLA メニュー

1. Security > Authentication > Login Profiles > SLA 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。

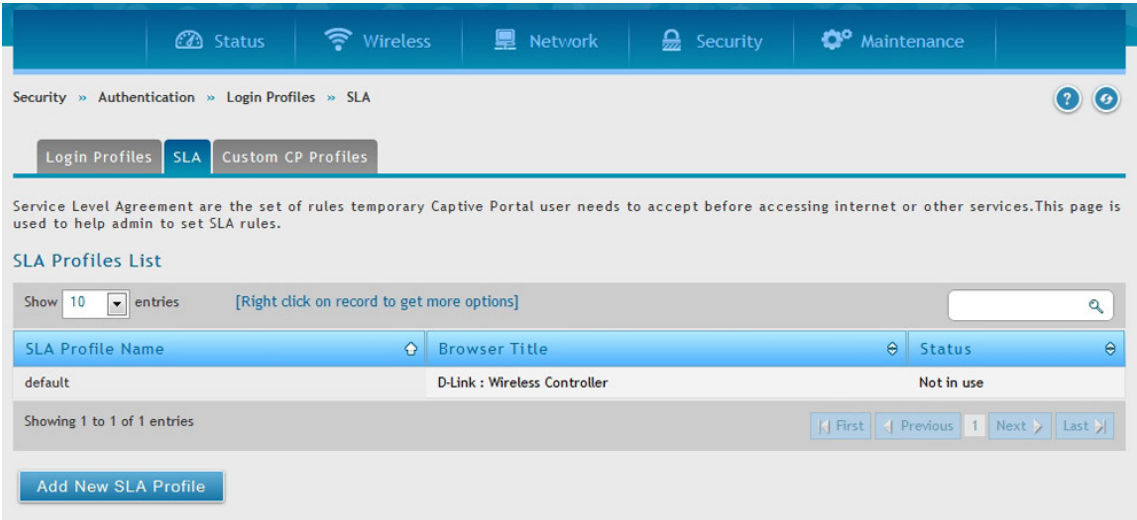


図 7-23 SLA Profiles List 画面

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 7-24 SLA Profile Configuration 画面

3. 以下の情報を表示または指定します。

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、これから追加する他のものから、この SLA を容易に特定できるものにするべきです。
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。
Term 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。

4. 「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。

カスタマイズプロファイルのアップロード

Security > Authentication > Login Profiles > Custom CP Profile メニュー

カスタムしたプロファイルをアップロードします。「Browse（参照）」をクリックし、プロファイルの場所を指定、「Save」をクリックしアップロード完成です。

1. Security > Authentication > Login Profiles > Custom CP Profile 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。

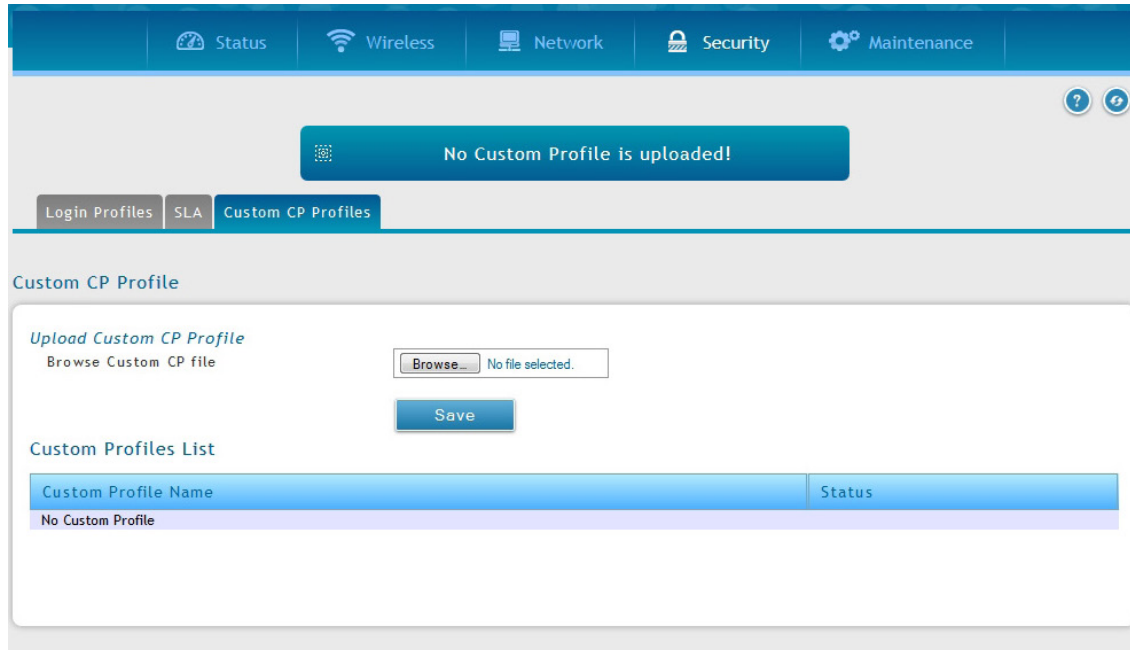


図 7-25 Upload a Custom Profile 画面

外部認証

Security > Authentication > External Auth Server メニュー

コントローラ自身の現在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のに使用されます。外部認証サーバは、一般的に安全であり、無線アクセスポイントの接続を許可するため、IPSec エンドポイントを認証するため、さらに、VLAN 上のキャプティブポータルを通じたアクセスを許可する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。すべての場合で、「Server Checking」ボタンは、設定したサーバへの接続性を検証するのに使用されます。

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 および / または WPA2 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 は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 認証を試み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** 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。

The screenshot displays the 'RADIUS Server Configuration' page. At the top, there is a navigation bar with tabs: Status, Wireless, Network, Security, and Maintenance. Below this, a breadcrumb trail shows: Security > Authentication > External Auth Server > Radius Server. A sub-menu bar contains: Radius Server (selected), Radius Accounting, Radius Accounting Global Setting, POP3 Server, POP3 Trusted CA, LDAP Server, and AD Server. The main content area has a title 'Radius Server Configuration' and a descriptive paragraph. Below this, the 'Server Check' section includes a 'Server Checking' button. The configuration fields are organized into three sections for three different servers. Each section contains: Authentication Server IP Address, Authentication Port, Secret, Timeout, and Retries. The first server's fields are pre-filled with 192.168.1.2, 1812, a masked secret, 1 second timeout, and 2 retries. The second and third servers have similar pre-filled values. At the bottom, there are 'Save' and 'Cancel' buttons.

図 7-26 RADIUS Server Configuration 画面

2. 以下の情報を表示または指定します。

項目	説明
Authentication Server 1-3 IP Address	RADIUS 認証サーバの IP アドレスを指定します。
Authentication Port	RADIUS メッセージを送信する RADIUS 認証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 サーバにログインできる秘密鍵を指定します。それは RADIUS サーバの秘密鍵に一致する必要があります。
Timeout	RADIUS 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	コントローラが処理をやめる前に RADIUS サーバに行う試みの数を指定します。

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。

RADIUS アカウンティングの設定

Security > Authentication > External Auth Server > RADIUS Accounting メニュー

RADIUS アカウンティングの設定を行います。

1. Security > Authentication > External Auth Server > RADIUS Accounting 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。

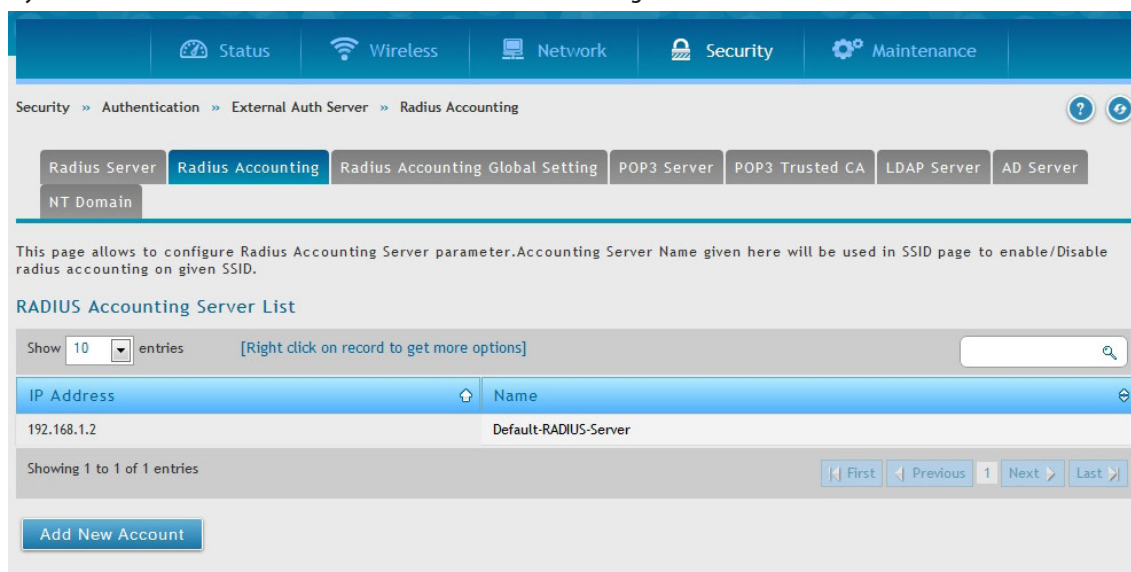


図 7-27 RADIUS Accounting 画面

2. 「Add New Account」をクリックして以下の画面を表示します。

図 7-28 RADIUS Accounting - Add New Account 画面

3. 以下の情報を表示または指定します。

項目	説明
Accounting Server IP Address	RADIUS アカウンティングサーバの IP アドレスを入力します。
Authentication Server Name	RADIUS アカウンティングサーバ名を指定します。
Port	RADIUS アカウンティングサーバのポートを指定します。
Secret	RADIUS サーバにログインできる秘密鍵を指定します。

4. 「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。

RADIUS アカウンティンググローバル設定

Security > Authentication > External Auth Server > RADIUS Accounting Global Setting メニュー

RADIUS アカウンティングサーバのいくつかのパラメータに対して、設定、表示を行います。指定の SSID に対してアカウンティングモードを使用してグローバルにアカウンティングを有効 / 無効にします。

1. Security > Authentication > External Auth Server > RADIUS Accounting Global Setting 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。

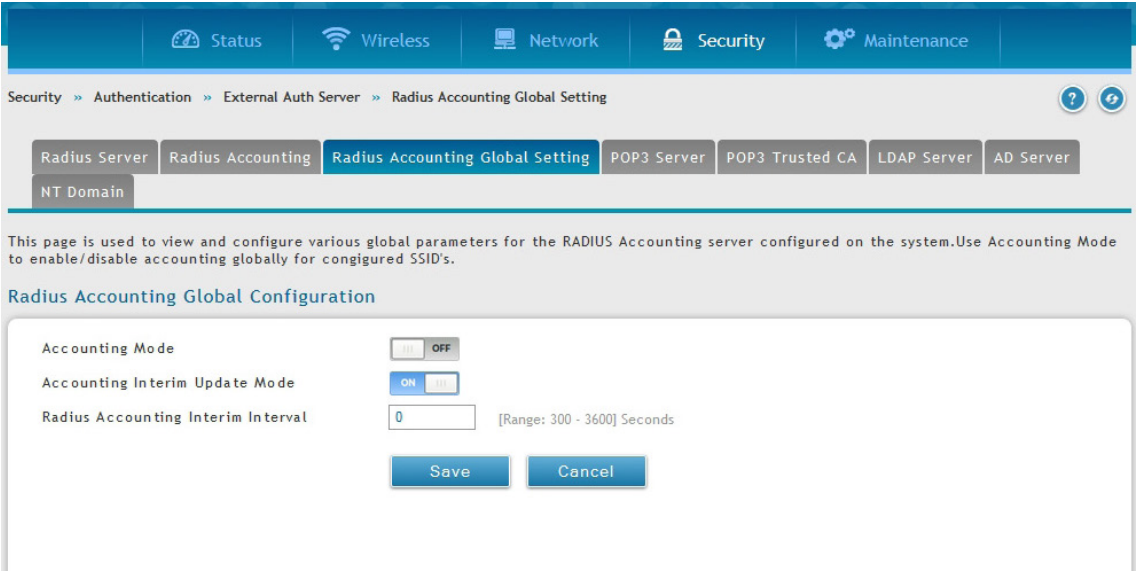


図 7-29 RADIUS Accounting Global Setting 画面

2. 以下の情報を表示または指定します。

項目	説明
Accounting Mode	「ON」してアカウンティングモードを有効にします。
Accounting Interim Update Mode	「ON」して「Interim Interval Period」を基準にしたアカウンティング（Interim-Update）モードを有効にします。初期値は無効です。
RADIUS Accounting Interim Interval	コントローラから送信される RADIUS アカウンティング（Interim-Update）パケットの「Interim Interval」を指定します。値は 300 から 3600 の間で指定できます。

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。

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 サーバに送信するのに、ポート 995 経由の 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 は 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 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。

The screenshot shows the 'POP3 Server Configuration' page. At the top, there's a navigation bar with tabs: Status, Wireless, Network, Security, and Maintenance. Below this, a breadcrumb trail reads 'Security > Authentication > External Auth Server > POP3 Server'. A secondary set of tabs includes 'Radius Server', 'Radius Accounting', 'Radius Accounting Global Setting', 'POP3 Server' (which is selected), 'POP3 Trusted CA', 'LDAP Server', and 'AD Server'. A 'NT Domain' tab is also visible. The main content area has a message: 'This page allow user to configure pop3 authentication servers.' Below this is the 'POP3 Server Configuration' section. It contains a 'Server Check' section with a 'Server Checking' button. The configuration fields are: 'Authentication Server1 (Primary)' (text input), 'Authentication Port' (110, with a note '[Default: 110, Range: 1 - 65535]'), 'SSL Enable' (OFF), 'Authentication Server2 (Secondary)' (text input, marked 'Optional'), 'Authentication Port' (110, with a note '[Default: 110, Range: 1 - 65535]'), 'SSL Enable' (OFF), 'Authentication Server3' (text input, marked 'Optional'), 'Authentication Port' (110, with a note '[Default: 110, Range: 1 - 65535]'), 'SSL Enable' (OFF), 'Timeout' (text input, with a note '(Second)'), and 'Retries' (text input). At the bottom are 'Save' and 'Cancel' buttons.

図 7-30 POP3 Server Configuration 画面

2. 以下の情報を表示または指定します。

項目	説明
Authentication Server	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 RADIUS 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	これはコントローラが処理をやめる前に POP3 サーバに行う試みの数を指定します。

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。

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 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。

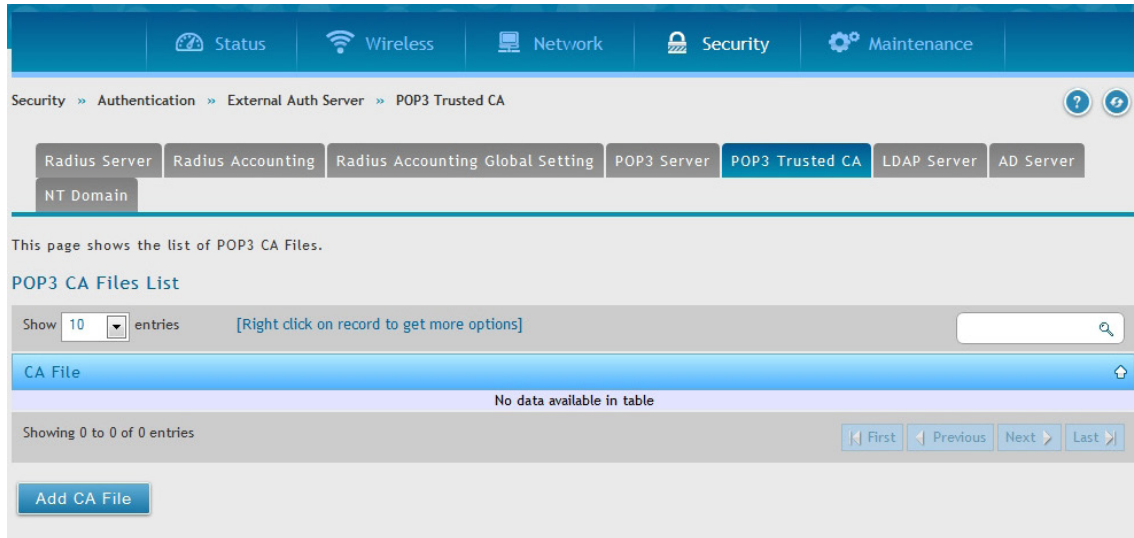


図 7-31 POP3 CA Files List 画面

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 7-32 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のに LDAP を使用します。LDAP サーバは、ディレクトリ構成内に大容量のユーザデータベースを保持します。そのため、同じユーザ名でも異なるグループに所属するユーザは、ユーザ情報が階層的な方法に保存されることから、認証されます。なお、Windows における LDAP サーバまたは Linux 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詳細情報は、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)、およびいくつかの場合では管理者アカウント & 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 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。

The screenshot displays the 'LDAP Server Configuration' page. At the top, there's a navigation bar with tabs: Status, Wireless, Network, Security, and Maintenance. Below this, a breadcrumb trail shows 'Security > Authentication > External Auth Server > LDAP Server'. A secondary set of tabs includes 'Radius Server', 'Radius Accounting', 'Radius Accounting Global Setting', 'POP3 Server', 'POP3 Trusted CA', 'LDAP Server' (which is selected), and 'AD Server'. Below the tabs, a message states: 'This page allows a user to configure authentication servers for LDAP authentication.' The main configuration area is titled 'LDAP Server Configuration' and contains several sections: 'Server Check' with a 'Server Checking' button; 'Authentication Server 1', 'Authentication Server 2', and 'Authentication Server 3' each with an input field and an 'Optional' label; 'LDAP Attribute 1' through 'LDAP Attribute 4' each with an input field and an 'Optional' label; 'LDAP Base DN' with an input field; 'Second LDAP Base DN' and 'Third LDAP Base DN' each with an input field and an 'Optional' label; 'Timeout' with an input field and a range '[Range: 1 - 999] Seconds'; 'Retries' with an input field containing '2' and a range '[Range: 1 - 9]'; 'First Administrator Account' with an input field containing 'admin' and an 'Optional' label; 'Password' with a masked input field and an 'Optional' label; 'Second Administrator Account' with an input field and an 'Optional' label; 'Password' with a masked input field and an 'Optional' label; 'Third Administrator Account' with an input field and an 'Optional' label; and 'Password' with a masked input field and an 'Optional' label. At the bottom, there are 'Save' and 'Cancel' buttons.

図 7-33 LDAP Server Configuration 画面

2. 以下の情報を表示または指定します。

項目	説明
Authentication Server (1-3)	LDAP 認証サーバの IP アドレスを指定します。
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のにこれらを使用できます。
LDAP Base DN	LDAP 認証におけるベースドメイン名を指定します。このドメインに 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。
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	コントローラが処理をやめる前に LDAP サーバに行う試みの数を決定します。
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。

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。

アクティブディレクトリサーバ（AD Server）の設定

Security > Authentication > External Auth Server > AD Server メニュー

アクティブディレクトリ認証は NT ドメイン認証の高機能バージョンです。Organizational Units（OUs）内でグループ化されているユーザの認証に「Kerberos」プロトコルが使用されます。通常アクティブディレクトリサーバは百万単位のユーザをサポートすることができるストラクチャを有していますが、NT ドメインサーバの場合数千程度です。

設定された認証サーバとアクティブディレクトリドメインは、外部の Windows ベースサーバのユーザディレクトリを使用して、ユーザを認証します。この認証方法は「SSL VPN」クライアントや「IPSec」「PPTP」「L2TP」クライアント認証などで有効です。

AD サーバの設定

1. Security > Authentication > External Auth Server > AD Server 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。

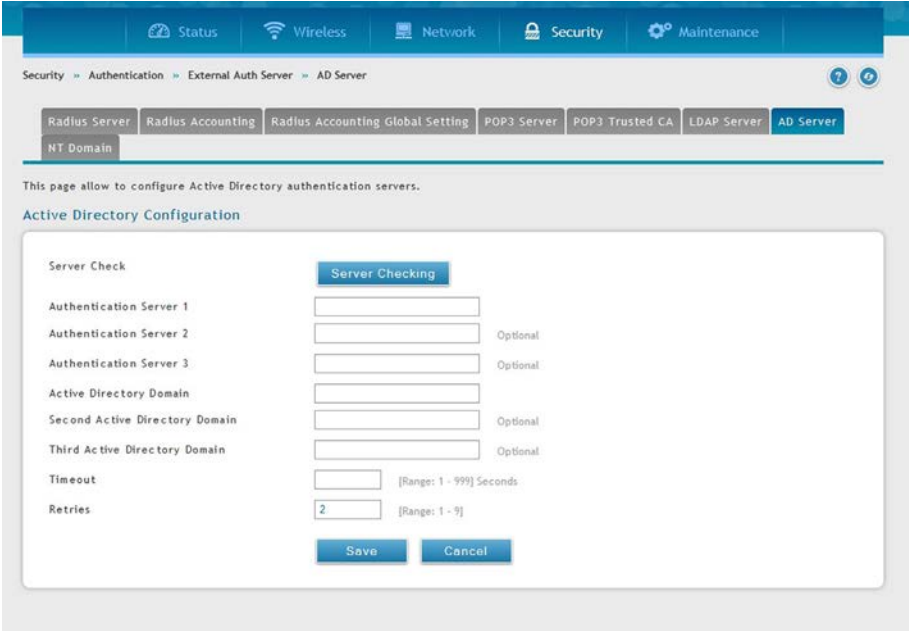


図 7-34 Active Directory Server 設定

2. 以下の情報を表示または指定します。

項目	説明
Authentication Server	AD サーバの IP アドレスを指定します。
Active Directory Domain	ドメインが Active Directory 認証を使用する場合、本欄にアクティブなディレクトリドメイン名を入力する必要があります。それらのアクティブディレクトリのユーザ名とパスワードを使用することによって、アクティブディレクトリデータベースに登録されているユーザは、SSL VPN ポータルにアクセスすることができます。
Timeout	AD サーバに到達するタイムアウト時間
Retries	コントローラが認証サーバへの到達を停止してから認証サーバによる認証を再試行する回数。

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。

NT ドメインサーバ (NT Domain Server) の設定

Security > Authentication > External Auth Server > NT Domain Server メニュー

NT ドメインサーバは事前に設定済みのワークグループフィールドを経由したユーザとホストの認証を行います。通常、認証ユーザのディレクトリ集約のため、認証ドメインの管理は「Windows」または「Samba」サーバを使用します。

NT ドメインサーバの設定

1. Security > Authentication > External Auth Server > NT Domain Server 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 7-35 NT Domain Server 設定

2. 以下の情報を表示または指定します。

項目	説明
Authentication Server	NT ドメインサーバの IP アドレスを指定します。
Workgroup	これは NT ドメイン認証に必要なワークグループです。
Timeout	NT ドメインサーバに到達するタイムアウト時間。
Retries	NT ドメインサーバへの到達を停止してから、再度サーバによる認証を再試行する回数。

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。

Facebook Wi-Fi

Security > Authentication > Facebook Wi-Fi メニュー

コントローラに Facebook を登録するとネットワーク接続時、直接当該の Facebook ページにアクセスする事が可能です。

NT ドメインサーバの設定

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

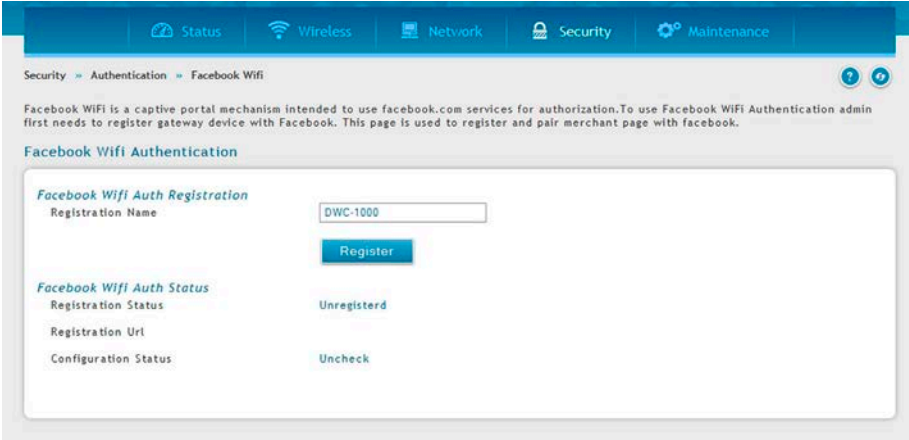


図 7-36 Facebook Wi-Fi 設定

2. 以下の情報を表示または指定します。

項目	説明
Registration Name	登録名を入力します。入力後「Register」をクリックします。
Registration Status	コントローラの Facebook への登録状況を表示します。
Registration URL	登録後、Facebook ページとその URL を直結させます。
Configuration Status	コントローラの Facebook ページへの登録状況を表示します。
Reset	設定をリセットします。

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。

Web コンテンツフィルタリング

Security > Web Content Filter メニュー

コントローラは、管理者が安全な LAN と安全でない Option 間に簡単にアクセスポリシーを作成することができる標準的な Web フィルタリングオプションです。トラフィックタイプに基づいたポリシーを作成する代わりに（ファイアウォールルールを使用する場合など）、Web ベースコンテンツ自身がトラフィックが許可または破棄されるかを決定するために使用されます。

注意 本機能は追加ライセンス「DWC-1000-WCF-12」が有効の場合にのみ利用可能です。

スタティックフィルタリング

Security > Website Filter > Static Filtering メニュー

コンテンツフィルタリングは機能そのものの有効後に、続く別の機能（トラストドメインのリスト、ブロックするキーワードにおけるフィルタリングなど）を設定および使用する必要があります。指定のファイアウォールなど、セキュリティを回避などに使われるプロキシサーバなどをすべての LAN 機器のためにブロックすることが可能です。Java アプレットのインターネットサイトからのダウンロードを防ぎ、同様に ActiveX の Internet Explorer 経由でのダウンロードも防ぎます。セキュリティクッキーの追加には通常セッション情報が含まれており、プライベートネットワーク上でのすべてのデバイスはブロックされます。

1. Security > Web Content Filter > Static Filtering の順にメニューをクリックして、以下の画面を表示します。

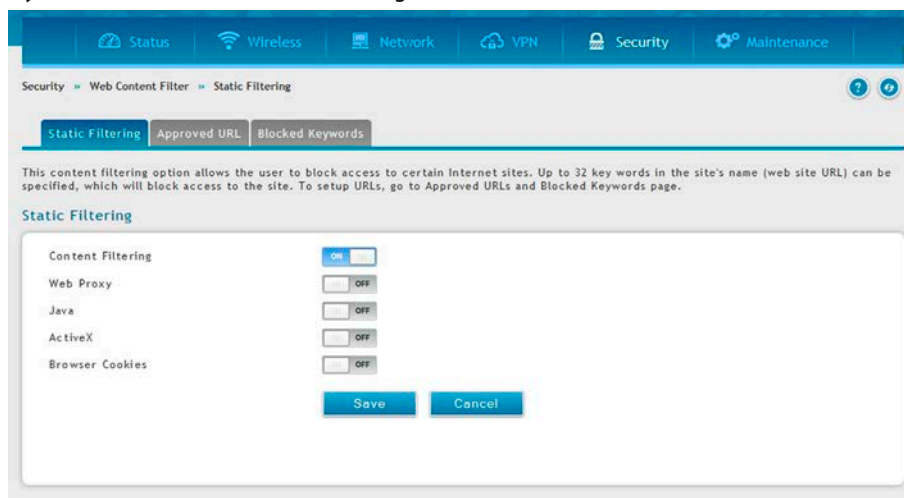


図 7-37 Static Filtering 設定

2. 以下の情報を表示または設定します。

項目	説明
Content Filtering	コンテンツフィルタリングを手動で「有効 / 無効」にします。
Web Proxy	特定のファイアウォールルールを回避するために使用されるプロキシサーバは潜在的なセキュリティの隙間であり、すべての LAN インタフェースデバイスでブロックされます。
Java	Java アプレットはインターネットサイトからダウンロードされるのを防ぐことができます。
ActiveX	ゲートウェイは ActiveX コントロールがインターネットエクスプローラ経由でダウンロードされるのを防ぐことができます。
Browser Cookies	プライベートネットワークにおけるすべてのデバイスのために、また、追加されたセキュリティクッキー（セッション情報を通常含む）をブロックすることができます。

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。

承認済み URL

Security > Web Content Filter > Static Filtering > Approved URL メニュー

URL ドメイン名のための承認リストの表示および追加を行います。

このリストに追加されたドメインは、どんな形式でも許可されます。例えば、ドメイン「dlink」がこのリストに追加されると、次の URL のすべてが LAN からのアクセスを許可されます。: www.dlink.com、support.dlink.com など

また、Approved URL のためのテキストまたは CSV ファイルからのインポート / エクスポートをサポートしています。

1. Security > Web Content Filter > Static Filtering > Approved URL の順にメニューをクリックして、以下の画面を表示します。

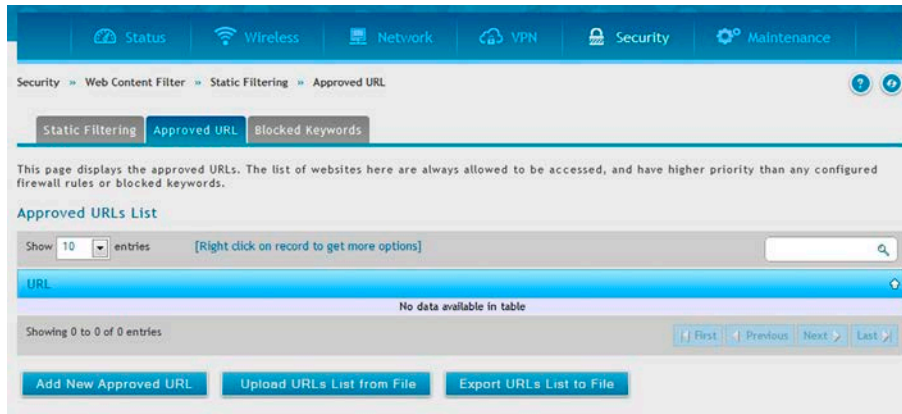


図 7-38 Approved URL List 画面

URL のインポート / アップロード

1. テキスト / CSV ファイルからインポートする場合は、「Upload URLs List from File」をクリックします。
2. 「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。

URL のエクスポート

1. 現状をエクスポートする場合は、「Export URLs List to File」をクリックします。
2. 「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。

URL の追加

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

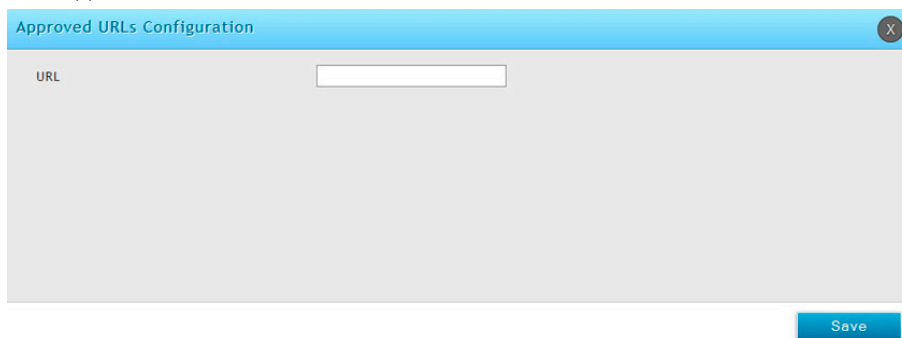


図 7-39 URL の追加

2. 「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。

ブロックキーワード

Security > Web Content Filter > Static Filtering > Blocked Keywords メニュー

URL またはキーワードを入力することで、Web サイトへのアクセスをブロックします。

キーワードブロッキングでは、設定済みリスト内にあるキーワードを含むすべての Web サイトの URL またはサイトのコンテンツをブロックすることができます。これは「Approved URLs List」より低い優先度です。つまり、ブロックキーワードが「Approved URLs List」のトラストドメインによって許可されたサイトに存在している場合、そのサイトへのアクセスは許可されます。また、キーワードブロックのためのテキストまたは CSV ファイルからのインポート / エクスポートをサポートしています。

1. Security > Web Content Filter > Static Filtering > Blocked Keywords の順にメニューをクリックして、以下の画面を表示します。

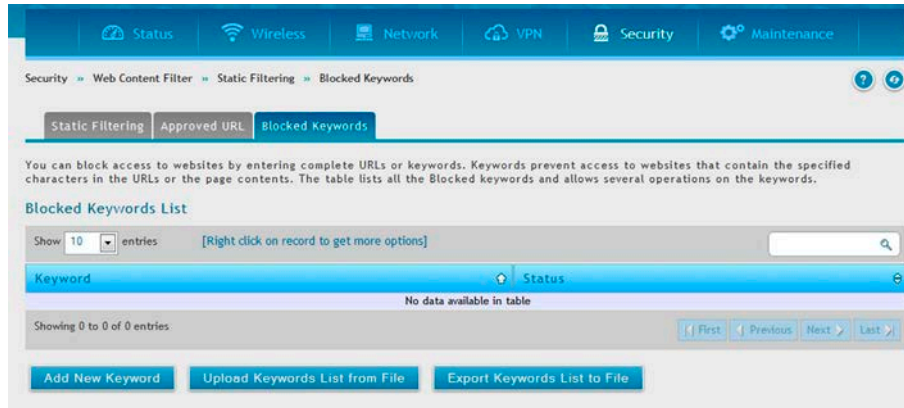


図 7-40 ブロックキーワード

キーワードのインポート / アップロード

1. テキスト / CSV ファイルからインポートする場合は、「Upload Keywords List from File」をクリックします。
2. 「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。

キーワードのエクスポート

1. 現状をエクスポートする場合は、「Export Keywords List to File」をクリックします。
2. 「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。

キーワードの追加

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

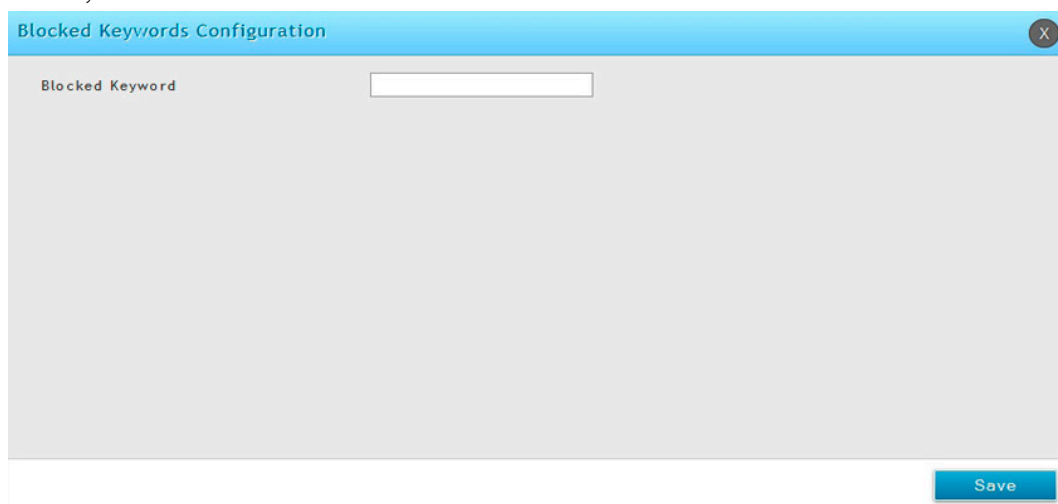


図 7-41 キーワードの追加

2. 「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。

ファイアウォールの設定（Firewall）

Security > Firewall メニュー

コントローラのファイアウォール設定を行います。

注意 本機能は追加ライセンス「DWC-1000-VPN」が有効の場合にのみ利用可能です。

ファイアウォールルールの設定

Security > Firewall > Firewall Rules メニュー

内向き（Option から LAN/DMZ）ルールはご使用のネットワークに入力されるトラフィックに対してアクセス制限を行い、選択的に特定の外部ユーザのみ特定のローカルリソースにアクセスすることを許可することができます。初期値では、LAN または DMZ からの要求に応答する場合を除き、安全でない Option 側からセキュアな LAN に対するすべてのアクセスをブロックします。外部のデバイスがセキュアな LAN 上のサービスにアクセスすることを許可するために、各サービスに内向きのファイアウォールルールを作成する必要があります。

入トラフィックを許可したい場合、コントローラの Option ポートの IP アドレスをパブリックに知らせる必要があります。これは「ご使用のホストの露出」と呼びます。アドレスを知らせる方法は Option ポートの設定方法によって異なります。このコントローラでは、スタティックなアドレスを Option ポートに割り当てる場合には IP アドレスを使用し、または、ご使用の Option アドレスがダイナミックである場合は、DDNS（Dynamic DNS）名を使用できます。

外向き（LAN/DMZ から Option）ルールはご使用のネットワークから出力するトラフィックに対してアクセス制限を行い、選択的に特定のローカルユーザのみ外部リソースにアクセスすることを許可することができます。外向きの初期ルールは、安全なゾーン（LAN）からパブリック DMZ または安全でない Option のいずれかへのアクセスを許可するものです。一方、外向き初期ルールは、DMZ から安全でない Option までのアクセスを拒否するものです。デフォルトの内向きポリシーが「すべて許可」である場合、各サービスに内向きファイアウォールルールを作成することで、ホストのインターネットサービスへアクセスをブロックすることができます。

ここではファイアウォールの設定手順を説明します。

コントローラに関するすべての設定済みファイアウォールルールは「Firewall Rules」リストに表示されます。このリストは、ルールが有効（アクティブ）かどうかを示して、ルールが影響するサービスまたはユーザと共に From/To ゾーンの概要を表示します。

以下の手順に従って新しいファイアウォールルールを登録します。:

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

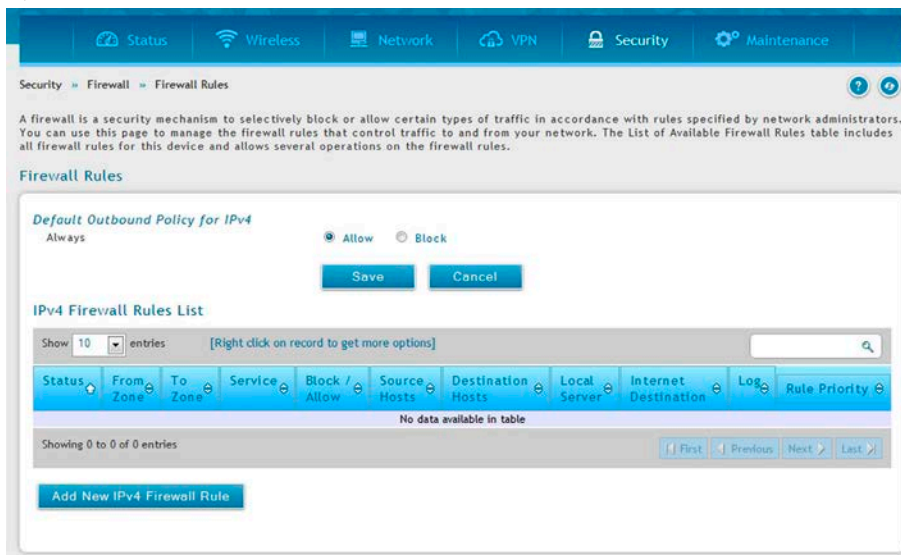


図 7-42 利用可能なファイアウォールスケジュールのリスト

2. ルールを編集、削除するにはエントリで右クリック、「Edit」または「Delete」ボタンをクリックします。
3. 新しいルールを追加するためには、「Add New IPv4 Firewall Rule」ボタンをクリックして新しいルールの設定ページにリンクします。一度作成されると、新しいルールは元々のテーブルに自動的に追加されます。

The image shows a screenshot of the 'IPv4 Firewall Rules Configuration' window. It has a light blue header with a close button (X). The main area is a form with several settings: 'From Zone' is set to 'SECURE (LAN)', 'To Zone' is 'INSECURE (Dedicated WAN)', 'Service' is 'ANY', 'Action' is 'Always Block'. Below these are radio button options for 'Source Hosts' and 'Destination Hosts', both set to 'Any'. There are also radio button options for 'Log', set to 'Never'. At the bottom, 'QoS Priority' is set to 'Normal-Service'. A 'Save' button is located at the bottom right of the window.

図 7-43 ファイアウォールルール設定

4. ファイアウォールルールを定義するパラメータには以下の項目があります。:

項目	説明
From Zone	トラフィックを生成するソースとなる「From Zone」を選択します。「SECURE(LAN)」「public DMZ」「INSECURE WAN」から選択可能です。インバウンドルールには「WAN」を選択する必要があります。
To Zone	このルールでカバーされるトラフィックの宛先になる「To Zone」を選択します。If the「From Zone」が「WAN」の場合、「To Zone」は「public DMZ」または「SECURE (LAN)」である必要があります。「From Zone」が「LAN」であれば、「To Zone」は「public DMZ」または「INSECURE WAN」となります。
Service	「ANY」はすべてのトラフィックがこのルールの影響を受けることを意味しています。特定のサービスのために、プルダウンメニューには一般的なサービスが表示されます。またはカスタム定義サービスを選択できます。
Action	このルールが定義する以下の4つの操作から1つを選択します。: <ul style="list-style-type: none"> • Always Block (常にブロック) • Always Allow (常に許可) • Block by schedule, otherwise Allow (スケジュールによりブロック、その他は許可)。 • Allow by schedule, otherwise Block (スケジュールにより許可、その他はブロック)。 このルールに割り当てるためにはプルダウンメニューで利用可能となるようにスケジュールをあらかじめ設定する必要があります。
Source / Destination Hosts	それぞれの関連するカテゴリで、ルールを適用するユーザを選択します。: <ul style="list-style-type: none"> • Any (すべてのユーザ) • Single Address (IP アドレスを入力します。) • Address Range (適切な IP アドレス範囲を入力します。)
Log	このルールによってフィルタされるトラフィックをログに出力することができます。これには、別途コントローラのログ出力機能を設定する必要があります。
QoS Priority	外向きルール (To Zone = insecure Option only の場合) は、QoS のプライオリティタグでトラフィックをマークすることができます。以下のプライオリティレベルを選択します。: <ul style="list-style-type: none"> • Normal-Service : ToS=0 (最も低い QoS) • Minimize-Cost : ToS=1 • Maximize-Reliability : ToS=2 • Maximize-Throughput : ToS=4 • Minimize-Delay : ToS=16 (最も高い QoS)

5. 「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。

ファイアウォールスケジュール設定

Security > Firewall > Schedules メニュー

ファイアウォールのルールは設定されたスケジュールに基づき、自動的に有効 / 無効に指定することが可能です。スケジュール設定ページでは週 / 日 / 時の単位で新しくスケジュールを設定することが可能です。設定したスケジュールをファイアウォールルール設定ページで選択して適用します。

注意 全てのスケジュールはコントローラで設定された時刻とタイムゾーンを基準としています。時刻、タイムゾーンの設定については対象の項目でご確認ください。

以下の手順に従って新しいファイアウォールスケジュールプロファイルを登録します。:

1. Security > Firewall > Schedules Profiles の順にメニューをクリックして、以下の画面を表示します。

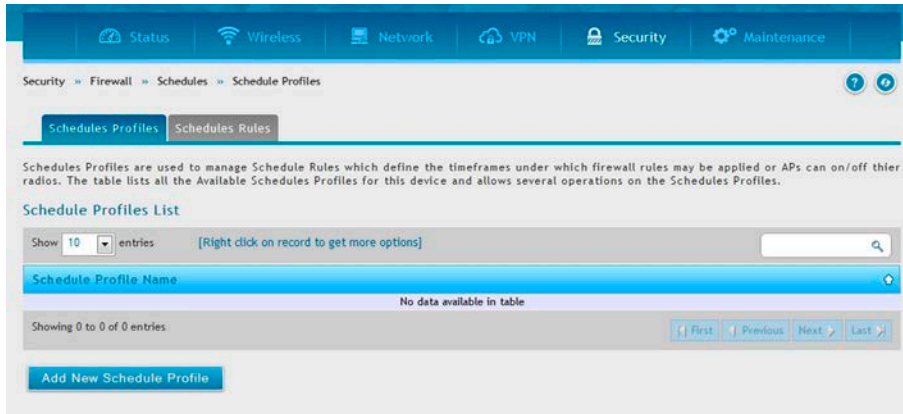


図 7-44 Schedules Profiles 設定

2. 「Add New Schedule Profile」 ボタンをクリックして、プロファイル名を入力、「Save」をクリックします。



図 7-45 Add New Schedule Profile 設定

3. 「Schedules Rules」 タブをクリックし、以下の画面を表示します。「Schedule Name」で設定するスケジュールプロファイルを選択します。

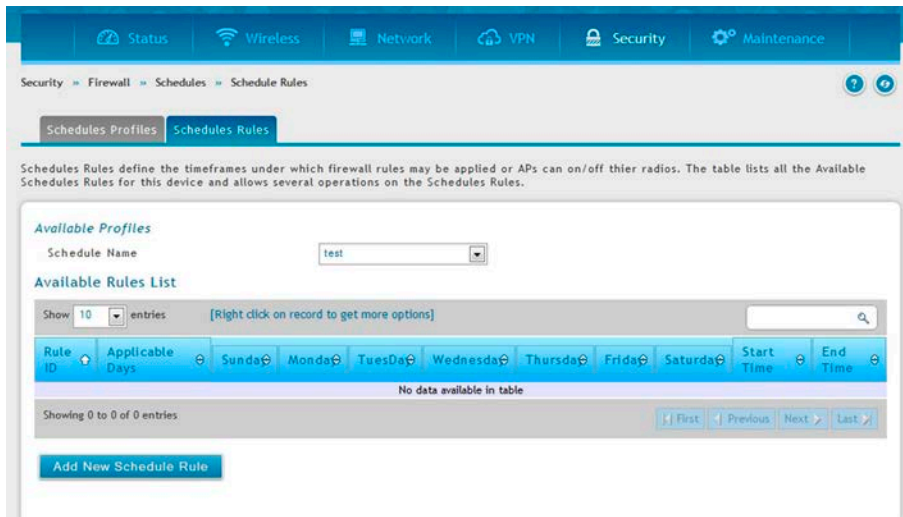


図 7-46 Schedule Rules 設定

4. エントリを編集、削除する場合は、エントリで右クリックし、「Edit」または「Delete」をクリックします。スケジュールを追加する場合は「Add New Schedule」ボタンをクリックします。

The image shows a 'Schedule Rule Configuration' window. It has a title bar with a close button. Inside, there's a 'Schedule Profile' dropdown set to 'test'. Below it are 'Entry ID' (1-UNSET), 'Applicable Days' (Daily), 'Start Time' (12:00 AM), and 'End Time' (12:00 AM). Each time field has a digital clock interface with HH, MM, and AM/PM buttons. A 'Save' button is located at the bottom right.

図 7-47 Schedule Configuration 設定

5. 以下の情報を表示または指定します。

項目	説明
Entry ID	編集するエントリの ID を選択します。
Applicable Days	対象となる月日を選択します。
Start Time	開始時間を指定します。
End Time	終了時間を指定します。

6. 「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。

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。

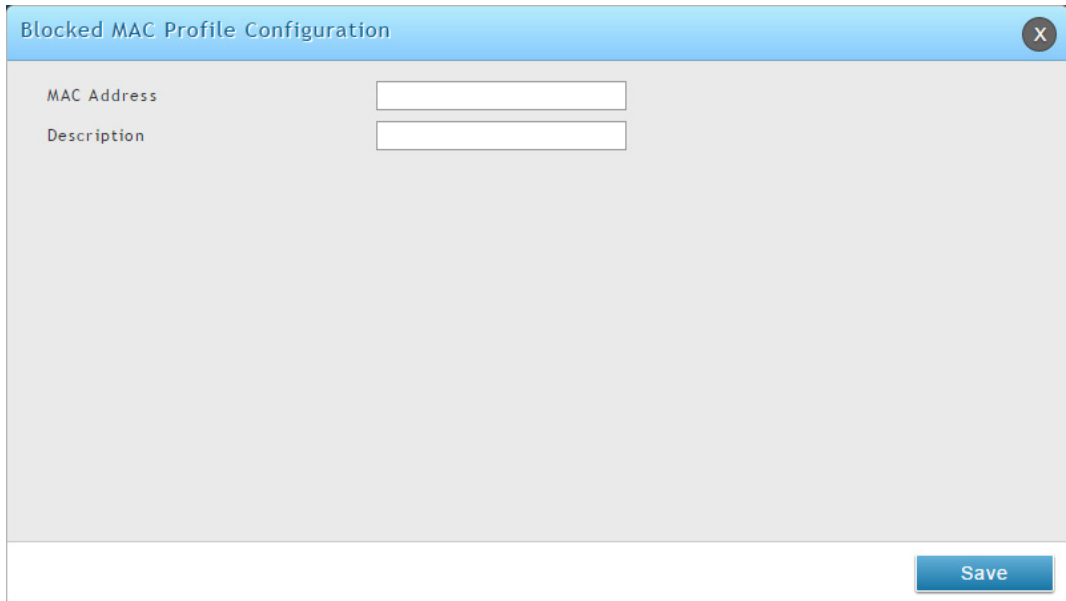
ブロックするクライアントの追加

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。

The screenshot shows the 'Blocked Clients' page. At the top is a navigation bar with tabs: Status, Wireless, Network, Security (selected), and Maintenance. Below the navigation bar, the breadcrumb is 'Security > Firewall > Blocked Clients'. The main content area says 'This page shows a list of clients MAC addresses blocked by admin.' and 'Block MAC Clients List'. There's a 'Show 10 entries' dropdown and a search bar. Below is a table with columns 'MAC Address' and 'Description'. The table is empty, with the message 'No data available in table'. At the bottom, there are navigation buttons (First, Previous, Next, Last) and an 'Add New Blocked Clients' button.

図 7-48 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。



The image shows a dialog box titled "Blocked MAC Profile Configuration". It has a blue header bar with a close button (X) in the top right corner. The main area is light gray and contains two input fields: "MAC Address" and "Description". Below these fields is a large, empty rectangular area. At the bottom right of the dialog is a blue button labeled "Save".

図 7-49 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。

カスタムサービスにおけるセキュリティ

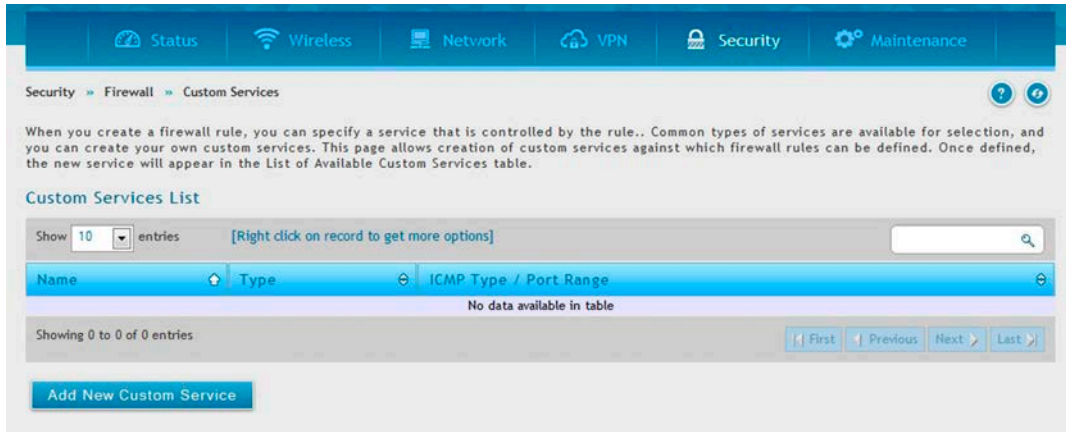
Security > Firewall > Custom Services メニュー

ここではファイアウォールルールを定義するカスタムサービスを作成することができます。

ファイアウォールルールを作成する場合、ルールによって制御されるサービスを指定することができます。一般的なサービスタイプを選択して利用可能であり、自身のカスタムサービスを作成することもできます。

一般的なサービスは既知の TCP/UDP/ICMP ポートを使用しますが、多くのカスタムまたは一般的でないアプリケーションは LAN または Option に存在します。カスタムサービス設定メニューでは、このサービスのためにポート範囲を定義して、トラフィックタイプ (TCP/UDP/ICMP) を確認することができます。定義されると、新しいサービスは「ファイアウォールルール設定」メニューのサービスリストに表示されます。

1. Security > Firewall > Custom Services メニューをクリックして、以下の画面を表示します。



The image shows the "Custom Services List" screen in the Security > Firewall > Custom Services menu. The top navigation bar includes tabs for Status, Wireless, Network, VPN, Security, and Maintenance. The main content area has a blue header with the title "Custom Services List". Below the header is a text box explaining that users can create custom services for firewall rules. A table with columns "Name", "Type", and "ICMP Type / Port Range" is shown, but it is empty with the message "No data available in table". At the bottom is a blue button labeled "Add New Custom Service".

