DAP-3666

IEEE 802.11AC Dual Band PoE Outdoor Access Point

ユーザマニュアル

D-Link®
Building Networks for People

目次

1. お使いになるまえに 4
本製品について 5
機能概要 5
本製品の特長 5
製品名/品番一覧 5
本製品の接続モード 6
Nuclias Connectについて 7
概要 7
Nuclias Connectの特長 7
本マニュアルについて 8
マニュアルの構成 8
マニュアルの対象者 8
表記規則 8
安全にお使いいただくために 9
ご使用上の注意 11
静電気障害を防止するために 11
電源の異常 11
無線LANについて 12
WLAN 技術を利用するさまざまな理由 12
無線に関するご注意 13

2. 設置のしかた 16
パッケージの内容 17
動作環境 17
ネットワーク接続前の準備 17
本体各部名称 19
前面パネル/背面パネル 19
底面 19
LED表示 19
製品の設置 20
ネットワークと電源への接続 23

3. WEB GUI 画面について 24
WEB GUI画面へのログイン 25
初回ログイン時のセットアップ 26
画面の構成 28

4. Basic Settings (基本設定) 29
Basic Settings について 30
Wireless Settings（ワイヤレス設定） 30
Access Point モードを選択した場合 31
WDSモード／WDS with APモードを選択した場合 33
Wireless Clientモードを選択した場合 35
Authentication（認証）の設定について 37
LAN Settings（LAN設定） 42
IPv6 Settings（IPv6設定） 43

5. Advanced Settings (詳細設定) 44
Advanced Settings について 45
Performance Settings（パフォーマンス設定） 45
Wireless Resource Control（ワイヤレスリソースコントロール） 48
Multi-SSID Settings（マルチSSID設定） 49
VLAN Settings（VLAN設定） 51
Wireless Intrusion Protection（不正AP検知） 55
Wireless Schedule Settings（スケジュール設定） 56
Internal RADIUS Server（RADIUSサーバ） 58
ARP Spoofing Prevention Settings
（ARPスプーフィング防止設定） 59

Bandwidth Optimization（帯域幅最適化） 60
Hotspot2.0（ホットスポット2.0） 62
Captive Portal（キャプティブポータル） 68
Captive Portal Authentication（キャプティブポータル認証） 68
Login Page Upload（ログイン画面アップロード） 77
MAC Bypass（MAC Bypass 設定） 78
DHCP Server（DHCPサーバ設定） 79
Dynamic Pool Settings（ダイナミックプール設定） 79
Static Pool Settings（スタティックプール設定） 80
Current IP Mapping List（IPマッピングリスト） 81
Filters（フィルタ） 82
Wireless MAC ACL Settings（ワイヤレスMAC ACL） 82
WLAN Partition（WLANパーティション） 84
IP Filter Settings（IPフィルタ） 85
Traffic Control（トラフィックコントロール） 86
Uplink and Downlink Setting（アップリンク／ダウンリンク設定） 86
QoS（QoS設定） 87
Traffic Manager（トラフィックマネージャ） 88

6. Status (ステータス) 90
Statusについて 91
Device Information（デバイス情報） 91
Client Information（クライアント情報） 93
WDS Information（WDS情報） 93
Statistics（統計情報） 94
Ethernet Traffic Statistics（イーサネットトラフィック統計情報） 94
WLAN Traffic Statistics（WLANトラフィック統計情報） 95
Log（ログ） 96
View Log（ログの表示） 96
Log Settings（ログ設定） 97

7. 管理メニュー 99
管理メニューについて 100
Home (ホーム画面) 100
Maintenance（メンテナンス） 101
Administration Settings（管理設定） 101
Firmware and SSL Certification Upload（ファームウェアとSSL証明書のアップロード） 105
Configuration File Upload and Download
（コンフィグレーションファイルのアップロードとダウンロード） 107
Time and Date Settings（時刻と日付の設定） 108
Configuration（コンフィグレーション） 110
設定の保存と有効化 110
設定の破棄 110
System（システム設定） 111
本製品の再起動 111
工場出荷時設定へのリセット 111
Language Packの削除 112
Logout（ログアウト） 113
Help（ヘルプ） 113

8. 付録 114
工場出荷時設定に戻す 115
リセットボタンで設定リセット行う 115
Web GUIから設定リセットを行う 115
FAQ 116
機能設定例 119
対象機器について 119
VLAN 119

お使いになるまえに

1

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。

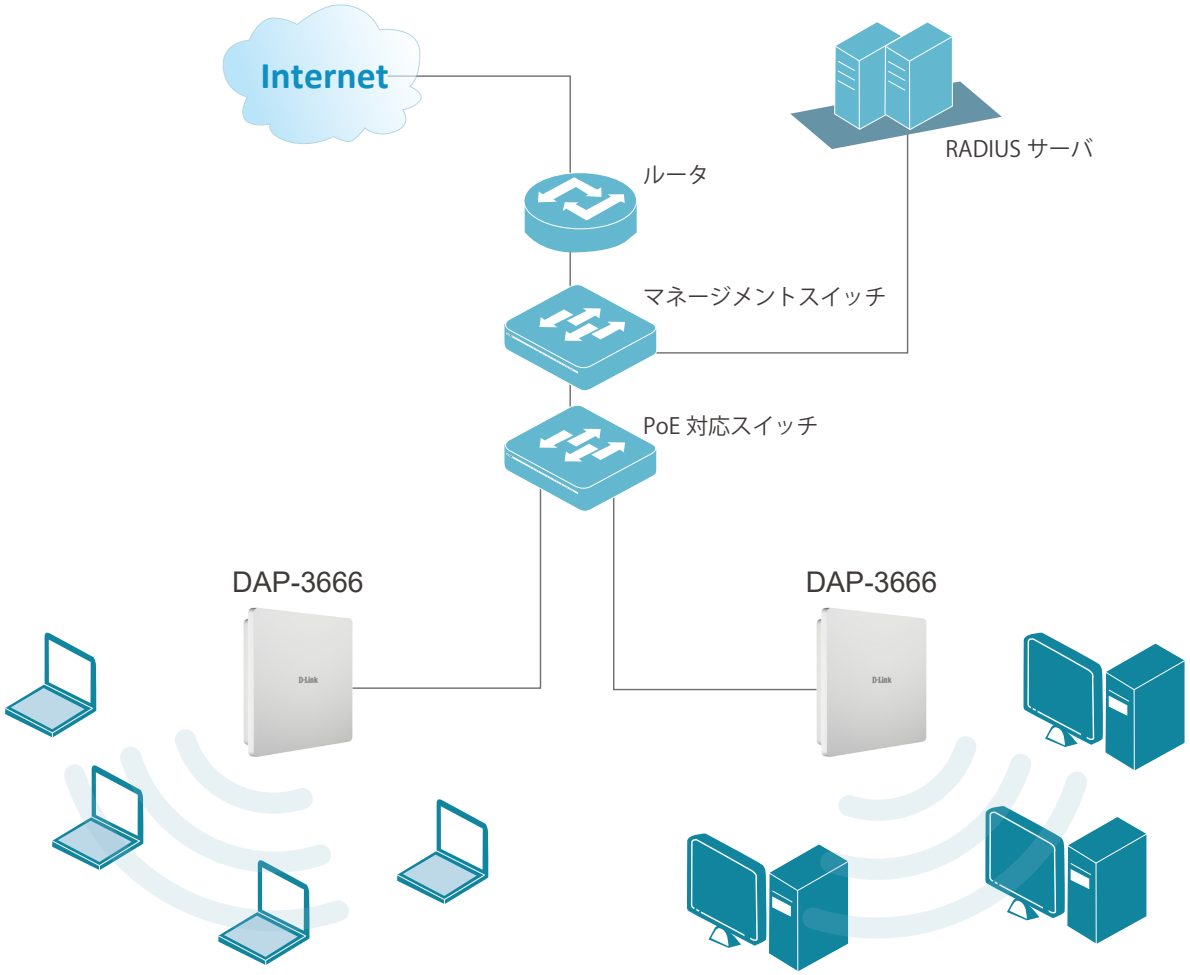
また、必ず本書および設置マニュアルをよくお読みいただき、内容をご理解いただいた上で記載事項に従ってご使用ください。

■ 本製品について.....5
機能概要.....5
本製品の特長.....5
製品名/品番一覧.....5
本製品の接続モード.....6
■ Nuclias Connectについて.....7
概要.....7
Nuclias Connectの特長.....7
■ 本マニュアルについて.....8
マニュアルの構成.....8
マニュアルの対象者.....8
表記規則.....8
■ 安全にお使いいただくために.....9
■ ご使用上の注意.....11
■ 静電気障害を防止するために.....11
■ 電源の異常.....11
■ 無線LANについて.....12
WLAN 技術を利用するさまざまな理由.....12
無線に関するご注意.....13

本製品について

■機能概要

D-Link DAP-3666はビジネス環境において最適なソリューションを提供するIEEE 802.11ac準拠のアクセスポイントです。



■本製品の特長

- IEEE 802.11a/b/g/n/ac 準拠
- デュアルバンド通信(2.4GHz/5GHz同時利用)
- WPA/WPA2/WPA3※1 Enterprise/Personal暗号方式
- MAC アドレスフィルタリング
- ARP スプーフィング防止
- マルチSSID（周波数帯ごと8個）
- SNMPv1/v2c※2
- QoS（WMM 準拠）
- GUI、SSL、SSH、Telnetによる設定/ 管理
- 4つの通信モード
- Nuclias Connectによる管理
- Wave2 対応
- MU-MIMO
- IP68対応

※1 WPA3はPersonalのみ
※2 一部のMIBのみのサポートであるため、限定的な管理のみの対応となります。

■製品名/品番一覧

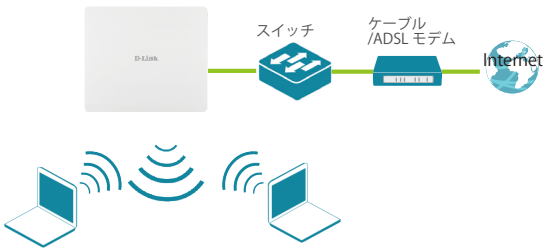
製品名	品番
DAP-3666	DAP-3666/A1

■本製品の接続モード

本製品には以下の4つの接続モードがあります。

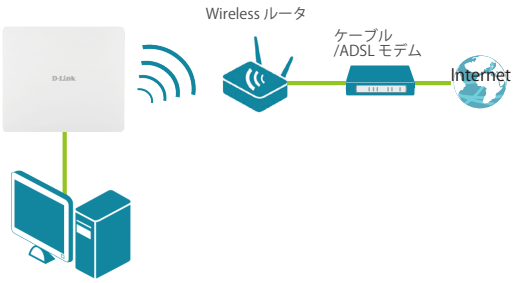
■アクセスポイントモード

無線アクセスポイントと無線クライアントのネットワークを構築します。



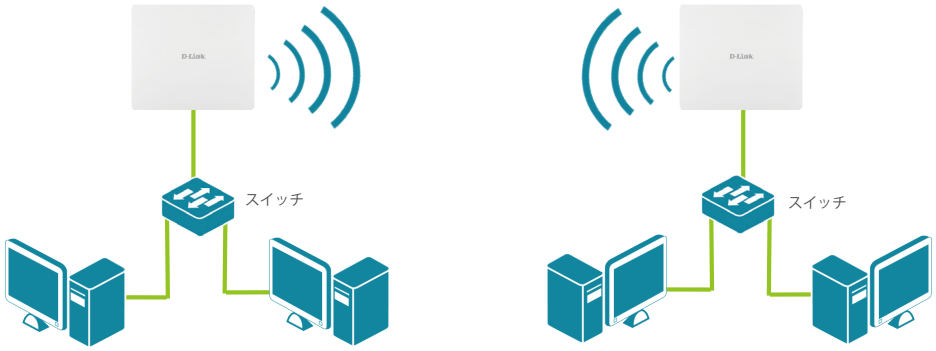
■ワイヤレスクライアントモード

イーサネット用機器向けの無線ネットワークアダプタとして動作します。



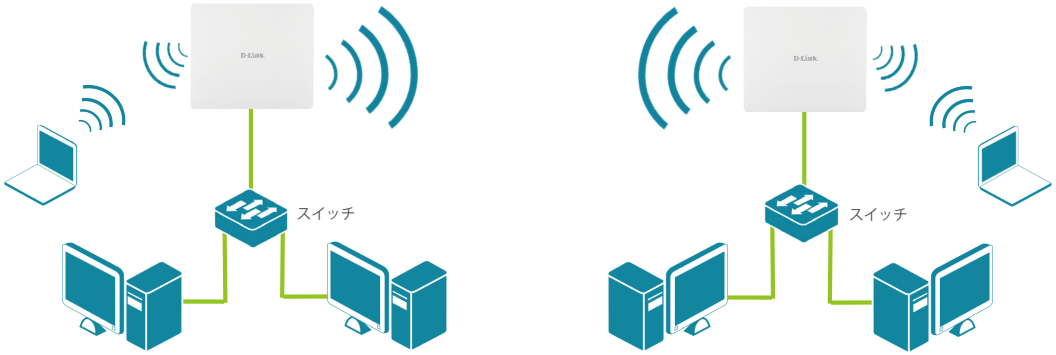
■WDS モード

複数のネットワークを無線接続します。



■WDS with AP モード

無線 LAN アクセスポイントとして動作しながら、複数のネットワークと無線接続します。



重要

異機種間、異なるファームウェアバージョン間でWDSモード、WDS with APモードを使用することはできません。

Nuclias Connectについて

■概要

Nuclias Connectは、中小企業向けのD-Linkの一元管理ソリューションです。Nuclias Connectを使用することで、ネットワークの分析、自動化、設定、最適化、拡張、セキュリティ保護が容易になり、企業ネットワークの包括的な管理ソリューションを実現します。本システムでは、堅牢で一元化された管理システムの維持と、小規模ネットワークから大規模ネットワーク（最大1000AP）へ拡張可能なコスト的/技術的な柔軟性を提供します。また、直感的なグラフィカルユーザインタフェース（GUI）、豊富な拡張AP機能、11言語をサポートするセットアップウィザードにより、導入、設定、および管理作業の煩わしさを最小限に抑えます。

Nuclias Connectは無償のダウンロードソフトウェアであり、ライセンス不要でWindowsサーバ（またはDocker経由によりLinux※1）、スマートフォン※2（簡易マネージメントアプリ）に導入して最大1,000台まで管理することができます。Nuclias Connectを搭載した安価なアプライアンス製品（Nuclias Connect Hub DNH-100）を利用することも可能です。

Nuclias Connectは、ネットワーク上のすべての無線アクセスポイント（AP）に対し、ソフトウェアベースによる監視・リモート管理を提供します。これにより、従来のハードウェアベースの統合管理システムに比べ、より柔軟性の高い管理ソリューションを実現します。（リモートからの設定、包括的/部分的なネットワークトラフィック分析、負荷分散、エアタイムフェアネス、ローカライズされたスロットリング）

Nuclias Connectでは、各ネットワークに対しローカル管理権限を付与することで、ネットワーク毎の管理を行うことができます。また、APは周波数帯ごとに8つのSSID（APごと最大16個のSSID）をサポートしており、管理者はこれらのSSIDを訪問者用のゲストネットワークとして設定することもできます。

Nuclias Connectは、APが同じレイヤ2/レイヤ3ネットワークに存在する場合に、最小限のユーザの労力によりAPの検出とプロファイルのインポートを実行します。これらの処理は、必要に応じてグループまたは個々のAPに対しても実施可能です。

Nuclias Connectのソフトウェアはネットワーク上で透過的に動作するため、APはNAT環境内の任意の場所に配置できます。管理者は各配置について、構成や管理者アカウントの設定など、さまざまな設定を提供および管理できます。

Nuclias Connectでは、SSIDごとにアクセス制御やユーザ認証を設定することが可能です。そのほか、キャプティブポータルやWi-Fiホットスポットなど、より高度な付加価値サービスを有効にすることもできます。これにより、異なるサブネットに対して個別の内部ネットワークを設定することができます。

※1 対応予定
※2 スマートフォンアプリは複数の拠点を管理したい場合に、プロファイルを適用するために必要となります。

■Nuclias Connectの特長

- 無償の管理ソフトウェア
- 各種ログ
- トラフィックのレポートと分析
- カスタマイズ可能なキャプティブポータル、802.1X認証、MACフィルタリング
- リモート設定およびバッチ設定
- 日本語GUI
- 直感的なインタフェース
- ネットワーク毎のアクセス権限

メモ

- Nuclias ConnectでDAP-3666を管理する手順に関する詳細は、Nuclias Connectユーザマニュアルを参照してください。

本マニュアルについて

■マニュアルの構成

1章：お使いになるまえに
本マニュアルの紹介と、本製品をお使いになる前の注意事項を記載しています。
→『お使いになるまえに：p.4』

2章：設置のしかた
本製品の各部名称と設置方法について説明します。
→『設置のしかた：p.16』

3章：WEB GUI画面について
WEB GUIへのログイン方法と画面構成について説明します。
→『WEB GUI 画面について：p.24』

4章：Basic Settings（基本設定）
アクセスポイントの無線モードやセキュリティなど、基本的な設定について説明します。
→『Basic Settings (基本設定)：p.29』

5章：Advanced Settings（基本設定）
マルチSSIDやVLAN、キャプティブポータルなど、アクセスポイントの詳細設定について説明します。
→『Advanced Settings (詳細設定)：p.44』

6章：Status（ステータス）
ファームウェアバージョンやクライアント情報、ログなど、ステータスの確認方法について説明します。
→『Status (ステータス)：p.90』

7章：管理メニュー
本製品の再起動やファームウェアアップデート、設定のリセットなど、管理を行う方法を説明します。
→『管理メニュー：p.99』

8章：付録
製品を向上出荷時の設定に戻す方法と、FAQ（よくご質問いただく内容）について記載しています。
→『付録：p.114』

■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

本マニュアルでは以下の記号を使用します。

⚠警告　この表示を無視し、間違った使い方をすると、火災や感電などにより人身事故になるおそれがあります。

⚠注意　この表示を無視し、間違った使い方をすると、傷害または物的損害が発生するおそれがあります。

重要　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。

メモ　特長や技術についての詳細情報を記述します。

本マニュアル中での字体、・記号についての表記規則は以下のとおりです。

字体	解説	例
『水色』	マニュアル内の参照先	『Basic Settings (基本設定)：p.29』

安全にお使いいただくために

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

安全上のご注意　必ずお守りください

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

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

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

⚠危険

🚫 禁止
分解・改造をしない
火災、やけど、けが、感電などの原因となります。

🚫 禁止
ぬれた手でさわらない
感電の原因となります。

🚫 禁止
水をかけたり、ぬらしたりしない
内部に水が入ると、火災、感電、故障の原因となります。

🚫 禁止
水などの液体（飲料水、汗、海水、ペットの尿など）でぬれた状態で触ったり、電源を入れたりしない
火災、やけど、けが、感電、故障の原因となります。

🚫 禁止
各種端子やスロットに水などの液体（飲料水、汗、海水、ペットの尿など）をいれない。万が一、入ってしまった場合は、直ちに電源プラグをコンセントから抜く
火災、やけど、けが、感電、故障の原因となります。

🚫 禁止
油煙、湯気、湿気、埃の多い場所、高温になる場所や熱のこもりやすい場所（火のそば、暖房器具のそば、こたつや布団の中、直射日光の当たる場所、炎天下の車内、風呂場など）、振動の激しい場所では、使用、保管、放置しない
火災、やけど、けが、感電、故障の原因となります。

🚫 禁止
内部に金属物や燃えやすいものを入れない
火災、感電、故障の原因となります。

🚫 禁止
砂や土、泥をかけたり、直に置いたりしない。また、砂などが付着した手で触れない
火災、やけど、けが、感電、故障の原因となります。

🚫 禁止
電子レンジ、IH 調理器などの加熱調理機、圧力釜など高圧容器に入れたり、近くに置いたりしない
火災、やけど、けが、感電、故障の原因となります。

⚠警告

🚫 禁止
落としたり、重いものを乗せたり、強いショックを与えたり、圧力をかけたりしない
故障の原因となります。

🚫 禁止
発煙、焦げ臭い匂いの発生などの異常状態のまま使用しない
感電、火災の原因になります。
使用を止めて、ケーブル / コード類を抜いて、煙が出なくなってから販売店に修理をご依頼ください。

🚫 禁止
表示以外の電圧で使用しない
火災、感電、または故障の原因となります。

🚫 禁止
たこ足配線禁止
たこ足配線などで定格を超えると火災、感電、または故障の原因となります。

❗
設置、移動のときは電源プラグを抜く
火災、感電、または故障の原因となります。

🚫 禁止
雷鳴が聞こえたら、ケーブル / コード類にはさわらない
感電の原因となります。

🚫 禁止
ケーブル / コード類や端子を破損させない
無理なねじり、引っ張り、加工、重いものの下敷きなどは、ケーブル / コードや端子の破損の原因となり、火災、感電、または故障の原因となります。

❗
本製品付属の AC アダプタもしくは電源ケーブルを指定のコンセントに正しく接続して使用する
火災、感電、または故障の原因となります。

🚫 禁止
各光源をのぞかない
光ファイバケーブルの断面、コネクタおよび本製品のコネクタや LED をのぞきますと強力な光源により目を損傷するおそれがあります。

🚫 禁止
各種端子やスロットに導電性異物（金属片、鉛筆の芯など）を接触させたり、ほこりが内部に入ったりしないようにする
火災、やけど、けが、感電または故障の原因となります。

🚫 禁止
使用中に布団で覆ったり、包んだりしない
火災、やけどまたは故障の原因となります。

❗
ガソリンスタンドなど引火性ガスが発生する可能性のある場所や粉じんが発生する場所に立ち入る場合は、必ず事前に本製品の電源を切る
引火性ガスなどが発生する場所で使用すると、爆発や火災の原因となります。

🚫 禁止
カメラのレンズに直射日光などを長時間あてない
素子の退色、焼付きや、レンズの集光作用により、火災、やけど、けがまたは故障の原因となります。

❗
無線製品は病院内で使用する場合は、各医療機関の指示に従って使用する
電子機器や医療電気機器に悪影響を及ぼすおそれがあります。

🚫 禁止
本製品の周辺に放熱を妨げるようなもの（フィルムやシールでの装飾を含む）を置かない
火災、または故障の原因となります。

❗
耳を本体から離してご使用ください
大きな音を長時間連続して聞くと、難聴などの耳の障害の原因となります。

❗
無線製品をご使用の場合、医用電気機器などを装着している場合は、医用電気機器メーカーもしくは、販売業者に、電波による影響について確認の上使用する
医療電気機器に悪影響を及ぼすおそれがあります。

❗
高精度な制御や微弱な信号を取り扱う電子機器の近くでは使用しない
電子機器が誤作動するなど、悪影響を及ぼすおそれがあります。

❗
ディスプレイ部やカメラのレンズを破損した際は、割れたガラスや露出した端末内部に注意する
破損部や露出部に触れると、やけど、けが、感電の原因となります。

❗
ペットなどが本機に噛みつかないように注意する
火災、やけど、けがなどの原因となります。

🚫 禁止
コンセントに AC アダプタや電源ケーブルを抜き差しするときは、金属類を接触させない
火災、やけど、感電または故障の原因となります。

🚫 禁止
AC アダプタや電源ケーブルに海外旅行用の変圧器等を使用しない
発火、発熱、感電または故障の原因となります。

⚠警告

- AC アダプタもしくは電源プラグについたほこりは、拭き取る
  ほこりが付着した状態で使用すると、
  火災、やけど、感電または故障の原因となります。
- AC アダプタや電源ケーブルをコンセントに
  さしこむときは、確実に差し込む
  確実に差し込まないと、火災、やけど、
  感電もしくは故障の原因となります。
- 接続端子が曲がるなど変形した場合は、直ちに使用を中止する。
  また、変形をもとに戻しての使用も行わない
  端子のショートにより、火災、やけど、けが、
  感電または故障の原因となります。
- 各種接続端子を機器本体に接続する場合、斜めに差したり、
  差した状態で引っ張ったりしない
  火災、やけど、感電または故障の原因となります。
- 使用しない場合は、AC アダプタもしくは
  電源ケーブルをコンセントから抜く
  電源プラグを差したまま放置すると、火災、やけど、
  感電または故障の原因となります。
- お手入れの際は、AC アダプタもしくは
  電源ケーブルをコンセントから抜く
  抜かずに行うと、火災、やけど、感電または故障の原因となります。
- 禁止 SD や MicroSD カード、USB メモリの使用中は、
  カードやメモリを取り外したり、本製品の電源を切ったりしない
  データの消失、機器本体の故障の原因となります。
- 禁止 磁気カードや磁気を帯びたものを本製品に近づけない
  磁気カードのデータが消えてしまうおそれもしくは
  機器本体の誤作動の原因となります。
- ディーリンクジャパンが販売している無線機器は
  国内専用のため、海外で使用しない
  海外では国によって電波使用制限があるため、
  本製品を使用した場合、罰せられる場合があります。
  海外から持ち込んだディーリンク製品や並行輸入品を
  日本国内で使用する場合も同様に、罰せられる場合があります。