図 7-50 Custom Service

2. エントリを編集、削除する場合は、エントリで右クリックし、「Edit」または「Delete」をクリックします。スケジュールを追加する場合は「Add New Custom Service」ボタンをクリックします。

図 7-51 Add New Custom Service

3. 以下の情報を表示または指定します。

項目	説明
Name	カスタムサービス名を入力します。
Type	サービスを使用する L3 プロトコル (TCP、UDP、BOTH、ICMP) を選択します。
Port Type	「Port Range」または「Multiple Ports」を選択します。
Start Port	「Port Range」を選択時に、サービスに使用する開始ポートを指定します。
Finish Port	「Port Range」を選択時に、サービスに使用する終了ポートを指定します。
Ports	「Multiple Port」を選択時に、サービスに使用する複数ポートを「,」（コンマ）で区切り指定します。
ICMP Type	「ICMP Type」を選択時に、適用する数値を 0 から 40 の間で指定します。

4. 「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。

ALG サポート

Security > Firewall > ALGs メニュー

ALG を有効 / 無効にします。

ALG (Application Level Gateways) は、シームレスにアプリケーションレイヤプロトコルをサポートするためにこのコントローラのファイアウォールと NAT サポートを機能強化するセキュリティコンポーネントです。

いくつかの場合では、管理者が同じサポートを実行するために大きなポート番号をオープンしなくても、ALG により、特定のクライアントアプリケーション (H.323 または RSTP など) が必要とする既知のポートと通信するために、ファイアウォールがダイナミックなエフェメラル TCP/UDP ポートを使用することができます。ALG は、それをサポートする特定のアプリケーションが使用するプロトコルを理解しているので、コントローラのファイアウォールを通じたクライアントアプリケーションのサポートを導入する非常に安全で効率的な方法です。

1. Security > Firewall > ALGs メニューをクリックして、以下の画面を表示します。

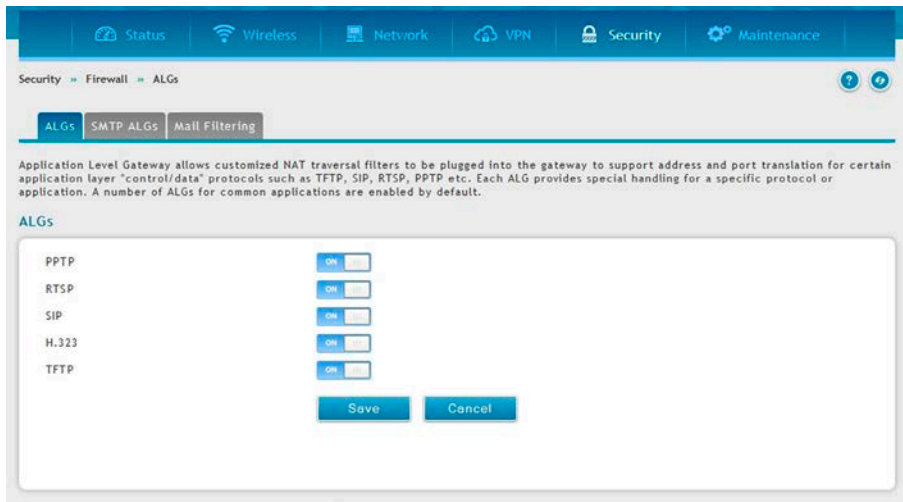


図 7-52 ALGs

2. コントローラへのスルーを許可するプロトコルを「ON」にし、「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。

SMTP ALGs

Security > Firewall > ALGs > SMTP ALGs メニュー

Simple Mail Transfer Protocol (SMTP) は、インターネット経由で E-mail を送信するために使用されるテキストベースのプロトコルです。通常、ローカルの SMTP サーバは、DMZ に置かれるため、リモート SMTP サーバが送信したメールは、ローカルサーバに到達するようにコントローラを横断します。ローカルユーザは、E-mail のクライアントソフトウェアを使用してローカルの SMTP サーバから E-mail を取得します。SMTP はクライアントが E-mail を送信している場合に使用されます。また、SMTP ALG は、クライアントとサーバの両方から生成される SMTP トラフィックをモニターするために使用されます。

1. Security > Firewall > ALGs > SMTP ALGs メニューをクリックして、以下の画面を表示します。

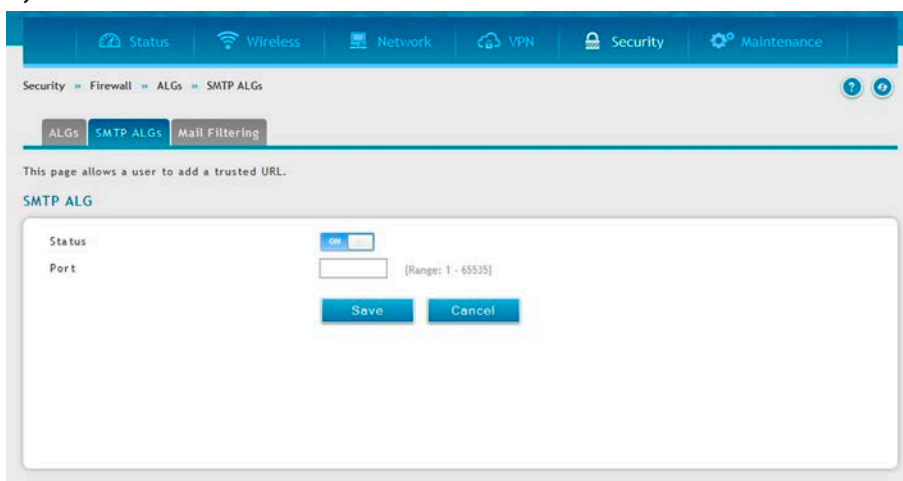


図 7-53 SMTP ALGs

2. 「Status」を「ON」にし、SMTP パケットを精査するポートを指定します。「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。

Mail Filtering

Security > Firewall > ALGs > Mail Filtering メニュー

メールフィルタリングを行います。

1. Security > Firewall > ALGs > Mail Filtering メニューをクリックして、以下の画面を表示します。

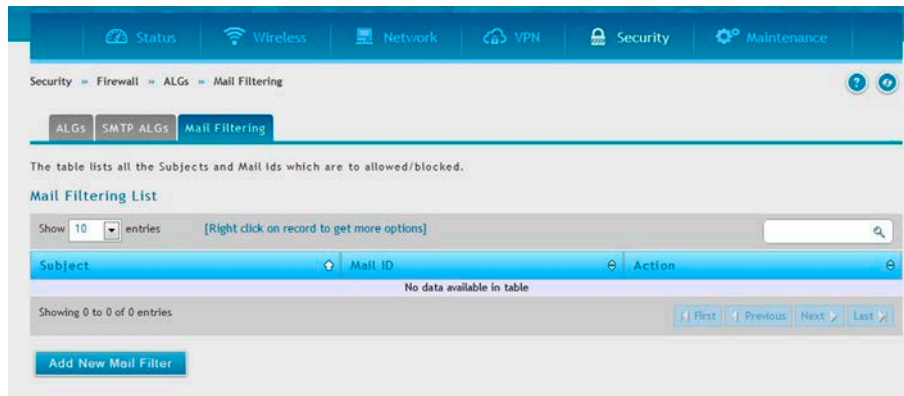


図 7-54 Mail Filtering

2. エントリを編集、削除する場合は、エントリで右クリックし、「Edit」または「Delete」をクリックします。メールフィルタを追加する場合は「Add New Mail Filter」ボタンをクリックします。

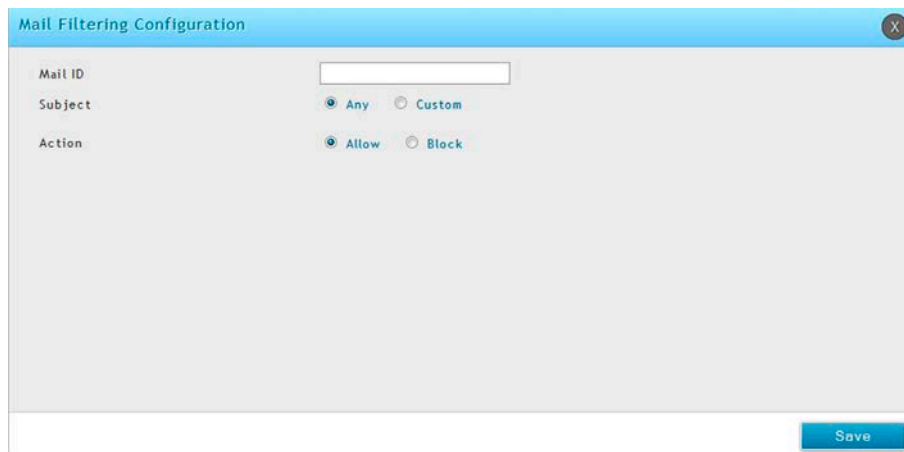


図 7-55 Add New Mail Filter

3. 「Mail ID」を入力し、「Subject」を「Any」「Custom」から指定します。「Action」を「Allow」（許可）「Deny」（拒否）から指定し、「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。

ファイアウォールのための VPN パススルー

Security > Firewall > VPN Passthrough メニュー

LAN とインターネット間の IPSec、PPTP、および L2TP VPN トンネル接続用の暗号化された外向き VPN トラフィックを許可する（パススルー）ようにファイアウォール設定を行います。特定のファイアウォールルールまたはサービスはこのパススルーを行うように設定されていません。そのため、「VPN PASSTHROUGH」（パススルーチェックボックス）を有効にすることで、同じサービスに基づくファイアウォールルールより高い優先度を持つことができます。

1. Security > Firewall > VPN Passthrough の順にメニューをクリックして、以下の画面を表示します。

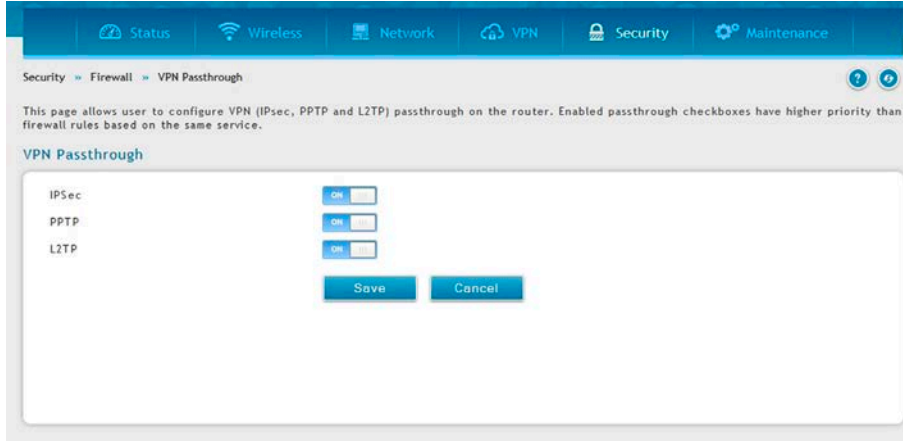


図 7-56 VPN Passthrough

2. 許可する VPN プロトコルを「ON」にし、「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。

ダイナミックポートフォワーディング

アプリケーションルール設定

Security > Firewall > Dynamic Port Forwarding > Application Rules メニュー

アプリケーションルールはポートトリガルールとも呼ばれます。本機能により、LAN または DMZ におけるデバイスは、それらに送信されるように 1 つ以上のポートを要求することができます。ポートトリガは、定義済みの出力ポートの 1 つにある LAN/DMZ からの外向き要求を待っており、特定のトラフィックタイプ用の入力ポートをオープンします。これは、アプリケーションがオープンした出力または入力ポートでデータを送信している間、ダイナミックなポートフォワーディングの形式として考えることができます。

ポートトリガを行うアプリケーションルールはファイアウォールルールの設定時に利用可能なオプションであるスタティックポートフォワーディングより柔軟性があります。これはポートトリガルールが特定の LAN IP または IP 範囲を参照する必要がないためです。その上、使用中でない場合でもポートはオープンされたままとなるため、その結果、ポートフォワーディングが提供しないセキュリティのレベルを提供します。

注意 入力ポートのオープン前に出力用の接続を行う LAN デバイスに依存するため、ポートトリガは LAN 上のサーバには適切ではありません。

いくつかのアプリケーションでは、外部デバイスがそれらに接続する場合に適切に機能するよう特定のポートまたはポート範囲にデータを受信することが必要です。コントローラは必要とされるポートまたはポート範囲にあるアプリケーションだけにすべての入力データを送信する必要があります。コントローラには、対応する外向き/内向きのポートを持つ一般的なアプリケーションやゲームのリストがあり、オープンできます。また、有効になると、オープンすべきトラフィックタイプ（TCP または UDP）および入出力ポートの範囲を定義することでポートトリガルールを指定することができます。

1. Security > Firewall > Dynamic Port Forwarding > Application Rules の順にメニューをクリックして、以下の画面を表示します。

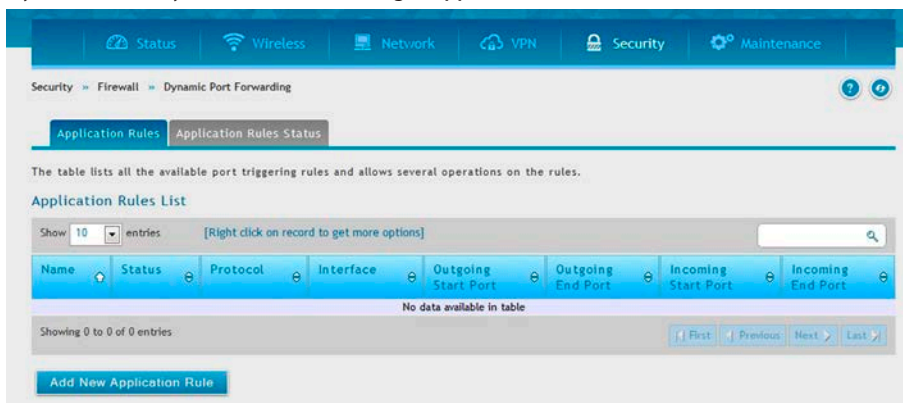


図 7-57 Application Rules

2. エントリを編集、削除する場合は、エントリで右クリックし、「Edit」または「Delete」をクリックします。ルールを追加する場合は「Add New Application Rule」ボタンをクリックします。

The screenshot shows the 'Application Rules Configuration' window. It has a title bar with a close button. The main area is divided into sections: 'Application Rules' with fields for Name, Enable (a toggle switch set to OFF), Protocol (radio buttons for TCP and UDP, with TCP selected), and Interface (radio buttons for LAN and DMZ, with LAN selected). Below this is the 'Outgoing (Trigger) Port Range' section with 'Start Port' and 'To' input fields, each with a range hint '[Range: 0 - 65535]'. The 'Incoming (Response) Port Range' section also has 'Start Port' and 'To' input fields with the same range hint. A 'Save' button is located at the bottom right of the window.

図 7-58 Add New Application Rule

3. 以下の情報を表示または指定します。「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。

項目	説明
Name	ルール名を入力します。
Enable	「ON」にしてルールを有効にします。
Protocol	プロトコルを「TCP」「UDP」から選択します。
Interface	インタフェースを「LAN」「DMZ」から選択します。
Outgoing (Trigger) Port Range	開始 / 終了トリガポートを指定します。
Incoming (Response) Port Range	開始 / 終了受信ポートを指定します。

4. 「Application Rules Status」ボタンをクリックし、ルールの一覧と状態を表示します。

The screenshot shows the 'Application Rules Status' page. At the top is a navigation bar with tabs: Status, Wireless, Network, VPN, Security, and Maintenance. Below this is a breadcrumb trail: Security > Firewall > Dynamic Port Forwarding > Application Rules Status. There are two tabs: 'Application Rules' and 'Application Rules Status', with the latter being selected. The main content area starts with the text: 'This page lists the application rules containing status, open ports and expiry time for a particular rule.' Below this is a section titled 'Application Rules Status List'. It includes a search bar and a dropdown menu set to 'Show 10 entries'. Below the search bar is a table with three columns: 'LAN / DMZ IP Address', 'Open Ports', and 'Time Remaining (Sec.)'. The table is currently empty, with the text 'No data available in table' centered. At the bottom of the table area, it says 'Showing 0 to 0 of 0 entries' and has navigation buttons: 'First', 'Previous', 'Next', and 'Last'.

図 7-59 Application Rules Status

インターネット攻撃から保護する

Security > Firewall > Attack Checks メニュー

攻撃は、コントローラを使用不能にする悪意あるセキュリティ違反または意図的ではないネットワーク問題であるかもしれません。攻撃のチェックにより連続する ping リクエストや ARP スキャンを経由するディスカバリなど WAN のセキュリティの脅威を管理することができます。TCP および UDP フラッド攻撃のチェックを有効にすると、WAN リソースの極端な利用を管理することができます。

さらに Denial-Of-Service (DoS) 攻撃がブロックされます。これらの攻撃は、処理能力と帯域幅を使い切り、通常、定期的なネットワークサービスの動作を妨げてしまいます。ICMP パケットフラッディング、SYN トラフィックフラッディング、および Echo ストームのしきい値は問題となるソースからのトラフィックを一時的に疑うために設定されます。

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

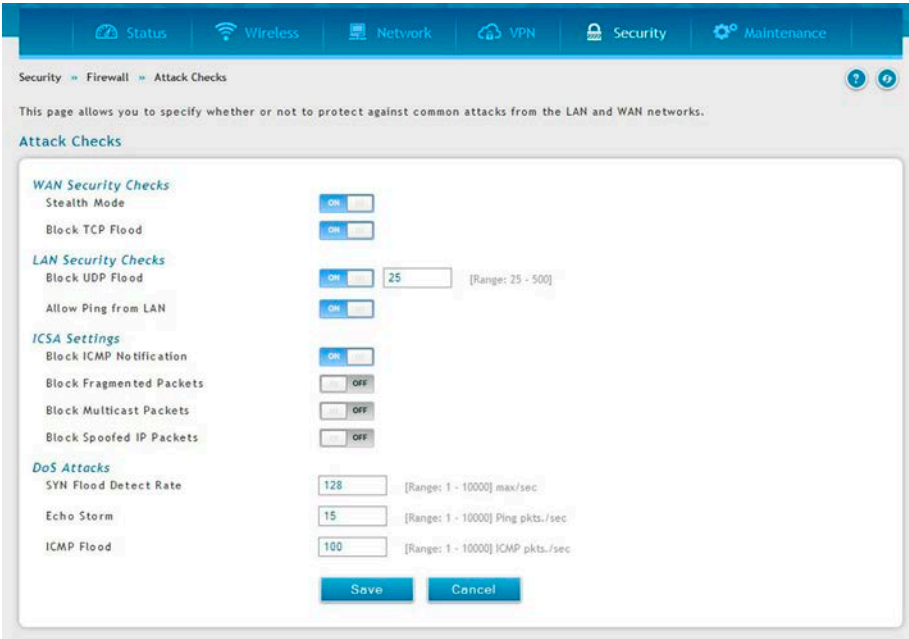


図 7-60 インターネット攻撃からコントローラと LAN を保護する

2. 以下の項目を指定します。

項目	説明
WAN Security Checks	
Stealth Mode	「Stealth Mode」モードが有効になると、ルータは WAN からのポートスキャンに応答しません。これにより検出と攻撃による影響を低減します。
Block TCP Flood	本オプションを有効にすると、ルータは不正な TCP パケットをすべて破棄して、SYN フラッド攻撃から保護されます。
LAN Security Checks	
Block UDP Flood	本オプションが有効になると、ルータは LAN 上の単一のコンピュータから同時に行われる 25 個以上のアクティブな UDP 接続を受け付けません。
Allow Ping from LAN	ローカルコンピュータからの Ping を許可します。
ICSA Settings	
Block ICMP Notification	これを選択すると、ICMP パケットが特定されることを防止します。ICMP パケットは、特定されるとキャプチャされて Ping (ICMP) フラッド DoS 攻撃に使用されてしまいます。
Block Fragmented Packets	このオプションを選択すると、ゲートウェイを経由するどんなフラグメント化パケットも破棄します
Block Multicast Packets	このオプションを選択すると、ゲートウェイを経由するマルチキャストパケットを破棄します。
Block Spoofed IP Packets	このオプションを選択すると、IP スプーフィングパケットを破棄します。
DoS Attacks	
SYN Flood Detect Rate	SYN フラッドを検出できるレート。
Echo Storm	ルータが WAN からエコーストーム攻撃を検出して、その外部アドレスから更に ping トラフィックを防止する 1 秒あたりの ping パケット数。
ICMP Flood	ルータが WAN から ICMP フラッド攻撃を検出して、その外部アドレスから更に ICMP トラフィックを防止する 1 秒あたりの ICMP パケット数。

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。

第 8 章 VPN 設定

以下は本章の設定項目の説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

設定項目	説明	参照ページ
IPSec VPN (IPSec VPAN の設定)	IPSec VPN の設定とポリシーを作成します。	203
PPTP VPN (PPTP VPN 設定)	PPTP VPN の設定とポリシーを作成します。	214
L2TP VPN (L2TP VPN 設定)	L2TP VPN の設定とポリシーを作成します。	216
SSL VPN (SSL VPN 設定)	SSL VPN の設定とポリシーを作成します。	218
OpenVPN サポート	Open VPN サポートの設定を行います。	226

VPN は 2 つのゲートウェイコントローラ間またはリモート PC クライアント間に安全な通信チャンネル（「トンネル」）を提供します。以下のトンネルタイプを作成することができます。:

- Gateway-to-gateway VPN
リモートサイト間のトラフィックを保証するために 2 つ以上のコントローラを接続します。
- リモートクライアント (client-to-gateway VPN トンネル)
リモート PC クライアントの IP アドレスが事前に知られていない場合に、リモートクライアントが VPN トンネルを開始します。この場合、ゲートウェイは応答者として動作します。
- NAT コントローラの背後のリモートクライアント
クライアントはダイナミック IP アドレスを持ち、NAT コントローラの背後にあります。リモート NAT コントローラの IP アドレスが事前に知られていない場合に、NAT コントローラにあるリモート PC が VPN トンネルを開始します。ゲートウェイの Option ポートが応答者として動作します。
- LAN/WAN PPTP クライアント接続用の PPTP サーバ
- LAN/WAN L2TP クライアント接続用の L2TP サーバ

注意 本機能は追加ライセンス「DWC-1000-VPN」が有効の場合にのみ利用可能です。

IPSec VPN (IPSec VPAN の設定)

VPN > IPSec VPN

外部 IPSec クライアントは、DHCP over IPsec を使用してコントローラへの VPN を形成し、どんなサーバにもアクセスするなどご使用の LAN にかのように動作することができます。DHCP over IPsec を使用して接続するためには、クライアントを許可するように DHCP を有効化にして IPSec ポリシーを作成します。また、接続クライアントは指定した範囲から IP アドレスを取得します。

Policies (IPSec VPN ポリシーの設定)

VPN > IPSec VPN > Policies

ここではコントローラに設定済みの IPSec VPN ポリシーのリストを表示します。さらに、IPsec VPN ポリシーの追加、削除、編集、および有効化 / 無効化ができます。

IPSec ポリシーは本コントローラと他のゲートウェイ間、または本コントローラとリモートホストの IPSec クライアント間にあります。IPSec モードは、2 つのポリシーのエンドポイント間を横切るネットワークによって「Tunnel Mode」または「Transport Mode」になります。

- Transport (転送モード) :
これはこのコントローラとトンネルのエンドポイント（ホスト上の別の IPSec ゲートウェイまたは IPSec クライアントのいずれか）間の end-to-end 通信のために使用されます。データペイロードだけが暗号化されて、IP ヘッダは、変更または暗号化されません。
- Tunnel (トンネルモード) :
このモードはこのゲートウェイがトンネルの 1 つのエンドポイントである network-to-network IPSec トンネルに使用されます。このモードでは、ヘッダを含むすべての IP パケットは、暗号化と認証の両方、またはどちらかが行われています。

トンネルモードを選択した場合、NetBIOS および DHCP over IPsec を有効にすることができます。DHCP over IPsec によりこのコントローラはリモート LAN のホストに IP リースをサービスすることができます。また、このモードでは、1 つの IP アドレス、IP アドレス範囲、またはトンネル上で通信できるローカルおよびリモート両方のプライベートネットワークにおけるサブネットを定義できます。

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

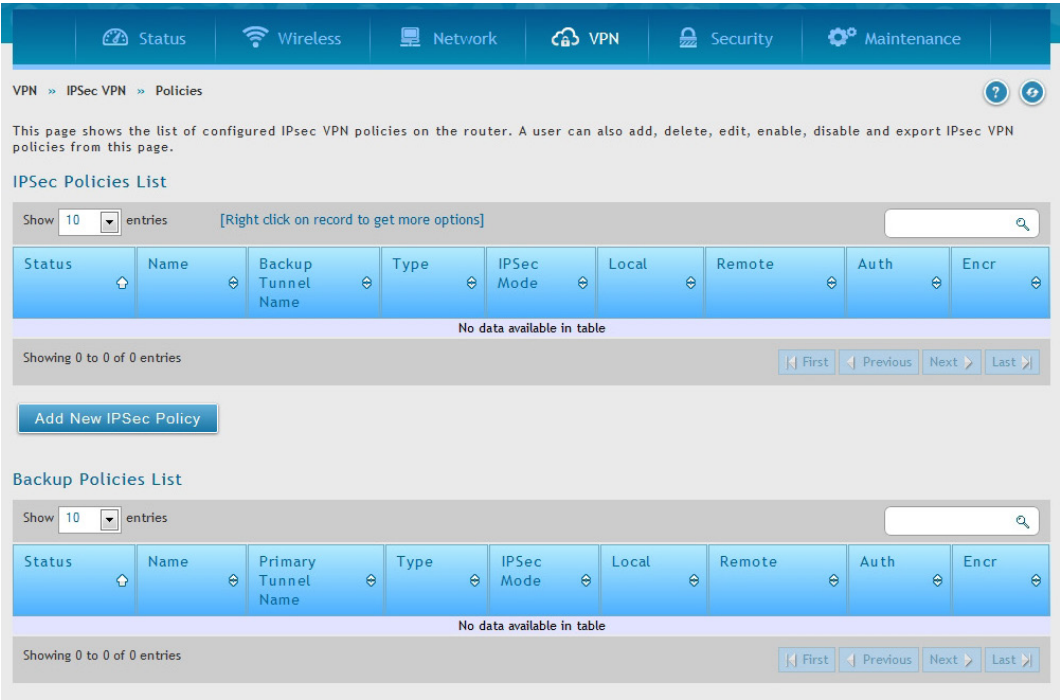


図 8-1 IPsec ポリシーリスト画面

Add New IPsec Policy (IPsec VPN ポリシーの追加)

1. 「Add New IPsec Policy」 ボタンをクリックし、以下の画面を表示します。「VPN 名」「ポリシータイプ」「トンネルタイプ」「エンドポイント」などを指定します。

IPsec Policy Configuration

General

Policy Name

Policy Type

Auto Policy

IP Protocol Version

IPv4

IKE Version

IKEv1

IPsec Mode

Tunnel Mode

Select Local Gateway

WAN1

Remote Endpoint

IP Address

IP Address / FQDN

Enable Mode Config

OFF

Enable NetBIOS

OFF

Enable RollOver

OFF

Protocol

ESP

Enable DHCP

OFF

Local IP

Subnet

Local Start IP Address

Local Subnet Mask

Remote IP

Subnet

Remote Start IP Address

Remote Subnet Mask

Enable Keepalive

OFF

図 8-2 IPsec ポリシー設定

2. 以下の項目を設定します。

項目	説明
Policy Name	VPN ポリシー名を入力します。これはリモート WAN/ クライアントの識別名とはなりません。

項目	説明
Policy Type	<p>VPAN ポリシーの種類を「Manual」「Auto」から指定します。</p> <ul style="list-style-type: none"> Manual - キーなども含め VPN トンネルにすべての設定を各エンドポイントに手動で行います。第三者機関サーバーや組織などは含まれません。 Auto - VPN トンネルのいくつかのパラメータは自動的に生成されます。これには二つの VPN エンドポイント間での IKE プロトコルを使用した交渉が必要になります。
IP Protocol Version	IP バージョン (IPv4 または IPv6) を選択します。
IKE Version	IKE バージョン (IKEv1 または IKEv2) を選択します。
IPSec Mode	<p>IPSec モードを「Tunnel」「Transport」から指定します。</p> <p>IPsec トンネルモードは信頼性の低いネットワークを通過するトラフィックを保護する際に有効です。トンネルモードは特に「L2TP/IPsec」「PPTP」接続などをサポートしていないゲートウェイやエンドシステムなどの相互運用に使用されます。「トランスポートモード」は IPsec の通常モードです。エンド間の通信に使用されます。(例; クライアント / サーバ間など)</p>
Select Local Gateway	IPsec トンネルのためのローカルゲートウェイを決定します。1 つ以上の設定済み WAN がある場合、トンネルはゲートウェイのいずれかに対して設定されます。
Remote Endpoint	FQDN または IP アドレスによってトンネルのリモートエンドポイントを識別します。
IP Address / FQDN	接続を試みるピアがゲートウェイである場合にだけ、本欄は有効にされます。VPN クライアントでは、クライアントから接続要求を受信する場合に、この IP アドレスまたはインターネット名が決定されます。
Enable Mode Config	<p>「ON」で「Mode Config」を有効にします。</p> <p>「Mode Config」はリモートの VPN クライアントに IP アドレスをアサインする機能で、DHCP に似ています。</p>
Enable NetBIOS	「ON」で「NetBIOS」ブロードキャストによる VPN トンネルの通過を許可します。
Enable RollOver	「ON」で VPN ロールオーバーを有効にします。WAN モードが「Rollover」に指定されます。
Protocol	プロトコルを選択します。
Enable DHCP	「ON」で DHCP を使用して IPsec 経由での VPN クライアントへの IP アドレス付与を有効にします。
Remote IP / Local IP	<p>エンドポイント用の識別の種類を指定します。</p> <ul style="list-style-type: none"> Any - エンドポイントからのトラフィック用のポリシー (ローカル / リモート) を指定します。「ローカル」「リモート」どちらも有効にすることはできません。 Single - 1 ホストのみに限定します。入力したホストの IP アドレスが VPN の一部とされます。 Range - VPN に接続する IP アドレスの範囲の端末に許可します。開始 IP アドレスと終了 IP アドレスを表示される項目に入力します。 Subnet - VPN に接続するすべてのサブネットを許可します。ネットワークアドレスとサブネットを表示される項目に入力します。
Enable Keepalive	「ON」にしてトンネルを有効にするためネットワークのピアサイドに定期的に Ping を送信します。

3. トンネルタイプとトンネルのエンドポイントが定義されると、トンネルに使用するフェーズ 1/ フェーズ 2 のネゴシエーションを決定できます。ポリシーは、「Manual Policy」（手動ポリシー）または「Auto Policy」（自動ポリシー）とすることができるため、IPSec モード設定でこれに対応します。「Auto Policy」ポリシーでは、IKE（Internet Key Exchange）プロトコルは 2 つの IPSec ホスト間でダイナミックに鍵交換を行います。フェーズ 1 の IKE パラメータは、トンネルのセキュリティ関係の詳細を定義するのに使用されます。フェーズ 2 の「Auto Policy Parameters」セクションはフェーズ 2 のキーネゴシエーションに関するセキュリティ関係のライフタイムと暗号化/認証の詳細に対応しています。VPN ポリシーは、自動 IPSec VPN トンネルを確立するのに必要とされる IKE/VPN ポリシーのペアの片方です。2 つの VPN エンドポイントにあるマシンの IP アドレスは、トンネルをセキュアにするために必要とされるポリシーパラメータと共にここで設定されます。

The screenshot displays the configuration interface for an IPSec policy, divided into two main sections: Phase 1 (IKE SA Parameters) and Phase 2 (Auto Policy Parameters).

Phase 1 (IKE SA Parameters):

- Exchange Mode:** Main
- Direction / Type:** Both
- Nat Traversal:** ON
- Local Identifier Type:** Local Wan IP
- Remote Identifier Type:** Remote Wan IP
- Encryption Algorithm:**
 - DES: OFF
 - AES-128: ON
 - AES-256: OFF
 - BLOWFISH: OFF
 - CAST128: OFF
 - 3DES: OFF
 - AES-192: OFF
- Authentication Algorithm:**
 - MD5: OFF
 - SHA2-256: OFF
 - SHA2-512: OFF
 - SHA-1: ON
 - SHA2-384: OFF
- Authentication Method:** Pre-Shared Key
- Pre-Shared Key:** [Empty field] [Length: 8 - 49]
- Diffie-Hellman (DH) Group:** Group 2 (1024 bit)
- SA-Lifetime:** 28800 [Default: 28800, Range: 300 - 2147483647] Seconds
- Enable Dead Peer Detection:** OFF
- Extended Authentication:** None

Phase 2 (Auto Policy Parameters):

- SA Lifetime:** 3600 Seconds
- Encryption Algorithm:**
 - DES: OFF
 - 3DES: OFF
 - AES-192: OFF
 - AES-CCM: OFF
 - TWOFISH (128): OFF
 - TWOFISH (256): OFF
 - BLOWFISH: OFF
 - CAST128: OFF
 - NONE: OFF
 - AES-128: ON
 - AES-256: OFF
 - AES-GCM: OFF
 - TWOFISH (192): OFF
- Integrity Algorithm:**
 - MD5: OFF
 - SHA2-224: OFF
 - SHA2-384: OFF
 - PFS Key Group: OFF
 - SHA-1: ON
 - SHA2-256: OFF
 - SHA2-512: OFF

A **Save** button is located at the bottom right of the configuration area.

図 8-3 IPSec ポリシー設定 (IKE を経由した自動ポリシー)

「Manual Policy」は、代わりに 2 つの IPSec ホスト間で認証パラメータを交換するために、IKE を使用しないで、代わりに手動のキー操作に依存します。リモートトンネルのエンドポイントで入出力する SPI (security parameter index) 値を反映する必要があります。また、トンネルの確立に成功するためには、暗号化、保全アルゴリズム、およびキーはリモート IPSec ホストに一致する必要があります。SPI (security parameter index) 値を各エンドポイントで変換する必要があるいくつかの IPSec の実行において IKE 経由をした「Auto Policy」を使用することが望ましいことに注意してください。

DWC-1000 は VPN ロールオーバー機能をサポートしています。これは、プライマリ WAN に設定されたポリシーがプライマリ WAN におけるリンク障害の場合にセカンダリ WAN にロールオーバーすることを意味します。WAN が「Auto-Rollover」モードに設定されている場合にだけ、本機能を使用することができます。

4. 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。

Tunnel Mode（トンネルモード）

VPN > IPSec VPN > Tunnel Mode

トンネルモードを選択した場合、NetBIOS および DHCP over IPSec を有効にすることができます。DHCP over IPSec によりこのコントローラはリモート LAN のホストに IP リースをサービスすることができます。また、このモードでは、1 つの IP アドレス、IP アドレス範囲、またはトンネル上で通信できるローカルおよびリモート両方のプライベートネットワークにおけるサブネットを定義できます。

本コントローラは「Full Tunnel」（フルトンネル）と「Split Tunnel」（スプリットトンネル）のサポートを許可します。「Full Tunnel」モードは VPN トンネル中のクライアントからコントローラにすべてのトラフィックを送信します。「Split Tunnel」モードは事前に指定したクライアントのルートに基づいてプライベート LAN にトラフィックを送信します。

Tunnel Mode（トンネルモード）

1. VPN > IPSec VPN > Tunnel 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。

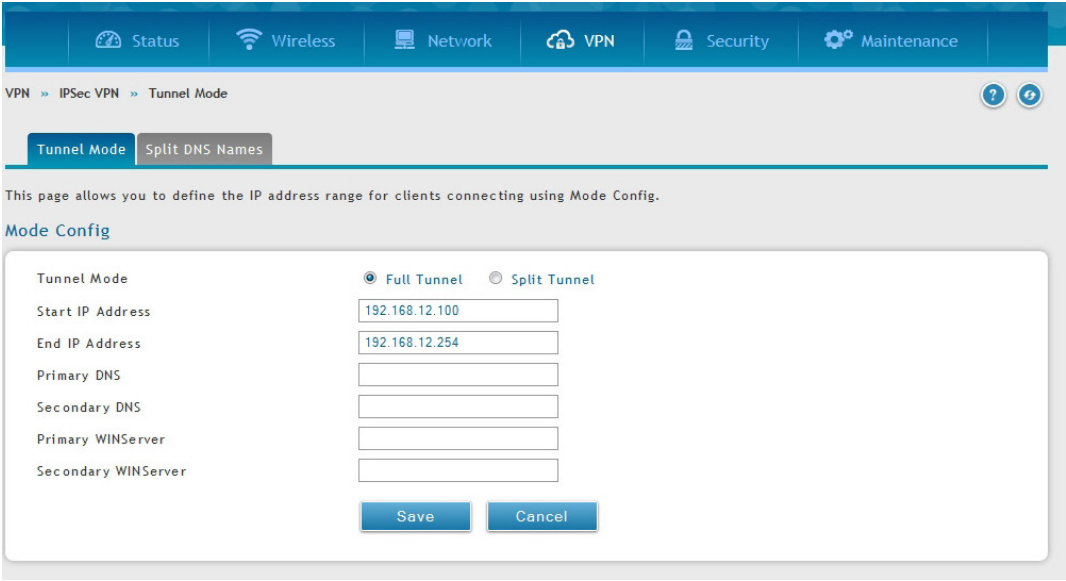


図 8-4 Tunnel Mode タブ

2. 以下の項目を設定します。

項目	説明
Tunnel Mode タブ	
Tunnel Mode	「Full Tunnel」（フルトンネル）または「Split Tunnel」（スプリットトンネル）。フルトンネルでは、すべてのパケット（インターネットまたはリモートサーバに向かう）が、スプリットトンネルのようなインターネットに向かうトラフィックを通過させないトンネルも通過します。
Start IP Address	このプールに割り当てられるべき最初のアドレス。
End IP Address	このプールに割り当てられるべき最後のアドレス。
Primary /Secondary DNS	プライマリ / セカンダリ DNS サーバは、ドメイン名を解決するためにこのコントローラに接続するクライアントに使用されます。トンネルモードがスプリットトンネルである場合、DNS サーバを内部のドメイン名サーバとするする必要があります。
Primary/Secondary WINS Server	プライマリ / セカンダリの WINS サーバを指定します。

「Save」をクリックし、設定を適用します。

Split DNS Names（スプリット DNS 名）

このデバイスに接続するクライアントは、ダイナミック IP 範囲ページで提供する DNS を使用して、このドメイン名を解決します。これはスプリットトンネルでのみ適用されます。

1. VPN > IPsec VPN > Tunnel Mode > Split DNS 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。

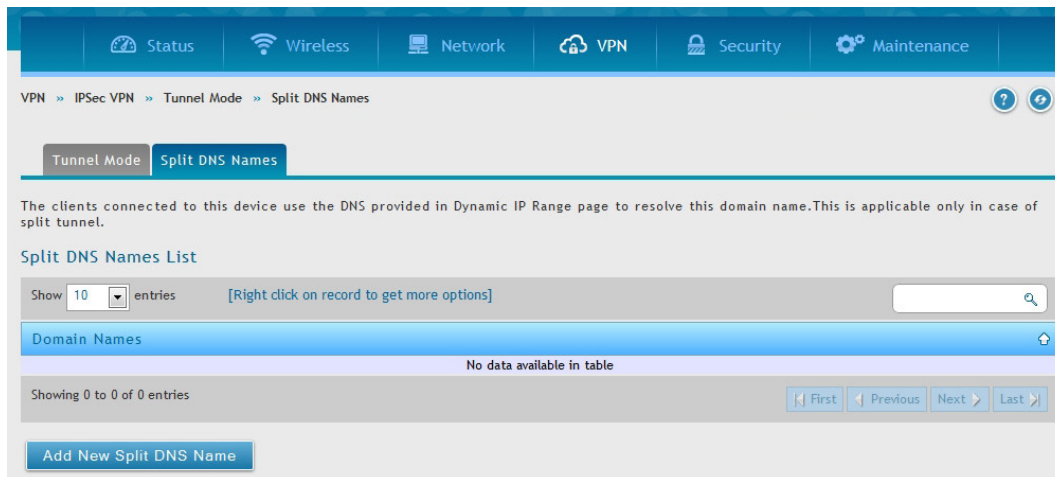


図 8-5 Split DNS Names 設定

2. 「Split DNS Names」タブの「Add New Split DNS name」ボタンをクリックして以下の画面を表示します。

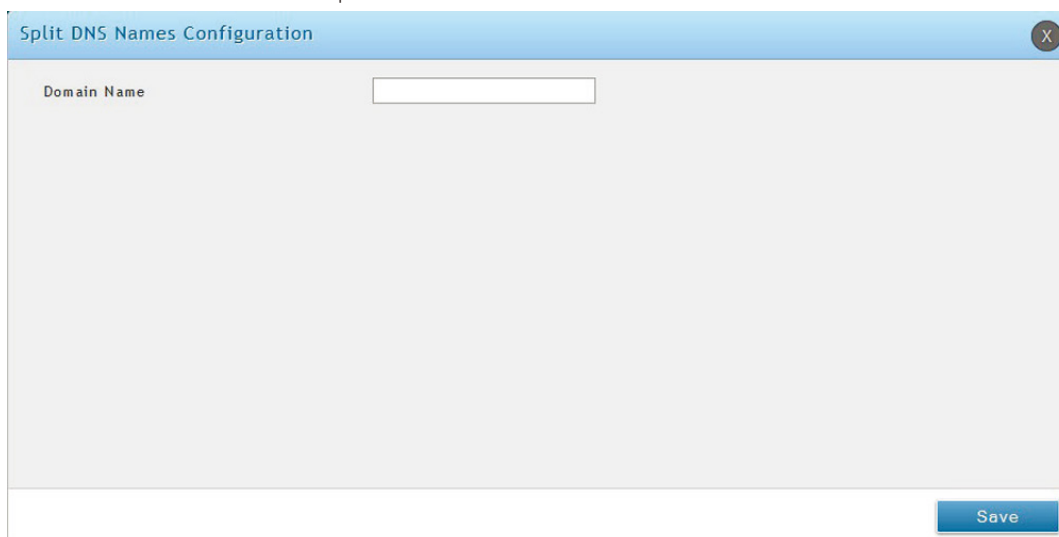


図 8-6 Add New Split DNS name

3. 「Domain Name」にドメイン名を入力します。
4. 「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。

DHCP Range (IP アドレス範囲の設定)

VPN > IPsec VPN > DHCP Range

DHCP over IPsec を使用して接続するクライアント用の IP アドレス範囲を定義します。

1. VPN > IPsec VPN > DHCP Range の順にメニューをクリックし、以下の画面を表示します。

The screenshot shows a web-based configuration interface for a VPN. At the top, there is a navigation bar with tabs: Status, Wireless, Network, VPN, Security, and Maintenance. Below this, the breadcrumb path is 'VPN > IPsec VPN > DHCP Range'. A note states: 'This page allows you to define the IP address range for clients connecting using DHCP over IPsec. Note: To support DHCP over IPsec, enable DHCP server on the LAN.' The main section is titled 'DHCP Range' and contains three input fields: 'Starting IP Address' with the value '192.168.12.100', 'Ending IP Address' with the value '192.168.12.254', and 'Subnet Mask' with the value '255.255.255.0'. At the bottom of this section are two buttons: 'Save' and 'Cancel'.

図 8-7 DHCP Range 設定

2. 「Starting IP Address」および「Ending IP Address」に IP 範囲の開始および終了アドレスを入力し、「Subnet Mask」にサブネットマスクを指定します。
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。

Certificate（認証証明書）

VPN > IPSec VPN > Certificate

本コントローラは IPSec VPN 認証にデジタル証明書を使用します。VeriSign（ベリサイン）などのよく知られている認証局（CA）からデジタル証明書を入手するか、または、利用可能な機能を使用してあなた自身の証明書を生成および署名することができます。

本コントローラには self-signed certificate（自己署名証明書）があり、ご使用のネットワーク要件に応じて認証局によって署名されたものと交換することができます。CA 証明書がサーバのアイデンティティに関する強力な保証を提供しており、多くの企業ネットワーク VPN ソリューションの必要条件となっています。

Trusted Certificates（トラスト証明書）

VPN > IPSec VPN > Certificate > Trusted Certificates

証明書メニューでは、現在コントローラにロードされている証明書（CA および自己署名の両方）のリストを参照することができます。トラスト（CA）証明書のリストには以下の証明書データが表示されます。

項目	説明
CA Identity（サブジェクト名）	人または組織に証明書を発行します。
Issuer Name（発行者）	この証明書を発行した CA 名です。
Expiry Time（期限）	このトラスト証明書が無効になる日付。

1. VPN > IPSec VPN > Certificate > 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。

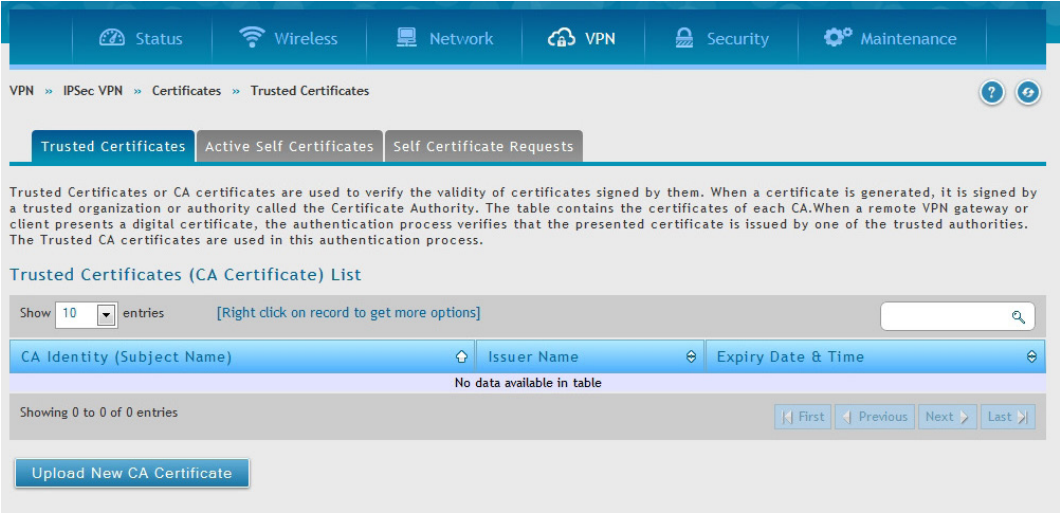


図 8-8 Trusted Certificates 画面

2. 「Upload New Certificate」をクリックします。
3. 表示された以下の画面で「Browse」（参照）をクリック、証明書の場所を指定し「Upload」をクリックします。

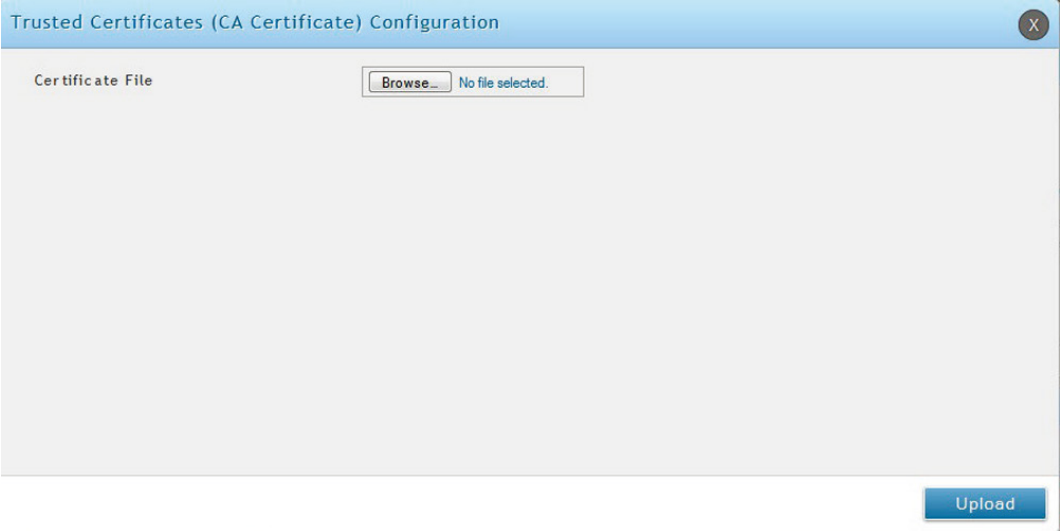


図 8-9 Trusted Certificates - Upload

Active Self Certificates（自己証明書）

VPN > IPsec VPN > Certificate > Active Self Certificates

自己証明書は、ご使用のデバイスを確認する CA によって発行された証明書です（または、CA のアイデンティティ保護が必要ない場合には自己署名証明書）。Active Self Certificate タブでは、現在コントローラにロードされている自己証明書を表示します。各アップロードされている自己証明書に対して以下の情報が表示されます。

項目	説明
Name（名称）	この証明書を特定するのに使用する名前であり、IPsec VPN ピアまたは SSL ユーザには表示されません。
Subject Name（サブジェクト名）	この証明書の所有者として表示される名前です。IPsec または SSL VPN ピアが本欄に表示されるため、これは公式に登録されるか会社名であるべきです。
Serial Number（シリアル番号）	シリアル番号は CA によって保持され、この署名された証明書を特定するために使用されます。
Issuer Name（発行者）	この証明書を発行した（署名した）CA 名です。
Expiry Time（期限）	署名証明書が無効になる日付。期限が切れる前に証明書を更新する必要があります。

1. VPN > IPsec VPN > Certificate > 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。

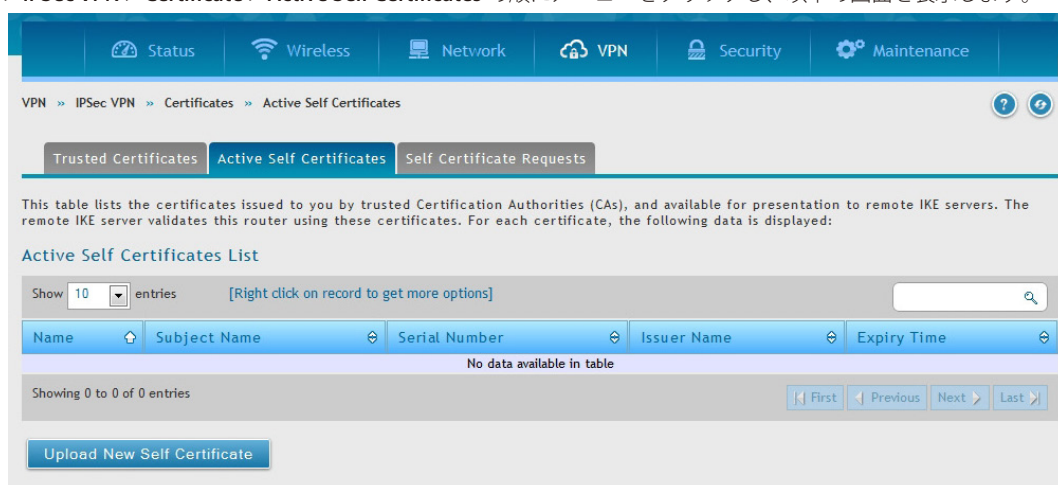


図 8-10 Active Self Certificates 画面

2. 「Upload New Self Certificate」をクリックします。
3. 表示された以下の画面で「Browse」（参照）をクリック、自己証明書の場所を指定し「Upload」をクリックします。