⚠注意

- 禁止 乳幼児の手の届く場所では使わない
  やけど、ケガまたは感電の原因となります。
- 静電気注意
  コネクタや電源プラグの金属端子に触れたり、
  帯電したものを近づけますと故障の原因となります。
- 禁止 コードを持って抜かない
  コードを無理に曲げたり、引っ張ると、
  コードや機器本体の破損の原因となります。
- 禁止 振動が発生する場所では使用しない
  故障の原因となります。
- 付属品の使用は取扱説明書に従う
  本製品の付属品は、取扱説明書に従い、
  他の製品に使用しないでください。機器の破損の原因となります。
- 禁止 破損したまま使用しない
  火災、やけどまたはけがの原因となります。
- 禁止 ぐらついた台の上や傾いた場所などの
  不安定な場所や高所には置かない
  落下して、けがなどの原因となります。
- 禁止 子供が使用する場合は、保護者が取扱いの方法を教え、
  誤った使い方をさせない
  けがや故障などの原因となります。
- 本製品を長時間連続使用する場合は、
  温度が高くなることがあるため、注意する。
  また、使用中に眠ってしまうなどして、
  意図せず長時間触れることがないようにする
  温度の高い部分に直接長時間触れると
  お客様の体質や体調によっては肌の赤みや
  かゆみ、かぶれ、低温やけどの原因となります。
- 禁止 コンセントにつないだ状態で、AC アダプタや
  電源コンセントに長時間触れない
  やけど、感電の原因となります。
- 一般の電話機やコードレス電話、テレビ、ラジオなどを
  お使いになっている近くで使用しない
  近くで使用すると、本製品が悪影響を及ぼす原因となる場合があるため、
  なるべく離れた場所で使用してください。
- 禁止 D-Link が指定したオプション品がある場合は、
  指定オプションを使用する
  不正なオプション品を使用した場合、故障、破損の原因となります。

電波障害自主規制について

この装置は、クラス A 機器です。この装置を住宅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。

VCCI-A

ご使用上の注意

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

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

静電気障害を防止するために

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

1. 機器を箱から取り出すときは、機器をシステム等に取り付ける準備が完了するまで、本製品を静電気防止包装から取り出さないでください。静電気防止包装から取り出す直前に、必ず身体の静電気を逃がしてください。
2. 静電気に敏感な部品を運ぶ場合、最初に必ず静電気対策を行ってください。
3. 静電気に敏感な機器の取り扱いは、静電気のない場所で行います。可能であれば、静電気防止床パッド、作業台パッド、および帯電防止接地ストラップを使用してください。

電源の異常

万一停電などの電源異常が発生した / する場合は、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。

無線LANについて

業界標準に基づく弊社の無線 LAN 製品は、ご家庭や職場または公共の施設において、使いやすく互換性の高い高速の無線接続を提供します。これらを使用して時間や場所に関わらず必要なデータにアクセスすることができます。
WLAN は家庭やオフィス環境のみならず、空港やコーヒーショップ、または大学など公共の施設においても幅広く利用されるようになってきました。
この WLAN 技術を用いることにより、仕事やコミュニケーションがさらに効率的に行えるようになってきています。無線技術により可動性が増し、配線や固定のインフラが減少したことでユーザに大きなメリットが生まれました。
ノート型やデスクトップ型 PC に使用する無線アダプタはイーサネットのアダプタカードと同じプロトコルをサポートしており、無線ユーザは有線ネットワークと同じアプリケーションを利用できるようになりました。

■WLAN 技術を利用するさまざまな理由

可動性
WLAN の動作範囲内のどこからでもデータにアクセス可能であり、生産性を向上します。また、リアルタイムな情報に基づく管理により作業効率が向上します。

低い実現コスト
WLAN は設置、管理、変更、移転のすべてが簡単です。このような WLAN の扱いやすさはネットワークの変更が頻繁に要求される環境に適しています。WLAN は有線ネットワークでは困難であった場所へのネットワーク導入を可能にします。

簡単な設置と拡張
煩わしい複雑なケーブル配線作業、特に壁や天井へのケーブル敷設の必要がないため、手早く簡単にシステムの設置を行うことができます。無線技術は、ネットワークを家庭やオフィスを超えて拡張することで、さらなる多用途性を提供します。

低コストのソリューション
無線 LAN デバイスは、従来のイーサネット用機器とほぼ同等の価格設定となっています。本製品は設定可能な複数のモードで多機能性を提供し、コスト削減を行います。

柔軟性
配置する無線 LAN デバイスの数によって、ピアツーピアのネットワークが適している小さなユーザグループから大規模なインフラネットワークまで、自由自在に構築することができます。

世界基準対応の技術
無線機器は、IEEE802.11a、IEEE 802.11b、IEEE 802.11g、IEEE 802.11n および IEEE 802.11ac に準拠しています。

● IEEE 802.11ac 規格

IEEE 802.11ac 規格の無線通信速度は、最大 866.7Mbps までと高速化されており、5GHz 帯の周波数と「OFDM」技術をサポートしています。

● IEEE 802.11n 規格

IEEE 802.11n 規格は、従来の IEEE 802.11a、IEEE 802.11b および IEEE 802.11g の機能を拡張した規格です。無線通信速度は、最大 300Mbps までと高速化され、2.4GHz 帯および 5GHz 帯の周波数を利用し、こちらも「OFDM」技術をサポートしています。

これらにより、多くの環境化において、無線サービスエリア内でネットワークによる大容量の送受信や遅延の少ない MPEG 形式の映像の視聴などが可能になります。OFDM(Orthogonal Frequency Division Multiplexing) という技術により、この大容量のデジタルデータの高速伝送を無線で行うことができます。OFDM では、無線信号を小さいサブ信号に分割し、それらを同時に異なる周波数で送信します。OFDM により、信号伝送時のクロストーク（干渉）の発生を抑えることが可能です。

IEEE 802.11n 規格は、「WPA」を含む現在最も先進的なネットワークセキュリティ機能を提供します。
WPA/WPA2/WPA3 には企業向けの「 Enterprise」とホームユーザ向けの「Personal」の 2 種類があります。「WPA-Personal」と「WPA2-Personal」はユーザ認証に必要なサーバ機器を持たないホームユーザを対象としています。その認証方法は、無線ルータやアクセスポイントに「 Pre-Shared Key（ 事前共有鍵）」の定義を行うという点で WEP と似ています。クライアントとアクセスポイントの両方において、事前共有鍵が確認され条件が満たされた時にアクセスが認められます。

「WPA-Enterprise」と「 WPA2-Enterprise」「WPA3-Enterprise」は既にセキュリティ用にインフラが整備されている企業を対象としています。ネットワーク内のサーバを中心にネットワーク管理とセキュリティの実施を行うような環境を想定しています。
ネットワーク管理者は、RADIUS サーバ上で 802.1X を使用し、無線 LAN へのアクセスを許可するユーザのリストを定義します。「WPA-Enterprise」または「 WPA2-Enterprise」「WPA3-Enterprise」を実装した無線 LAN にアクセスする場合、ユーザはユーザ名とパス

ワードの入力を要求されます。ユーザがネットワーク管理者によってアクセスを許可されており、正しいユーザ名とパスワードを入力すると、ネットワークへのアクセスが可能になります。例えば、ある社員が会社を辞めるというような場合、ネットワーク管理者がアクセス許可者のリストからその社員のデータを削除すれば、ネットワークを危険にさらすことは避けることができます。

EAP（ Extensible Authentication Protocol）は Windows OS に実装されています。802.1X の機能を使用する際には、ネットワークにおけるすべてのデバイスの EAP タイプを同一にする必要があります。

重要

最大の無線信号速度は理論値であり、実際のデータスループットは異なります。ネットワーク条件と環境には、ネットワークトラフィック量、建築材料や工事、ネットワークオーバヘッドが含まれ、実際のデータスループット速度は低くなります。環境条件は無線信号範囲に悪影響を与えます。

■無線に関するご注意

電波に関するご注意

本製品は、電波法に基づく小電力データ通信システムの無線製品として、技術基準適合証明を受けています。従って、本製品を使用する上で、無線局の免許は必要ありません。
本製品は、日本国内でのみ使用できます。

以下の注意をよくお読みになりご使用ください。

● 本製品を以下の場所では使用しないでください。

- 心臓ペースメーカー等の産業・科学・医療用機器の近くで使用すると電磁妨害を及ぼし、生命の危険があります。
- 工場の製造ライン等で使用されている移動体識別用の構内無線局 (免許を必要とする無線局) および特定小電力無線局 (免許を必要としない無線局)
- 電子レンジの近くで使用すると、電子レンジによって無線通信に電磁妨害が発生します。
- 電気製品、AV 機器、OA 機器などの磁気を帯びているところや電磁波が発生しているところで使用すると下記のような影響があります。
  - 磁気や電気雑音の影響を受けると雑音が大きくなったり、通信ができなくなったりすることがあります。
  - テレビ、ラジオなどに近いと受信障害の原因となったり、テレビ画面が乱れたりすることがあります。
  - 近くに複数の無線 LAN アクセスポイントが存在し、同じチャネルを使用していると、正しく検索できない場合があります。

● 本製品は技術基準適合証明を受けています。本製品の分解、改造、および裏面の製品ラベルをはがさないでください。

2.4GHz 帯使用の無線機器の電波干渉に関するご注意

本製品の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用している移動体識別用の構内無線局 (免許を必要とする無線局) および特定小電力無線局 (免許を必要としない無線局) 並びにアマチュア無線局 (免許を必要とする無線局) が運用されています。

● 本製品を使用する前に、近くで移動体識別用の構内無線局および特定小電力無線局並びにアマチュア無線局が運用されていないことを確認してください。

● 万一、本製品から移動体識別用の構内無線局に対して有害な電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか、または電波の発射を停止してください。

● その他、本製品から移動体通信用の特定小電力無線局に対して電波干渉の事例が発生した場合など、何かお困りのことが起きたときは、弊社サポート窓口へお問い合わせください。

使用周波数帯域	2.4GHz 帯
変調方式	DS-SS 方式 /OFDM 方式
想定干渉距離	40m 以下
周波数変更可否	全帯域を使用し、かつ移動体識別用の構内無線局および特定小電力無線局並びにアマチュア無線局の帯域を回避可能

5GHz 帯使用に関するご注意

無線 LAN の 5.2/5.3GHz（W52/W53）をご利用になる場合、電波法の定めにより屋外ではご利用になれません。

無線 LAN 製品ご使用時におけるセキュリティに関するご注意

無線 LAN では、LAN ケーブルを使用する代わりに、電波を利用してパソコン等と無線アクセスポイント間で情報のやり取りを行うため、電波の届く範囲であれば自由に LAN 接続が可能であるという利点があります。
その反面、電波はある範囲内であれば障害物（壁等）を越えてすべての場所に届くため、セキュリティに関する設定を行っていない場合、以下のような問題が発生する可能性があります。

● 通信内容を盗み見られる

悪意ある第三者が、電波を故意に傍受し、以下の通信内容を盗み見られる可能性があります。
- ID やパスワード又はクレジットカード番号等の個人情報
- メールの内容

● 不正に侵入される

悪意ある第三者が、無断で個人や会社内のネットワークへアクセスし、以下の行為を行う可能性があります。
- 個人情報や機密情報を取り出す（情報漏洩）
- 特定の人物になりすまして通信し、不正な情報を流す（なりすまし）
- 傍受した通信内容を書き換えて発信する（改ざん）
- コンピュータウィルスなどを流しデータやシステムを破壊する（破壊）

本来、無線 LAN カードや無線アクセスポイントは、これらの問題に対応するためのセキュリティの仕組みを持っていますので、無線 LAN 製品のセキュリティに関する設定を行って製品を使用することで、その問題が発生する可能性は少なくなります。
セキュリティの設定を行わないで使用した場合の問題を充分理解した上で、お客様自身の判断と責任においてセキュリティに関する設定を行い、製品を使用することをお奨めします。

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

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

⚠注意

製品に貼られているラベルや「Warranty Void Sticker」（シール）をはがさないでください。はがしてしまうとサポートを受けられなくなります。
※当社出荷時に「Warranty Void Sticker」（シール）が貼られていない製品もあります。

- 本書の記載内容に逸脱した使用の結果発生した、いかなる障害や損害において、弊社は一切の責任を負いません。あらかじめご了承ください。
- 弊社製品の日本国外でご使用の際のトラブルはサポート対象外になります。
- 弊社は、予告なく本書の全体または一部を修正・改訂することがあります。
- 弊社は改良のため製品の仕様を予告なく変更することがあります。

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

⚠警告

本書の内容の一部、または全部を無断で転載したり、複写することは固くお断りします。

設置のしかた

2

本製品の各部名称や、設置する際の準備・方法について説明します。
設置を行う際にお読みください。

■ パッケージの内容 17

■ 動作環境 17

■ ネットワーク接続前の準備 17

設置にあたってのご注意 17

■ 本体各部名称 19

前面パネル/背面パネル 19

底面 19

■ LED表示 19

■ 製品の設置 20

■ ネットワークと電源への接続 23

PoEスイッチによる電源投入 23

PoEインジェクタによる電源投入 23

パッケージの内容

本製品には、以下のものが同梱されています。

- 本体
- 柱/壁取り付けキット
  - マウントプレート
  - 壁取り付け用ネジ、アンカー
  - 柱取り付け用ストラップ
  - マウント用ネジ
- 六角レンチ
- LANポート用防水コネクタキット
- LANポートカバー
- アース線
- アース線用ネジ
- クイックインストールガイド
- PLシート

メモ

電源アダプタは付属していません。システムの電源供給には、PoEスイッチまたはPoEインジェクタを使用します。

万一、不足しているものや損傷を受けているものがありましたら、ご購入いただきました代理店にご連絡ください。

動作環境

本製品の動作には、以下の環境が必要です。

- Webブラウザ
  - Mozilla Firefox
  - Apple Safari
  - Google Chrome

※ブラウザの仕様により互換性が確保されない場合があります。

- イーサネットへの接続

ネットワーク接続前の準備

アクセスポイントの設置場所が性能に大きな影響を与えます。以下の注意事項に従って本製品を設置してください。

⚠注意

- 弊社が承認していないPoE 給電機器に本アクセスポイントを接続すると、本アクセスポイントが破損する場合があります。
- 本製品の設置は各地の建築条例等に関しての知識があり、資格保有者及び経験のある管理者によって設置を行ってください。経験及び資格保有のある管理者以外が設置し問題が発生した場合は、D-Link 製品の保証が無効となります。本製品やアンテナの屋外での設置に際して、怪我や破損、また違法行為に関してD-Link は一切の責任を負いませんのでご注意ください。
- 屋外設置時には雷や静電気からの感電防止のために、必ずアースを取り付けてください。また、各国の安全基準に準じて設置する必要があります。本製品の屋外設置に関して不明な点がある場合は、必ず資格のある電気工事士にご相談ください。
- DAP-3666 はIEC 規格の一つであるIP68 を取得しており、防塵構造及びすべての方向からの水の直接噴流によっても影響を受けない保護構造となっております。ただし、水中・水圧のかかる場所での使用は避け、屋外でも屋根等がある場所での使用を推奨いたします。
- DAP-3666は、ヒーターを内蔵していないため、マイナス温度の環境では、初期起動させることができませんので、ご注意ください。

● 設置にあたってのご注意

本製品の使用により、動作範囲内にて無線でネットワークアクセスが可能になります。
しかし、壁や天井など、無線信号が通過する物体の数や厚さ・場所などにより、動作範囲が制約を受ける場合があります。
一般的には、構造物の材質や設置場所での無線周波数のノイズが動作範囲に影響を与えます。

◆ 本製品と他のネットワークデバイスとの間に入る壁や天井の数をできるだけ少なくしてください。壁や天井の影響により、本製品の動作範囲は 1 ～ 30 メートルの範囲となります。間に入る障害物の数を減らすようデバイスの位置を工夫してください。

- ネットワークデバイス間の直線距離にご注意ください。厚さ 50 センチの壁を 45 度の角度で無線信号が通過する時、通り抜ける壁の厚みは約 1 メートルになります。2 度の角度で通過すると、通り抜ける厚みは 14 メートルになります。
  信号が障害物をなるべく直角に通過するような位置にデバイスを設置し、電波を受信しやすくしてください。

- 無線信号の通過性能は建築材料により異なります。金属製のドアやアルミの金具などは動作範囲を小さくする可能性があります。無線 LAN デバイスや無線 LAN アダプタ使用のコンピュータの設置は、信号がなるべく乾式壁か開放された戸口などを通るような位置に設置してください。

- 周波数ノイズを発生する電気機器や家電製品からは、最低でも 1、2 メートル離してデバイスを設置してください。

- 2.4GHz のコードレス電話または X-10（シーリングファン、ライト、およびホームセキュリティシステムなどの無線製品）を使っている場合、ご使用の無線接続は著しく性能が低下するか、または完全に切断される可能性があります。2.4GHz 電話の親機は可能な限りご使用の無線機器から離れていることを確認してください。電話を使用していない場合でも、親機は信号を送信します。

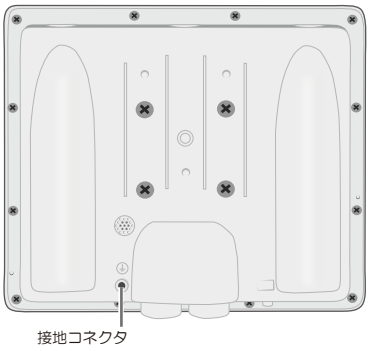
⚠注意

本アクセスポイントは、IEEE 802.3af 準拠の給電スイッチまたは弊社が承認する給電機器から受電することができます。弊社が承認していないPoE 給電機器に本アクセスポイントを接続すると、本アクセスポイントが破損する場合があります。

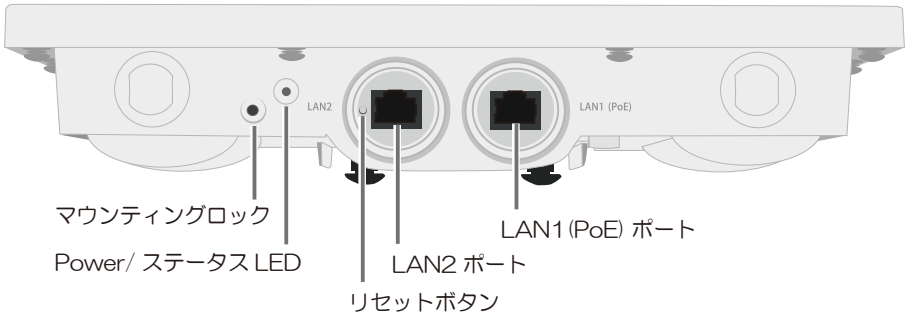
本体各部名称

アクセスポイントの各部名称について説明します。

■前面パネル/背面パネル



■底面



名称	説明
マウンティングロック	マウントキットで本製品を設置する際に使用します。
Power/ ステータスLED	電源およびネットワークのステータスを表します。
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。
LAN2ポート	RJ-45ケーブルを挿入し、ネットワークへの接続を行います。
LAN1 (PoE) ポート (10BASE-T/100BASE-TX/1000BASE-T)	RJ-45ケーブルを挿入し、ネットワークへの接続を行います。 PoE による受電を行うこともできます。

LED表示

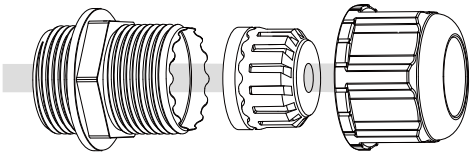
Power/ステータスLEDの表示内容について説明します。

LED	色	状態	状況説明
POWER/ ステータス LED	緑	点灯	動作中です。 正しく起動しました。
	赤	点灯	故障・不具合が発生しています。
		点滅	起動中です。

製品の設置

1. イーサネットケーブルに防水コネクタを装着し、DAP-3666 の LAN1（PoE）ポートに接続します。

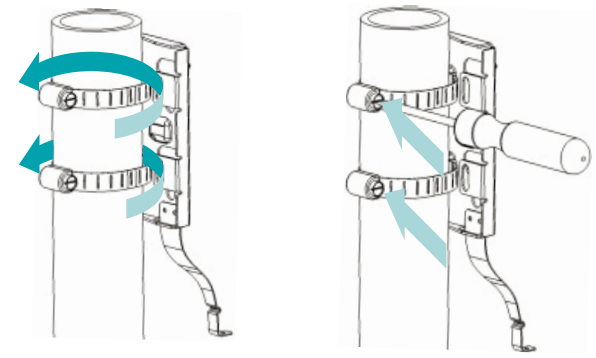
   防水コネクタは以下のように装着してください。



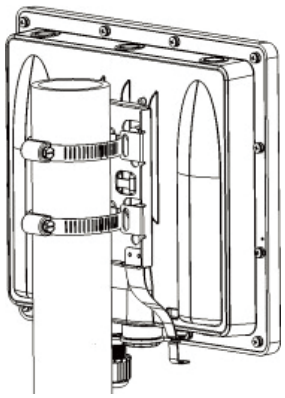
2. アクセスポイントを柱または壁に取り付けます。

◆ **柱に取り付ける場合：**

1. 2 つのストラップを使用し、マウントプレートを柱に取り付けます。
   ストラップのロック部分がしっかりと固定されていることを確認してください。

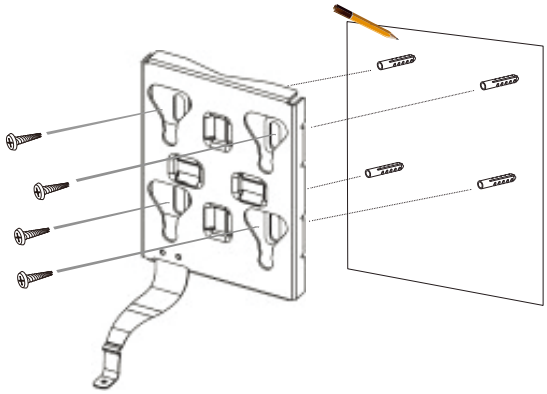


2. DAP-3666 の位置を合わせ、下にスライドさせてマウントプレートに取り付けます。

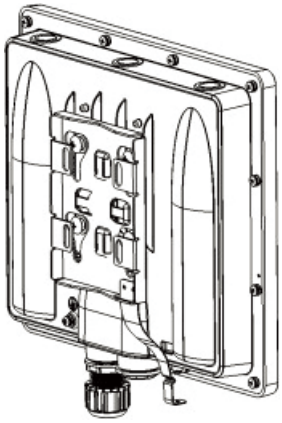


◆ **壁に取り付ける場合：**

1. アクセスポイントを取り付ける壁にマウントプレートを合わせ、穴をあける位置に印を付けます。

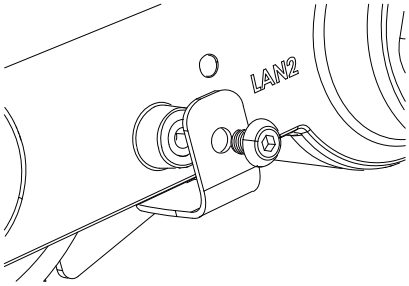


2. 印を付けた位置に穴を開け、付属のアンカーを挿入します。
3. マウントプレートをアンカーの上に配置し、付属のネジを使用してマウントプレートを壁面に取り付けます。
4. DAP-3666 の位置を合わせ、下にスライドさせてマウントプレートに取り付けます。