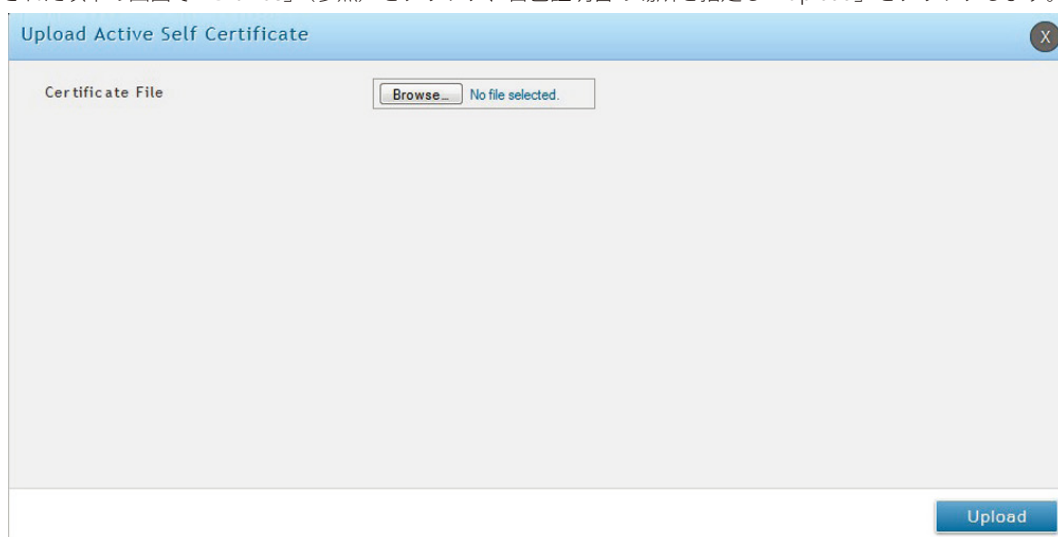


図 8-11 Active Self Certificates - Upload 画面

Self Certificate Requests（自己証明書リクエスト）

VPN > IPSec VPN > Certificate > Self Certificates Requests

自己証明書に CA が署名するようにリクエストするためには、識別子パラメータの入力をすることによって、コントローラから証明書署名要求（CSR）を生成することができます。そして、署名のためにそれを CA に渡します。署名されると、CA からのトラスト証明書と署名証明書がアップロードされ、ゲートウェイのアイデンティティを有効にする自己証明書をアクティベートすることができます。自己証明書は、ゲートウェイの真正性を有効にするのにピアとの IPSec および SSL 接続に使用されます。

1. VPN > IPSec VPN > Certificate > 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。

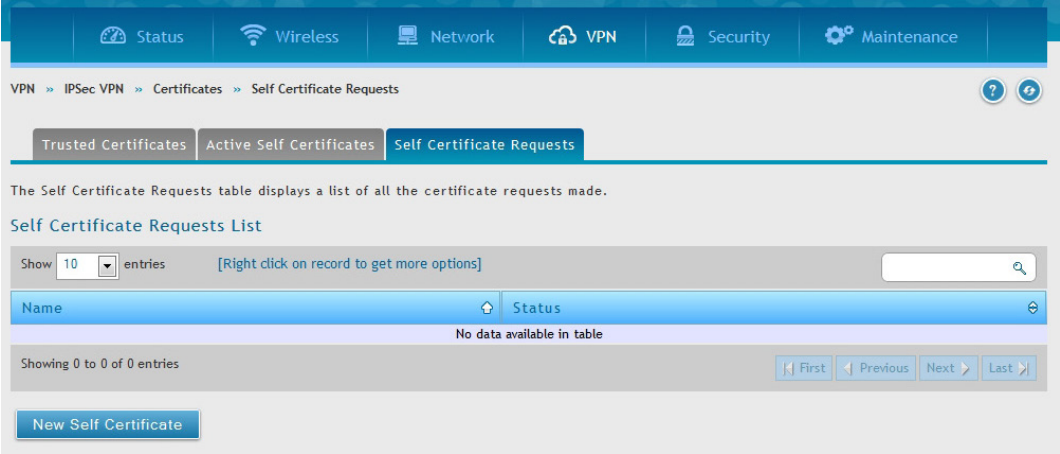


図 8-12 Self Certificate Requests 画面

- 2. 「New Self Certificate」をクリックします。
- 3. 表示された以下の画面を入力します。

Generate Self Certificate Request

Name

Subject

Hash AlgorithmMD5

Signature Key Length512

Application TypeHttps

IP Address

Domain Name

Email Address

Save

図 8-13 Self Certificate Requests - New Self Certificate 画面

項目	説明
Name	自己証明書の名前を入力します。
Subject	証明書エントリの CN (Common Name/ 通常名) を生成させます。サブジェクト名は通常次のフォーマットによって定義されます。CN=<device name/ デバイス名>, OU=<department/ 部署>, O=<organization/ 組織>, L=<city/ 市町>, ST=<state/ 県、州>, C=<country/ 国>。(例: CN=router1, OU=my_company, O=mydept, L=SFO, C=US.)
Hash Algorithm	アルゴリズムを指定します。「MD5」「SHA-1」から指定します。
Signature Key Length	シグニチャキーの長さを指定します。「512」「1024」「2048」から選択します。
Application Type	アプリケーションの種類を指定します。「HTTPS」「IPSec」から選択します。
IP Address	IP アドレスを入力します。(オプション)
Domain Name	ドメイン名を入力します。(オプション)
Email Address	メールアドレスを入力します。

「Save」をクリックし、設定を適用します。

Easy VPN Setup (VPN セットアップ)

VPN > IPSec VPN > Easy VPN Setup

エクスポートされた IPSec VPN ポリシーをアップロードします。

1. VPN > IPSec VPN > Easy VPN Setup の順にメニューをクリックします。
2. 表示された以下の画面で「Browse」（参照）をクリック、ポリシーの場所を指定し「Upload」をクリックします。

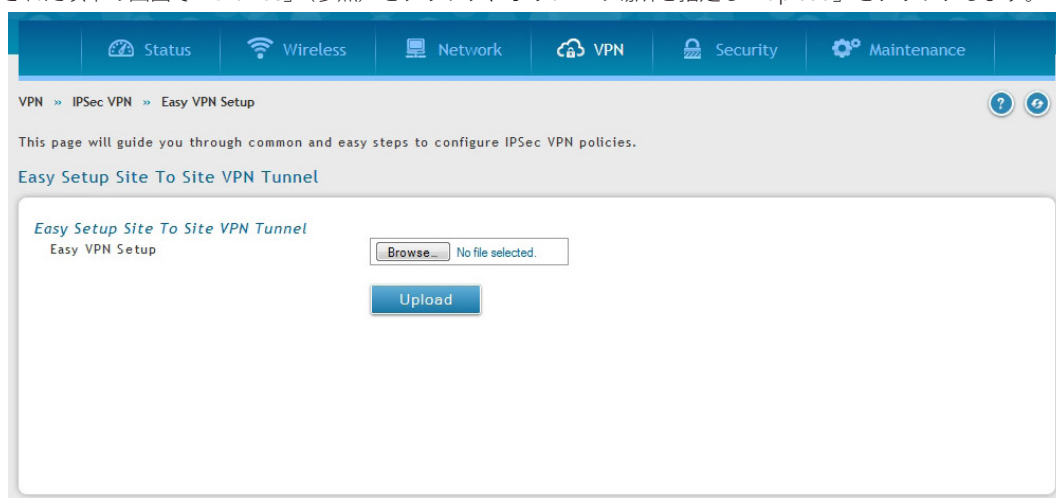


図 8-14 Easy VPN Setup 画面

3. 一度アップロードされると「VPN > IPSec VPN > Policies」でロードされた VPN としてリストされます。右クリックで「Edit」「Delete」などを行ってください。

PPTP VPN（PPTP VPN 設定）

VPN > PPTP VPN

このコントローラは PPTP サーバから開始する VPN トンネルをサポートしています。コントローラは、ISP のサーバが LAN VPN クライアントと VPN サーバ間の TCP 制御接続を作成できる仲介デバイスとして機能します。

Server（PPTP VPN サーバ設定）

VPN > PPTP VPN > Server

ここでは、PPTP サーバの有効化 / 無効化、およびコントローラに接続するクライアントの IP アドレスの範囲を定義することができます。PPTP によりインターネットを通して外部ユーザがこのコントローラに接続することができます。接続するクライアントは、LAN ホストと通信し、どんなサーバにもアクセスするなどご使用の LAN にいるかのように動作することができます。

PPTP サーバを有効にすると LAN および WAN PPTP クライアントユーザがアクセスするコントローラで利用可能になります。さらに、許可されたクライアントの設定済み IP アドレス範囲内にある PPTP クライアントは、コントローラの PPTP サーバに到達することができます。PPTP サーバ（トンネルのエンドポイント）によって一度認証されると、PPTP クライアントはコントローラが管理するネットワークにアクセスすることができます。

PPTP クライアントに割り当てる IP アドレス範囲は LAN サブネットと同じにできます。また、PPTP サーバは、ローカルな PPTP ユーザ認証をデフォルトとしますが、外部認証サーバを使用するように設定できます。

1. VPN > PPTP VPN > 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。

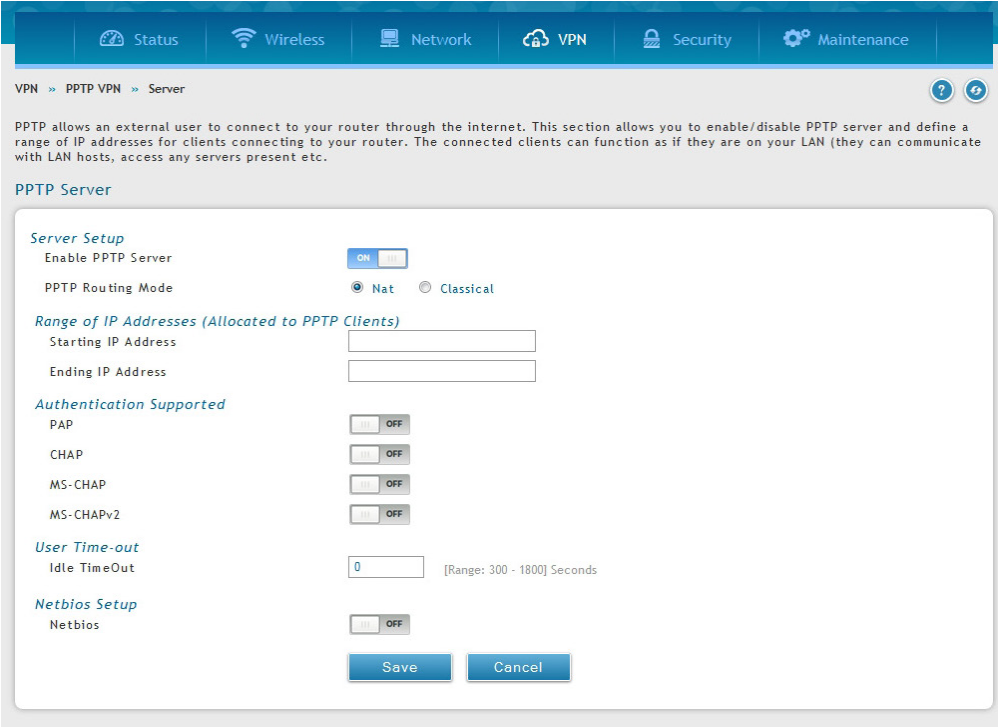


図 8-15 PPTP サーバ設定

2. 以下の項目を設定します。

項目	説明
Enable PPTP Server	PPTP サーバを有効にします。
PPTP Routing Mode	PPTP ルーティングモード (NAT/Classical) から選択します。
Starting IP Address	接続するユーザに割り当てるべき IP アドレス範囲の開始の IP アドレスを入力します。この IP アドレスはサーバの IP アドレスとして使用され、範囲内の残りの IP アドレスはクライアントに割り当てられます。
Ending IP Address	接続するユーザに割り当てるべき IP アドレス範囲の終了の IP アドレスを入力します。
PAP	PAP 認証方式のサポートを有効にします。
CHAP	CHAP 認証方式のサポートを有効にします。
MS-CHAP	MS-CHAP 認証方式のサポートを有効にします。
MS-CHAPv2	MS-CHAPv2 認証方式のサポートを有効にします。
Idle Timeout	指定したタイムアウトを経過してもユーザからのトラフィックがない場合、接続は切断されます。
Netbios	Netbios サポートを有効にします。

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。

Client (PPTP クライアント)

VPN > PPTP VPN > Client

本コントローラに PPTP VPN クライアントを設定します。クライアントが有効になると、ユーザは、**Status > Active VPNs** ページにアクセスし、「Connect」ボタンをクリックして PPTP VPN トンネルを確立します。

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

VPN > PPTP VPN > Client

PPTP VPN Client can be configured on this router. Using this client we can access remote network which is local to PPTP server.

PPTP Client

Client ☒ ON

Server IP

Remote Network

Remote Netmask [Range: 0 - 32]

Username

Password

MPPE Encryption ☐ OFF

Idle Time Out [Range: 300 - 1800] Seconds

図 8-16 PPTP クライアント設定

2. 以下の項目を設定します。

項目	説明
Client	PPTP クライアントを有効にします。
Server IP	接続する PPTP サーバの IP アドレスを指定します。
Remote Network	PPTP サーバにとってローカルとなるリモートネットワークアドレスを指定します。
Remote Netmask	リモートネットワークマスクを指定します。
Username	PPTP ユーザ名を指定します。
Password	PPTP パスワードを指定します。
MPPE Encryption	「ON」にして Microsoft Point-to-Point Encryption (MPPE) を有効にします。
Idle Time Out	アイドル状態時に PPTP サーバから切断するまでの時間を指定します。(秒)

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。

PPTP Active Users List (PPTP アクティブユーザリスト)

PPTP の接続状況について表示します。接続ユーザで右クリックをし「Connect/ 接続」「Disconnect/ 切断」を選択します。

VPN > PPTP VPN > Active Users

Active PPTP tunnels connections are listed here, as LAN VPN clients are active PPTP users.

PPTP Active Users List

Show entries [No right click options]

User Name	Remote IP	PPTP IP
No data available in table		

Showing 0 to 0 of 0 entries

図 8-17 PPTP Active Users List

L2TP VPN（L2TP VPN 設定）

VPN > L2TP VPN

このコントローラは L2TP サーバから開始する VPN トンネルをサポートしています。ISP のサーバが LAN L2TP クライアントと VPN サーバ間の TCP 制御接続を作成できる仲介デバイスとして機能します。

Server（L2TP VPN サーバ設定）

VPN > L2TP VPN > Server

ここでは L2TP サーバの有効化 / 無効化、およびコントローラに接続するクライアントの IP アドレスの範囲を定義することができます。このコントローラを通して L2TP VPN を確立することができます。有効にされると、L2TP サーバは LAN および WAN L2TP クライアントユーザがアクセスするコントローラで利用可能になります。一度、L2TP サーバが有効になると、リモートの L2TP ネットワークサーバ範囲 (IP アドレスおよびネットマスク) で設定される L2TP クライアントは、エンドポイントコントローラの L2TP サーバに到達することができます。L2TP サーバ (トンネルのエンドポイント) によって一度認証されると、L2TP クライアントはコントローラが管理するローカルネットワークにアクセスすることができます。

1. VPN > L2TP VPN > 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。

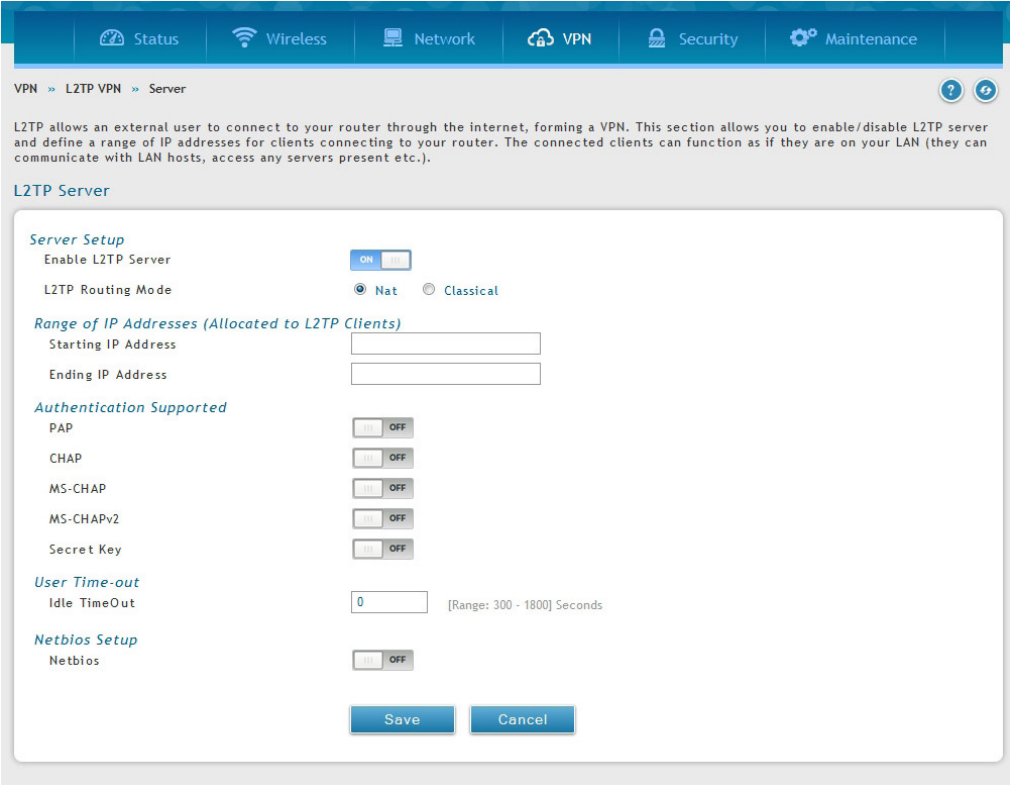


図 8-18 L2TP トンネル設定 - L2TP サーバ

2. 以下の項目を設定します。

項目	説明
Enable L2TP Server	L2TP モードを有効にします。
L2TP Routing Mode	L2TP ルーティングモードを選択します。「NAT」「Classical」
Starting IP Address	接続するユーザに割り当てる IP アドレス範囲の開始 IP アドレスを入力します。
Ending IP Address	接続するユーザに割り当てる IP アドレス範囲の終了 IP アドレスを入力します。
PAP	PAP 認証方式のサポートを有効にします。
CHAP	CHAP 認証方式のサポートを有効にします。
MS-CHAP	MS-CHAP 認証方式のサポートを有効にします。
MS-CHAPv2	MS-CHAPv2 認証方式のサポートを有効にします。
Idle Timeout	指定したタイムアウトを経過してもユーザからのトラフィックがない場合、接続は切断されます。
Netbios	Netbios サポートを有効にします。

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。

L2TP Active Users List（L2TP アクティブユーザリスト）

PPTP の接続状況について表示します。接続ユーザで右クリックをし「Connect/ 接続」「Disconnect/ 切断」を選択します。

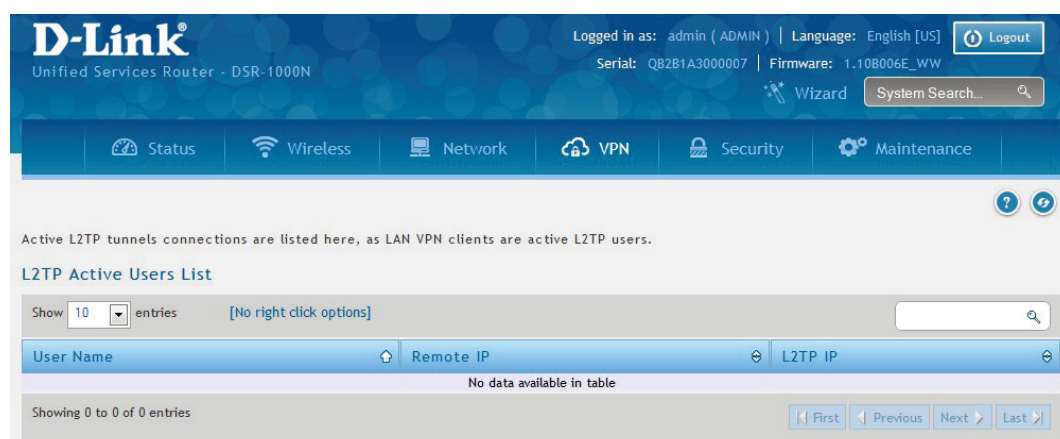


図 8-19 L2TP Active Users List

SSL VPN（SSL VPN 設定）

VPN > SSL VPN

SSL VPN ポリシーはグローバル、グループまたはユーザレベルで作成されます。ユーザレベルポリシーはグループレベルポリシーより優先され、グループレベルポリシーはグローバルポリシーより優先されます。これらのポリシーは、LAN の特定のネットワークリソース、IP アドレスまたは範囲に、または、コントローラによってサポートされる様々な SSL VPN サービスに適用できます。利用可能なポリシーのリストは、ユーザ、グループ、またはすべてのユーザ（グローバル）に適用するかどうかに基づいてフィルタされます。

最初にユーザ、グループ、またはグローバル（つまり、すべての SSL VPN ユーザに適用する）に割り当てする必要があります。ポリシーがグループ用であれば、利用可能な設定グループは、プルダウンメニューに表示され、1 つを選択する必要があります。同様に、ユーザ定義ポリシーには、設定済みユーザの使用可能リストから SSL VPN ユーザを選択する必要があります。

次に、ポリシーの詳細を定義します。ポリシー名はこのルールに固有の識別子です。コントローラの LAN における特定のネットワークリソース（詳細は続くセクションに記述）、IP アドレス、IP ネットワーク、またはすべてのデバイスにポリシーを割り当てることができます。これら 4 つのオプションの 1 つの選択に基づいて、適切な設定欄が必要となります。（つまり、定義済みリソースのリストから行うネットワークリソースの選択、または IP アドレスの定義）。ポリシーをアドレスに適用するために、ポート範囲 / ポート番号を定義できます。

最後の手順では選択したアドレスまたはネットワークリソースへのアクセスを許可、または拒否するように設定するポリシーの許可が必要とされます。また、サポートしている SSL VPN サービス（VPN トンネル）のうち 1 つまたはすべてにポリシーを指定できます。

一度定義すると、ポリシーは直ちに実行されます。ポリシー名、適用する SSL サービス、送信先（ネットワークリソースまたは IP アドレス）、許可（許可 / 拒否）はコントローラに設定されたポリシーのリストに概説されています。

注意 「Remote Management」でリモート管理を有効にする必要があります。

SSL VPN Server Policy（SSL VPN ポリシー設定）

VPN > SSL VPN > SSL VPN Server Policy メニュー

SSL VPN ポリシーを設定します。

注意 SSL VPN ポリシーの作成には「Remote Management」（リモート管理）を有効にしている事、ポリシーを適用するユーザまたはグループを作成済みである必要があります。

1. VPN > SSL VPN > SSL VPN Server 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。

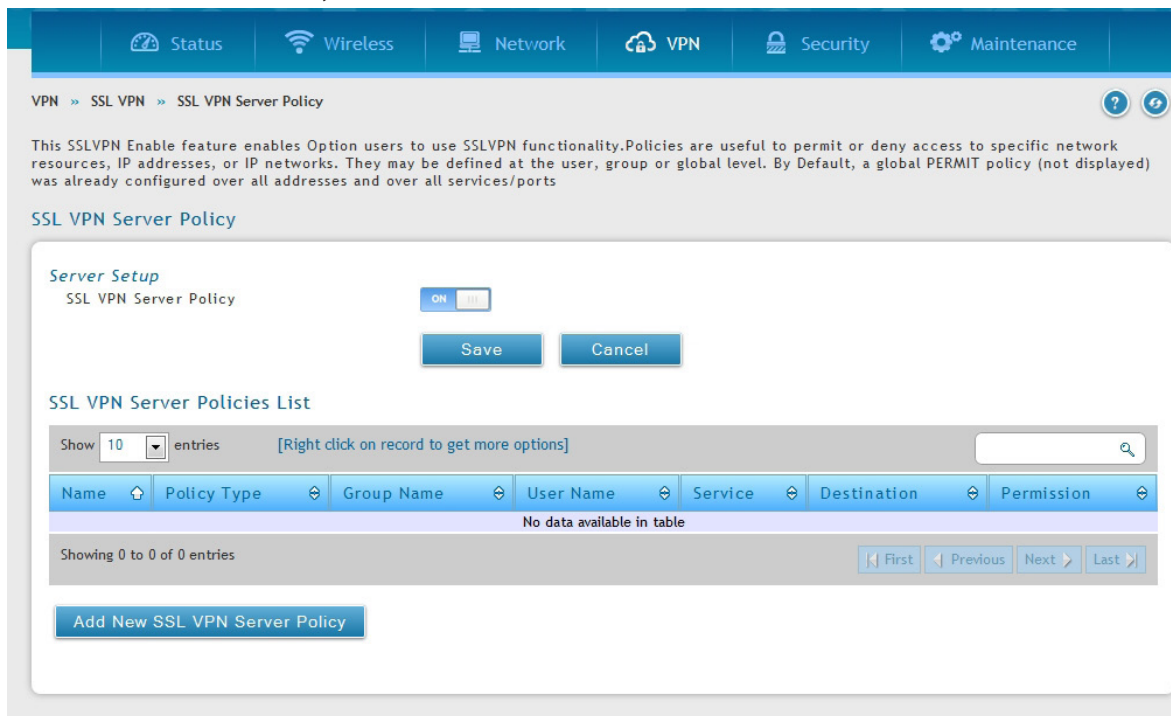


図 8-20 SSL VPN ポリシーのリスト

2. 「SSL VPN Server Policy」を「ON」にして「Save」をクリックします。

SSL VPN ポリシーの追加

- 「Add New SSL VPN Server Policy」ボタンをクリックして、以下の画面を表示します。

図 8-21 SSL VPN ポリシーの追加 (Network Resource)

図 8-22 SSL VPN ポリシーの追加 (IP Address)

- 以下の項目を設定します。

項目	説明
Policy Type	ユーザ (User)、ユーザグループ (Group)、またはすべてのユーザ (Global) にポリシーを割り当てます。
SSL VPN Policy	
Apply Policy to	ポリシーをネットワークリソース (Network Resource)、IP アドレス (IPAddress)、IP ネットワーク (IP Network)、全アドレス (All Addresses) のアサインします。
Policy Name	ポリシーを識別名を指定します。
IP Address	アサインされたポリシーが IP アドレス (IPAddress)、IP ネットワーク (IP Network) の場合に IP アドレスを入力します。
Mask Length	アサインされたポリシーが IP ネットワーク (IP Network) の場合にマスク長を入力します。
ICMP	「ON」にし ICMP トラフィックを有効にします。
Port Range / Port Number	
Begin / End	管理トラフィックに対応する TCP または UDP ポートの範囲を定義します。
Service	本ポリシーによって利用可能な SSL VPN サービスです。提供されるサービスは、VPN トンネル (VPN Tunnel)、ポートフォワーディング (Port Forwarding)、または両方 (All) です。
Defined Resources	このポリシーは特定のネットワークリソースへのアクセスを提供します。定義済みリソースとして選択できるようにポリシーを作成する前に、ネットワークリソースを設定する必要があります。ネットワークリソースは次のセクションで作成します。
Permission	このポリシーによって定義したリソースを許可 (Permit) または拒否 (Deny) に設定します。

- 「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。

ポータルレイアウトの作成

VPN > SSL VPN > Portal Layouts メニュー

ポータルレイアウトを作成します。
コントローラは、リモート VPN ユーザに対して認証時に提示されるカスタムページを作成することができます。ドメインのためにカスタマイズ可能なポータルには様々な欄があり、これにより、コントローラの管理者は、リモートユーザにポータルで目に見えるログインの手順、可能なサービス、およびその他利用の詳細などを通信することができます。

1. VPN > SSL VPN > Portal Layouts の順にメニューをクリックして、以下の画面を表示します。

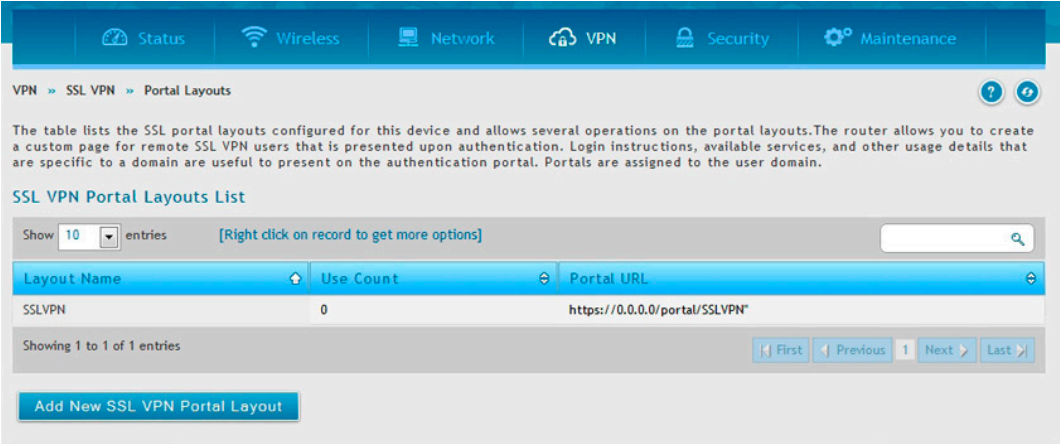


図 8-23 SSL VPN ポータルのリスト

2. レイアウトで右クリック、「Edit」「Delet」でレイアウトを削除、編集します。

ポータルレイアウトの作成

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

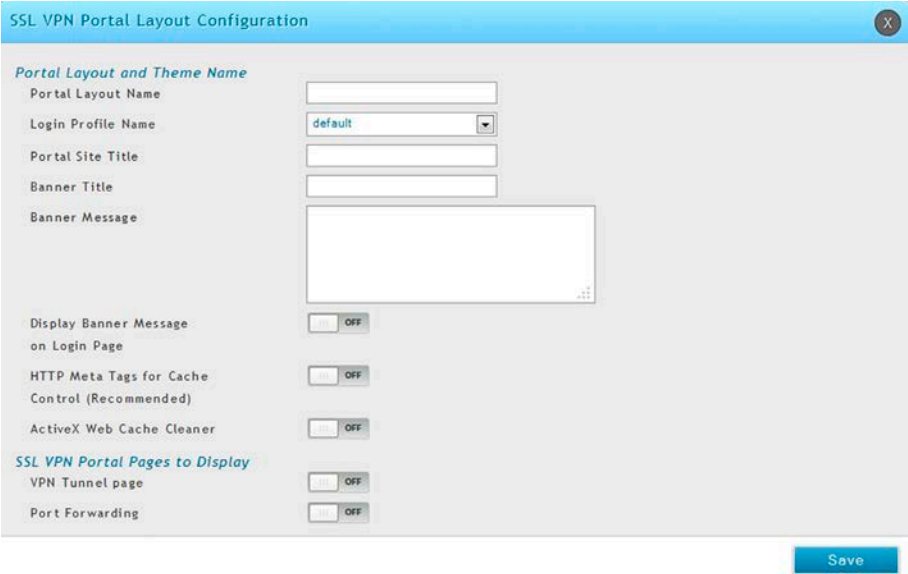


図 8-24 SSL VPN ポータル設定

注意 ポータル LAN の IP アドレスの初期値は [https://192.168.10.1/scgibin/ userPortal/portal](https://192.168.10.1/scgibin/userPortal/portal) です。これは、「User Portal」リンクがコントローラ GUI の SSL VPN メニューでクリックされると開くページと同じです。

2. 以下の項目を設定します。

項目	説明
Portal layout name	設定されているカスタムポータル名を入力します。
Login Profile Name	ログインプロファイル名を指定します。
Portal Site Title	クライアントがこのポータルにアクセスする場合に表示されるポータル Web ブラウザ画面のタイトルです。この項目はオプションです。
Banner Title	ログイン前に SSL VPN クライアントに表示されるバナータイトルです。この項目はオプションです。
Banner Message	ログイン前に SSL VPN クライアントに表示されるバナーメッセージです。この項目はオプションです。

項目	説明
Display Banner Message on Login Page	ログインページのバナーメッセージを表示（ON）または隠す（OFF）機能です。
HTTP Meta Tags for Cache Control	期限切れの Web ページとデータがクライアントの Web ブラウザキャッシュに保存されるのを防ぎます。「ON」を選択することをお勧めします。
ActiveX Web Cache Cleaner	ActiveX キャッシュ制御 Web クリーナ機能は、この SSL VPN ポータルにユーザがログインする時はいつも、ゲートウェイからクライアントのブラウザに対して実行されます。
VPN Tunnel Page	このポータルに表する SSL サービスに従って VPN トンネルのページを有効にすることができます。ポータル設定が行われると、新しく設定されたポータルは、ポータルレイアウトのリストに追加されます。
Port Forwarding	このポータルに表する SSL サービスに従ってポートフォワーディングを有効にすることができます。ポータル設定が行われると、新しく設定されたポータルは、ポータルレイアウトのリストに追加されます。

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。

ネットワークリソース

VPN > SSL VPN > Resources メニュー

ネットワークリソースの追加

SSL VPN ポリシーを設定する場合に使用するリソースを設定します。テーブルには登録されたリソースが表示され、そのリソースにいくつかの操作を許可します。ネットワークリソースは、SSL VPN ポリシーを簡単に作成および設定するのに使用される LAN IP アドレスのサービスまたはグループです。複数のリモート SSL VPN ユーザのために同様のポリシーを作成する場合、このショートカットが時間を節約します。

ネットワークリソースを追加する場合、リソースを識別する固有名を作成し、それにサポートする SSL サービスの 1 つまたはすべてを割り当てる必要があります。これが実行されると、作成済みのネットワークリソースの 1 つを編集することでサービスに関連しているオブジェクトタイプ（IP アドレスまたは IP 範囲のいずれか）を設定することができます。必要に応じてこのリソースにネットワークアドレス、マスク長、およびポート範囲/ポート番号を定義できます。

1. VPN > SSL VPN > Resources の順にメニューをクリックして、以下の画面を表示します。

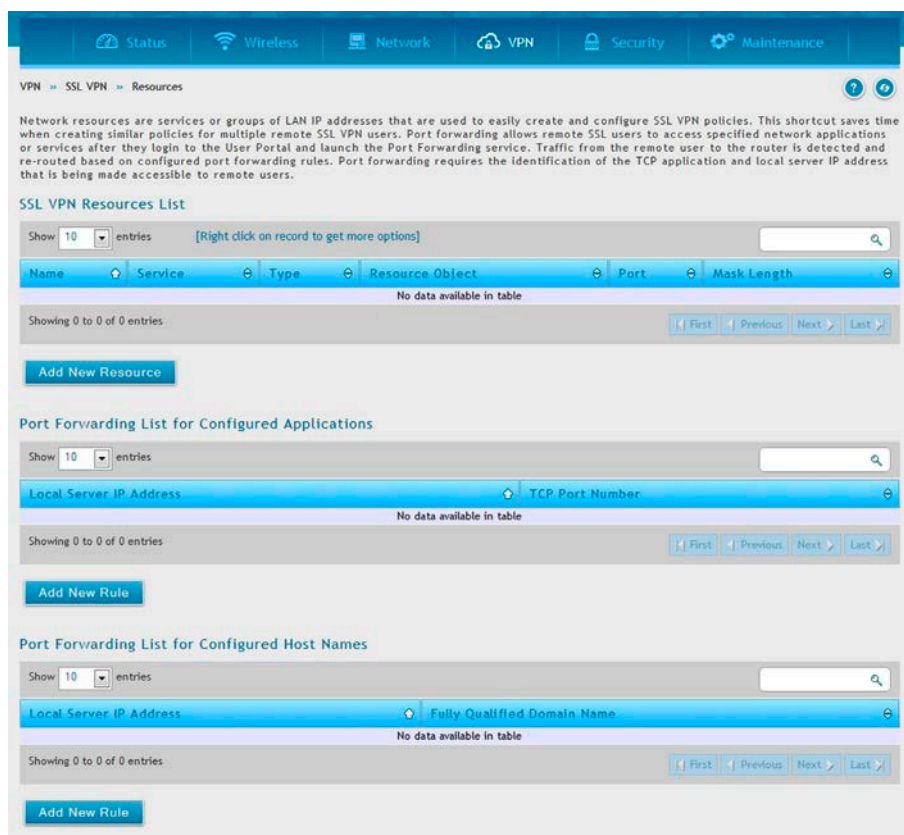


図 8-25 SSL VPN ポリシーに割り当てるために利用可能な設定済みリソースのリスト

リソースの追加

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

SSL VPN Resources Configuration

SSL VPN Resources

Resource Name

Service

VPN Tunnel

Port Forwarding

All

Resource Object Configuration

ICMP

OFF

Object Type

IP Address

Object Address

Port Range / Port Number

Begin

[Range: 0 - 65535]

End

[Range: 0 - 65535]

Save

図 8-26 リソースの設定画面

2. 以下の項目を設定します。

項目	説明
SSL VPN Resource	
Resource name	リソースの独自の識別名
Service	リソース（VPN Tunnel、Port Forwarding、または All） に対応する SSL VPN サービス。
Resource Object Configurariion	
ICMP	「ON」 にして ICMP トラフィックを有効にします。
Object Type	オブジェクトのタイプを「Single IP Address」「IP Network」 から選択します。
Object Address	IP アドレスを入力します。
Port Range / Port Number	
Begin / End	オブジェクトのポート範囲（開始 / 終了） を指定します。

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。

アプリケーションポートフォワーディング

ポートフォワーディング機能により、リモート SSL ユーザはユーザポータルにログインしてポートフォワーディングを起動した後に、特定のネットワークアプリケーションにアクセスできます。リモートユーザからコントローラまでのトラフィックは、設定済みのポートフォワーディングルールに基づいて検出されて、別ルートで送信されます。

内部のホストサーバまたは TCP アプリケーションをリモートユーザにアクセスをできるように指定する必要があります。LAN サーバへのアクセスを許可するためには、ローカルサーバの IP アドレスとトンネルされるアプリケーションの TCP ポート番号の入力が必要です。以下の表では一般的なアプリケーションと対応する TCP ポート番号を示しています。:

1. VPN > SSL VPN > Resources の順にメニューをクリックして、以下の画面を表示します。

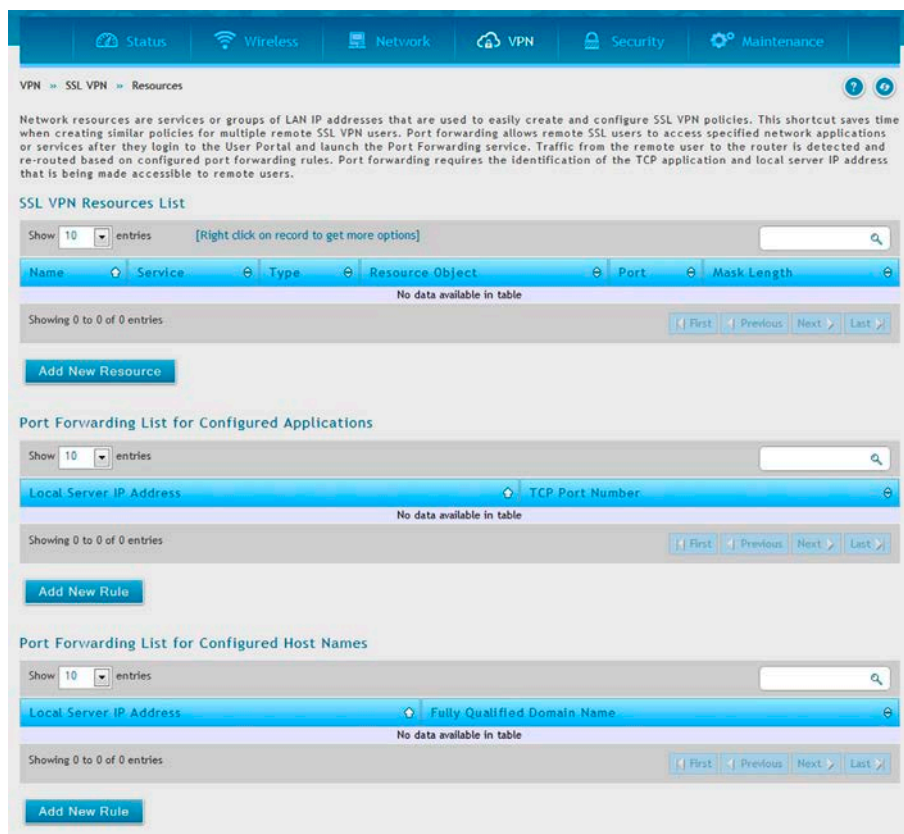


図 8-27 SSL VPN Resources list

2. 「Port Forwarding List for Configured Applications (TCP Port)」または「Port Forwarding List for Configured Host Names (FQDN)」内にある「Add New Rule」をクリックします。
3. ローカルサーバの IP アドレスを入力、その後「TCP ポート番号」または「ドメイン名 (FQDN)」を入力します。

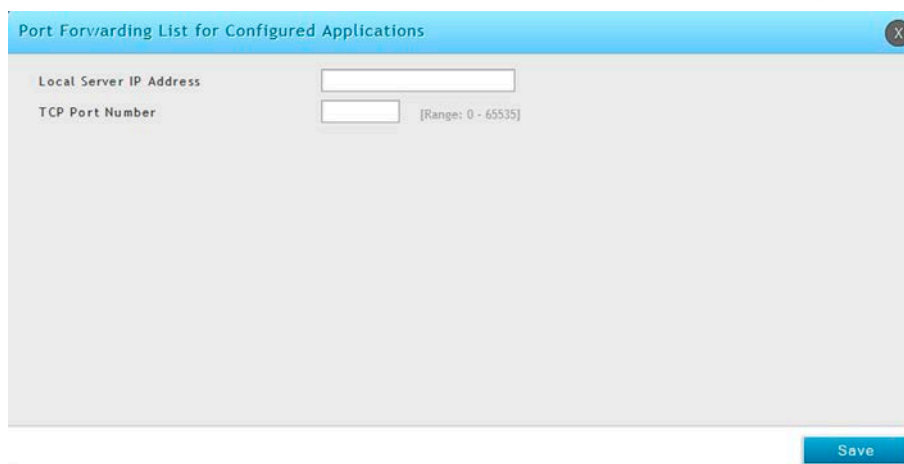


図 8-28 Add New Rule (Port Forwarding)

4. 「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。

SSL VPN クライアント設定

VPN > SSL VPN > SSL VPN Client メニュー

SSL VPN トンネルクライアント設定を行います。

SSL VPN トンネルクライアントはブラウザ側マシンとこのコントローラ間のポイントツーポイント接続を提供します。SSL VPN クライアントがユーザポータルから起動される場合、企業のサブネットから IP アドレス、DNS、および WINS 設定を持つ「ネットワークアダプタ」が自動的に作成されます。これにより、リモート SSLVPN クライアントマシン上に特別なネットワーク設定をせずに、ローカルアプリケーションがプライベートネットワーク上のサービスにアクセスすることができます。

VPN トンネルクライアントの仮想 (PPP) のインタフェースアドレスが LAN 上の物理デバイスと重複しないことを保証することが重要です。SSL VPN 仮想ネットワークアダプタ用の IP アドレス範囲は、コーポレート LAN と異なるサブネットまたは重複しない範囲とすべきです。

コントローラは「Full tunnel」と「Split tunnel」のサポートを許可します。「Full tunnel」モードは VPN トンネル中のクライアントからコントローラにすべてのトラフィックを送信します。「Split tunnel」モードは事前に指定したクライアントのルートに基づいてプライベート LAN にトラフィックを送信します。これらのクライアントのルートは SSL クライアントに特定のプライベートネットワークへのアクセスを与えて、その結果、特定の LAN サービス上のアクセス制御を許可します。

1. VPN > SSL VPN > SSL VPN Client の順にメニューをクリックして、以下の画面を表示します。

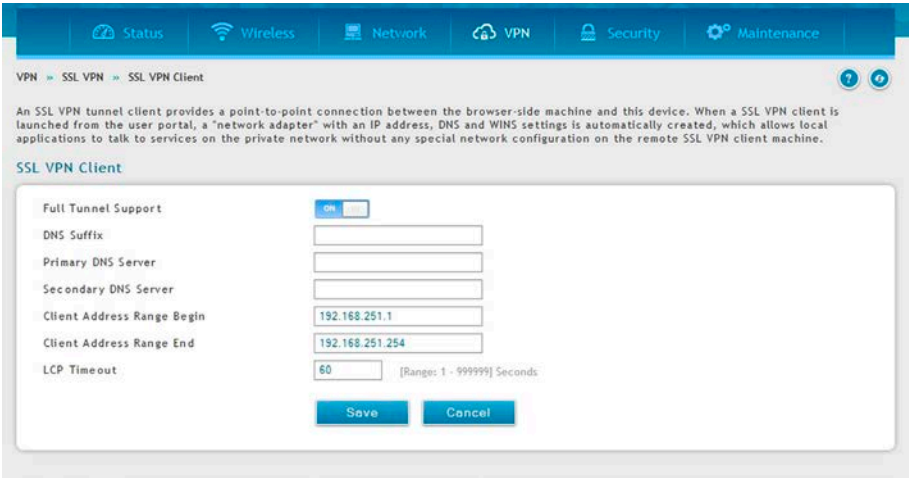


図 8-29 SSL VPN Client 設定

2. 以下の項目を設定します。

項目	説明
Full Tunnel Support	Full トンネルを有効にします。使用するとプライベートネットワークにおける全 IP アドレスが VPN トンネル上でアクセスされます。クライアントルートは必要とされません。
DNS Suffix	SSL VPN クライアントに付与される DNS サフィックス名です。
Primary DNS Server	クライアントホストに作成したネットワークアダプタに設定する DNS サーバの IP アドレスです。
Secondary DNS Server	クライアントホストに作成したネットワークアダプタに設定するセカンダリ DNS サーバの IP アドレスです。
Client Address Range Begin	トンネルに接続するクライアントは、この IP アドレスで開始するアドレスの範囲からネットワークアダプタに割り当てるために DHCP が配布する IP アドレスを取得します。
Client Address Range End	クライアントネットワークアダプタに配布する DHCP のアドレス範囲の終了 IP アドレスです。
LCP Timeout	LCP Echo Interval の値 (秒) を入力します。

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。

SSL VPN クライアントルート設定

VPN > SSL VPN > SSL VPN Client メニュー

ここでは SSL VPN クライアントに設定されている宛先ルートの表示、クライアントルートの追加を行います。

SSL VPN クライアントが違うサブネットの IP アドレスにアサインされた場合、クライアントが VPN トンネルを通じてプライベート LAN にアクセスするために、クライアントルートが追加される必要があります。ファイアウォールのプライベート LAN 上のスタティックルート同様に、VPN ファイアウォールからリモート SSL VPN クライアントにプライベートトラフィックを転送する必要があります。

Split トンネルモードが有効である場合、VPN トンネルクライアントにルートを設定する必要があります。

- 宛先ネットワーク：LAN のネットワークアドレスまたは VPN トンネルクライアントからの宛先ネットワークのサブネット情報を指定します。
- サブネットマスク：宛先ネットワークのサブネット情報を指定します。

- VPN > SSL VPN > Client Routes の順にメニューをクリックして、以下の画面を表示します。

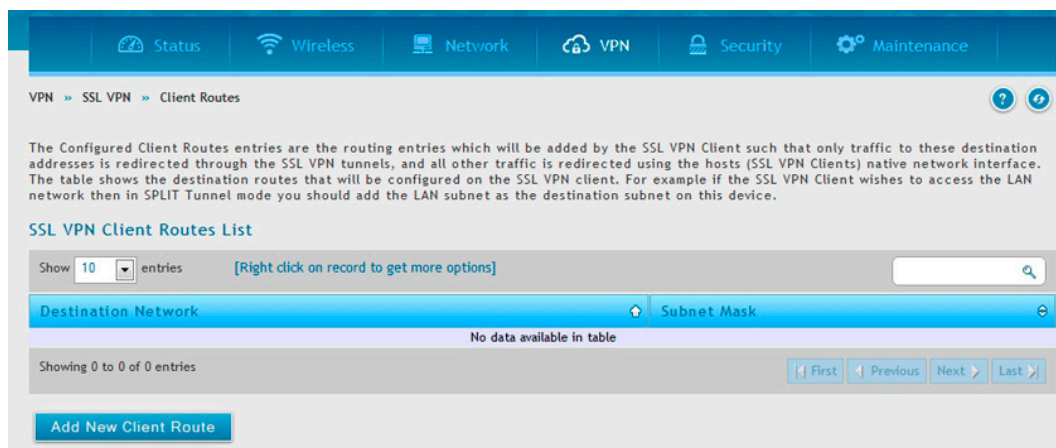


図 8-30 SSL VPN クライアントルートリスト

クライアントルートの追加

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



図 8-31 クライアントルートの設定画面

- 以下の項目を設定します。

項目	説明
Destination network	VPN トンネルクライアントから送信先ネットワークの LAN のネットワークアドレスまたはサブネット情報をここに設定します。
Subnet mask	送信先ネットワークのサブネット情報をここに設定します。

- 「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。

OpenVPN サポート

VPN > OpenVPN メニュー

Open VPN の設定を行います。

OpenVPN 設定

VPN > OpenVPN > Settings メニュー

OpenVPN では、ピアが事前共有秘密鍵、証明書、またはユーザ名 / パスワードを使用することで相互に認証することができます。マルチクライアント - サーバ設定で使用されると、サーバはすべてのクライアントのために署名と CA (認証局) を使用して認証証明書をリリースすることができます。このコントローラを通して OpenVPN を確立することができます。これをチェックまたはチェックを外し、「Save Settings」 ボタンをクリックして OpenVPN サーバの起動 / 停止を行います。

「Server」 モード、「Client」 モード、「Access Server Client」 モードから選択します。アクセスサーバクライアントモードでは「OpenVPN Access Server」 から自動ログインプロファイルをダウンロードし、接続にはアップロードをする必要があります。

1. VPN > OpenVPN > 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。

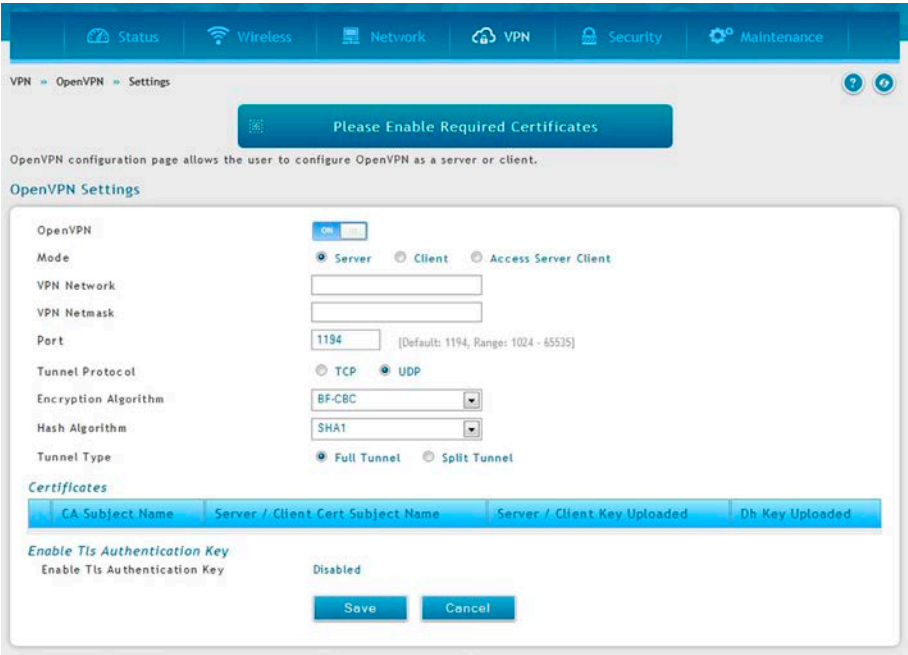


図 8-32 OpenVPN 設定（サーバモード）

2. 以下の項目を設定または表示します。

項目	説明
Open VPN	「ON」 にして Open VPN を有効にします。
Mode	「Server」（サーバモード）、「Client」（クライアントモード）、「Access Server Client」（アクセスサーバクライアントモード）から選択します。指定したモードによって表示される項目が異なります。 「アクセスサーバクライアントモード」では、ユーザは、接続するために OpenVPN アクセスサーバから自動ログインプロファイルをダウンロードして、同じものをアップロードする必要があります。
Server IP（Client）	クライアントが接続する OpenVPN サーバ IP アドレス
VPN Network（Server）	仮想ネットワークアダプタのアドレス
VPN Netmask（Server）	仮想ネットワークのネットマスク
Port	OpenVPN サーバ（またはアクセスサーバ）を実行するポート番号
Tunnel Protocol（Server/Client）	リモートホストと通信を行うために使用するプロトコル。例 :TCP、UDP。初期値は UDP です。
Encryption Algorithm（Server/Client）	パケットが暗号化される方式。例 : BF-CBC、AES-128、AES-192 および AES-256。初期値は BF-CBC はです。
Hash algorithm（Server/Client）	パケット認証に使用されるメッセージダイジェストアルゴリズム。例 : SHA1、SHA256、および SHA512。初期値は SHA1 です。
Tunnel Type（Server）	<ul style="list-style-type: none">Full Tunnel - トンネルを通じてすべてのトラフィックをリダイレクトします。（初期値）Split Tunnel - トンネルを通じて指定リソース（OpenVPN クライアントから追加されたルート）だけにトラフィックをリダイレクトします。
Upload Status（Access Server Client）	設定ファイルのアップロード状況について表示します。