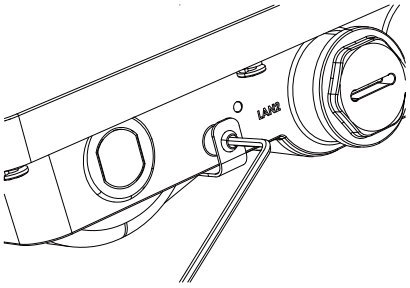


3. 取り付けネジを固定します。

1. マウント用ネジ（六角穴）を使用し、DAP-3666 を柱用 / 壁用マウントプレートに固定します。

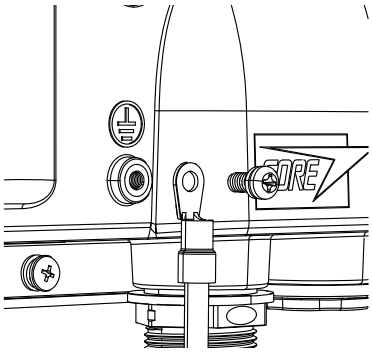


2. 付属の六角レンチを使用し、マウント用ネジをしっかりと締めてください。

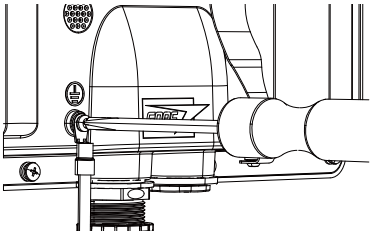


4. アース線を DAP-3666 に接続します。

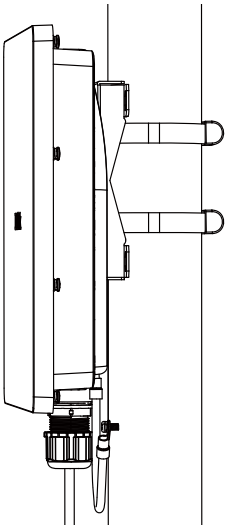
1. アース線は、落雷や静電気の蓄積からデバイスを保護するためのものです。付属のアース線用ネジを使用して、アース線を DAP-3666 に取り付けます。



2. アース線がしっかり固定されるようにネジを締めてください。



3. アース線のもう片方を柱または壁に取り付けます。



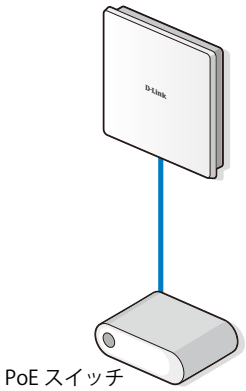
ネットワークと電源への接続

次のいずれかの方法により、アクセスポイントに電力を供給します。

- PoEスイッチによる電源投入
- PoEインジェクタによる電源投入

● PoEスイッチによる電源投入

1. イーサネットケーブルの一端を本製品の「LAN1 (PoE) 」ポートに接続し、もう一端を PoE スイッチに接続します。

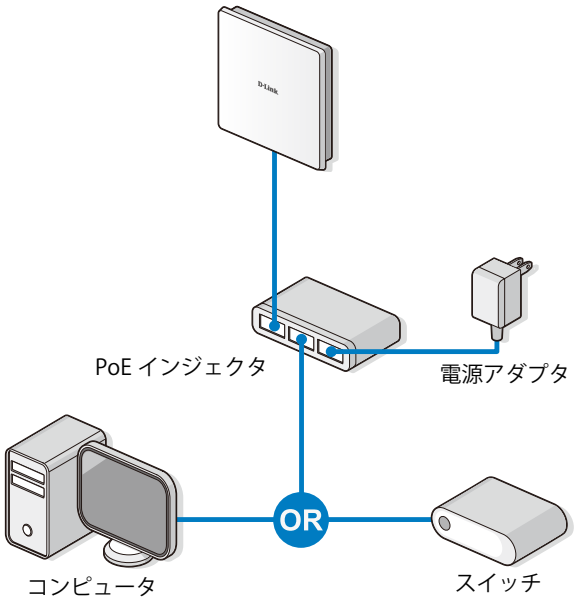


重要

本製品はPoEスイッチ側でClass4として認識されますが、Class3での給電で問題なく動作いたします。

● PoEインジェクタによる電源投入

1. イーサネットケーブルの一端を PoE インジェクタの入力ポートに接続し、もう一端をスイッチやルータ、コンピュータのポートに接続します。
2. イーサネットケーブルの一端を PoE インジェクタの出力ポートに接続し、もう一端を本製品の「LAN1 (PoE) 」ポートに接続します。
3. PoE インジェクタの電源アダプタを接続します。



メモ

本製品に電源が供給されると、POWER/ステータス LED が点灯します。

WEB GUI 画面について 3

本製品は、WEB GUI画面から設定・操作を行うことができます。
WEB GUI画面へのログイン方法と画面構成について説明します。

■ WEB GUI画面へのログイン 25
初回ログイン時のセットアップ 26
■ 画面の構成 28

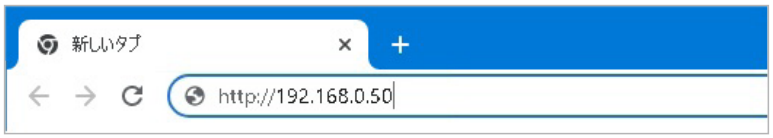
WEB GUI画面へのログイン

1. LAN に接続します。

◆ **イーサネット接続の場合：**
イーサネットケーブルを使用して、DAP-3666を管理用コンピュータ、または管理用コンピュータが接続されているスイッチやルータに接続します。

◆ **無線接続の場合：**
管理コンピュータをDAP-3666のデフォルトのマルチSSID「dlink」に接続します。

2. Web ブラウザを起動し、本製品のアドレスを入力します。

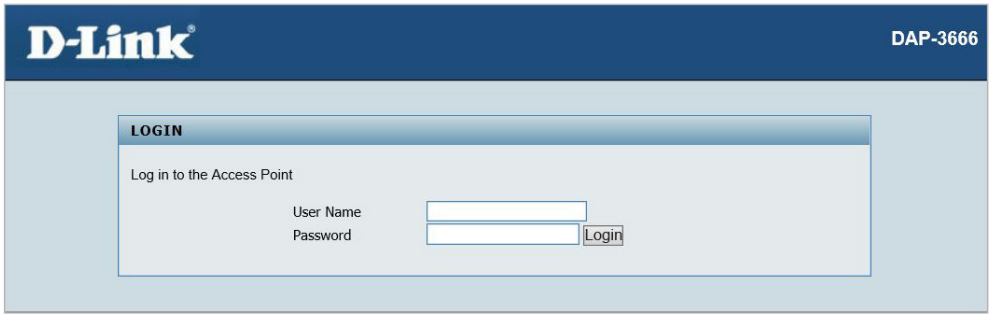


メモ

本製品は初期値で「DHCPクライアント」として設定されています。
・DHCPサーバからIP アドレスを割り振られる環境にある場合、「http://dap3666XXXX.local」と入力し、ログインします。
・DHCPサーバが無効の環境の場合、「http://192.168.0.50」と入力しログインします。

※「XXXX」は、AP本体の背面にあるデバイスラベルに記載されている、MACアドレスの最後の4ケタです。ご利用の環境に複数のAPが存在する場合は指定する必要があります。

3. 「User Name」と「Password」を入力し、管理インタフェースにログインします。

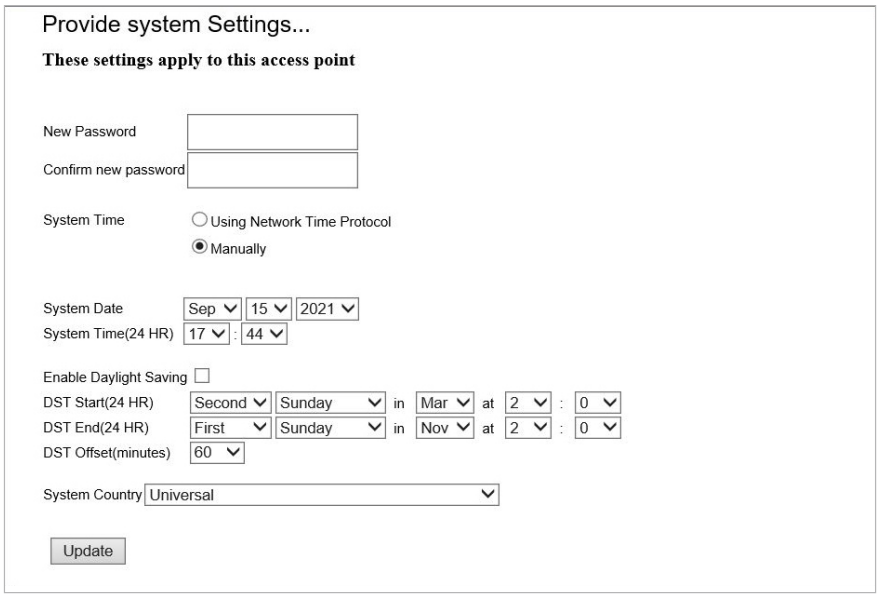


工場出荷時の設定は以下の通りです。
・User Name：admin
・Password：admin

■初回ログイン時のセットアップ

1. WEB GUI 画面への初回ログイン後、以下のセットアップウィザードが表示されます。

管理者パスワードや時刻、国の設定を行ってください。



項目	説明
New Password	本製品の新しい管理者パスワードを入力します。 入力した文字は他人から見えないように「●●●」と表示されます。 ・入力可能文字数：8-30文字以内（半角英数字）
Confirm new password	確認のため、新しい管理者パスワードを再度入力します。
System Time	時間の設定方法を以下から選択します。 ・[Using Network Time Protocol]：NTPサーバを使用して時間設定を行います。 ・[Manually]：手動で時間設定を行います。
NTP Server Address/ Name	NTPサーバのホスト名またはIPアドレスを設定します。 本項目は [Using Network Time Protocol（NTP）] を選択した場合にのみ表示されます。
Time Zone	プルダウンメニューからローカルタイムゾーンを選択します。 本項目は [Using Network Time Protocol] を選択した場合にのみ表示されます。 ・初期値：[Pacific Time（US/Canada）, Tijuana]
System Date	本製品に設定する日付を設定します。 本項目は [Manually] を選択した場合にのみ表示されます。
System Time（24 HR）	本製品に設定する時刻を設定します。 本項目は [Manually] を選択した場合にのみ表示されます。
Enable Daylight Saving	チェックを入れ、Daylight Savings Time（DST/サマータイム）を有効化します。
DST Start（24 HR）	Daylight Savings Time（サマータイム）の開始日時を設定します。
DST End（24 HR）	Daylight Savings Time（サマータイム）の終了日時を設定します。
DST Offset（minutes）	Daylight Savings Time（サマータイム）のオフセット時間（単位：分）を設定します。
System Country	本製品をご利用になる国として、[Japan]（日本）を選択してください。

2. 「Update」ボタンをクリックし、設定を適用します。

メモ

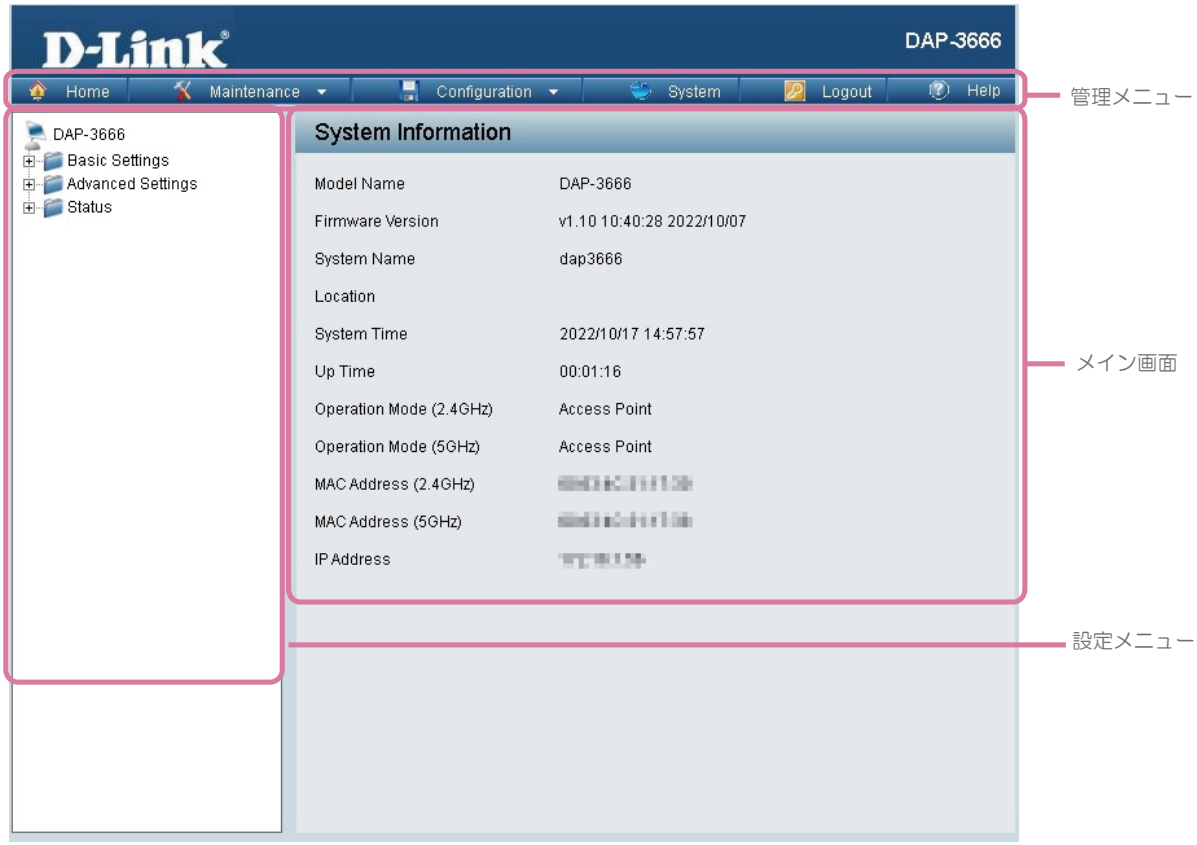
・パスワードはアルファベット＋数字を含む8-30文字以内で指定する必要があります。
・設定完了後、デバイスが再起動されます。

3. 新しいパスワードを入力して再度ログインします。以下の画面が表示されます。

WEB GUIからログアウトする場合は、画面右上の「Logout」からログアウトを行ってください。

画面の構成

WEB GUI画面の構成について説明します。



● 管理メニュー

- Home :
  クリックすると、System Information 画面が表示されます。
- Maintenance :
  管理者権限の設定やファームウェアのアップロードなど、本製品のメンテナンスを行います。
- Configuration :
  設定の保存・取り消しを行います。
- System :
  本製品の再起動・工場出荷時設定へのリセットを行います。
- Logout :
  WEB GUIからのログアウトを行います。
- Help :
  ヘルプ画面が表示されます。

メモ

管理メニューの詳細については、『管理メニュー：p.99 』を参照してください。

● 設定メニュー

アクセスポイントの無線モードやセキュリティなど、各機能の設定を行います。

メモ

設定メニューの詳細については、『Basic Settings (基本設定)：p.29 』『Advanced Settings (詳細設定)：p.44 』『Status (ステータス)：p.90 』を参照してください。

● メイン画面

設定メニューおよび管理メニューで選択した項目の設定画面が表示されます。

Basic Settings（基本設定）

4

アクセスポイントの無線モードやセキュリティなどの設定を行います。

■ Basic Settings について 30

■ Wireless Settings（ワイヤレス設定）..... 30

Access Point モードを選択した場合 31

WDSモード／WDS with APモードを選択した場合 33

Wireless Clientモードを選択した場合 35

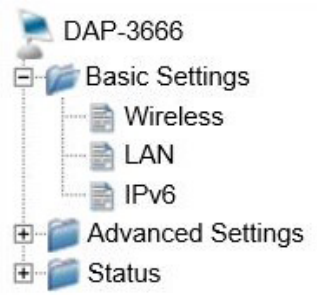
Authentication（認証）の設定について 37

■ LAN Settings（LAN設定）..... 42

■ IPv6 Settings（IPv6設定）..... 43

Basic Settings について

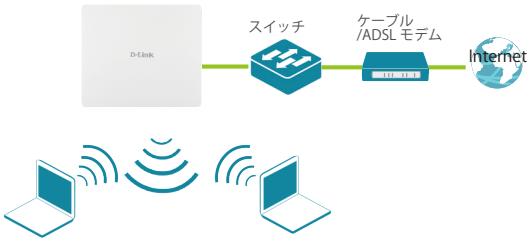
Basic Settings（基本設定）では、アクセスポイントの通信モードの選択やセキュリティ設定、LANの設定などを行います。



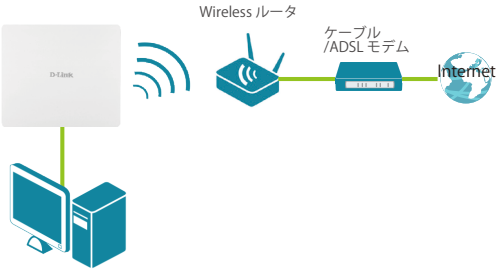
Wireless Settings （ワイヤレス設定）

アクセスポイントの通信モードを選択し、それに応じてネットワーク名（SSID）や認証方法などの設定を行います。
選択できる通信モードは以下の通りです。
※WDSモード、WDS with APモードは2.4GHz帯でのみ利用可能です。

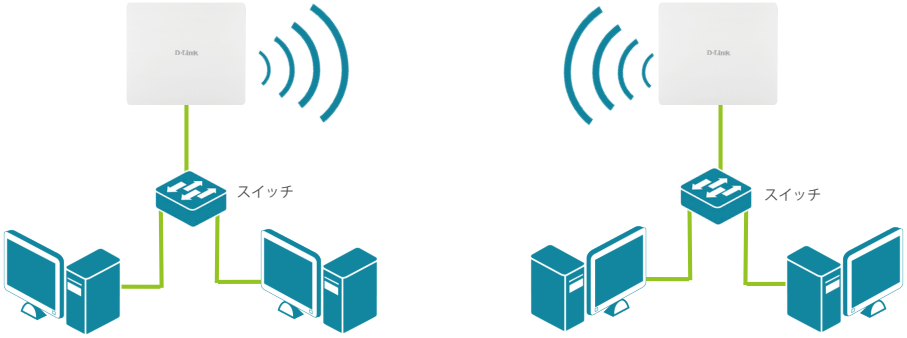
■アクセスポイントモード
無線アクセスポイントと無線クライアントのネットワークを構築します。



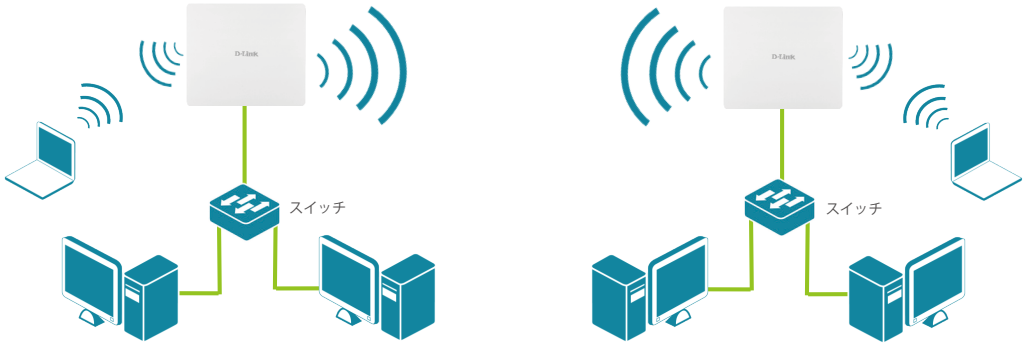
■ワイヤレスクライアントモード
イーサネット用機器向けの無線ネットワークアダプタとして動作します。



■WDS モード
複数のネットワークを無線接続します。



■WDS with AP モード
無線 LAN アクセスポイントとして動作しながら、複数のネットワークと無線接続します。



1. [Basic Settings] > [Wireless] を選択します。
2. [Wireless Band] で周波数帯を [2.4GHz] または [5GHz] に設定します。
3. [Operation Mode] で、アクセスポイントの通信モードを以下から選択します。
   - [Access Point] /[WDS with AP]/ [WDS] /[Wireless Client]
     ※WDSモード、WDS with APモードは2.4GHz帯でのみ利用可能です。
4. 選択した通信モードに応じて必要な設定を行います。
5. 設定完了後、[Save] をクリックします。

■Access Point モードを選択した場合

本製品は無線アクセスポイントとして動作し、無線クライアントとのネットワークを構築します。

項目	説明
Wireless Band	周波数帯を [2.4GHz] または [5GHz] に設定します。
Operation Mode	通信モードを選択します。 ・選択肢：[Access Point] [WDS with AP] [WDS] [Wireless Client]
Network Name (SSID)	ネットワーク名（SSID）を入力します。 ・初期値：[dlink] ・入力可能文字数：32文字以内（大文字と小文字は区別されます。） SSID（Service Set Identifier）とは、無線LANのアクセスポイントを識別するための名前です。無線LANのアクセスポイントが複数ある場合、どのアクセスポイントに接続するかを指定する必要があり、SSIDはその際に使用されます。

項目	説明
SSID Visibility	SSIDの表示を有効または無効にします。 ・選択肢：[Enable]（有効）[Disable]（無効） [Enable]（有効）に設定すると、SSIDがネットワークにブロードキャストされ、すべてのネットワークユーザがSSIDを閲覧できるようになります。
Auto Channel Selection	自動チャネル選択を有効または無効にします。 ・選択肢：[Enable]（有効）[Disable]（無効） [Enable]（有効）に設定すると、アクセスポイント起動時、自動的に最適なチャネルを選択します。
Channel	[Auto Channel Selection] を無効にした場合に、チャネルを選択します。
Channel Width	チャネル帯域を選択します。 ・選択肢：[20MHz][Auto 20/40MHz][Auto 20/40/80MHz] [Auto 20/40/80MHz]は5GHzを選択した場合のみ選択可能です。
Authentication	認証方式を選択します。 ・選択肢：[Open System][Shared Key][WPA-Personal][WPA-Enterprise][802.1X] [Enhance Open]
802.11k/v/r	ファストローミング機能を有効または無効にします。 ・選択肢：[Enable]（有効）[Disable]（無効） 重要 DAP-3666は802.11k/rのみサポートしています。802.11vはサポートしていません。

メモ

[Authentication]（認証）の設定内容は、選択した方式によって異なります。
詳細は『Authentication（認証）の設定について：p.37 』を参照してください。

重要

- 周辺APが多い（128以上のSSIDがある)場合、Auto Channel Selectionが適切に機能しません。実際の上限数はビーコン情報量に依存し、これより少なくなる可能性があります。
- Channel設定において、144chはサポートされていません。
- WPA/WPA2-PSK、WPA/WPA2-EAP、802.1xなどの認証を使用する場合、対象のSSIDはいずれかの VLANが割り当てられている必要があります。
- 5GHz帯をご利用の際、DFSによるレーダー検知によりW56帯の空きチャネルがない場合、既定の時間、停波します。

■WDSモード／WDS with APモードを選択した場合

WDSモードの場合：
複数のネットワークと無線接続します。

WDS with APモードの場合：
本製品は無線LAN アクセスポイントとして動作しながら、複数のネットワークと無線接続します。

※WDSモード、WDS with APモードは2.4GHz帯でのみ利用可能です。

項目	説明
Wireless Band	周波数帯を [2.4GHz] に設定します。
Operation Mode	通信モードを選択します。 ・選択肢：[Access Point] [WDS with AP] [WDS] [Wireless Client]
Network Name (SSID)	ネットワーク名（SSID）を入力します。 ・初期値：[dlink] ・入力可能文字数：32文字以内（大文字と小文字は区別されます。） SSID（Service Set Identifier）とは、無線LANのアクセスポイントを識別するための名前です。 無線LANのアクセスポイントが複数ある場合、どのアクセスポイントに接続するかを指定する必要があり、SSIDはその際に使用されます。
Auto Channel Selection	通信モードに [WDS][WDS with AP] を選択した場合はご利用できません。
Channel	固定のチャネルを設定します。
Channel Width	チャネル帯域を選択します。 ・選択肢：[20MHz][Auto 20/40MHz][Auto 20/40/80MHz] ※[Auto 20/40/80MHz] は5GHzを選択した場合のみ選択可能です。
AP MAC Address	ネットワーク上にある対向のアクセスポイントのMACアドレスを入力します。

項目	説明
Site Survey	[Scan] をクリックしてサイトサーベイを実行します。 サイトサーベイを実行し、検出された稼働中のアクセスポイントから、接続するネットワークをクリックします。
Authentication	認証方式を選択します。 ・選択肢：[Open System][WPA-Personal]