項目	説明
File (Access Server Client)	設定ファイルをアップロードします。 「Browse」(参照)をクリックし、設定ファイルを指定、「Open」をクリック、「Upload」でアップロードします。

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。

Local Networks 設定

VPN > OpenVPN > Local Networks メニュー

「Split Tunnel」を選択した場合、以下の手順でローカルネットワークを作成します。

1. VPN > OpenVPN > Local Networks の順にメニューをクリックし、以下の画面を表示します。

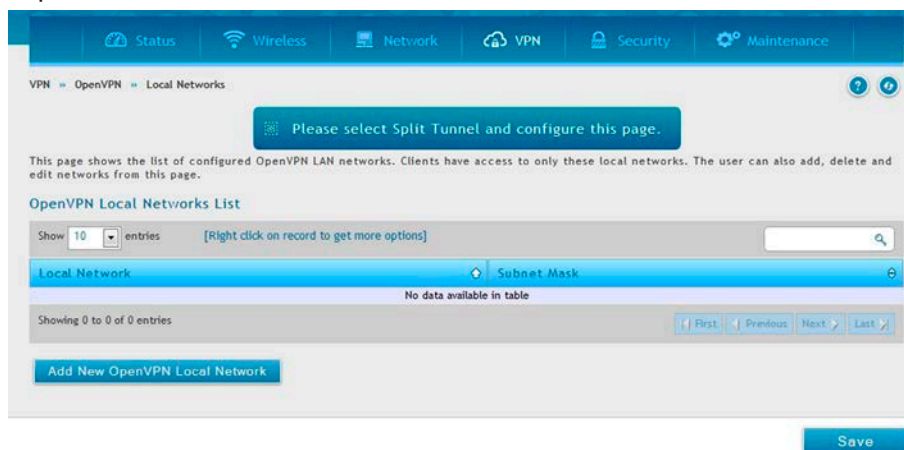


図 8-33 Local Networks

2. 「Add New OpenVPN Local Network」をクリックし以下の画面を表示します。

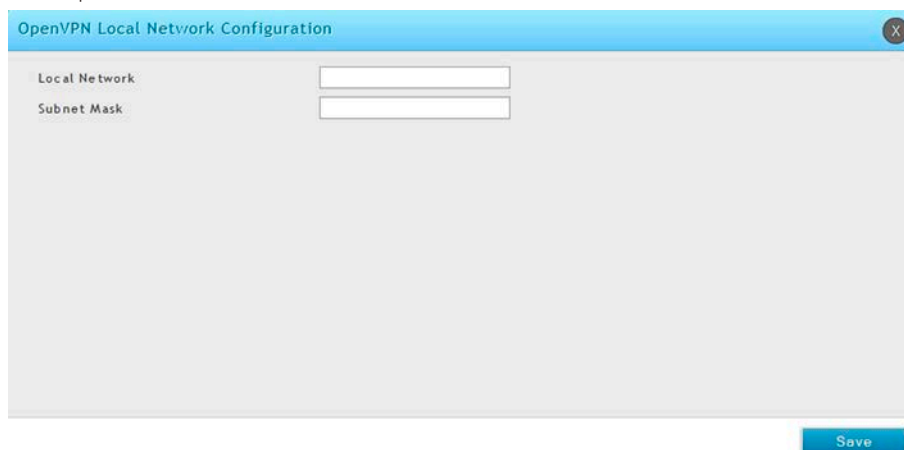


図 8-34 Add New OpenVPN Local Network

3. 以下の項目を設定または表示します。

項目	説明
Local Network	ローカルネットワークのアドレス
Subnet Mask	ローカルネットワークのサブネットマスク

4. 「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。

Remote Networks 設定

VPN > OpenVPN > Remote Networks メニュー
リモートネットワークを作成します。

1. VPN > OpenVPN > Remote Networks の順にメニューをクリックし、以下の画面を表示します。

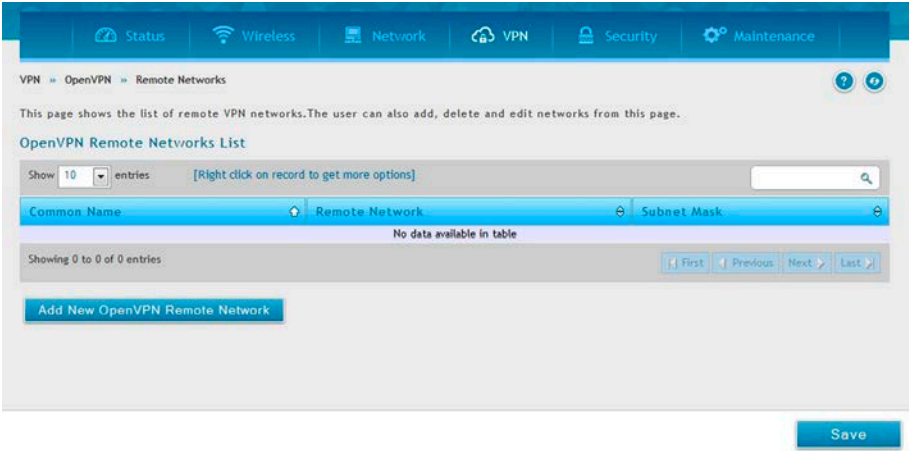


図 8-35 Remote Networks

2. 「Add New OpenVPN Local Network」をクリックし以下の画面を表示します。

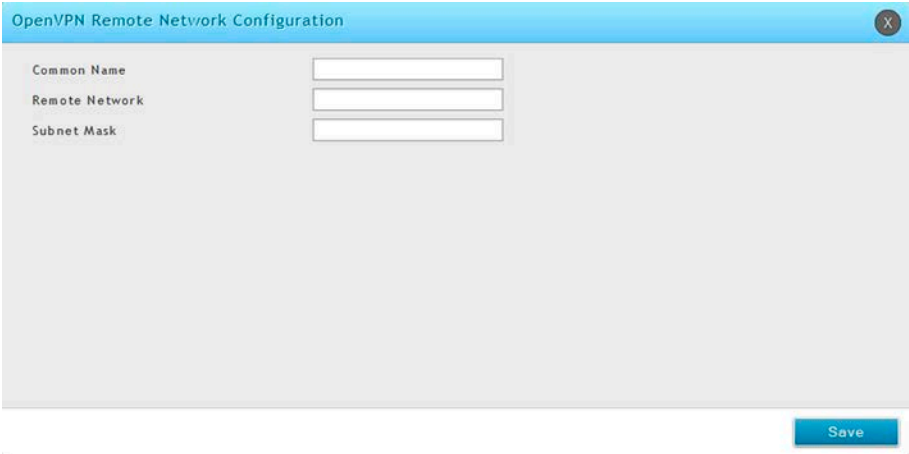


図 8-36 Add New OpenVPN Remote Network

3. 以下の項目を設定または表示します。

項目	説明
Common Name	リモートネットワークの名前を指定します。
Remote Network	リモートネットワークのアドレス
Subnet Mask	リモートネットワークのサブネットマスク

4. 「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。

Authentication 設定

VPN > OpenVPN > Authentication メニュー

Open VPN の認証を設定します。鍵や証明書をアップロードすることができます。「Browse」をクリックしアップロードするファイルを指定、「Open」をクリックして「Upload」します。

1. VPN > OpenVPN > 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。

VPN > OpenVPN > Authentication

Openvpn provides authentication using certificates. This page allows you to upload required certificates and keys which are in pem format.

OpenVPN Authentication

Trusted Certificate (CA Certificate) Certificate Status	No
Browse Certificate File	<input type="button" value="Browse..."/> No file selected.
	<input type="button" value="Upload"/>
Server / Client Certificate Certificate Status	No
Browse Certificate File	<input type="button" value="Browse..."/> No file selected.
	<input type="button" value="Upload"/>
Server / Client Key Key Status	No
Browse Key File	<input type="button" value="Browse..."/> No file selected.
	<input type="button" value="Upload"/>
DH Key Key Status	No
Browse Key File	<input type="button" value="Browse..."/> No file selected.
	<input type="button" value="Upload"/>
Tls Authentication Key Key Status	No
Browse Key File	<input type="button" value="Browse..."/> No file selected.
	<input type="button" value="Upload"/>

図 8-37 Authentication

2. 「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。

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ページについて説明します。

メニュー	説明	参照ページ
統計情報と利用率の参照	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。	231
ダッシュボードの管理	ダッシュボードの設定を行います。	232
システム状態の参照	コントローラのシステム情報について参照します。	235
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について参照します。	237
無線情報の参照	コントローラの無線情報について参照します。	241

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。

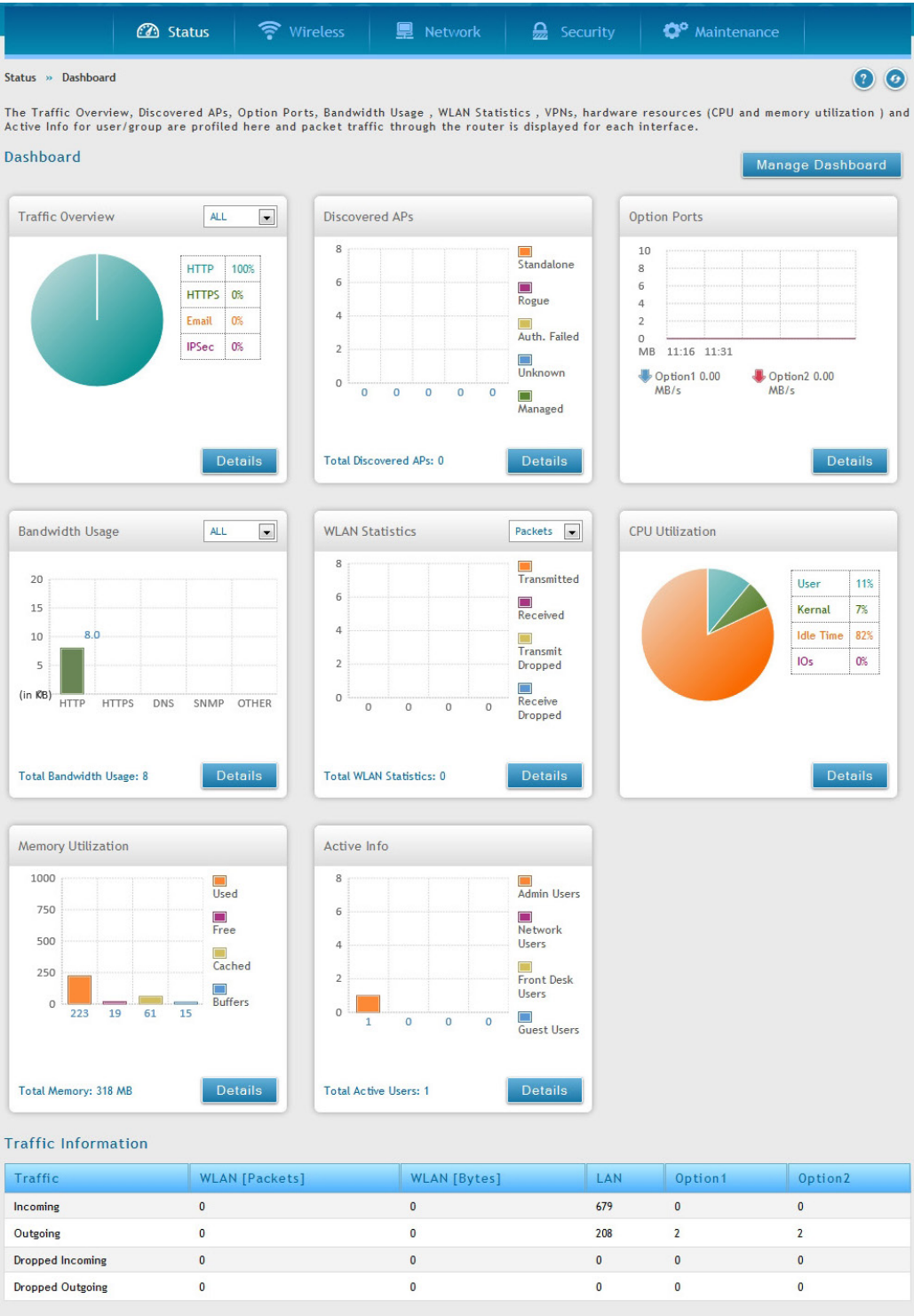


図 8-1 Dashboard 画面

セクション	説明
Traffic Overview	各インタフェースのトラフィック概要のチャートを表示します。
Discovered APs	検出した現在の状態ごとに発見されたアクセスポイントのチャートを表示します。
Bandwidth Usage	「WLAN」や「LAN」などのネットワークセグメントに使用された帯域の使用率を表示します。データは「HTTP」「HTTPS」「DNS」「SNMP」などのアプリケーションサービスごとに表示されます。
WLAN Statistics	現在関連付けされている、管理下の全アクセスポイントが取得した WLAN トラフィックについて、帯域幅ごとのトラフィックの概要およびパケット情報のチャートを表示します。

セクション	説明
CPU Utilization	現在デバイスが消費している CPU 使用率 (%) を表示します。CPU 使用率では、管理操作、カーネル空間のプロセス、CPU アイドル時間または IO など、すべてのユーザ空間のプロセスを細かく分割しています。
Memory Utilization	使用量、空き、キャッシュ、システムバッファ内の現在の状況ごとにメモリ使用の状態を分けて表示します。
Traffic Information	各インタフェースのトラフィック状況を表示します。

ダッシュボードの管理

ダッシュボードの管理：

1. 「Manage Dashboard」ボタンをクリックします。

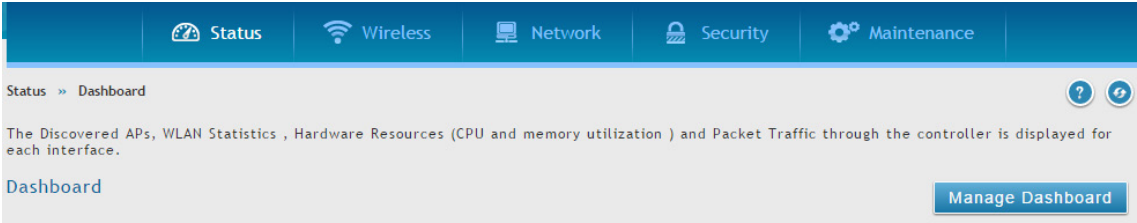


図 8-2 Dashboard 画面

2. 以下の画面が表示されます。

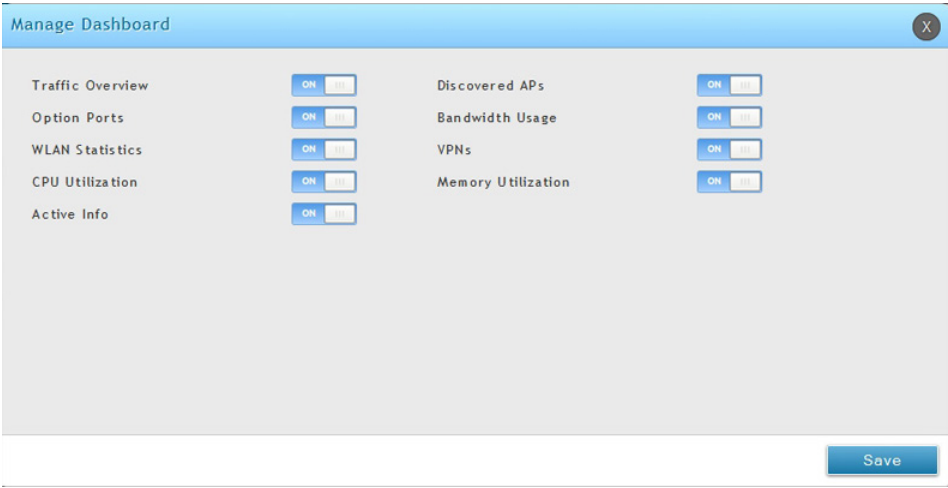


図 8-3 Managed Dashboard 画面

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。

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。

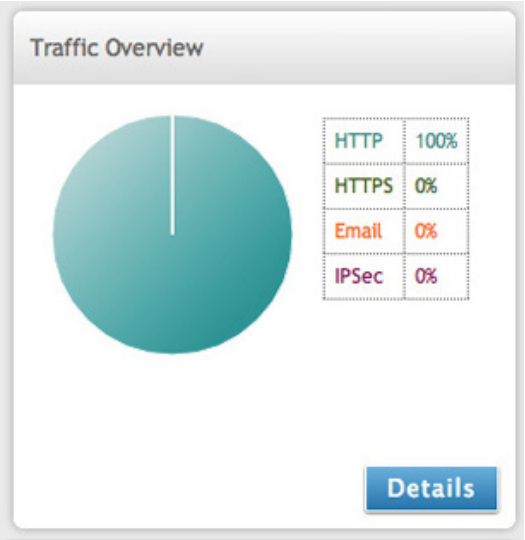


図 8-4 Memory Utilization 画面

The 'Traffic Overview Details' dialog box displays a list of LAN traffic types and their corresponding sizes in KB. The list includes HTTP (28.303711 KB), HTTPS (0.000000 KB), DNS (0.000000 KB), IMAP2 (0.000000 KB), IMAP3 (0.000000 KB), NFS (0.000000 KB), POP3 (0.000000 KB), SMTP (0.000000 KB), SNMP (0.000000 KB), and SSH (0.000000 KB).

Traffic Type	Size (KB)
HTTP	28.303711
HTTPS	0.000000
DNS	0.000000
IMAP2	0.000000
IMAP3	0.000000
NFS	0.000000
POP3	0.000000
SMTP	0.000000
SNMP	0.000000
SSH	0.000000

図 8-5 Traffic Overview Details 画面

The 'Discovered Aps Details' dialog box displays a list of AP statistics. The list includes Total APs (1), Managed APs (1), Standalone APs (0), Rogue APs (0), Discovered APs (0), Connection Failed APs (0), Authentication Failed APs (0), and Unknown APs (0).

AP Type	Count
Total APs	1
Managed APs	1
Standalone APs	0
Rogue APs	0
Discovered APs	0
Connection Failed APs	0
Authentication Failed APs	0
Unknown APs	0

図 8-6 Discovered APs Details 画面

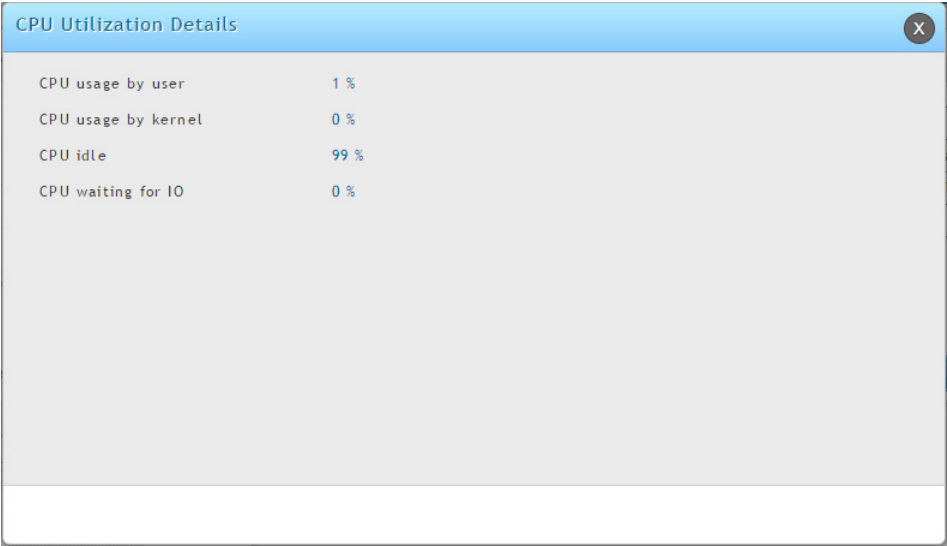


図 8-7 CPU Utilization Details 画面



図 8-8 WLAN Utilization 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)

有線ポートのどれかについて問題を疑う場合、このテーブルを使用して、ポートが持つ稼働時間または送信レベル問題の診断します。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制御があります。このページの自動更新の初期値は 10 (秒) です。

システム状態の参照

Status > System Information メニュー

機器状態の参照

Status > System Information > Device メニュー

「Setup」と「Advanced」メニューで設定された無線コントローラのコンフィグレーション設定を概説します。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、およびシリアル番号を表示します。
- 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 ではコントローラのローカルインタフェースを表示することにご注意ください。LAN ポートのどれかを「Standalone」に設定すると、対応する LAN の下に情報を表示します。

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。

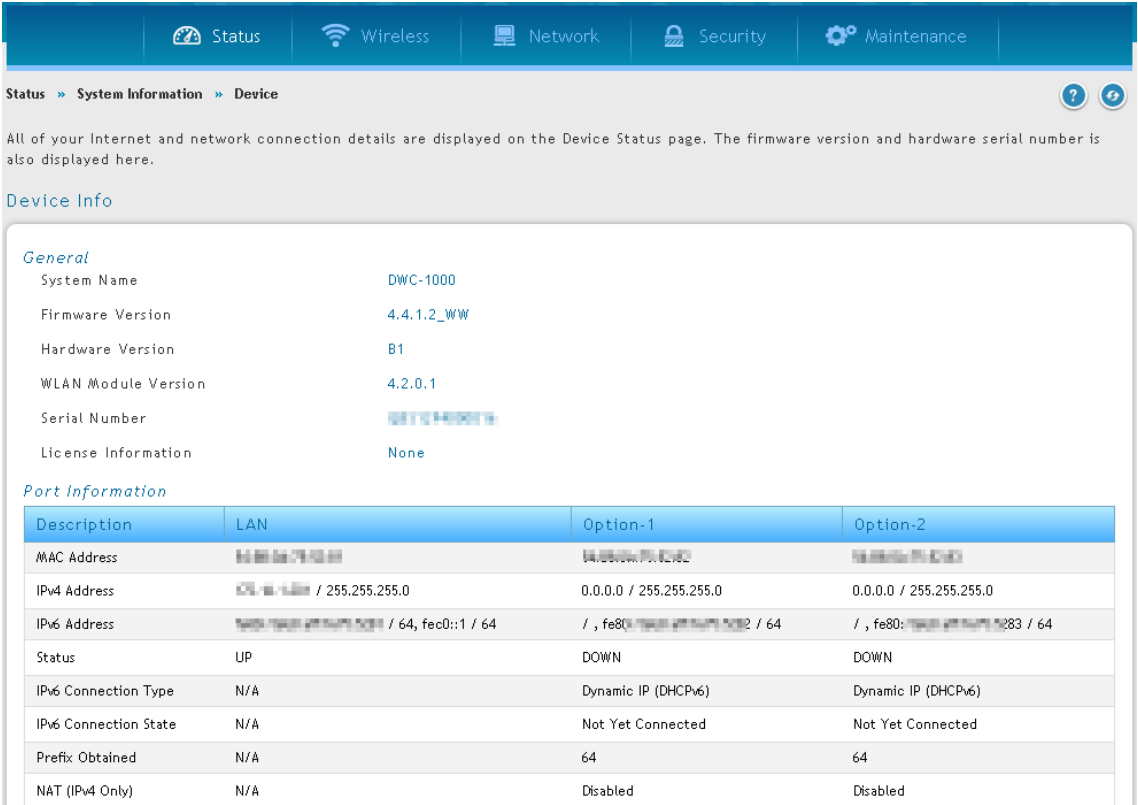


図 8-9 Device Info 画面

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。
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。
Hardware Version	コントローラのハードウェアリビジョン。
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。
Serial Number	コントローラのメーカーのシリアル番号。
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。

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まとめています。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 8-10 USB (s) Status 画面

以下の項目があります。

項目	説明
Description	
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。
USB Port 1	USB ポート 1 に接続するデバイスに関する情報を表示します。
USB Port 2	USB ポート 2 に接続する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

Status > Network Information メニュー

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 をリースしているクライアントのリストを表示します。: LAN のリースクライアントと LAN IPv6 のリースクライアント

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。

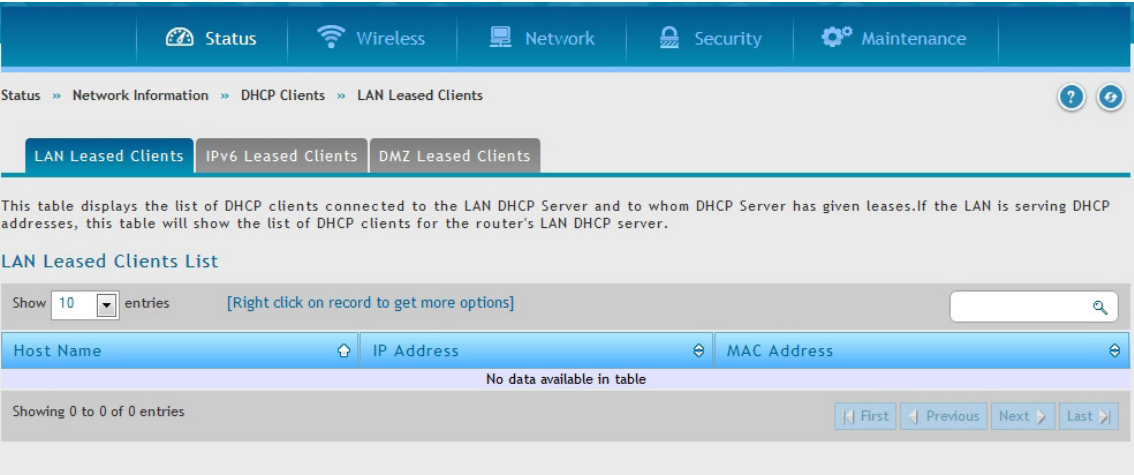


図 8-11 LAN Leased Clients List 画面

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。
IP Address	予約 IP リストに一致するホストの LAN IP アドレス。
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。

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。

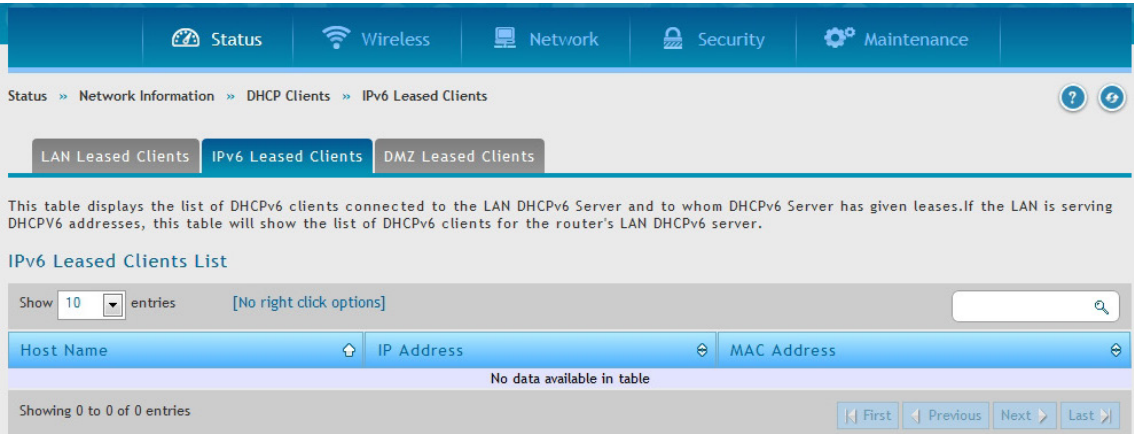


図 8-12 IPv6 Leased Clients List 画面

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。
IP Address	DHCP IPv6 サーバが予約する LAN IPv6 アドレス。
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。

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。

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選択的に切断できます。

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」ボタンは結果的にブロックリスト (Security > Firewall > Blocked Clients) に追加することになり、このクライアントの現在および今後のセッションを防止します。

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。

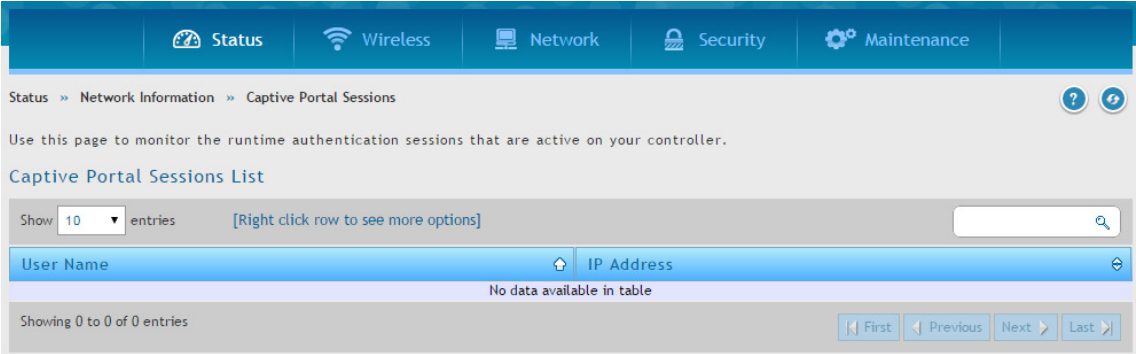


図 8-13 Captive Portal Sessions List 画面

以下の項目があります。

項目	説明
User Name	ランタイム認証ユーザのユーザ名。
IP Address	ログインするユーザの IP アドレス。ユーザ名と IP アドレスをブロックするには、「Captive Portal Sessions List」の右クリックメニューから「Block」を選択することで、実行できます。
Disconnect	選択ユーザの現在のセッションを切断します。

アクティブセッションの参照

Status > Network Information > Active Sessions メニュー

アクティブセッションでは、以下の項目の無線コントローラ経由のアクティブなインターネットセッションについての情報を表示します。

- Source (送信元)
- Destination (宛先)
- Protocol used during the Internet sessions (インターネットセッションに使われたプロトコル)
- State (状態)

Status > Network Information > Active 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。

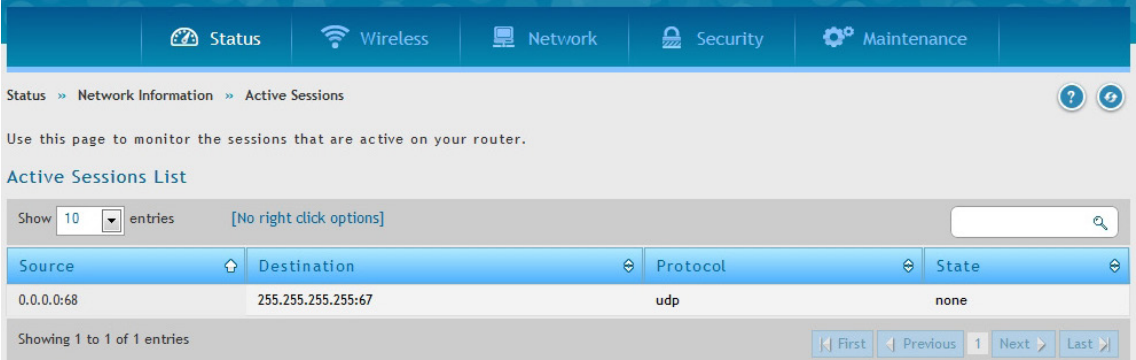


図 8-14 Active Sessions List 画面

VPN セッションの参照

Status > Network Information > Active VPN Sessions メニュー

アクティブ VPN セッションでは、以下の項目の無線コントローラ経由のアクティブな VPN セッションについての情報を表示します。

- Policy Name (ポリシー名)
- Endpoint (エンドポイント)
- Transfer Rate (KB and Packets) (送信レート)
- Configuration State (設定状況)

注意 本機能は追加ライセンス「DWC-1000-VPN」が有効の場合にのみ利用可能です。

表示する VPN セッションを選択します。(IPSec、SSL、PPTP、Open VPN)

Status > Network Information > Active VPN 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。

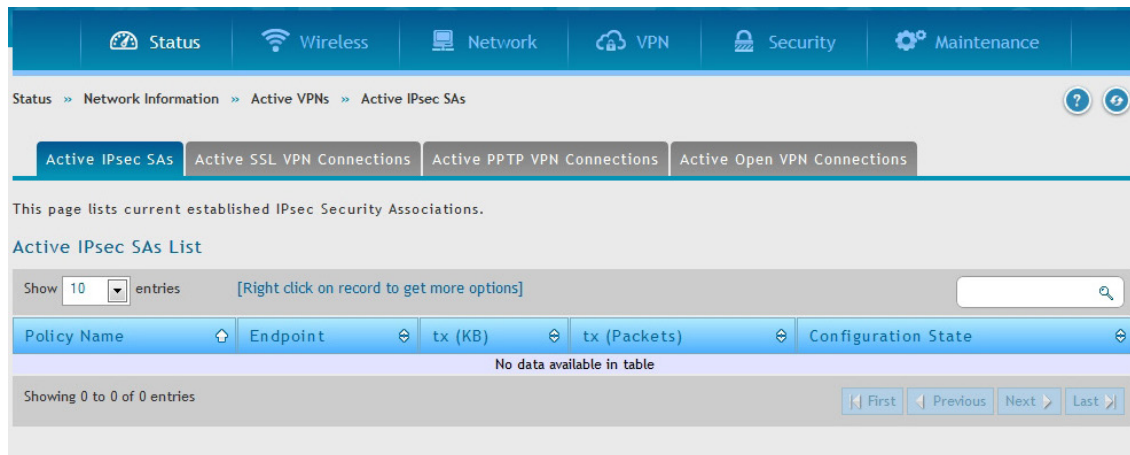


図 8-15 Active VPN Sessions List 画面 (IPsec)

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。

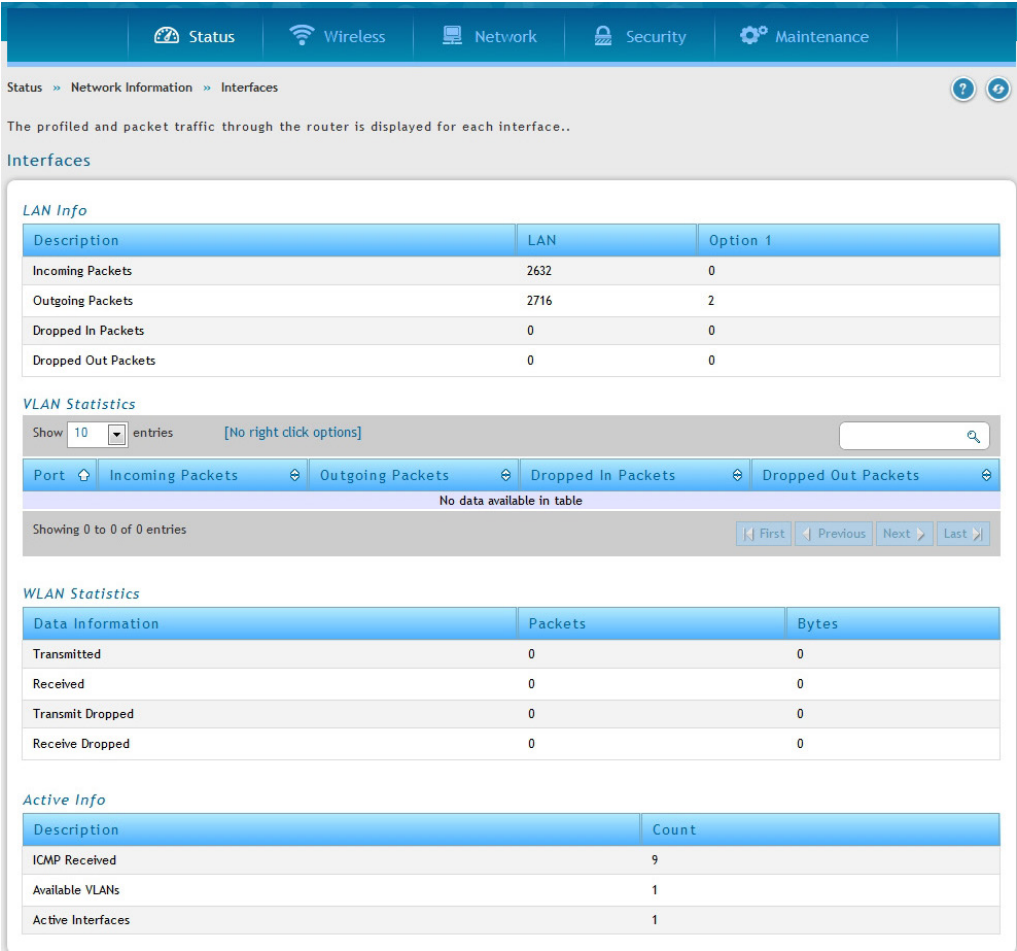


図 8-16 Interfaces 画面

以下の項目があります。

項目	説明
LAN Info (LAN 1-4)	
Incoming Packets	ポートに入力する IP パケット数。
Outgoing Packets	ポートから出力するパケット数。
Dropped In Packets	インタフェースの内向き方向で破棄されたパケット。
Dropped Out Packets	インタフェースの外向き方向で破棄されたパケット。
VLAN Statistics	
Port	VLAN に対応するポート番号
Incoming Packet	ポートに入力する IP パケット数。
Outgoing Packet	ポートから出力するパケット数。
Dropped In Packet	インタフェースの内向き方向で破棄されたパケット。
Dropped Out Packet	インタフェースの外向き方向で破棄されたパケット。
WLAN Statistics	
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。
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。
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。
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。
Active Info	
ICMP Received	インタフェースに受信した ICMP パケットの総数。
Available VLAN	有効とされたアクティブな VLAN インタフェース。
Active Interfaces	有効なインタフェースの数。

無線情報の参照

Status > Wireless Information メニュー

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。

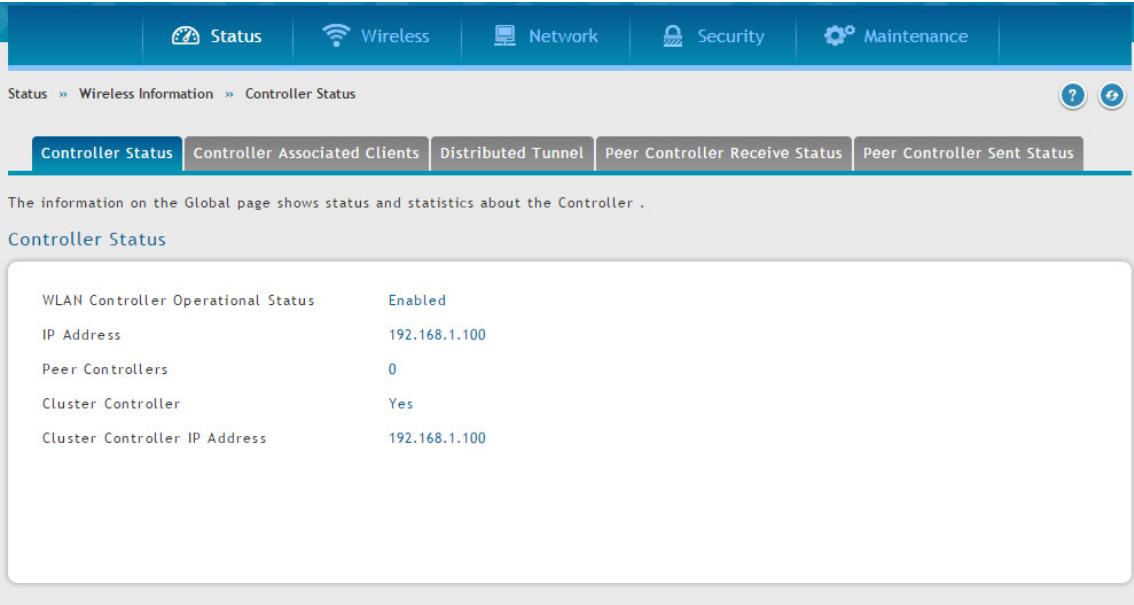


図 8-17 Controller Status 画面

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。
IP Address	無線コントローラの IP アドレス。
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。
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。 <div>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。</div>
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。

コントローラに関連付けされているクライアント

Status > Wireless Information > Controller Status > Controller Associated Clients メニュー

コントローラと関連付けされている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。

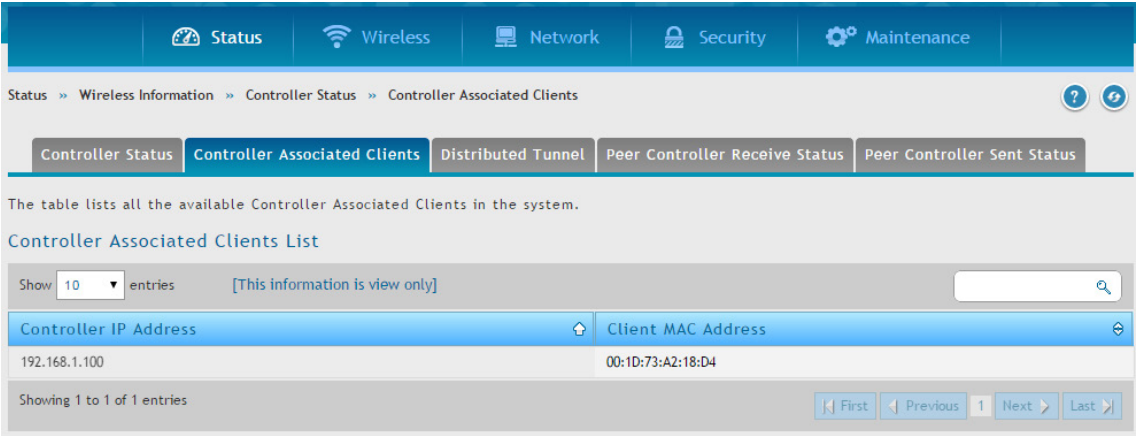


図 8-18 Controller IP Address 画面

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。

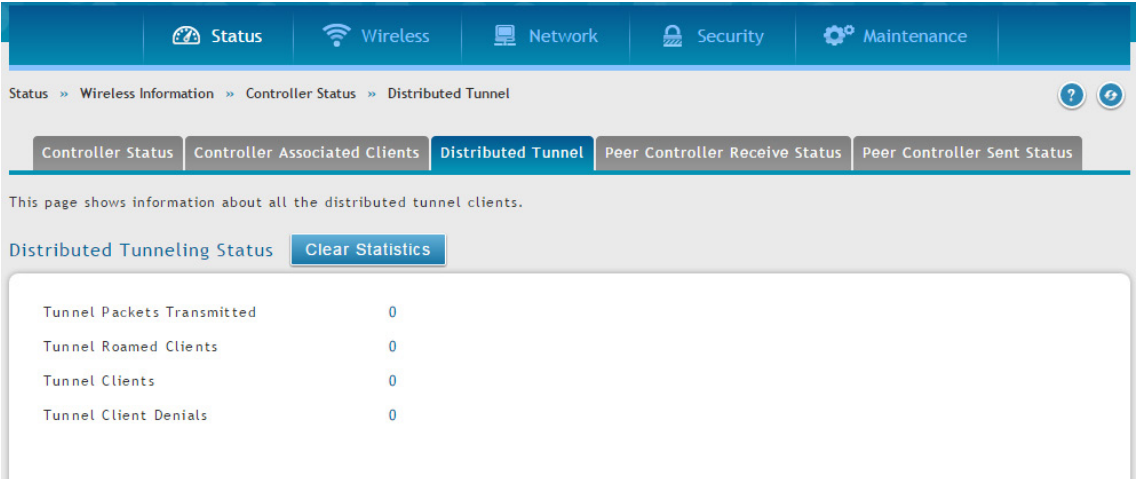


図 8-19 Distributed Tunneling Status 画面

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。
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。
Tunnel Clients	分散型トンネルを使用しているアクセスポイントに接続するクライアントの総数。
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。

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。コントローラの同期を維持することに加え、本機能では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します。「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。

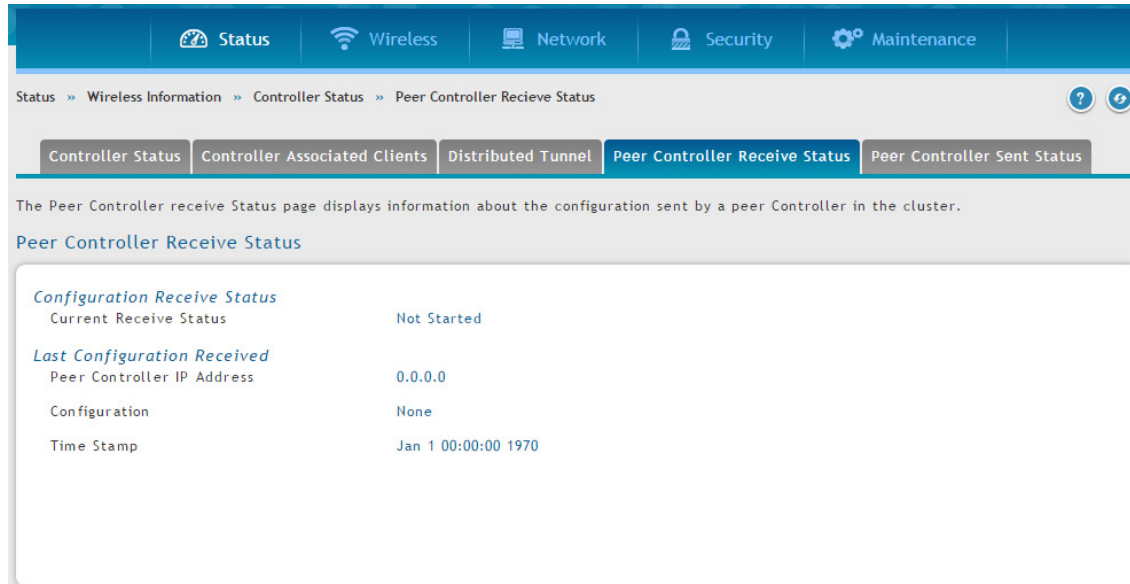


図 8-20 Peer Controller Received Status 画面

以下の項目があります。

項目	説明
Current Receive Status	
Current Receive Status	<p>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ステータスを表示します。</p> <ul style="list-style-type: none"> 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。
Configuration	<p>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一部を表示します。</p> <ul style="list-style-type: none"> 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までの設定を表示します。また、クラスタ内のピアコントローラが送信した設定に関する情報、設定情報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。

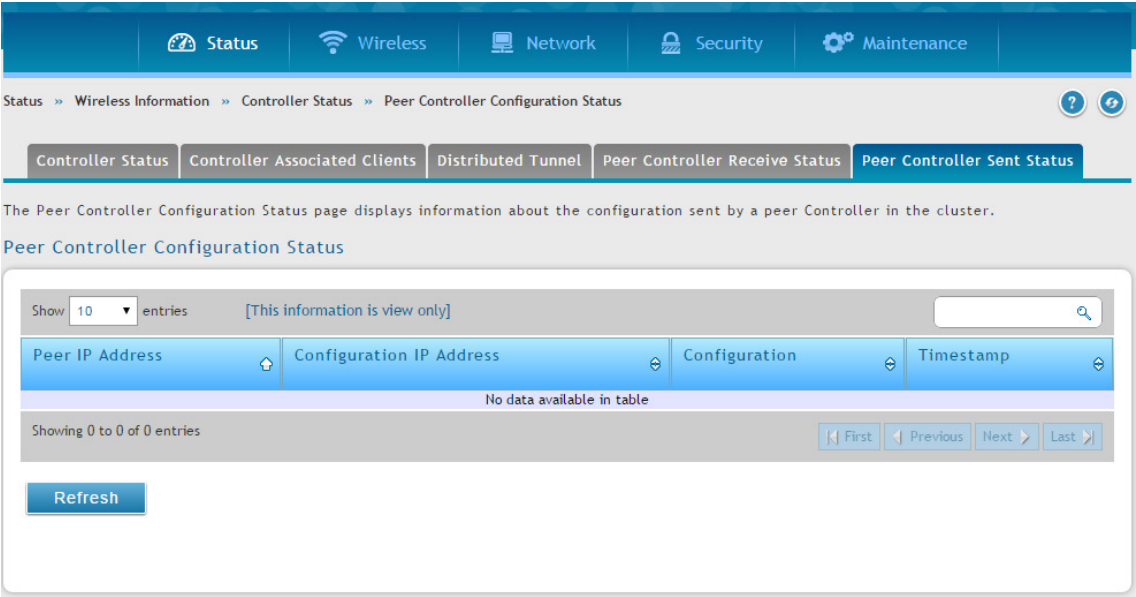


図 8-21 Peer Controller Sent Status 画面

以下の項目があります。

項目	説明
Peer IP Address	設定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 IP Address	設定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設定の一部を表示します。
Timestamp	設定がコントローラに適用された日時を表示します。管理者が NTP を使用するために各ピアコントローラを設定した場合にだけ、時間が UTC で表示されるため便利です。

「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

Status > Wireless Information > Access Point メニュー

Global Status

Status > Wireless Information > Access Point > Global Status メニュー

無線コントローラが発見したアクセスポイント（管理、接続失敗、不正）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。

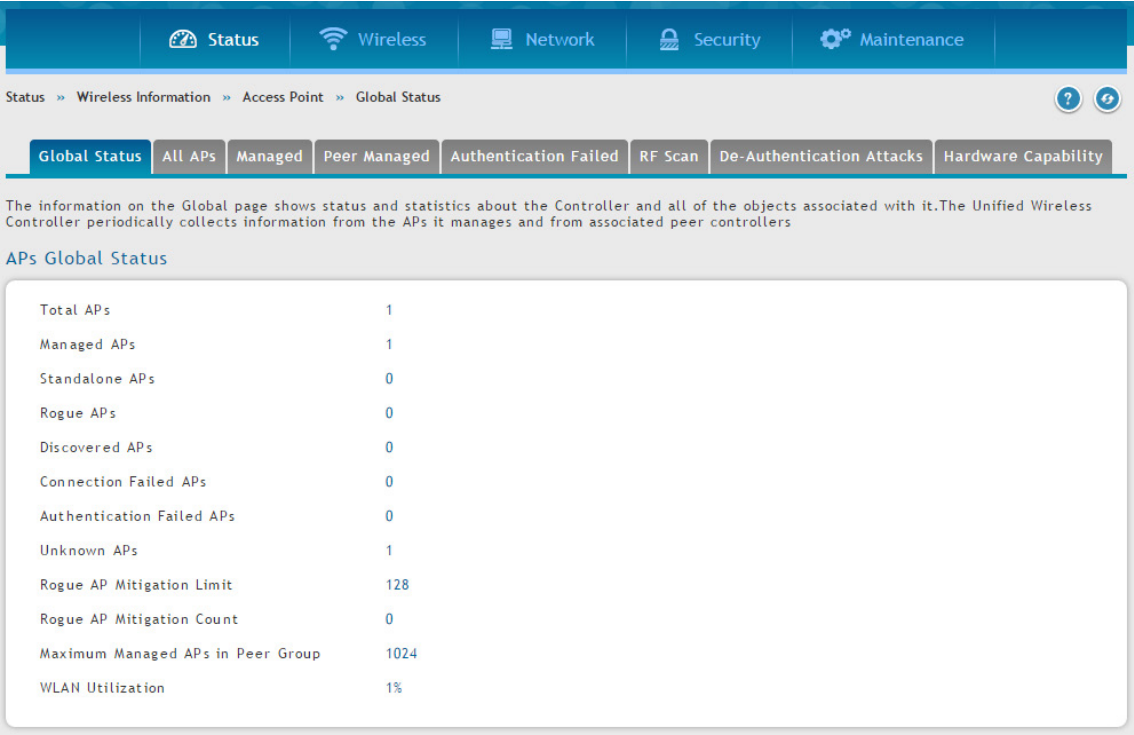


図 8-22 APs Global Status 画面

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。この値は常に「Managed APs」、「Connection Failed APs」、「Discovered APs」の値の和と等しくなります。
Managed APs	管理対象 AP データベース内のアクセスポイント数。これは、認証、設定が行われており、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 モードのトラストアクセスポイント数。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。アクセスポイントが RF スキャンする時、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「Rouge」（不正）として報告します。
Discovered APs	コントローラと接続しているが、完全に設定されていないアクセスポイント。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が、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。
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。
Unknown APs	現在 WLAN 上に検出された「Unknown」（未知）のアクセスポイントの数。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。
Rogue AP Mitigation Count	不正なアクセスポイントを減少させるために、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。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。
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。本値はグローバル統計値を基にしています。