メモ

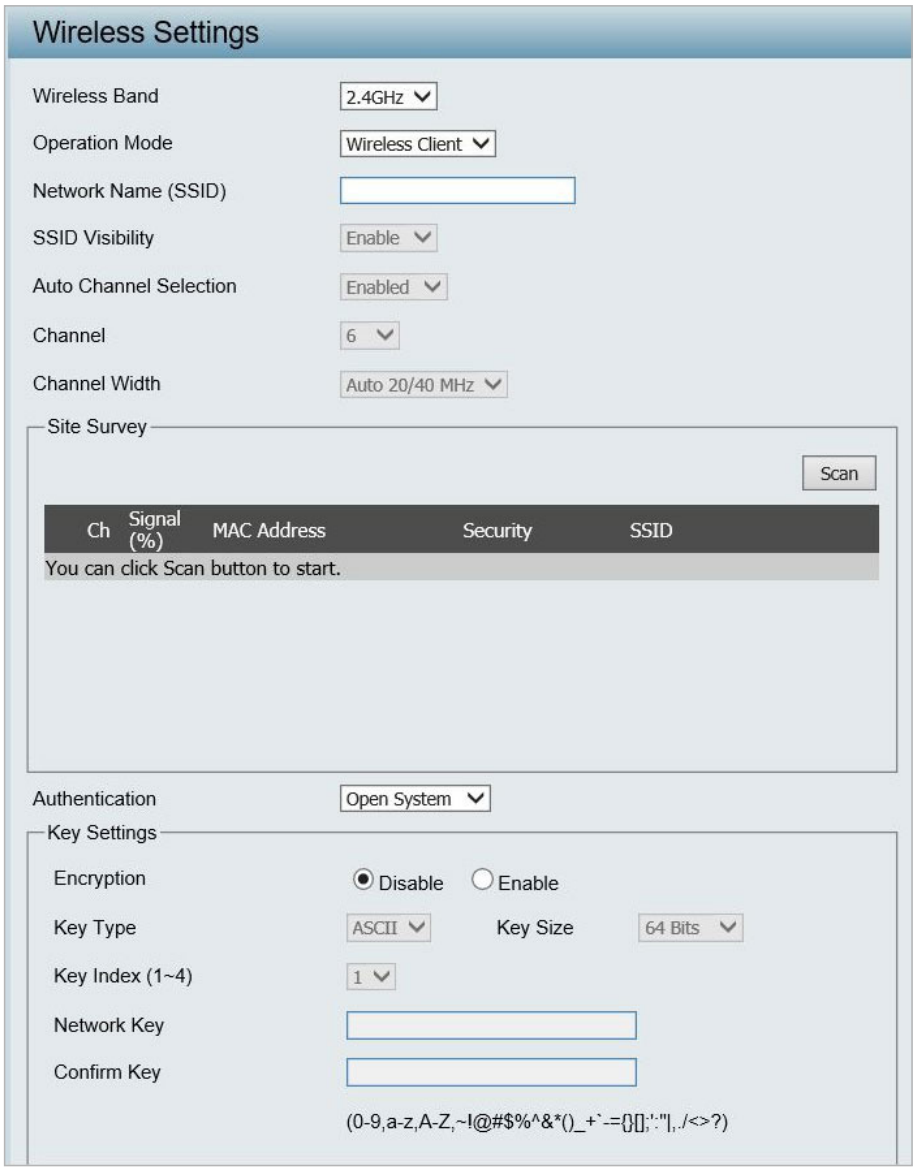
[Authentication](認証方式)の設定内容は、選択した方式によって異なります。
詳細は『Authentication（認証）の設定について：p.37 』を参照してください。

重要

- 異機種間、異なるファームウェアバージョン間でWDSモード、WDS with APモードを使用することはできません。
- DAP-3666のWDS構成では、子側にのみ、「AP MAC Address」に親側のMACアドレスを設定してください。
- WDS有効時、STPは無効となります。WDSの対向設定は1対向のみとしてください。
- WDS有効時、対象周波数帯の「Primary SSID（Primary）」、「SSID1（S-1）」を vlan1に所属させる必要があります。
- WDS間でVLANタグを通すには、「Primary SSID（Primary）」、「SSID1（S-1）」に対し対象のVLANを割り当てる必要があります。
- WDS with APモードを使用する場合、「Primary SSID（Primary）」、「SSID1（S-1）」はクライアント用には使えません。

■Wireless Clientモードを選択した場合

本製品は、イーサネット機器用の無線ネットワークアダプタとして動作します。



項目	説明
Wireless Band	周波数帯を [2.4GHz] または [5GHz] に設定します。
Operation Mode	通信モードを選択します。 ・選択肢：[Access Point] [WDS with AP] [WDS] [Wireless Client]
Network Name (SSID)	ネットワーク名（SSID）を入力します。 ・初期値：[dlink] ・入力可能文字数：32文字以内（大文字と小文字は区別されます。） SSID（Service Set Identifier）とは、無線LANのアクセスポイントを識別するための名前です。無線LANのアクセスポイントが複数ある場合、どのアクセスポイントに接続するかを指定する必要があり、SSIDはその際に使用されます。
SSID Visibility	通信モードに [Wireless Client] を選択した場合は設定できません。
Auto Channel Selection	通信モードに [Wireless Client] を選択した場合は設定できません。
Channel	通信モードに [Wireless Client] を選択した場合は設定できません。
Channel Width	通信モードに [Wireless Client] を選択した場合は設定できません。

項目	説明
Site Survey	[Scan] をクリックしてサイトサーベイを実行します。 サイトサーベイを実行し、検出された稼働中のアクセスポイントから、接続するネットワークをクリックします。
Authentication	認証方式を選択します。 ・選択肢：[Open System][WPA-Personal]
Wireless MAC Clone	Wireless MAC Cloneを有効にすると、本製品のMACアドレスをクライアントのMACアドレスに変更することができます。 1. [Enable]（有効）にチェックをいれると設定が有効になります。 2. [Enable]（有効）にチェックをいれた場合、[MAC Source] を [Auto]（自動）または [Manual]（手動）に設定します。 3. [MAC Source] を [Manual]（手動）にした場合は、[MAC Address] 欄にMACアドレスを入力するか、[Scan] をクリックして検索したMACアドレスを選択します。

メモ

[Authentication](認証方式)の設定内容は、選択した方式によって異なります。
詳細は『Authentication（認証）の設定について：p.37 』を参照してください。

■Authentication（認証）の設定について

[Wireless Setting] 画面では、認証方式として以下を選択できます。

◆ **Open System**
オープンシステム認証を行います。ネットワーク側での認証を行いません。
設定方法については、『[Open System] または [Shared Key] を選択した場合：p.37 』を参照してください。

◆ **Shared Key**
同じWEP設定を行ったデバイス同士の通信のみ可能になります。
設定方法については、『[Open System] または [Shared Key] を選択した場合：p.37 』を参照してください。

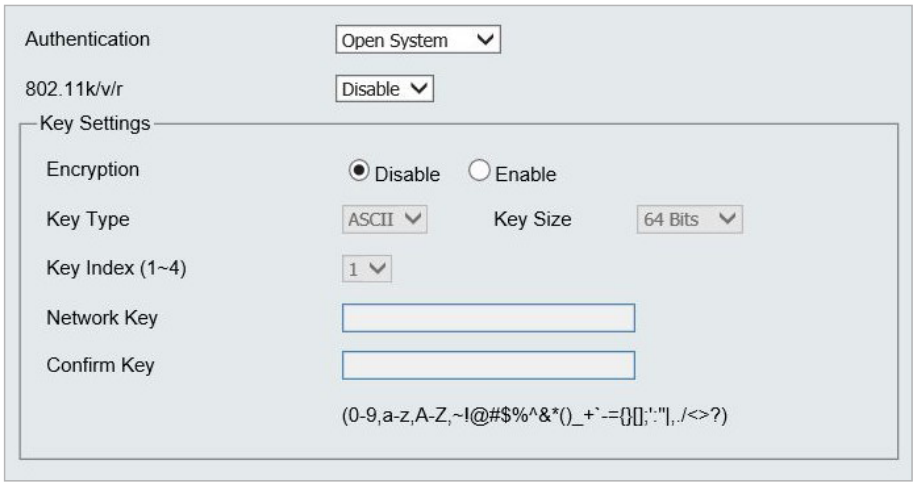
◆ **WPA-Personal**
パスワードと認証キーの自動変更機能によるセキュリティを提供します。RADIUS サーバは必要ありません。
設定方法については、『[WPA-Personal] を選択した場合：p.38 』を参照してください。

◆ **WPA-Enterprise**
ネットワーク内のRADIUS サーバを使用して認証を行います。
設定方法については、『[WPA-Enterprise] を選択した場合：p.39 』を参照してください。

◆ **802.1X**
802.1X ネットワーク認証を使用します。
設定方法については、『[802.1 X] を選択した場合：p.40 』を参照

◆ **Enhance Open**
Enhanced Openを使用します。

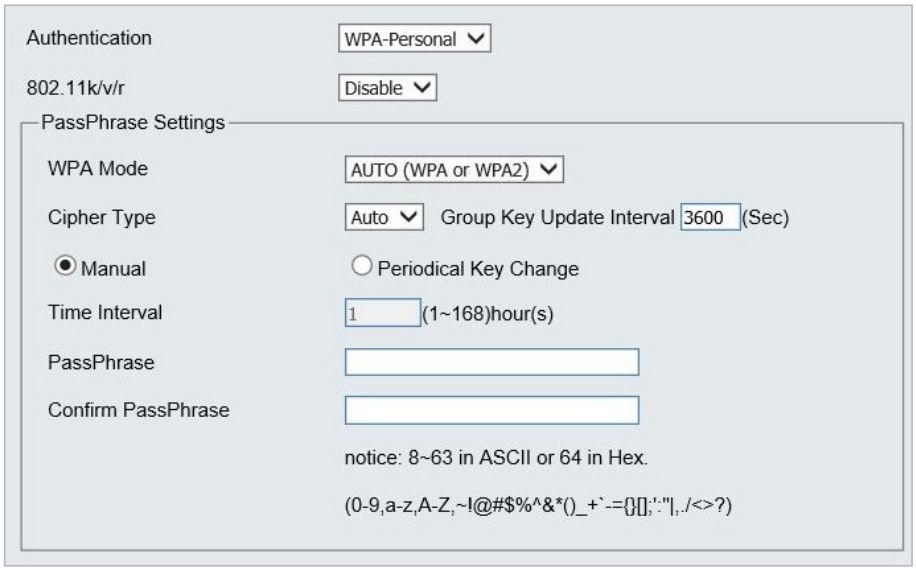
● [Open System] または [Shared Key] を選択した場合



項目	説明
Encryption	暗号化を有効または無効にします。 • 選択肢：[Enable]（有効）[Disabled]（無効）
Key Type	キーのタイプを選択します。 • 選択肢： - [HEX]（16 進数）：0 ～ 9、A ～ F までの半角英数字のキーを使用します。 - [ASCII]（半角英数字）：半角英数字のキーを使用します。
Key Size	キーのサイズを選択します。 • 選択肢：[64 Bits] [128 Bits]
Key Index	有効にするキーを選択します。 • 選択肢：[1] [2][3][4]
Network Key	キーを入力します。
Confirm Key	確認のため、再度キーを入力します。

● [WPA-Personal] を選択した場合

以下の画面でパスフレーズの設定を行います。



項目	説明
WPA Mode	WPAのモードを選択します。 ・選択肢：[AUTO（WPA or WPA2）][WPA2 Only][WPA2 or WPA3][WPA3 ONLY]
Cipher Type	暗号化タイプを選択します。 ・選択肢：[Auto][AES] [WPA2 or WPA3] または [WPA3 ONLY] を選択した場合、[AES] のみ指定可能です。
Group Key Update Interval	グループキーを更新する間隔を設定します。 ・推奨値：3600（秒）
Manual	パスフレーズを手動で設定するようにします。 [Manual] を選択した場合、使用するパスフレーズを入力します。
Periodical Key Change	アクセスポイントが自動的にパスフレーズを変更するようにします。 [Periodical Key Change] を選択した場合、変更を行う周期を設定します。
Time Interval	[Periodical Key Change] を選択した場合、パスフレーズを変更する間隔を設定します。
PassPhrase	[Manual] を選択した場合、パスフレーズを入力します。
Confirm PassPhrase	[Manual] を選択した場合、確認のため再度パスフレーズを入力します。

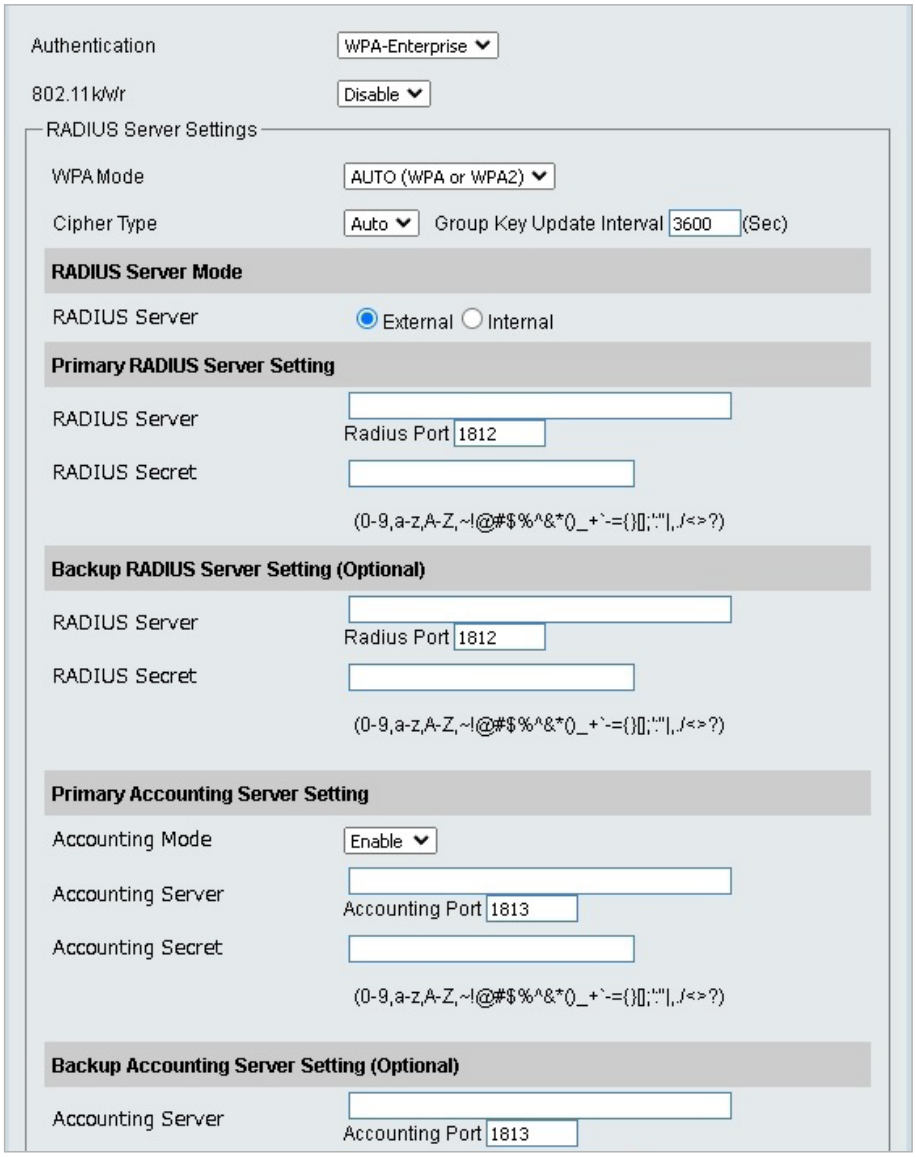
メモ

以下の項目は、アクセスポイントの通信モードをAccess Point モードに設定した場合のみ表示されます。
- [Manual] [Periodical Key Change][Time Interval]

重要

- WPA3は[WPA-Personal]でのみサポートされます。[WPA-Enterprise]ではサポートされません。
- [WPA Only]および[TKIP]はサポートされません。

● [WPA-Enterprise] を選択した場合



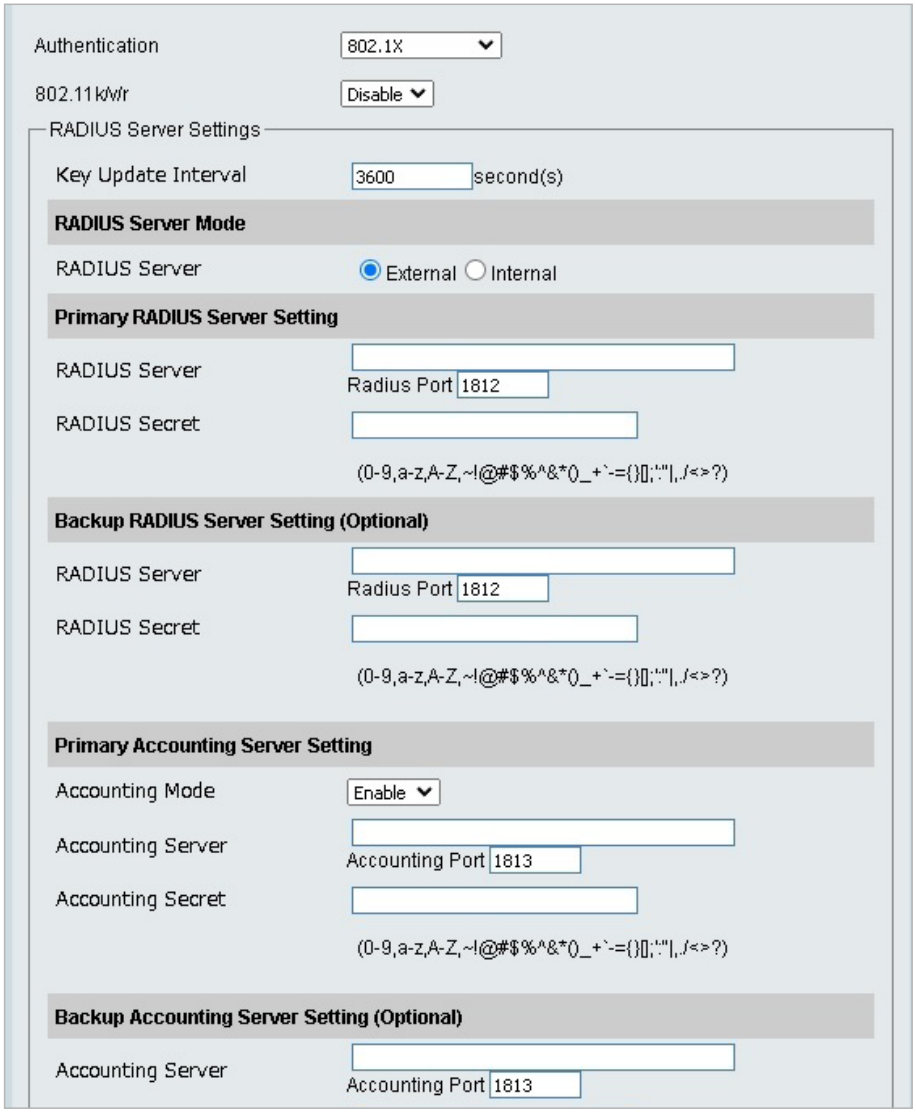
項目	説明
WPA Mode	WPAのモードを選択します。 • 選択肢：[AUTO（WPA or WPA2）][WPA2 Only][WPA2 or WPA3][WPA3 ONLY]
Cipher Type	暗号化タイプを選択します。 • 選択肢：[Auto][AES] [WPA2 or WPA3] または [WPA3 ONLY] を選択した場合、[AES] のみ指定可能です。
Group Key Update Interval	グループキーを更新する間隔を設定します。 • 推奨値：3600（秒）
RADIUS Server Mode	RADIUSサーバのモードを選択します。 • 選択肢：[External]（外部）[Internal]（内部）
Primary RADIUS Server Settings	プライマリRADIUSサーバの設定を行います。 • RADIUS Server: RADIUS サーバのIP アドレスを入力します。 • RADIUS Port: RADIUS サーバのポート番号を入力します。 初期値：[1812] • RADIUS Secret: RADIUS シークレット（パスワード）を入力します。
Backup RADIUS Server Settings (Optional)	バックアップRADIUSサーバの設定を行います。 • RADIUS Server: RADIUS サーバのIP アドレスを入力します。 • RADIUS Port: RADIUS サーバのポート番号を入力します。 初期値：[1812] • RADIUS Secret: RADIUS シークレット（パスワード）を入力します。

項目	説明
Primary Accounting Server Settings	プライマリアカウンティングサーバの設定を行います。 • Accounting Mode: アカウンティングモードを有効または無効にします。 • Accounting Server: アカウンティングサーバのIPアドレスを入力します。 • Accounting Port: アカウンティングサーバのポート番号を入力します。 初期値:[1813] • Accounting Secret: アカウンティングシークレット(パスワード)を入力します。
Backup Accounting Server Settings (Optional)	バックアップアカウンティングサーバの設定を行います。 • Accounting Server: アカウンティングサーバのIPアドレスを入力します。 • Accounting Port: アカウンティングサーバのポート番号を入力します。 初期値:[1813] • Accounting Secret: アカウンティングシークレット(パスワード)を入力します。

重要

- WPA3は[WPA-Personal]でのみサポートされます。[WPA-Enterprise]ではサポートされません。
- [WPA Only]および[TKIP]はサポートされません。

● [802.1 X] を選択した場合



項目	説明
Key Update Interval	キーを更新する間隔を設定します。 • 推奨値:300(秒)

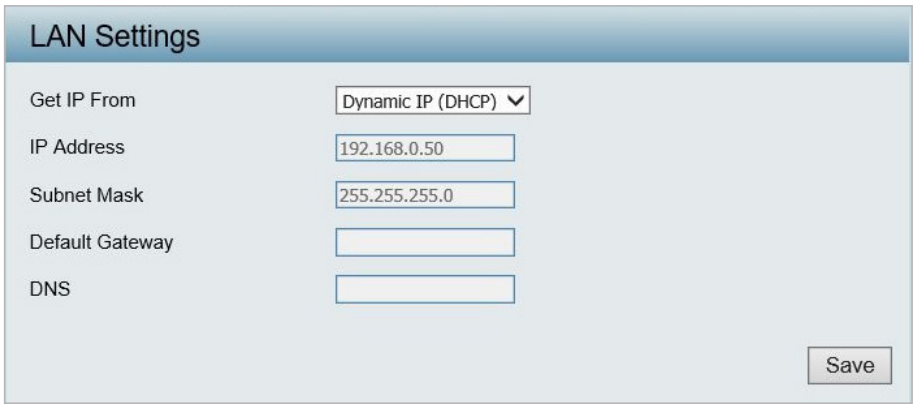
項目	説明
RADIUS Server Mode	RADIUSサーバのモードを選択します。 • 選択肢：[External]（外部）[Internal]（内部）
Primary RADIUS Server Settings	プライマリRADIUSサーバの設定を行います。 • RADIUS Server: RADIUS サーバのIP アドレスを入力します。 • RADIUS Port: RADIUS サーバのポート番号を入力します。 初期値：[1812] • RADIUS Secret: RADIUS シークレット（パスワード）を入力します。
Backup RADIUS Server Settings (Optional)	バックアップRADIUSサーバの設定を行います。 • RADIUS Server: RADIUS サーバのIP アドレスを入力します。 • RADIUS Port: RADIUS サーバのポート番号を入力します。 初期値：[1812] • RADIUS Secret: RADIUS シークレット（パスワード）を入力します。
Primary Accounting Server Settings	プライマリアカウンティングサーバの設定を行います。 • Accounting Mode: アカウンティングモードを有効または無効にします。 • Accounting Server: アカウンティングサーバのIPアドレスを入力します。 • Accounting Port: アカウンティングサーバのポート番号を入力します。 初期値：[1813] • Accounting Secret: アカウンティングシークレット（パスワード）を入力します。
Backup Accounting Server Settings (Optional)	バックアップアカウンティングサーバの設定を行います。 • Accounting Server: アカウンティングサーバのIPアドレスを入力します。 • Accounting Port: アカウンティングサーバのポート番号を入力します。 初期値：[1813] • Accounting Secret: アカウンティングシークレット（パスワード）を入力します。

LAN Settings（LAN設定）

本製品のLAN インタフェースのIP 設定を行います。LAN IP アドレスは必要に応じて変更することも可能です。
LAN IP アドレスはネットワーク内部で使用されます。インターネット上には公開されません。

1. [Basic Settings] > [LAN] を選択します。

2. 以下の画面で設定を行います。



項目	説明
Get IP From	IPアドレスの取得方法を選択します。 • [Static IP (Manual)]: 固定のIPアドレスを手動で設定します。 • [Dynamic (DHCP)]: DHCPサーバを使用してIPアドレスを設定します。 本製品のIPアドレスは、DHCPサーバから自動的に取得されます。[Dynamic (DHCP)]を選択した場合、その他の項目の設定は不要です。
IP Address	IPアドレスを入力します。 • 初期値: 192.168.0.50
Subnet Mask	サブネットマスクを入力します。 • 初期値: 255.255.255.0
Default Gateway	デフォルトゲートウェイのIP アドレスを入力します。
DNS	DNSのIPアドレスを入力します。

3. [Save] をクリックして設定を保存します。

IPv6 Settings（IPv6設定）

LAN インタフェースのIPv6 設定を行います。
本機能を有効にすると、IPv6 アドレスを使用してDAP-3666にアクセスすることが可能となります。

1. [Basic Settings] > [IPv6] を選択します。

2. 以下の画面で設定を行います。

項目	説明
Enable IPv6	チェックをいれると、IPv6アドレスが有効になります。
Get IP From	IPv6アドレスの取得方法を選択します。 • [Static]: 固定のIPv6アドレスを手動で設定します。 • [Auto]: 本製品のIPv6アドレスは、自動的に取得されます。[Auto] を選択した場合、その他の項目の設定は不要です。
IP Address	IPv6アドレスを入力します。
Prefix	プレフィックス長の値を入力します。
Default Gateway	デフォルトゲートウェイのIP アドレスを入力します。

3. [Save] をクリックして設定を保存します。

メモ

Telnet/SSH、DNS Proxyについて、IPv6接続はサポートされません。

Advanced Settings（詳細設定）

5

マルチSSIDやVLAN、キャプティブポータルなど、アクセスポイントの詳細設定を行います。

■ Advanced Settings について 45

■ Performance Settings（パフォーマンス設定） 45

■ Wireless Resource Control（ワイヤレスリソースコントロール） 48

■ Multi-SSID Settings（マルチSSID設定） 49

■ VLAN Settings（VLAN設定） 51

■ Wireless Intrusion Protection（不正AP検知） 55

■ Wireless Schedule Settings（スケジュール設定） 56

■ Internal RADIUS Server（RADIUSサーバ） 58

■ ARP Spoofing Prevention Settings
（ARPスプーフィング防止設定） 59

■ Bandwidth Optimization（帯域幅最適化） 60

■ Hotspot2.0（ホットスポット2.0） 62

■ Captive Portal（キャプティブポータル） 67
- Login Page Upload（ログイン画面アップロード） 76
- MAC Bypass（MAC Bypass 設定） 77

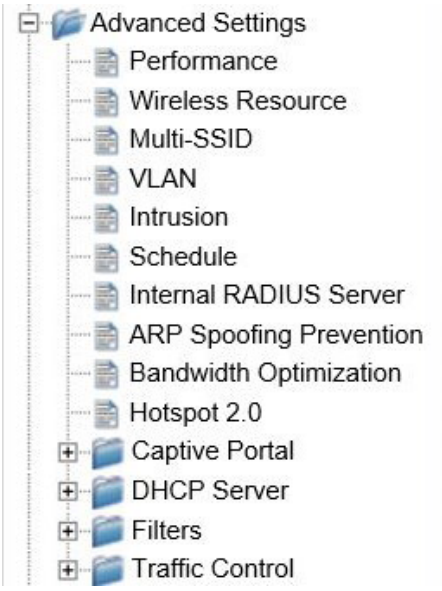
■ DHCP Server（DHCPサーバ設定） 78
- Dynamic Pool Settings（ダイナミックプール設定） 78
- Static Pool Settings（スタティックプール設定） 79
- Current IP Mapping List（IPマッピングリスト） 80

■ Filters（フィルタ） 81
- Wireless MAC ACL Settings（ワイヤレスMAC ACL） 81
- WLAN Partition（WLANパーティション） 83
- IP Filter Settings（IPフィルタ） 84

■ Traffic Control（トラフィックコントロール） 85
- Uplink and Downlink Setting（アップリンク／ダウンリンク設定） 85
- QoS（QoS設定） 86
- Traffic Manager（トラフィックマネージャ） 87

Advanced Settings について

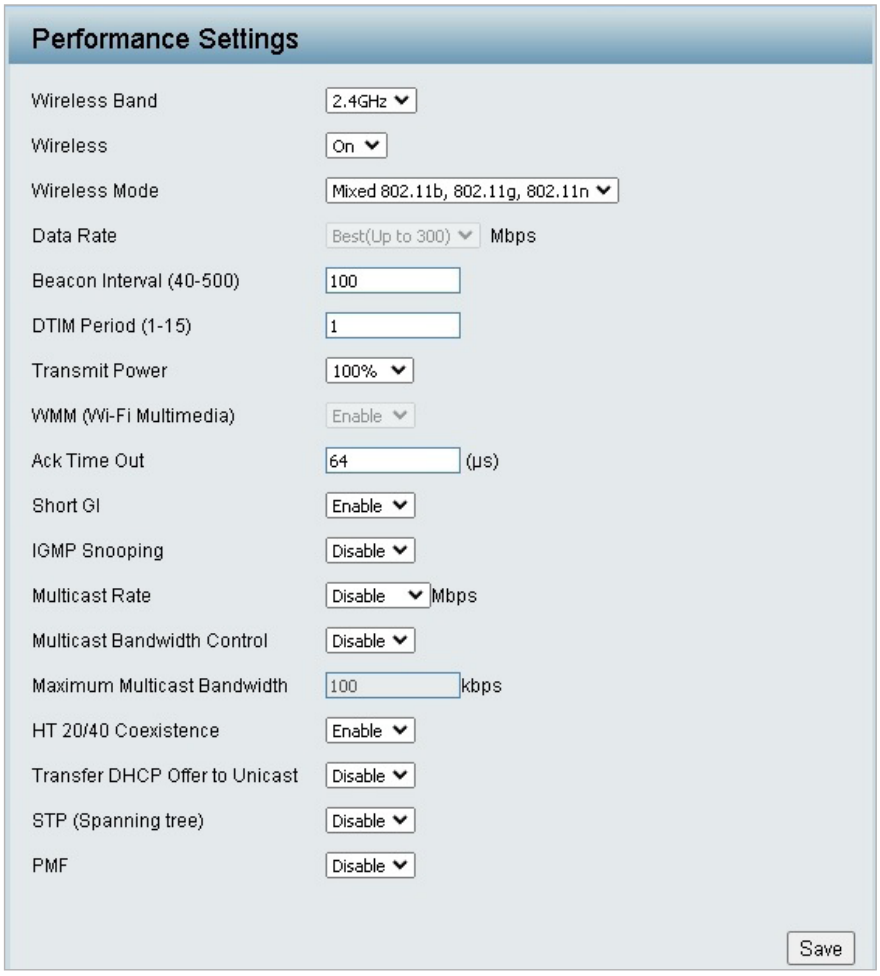
マルチSSIDやVLAN、キャプティブポータルなど、アクセスポイントの詳細設定を行います。



Performance Settings（パフォーマンス設定）

無線のパフォーマンス設定を行います。

1. [Advanced Settings] > [Performance] を選択します。
2. 以下の画面で設定を行います。



項目	説明
Wireless Band	周波数帯を [2.4GHz] または [5GHz] から選択します。
Wireless	無線機能を [On] または [Off] に選択します。 • 選択肢：[On]または[Off]
Wireless Mode	ワイヤレスモードを選択します。選択肢は設定した周波数帯によって異なります。 • 選択肢([2.4GHz] を選択した場合)： [Mixed 802.11b, 802.11g, 802.11n][Mixed 802.11b, 802.11g][802.11n only] • 選択肢([5GHz] を選択した場合)： [Mixed 802.11n, 802.11a][802.11a Only][802.11n Only] [Mixed 802.11ac] レガシークライアント（802.11a/g/b）向けに互換性がある場合は、802.11n規格の無線性能は低下します。
Data Rate	ワイヤレスアダプタのベース転送速度を設定します。（単位：Mbps） • 選択肢([2.4GHz] を選択した場合)：Best (Up to 54), 54, 48, 36, 24, 18, 12, 9, 6, 11, 5.5, 2,1 • 選択肢([5GHz] を選択した場合)：54, 48, 36, 24, 18, 12, 9, 6 本製品のベース転送速度は接続しているデバイスのベース転送速度に左右されます。 障害物や干渉がある場合、転送速度は低下します。 本項目は、[Wireless Mode] で [802.11a Only][Mixed 802.11b, 802.11g]レガシークライアント）を選択した場合のみ設定できます。それ以外の場合は [Best (Up to 300)] または [Best (Up to 867)] となります。
Beacon Interval (40-500)	ビーコンを送信する間隔を設定します。(単位：ミリ秒) • 初期値：100（※本値を推奨します） • 設定可能範囲：40-500 ビーコンとはアクセスポイントがネットワークと同期するために送信するパケットです。ビーコン送信間隔を長く設定すると、無線クライアントの電力の節約になり、短く設定すると、無線クライアントがアクセスポイントに速く接続できるようになります。
DTIM Period (1-15)	DTIM（Delivery Traffic Indication Message）の間隔を設定します。 • 初期値：1 • 設定可能範囲：1-15 DTIM とは、省電力モードの無線クライアントに対して、パケットが送信待ちであることを伝えるメッセージです。
Transmit Power	無線の送信電力を設定します。 • 選択肢：100%、50%、25%、12.5% 送信電力を調整することで、2 つのアクセスポイント間の干渉による無線適用範囲の重複を削減することができます。 例：無線適用範囲がエリアの半分をカバーしている場合は、50%を選択します。
WMM (Wi-Fi Multimedia)	WMM（Wi-Fi Multimedia）を有効または無効にします。 • 選択肢：[Enable]（有効）[Disable]（無効） 本機能を「Enable」（有効）にするとWi-Fiネットワークを使用して快適にオーディオやビデオアプリケーションを利用できるようになります。 [Wireless Mode] が [Mixed 802.11b, 802.11g]または [802.11a Only] の場合に使用できます。
Ack Time Out	「Acknowledgement Time Out」の値を入力します。 設定可能範囲は設定した周波数帯によって異なります。 • 設定可能範囲([2.4GHz] を選択した場合)：48-200 μs • 設定可能範囲([5GHz] を選択した場合）：25-200 μs 本項目を設定することで、効率的に長距離のスループットを最適化します。
Short GI	Short GI（ショートガードインターバル）を有効または無効にします。 • 選択肢：[Enable]（有効）[Disable]（無効） ショートガードインターバルを有効にすると、スループットが増加します。同時に無線周波数の感度が上がるため、設置環境によってはエラー率が増加する場合もありますので、ご注意ください。 [Wireless Mode] が [Mixed 802.11b, 802.11g][Mixed 802.11n, 802.11a][802.11a Only] の場合には使用できません。

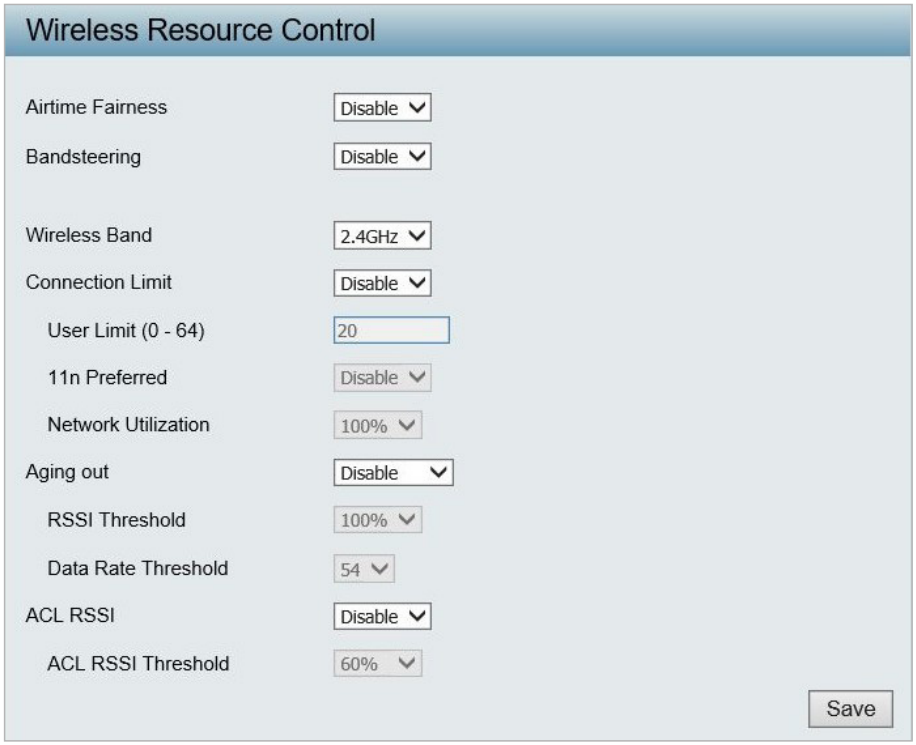
項目	説明
IGMP Snooping	IGMP（Internet Group Management Protocol）スヌーピングを有効または無効にします。 • 選択肢：[Enable]（有効）[Disable]（無効） IGMPスヌーピング機能を利用すると、アクセスポイントはルータとIGMPホスト間で送信されるIGMP クエリとIGMP レポートを認識するようになります。本機能が有効な場合、アクセスポイントを通過したIGMP メッセージに基づき、ホストにマルチキャストパケットを送信します。 APモードまたはWDS with APモードの場合に使用できます。
Multicast Rate	マルチキャストレートの数値を設定、または無効（[Disable])にします。（単位：Mbps） APモードまたはWDS with APモードの場合に使用できます。 本項目は、[Wireless Mode] で[Mixed 802.11b, 802.11g, 802.11n][Mixed 802.11b, 802.11g][Mixed 802.11n, 802.11a][802.11a Only] を選択した場合に設定できます。
Multicast Bandwidth Control	マルチキャスト帯域幅管理を有効または無効にします。 • 選択肢：[Enable]（有効）[Disable]（無効）
Maximum Multicast Bandwidth	イーサネットインタフェースとアクセスポイント間における、最大マルチキャスト帯域幅を設定します。 • 初期値：100Kbps [Multicast Bandwidth Control] を有効にした場合のみ設定できます。
HT 20/40 Coexistence	20/40MHz 通信の同時利用を有効または無効にします。 • 選択肢：[Enable]（有効）[Disable]（無効） 本項目を有効化すると、エリア内の無線ネットワークからの干渉を抑制します。チャンネル帯域を40MHzで使用中に他の無線ネットワークチャンネルからの干渉を受ける場合、本製品は自動的に20MHzへ変更し干渉を避けます。 本項目は、[Basic Settings] > [Wireless] で [Channel Width] が [Auto 20/40MHz]、本画面の [Wireless Band] が [2.4GHz] の場合に使用できます。
Transfer DHCP Offer to Unicast	LANからWANに対するユニキャストへのDHCPオファー送信を有効または無効にします。ステーション数が30台を超える場合は本機能を有効にすることを推奨します。 • 選択肢：[Enable]（有効）[Disable]（無効）
STP (Spanning tree)	STP機能を有効または無効にします。 • 選択肢：[Enable]（有効）[Disable]（無効）
PMF	PMF（Protected Management Frames）機能を有効または無効にします。 • 選択肢：[Enable]（有効）[Disable]（無効）

3. [Save] をクリックして設定を保存します。

Wireless Resource Control（ワイヤレスリソースコントロール）

ワイヤレス接続設定を行い、デバイスがより適したワイヤレス接続を検知できるようにします。

1. [Advanced Settings] > [Wireless Resource] を選択します。
2. 以下の画面で設定を行います。



項目	説明
Airtime Fairness	エアタイムフェアネス機能を有効または無効にします。 • 選択肢：[Enable]（有効）[Disable]（無効）
Band Steering	バンドステアリング機能を有効または無効にします。 バンドステアリングは、ワイヤレスクライアントが2.4GHzと5GHzの両方をサポートしている場合、2.4GHzのシグナルの強さが十分でないときに、クライアントを5GHzに誘導する機能です。
Wireless Band	周波数帯を [2.4GHz] または [5GHz] から選択します。
Connection Limit	接続するユーザ数の制限を有効または無効にします。 • 選択肢：[Enable]（有効）[Disable]（無効） Connection Limitが有効に設定され、接続ユーザ数がUser LimitまたはNetwork Utilizationの設定値を超えた場合、クライアントの接続を受け付けなくなります。 • User Limit (0-64) : 接続可能なユーザ数を0-64から指定します。 初期値：20 • 11n Preferred : [Enable]（有効）または [Disable]（無効）を選択します。 有効にすると、11nクライアントの接続が優先されます。 • Network Utilization : 最大ネットワーク使用率を100%、80%、60%、40%、20%、0%から選択します。 設定値に達した場合、ネットワークの過密状態を解消するために1分間休止状態となります。
Aging out	ワイヤレスクライアントを切断する基準を設定します。 • 選択肢：[RSSI][Data Rate][Disable]（無効） • RSSI Threshold: RSSIのしきい値を10%～100%間で指定します。無線クライアントのRSSIが設定値を下回ると、無線接続が切断されます。 • Data Rate Threshold: データレートのしきい値を6、9、12、18、24、36、48、54から指定します。無線クライアントのデータレートが設定値を下回ると、無線接続が切断されます。

項目	説明
ACL RSSI	ACL RSSIを有効または無効にします。 • 選択肢：[Enable]（有効）[Disable]（無効） 本項目を有効化すると、下記項目で指定されたRSSIのしきい値を下回っている無線クライアントからの接続リクエストを拒否します。 • ACL RSSI Threshold : ACL RSSIのしきい値を10%～100%間で指定します。

3. [Save] をクリックして設定を保存します。

Multi-SSID Settings（マルチSSID設定）

マルチSSIDの設定を行います。

1. [Advanced Settings] > [Multi SSID] を選択します。
2. 以下の画面で設定を行います。

項目	説明
Enable Multi-SSID	チェックを入れるとマルチSSIDが有効になります。
Enable Priority	チェックを入れるとSSID の優先機能が有効になります。 有効にすると、[Priority] で0 から7 までの優先値をSSID に設定できます。

項目	説明
Wireless Settings	マルチSSIDのワイヤレス設定を行います。 • Band : 周波数帯を [2.4GHz] または [5GHz] に設定します。 • Index : マルチSSIDを以下から選択します。 [Primary SSID][SSID1][SSID2][SSID3][SSID4][SSID5][SSID6][SSID7] • SSID : SSID名を入力します。 • SSID Visibility : [Enable]（有効）または[Disable]（無効）に設定します。 有効にするとSSID がネットワーク上にブロードキャストされ、すべてのネットワークユーザから閲覧できるようになります。 • Security セキュリティを [Open System][Shared Key][WPA-Personal][WPA-Enterprise][802.1X][Enhance Open] から選択します。 選択した設定によって、画面下部に詳細設定を行う項目が表示されます。 セキュリティの詳細設定については『Authentication（認証）の設定について：p.37 』を参照してください。 • Priority SSIDの優先値を「0」～「7」の間で設定します。 • WMM (Wi-Fi Multimedia) [Enable]（有効）または[Disable]（無効）に設定します。 本機能を[Enable]（有効） にするとWi-Fiネットワークを使用して快適にオーディオやビデオアプリケーションを利用できるようになります。 [Advanced Settings] > [Performance] で [Wireless Mode] が [Mixed 802.11b, 802.11g] または [802.11a Only] の場合に使用できます。 • 802.11k/v/r 802.11k/v/r（高速ローミング）機能を [Enable]（有効）[Disable]（無効）にします。

3. [Add] で SSID を追加した後、[Save] をクリックして設定を保存します。

◆ 追加した SSID を削除する場合：

1. [Delete] 欄の [Delete] をクリックします。

◆ 追加した SSID を編集する場合：

1. [Index] 欄のインデックス名をクリックします。
2. [Add] をクリックして設定を保存します。

VLAN Settings（VLAN設定）

本製品はVLAN をサポートしています。
VIDとVLAN名とを指定してVLANを作成します。Mgmt（TCPスタック）、LAN、プライマリ/ マルチSSID、WDS接続は、物理ポートであるVLANに割り当てることができます。
VLAN タグなしで本製品に送信されたパケットには、PVIDを持つVLAN タグが付けられます。

1. [Advanced Settings] > [VLAN] を選択します。

2. [VLAN Status] で、VLAN を [Enable]（有効）または [Disable]（無効）に設定します。

メモ

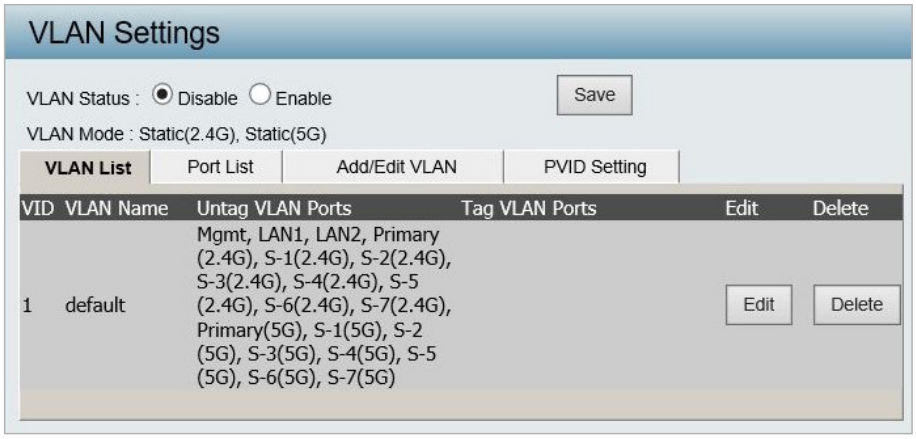
[VLAN Status] には、現在のVLANモードが表示されます。

3. 以下のタブを使用して必要な設定を行います。

- 『VLAN List タブ：p.51 』
- 『Port List タブ：p.52 』
- 『Add/Edit VLAN タブ：p.53 』
- 『PVID Settingタブ：p.54 』

● VLAN List タブ

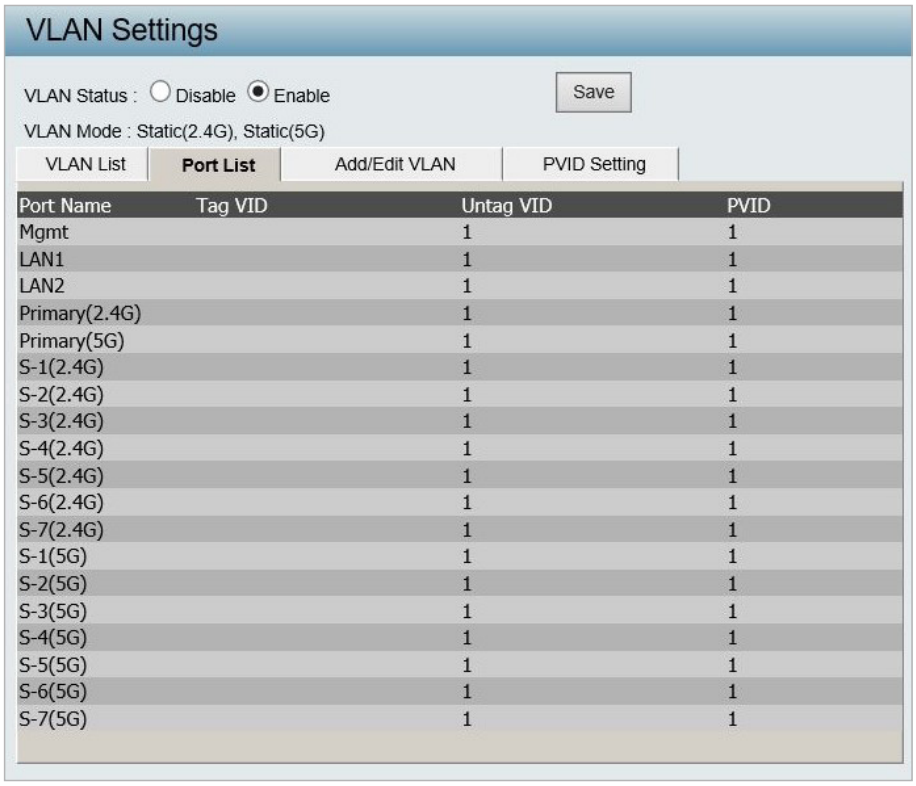
現在設定されているVLANのリストが表示されます。



項目	説明
VID	VLAN のIDが表示されます。
VLAN Name	VLAN名が表示されます。
Untag VLAN Ports	タグ無しVLANポートが表示されます。
Tag VLAN Ports	タグ付きVLANポートが表示されます。
Edit	[Edit] をクリックすると [Add/Edit VLAN] タブの内容が表示され、VLANの編集を行うことができます。
Delete	[Delete] をクリックするとVLANを削除できます。

● Port List タブ

現在のポートのリストが表示されます。
VLAN にゲストネットワークと内部ネットワークを設定するためには、使用しているスイッチとDHCP サーバがVLAN をサポートしている必要があります。事前にスイッチのポートがIEEE 802.1Q 定義のVLAN タグ付きパケットをサポートするように設定を行ってください。