All APs

Status > Wireless Information > Access Point > All APs メニュー

無線コントローラが発見または削除したアクセスポイント（管理、接続失敗、不正）に関するサマリ情報を表示します。ステータスエントリを手動で削除できます。

Status > Wireless Information > Access Point > All 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。

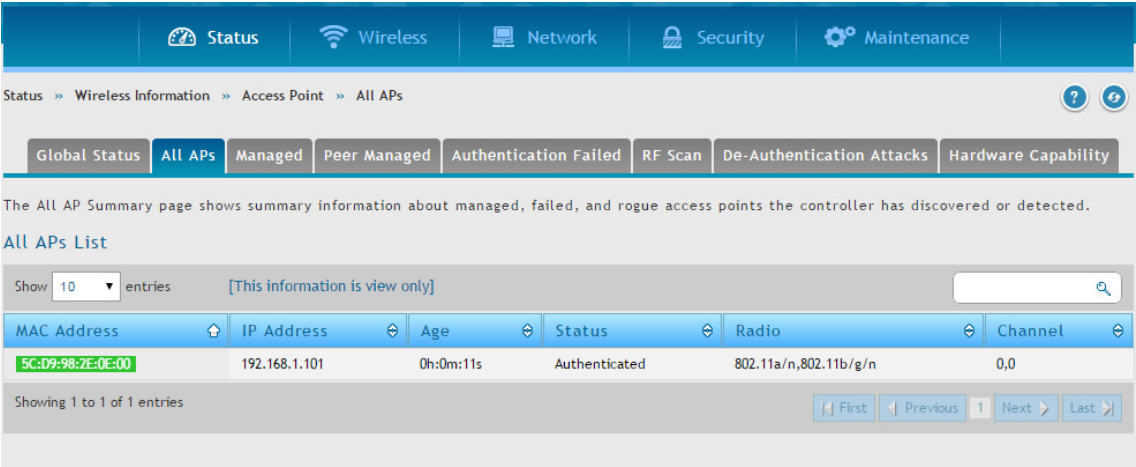


図 8-23 All APs List 画面

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。
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。
Status	アクセスポイントステータス。 <ul style="list-style-type: none">Managed - アクセスポイント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。No Database Entry - アクセスポイントの MAC アドレスがローカルまた RADIUS Valid AP に存在しません。Authentication (Failed AP) - アクセスポイントは、無線コントローラまたは RADIUS サーバによる認証に失敗しました。Failed - 無線コントローラはアクセスポイントとの接続が失われました。エラーのエントリは、削除するまでは Managed AP データベースに残ります。 <div>注意 管理下のアクセスポイントは、再起動中、一時的に「Failed」のステータスになります。</div> <ul style="list-style-type: none">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。
Radio	アクセスポイントが使用している無線帯域モード。
Channel	無線帯域で運用中のチャンネル。

Managed

Status > Wireless Information > Access Point > 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。管理されているアクセスポイントを右クリックすると、さらにオプションを有効にできます。

Status > Wireless Information > Access Point > 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。

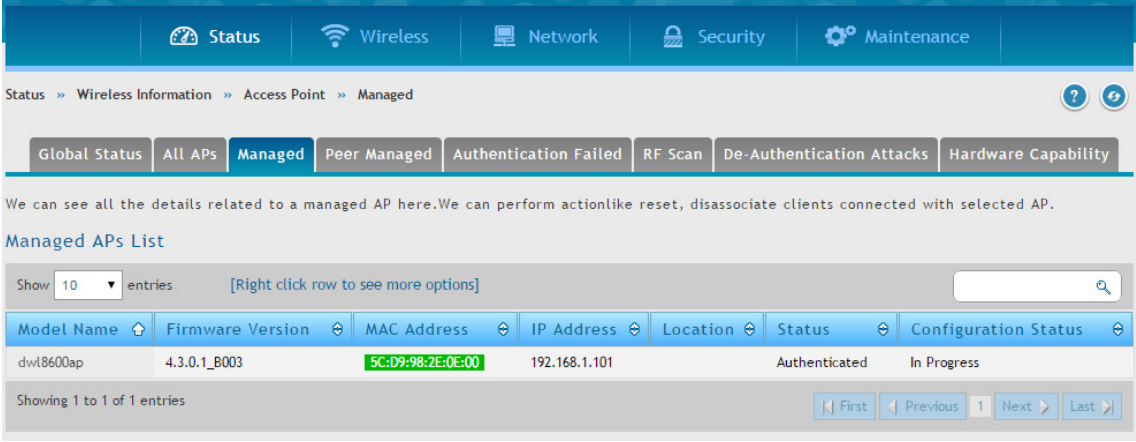


図 8-24 Managed APs List 画面

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。
Firmware Version	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。
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。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。
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記述。アクセスポイントの管理セクションを通じて設定済みのものです。
Status	アクセスポイントの現在の管理状態。 <ul style="list-style-type: none">Discovered - アクセスポイントは、無線コントローラによって発見されていますが、認証されていません。Authenticated - コントローラにより認可および認証されました（認証が有効である場合）が、設定されていません。Managed - 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。Failed - 無線コントローラはアクセスポイントとの接続が失われました。エラーのエントリは、削除するまで Managed 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、リセット中、一時的に「Failed」のステータスになります。 <div>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方のインタフェースはダウンします。アクセスポイントに関連付けられたすべてのクライアントの接続が解除されます。そのアクセスポイントが再度管理されると、無線インタフェースは動作状態になります。</div>
Configuration Status	管理対象のアクセスポイントに対して設定プロファイルの適用に成功しているかどうかを表示します。

右クリックすると、オプションメニューを選択することができます。

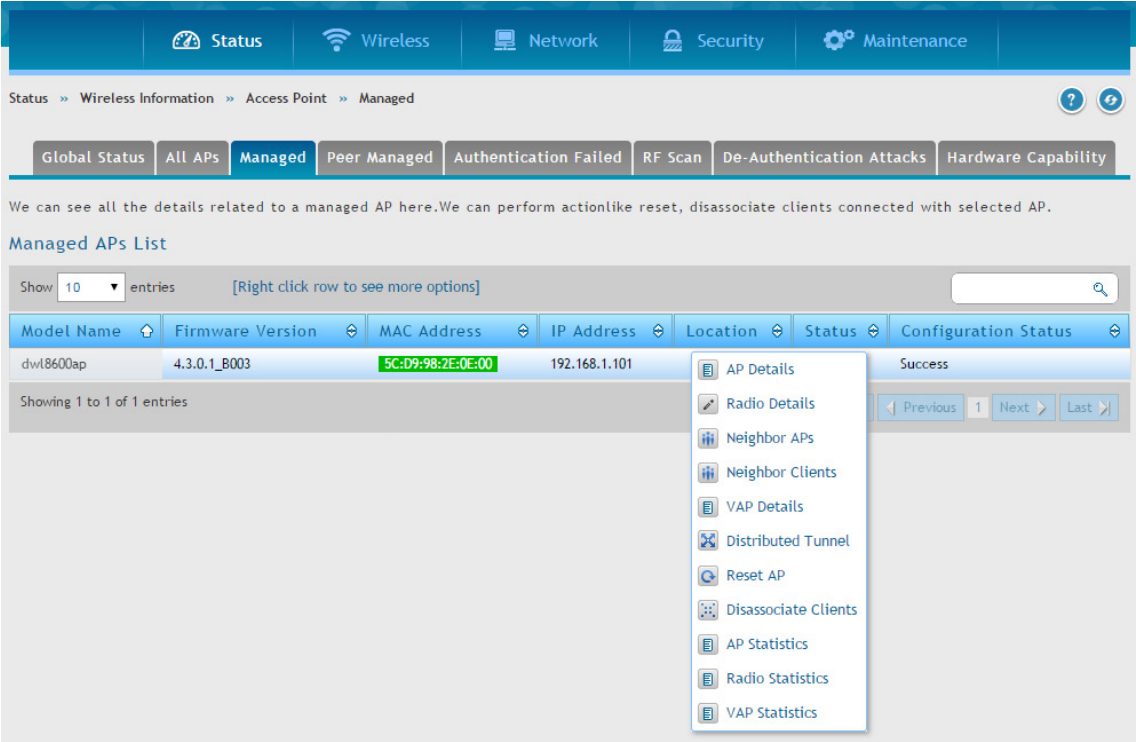


図 8-25 Managed APs List 画面

以下のメニューがあります。

項目	説明
AP Details	アクセスポイントから収集した詳細な状態情報を表示します。
Radio Details	無線インタフェースの詳細な状態を表示します。
Neighbor 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。
Neighbor 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。
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。
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。
Reset AP	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。
Disassociate Clients	選択したアクセスポイントから切断したクライアントを表示します。

また、アクセスポイントの有線 / 無線インタフェース上のトラフィックに関する情報を表示します。本情報をスループットの問題などネットワークのトラブルの診断に役立てることができます。管理するアクセスポイントの統計情報を表示するためには、「Managed APs List」内のエントリを右クリックして、以下のメニューを選択します。

項目	説明
AP Statistics	特定の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	特定の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	特定の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。

AP Details

「Managed APs List」内のエントリを右クリックして、「AP Details」を選択します。

Managed APs	
MAC address	78:54:2E:32:57:C0
IP Address	192.168.10.5
Managing Controller	Local Controller
IP Subnet Mask	255.255.255.0
Controller MAC Address	00:02:bc:9b:97:6a
Status	Managed
Controller IP Address	192.168.10.1
Software Version	4.3.0.1_B006
Profile	1 - Default
Code Download Status	Not Started
Discovery Reason	L2 Poll Received
Configuration Status	Not Started
Protocol	5
Vendor ID	D-Link
Authenticated Clients	0
Part Number	bcm953012er
System Up time	0d:00:50:33
Serial Number	RZ8Y1DB000004
Age	0d:00:00:04
Hardware Type	DWL-6600AP Dual Radio a/b/g/n

図 8-26 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。 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。
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。
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。
Status	<p>アクセスポイントの状態を示します。</p> <ul style="list-style-type: none"> 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。 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。 <p>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。</p>
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。
Software Version	アクセスポイントのソフトウェアバージョン。アクセスポイントの検出時に取得される情報です。
Profile	<p>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。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。</p> <p>注意 一度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。</p>

項目	説明
Code Download Status	<p>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。</p> <ul style="list-style-type: none"> 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。
Discovery Reason	<p>アクセスポイントを検出した方法を表示します。</p> <ul style="list-style-type: none"> 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	<p>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。</p> <ul style="list-style-type: none"> 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。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。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。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。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和です。
Part Number	アクセスポイントのハードウェアパート番号。アクセスポイントの検出の際に学習されます。
System Up time	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)。
Serial Number	アクセスポイントのシステムのシリアル番号。
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。
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。アクセスポイントの検出の際に学習されます。

Radio Details

「Managed APs List」内のエントリを右クリックして、「Radio Details」を選択します。

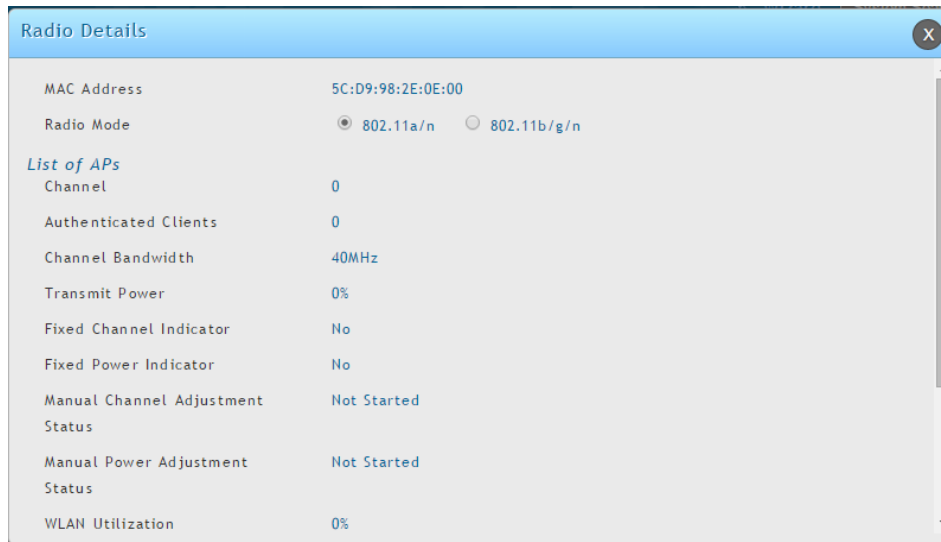


図 8-27 Radio Details 画面

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。
Radio Mode	広帯域の無線クライアントと無線ネットワーク要求に適応するために、Radio1 また Radio2 を選択できます。初期値では、Radio1 は IEEE 802.11a/n モードで動作し、Radio2 は IEEE 802.11b/g/n モードで動作します。
Supported Channels	アクセスポイントがコントローラに報告する、チャンネル割り当ての候補となるチャンネル。リスト中のエントリは国コード、ハードウェアの性能、および設定によるチャンネル制限により異なります。
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。
Channel Bandwidth	チャンネル帯域幅 (20MHz または 40MHz)。
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。
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。 <ul style="list-style-type: none"> 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。
WLAN Utilization	物理無線帯域のネットワーク利用量の合計。本値は無線帯域の統計情報に基づきます。
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。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。
Transmit Power	無線帯域の現在の送信電力。
Fixed Power Indicator	固定送信電力が設定され、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。固定送信電力は 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 Power Adjustment Status	変更する手動リクエストの現在の状況。
Total Neighbors	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。
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。
Radar Detection Required	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 デバイスとそのチャンネルで検出されたかどうかを表示します。
Time Since Radar Last Detected	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。

Neighbor APs

「Managed APs List」内のエントリを右クリックして、「Neighbor APs」を選択します。

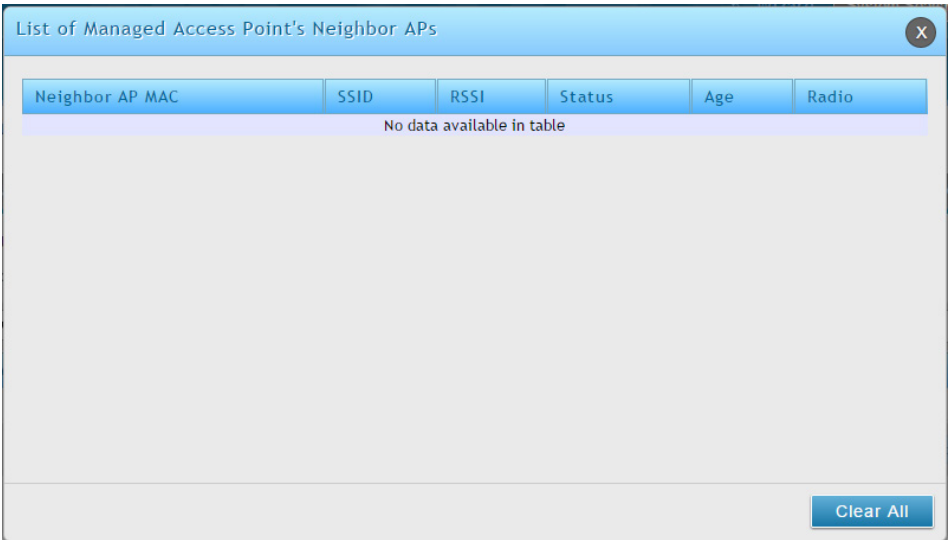


図 8-28 AP's Neighbor APs 画面

以下の項目があります。

項目	説明
Neighbor AP MAC	Neighbor アクセスポイントネットワークの MAC アドレス。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。Neighbor 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	Neighbor アクセスポイントのネットワークの SSID。
RSSI	Neighbor 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。 <ul style="list-style-type: none">Managed - 無線システムは Neighbor 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。
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	Neighbor アクセスポイントと Neighbor 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。これは、現在選択したアクセスポイントおよび無線インタフェースのみならず、全アクセスポイントの全無線インタフェースにおける全 Neighbor を削除します。リストは Neighbor が検出されると、再度ポピュレートされます。

Neighbor Clients

「Managed APs List」内のエントリを右クリックして、「Neighbor Clients」を選択します。

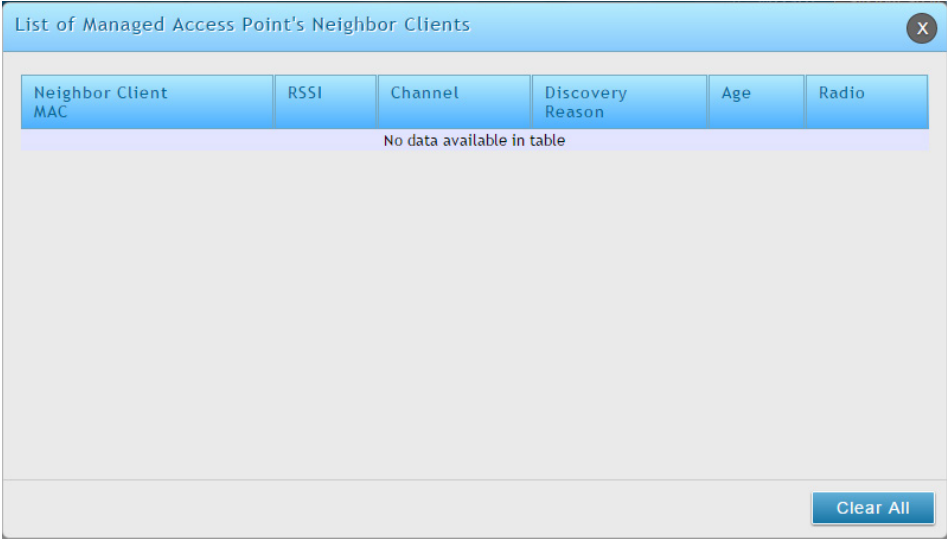


図 8-29 AP's Neighbor Clients 画面

以下の項目があります。

項目	説明
Neighbor Client MAC	Neighbor アクセスポイントネットワークの MAC アドレス。物理的な無線インタフェースまたは VAP の MAC アドレス。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。Neighbor 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	Neighbor 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 Neighbor 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。
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。
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。
Clear All	Neighbor アクセスポイントと Neighbor 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。リストは Neighbor が検出されると、再度ポピュレートされます。

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。

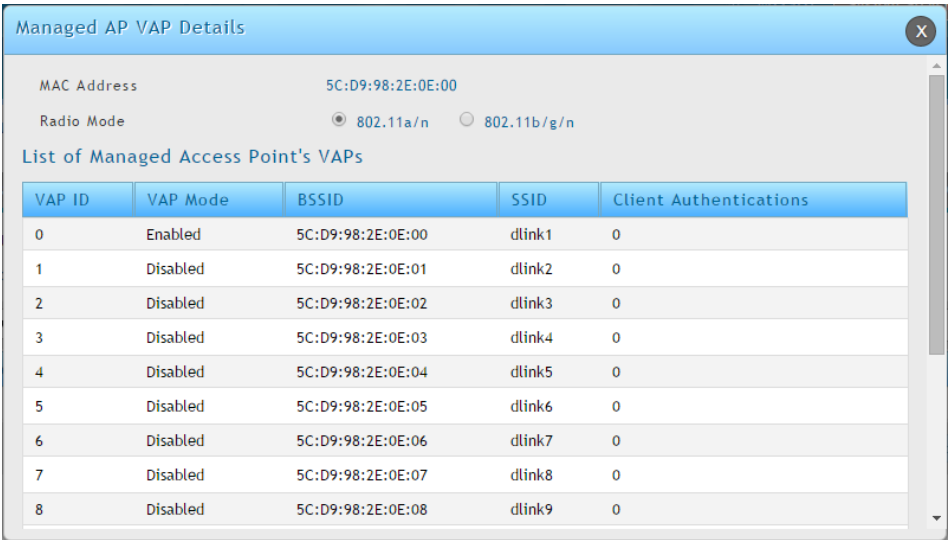


図 8-30 Managed AP VAP Details 画面

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イーサネットアドレス。
Radio Mode	広帯域の無線クライアントと無線ネットワーク要求に適応するために、Radio1 また Radio2 を選択できます。初期値では、Radio1 は IEEE 802.11a/n モードで動作し、Radio2 は IEEE 802.11b/g/n モードで動作します。
List of Managed Access Point's VAPs VAP ID	
VAP を識別するのに使用される 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。
SSID	VAP に割り当てたネットワーク。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きます。
Client Authentications	現在 VAP が認証しているクライアントの合計数。

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。

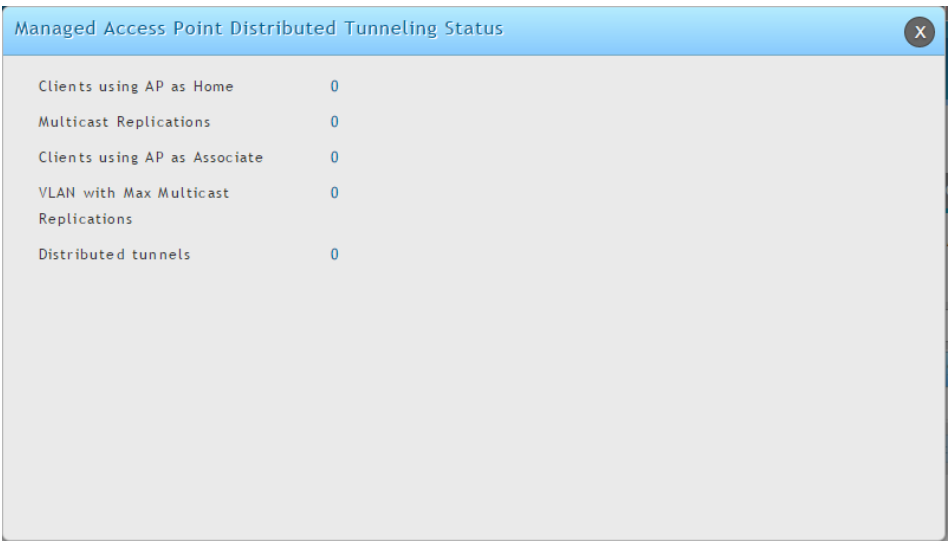


図 8-31 Managed AP Distributed Tunneling Status 画面

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。

項目	説明
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。
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。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。
Multicast Replications	同じ VLAN のメンバであるホーム AP の最大トンネル数。
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。

AP Statistics

「Managed APs List」内のエントリを右クリックして、「AP Statistics」を選択します。



Managed Access Point Statistics Details	
MAC Address	5C:D9:98:2E:0E:00
WLAN Packets Received	2378
WLAN Bytes Received	446866
WLAN Packets Transmitted	14160
WLAN Bytes Transmitted	2541339
WLAN Packets Receive Dropped	0
WLAN Bytes Receive Dropped	0
WLAN Packets Transmit Dropped	0
WLAN Bytes Transmit Dropped	0
Ethernet Packets Received	5017
Ethernet Bytes Received	1045615
Ethernet Packets Transmitted	7545

図 8-32 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。
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。
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)。
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。
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)。
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。
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)。
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。
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)。
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。
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)。
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。
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)。
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。
Total Receive Errors	有線ネットワーク上で検知した受信エラーの数。
Total Transmit Errors	有線ネットワーク上で検知した送信エラーの数。
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。
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。
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。このカウンタは WDS リンクを含みません。それが複数の VAP にブロードキャストされると、同じ ARP フレームが複数の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、「Radio Statistics」を選択します。



図 8-33 Managed Radio Statistics Details 画面

以下の項目があります。

項目	説明
Radio	広帯域の無線クライアントと無線ネットワーク要求に適應するために、2 個の Radio1 また Radio2 を選択できます。
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。
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)。
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。
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)。
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。
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)。
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。
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)。
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。
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。
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。
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。
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。
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。
Failed Transmit Count	MSDU が正しく送信された回数。コントローラの管理下にあるアクセスポイントの統計情報を参照するには、表の上部にあるプルダウンメニューから、アクセスポイントの MAC アドレスを選択します。
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。
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。
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。
ACK Failure Count	想定していた ACK フレームが受信されなかった数。
FCS Error Count	受信した MPDU により検知した FCS エラー数。
Frames Transmitted	送信に成功した MSDU の数。
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。

VAP Statistics

「Managed APs List」内のエントリを右クリックして、「VAP Statistics」を選択します。

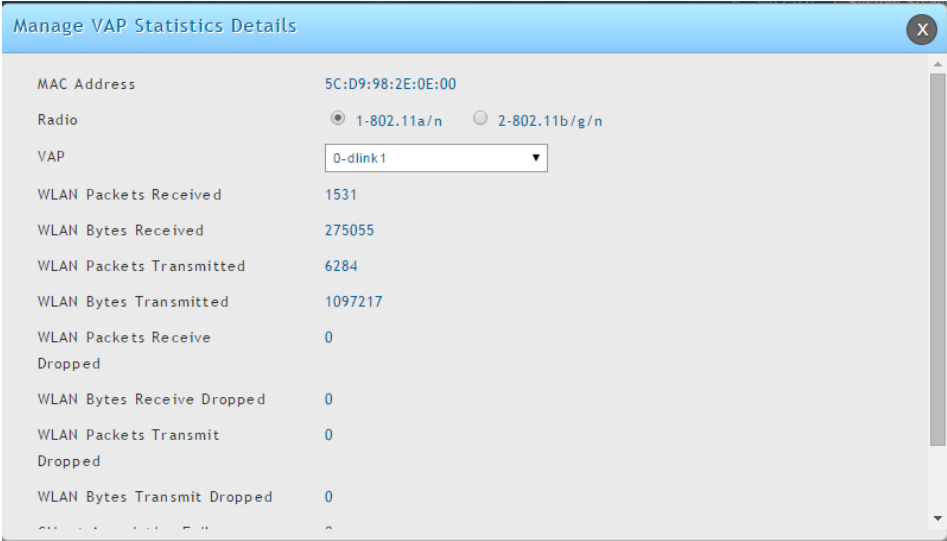


図 8-34 Managed VAP Statistics Details 画面

以下の項目があります。

項目	説明
Radio	広帯域の無線クライアントと無線ネットワーク要求に適応するために、2 個の Radio1 また Radio2 を選択できます。
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。
WLAN Bytes Received	指定した VAP が受信した総データ量。(バイト)
WLAN Packets Transmitted	指定した VAP が送信した総パケット数。
WLAN Bytes Transmitted	指定した VAP が送信した総データ量。(バイト)
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。
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)。
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。
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)。
Client Association Failures	VAP により接続を拒否されたクライアント数。
Client Authentication Failures	VAP への認証に失敗したクライアント数。

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。

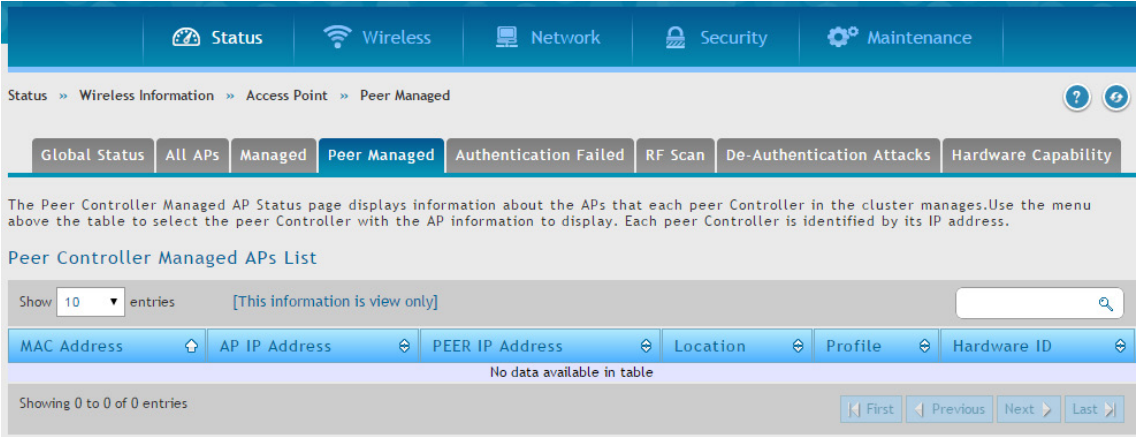


図 8-35 Peer Controller Managed APs List 画面

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。
AP IP Address	アクセスポイントの IP アドレス。
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。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。
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。
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。

Authentication Failed（認証エラー）

Status > Wireless Information > Access Point > 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。

Status > Wireless Information > Access Point > 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。

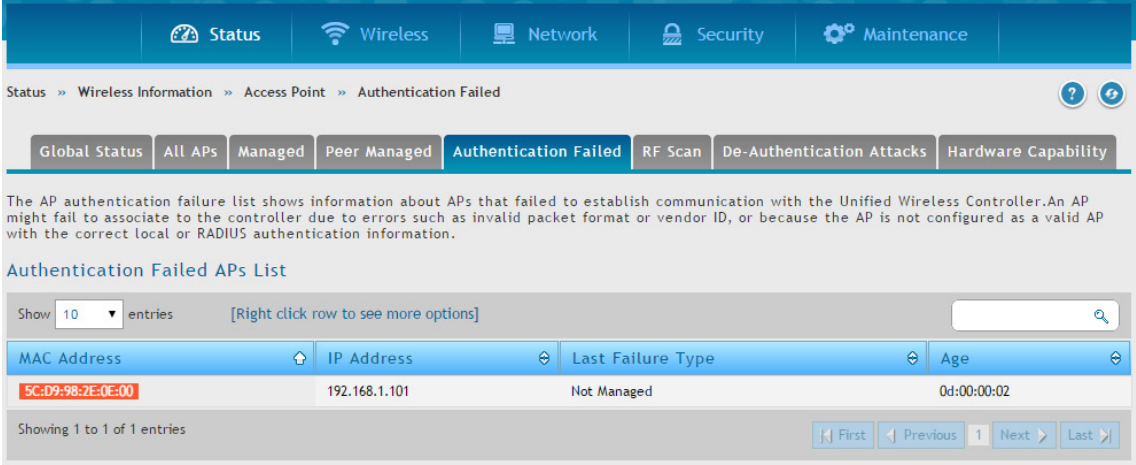


図 8-36 Authentication Failed APs List 画面

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 はスイッチに存在しない可能性があります。これは、ピアコントローラから設定を受信した場合にローカルのデータベースに起こります。
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はありません。

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。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、それはピアコントローラによって報告されます。
IP Address	アクセスポイントの IP アドレス。
Last Failure Type	最後に発生したエラーの種類。 <ul style="list-style-type: none">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 IDProfile Mismatch-Hardware Type - プロファイルが不一致のハードウェアタイプ
Age	エラー発生から経過した時間。

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

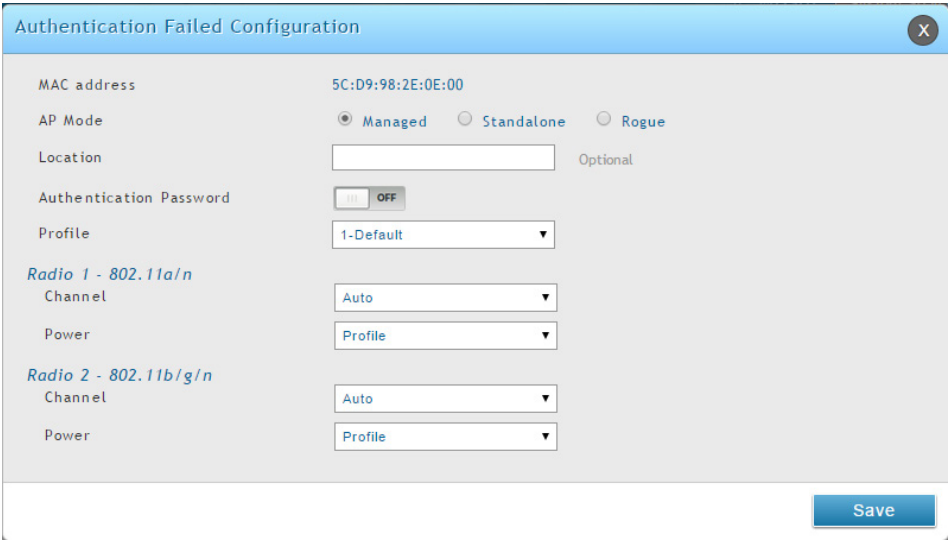


図 8-37 Authentication Failed Configuration 画面

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 8-38 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。
IP Address	アクセスポイントの IP アドレス。
Last Failure Type	発生した最後のエラーのタイプを表示します。 <ul style="list-style-type: none">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 IDProfile 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。
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。
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。

項目	説明
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。
Reporting Controller	認証失敗を報告したコントローラ。
Controller MAC Address	コントローラのイーサネットアドレス。
Controller IP Address	コントローラの IP アドレス。
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。

RF スキャン

Status > Wireless Information > Access Point > RF Scan 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 Scan の順にメニューをクリックし、以下の画面を表示します。

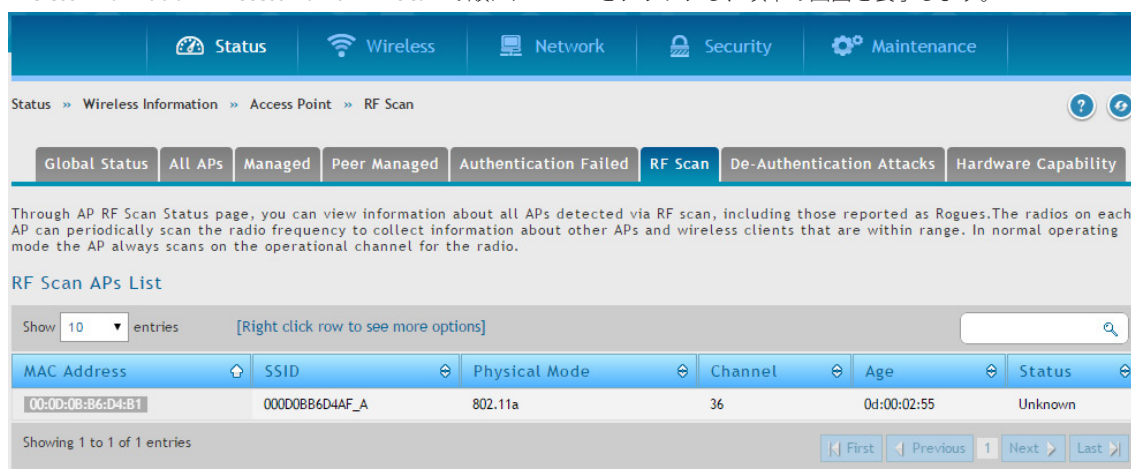


図 8-39 RF Scan APs List 画面

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。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、これは検出されるビーコンフレーム内のブロードキャストです。
Physical Mode	アクセスポイントで使用している 802.11 のモード。
Channel	アクセスポイントの送信チャンネル。
Age	本アクセスポイントが最後に RF スキャンで検出されてから経過した時間。ステータスエントリは、時間内のある時点で収集され、最後に削除されます。各エントリの「Age」値には、無線コントローラがエントリを記録した時間が表示されます。
Status	アクセスポイントの管理状態。 <ul style="list-style-type: none"> Managed - Neighbor 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、詳細を参照するオプションを起動します。

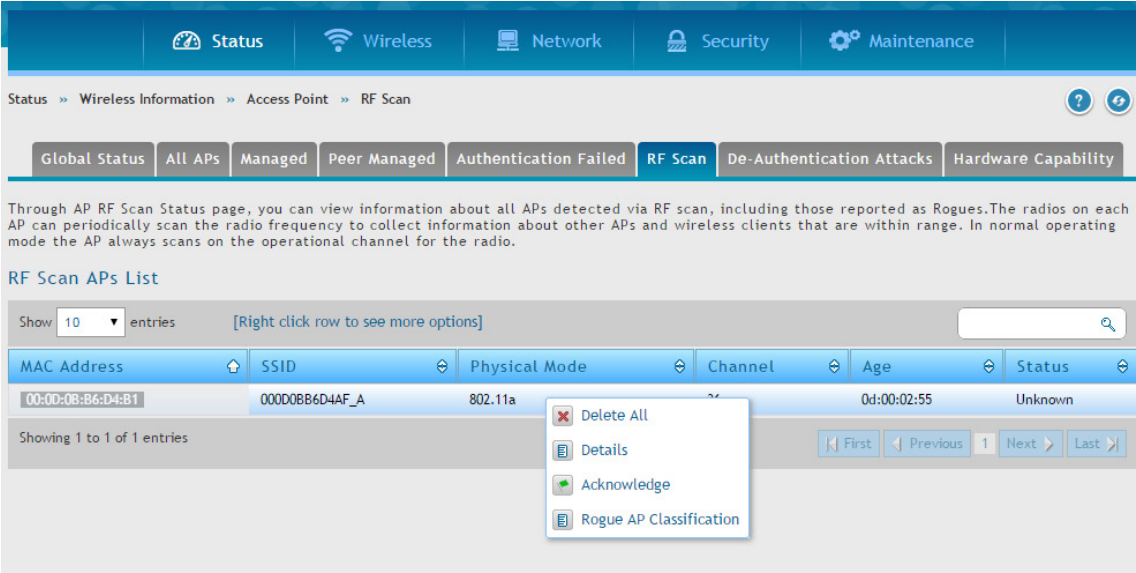


図 8-40 RF Scan APs List 画面 - オプションメニュー

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



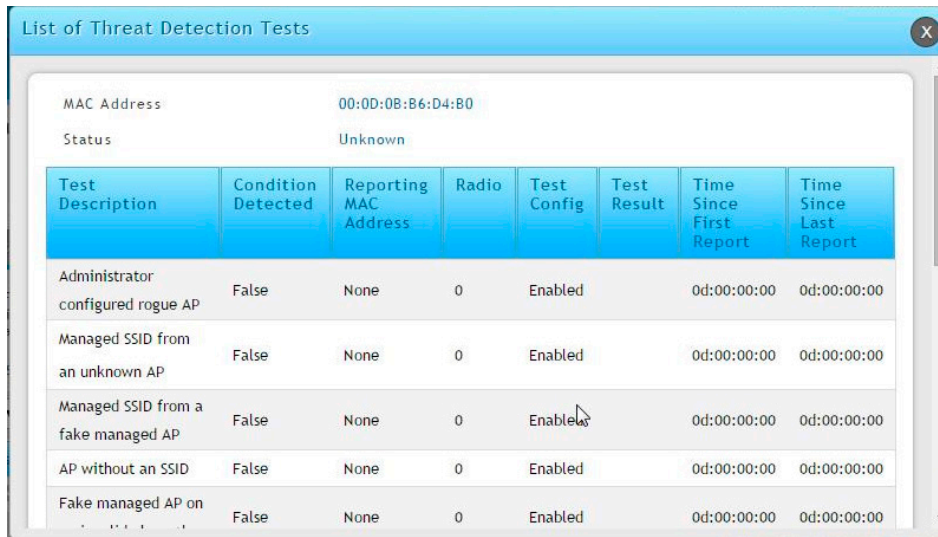
図 8-41 AP RF Scan Details Status 画面

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。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。
SSID	ネットワークの SSID。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。
Security Mode	アクセスポイントが使用するセキュリティモード。

項目	説明
Status	Neighbor 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。 <ul style="list-style-type: none"> Managed - Neighbor 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ければ、初期状態は「Managed」、「Standalone」、または「Unknown」となります。不正なアクセスポイントの初期状態はこのアクセスポイントが不正になる前の分類となります。
Beacon Interval	Neighbor アクセスポイントのネットワークへのビーコン間隔。
Transmit Rate	アクセスポイントの現在の送信速度。
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。レートは、1Mbps ずつ増加して表示されます。
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。

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



Test Description	Condition Detected	Reporting MAC Address	Radio	Test Config	Test Result	Time Since First Report	Time Since Last Report
Administrator configured rogue AP	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
Managed SSID from an unknown AP	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
Managed SSID from a fake managed AP	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
AP without an SSID	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
Fake managed AP on	False	None	0	Enabled		0d:00:00:00	0d:00:00:00

図 8-42 List of Threat Detection Tests 画面

De-Authentication Attacks

Status > Wireless Information > Access Point > De-Authentication Attacks メニュー

認証解除攻撃機能を使用して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するためには、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は、認知されないアクセスポイントは「Rogue」（不正）として分類されないことにご注意ください。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 8-43 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。

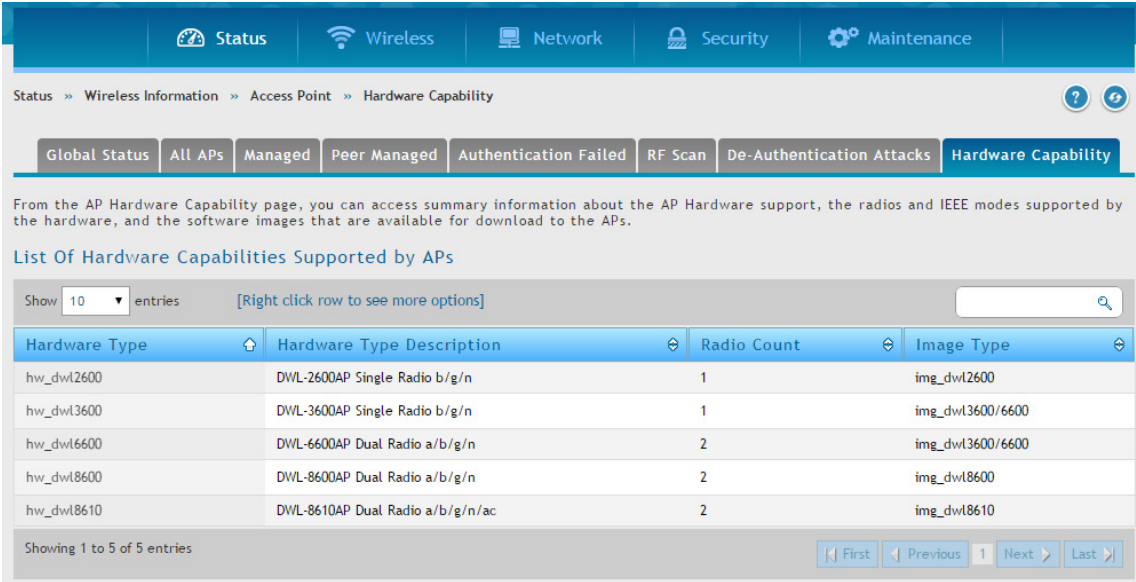


図 8-44 Hardware Capabilities Supported by APs List 画面

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。
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。
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 または 2)。
Image Type	ハードウェアが要求するソフトウェアのタイプ。

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 8-45 AP Hardware Radio Capability 画面

以下の項目があります。

項目	説明
Hardware Type Description	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。
Radio Mode	プラットフォームとサポートしている IEEE 802.11 モード。
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 または 2)。
802.11a Support	IEEE 802.11a モードのサポートが有効かどうか。
Radio Type Description	メーカー名やサポートする IEEE 802.11 モードなどの情報を含む無線帯域のタイプ。
802.11bg Support	IEEE 802.11bg モードのサポートが有効かどうか。

項目	説明
VAP Count	無線インタフェースがサポートする VAP 番号。
802.11n Support	IEEE 802.11n モードのサポートが有効かどうか。
802.11ac Support	IEEE 802.11ac モードのサポートが有効かどうか。

接続クライアントの参照

Status > Wireless Information > Associated Clients メニュー

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。

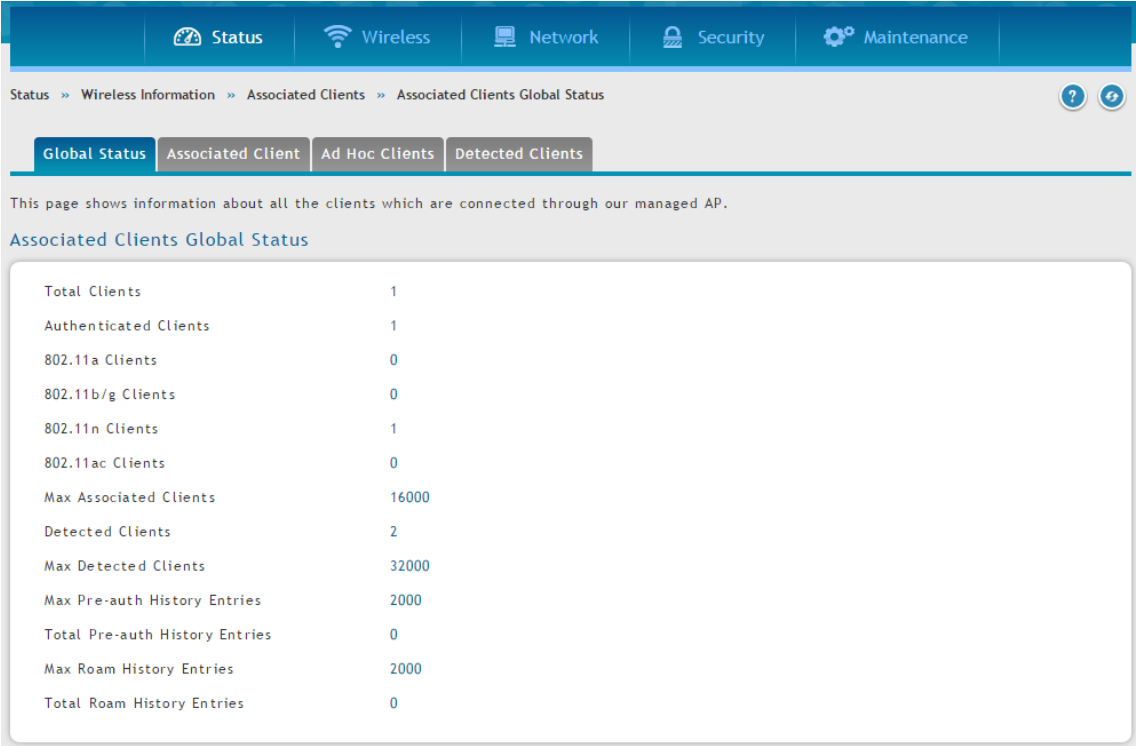


図 8-46 Associated Clients Global Status 画面

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。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。
802.11a Clients	認証された IEEE 802.11a クライアントの総数。
802.11b/g Clients	認証された IEEE 802.11b/g クライアントの総数。
802.11n Clients	認証された IEEE 802.11n クライアントの総数。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。
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。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。
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。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。
Total Pre-auth History Entries	システムで使用中の事前認証ヒストリエントリの現在の数。
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ヒストリに定義できるエントリの最大数。
Total Roam History Entries	システムで使用中の事前認証ヒストリ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。

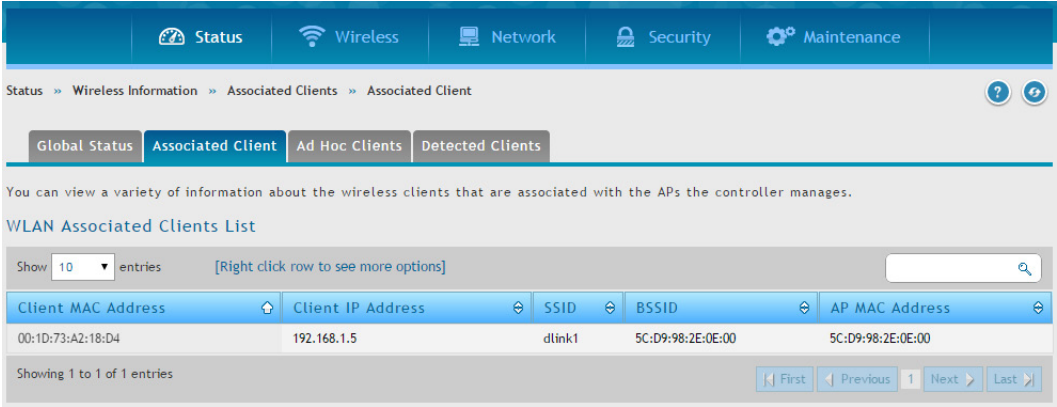


図 8-47 WLAN Associated Clients List 画面

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。
Client IP Address	クライアントステーションの IP アドレス。
SSID	クライアントが接続する無線ネットワークの名前。
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。
AP MAC Address	アクセスポイントのイーサネット MAC アドレス。

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。

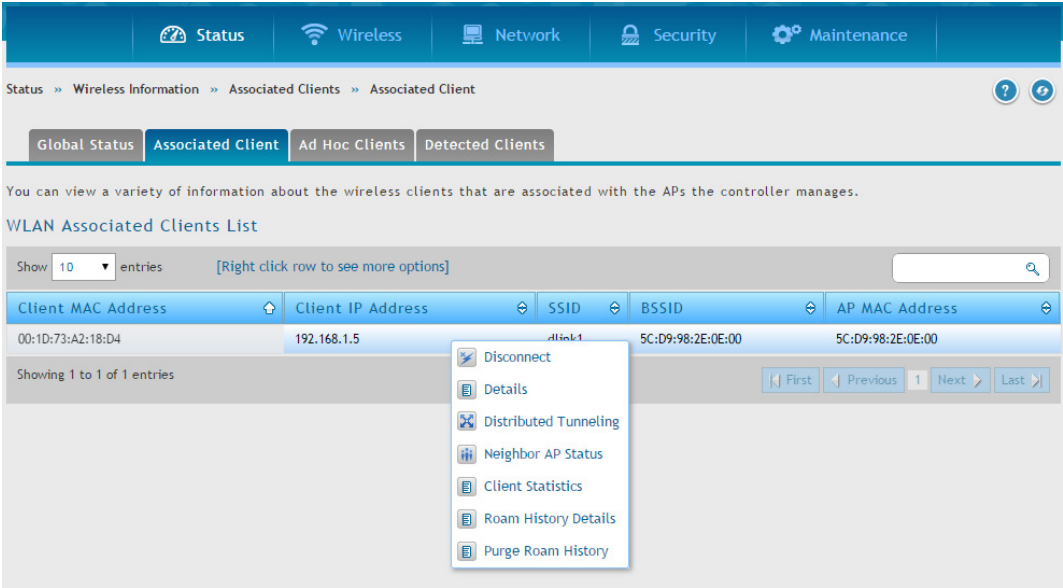


図 8-48 WLAN Associated Clients List 画面 - オプションメニュー

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。
Neighbor AP Status	Neighbor 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	クライアントを接続しており、DWC-1000 が管理する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 8-49 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。
SSID	クライアントが接続しているネットワーク。
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。
AP MAC Address	管理下にあるアクセスポイントの MAC アドレス。
Status	クライアントが接続中であるか、認証されているかを示します。 <ul style="list-style-type: none">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。
User Name	802.1X で認証されたクライアントのユーザ名。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。
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。
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。
NetBIOS Name	無線クライアントの NetBIOS 名。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で管理されているか。
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。
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。
Location	管理下にあるアクセスポイントの場所。
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。
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。
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。
Detected IP Address	必要に応じ、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。