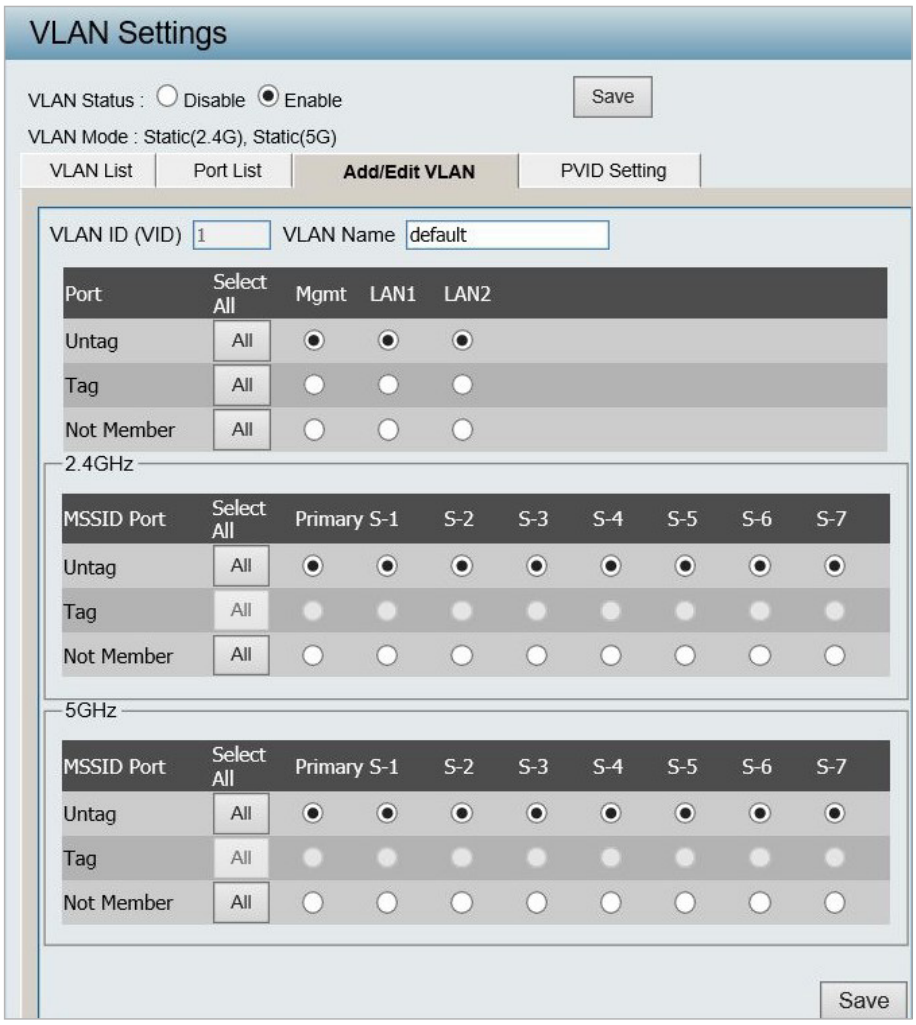


Port Name	Tag VID	Untag VID	PVID
Mgmt		1	1
LAN1		1	1
LAN2		1	1
Primary(2.4G)		1	1
Primary(5G)		1	1
S-1(2.4G)		1	1
S-2(2.4G)		1	1
S-3(2.4G)		1	1
S-4(2.4G)		1	1
S-5(2.4G)		1	1
S-6(2.4G)		1	1
S-7(2.4G)		1	1
S-1(5G)		1	1
S-2(5G)		1	1
S-3(5G)		1	1
S-4(5G)		1	1
S-5(5G)		1	1
S-6(5G)		1	1
S-7(5G)		1	1

項目	説明
Port Name	ポート名が表示されます。
Tag VID	タグ付きVLAN IDが表示されます。
Untag VID	タグ無しVLAN IDが表示されます。
PVID	ポートVLAN IDが表示されます。

● Add/Edit VLAN タブ

新しいVLANの追加または既存のVLANの編集を行います。



項目	説明
VLAN ID (VID)	内部VLAN 用の番号を入力します。 • 設定可能範囲: 1-4094
VLAN Name	追加または変更するVLAN 名を入力します。
Port **MSSID Port** **WDS Port**	• Untag - ポートをタグなしとして定義します。 • Tag - ポートをタグ付きとして定義します。 • Not Member - ポートをVLAN メンバとしないように定義します。 All を選択するとすべてのポートが選択されます。

◆ 新しい VLAN を追加する場合：

1. [VLAN Status] を [Enable] にします。
2. [VLAN ID（VID）] に識別番号、[VLAN Name] に識別名を入力します。
3. VLAN ポートを編集します。
4. [Save] をクリックして設定を保存します。

◆ 既存の VLAN を編集する場合：

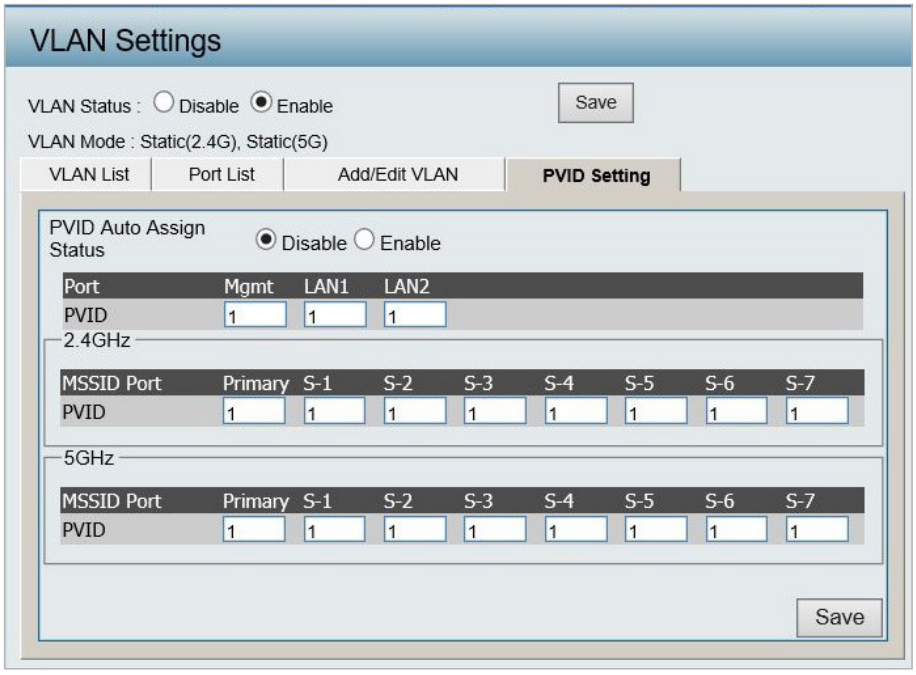
1. [VLAN List] タブで編集する VLAN の [Edit] をクリックします。
2. [Add/Edit VLAN] タブが表示されるので、VLAN の編集を行います。
3. [Save] をクリックして設定を保存します。

重要

WDS有効時、対象周波数帯の「Primary SSID (Primary)」、「SSID1 (S-1)」を vlan1に所属させる必要があります。

● PVID Settingタブ

PVID 自動割り当て設定および各PVID 設定を行います。



項目	説明
PVID Auto Assign Status	PVID自動割り当て設定を有効または無効にします。 ・選択肢：[Enable] (有効) [Disable] (無効)
Port **MSSID Port** **WDS Port**	PVID自動割り当て設定を無効にした場合に、PVIDの設定を行います。

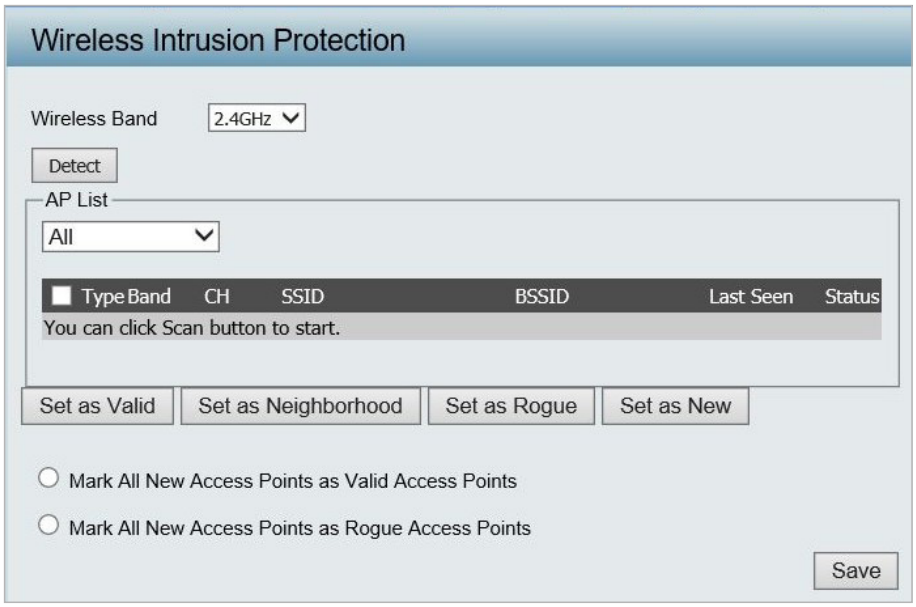
4. [Save] をクリックして設定を保存します。

Wireless Intrusion Protection（不正AP検知）

アクセスポイントの検知を行い、検知したアクセスポイントを分類することができます。

1. [Advanced Settings] > [Intrusion] を選択します。

2. 以下の画面でアクセスポイントの検知と分類を行います。



項目	説明
Wireless Band	周波数帯を [2.4GHz] または [5GHz] から選択します。
Detect	アクセスポイントの検知を実行します。
AP List	検知したアクセスポイントのリストを表示します。 表示するアクセスポイントは以下から選択できます。 • [All]：すべてのアクセスポイント • [Valid]：正しいアクセスポイント • [Neighborhood]：隣接したアクセスポイント • [Rogue]：不正なアクセスポイント（未認証） • [New]：新しいアクセスポイント
Set as Valid	チェックを入れたアクセスポイントを、正しいアクセスポイントとして分類します。
Set as Neighborhood	チェックを入れたアクセスポイントを、隣接したアクセスポイントとして分類します。
Set as Rogue	チェックを入れたアクセスポイントを、不正なアクセスポイントとして分類します。
Set as New	チェックを入れたアクセスポイントを、新しいアクセスポイントとして分類します。

メモ

- [Mark All New Access Points as Valid Access Points] を選択すると、新たに検知されたすべてのアクセスポイントが正しいアクセスポイントとして分類されます。
- [Mark All New Access Points as Rogue Access Points] を選択すると、新たに検知されたすべてのアクセスポイントが不正なアクセスポイントとして分類されます。

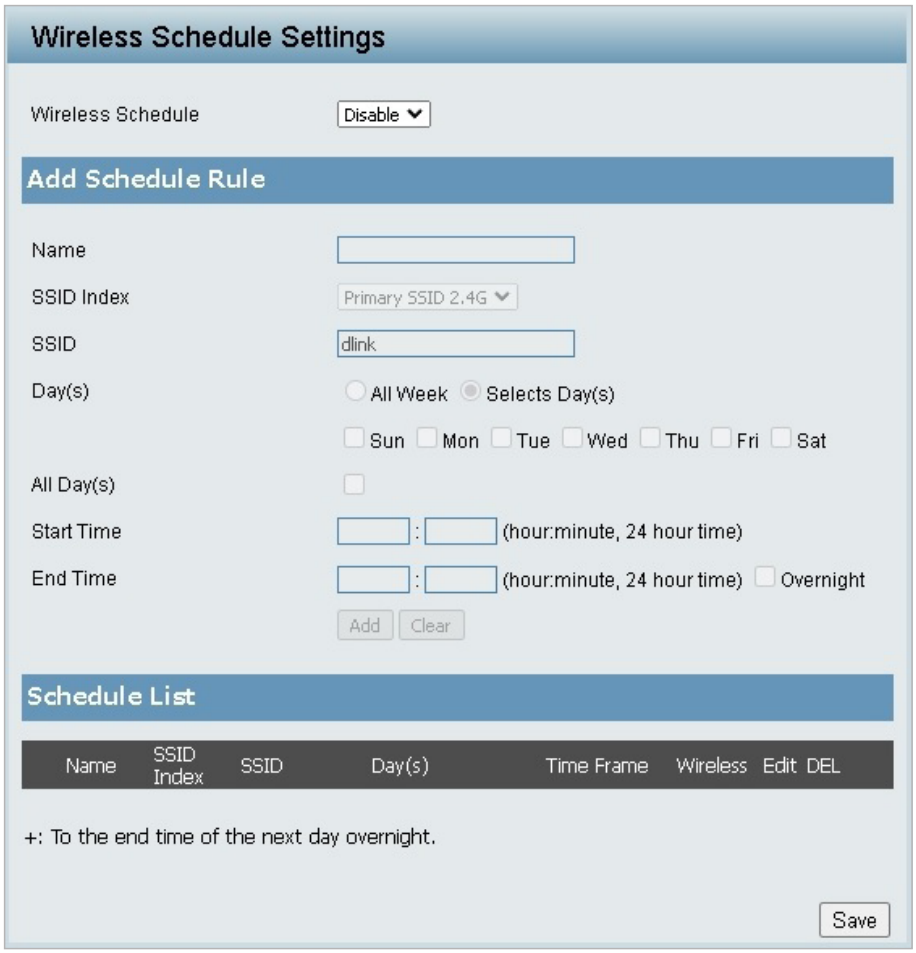
3. [Save] をクリックして設定を保存します。

Wireless Schedule Settings（スケジュール設定）

無線機能のスケジュールルールを追加または編集することができます。

1. [Advanced Settings] > [Schedule] を選択します。

2. 以下の画面で設定を行います。



項目	説明
Wireless Schedule	無線スケジュール設定を有効または無効にします。 • 選択肢：[Enable]（有効）[Disable]（無効）
Add Schedule Rule	スケジュールルールの追加・編集を行います。 • Name：ルール名を入力します。 • SSID Index：ドロップダウンリストから対象のSSIDを選択します。 • SSID：ネットワーク名（SSID）が表示されます。 • Day(s)：[All Week]（毎日）または [Select Day (s)]（曜日指定）を選択します。 [Select Day (s)] を選択した場合、ルールを適用する曜日を指定します。 • All Day(s)：チェックすると終日が選択されます。 • Start Time/End Time：開始時刻と終了時刻を指定します。 [Overnight]にチェックをいれると、開始時刻から日付を跨いで終了時刻を設定できます。 （例：21:00-07:00）時刻は24時間表記で指定してください。 • Add：設定した内容を追加します。 • Clear：設定した内容を取り消します。
Schedule List	設定したスケジュールルールが表示されます。

3. [Save] をクリックして設定を保存します。

- スケジュールルールを削除する場合：

  1. [Schedule List] 欄の [Delete] をクリックします。
  2. 確認メッセージが表示されるので、[OK] をクリックします。

- スケジュールルールを編集する場合：

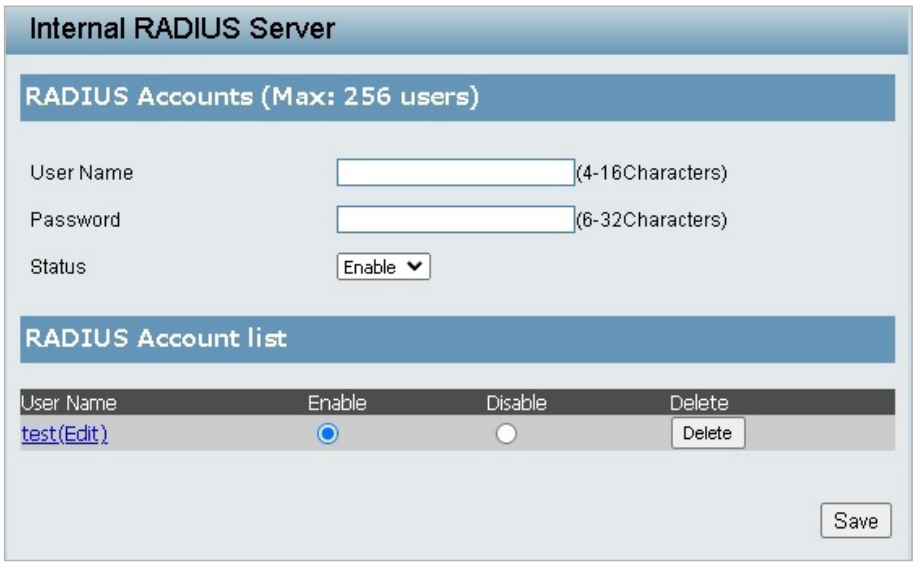
  1. [Schedule List] の [Edit] をクリックします。
  2. [Add Schedule Rule] でルールを編集します。
  3. [Add] をクリックして設定を保存します。

Internal RADIUS Server（RADIUSサーバ）

本製品はRADIUSサーバを内蔵しています。
本項目では、RADIUSアカウントの作成／削除方法およびアカウントを有効／無効にする方法について説明します。
作成するアカウント数は30個以内にすることをおすすめします。

1. [Advanced Settings] > [Internal RADIUS Server] を選択します。

2. 以下の画面で設定を行います。



項目	説明
RADIUS Accounts	RADIUSアカウントの追加を行います。 • User Name： アカウントのユーザ名を入力します。 入力可能文字数：4～16文字以内 • Password： アカウントのパスワードを入力します。 入力可能文字数：6～32文字以内 • Status： アカウントのステータスを [Enable]（有効）または [Disable]（無効）にします。
RADIUS Account list	作成したアカウントのリストが表示されます。

3. [Save] をクリックして設定を保存します。

◆ アカウントを削除する場合：

1. [RADIUS Account List] 欄の [Delete] をクリックします。
2. 確認メッセージが表示されるので、「OK」をクリックします。

◆ アカウントを編集する場合：

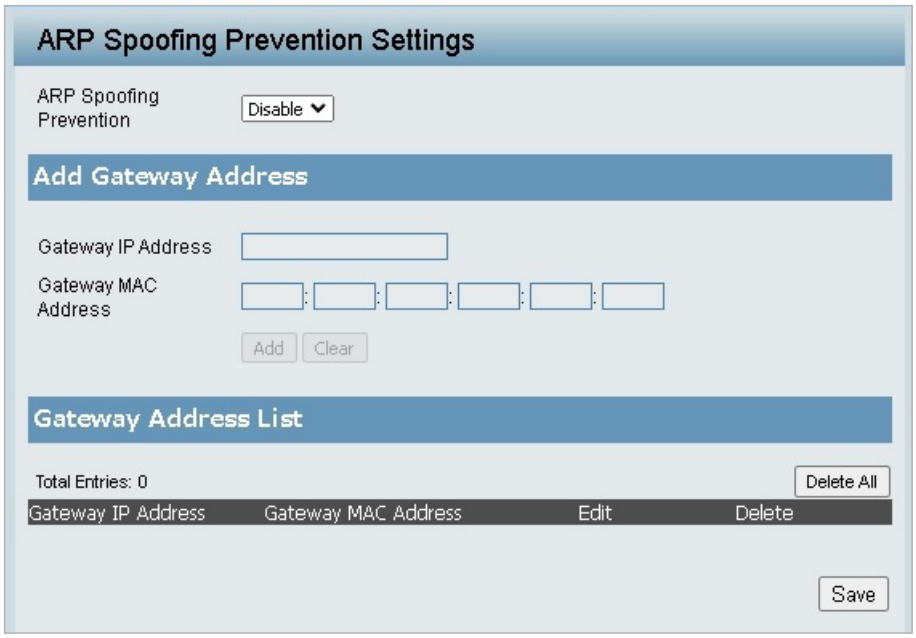
1. [RADIUS Account List] 欄のユーザ名 をクリックします。
2. [RADIUS Accounts] でアカウント設定を編集します。
3. [Save] をクリックして設定を保存します。

ARP Spoofing Prevention Settings（ARPスプーフィング防止設定）

ARP スプーフィング防止機能は、IP/MAC アドレスをマッピングすることにより、ARP スプーフィング攻撃を防止する機能です。

1. [Advanced Settings] > [ARP Spoofing Prevention] を選択します。

2. 以下の画面で設定を行います。



項目	説明
ARP Spoofing Prevention	ARPスプーフィング防止を有効または無効にします。 • 選択肢：[Enable]（有効）[Disable]（無効）
Add Gateway Address	ゲートウェイアドレスの追加・編集を行います。 • Gateway IP Address： ゲートウェイIPアドレスを入力します。 • Gateway MAC Address： ゲートウェイMACアドレスを入力します。 • Add：設定した内容を追加します。 • Clear：設定した内容を取り消します。
Gateway Address List	ゲートウェイアドレスのリストが表示されます。

3. [Save] をクリックして設定を保存します。

◆ ゲートウェイアドレスを削除する場合：

1. [Gateway Address List] 欄の [Delete] をクリックします。
2. 確認メッセージが表示されるので、「OK」をクリックします。

◆ ゲートウェイアドレスを編集する場合：

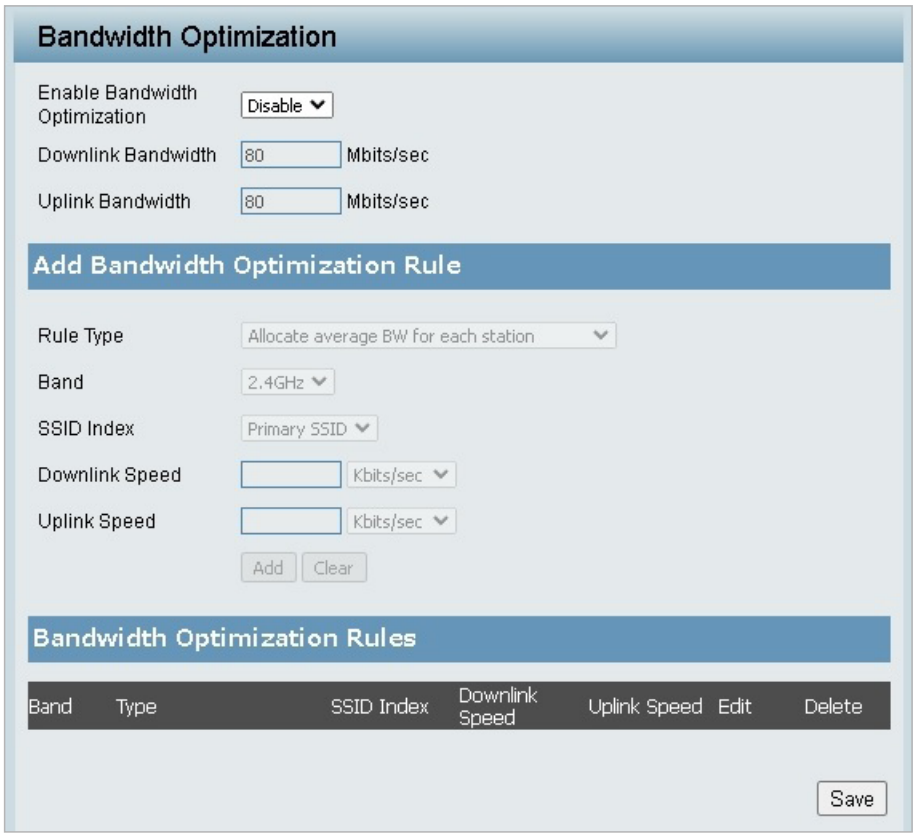
1. [Gateway Address List] の [Edit] をクリックします。
2. [Add Gateway Address] でルールを編集します。
3. [Add] をクリックして設定を保存します。

Bandwidth Optimization（帯域幅最適化）

帯域幅最適化機能を使用すると、本製品およびワイヤレスクライアントの帯域幅を管理することができます。
本項目では、帯域幅最適化機能の設定方法について説明します。

1. [Advanced Settings] > [Bandwidth Optimization] を選択します。

2. 以下の画面で設定を行います。



項目	説明
Enable Bandwidth Optimization	帯域幅最適化を有効または無効にします。 • 選択肢：[Enable]（有効）[Disable]（無効）
Downlink Bandwidth	本製品のダウンリンクの帯域幅を入力します。 • 単位：Mbits（秒）
Uplink Bandwidth	本製品のアップリンクの帯域幅を入力します。 • 単位：Mbits（秒）
Add Bandwidth Optimization Rule	帯域幅最適化ルールの追加・編集を行います。 • Rule Type：以下からルールタイプを指定します。 - Allocate average BW for each station Downlink/Uplink Speedの設定値を、各クライアントで平等にシェアします。 - Allocate maximum BW for each station Downlink/Uplink Speedの設定値が、各クライアントの最大値となります。 - Allocate different BW for a/b/g/n stations a/b/g/nのクライアントに異なる帯域幅を割り当てます。 ・11b/g/nクライアント：10% / 20% / 70% ・11a/nクライアント：20% / 80% - Allocate specific BW for SSID すべてのクライアントで全体の帯域幅をシェアします。 • Band： 周波数帯を [2.4GHz] または [5GHz] から選択します。 • SSID Index： ドロップダウンリストから対象のSSIDを選択します。

項目	説明
	• Downlink Speed： ダウンリンクの速度を設定します。単位はKbits/秒またはMbits/秒から選択できます。 • Uplink Speed： アップリンクの速度を設定します。単位はKbits/秒またはMbits/秒から選択できます。 • Add： 設定を追加します。 • Clear： 設定した内容を取り消します。
Bandwidth Optimization Rules	作成したルールのリストが表示されます。

3. [Save] をクリックして設定を保存します。

◆ 帯域幅最適化ルールを削除する場合：

1. [Bandwidth Optimization Rules] 欄の [Delete] をクリックします。
2. 確認メッセージが表示されるので、「OK」をクリックします。

◆ 帯域幅最適化ルールを編集する場合：

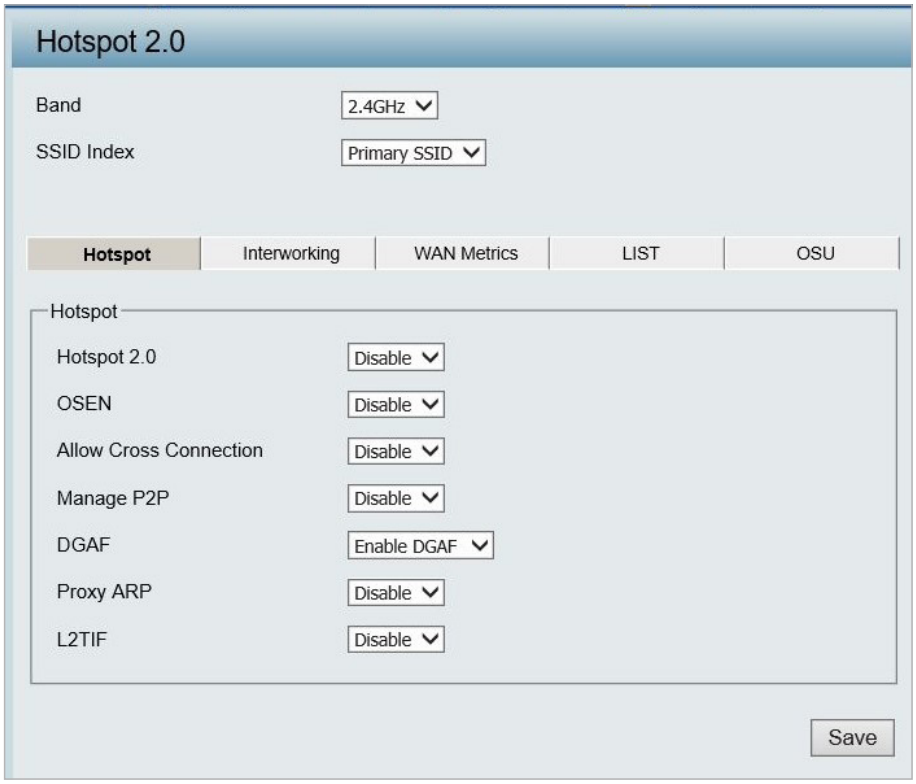
1. [Bandwidth Optimization Rules] の [Edit] をクリックします。
2. [Add Bandwidth Optimization Rule] でルールを編集します。
3. [Add] をクリックして設定を保存します。

Hotspot2.0（ホットスポット2.0）

ホットスポット2.0（HS2）は、デバイスとアクセスポイント間のシームレスな認証と暗号化により、パブリックワイヤレスホットスポットへの接続処理をより簡単かつ安全にするために設計された新しいネットワーク標準です。これはIEEE802.11u標準に基づいており、クライアントとアクセスポイント間の認証にWPA2 Enterpriseを使用しています。

1. [Advanced Settings] > [Hotspot2.0] を選択します。
2. [Band] で周波数帯を [2.4GHz] または [5GHz] に設定します。
3. [SSID Index] で SSID を選択します。
4. 以下のタブを使用して必要な設定を行います。
   - 『Hotspot タブ：p.62 』
   - 『Interworkingタブ：p.63 』
   - 『WAN Metricsタブ：p.64 』
   - 『LISTタブ：p.65 』
   - 『OSUタブ：p.66 』

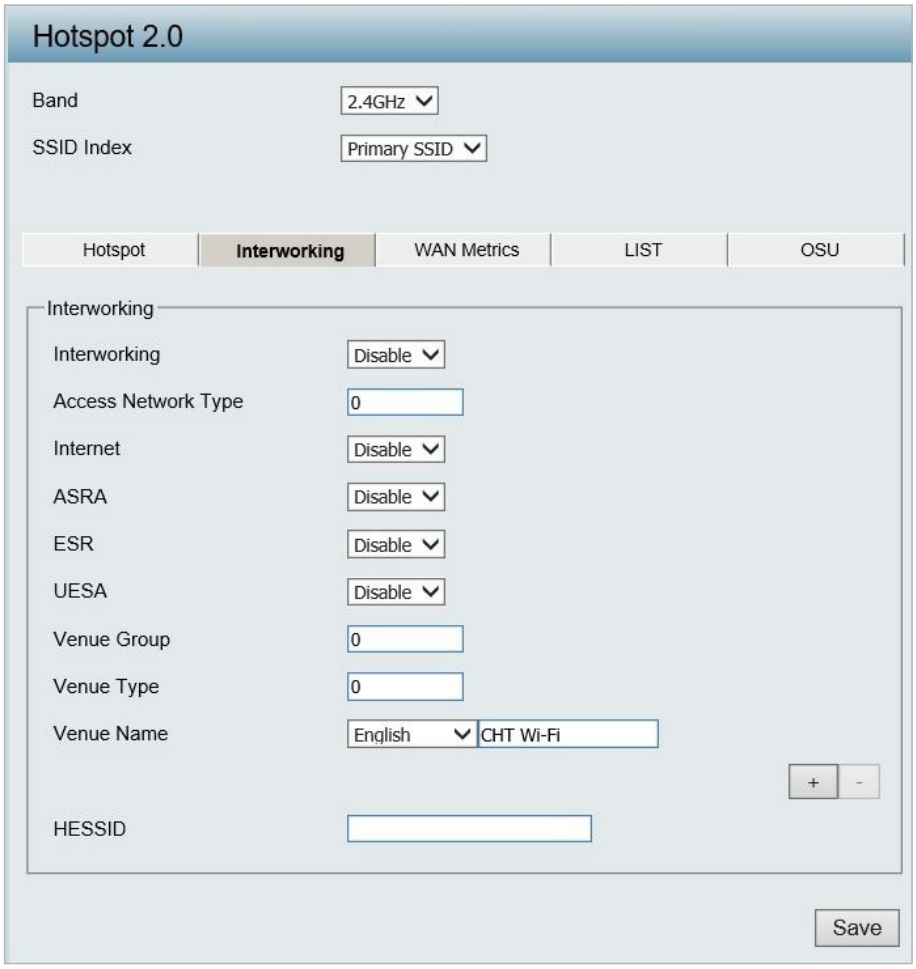
● Hotspot タブ



項目	説明
Hotspot 2.0	ホットスポット2.0機能を有効または無効にします。 ・選択肢：[Enable]（有効）[Disable]（無効）
OSEN	OSEN（OSU Server-only authenticated layer-2 Encryption Network）を有効または無効にします。ホットスポットがOSENネットワークタイプを使用している場合に有効に設定します。 ・選択肢：[Enable]（有効）[Disable]（無効）
Allow Cross Connection	クライアントのクロス接続を有効または無効にします。 ・選択肢：[Enable]（有効）[Disable]（無効）
Manage P2P	P2Pを有効または無効にします。 ・選択肢：[Enable]（有効）[Disable]（無効）

項目	説明
DGAF	DGAF (Downstream Group Addressed Forwardingを有効または無効にします。アクセスポイントがダウンストリームグループアドレスのフレームを転送できるようにします。 • 選択肢:[Enable DGAF] (有効) [Disable DGAF] (無効)
Proxy ARP	プロキシARPを有効または無効にします。 • 選択肢:[Enable] (有効) [Disable] (無効)
L2TIF	L2TIF (Layer 2 Traffic Inspection and Filtering) を有効または無効にします。 • 選択肢:[Enable] (有効) [Disable] (無効)

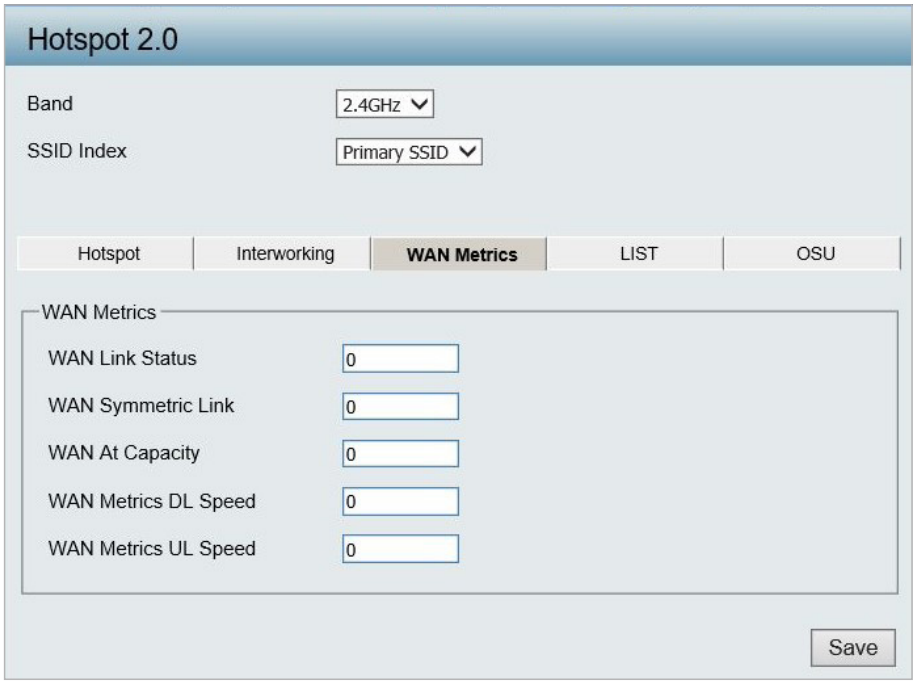
● Interworkingタブ



項目	説明
Interworking	インターワーキング機能を有効または無効にします。 • 選択肢:[Enable] (有効) [Disable] (無効)
Access Network Type	ネットワークの種類を指定します。 • 0:プライベートネットワーク • 1:ゲストアクセス付きプライベートネットワーク • 2:有料公衆ネットワーク • 3:無料公衆ネットワーク • 4:パーソナルデバイスネットワーク • 5:緊急サービスのみのネットワーク • 14:テストもしくは実験 • 15:ワイルドカード
Internet	ネットワークのインターネット接続を有効または無効にします。 • 選択肢:[Enable] (有効) [Disable] (無効)
ASRA	ASRA (Additional Steps required for Access) を有効または無効にします。 • 選択肢:[Enable] (有効) [Disable] (無効)

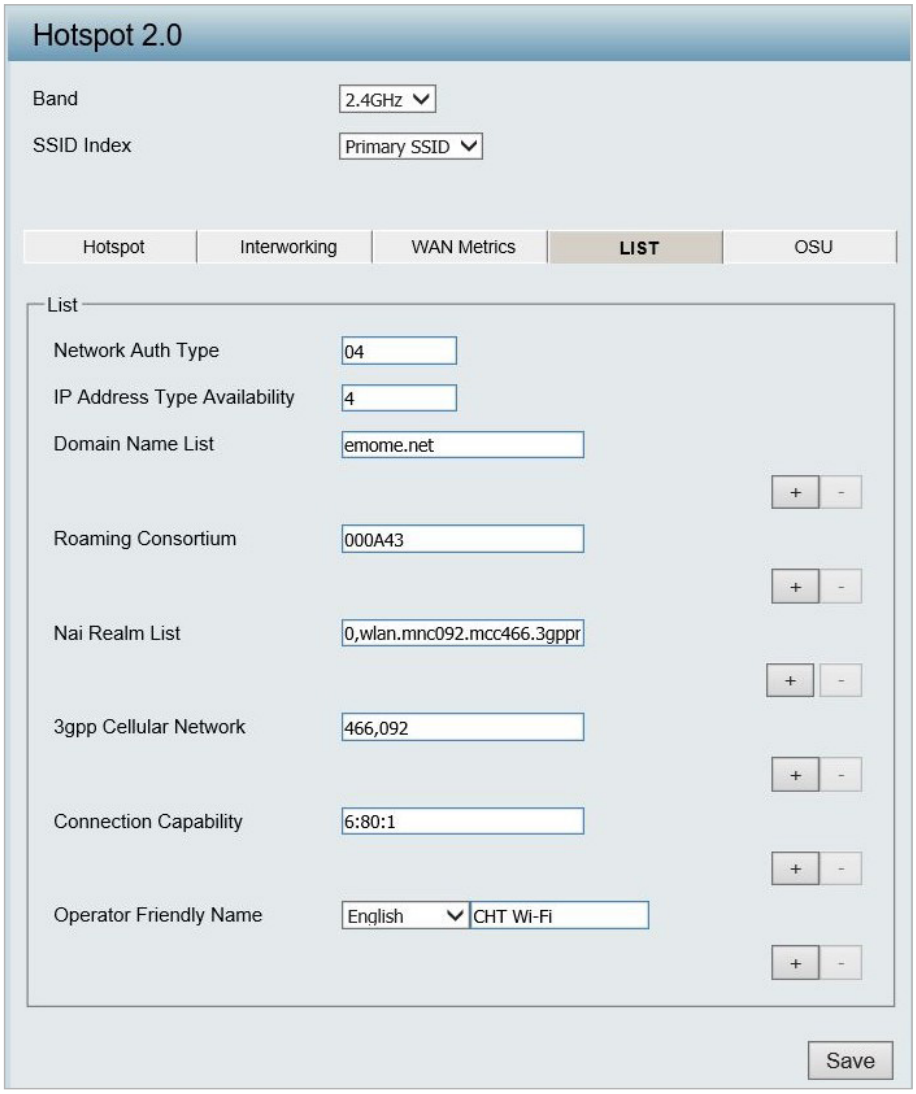
項目	説明
ESR	ESR(Emergency services reachable)を有効または無効にします。 • 選択肢:[Enable](有効)[Disable](無効)
UESA	UESR(Unauthenticated Emergency Service Accessible)を有効または無効にします。 • 選択肢:[Enable](有効)[Disable](無効)
Venue Group	Venue グループの値を入力します。
Venue Type	Venue タイプの値を入力します。
Venue Name	言語を選択し、Venue 名を入力します。
HESSID	Homogenous Extended Service Set(ESS) IDを入力します。サービスプロバイダネットワークを識別するために使用されます。

● WAN Metricsタブ



項目	説明
WAN Link Status	アクセスポイントのWAN接続のステータスを設定します。 • 1:リンクアップ • 2:リンクダウン • 3:テストステートでのリンク
WAN Symmetric Link	WANリンクが対称(アップロードとダウンロードの速度が同じ)の場合は1に設定し、そうでない場合は0に設定します。
WAN At Capacity	アクセスポイントまたはネットワークが最大容量の場合は1に設定し、そうでない場合は0に設定します。
WAN Metrics DL Speed	WAN接続のダウンリンク速度(kbps)を設定します。ダウンリンク速度が不明な場合は、0に設定します。
WAN Metrics UL Speed	WAN接続のアップリンク速度(kbps単位)を設定します。アップリンク速度が不明な場合は、0に設定します。

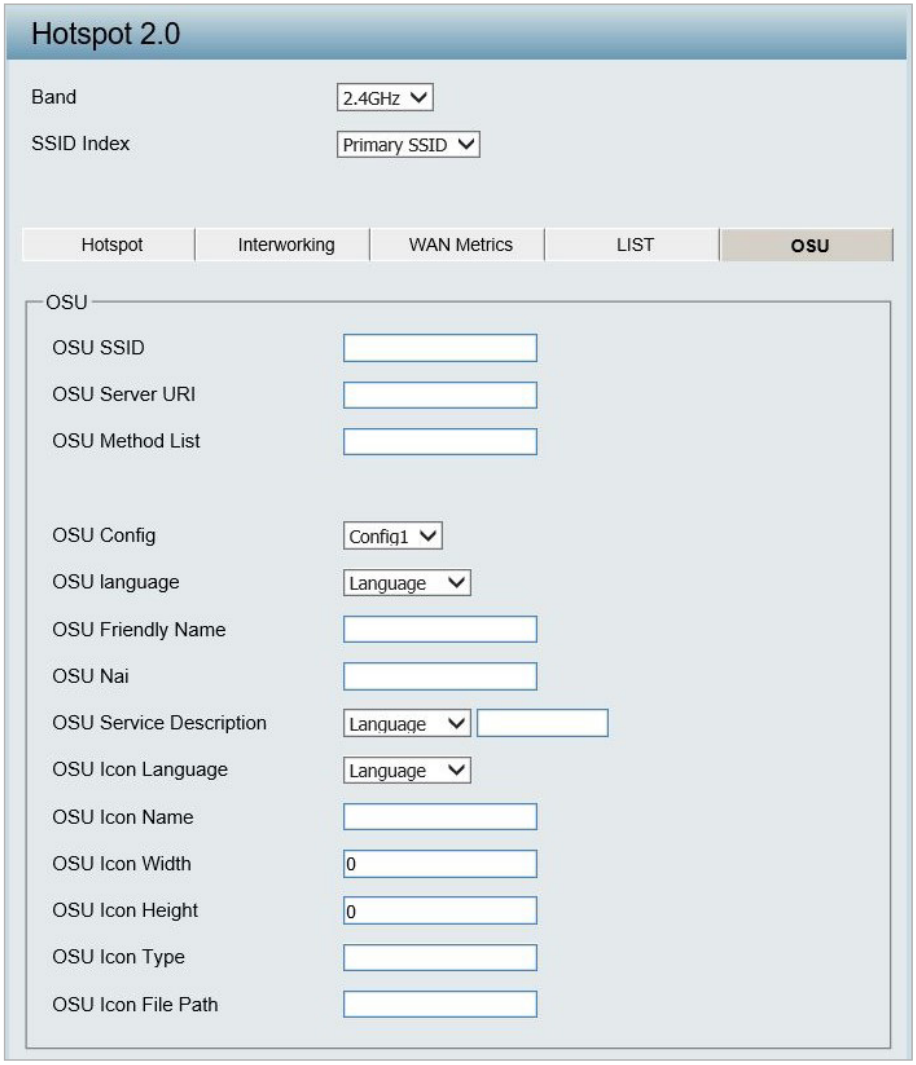
● LISTタブ



項目	説明
Network Auth Type	安全でないネットワークかどうかを識別します。<Type><URL>の形式で指定します。 （例：「01http://1.2.3.4」） • 00：利用規約への同意 • 01：オンライン登録をサポート • 02：http/httpsリダイレクション • 03：DNSリダイレクション
IP Address Type Availability	ホットスポット事業者が使用するIPアドレスのバージョンとタイプを識別します。これは、ネットワークの認証後にモバイルデバイスに割り当てられ、使用可能になります。 • 0：アドレスタイプは利用できません。 • 4：利用可能なグローバル IPv4 アドレス • 8：利用可能なポート制限されたIPv4 アドレス • c：利用可能なシングル NAT されたプライベート IPv4 アドレス • 10：「利用可能なダブル NAT されたプライベート IPv4 アドレス • 14：利用可能なポート制限された IPv4 アドレスとシングル NAT された IPv4 アドレス • 18：利用可能なポート制限された IPv4 アドレスとダブル NAT された IPv4 アドレス • 1c：アドレスタイプの IPv4 可用性は不明です。 • 1：利用可能な IPv6 アドレスタイプ • 2：アドレスタイプの IPv6 可用性は不明です。
Domain Name List	アクセスポイントを管理するエンティティのドメイン名を1つ以上指定します。
Roaming Consortium	ネットワークへの接続にセキュリティ資格情報を使用できるサービスプロバイダまたはローミングパートナーのグループを指定します。

項目	説明
Nai Realm List	BSSを介して使用可能なすべてのNAIレルムのリストを指定します。
3gpp Cellular Network	アクセスポイントを介して使用可能な3GPPセルラーネットワークを識別します。
Connection Capability	一般的なIPプロトコルとポートの可用性を識別します。 <IP Protocol>:<Port Number>:<Status>の形式で指定します。(例:「6:80:1」) IPプロトコルの指定パラメータは以下の通りです。 • 1: ICMP • 6:TCP • 17:UDP プロトコルステータスの指定パラメータは以下の通りです。 • 0:閉じる • 1:オープン • 2:不明
Operator Friendly Name	ホットスポットVenueオペレータを識別します。

● OSUタブ



項目	説明
OSU SSID	OSUサーバにアクセスする際にデバイスが関連付け、接続を行うマルチSSIDを指定します。
OSU Server URI	OSUサーバのURI(Uniform Resource Identifier)を指定します。

項目	説明
OSU Method List	OSUサーバがサポートするエンコード方式の優先リストを優先順に指定します。<language code>:<method>[,<language code>:<method>]の形式で指定します。（例：「en:11,de:22」）
OSU Config	使用する構成セットを選択します。
OSU language	使用する言語を選択します。
OSU Friendly Name	OSUフレンドリ名を各言語で指定し、モバイルデバイス側で選択した言語に基づいて代替言語のOSUフレンドリ名が表示されるようにします。
OSU Nai	OSUネットワークアクセス識別子を指定します。
OSU Service Description	サービス説明の言語を選択し、サービス提供を行うサービスプロバイダの説明を指定します。
OSU Icon Language	アイコンの言語を選択します。
OSU Icon Name	アイコン名を指定します。
OSU Icon Width	アイコンの幅をピクセル単位で指定します。
OSU Icon Height	アイコンの長さをピクセル単位で指定します。
OSU Icon Type	アイコンのファイルの種類を指定します。アイコンの種類は、MIMEタイプの画像形式です。
OSU Icon File Path	アイコンファイルの場所を指定します。

5. [Save] をクリックして設定を保存します。

Captive Portal（キャプティブポータル）

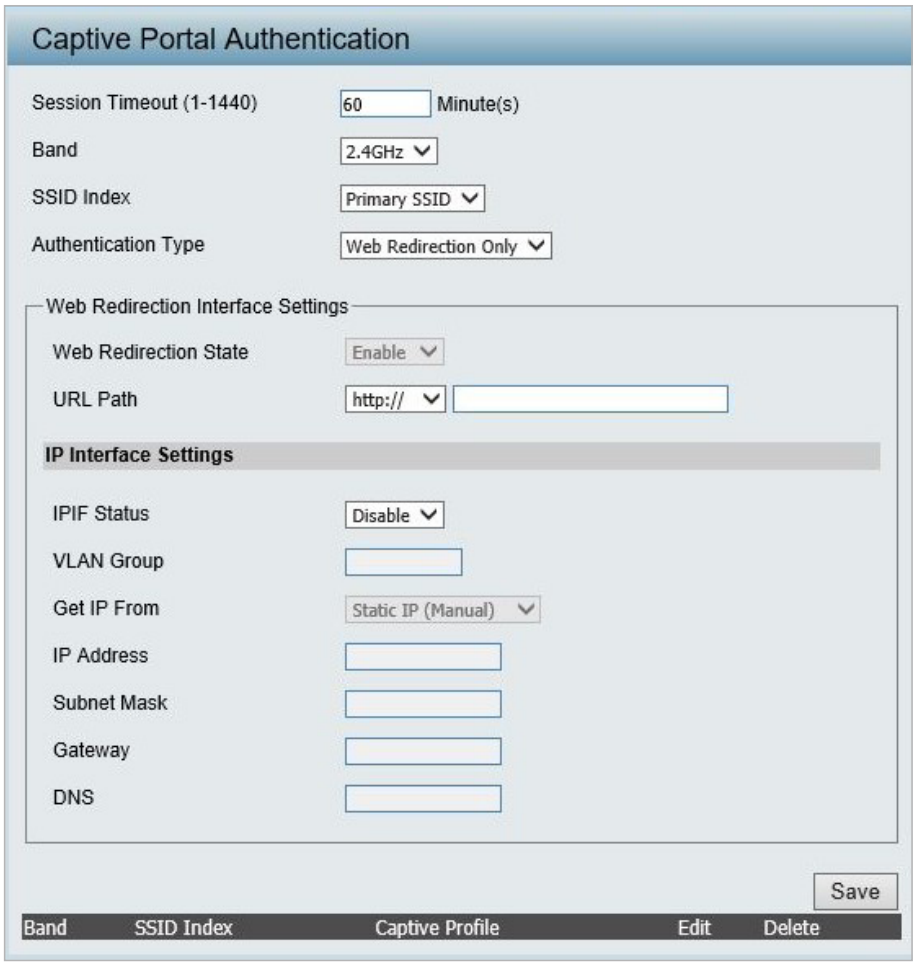
キャプティブポータルは、Web認証を行う機能です。
認証されていないクライアントがアクセスポイントに接続すると、Webブラウザによって認証画面へリダイレクトされます。