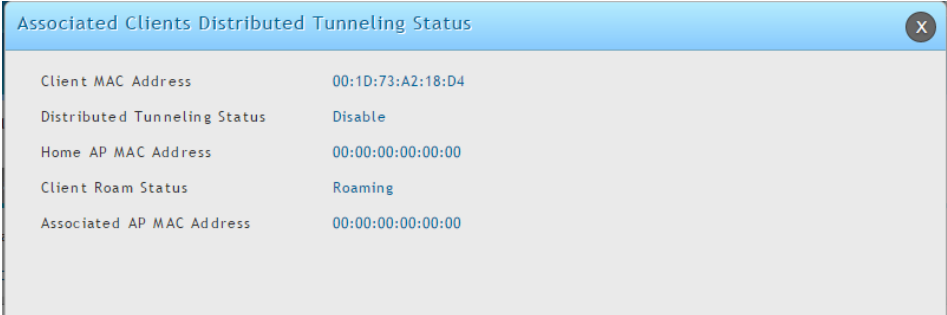


図 8-50 Associated Clients Distributed Tunneling Status 画面

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。
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。
Home AP MAC Address	クライアントに対するホーム AP の MAC アドレス。この値は、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だけに意味があります。
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ています。 <ul style="list-style-type: none">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を「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。

Neighbor AP 情報

クライアントを右クリックし、「Neighbor AP Status」をクリックして、以下の画面を表示します。

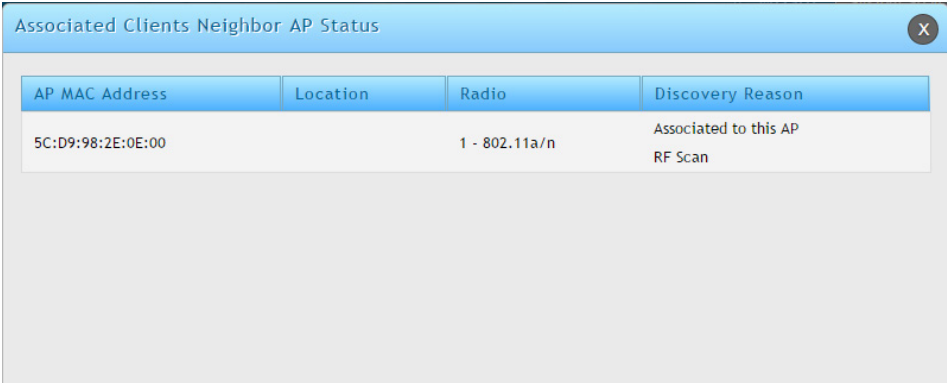


図 8-51 Associated Clients Neighbor AP Status 画面

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。

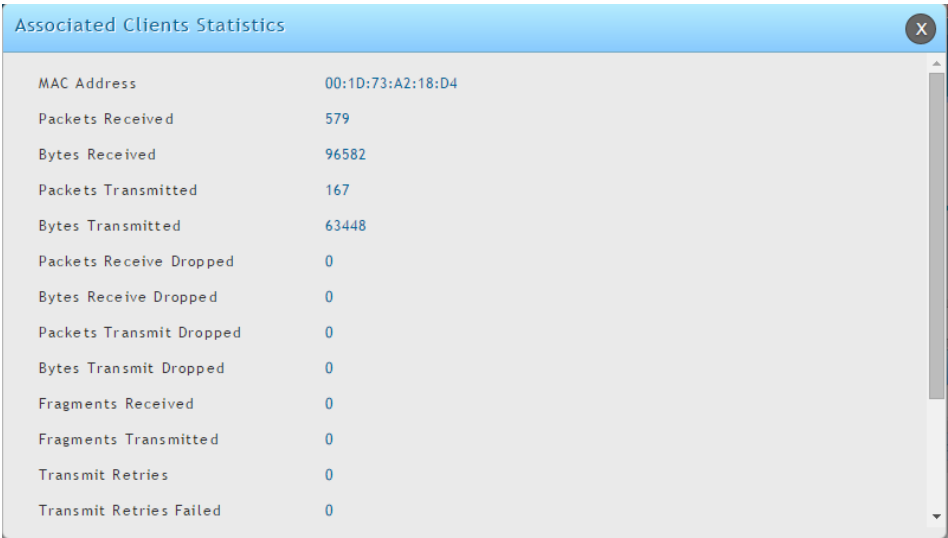


図 8-52 Associated Clients Statistics 画面

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。
Packets Received	クライアントから受信したパケット数の合計。
Bytes Received	クライアントから受信したバイト数の合計。
Packets Transmitted	クライアントに送信したパケット数の合計。
Bytes Transmitted	クライアントに送信したバイト数の合計。
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。
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。
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。
Bytes Transmit Dropped	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。
Fragments Received	クライアントに受信したフラグメント化されたパケット数の合計。
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。
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。
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。
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。
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。
Duplicates Received	クライアントから受信した重複パケットの合計数。

セッションの損失および事前認証を行わずに、認証クライアントのローミングを補助するためには、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。

ローミング履歴の詳細

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。

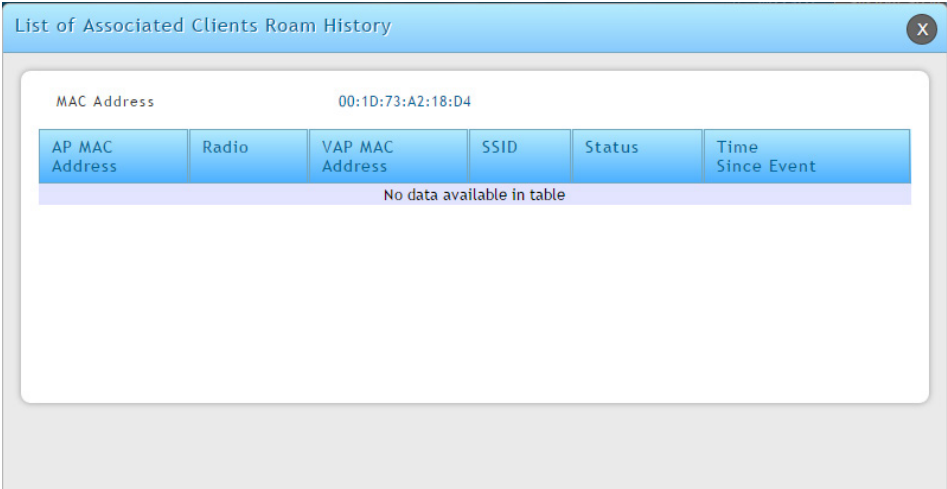


図 8-53 Associated Clients Roam History 画面

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。
AP MAC Address	クライアントを事前認証した管理するアクセスポイントの MAC アドレス。
Radio	クライアントが認証される無線インターフェースの番号。
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。
SSID	VAP が使用される SSID 名。
Status	履歴のエントリが新しい認証またはローミングイベントを示しているかどうかを示すフラグ。
Time Since Event	履歴エントリが追加されてから経過した時間。

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。

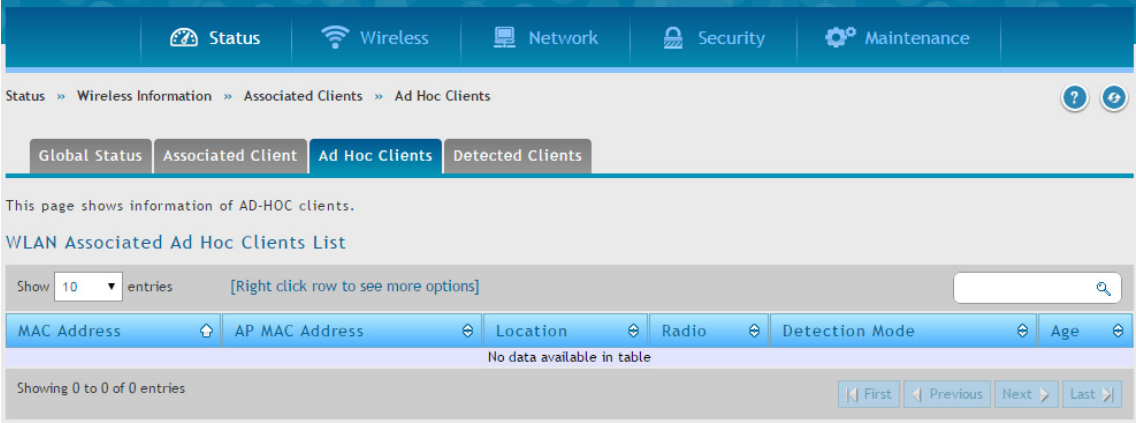


図 8-54 WLAN Associated Ad Hoc Clients 画面

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。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対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。
Location	管理下のアクセスポイントの設定場所の説明。
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。
Detection Mode	アドホックデバイスの検出方式。「Beacon Frame」または「Data Frame」
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。

「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。その 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。その 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。本画面には、離脱して、もうシステムに接続されないクライアントに関する情報などアクセスポイントで認証を行ったクライアントに関する情報を表示します。

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。

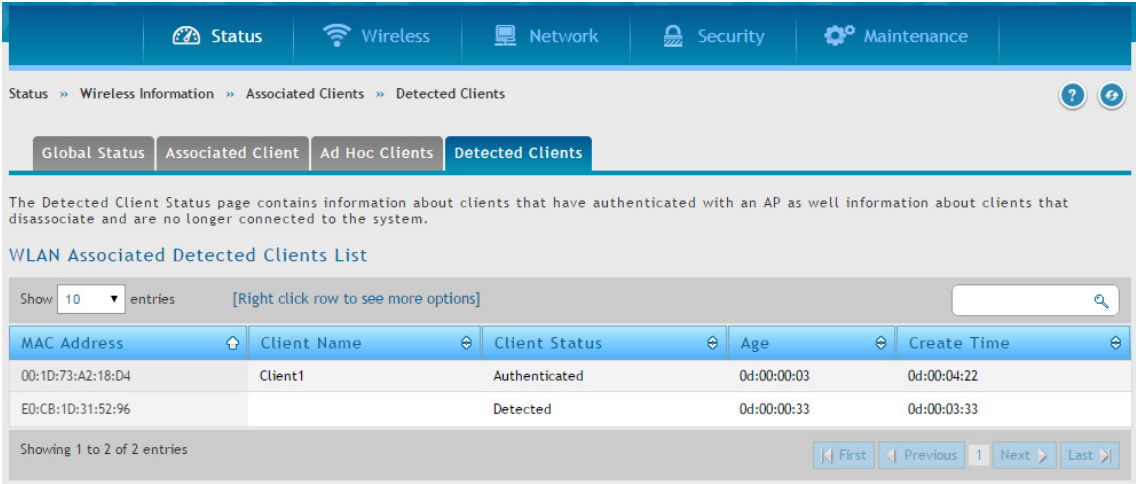


図 8-55 WLAN Associated Detected Clients List 画面

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。
Client Name	「Known Client」データベースにあるクライアントの名称。データベースにクライアントがない場合、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。 <ul style="list-style-type: none">Authenticated - 無線クライアントは無線システムで認証されます。Detected - 無線クライアントは無線システムで検出されますが、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。
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。

「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。

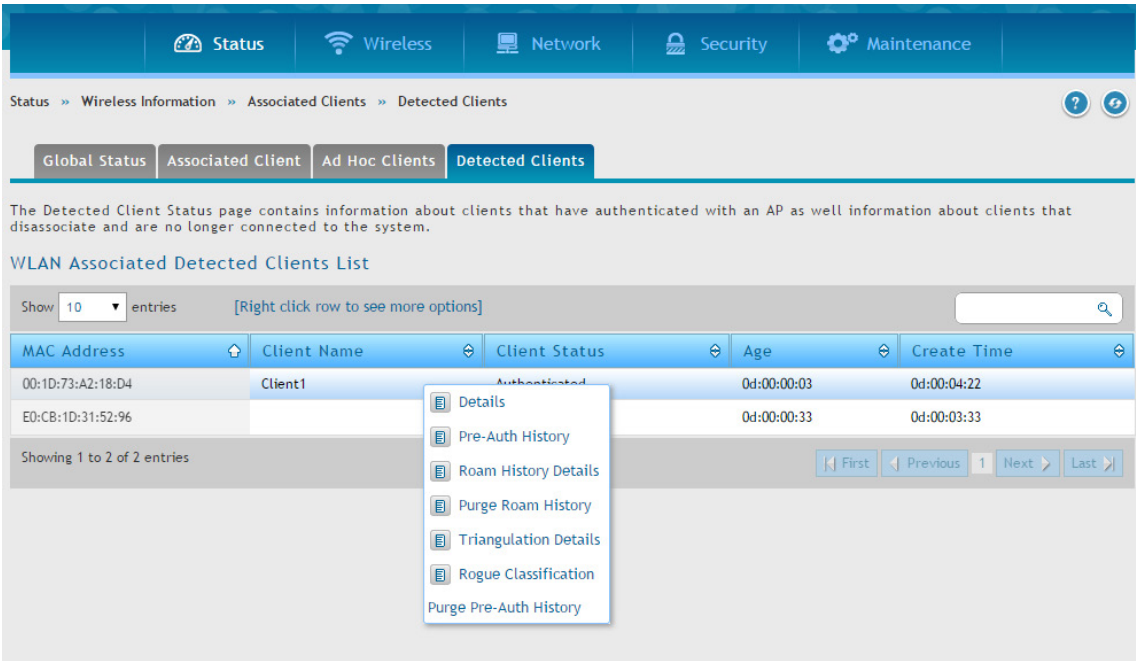


図 8-56 WLAN Associated Detected Clients List 画面 - オプションメニュー

ステータスおよび統計情報

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同様に管理下にある別のアクセスポイントまでローミングした時の記録。最大 10 個のアクセスポイントの履歴が各クライアントのために保持されます。
Purge Roam History	「Roam History」セクションから現在のローミング履歴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 および同じく 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。

Client Statistics（詳細情報）

クライアントを右クリックし、「Client Statistics」を選択して、以下の画面を表示します。



図 8-57 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。
Client Status	クライアントの状態を表示します。 <ul style="list-style-type: none">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すが、認証されず、「Rogue」ではなく、Known Clients データベースでは見つけられません。Known - クライアントは、Known Clients データベースで検出されますが、認証されません。Black Listed - クライアントは、システムに接続しようとしたが、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。 <div>注意 クライアントステータスが「Rogue」（不正）であっても、認証ステータスはまだ「Authenticated」であることもあります。</div>
Threat Detection	脅威検出テストの 1 つがこのクライアントに始動し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か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。
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。
Client Name	必要に応じ、「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)。
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)。
Probe Req Recorded	「Probe Collection Interval」に記録したプローブリクエスト数。

項目	説明
Probe Collection Interval	各プローブ収集に費やした時間。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。
Channel	クライアントが使用しているチャンネル。
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。
Auth Collection Interval	各認証収集に費やした時間。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」に検出した Authentication メッセージの最大数。
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。
De-Auth Collection Interval	各時間が認証解除の収集に費やした時間。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。
est 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。
Authentication Failures	クライアントに検出された 802.1X 認証エラーの数。
Probes Detected	最後の RF スキャンで検出したプローブ数。
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。
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。
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。
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。
Last Directed Probe BSSID	RF スキャンで検出し、最後にダイレクトされたプローブ BSSID。これは MAC アドレスです。
Last Directed Probe SSID	RF スキャンで検出し、最後にダイレクトされたプローブ SSID。
Threat Mitigation Sent	このクライアントに脅威の軽減を行ったか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。

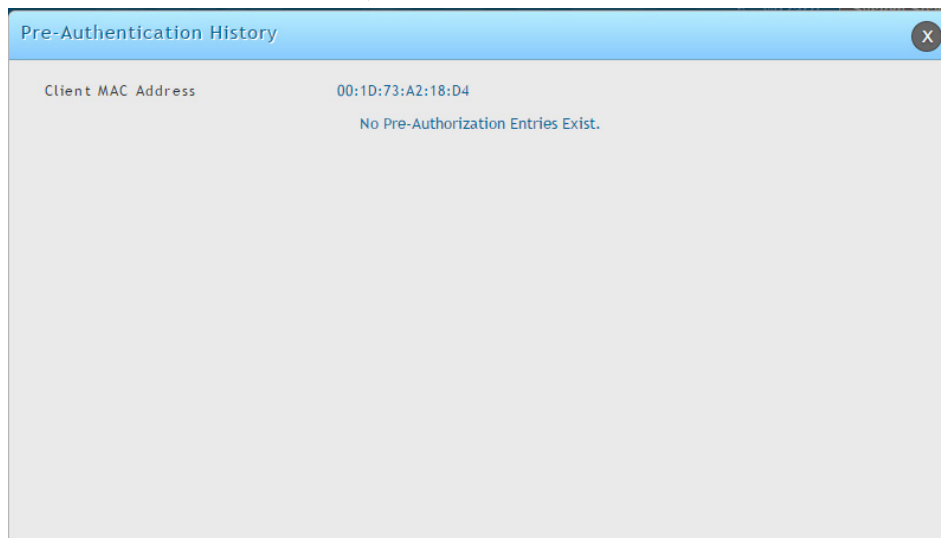


図 8-58 Pre-Authentication History 画面

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。
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。
Radio Interface Number	クライアントが認証される無線インターフェースの番号 (Radio1 または Radio2)。
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。
SSID	VAP が使用される SSID 名。
Age	ヒストリエントリが追加されてから経過した時間。
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。
Pre-Authentication 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。

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。

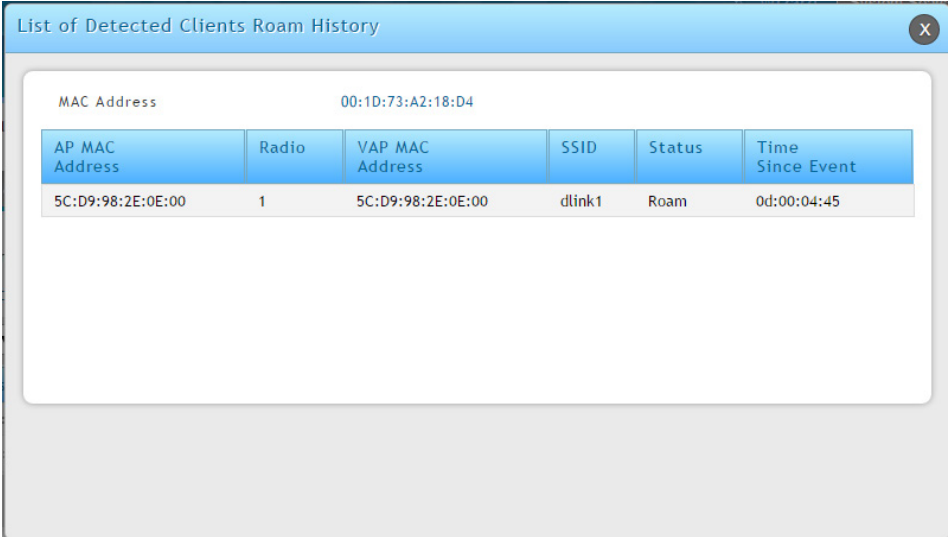


図 8-59 Detailed Clients Roam History 画面

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。
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。
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。
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。
SSID	VAP が使用される SSID 名。
Status	ヒストリのエントリが新しい認証またはローミングイベントを示しているかどうか示すフラグ。
Time Since Event	ヒストリエントリが追加されてから経過した時間。

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。

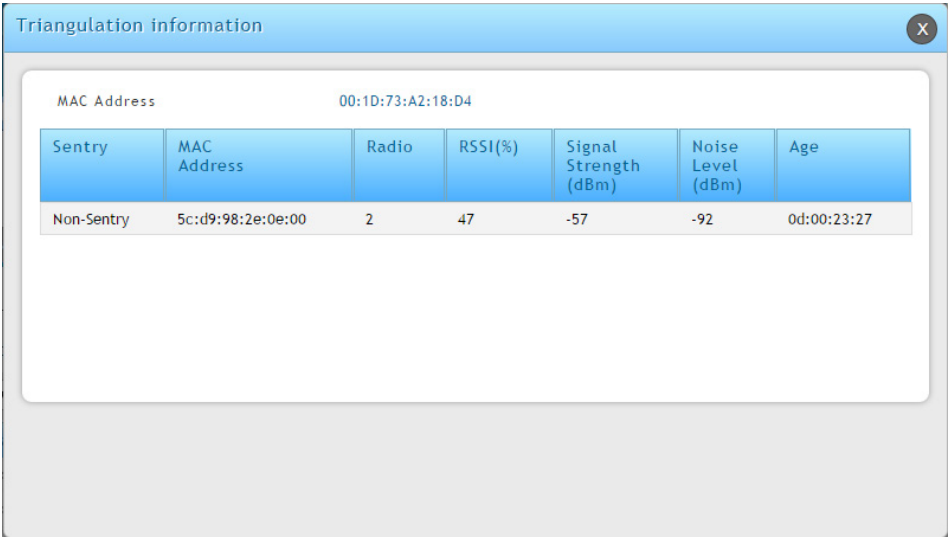


図 8-60 Triangulation Information 画面

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。
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。 <ul style="list-style-type: none">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。

項目	説明
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。
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)。
RSSI	non-sentry AP の受信信号強度 (0-100%)。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)。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)。
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。

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。

Test Description	Condition Detected	Reporting MAC Address	Radio	Test Config	Test Result	Time Since First Report	Time Since Last Report
Known Client Database Test	0	5c:d9:98:2e:0e:0	2	0	0	0d:00:28:45	0d:00:05:18
Client exceeds configured rate for auth msgs	0	5c:d9:98:2e:0e:0	2	1	0	0d:00:28:45	0d:00:05:18
Client exceeds configured rate for probe msgs	0	5c:d9:98:2e:0e:0	2	1	0	0d:00:28:45	0d:00:05:18
Client exceeds configured rate	0	5c:d9:98:2e:0e:0	2	1	0	0d:00:28:45	0d:00:05:18

図 8-61 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。
Test Description	<p>実行されたテストを表示します。</p> <ul style="list-style-type: none"> 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を検出された管理 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が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。
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。
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。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。デバイスはこのモードで動作を許可されているため、いくつかの場合、テストは肯定的な結果を報告するため、有効であり、不正なものとしてレポートされないかもしれません。
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。
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。

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。

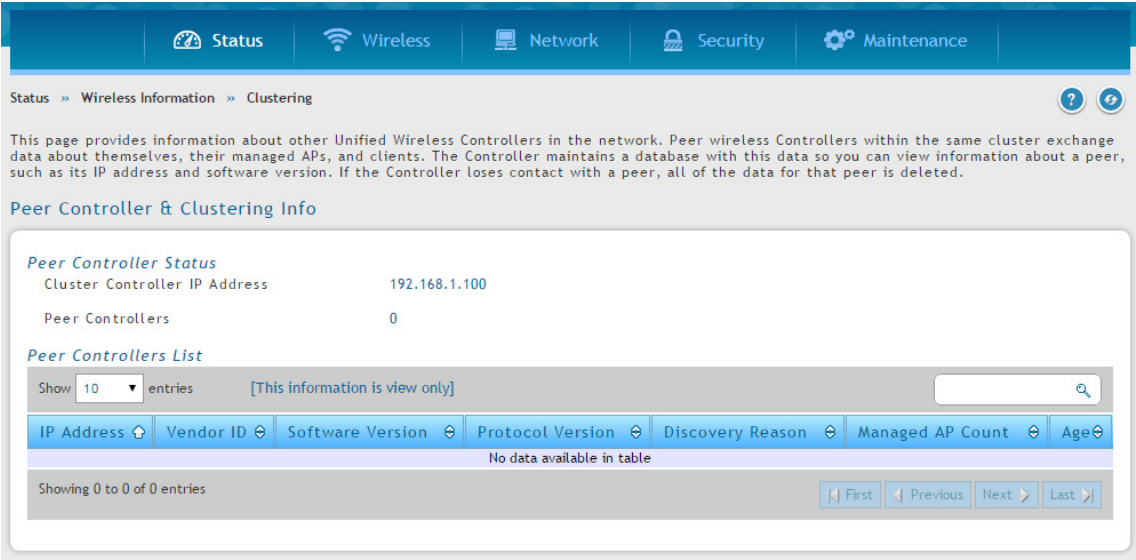


図 8-62 Peer Controller Clustering Info 画面

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。
Peer Controllers	ピアコントローラの数。
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。
Vendor ID	ピアコントローラのソフトウェアのベンダ ID。
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。
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。
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。
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。
Age	無線コントローラとの通信から経過した時間 (時:分:秒)。

WDS グループ状態

Status > Wireless Information > WDS Groups Status メニュー

WDS グループ状態の参照

Status > Wireless Information > WDS Groups Status > WDS Groups Status メニュー

WDS (Wireless Distribution System) は管理対象のアクセスポイントの機能で、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 を使用して、ネットワークへの優先接続ができない屋外や有線ネットワークを使用したメインキャンパスに接続していない離れたビルにアクセスポイントを置くことができます。

- 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。

WDS リンクは、WPA2 Personal 認証と AES 暗号化を使用して守られます。

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** ページを使用します。

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。

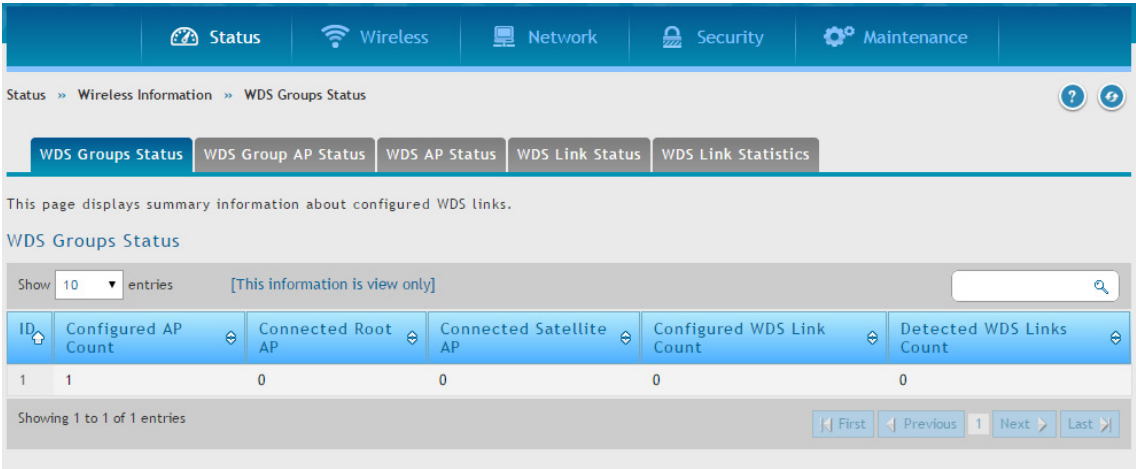


図 8-63 WDS Groups Status 画面

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。
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。
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。
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。
Configured WDS Link Count	WDS AP グループで設定されているリンクの数。
Detected WDS Links Count	システムに検出された WDS リンクの数。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。

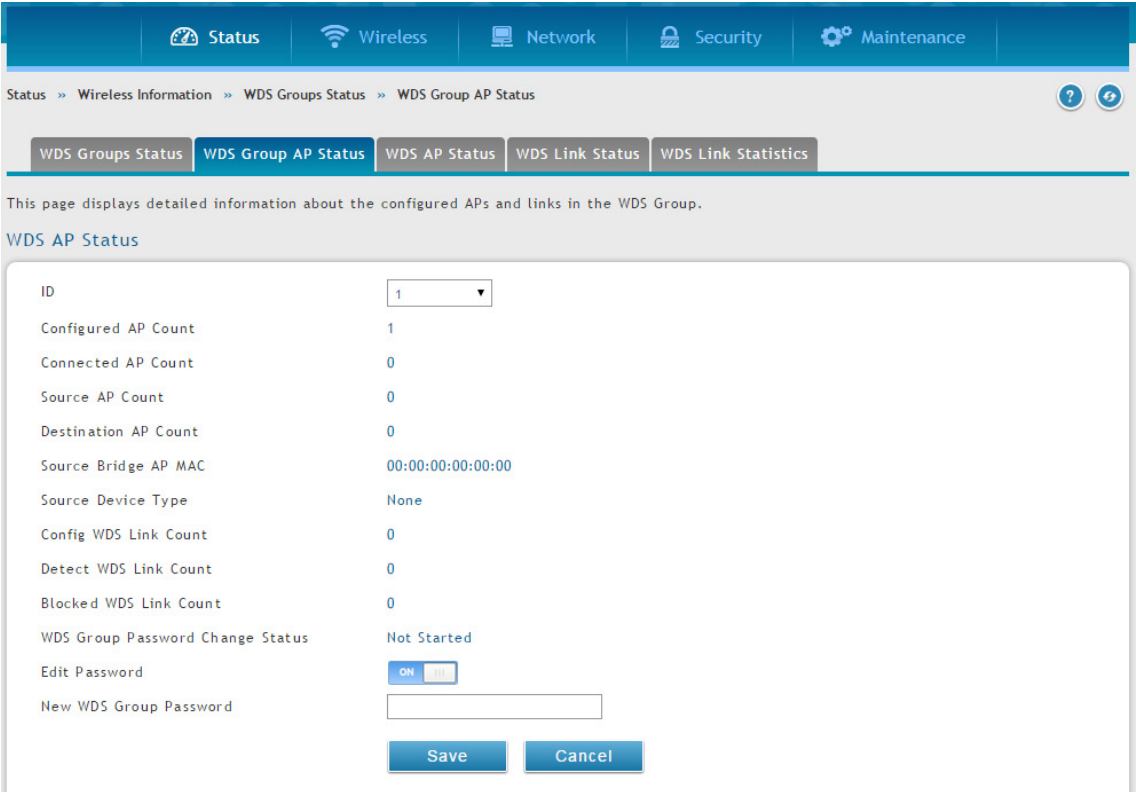


図 8-64 EDS AP Status 画面

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。
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。
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。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。
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。
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。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。 <ul style="list-style-type: none">• 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。
Detected WDS Links Count	システムに検出された WDS リンクの数。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。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、この状態パラメータがそのリンクをカウントします。
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。 <ul style="list-style-type: none">• 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。

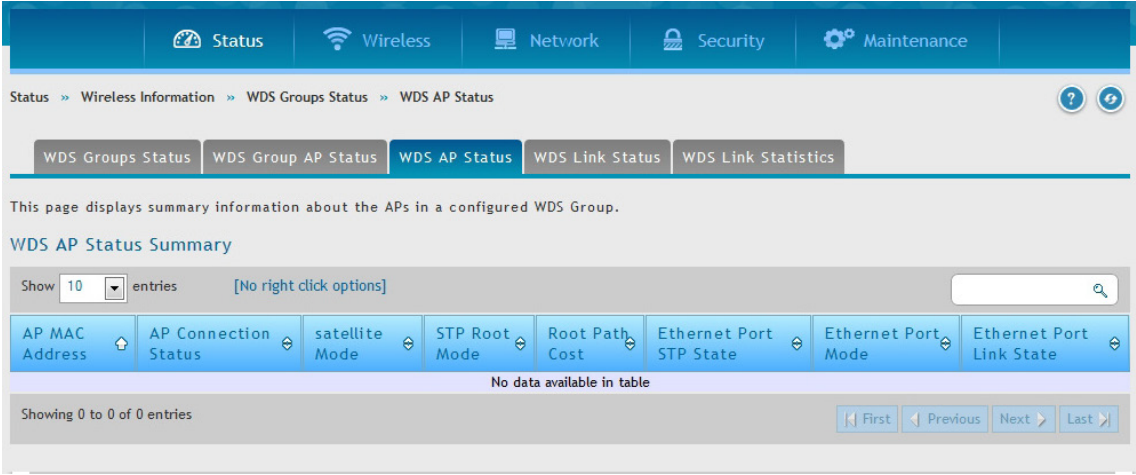


図 8-65 WDS AP Status Summary 画面

以下の項目があります。

項目	説明
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	現在の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すると、値もまた 0 です。
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、この状態パラメータは、イーサネットポートのスパニングツリーの状態を報告します。
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、この状態はポートのリンクステートを報告します。

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。

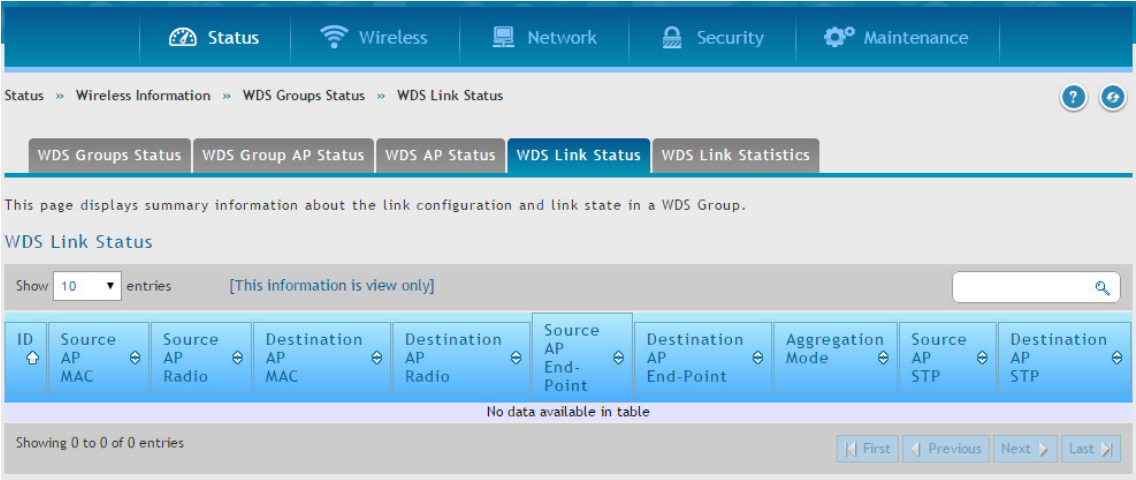


図 8-66 WDS Link Status 画面

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。
Source AP MAC	WDS リンクの片側のエンドポイントの MAC アドレス。
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。
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。
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。
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。
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。
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で、以下の項目の 1 つです。 <ul style="list-style-type: none">• 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で、以下の項目の 1 つです。 <ul style="list-style-type: none">• 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。

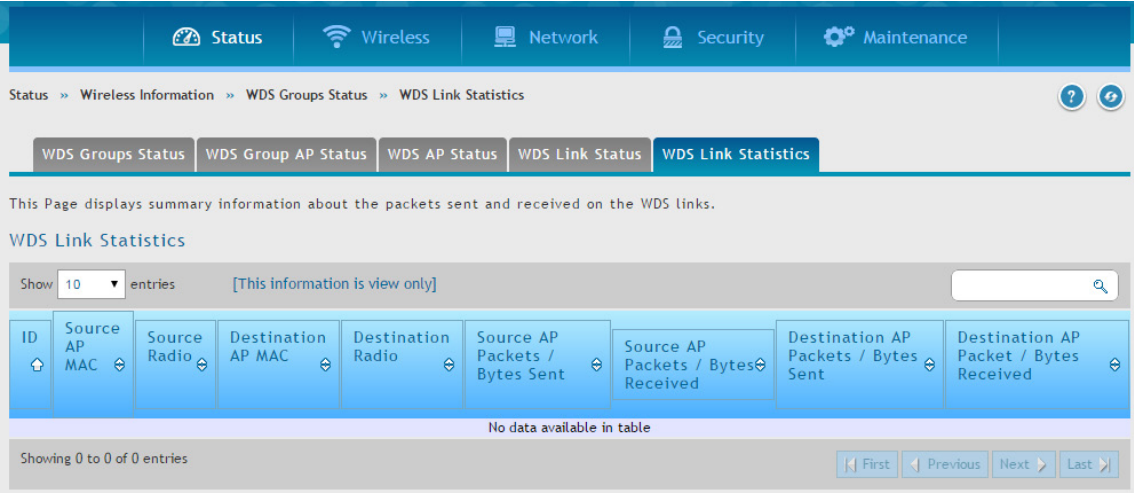


図 8-67 WDS Link Statistics 画面

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。
Source AP MAC	WDS リンクの片側のエンドポイントの MAC アドレス。
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。
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。
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。
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。
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。
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。
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。

第9章 メンテナンス

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	参照ページ
システム設定 (Administration)	コントローラの識別名、日付、セッション、USB 設定を行います。	284
管理設定 (Management)	ライセンスをアクティブ化、無線コントローラのリモート管理、SNMP 設定、コンフィギュレーションの保存と復元を行います。	288
ファームウェア (Firmware)	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。	298
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。	304

システム設定 (Administration)

Maintenance > Administration メニュー

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。

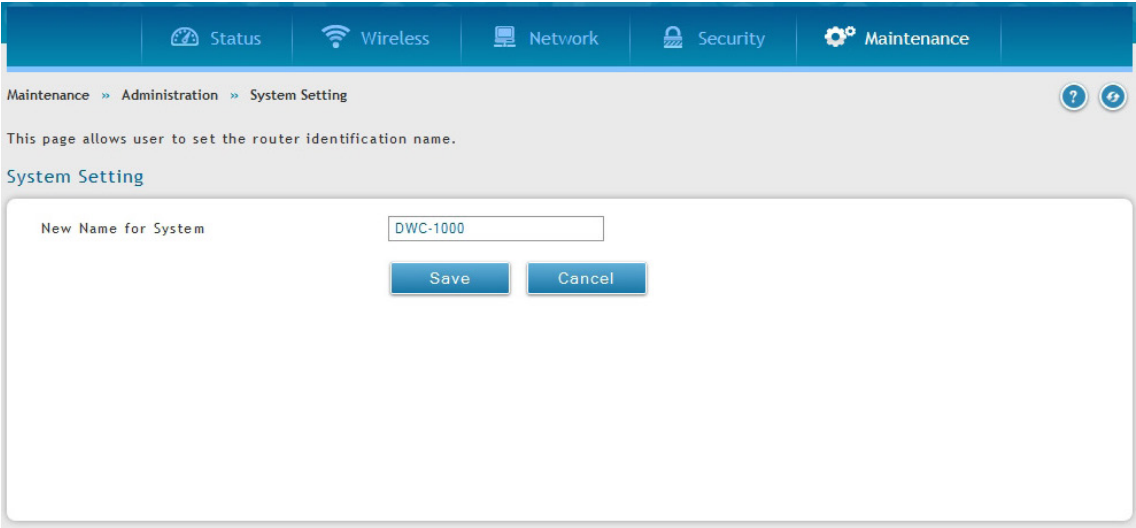


図 9-1 System Setting 画面

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。

The screenshot shows the 'Date and Time' configuration page. The breadcrumb trail is 'Maintenance >> Administration >> Date and Time'. The page title is 'Date and Time'. Below the title, there is a description: 'This page allows us to set the date, time and NTP servers. Network Time Protocol (NTP) is a protocol that is used to synchronize computer clock time in a network of computers. Accurate time across a network is important for many reasons.' The configuration fields are as follows:

- Current Device Time: Sat Nov 01 07:04:30 AM GMT+0900 2014
- Time Zone: (GMT+09:00) Osaka Sappo (dropdown menu)
- Daylight Saving: OFF (toggle switch)
- NTP Servers: ON (toggle switch)
- NTP Server Type: Default (radio button selected), Custom (radio button unselected)
- Time to re-synchronize: 120 (input field), [Default: 120, Range: 5 - 1440] Minutes

At the bottom, there are 'Save' and 'Cancel' buttons.

図 9-2 Date and Time 画面 (NTP サーバタイプが「Default」)

The screenshot shows the 'Date and Time' configuration page with the 'NTP Server Type' set to 'Custom'. The breadcrumb trail is 'Maintenance >> Administration >> Date and Time'. The page title is 'Date and Time'. Below the title, there is a description: 'This page allows us to set the date, time and NTP servers. Network Time Protocol (NTP) is a protocol that is used to synchronize computer clock time in a network of computers. Accurate time across a network is important for many reasons.' The configuration fields are as follows:

- Current Device Time: Sat Nov 01 07:04:30 AM GMT+0900 2014
- Time Zone: (GMT+09:00) Osaka Sappo (dropdown menu)
- Daylight Saving: OFF (toggle switch)
- NTP Servers: ON (toggle switch)
- NTP Server Type: Default (radio button unselected), Custom (radio button selected)
- Primary NTP Server: 0.us.pool.ntp.org (input field)
- Secondary NTP Server: 1.us.pool.ntp.org (input field)
- Time to re-synchronize: 120 (input field), [Default: 120, Range: 5 - 1440] Minutes

At the bottom, there are 'Save' and 'Cancel' buttons.

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。

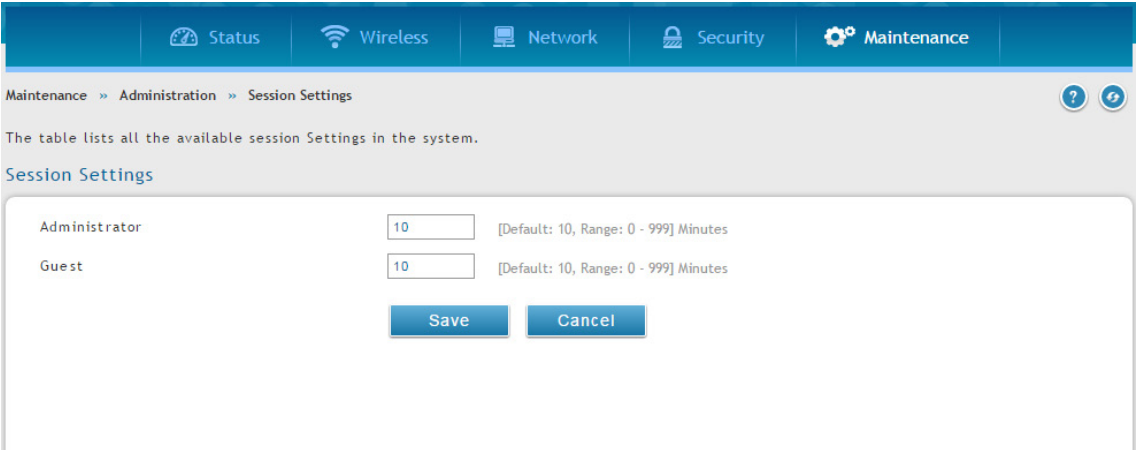


図 9-4 Session Settings 画面

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。

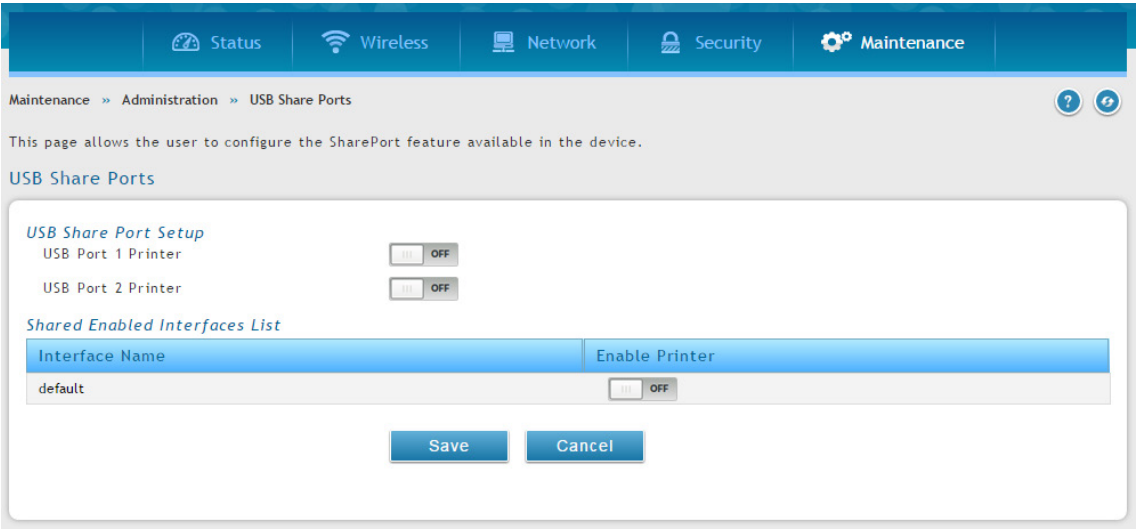


図 9-5 USB Share Ports 画面

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。

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探します。
 - 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 のサイトで登録します。
 - d. アカウントがない場合、新しいアカウントに登録します。
 - e. 自分の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「License Key Activation (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。

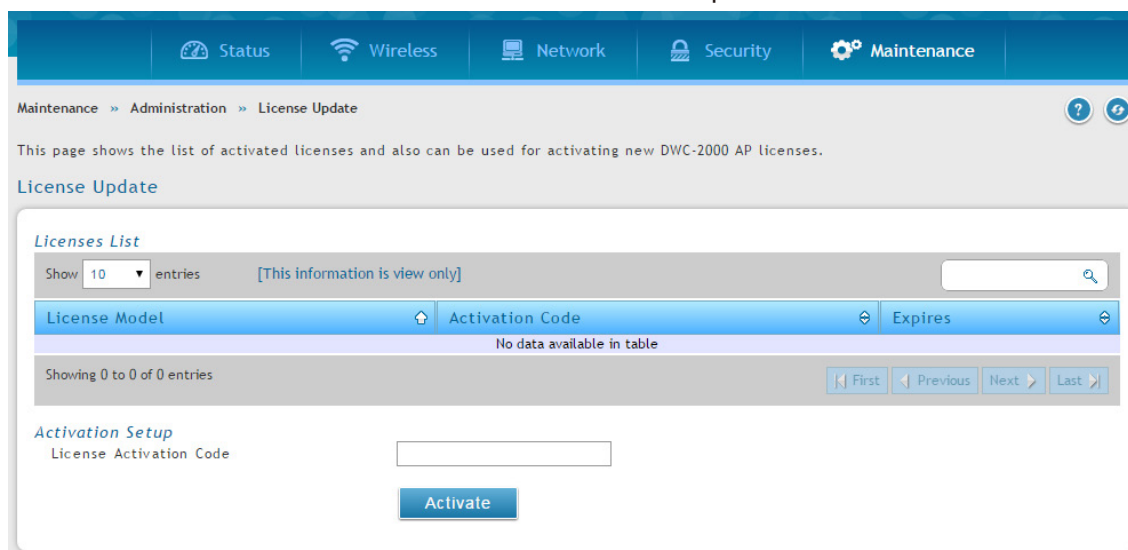


図 9-6 License Update 画面

3. 「Activation Setup」の「License Activation Code」フィールドにアクティブ化したいライセンスに対して D-Link が供給した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は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。(301 ページの「無線コントローラの再起動」参照)

管理設定（Management）

Maintenance > Management メニュー

リモート管理

Maintenance > Management > Remote Management メニュー

ローカルネットワーク外からの無線コントローラのリモート管理を有効にできます。HTTP および / または HTTPS を選択します。

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誰もがコントローラにアクセス可能です。引き続き操作をする前に、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。

注意 本機能は追加ライセンス「DWC-1000-VPN」が有効の場合にのみ利用可能です。

1. Maintenance > Management > Remote 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。

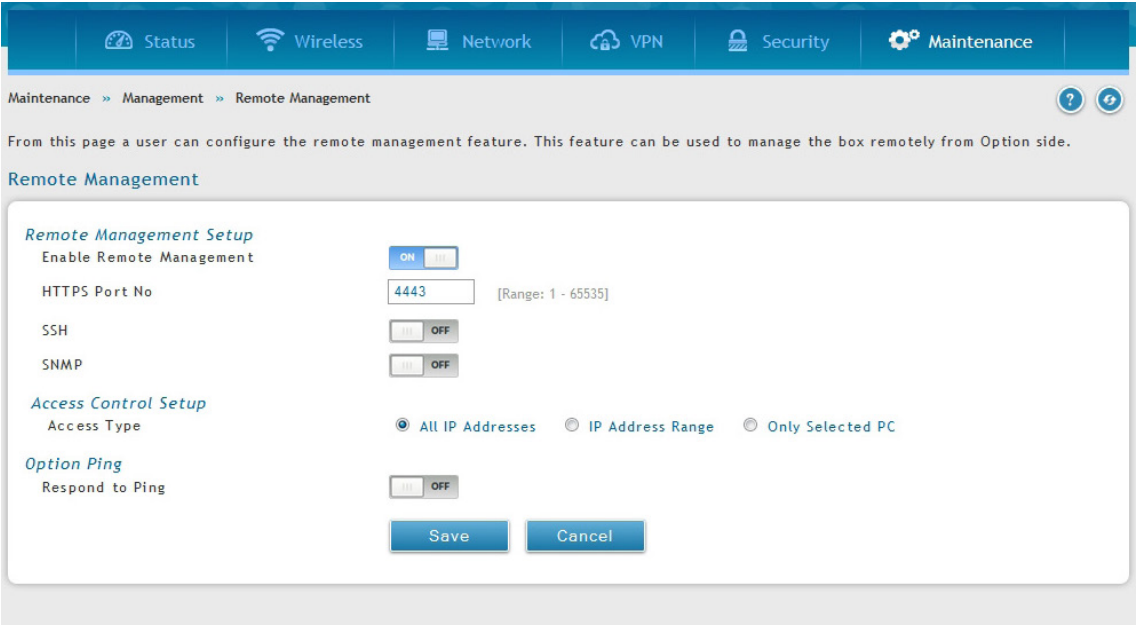


図 9-7 Remote Management 画面

以下の項目があります。

項目	説明
HTTP	有効にすると、HTTP からアクセスできます。
HTTPS	有効にすると、HTTPS からアクセスできます。
HTTPS Port No	HTTPS ポート番号を指定します。

2. HTTP および / または HTTPS を「ON」に設定します。「HTTPS」を選択した場合、ポート番号を入力します。(4443 は初期値)

3. 「Save」ボタンをクリックします。

省エネ設定

Maintenance > Management > Power Saving メニュー

コントローラの電力消費を抑える 2 つのオプションについて説明します。

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

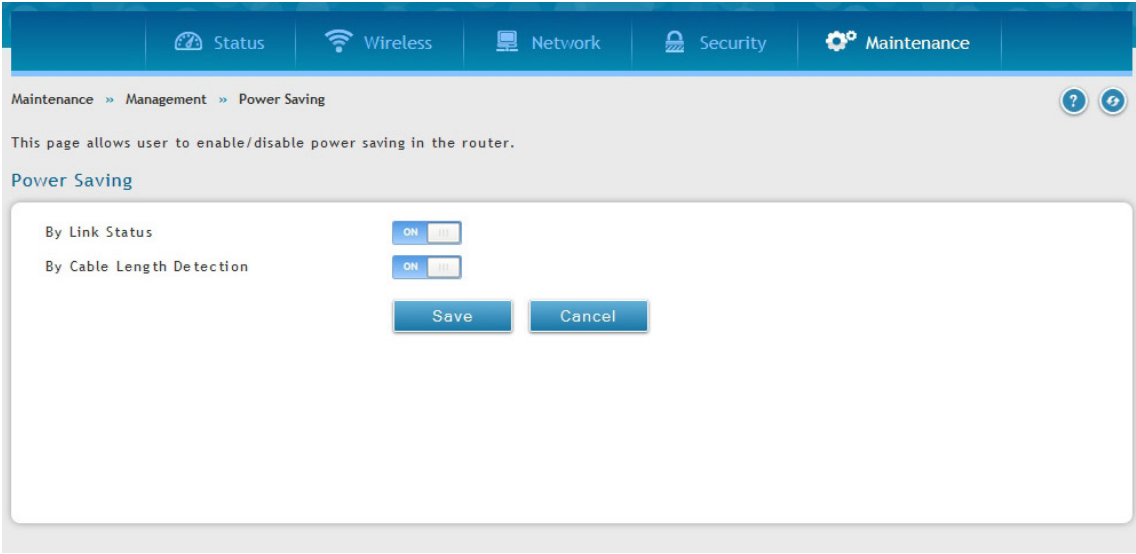


図 9-8 Power Saving 画面

2. 有効にする機能を「ON」に指定します。

項目	説明
By Link Status	有効にすると、コントローラの消費電力は接続したポートの数に依存するようになります。すべての有効な LAN ポートがアクティブなイーサネット接続を行っている状態よりも、単一ポートのみ接続状態にある方が、電力消費を抑えられます。
By Cable Length Detection	有効にすると、コントローラは短いケーブル長に接続した LAN ポートの消費電力を抑えることができます。より長いケーブルの場合、距離のあるパケット送信により多くの抵抗が生じます。このオプションではイーサネットケーブルが 10ft (約 3 メートル) 以下の場合の LAN ポートの消費電力を抑えることができます。

3. 「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のを許可する 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。トラップリストは、このコントローラからの通知が SNMP コミュニティ (マネージャ) に提供されるポートとトラップ用の SNMP バージョン (v1、v2c、v3) について概説します。

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 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。

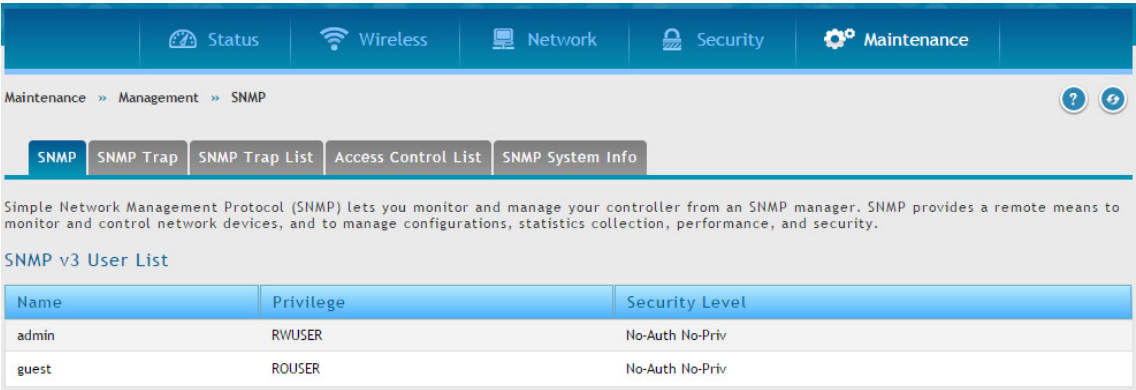


図 9-9 SNMP v3 User List 画面

以下の項目があります。

項目	説明
Name	SNMPv3 マネージャのユーザ名
Privilege	このコントローラへの読取専用 (ROUSER) または読み書き (RWUSER) アクセス権をユーザに割り当てることができます。
Security Level	このユーザの認証とプライバシー設定はここにまとめられます。

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。

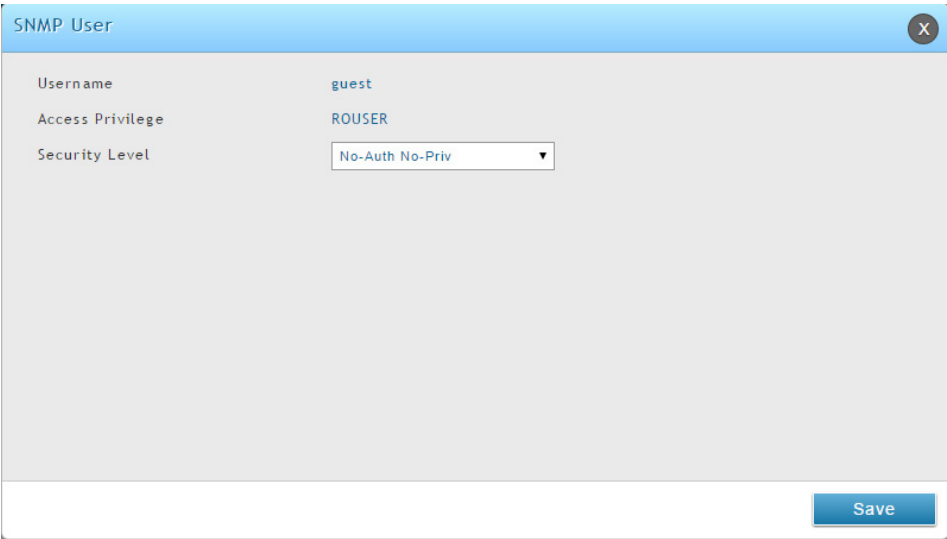
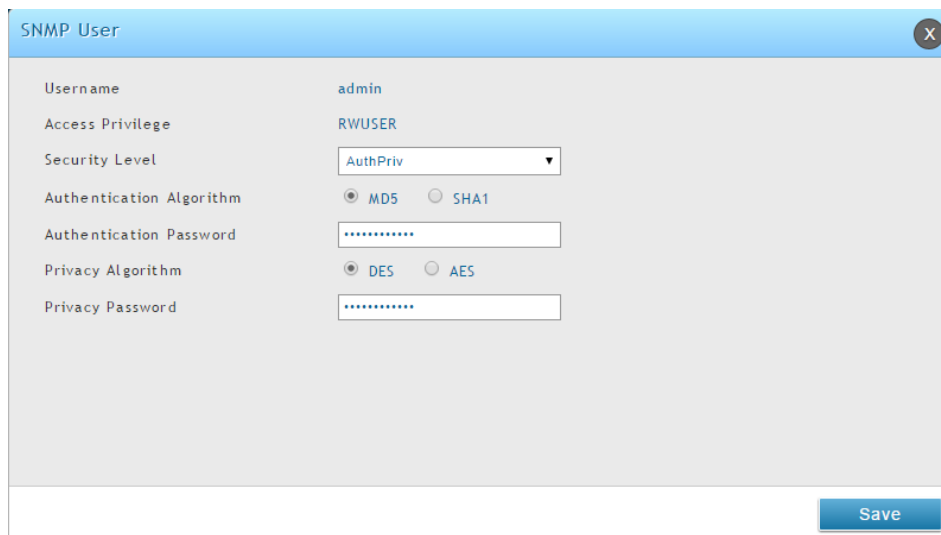


図 9-10 SNMP ユーザ画面 (guest)

以下の項目があります。

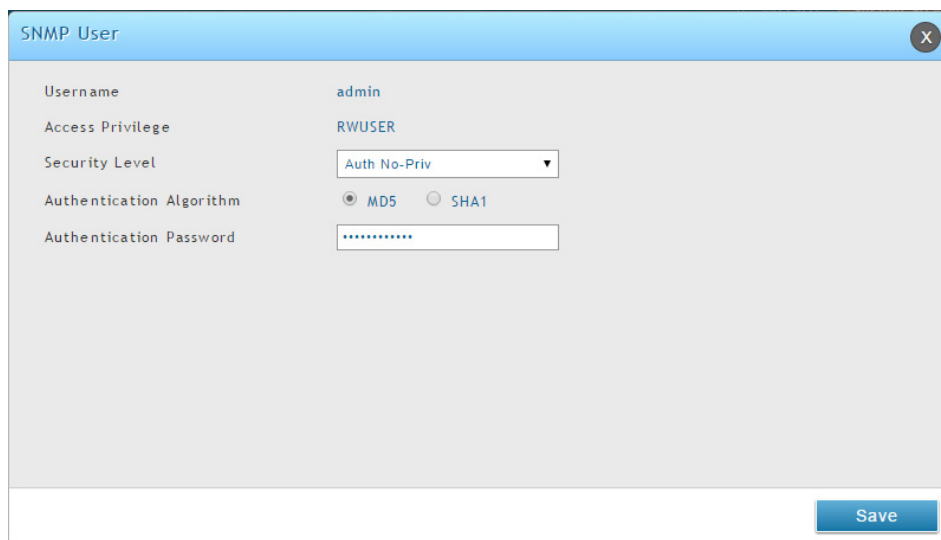
項目	説明
Username	SNMPv3 マネージャのユーザ名
Access Privilege	このコントローラへの読取専用 (ROUSER) または読み書き (RWUSER) アクセス権をユーザに割り当てることができます。

項目	説明
Security Level	<p>このユーザの認証とプライバシー設定を定義します。</p> <ul style="list-style-type: none"> noAuthnoPriv - 認証にユーザ名の一致だけを必要とします authNoPriv - 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をはじめとして MD5 または SHA アルゴリズムに基づいた認証を提供します。 Authentication Algorithm - 認証セキュリティの有効を選択する場合、MD5 または SHA 認証を選択します。 Authentication Password - SNMPv3 ユーザと共有される認証パスワード。 Privacy Algorithm - DES-56 プライバシーは認証ネゴシエーションに有効です。 Privacy Password - SNMPv3 ユーザと共有されるプライバシーパスワード。



The screenshot shows the 'SNMP User' configuration window. The 'Username' is 'admin' and 'Access Privilege' is 'RWUSER'. The 'Security Level' is set to 'AuthPriv' in a dropdown menu. Under 'Authentication Algorithm', the 'MD5' radio button is selected. The 'Authentication Password' field is filled with dots. Under 'Privacy Algorithm', the 'DES' radio button is selected. The 'Privacy Password' field is also filled with dots. A 'Save' button is at the bottom right.

図 9-11 SNMP ユーザ画面 (admin/AuthPriv)



The screenshot shows the 'SNMP User' configuration window. The 'Username' is 'admin' and 'Access Privilege' is 'RWUSER'. The 'Security Level' is set to 'Auth No-Priv' in a dropdown menu. Under 'Authentication Algorithm', the 'MD5' radio button is selected. The 'Authentication Password' field is filled with dots. The 'Privacy Algorithm' and 'Privacy Password' fields are not visible. A 'Save' button is at the bottom right.

図 9-12 SNMP ユーザ画面 (admin/Auth No-priv)

3. セキュリティのレベルを設定します。

項目	説明
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-256 ビットの標準を使用した暗号プライバシーをはじめとして MD5 または SHA アルゴリズムに基づいた認証を提供します。

4. 「Save」ボタンをクリックします。

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 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

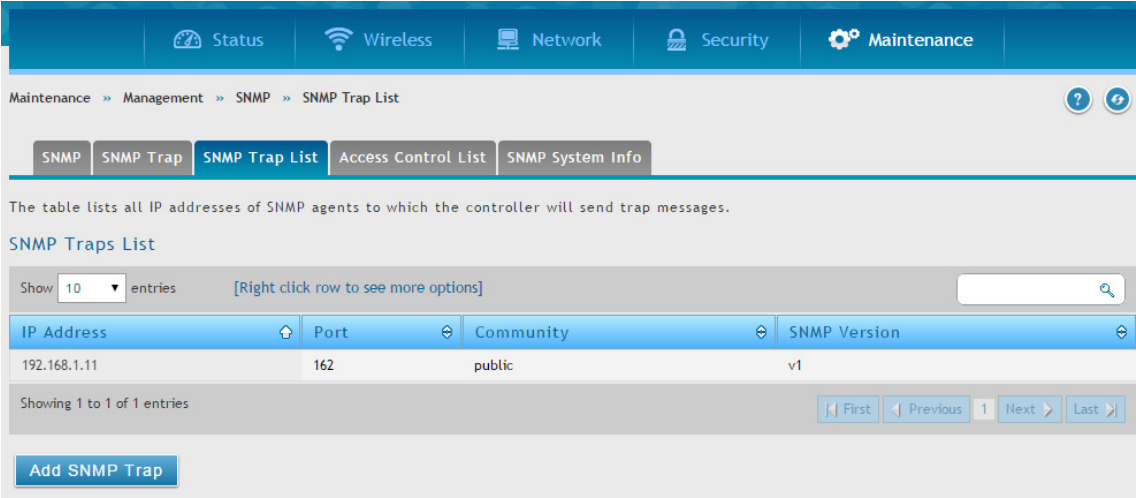


図 9-13 SNMP Traps List 画面

以下の項目があります。

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が送信される 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が、Public コミュニティでトラップにリッスンするように設定されます。
SNMP version	トラップエージェントが使用する SNMP バージョン。

SNMP エージェントに行われるアクションは、以下の通りです。

項目	説明
Edit	「Edit」ボタンは SNMP トラップ設定画面にリンクし、選択した SNMP トラップへの変更を行うことができます。
Delete	選択した SNMP トラップを削除します。
Add SNMP Trap	このボタンをクリックすると、SNMP トラップ設定画面にリンクします。

2. 「Add SNMP Trap」ボタンをクリックします。

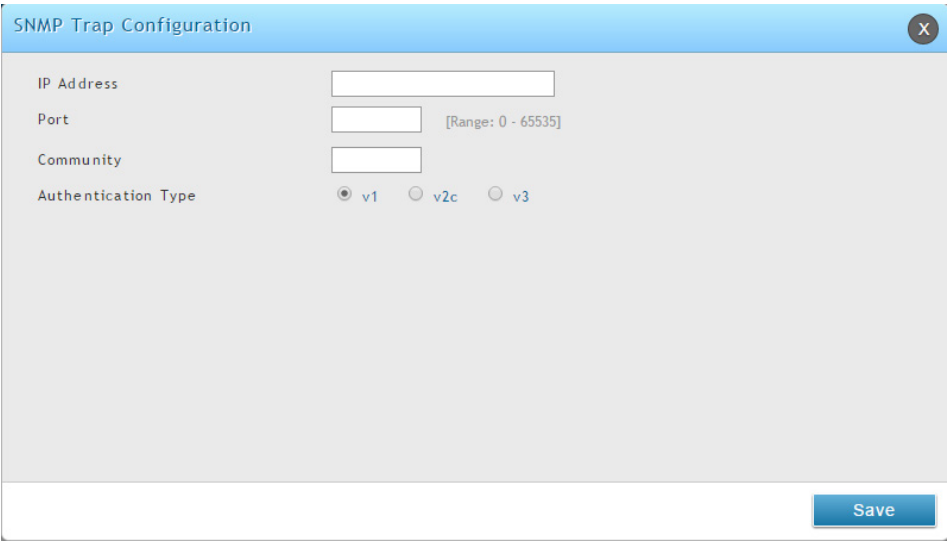


図 9-14 SNMP Trap Configuration 画面

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。

項目	説明
Port	トラップメッセージが送信される 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が、Public コミュニティでトラップにリッスンするように設定されます。
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)。

- 「Save」ボタンをクリックします。

エントリの編集

- 編集するエントリを右クリックし、「Edit」を選択します。
- 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。

- Maintenance > Management > SNMP > Access Control List 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

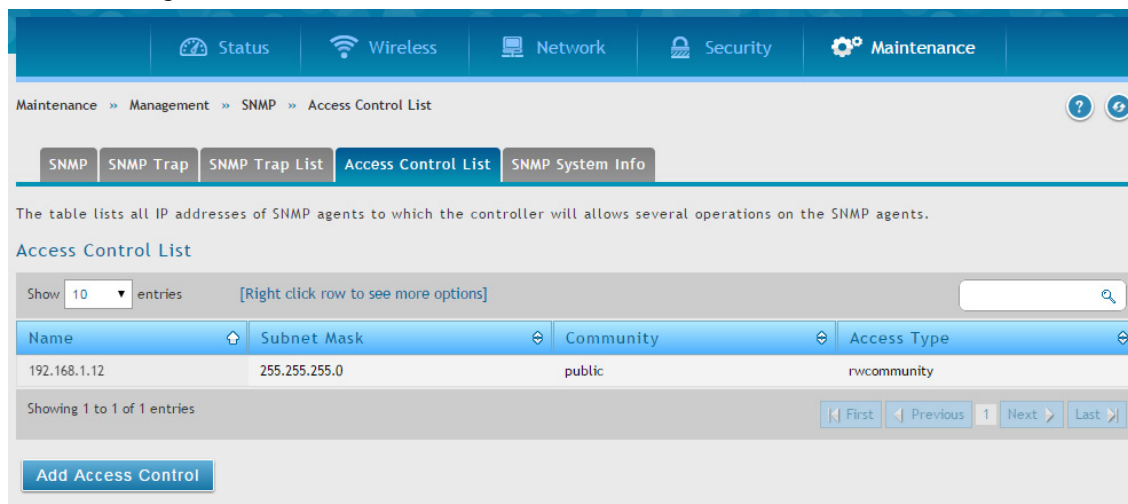


図 9-15 Access Control List 画面

以下の項目があります。

項目	説明
IP Address	SNMP マネージャの IP アドレス。
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。
Community	エージェントが所属するコミュニティストリング。
Access Type	アクセスは読取専用 (rocommunity) または読み書き (rwcommunity) のどちらかです。

SNMP アクセスコントロールリストに行われるアクションは、以下の通りです。

項目	説明
Edit	SNMP ACL 設定画面にリンクし、選択した SNMP ACL への変更を行うことができます。
Delete	選択した SNMP ACL エントリを削除します。
Add Access Control	このボタンをクリックすると、SNMP ACL 設定画面にリンクします。

2. 「Add Access Control」 ボタンをクリックします。

Access Control List

IP Address

Subnet Mask

Community

Access Type

☒ rocommunity

☐ rwcommunity

Save

図 9-16 Access Control List 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。
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。
Community	エージェントが所属するコミュニティストリング。
Access Type	アクセスは読取専用 (rocommunity) または読み書き (rwcommunity) です。

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 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 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

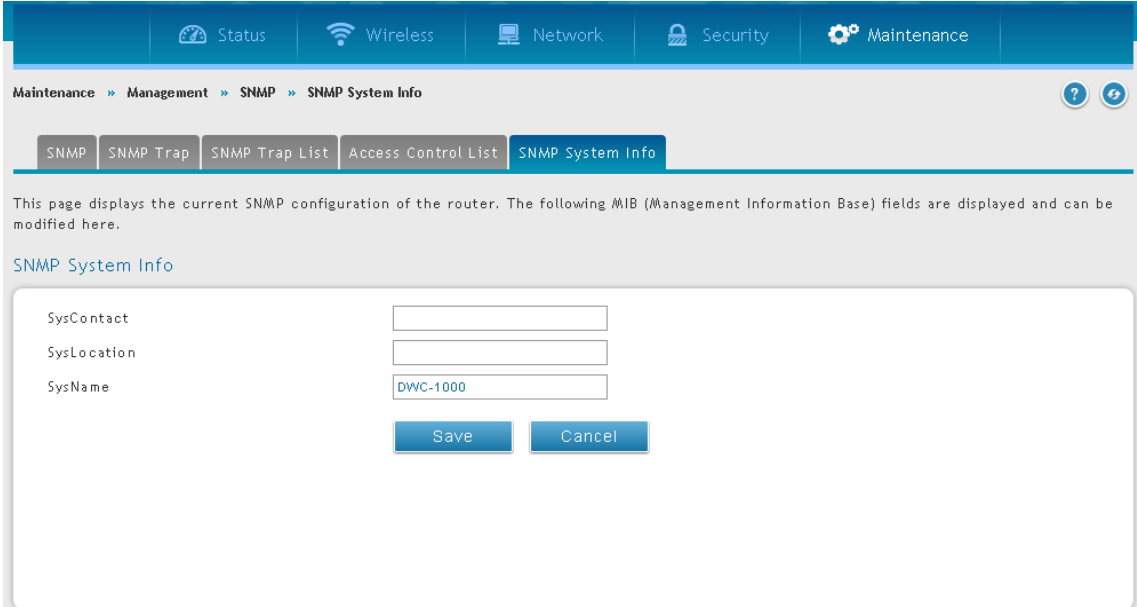


図 9-17 SNMP System Info 画面

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。例 : admin、 John Doe
SysLocation	コントローラの物理的な位置。 例 : Rack#2,4th Floor
SysName	コントローラの簡単な識別名。

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、本ページから使用するネットワークの SNMP マネージャにトラップを送信する必要があります。

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、どんなトラップも送出しません。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 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。

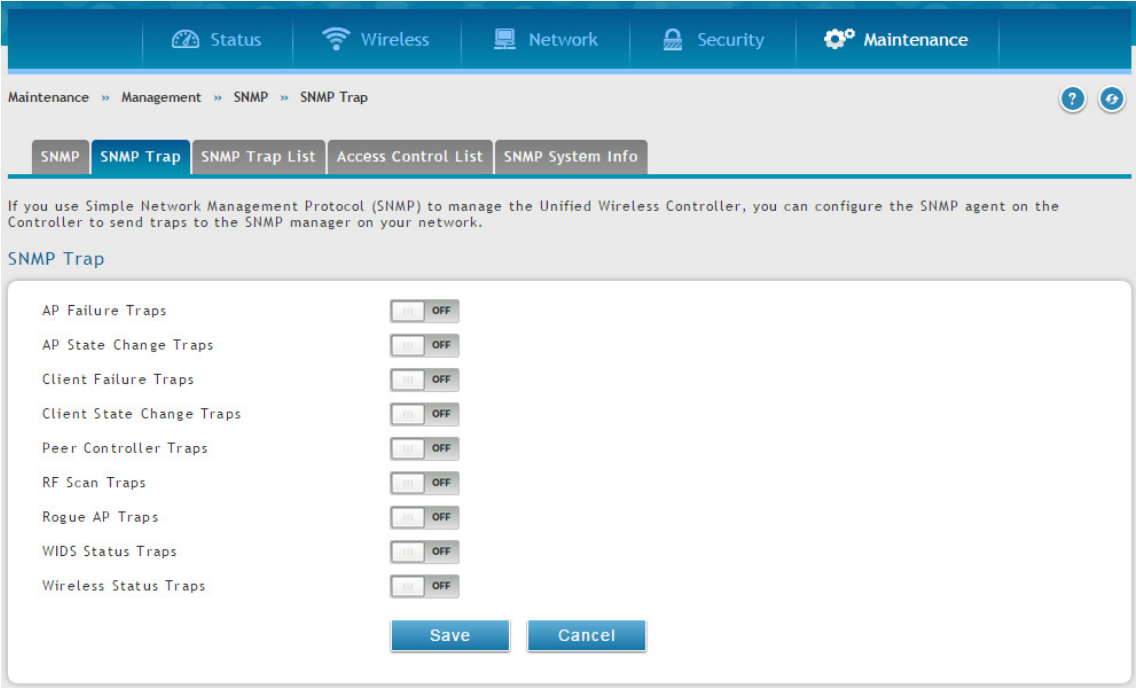


図 9-18 SNMP Trap 画面

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。 <ul style="list-style-type: none">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の検出)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。 <ul style="list-style-type: none">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。 <ul style="list-style-type: none">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の検出)Configuration command received from peer controller (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を必要としません。)
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。
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。

項目	説明
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。 <ul style="list-style-type: none">• 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。 <ul style="list-style-type: none">• 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

3. 「Save」ボタンをクリックします。

ファームウェア (Firmware)

Maintenance > Firmware メニュー

コンフィグレーションの保存と復元

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、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

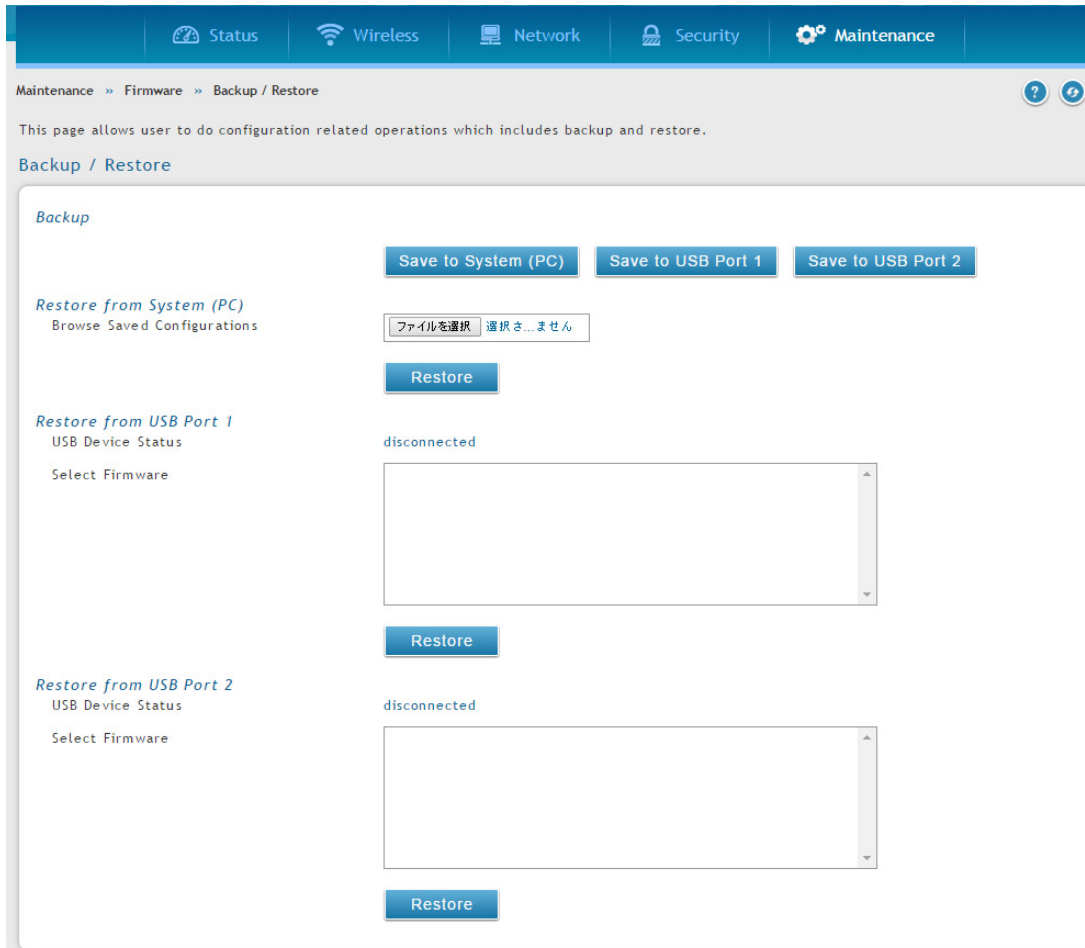


図 9-19 Backup / Restore 画面

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、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、プロンプトを出さずに、直ちに対応する 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 メディアがないと、これらのオプションは何もしません。

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

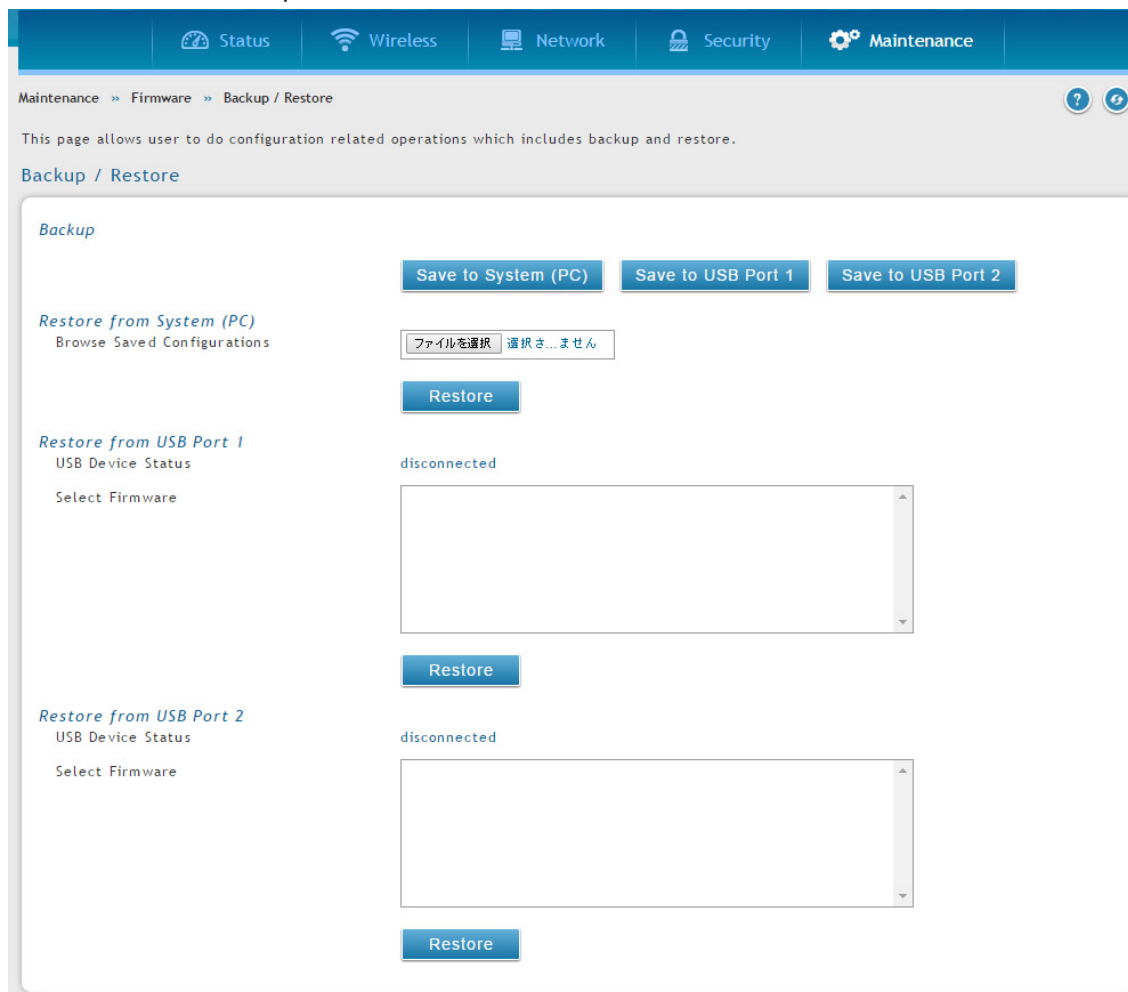
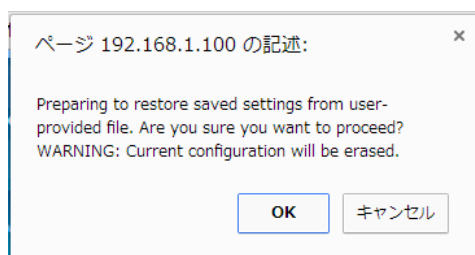


図 9-20 Backup / Restore 画面

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。

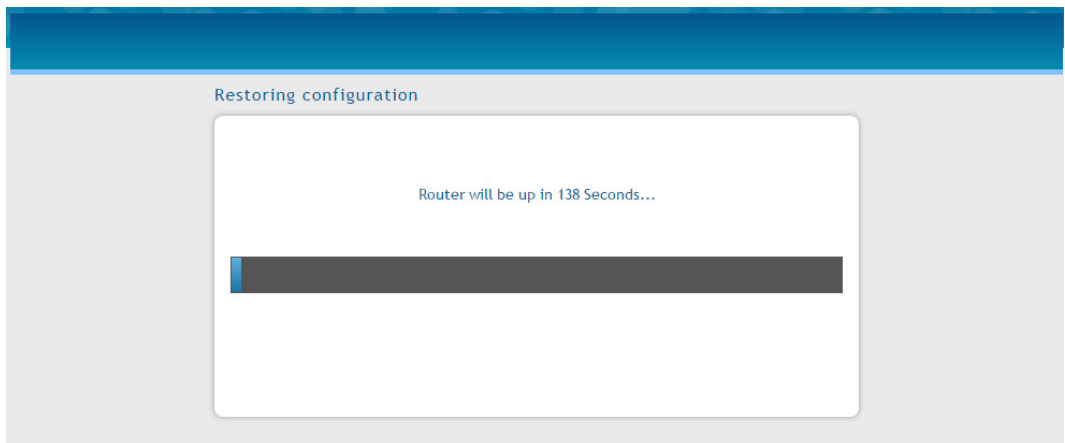


図 9-21 Restoring Configuration 画面

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 > Soft Reboot 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の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背面にあるリセットボタンを使用する。(306 ページの「リセットボタンを使用した、工場出荷時設定の復元」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 > Soft Reboot の順にメニューをクリックし、以下の画面を表示します

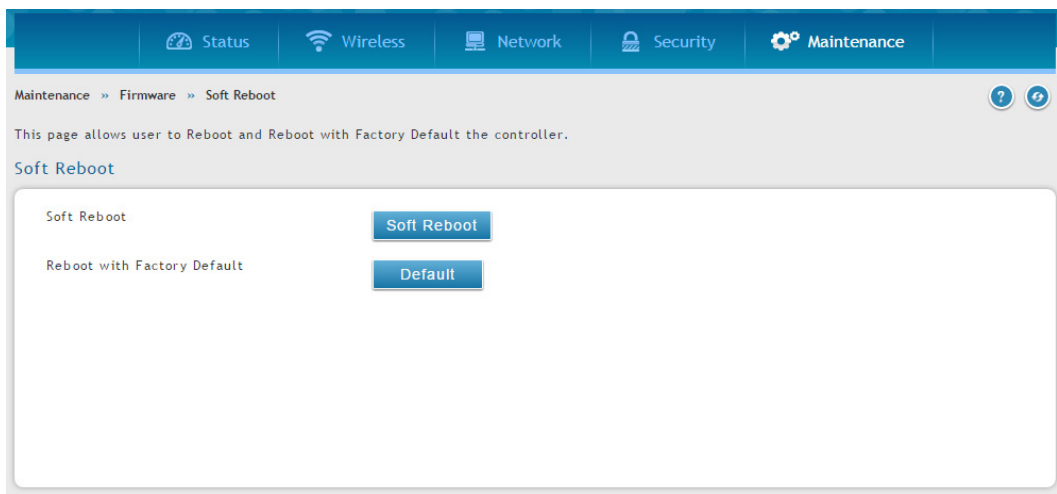
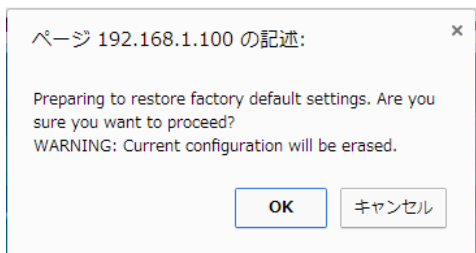


図 9-22 Soft Reboot 画面

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 > Soft Reboot 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 > Soft Reboot の順にメニューをクリックし、以下の画面を表示します。

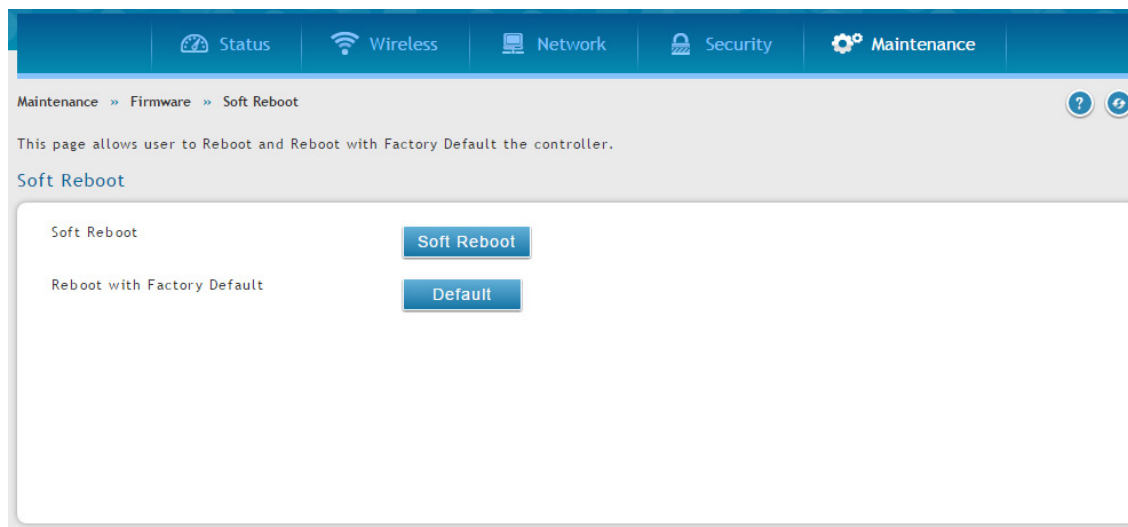
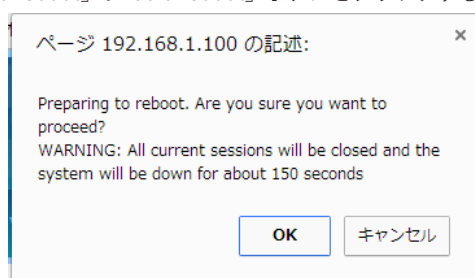


図 9-23 Soft Reboot 画面

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

Maintenance > Firmware > Firmware Upgrade メニュー

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

弊社では、無線コントローラの操作とパフォーマンスを常に向上させています。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を提供します。

無線コントローラのインストール後に、最新のファームウェアであ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、利用可能になれば、それらを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。

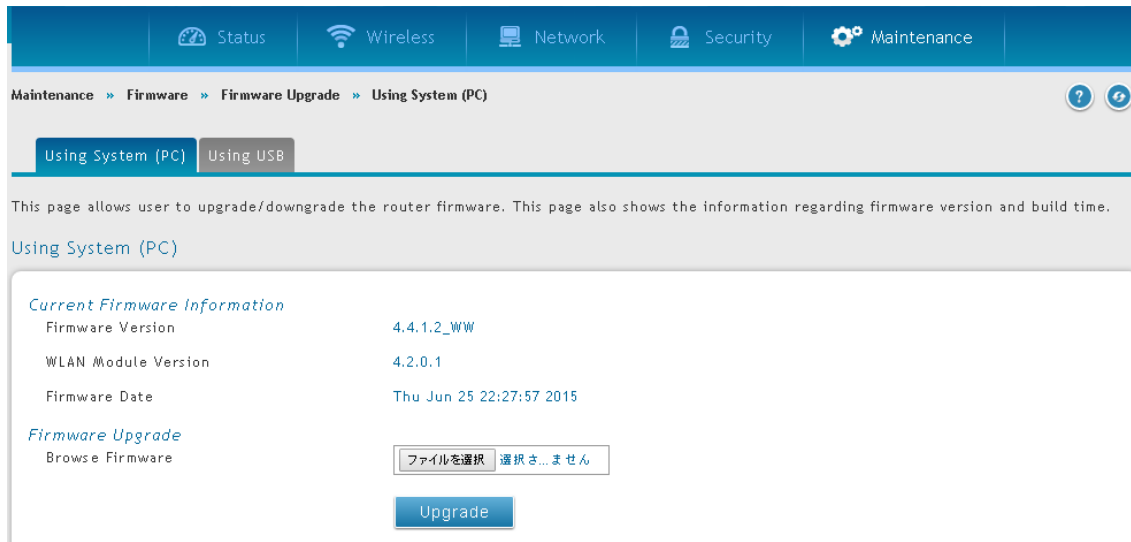
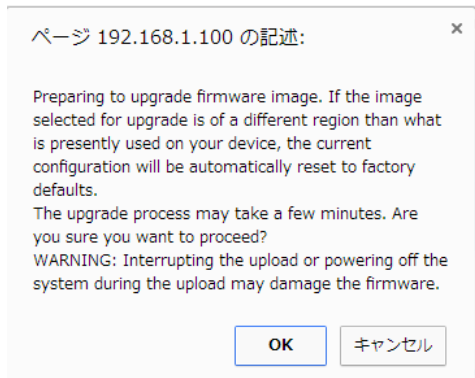


図 9-24 Using System (PC) 画面

2. 「Current Firmware Information」の「Firmware Version」で現在のファームウェアバージョンを確認し、インストールするファームウェアのバージョンでのアップグレードで問題なければ、この手順を続けます。
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。プログレスバーはアップグレードの進捗を表示します。

注意

アップグレードのプロセスには数分かかります。アップグレードの中止や、システムのオフをしないでください。オフにするとファームウェアを破損する場合があります。ブラウザからどのサイトへの参照も、アップグレードが完了するまでお待ちください。

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 [322 ページの「付録 A 基本計画のワークシート」](#)に記録します。

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 管理インターフェースで、**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。

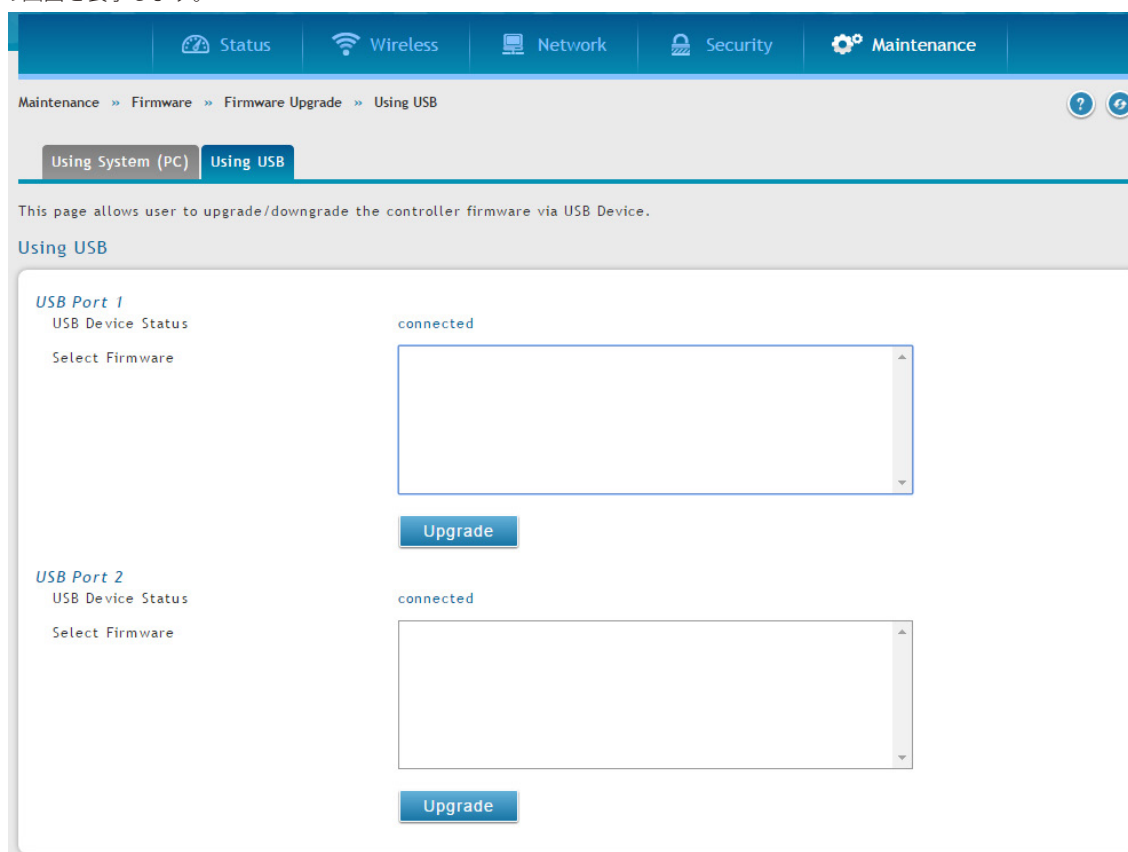


図 9-25 Using USB 画面

2. 「Current Firmware Information」の「Firmware Version」で現在のファームウェアバージョンを確認し、インストールするファームウェアのバージョンでのアップグレードで問題なければ、この手順を続けます。
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。プログレスバーはアップグレードの進捗を表示します。

注意 アップグレードのプロセスには数分かかります。アップグレードの中止や、システムのオフをしないでください。そうでないと、ファームウェアを破損する場合があります。ブラウザからどのサイトへの参照も、アップグレードが完了するまでお待ちください。

6. アップグレードが完了したら、無線コントローラの Web 管理インター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 [322 ページの「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、簡単なテキストベースでツリー構造であるインタフェースを経由し、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、モニターを行います。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 PC または Linux ワークステーションをコンソールに接続する場合、別売の USB-DB9F シリアルアダプタが役立ちます。RJ45-DB9M ケーブルは無線コントローラ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. CLI ログイン証明書は管理者ユーザ用の 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-1000 login:

注意 詳しくは、「Wireless Controller CLI Reference Guide DWC-1000」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

無線コントローラの電源をオンにした後に、以下の一連のイベントが起こる必要があります。:

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 デバイスを接続する場合は、ポート左の 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、ポート左の LED が緑色であることを確認します。ポートに 10Mbps デバイスが接続する場合は、ポート右の 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、ポート左の LED が緑色であることを確認します。

これらの条件のいずれも起こらない場合、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、電源コードが壁面スイッチにより制御されないで機能するコンセントに接続されていることを確認します。

エラーが続く場合、D-Link 社の技術サポートに連絡してください。

LAN ポート LED が消灯

イーサネット接続が行われているのに、LAN LED が点灯しない場合:

1. イーサネットケーブル接続が無線コントローラおよびスイッチで確実に行われていることをチェックします。
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 管理インタフェース

ご使用のローカルネットワーク上の PC から無線コントローラの Web 設定インタフェースにアクセスできない場合:

1. PC と無線コントローラ間のイーサネット接続をチェックしてください。
2. ご使用の PC の IP アドレスが無線コントローラと同じサブネットにあることを確認してください。推奨のアドレス指定を使用している場合、PC が「192.168.10.nnn」(nnn は 0 または 2-255) であるスタティックな IPv4 アドレスと「255.255.255.0」のサブネットを使用するように設定されているのを確認してください。
3. 無線コントローラの IP アドレスを変更したが、現在の IP アドレスがわからない場合、無線コントローラの設定を工場出荷時設定にリセットしてください。リセットすると、無線コントローラの IP アドレスは「192.168.10.1」([324 ページの「工場出荷時設定の復元」](#)を参照) にセットされますが、工場出荷時設定に行った変更はすべて失われます。
4. 工場出荷時設定に設定をリセットして、コンフィグレーションを失いたくない場合、無線コントローラを再起動して、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ァーを使用してください。ARP パケットを見て、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た、工場出荷時設定の復元

何らかの理由で無線コントローラの管理インターフェースにアクセスできない場合、背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. 少なくとも 15 秒間、リセットボタンを押し続けます。
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 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。

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明記されます。

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を確認してください。

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、アクセスポイントのいずれか、またはすべてを発見しない場合：

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。([305 ページ「LAN ポート LED が消灯」](#) 参照)
2. アクセスポイントが異なる VLAN で動作しているか、1 つの IP サブネット配下にあるか、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。([23 ページ「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。([72 ページの「AP ディスカバリ方式」](#) 参照) 1 つ以上のアクセスポイントが同じ IP アドレスを持つ場合、それらの中から 1 つだけが発見されます。この場合、管理リストに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、その IP アドレスを持つ次のアクセスポイントを発見してください。([25 ページの「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」モードに変換されると、スタティックな IP アドレスは DHCP サーバ (ネットワークにあるもの、または無線コントローラで設定されるもののいずれか) が発行する IP アドレスに変わります。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 1 つもないか、アクセスポイントが DHCP サーバに到達できないと、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 サーバが全くない場合、無線コントローラ上に設定してください。([23 ページ「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 を追加したのに、その SSID が 5 分以内に Wi-Fi ネットワーク下に現れない場合、以下の手順で無線コントローラを再起動します。

1. **Maintenance > Firmware > 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、断続的に短期間で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します。安全上の配慮がネットワーク性能より重要であれば、不正なアクセスポイントの検出を有効することができます。ネットワーク性能が安全上の配慮より重要であれば、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の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。

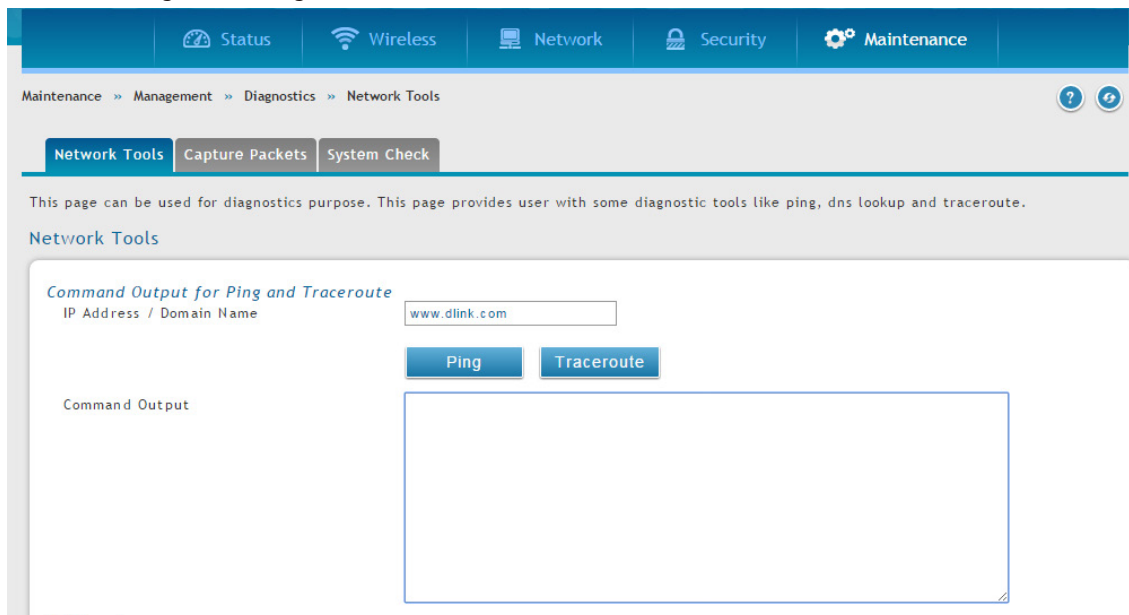


図 10-1 Network Tools 画面

2. 「Command Output for Ping and Traceroute」にある「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。

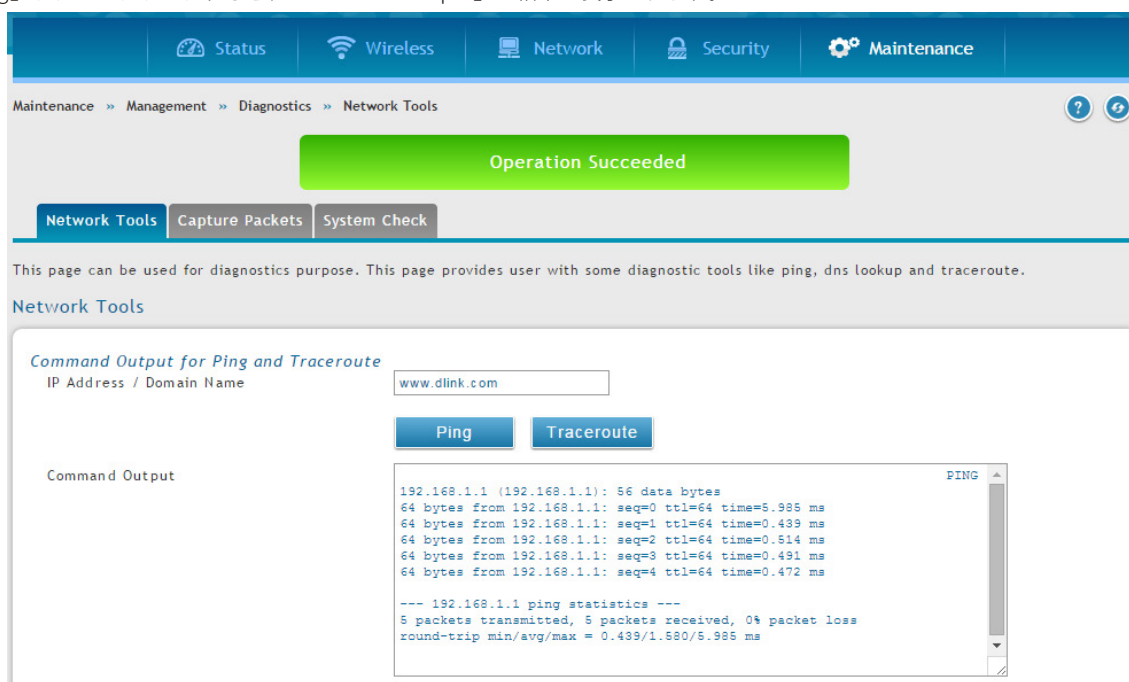


図 10-2 Network Tools 画面

Traceroute の使用

Maintenance > Management > Diagnostics > Network Tools メニュー

無線コントローラは、ネットワークのパスをパブリックホストにマップさせる Traceroute 機能を提供します。本無線コントローラと宛先の間に位置する最大 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

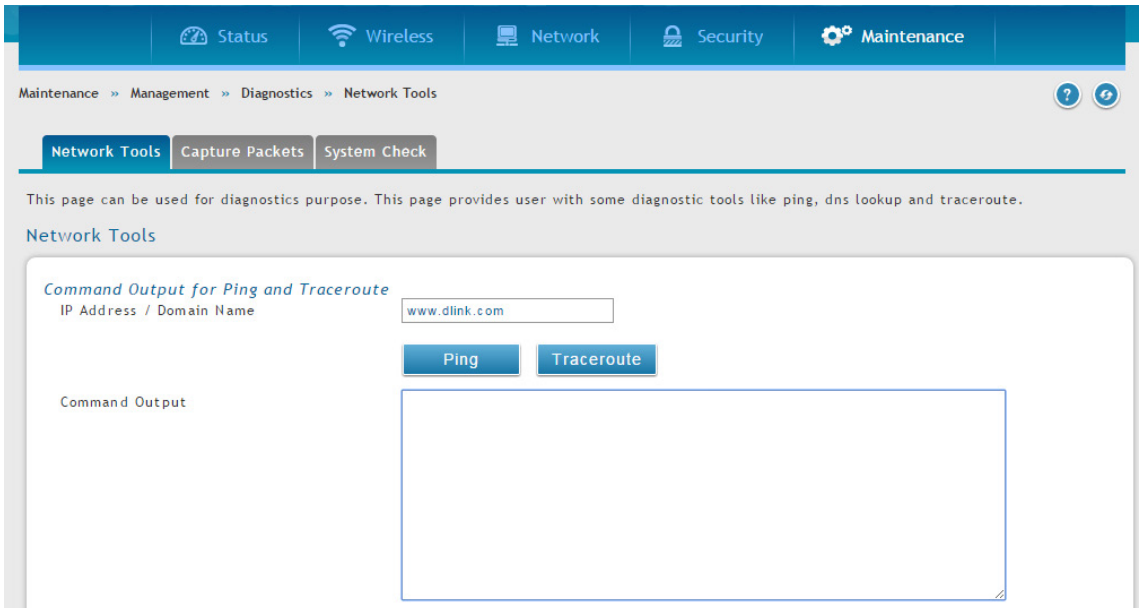


図 10-3 Network Tools 画面

2. 「Command Output for Ping and Traceroute」にある「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。

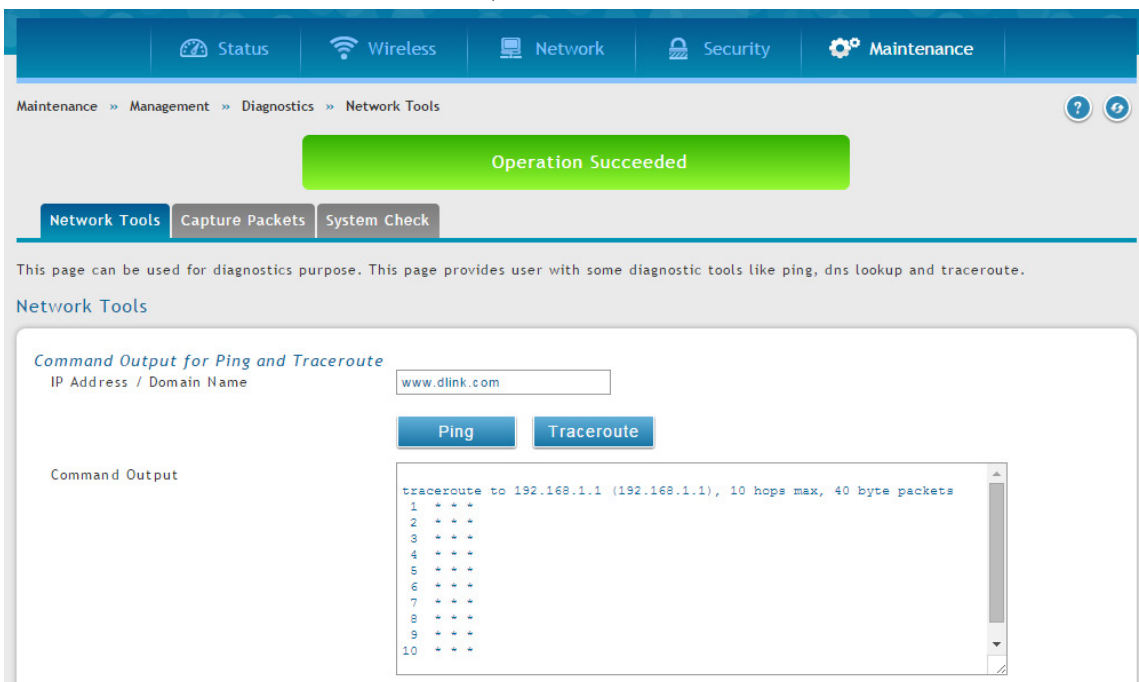


図 10-4 Network Tools 画面

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 アドレスも検索できる 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

Maintenance >> Management >> Diagnostics >> Network Tools

Network Tools | Capture Packets | System Check

This page can be used for diagnostics purpose. This page provides user with some diagnostic tools like ping, dns lookup and traceroute.

Network Tools

Command Output for Ping and Traceroute

IP Address / Domain Name:

Command Output:

DNS Lookup

Domain Name:

Command Output:

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。

- 「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 アドレスと共に応答を表示します。「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。

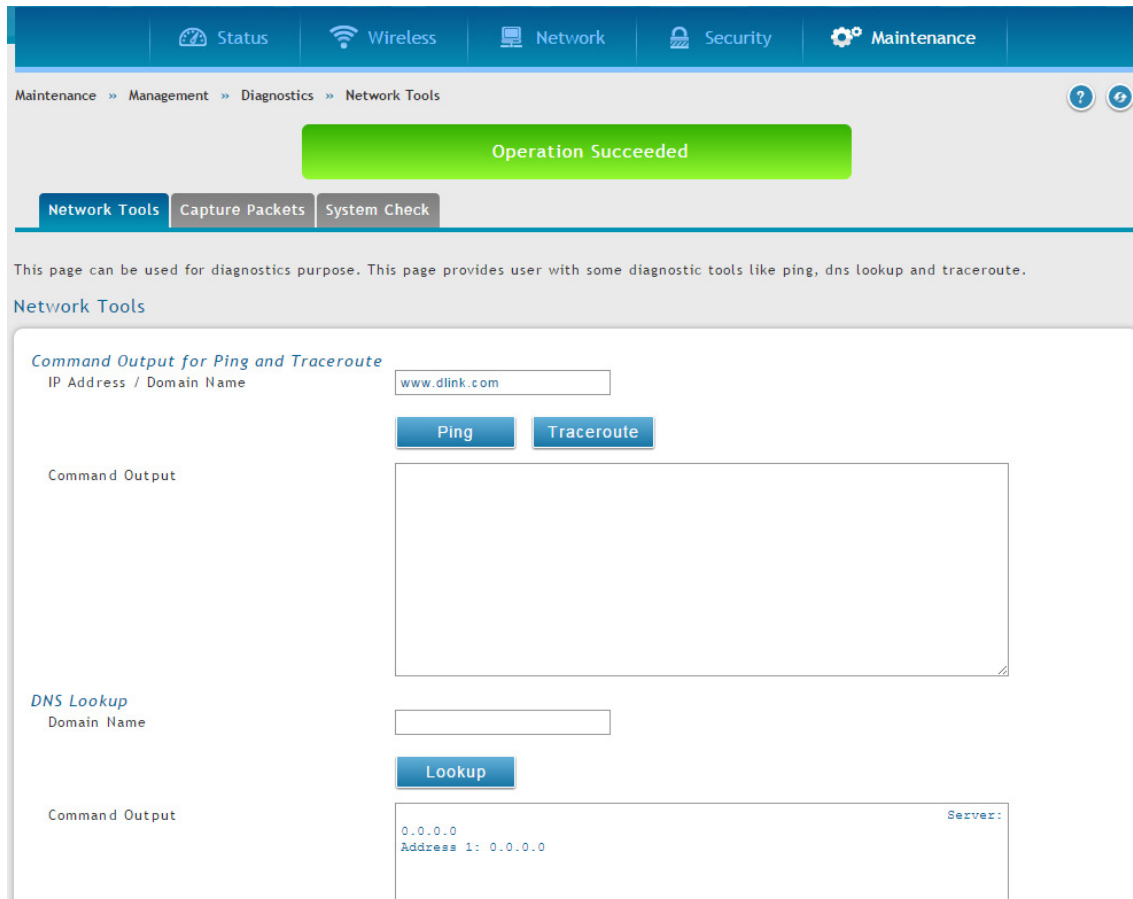


図 10-6 Network Tools 画面

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：

- 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

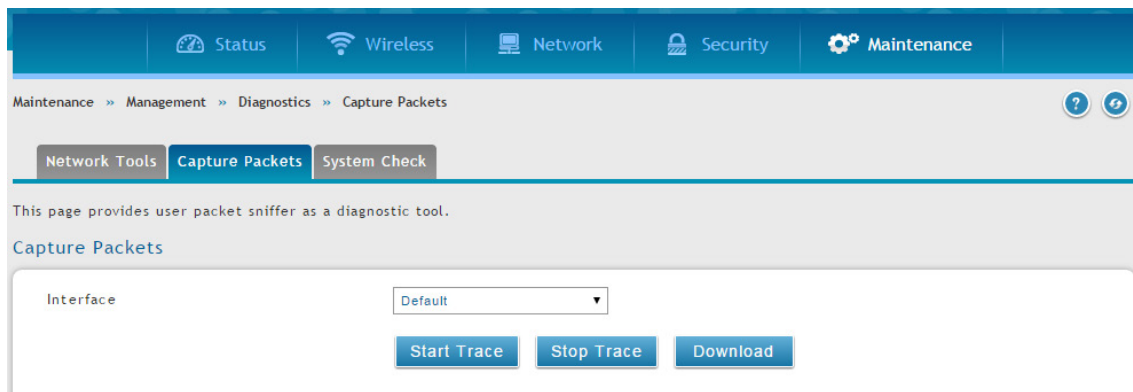


図 10-7 Capture Packets 画面

- 「Interface」のプルダウンメニューから「LAN」または「Option1」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。

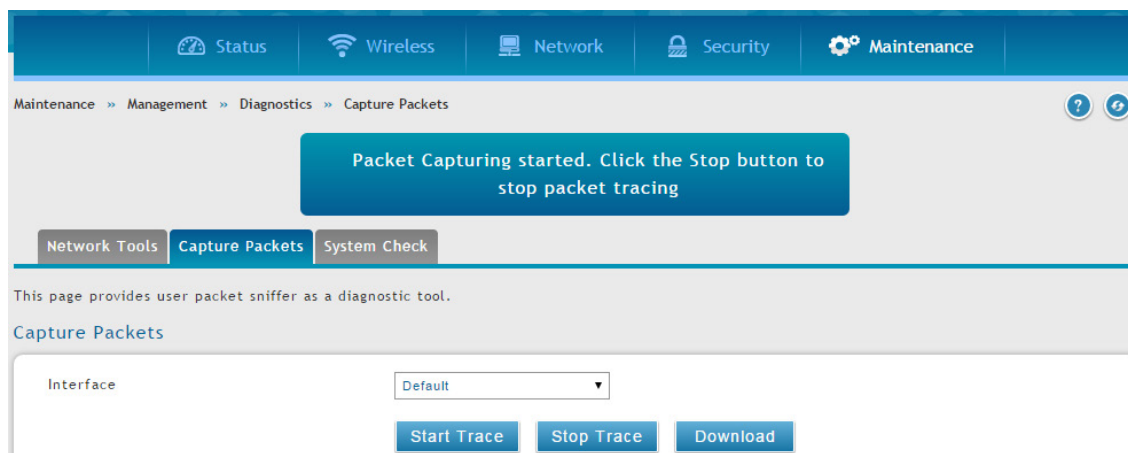


図 10-8 Capture Packets 画面

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。

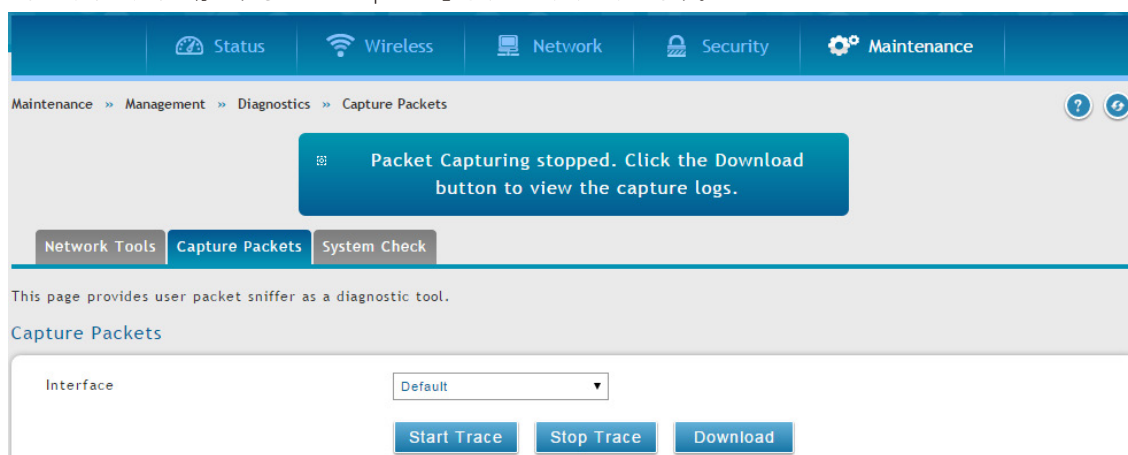


図 10-9 Capture Packets 画面

「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。直ちに、ブラウザのデフォルトのダウンロードフォルダに行われます。

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のに本機能を使用できます。

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

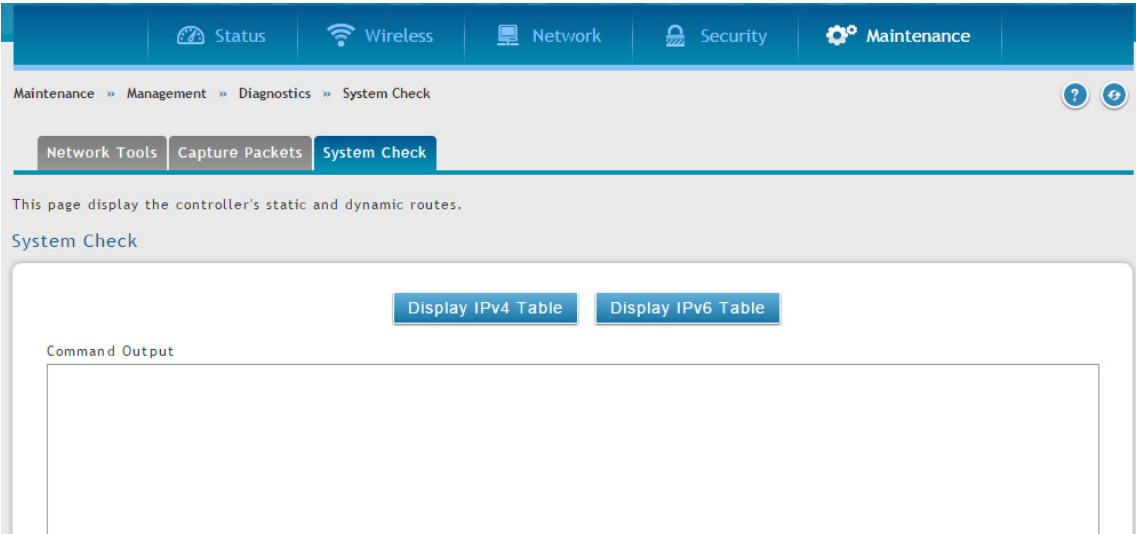


図 10-10 System Check 画面

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。

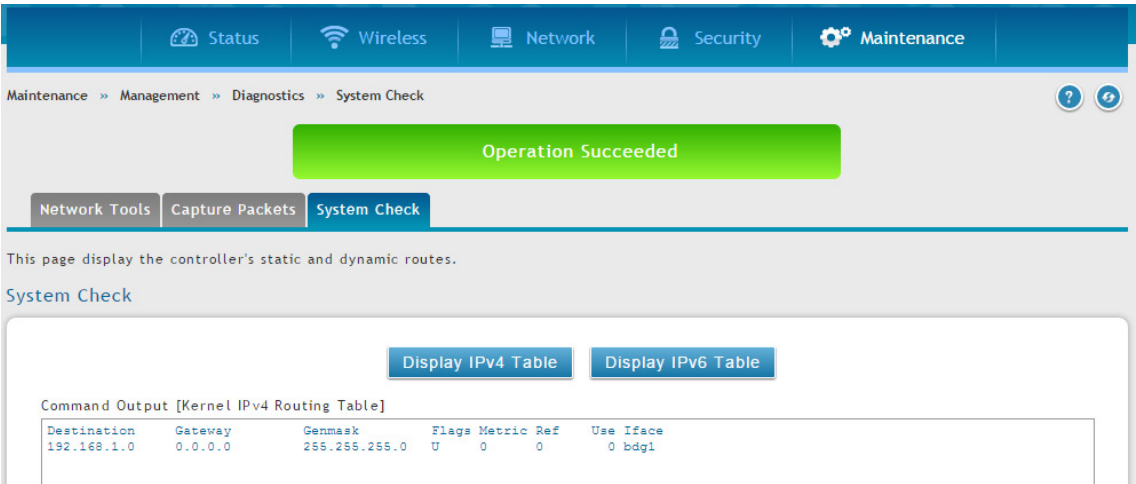


図 10-11 System Check 画面 (IPv4)

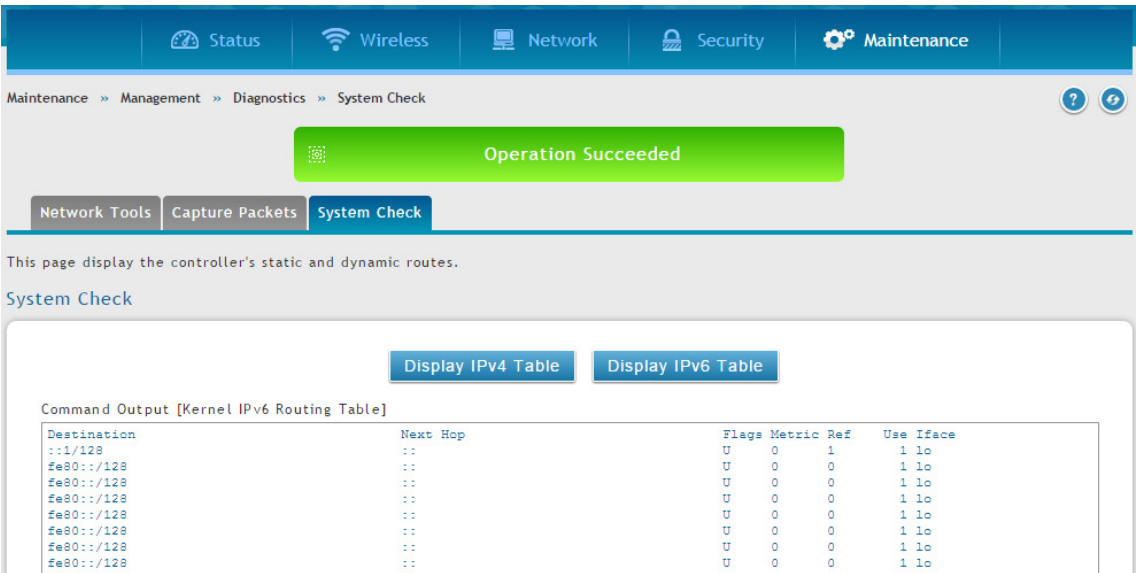


図 10-12 System Check 画面 (IPv6)

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。コントローラはログメッセージを検出すると、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ーして、潜在的な攻撃またはエラーについて通知することができます。以下のセクションはログ構成設定とこ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」 ページでは、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。

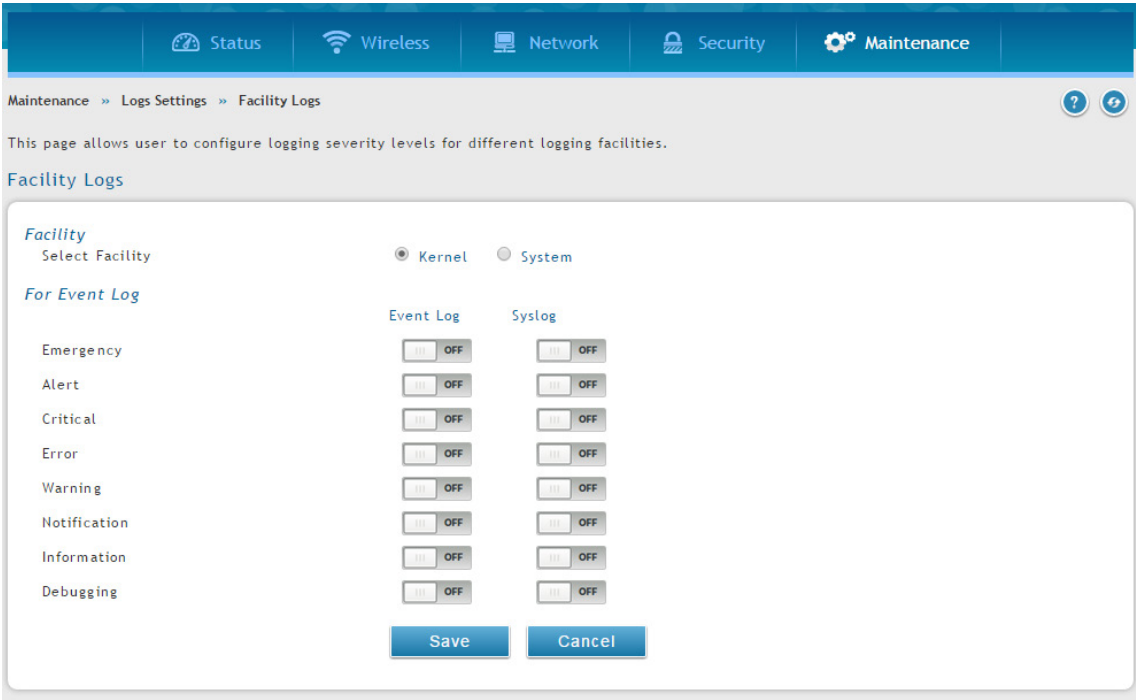


図 10-13 Facility Logs 画面

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対応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してトラフィックに対応します。
System	ユニットを管理するのにこ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	システムは使用不能
Alert	直ちに、アクションを行う必要があります。
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、イベント（厳しさの順）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、後で確認するためにログが送信される場所、Web 内のイベントログビューワ（Status > System Information > All Logs > Current Logs ページ）、またはリモート Syslog サーバに基づいてカスタマイズされます。続くセクションで記述されるメールログは、Syslog サーバに設定されたログと同じ設定が続きます。

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

ファイアウォールがパケットを受け付けたか、または破棄し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。

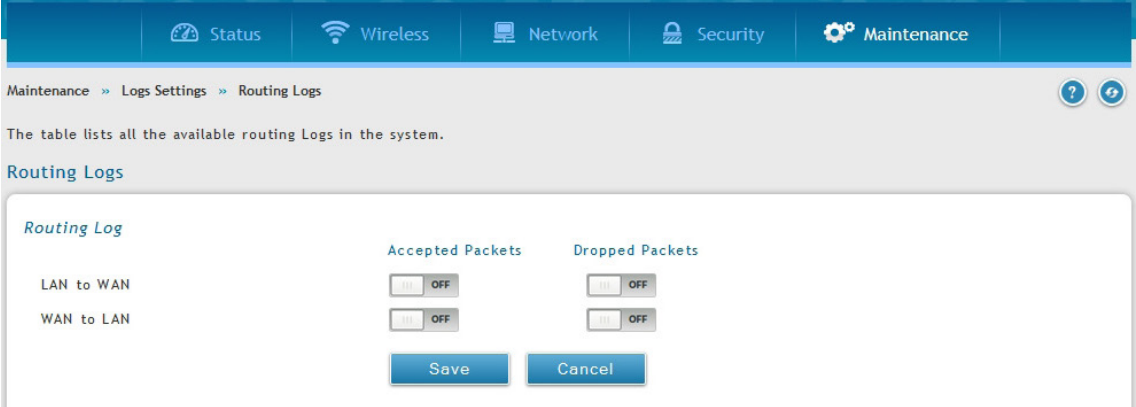


図 10-14 Routing Logs 画面

以下の項目があります。

項目	説明
Routing Log	
LAN to WAN	有効である場合、LAN ⇒ WAN または WAN ⇒ LAN ルーティングのログからトラフィックを追跡します。 <ul style="list-style-type: none">Accepted Packets - 有効にすると、トラックパケットであれば、セグメントを通じた転送に成功したパケットを追跡します。Dropped Packets - 有効にすると、セグメントを通じた転送からブロックされたパケットを追跡します。
WAN to LAN	

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。

Syslog ログ

Maintenance > Logs Settings > System Logs メニュー

Syslog、メールログ、またはイベントビューワへの表示のために、ログに出力する無線コントローラを経由したトラフィックのタイプを決定します。本ページは、DoS (denial-of-service) 攻撃、一般的な攻撃情報、ログインの試み、破棄したパケット、および類似のイベントなど、疑わしいアクティビティをキャプチャするのを補助します。ファイアウォールがパケットを受け付けたか、または破棄し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。

1. Maintenance > Logs Settings > System 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。

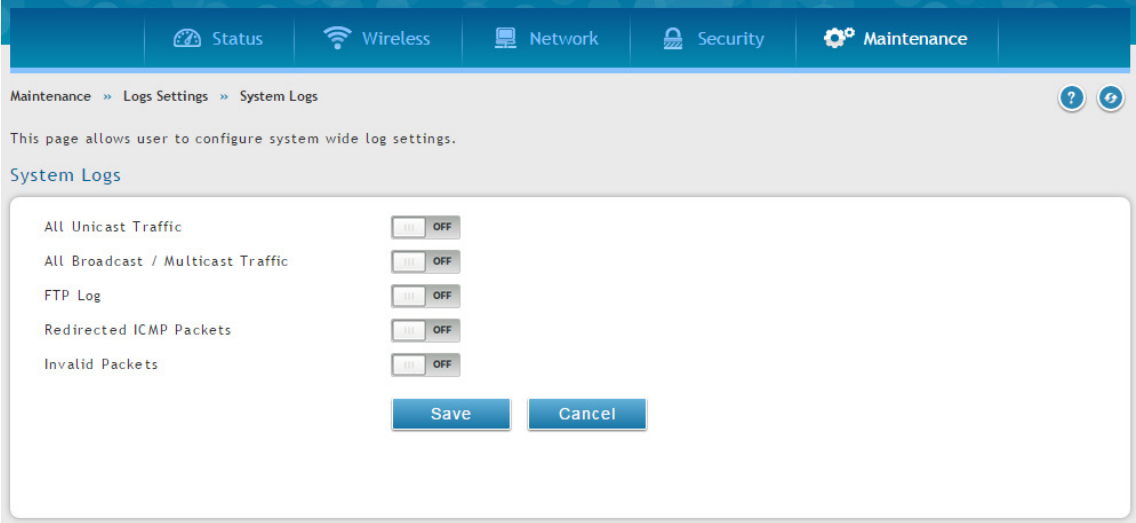


図 10-15 System Logs 画面

以下の項目があります。

項目	説明
All Unicast Traffic	有効にすると、無線コントローラに向けたパケットを追跡します。
All Broadcast / Multicast Traffic	有効にすると、無線コントローラに向けたすべてのブロードキャストまたはマルチキャストパケットを追跡します。
FTP Logs	有効にすると、ログ情報を FTP ログに送信します。
Redirected ICMP Packets	有効にすると、リダイレクトされた ICMP (Internet Control Message Protocol) パケット数を追跡します。
Invalid Packets	有効にすると、受信した無効なパケット数を追跡します。

2. トラフィックのタイプを選択後、「Save」ボタンをクリックして変更を保存します。

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。メールログは、頻度をはじめに選択することで、定義したスケジュールに基づいて送信されます。: 時、日、週

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 10-16 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	メッセージの送信元を識別するのに使用されるプレフィックスを入力します。この識別子はメールと Syslog メッセージ両方の先頭に付けられています。
E-Mail Log	メールログを有効、または無効にします。 <ul style="list-style-type: none"> ON - メールログを有効にします。このページの残り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。このページの残りのフィールドは利用できません。
E-Mail Server Address	「E-Mail Log」を有効とした場合、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	「E-Mail Log」を有効とした場合、メールサーバの SMTP ポートを入力します。
Return E-Mail Address	「E-Mail Log」を有効とした場合、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。(失敗メッセージに必要とされます。)
Send to E-mail Address (1-3)	「E-Mail Log」を有効とした場合、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。

項目	説明
Authentication with SMTP	「E-Mail Log」を有効とした場合、接続を受け入れる前に SMTP サーバが認証が必要であれば、認証を選択します。 <ul style="list-style-type: none"> None - 認証は使用されません。「User Name」および「Password」フィールドは利用できません。 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のに使用される認証。Base64 でコード化されたパスワードでは、どんな暗号の保護も提供しないため、被害を受けやすくなります。 CRAM-MD5 - HMAC-MD5 MAC アルゴリズムに基づき RFC 2195 で定義された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。
Respond to Identd from SMTP	「E-Mail Log」を有効にした場合、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決定します。 <ul style="list-style-type: none"> 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 Logs by Schedule	
スケジュールに基づいてメールログを受信するためには、スケジュール設定を行います。「E-Mail Log」を有効にすると、スケジューリングオプションが有効になります。	
Unit	ログの送信が必要な期間を選択します。本オプションはメールでログを受信しないが、メールオプションの設定を保持したい場合に便利です。「Event Log」ビューワページの「Send Log」機能を使用することができます。: <ul style="list-style-type: none"> Never - ログの送信を無効にします。 Hourly - 1 時間ごとにログを送信します。 Daily - 毎日指定した時間にログを送信します。 Weekly - 毎週指定した曜日と時間にログを送信します。
Day	「Unit」を「Weekly」に設定した場合、ログを送信する曜日を選択します。
Time	「Unit」を「Daily」または「Weekly」に設定した場合、ログを送信する時間を選択します。

Syslog サーバ構成

Maintenance > Logs Settings > Syslog Server メニュー

外部の Syslog サーバは、無線コントローラからログを集めて、保存するのにネットワーク管理者によって頻繁に使用されます。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に対してローカルなイベントビューワよりもメモリ制限が少なくなっています。そのため、持続期間中に、多くのログを集めることができます。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ーするのに役に立ちます。

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。各サーバは、「Remote Logs」ページを使用して、セベリティの異なる様々なログファシリティメッセージを受信するように設定されます。さらに、本ページでは、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 > 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。

The screenshot shows the 'Syslog Server Configuration' page. At the top, there's a navigation bar with 'Status', 'Wireless', 'Network', 'Security', and 'Maintenance'. Below it, the breadcrumb 'Maintenance > Logs Settings > Syslog Server' is visible. A message states: 'This page allows user to configure the syslog server logging options for the router.' The main section is titled 'Syslog Server Configuration'. It contains a form for 'SysLog Server 1' with fields for 'FQDN / IP Address', 'Facility' (set to 'All'), and 'Severity' (set to 'All'). Below this, there are eight rows for 'SysLog Server 2' through 'SysLog Server 8', each with a toggle switch currently set to 'OFF'. At the bottom, there are 'Save' and 'Cancel' buttons.

図 10-17 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。この設定ページ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 サーバのインターネット名 /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 で定義されます。
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 サーバにログを出力します。 <ul style="list-style-type: none"> 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

無線コントローラの Web 管理インターフェースは、「Status」メニューで設定したログメッセージを表示します。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（[313 ページの「ログ設定」](#)参照）、または **Maintenance > Log Settings > Routing Logs** ページ（[314 ページの「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 > 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。

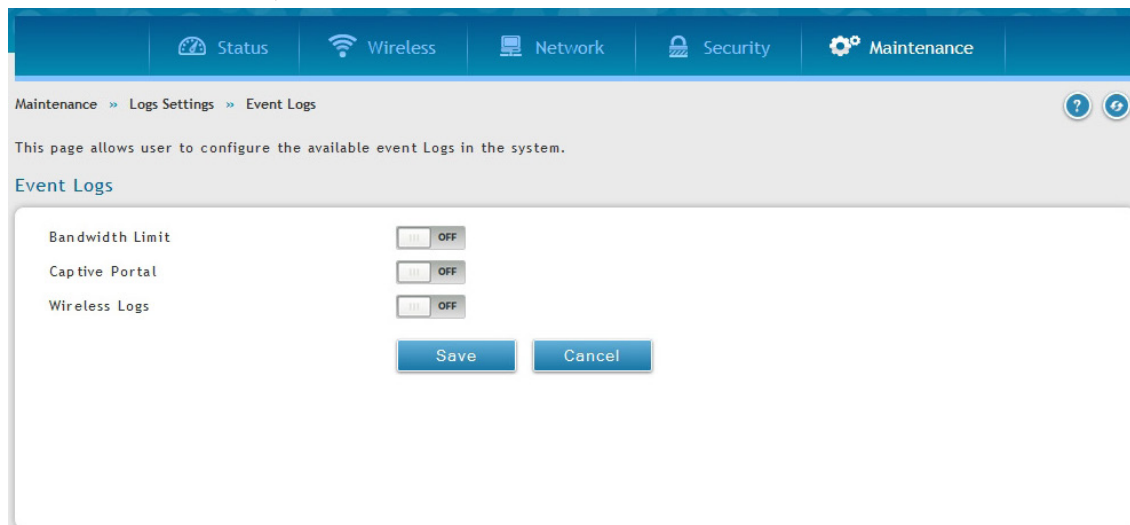


図 10-18 Event Logs 画面

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
Bandwidth Limit	有効にすると帯域制限に関連した無線クライアントの情報をログに出力します。
Captive Portal	有効であると、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	有効であると、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。

注意 ログメッセージを理解するためには、手動または NTP サーバより設定した正確なシステム時間を持つことが非常に重要です。

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、コントローラが設定し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ると、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。

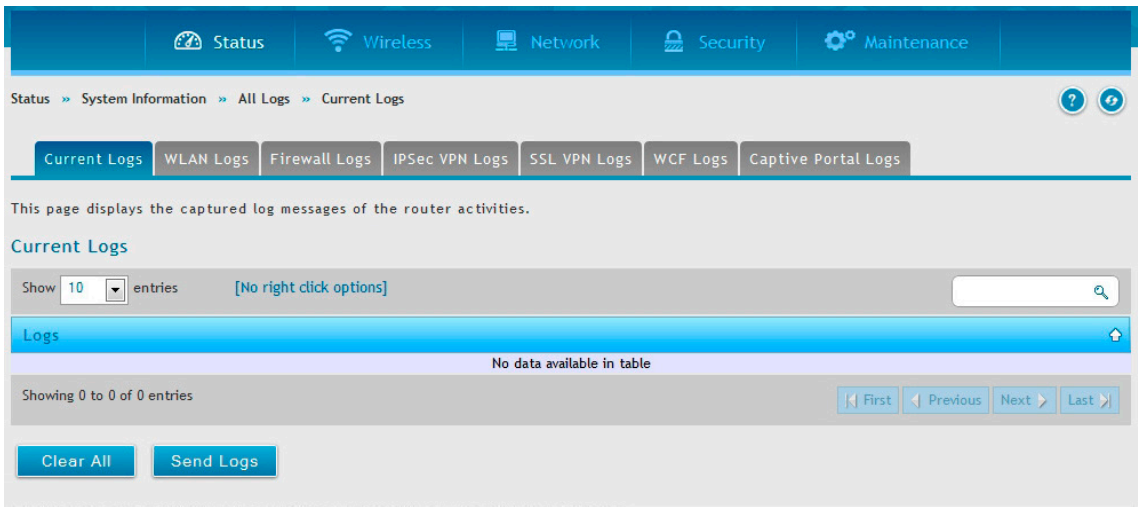



図 10-19 Current Logs 画面

ログのリフレッシュまたはページのリロードのためには、（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 インタフェースにある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、コントローラが設定し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 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。

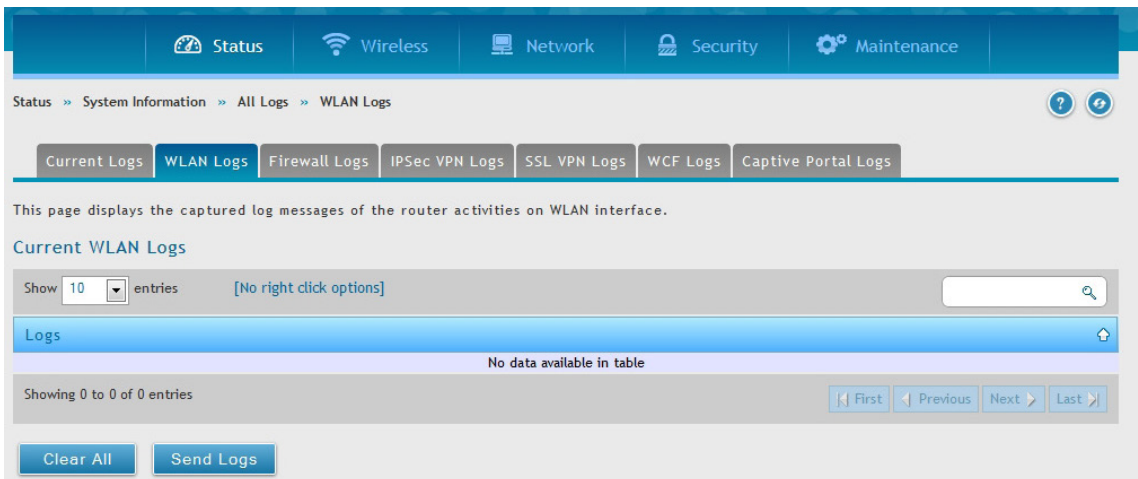



図 10-20 Current WLAN Logs 画面

ログのリフレッシュまたはページのリロードのためには、（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。

Firewall ログ

Status > System Information > All Logs > Firewall Logs メニュー

コントローラで設定したファイアウォールログメッセージを表示します。各ログはコントローラの指定した時間にタイプスタンプとともに表示されます。「シスログサーバ」や「E-mail ログギング」などが設定されている場合、表示されているログと同じログがリモートインタフェースに送信されます。

注意 本機能は追加ライセンス「DWC-1000-VPN」が有効の場合にのみ利用可能です。

Status > System Information > All Logs > Firewall 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。

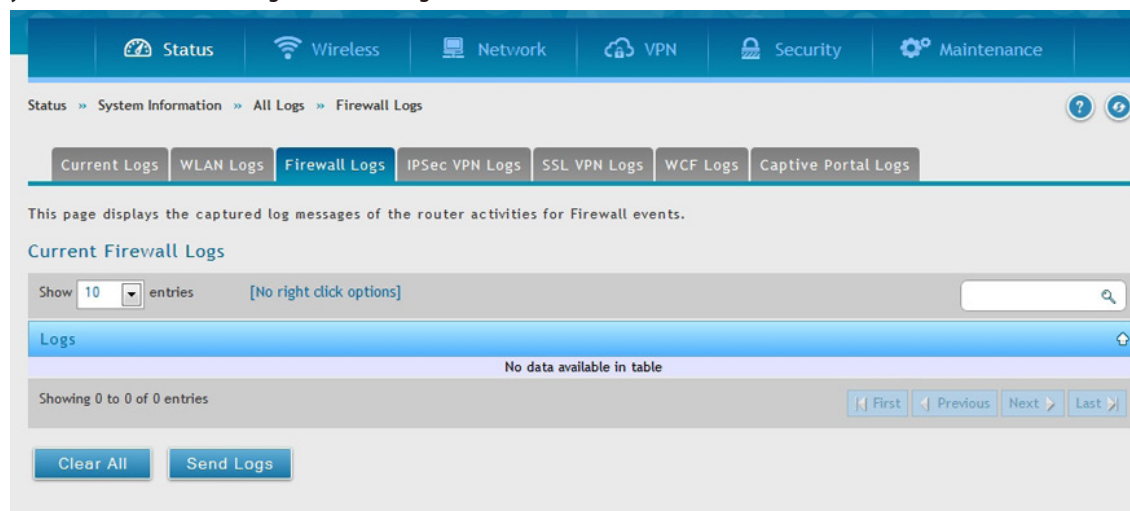



図 10-21 Firewall Logs 画面

ログのリフレッシュまたはページのリロードのためには、（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。

IPSec VPN ログ

Status > System Information > All Logs > IPsec VPN Logs メニュー

コントローラで設定し IPsec VPN ログメッセージを表示します。各ログはコントローラの指定した時間にタイプスタンプとともに表示されます。「シスログサーバ」や「E-mail ログギング」などが設定されている場合、表示されているログと同じログがリモートインタフェースに送信されます。

注意 本機能は追加ライセンス「DWC-1000-VPN」が有効の場合にのみ利用可能です。

Status > System Information > All Logs > IPsec VPN 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。

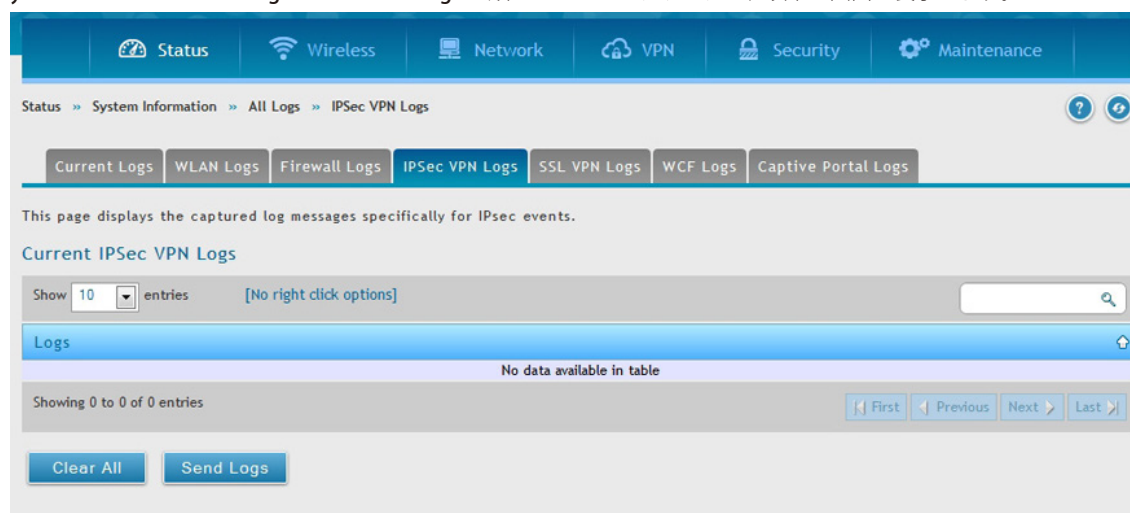



図 10-22 IPsec VPN Logs 画面

ログのリフレッシュまたはページのリロードのためには、（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。

SSL VPN ログ

Status > System Information > All Logs > SSL VPN Logs メニュー

コントローラで設定し SSL VPN ログメッセージを表示します。各ログはコントローラの指定した時間にタイプスタンプとともに表示されます。「シスログサーバ」や「E-mail ロギング」などが設定されている場合、表示されているログと同じログがリモートインタフェースに送信されます。

注意 本機能は追加ライセンス「DWC-1000-VPN」が有効の場合にのみ利用可能です。

Status > System Information > All Logs > SSL VPN 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。

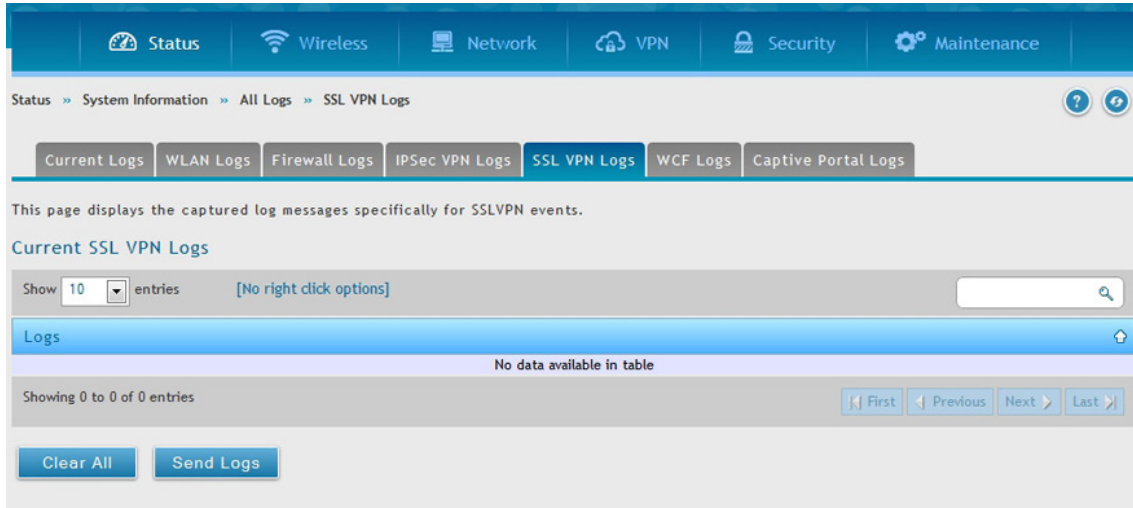



図 10-23 SSL VPN Logs 画面

ログのリフレッシュまたはページのリロードのためには、（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。

WCF ログ

Status > System Information > All Logs > WCF Logs メニュー

コントローラで設定し WCF ログメッセージを表示します。各ログはコントローラの指定した時間にタイプスタンプとともに表示されます。「シスログサーバ」や「E-mail ロギング」などが設定されている場合、表示されているログと同じログがリモートインタフェースに送信されます。

注意 本機能は追加ライセンス「DWC-1000-WCF-12」が有効の場合にのみ利用可能です。

Status > System Information > All Logs > WCF 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。

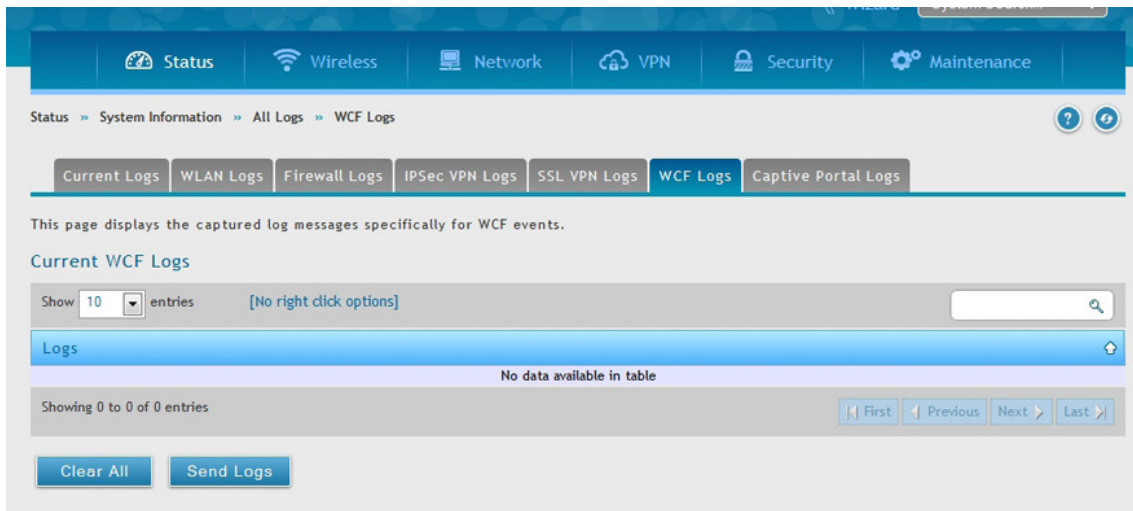



図 10-24 WCF Logs 画面

ログのリフレッシュまたはページのリロードのためには、（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。

Captive Portal ログ

Status > System Information > All Logs > Captive Portal Logs メニュー

コントローラで設定し Captive Portal ログメッセージを表示します。各ログはコントローラの指定した時間にタイプスタンプとともに表示されます。「シスログサーバ」や「E-mail ロギング」などが設定されている場合、表示されているログと同じログがリモートインタフェースに送信されます。

Status > System Information > All Logs > Captive Portal 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。

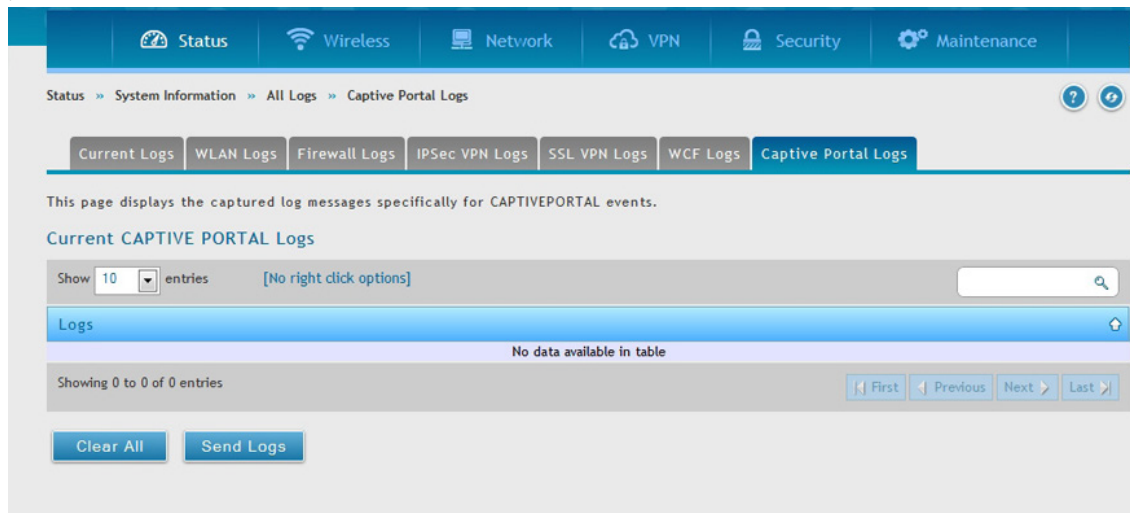



図 10-25 Captive Portal Logs 画面

ログのリフレッシュまたはページのリロードのためには、（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 A 基本計画のワークシート

RF 計画では、提供する Wi-Fi カバレッジの範囲を規定できます。追加のアクセスポイントを必要とするカバレッジマップ、弱信号の傾向にある位置やデッドスポットに適切な Wi-Fi カバレッジを提供します。

計画の取り組みを促進させるためには、この付録のような基本計画のワークシートにより、以下のクリティカル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？ <ul style="list-style-type: none"> • プロファイル名： _____ • クライアント _____ • 利用可能なモード： <ul style="list-style-type: none"> • 802.11 b/g: • 802.11 n: • 802.11 b/g/n: • 802.11 a - 5 GHz のみ: • 802.11 a/n - 5 GHz のみ: • 802.11 a/n/ac - 5 GHz のみ: 	
4	SSID 情報 <ul style="list-style-type: none"> • SSID 名 _____ • セキュリティ (none、WEP、WPA、または WPA2) _____ 	
5	無線コントローラを DHCP サーバとして使用しますか？ <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> - 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： _____ 	

ステップ	タスク	完了有無
6	LAN IP アドレス :	
7	サブネットマスク :	
8	IP アドレス範囲 : <ul style="list-style-type: none"> 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 : <ul style="list-style-type: none"> 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 ? <ul style="list-style-type: none"> 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。 : <ul style="list-style-type: none"> DWC-1000 無線コントローラ : DWL-6600AP 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。 : <ul style="list-style-type: none"> DWC-1000 無線コントローラ : DWL-6600AP 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。ホストがもう IP アドレスを必要としない時にアドレスを再利用できるようにダイナミックに IP アドレスを割り当てるプロトコル。
DNS	Domain Name System。H.323 ID、URL、またはメール ID を IP アドレスに変換するメカニズム。また、リモートゲートキーパの場所を見つけるのを補助して、IP アドレスを管理ドメインのホスト名にマップするために使用されます。
FQDN	FQDN（完全修飾ドメイン名）。ホスト部分を含むドメイン名を完成します。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部分として ISAKMP で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、ネットワークパケットとも言われるデータグラムを中継するの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責任があります。それは、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結合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。ルータまたはファイアウォールを通過するパケットとして IP アドレスを書き換える処理。NAT は、LAN のゲートウェイルータにおける単一のパブリック 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のを可能にします。
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。クロックマスタとして知られているルータをネットワークにおける単一のクロックに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トिंग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。

用語	説明
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の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が同じサブネットに所属します。
TCP	Transmission Control Protocol。信頼性と順序通りの配信を保証したインターネットにおけるデータ送信のプロトコル。
UDP	User Data Protocol。信頼性と順序通りの配信を保証せずにインターネットにおけるデータを送信するプロトコル。
VPN	Virtual private network。あるネットワークから別のネットワークにトラフィックすべてを暗号化することによって IP トラフィックがパブリックな TCP/IP ネットワークに進むことを可能とするネットワーク。IP レベルで全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	管理対象のアクセスポイントを単一に統合するソリューションに個別に集約することで、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。