■Captive Portal Authentication（キャプティブポータル認証）

キャプティブポータル認証の暗号化タイプを選択し、暗号化タイプごとに必要な設定を行います。

1. [Advanced Settings] > [Captive Portal] > [Authentication Settings] を選択します。

2. [Authentication Type] で暗号化タイプを選択します。



項目	説明
Session Timeout(1-1440)	セッションのタイムアウトを1から1440分までの値で設定します。クライアントがアクセスポイントから切断され、指定した時間が経過すると再認証が必要となります。Session Timeoutは、経過後にSTAを切断する時間ではなく、再接続に際して再認証が必要となる時間を設定します。 ・初期値：60分
Band	周波数帯を [2.4GHz] または [5GHz] から選択します。
SSID Index	認証するSSIDを設定します。
Authentication Type	キャプティブポータル認証の暗号化タイプを設定します。 ・選択肢：[Disable（無効）][Web Redirection Only][Username/Password][Passcode][Remote RADIUS][LDAP][POP3][SLA]
Web Redirection State	Webリダイレクションのステータスを有効または無効にします。 ・選択肢：[Enable]（有効）[Disable]（無効） ・初期値：[Enable]
URL Path	[http://] または [https://] を設定し、WebサイトのURLを入力します。

項目	説明
IRIF Status	キャプティブポータルのIPインタフェースを有効または無効にします。 • 選択肢：[Enable]（有効）[Disable]（無効） • 初期値：[Enable]
VLAN Group	VLAN Group IDを入力します。
Get IP From	IPアドレスの取得方法を選択します。 • [Static IP (Manual)]：固定のIPアドレスを手動で設定します。 • [Dynamic (DHCP)]：DHCPサーバを使用してIPアドレスを設定します。本製品のIPアドレスは、DHCPサーバから自動的に取得されます。[Dynamic (DHCP)] を選択した場合、その他の項目の設定は不要です。
IP Address	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。
Gateway	ゲートウェイのIPアドレスを入力します。
DNS	Domain Name System (DNS)サーバのアドレスを入力します。

3. 暗号化タイプごとに必要な設定を行います。

メモ

- 選択した暗号化タイプによって設定項目が異なります。
- 選択できる暗号化タイプは以下の通りです。
  - Web Redirection Only → 『暗号化タイプを [Web Redirection Only] または [SLA] にした場合：p.70 』を参照
  - Username/Password → 『暗号化タイプを [Username/Password] にした場合：p.71 』を参照
  - Passcode → 『暗号化タイプを [Passcode] にした場合：p.72 』を参照
  - Remote RADIUS → 『暗号化タイプを [Remote RADIUS] にした場合：p.73 』を参照
  - LDAP → 『暗号化タイプを [LDAP] にした場合：p.75 』を参照
  - POP3 → 『暗号化タイプを [POP3] にした場合：p.76 』を参照
  - SLA → 『暗号化タイプを [Web Redirection Only] または [SLA] にした場合：p.70 』を参照

重要

Captive Portal＋IPIFで設定したIPアドレスへは無線側からの接続はできません。

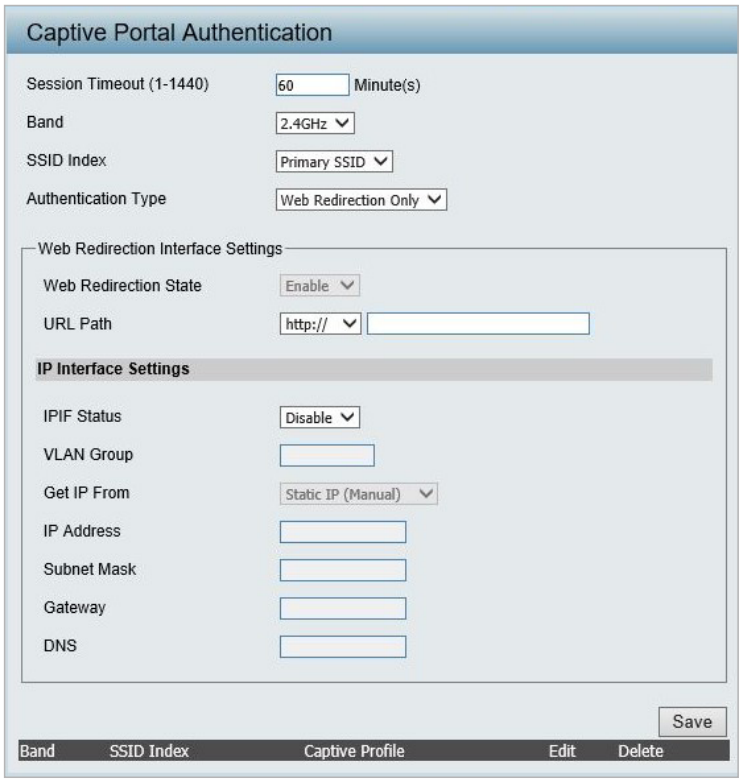
● 暗号化タイプを [Web Redirection Only] または [SLA] にした場合

WebリダイレクトまたはSLAを使用して認証を行います。

メモ

- WEBリダイレクトとは、サイトにアクセスしようとしたユーザを、最初にリクエストされた URL とは別の URL に移動させることです。クライアントは、キャプティブポータルによる認証の際に本項目で設定したWebサイトにリダイレクトされます。

1. 以下の画面でWebリダイレクトの設定を行います。

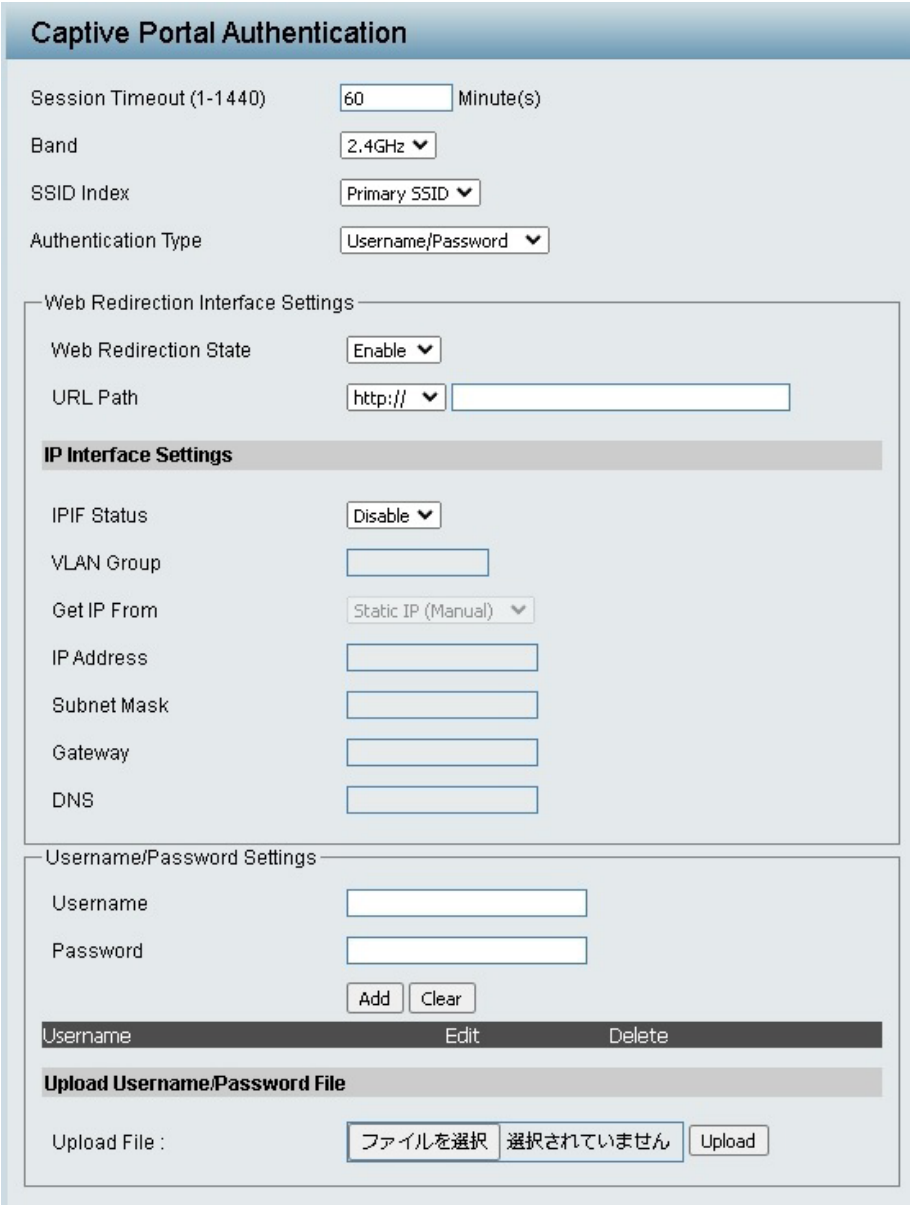


項目	説明
Web Redirection State	Webリダイレクションのステータスは [Enable] に固定されます。
URL Path	[http://] または [https://] を設定し、WebサイトのURLを入力します。
IRIF Status	キャプティブポータルのIPインタフェースを有効または無効にします。 • 選択肢：[Enable]（有効）[Disable]（無効） • 初期値：[Enable]
VLAN Group	VLAN Group IDを入力します。
Get IP From	IPアドレスの取得方法を選択します。 • [Static IP (Manual)]：固定のIPアドレスを手動で設定します。 • [Dynamic (DHCP)]：DHCPサーバを使用してIPアドレスを設定します。本製品のIPアドレスは、DHCPサーバから自動的に取得されます。[Dynamic (DHCP)] を選択した場合、その他の項目の設定は不要です。
IP Address	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。
Gateway	ゲートウェイのIPアドレスを入力します。
DNS	Domain Name System (DNS)サーバのアドレスを入力します。

● 暗号化タイプを [Username/Password] にした場合

ユーザ名とパスワードを使用して認証を行います。

1. 以下の画面でユーザ名とパスワードの設定を行います。



項目	説明
Username	アカウントのユーザ名を入力します。
Password	アカウントのパスワードを入力します。
Add	設定した内容を追加します。
Clear	入力した内容をクリアします。

2. [Add] をクリックしてユーザ名とパスワードの設定を追加します。

◆ ユーザ名とパスワードの設定を削除する場合：

1. [Delete] 欄の [Delete] をクリックします。
2. 確認メッセージが表示されるので、「OK」をクリックします。

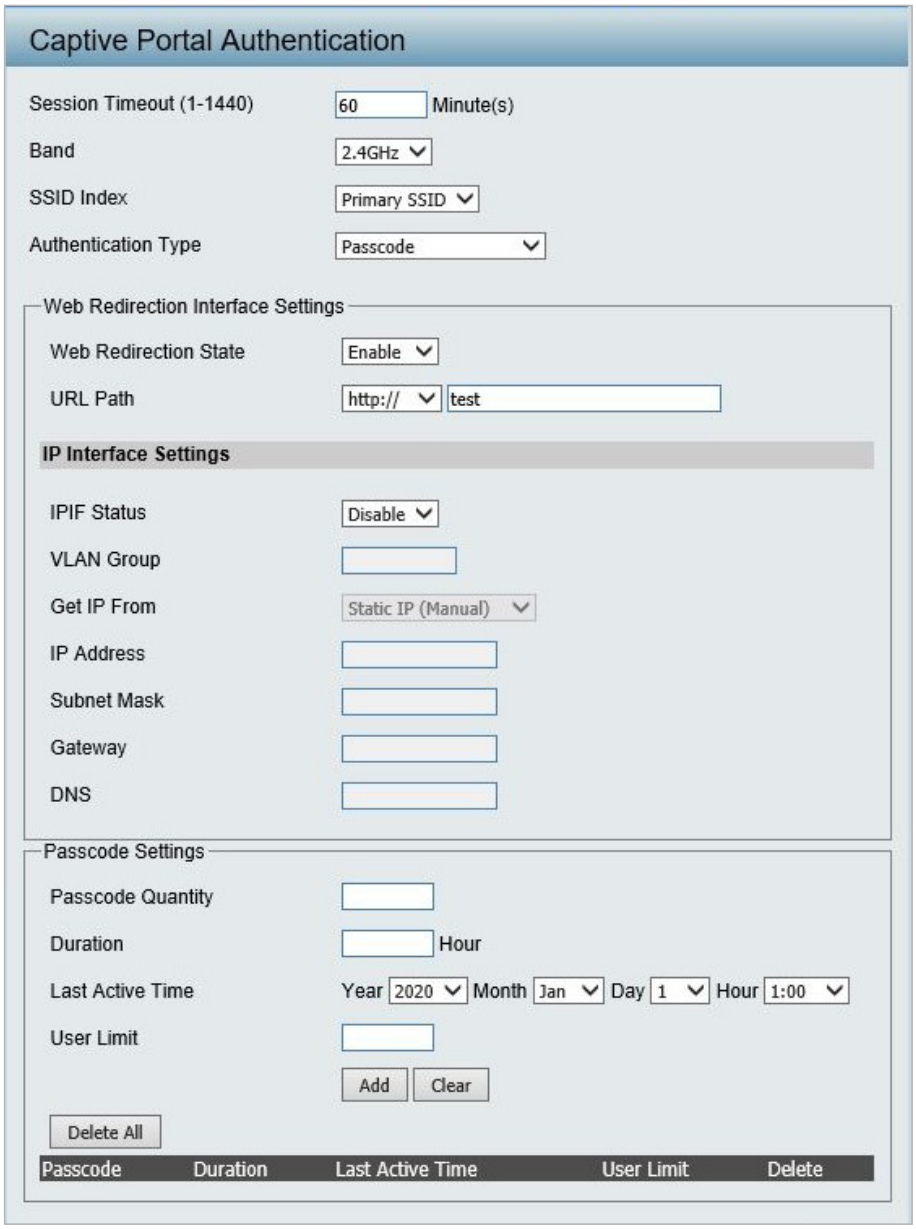
◆ ユーザ名とパスワードの設定を編集する場合：

1. [Edit] 欄の [Edit] をクリックします。
2. 設定を編集します。
3. [Add] をクリックして変更を保存します。

● 暗号化タイプを [Passcode] にした場合

パスコードを使用して認証を行います。

1. 以下の画面でパスコードの設定を行います。



項目	説明
Passcode Quantity	生成するパスコードの数を設定します。
Duration	生成したパスコードを有効にする時間（単位：時間）を設定します。
Last Active Time	生成したパスコードが有効となる最終日（年/月/日/時）を設定します。
User Limit	生成したパスコードを利用できるユーザ数の上限を設定します。
Add	設定した内容を追加します。
Clear	設定した内容を取り消します。
Delete All	設定したパスコードをすべて削除します。

2. [Add] をクリックしてパスコード設定を追加します。

生成されたパスコードは以下のように表示されます。

Passcode	Duration	Last Active Time	User Limit	Delete
65153939	1	2023-01-01-01:00	1	Delete

◆ パスコード設定を削除する場合：

1. [Delete] 欄の [Delete] をクリックします。
2. 確認メッセージが表示されるので、「OK」をクリックします。

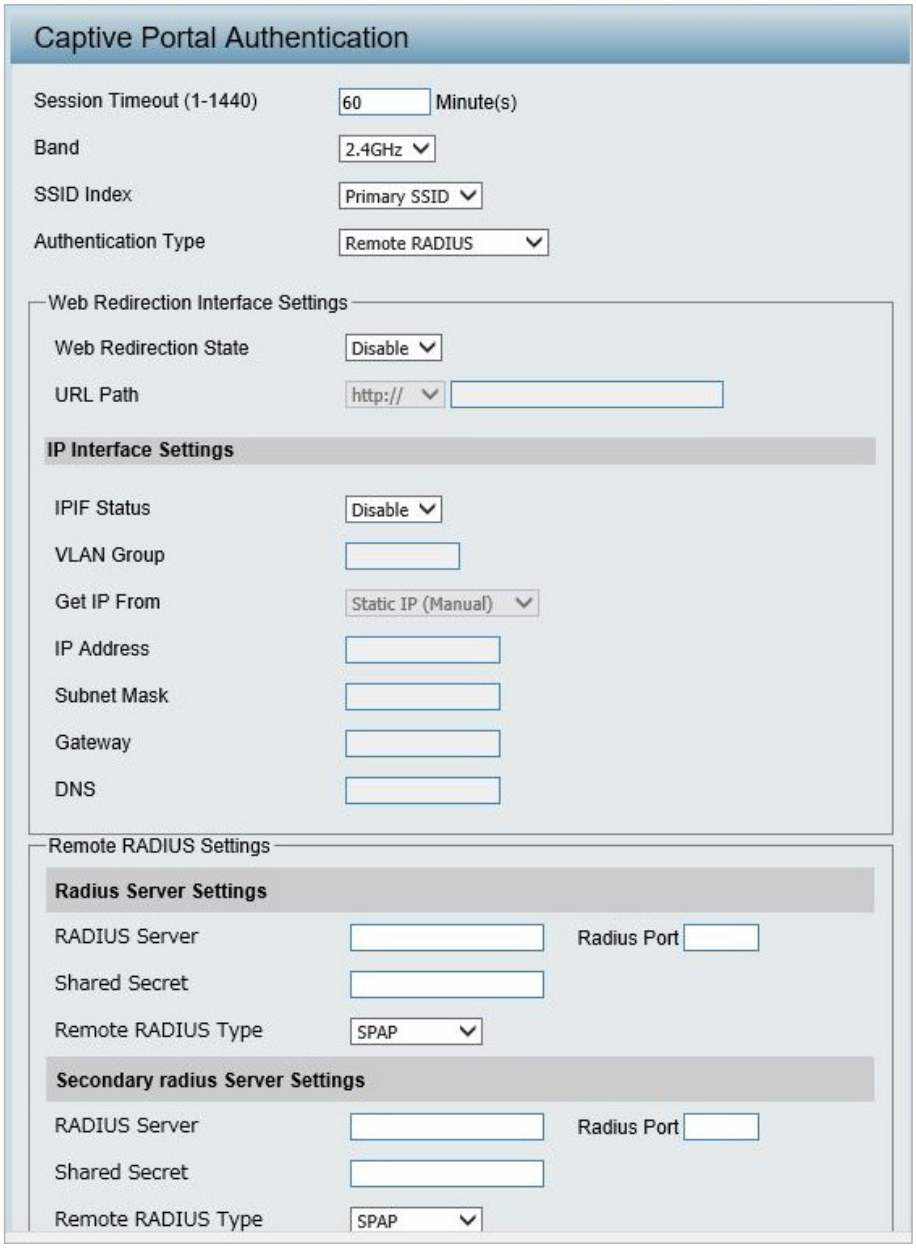
メモ

既知の問題により、「Passcode Settings」の「Clear」ボタンは動作しません。入力値は手動で削除してください。

● 暗号化タイプを [Remote RADIUS] にした場合

リモートRADIUSを使用して認証を行います。

1. 以下の画面でユーザ名とパスワードの設定を行います。

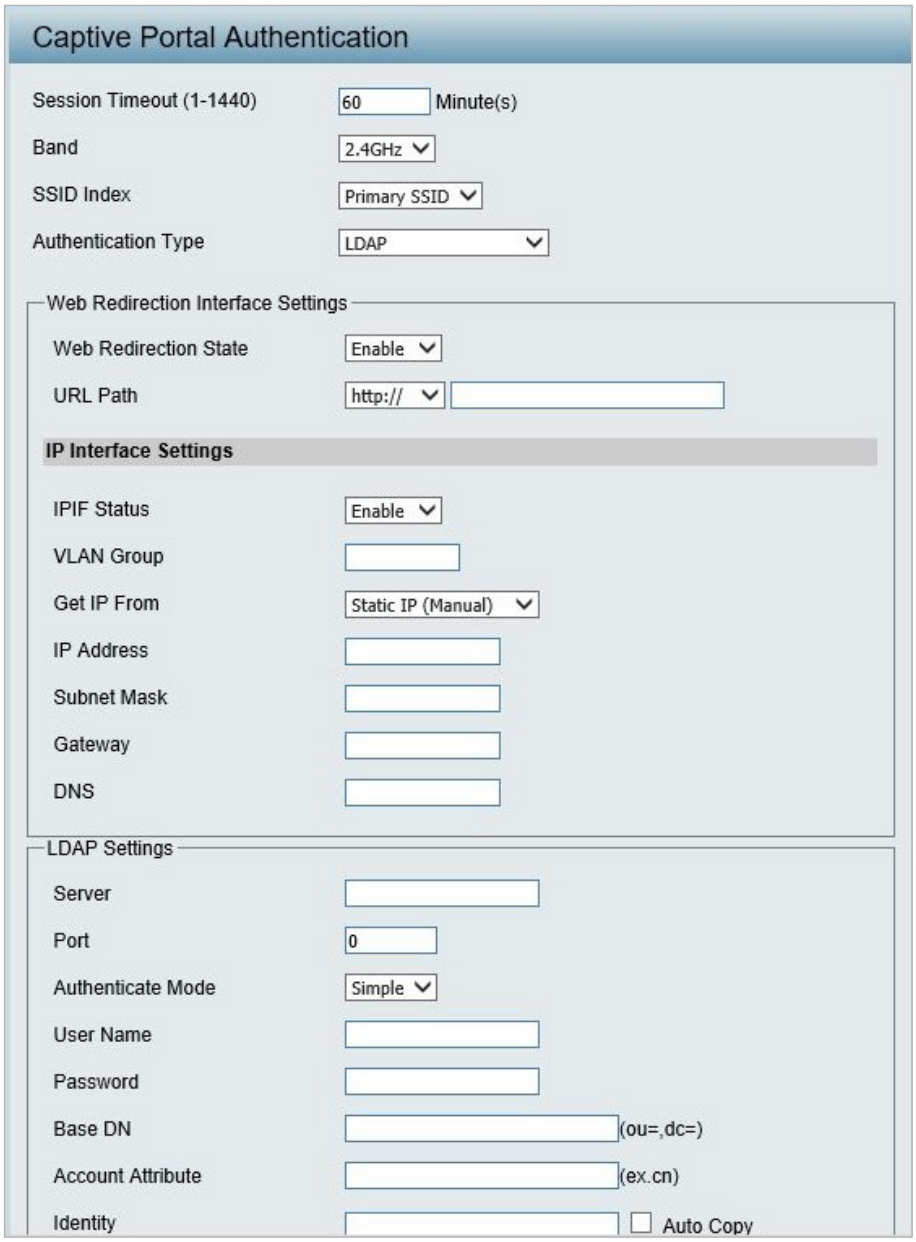


項目	説明
Radius Server Settings	RADIUSサーバの設定を行います。 • Radius Server： RADIUSサーバのIPアドレスを入力します。 • Radius Port： RADIUSサーバのポートを入力します。 初期値：1812 • Shared Secret： RADIUSシークレット（パスワード）を入力します。 • Remote Radius Type： リモートRADIUSのタイプを選択します。 選択肢：[SPAP][MS-CHAPv2]
Secondary radius Server Settings	セカンダリRADIUSサーバの設定を行います。 • Radius Server： RADIUSサーバのIPアドレスを入力します。 • Radius Port： RADIUSサーバのポートを入力します。 初期値：1812 • Shared Secret： RADIUSシークレット（パスワード）を入力します。 • Remote Radius Type： リモートRADIUSのタイプを選択します。 選択肢：[SPAP][MS-CHAPv2]
Third radius Server Settings	サード（ターシャリ）RADIUSサーバの設定を行います。 • Radius Server： RADIUSサーバのIPアドレスを入力します。 • Radius Port： RADIUSサーバのポートを入力します。 初期値：1812 • Shared Secret： RADIUSシークレット（パスワード）を入力します。 • Remote Radius Type： リモートRADIUSのタイプを選択します。 選択肢：[SPAP][MS-CHAPv2]

● 暗号化タイプを [LDAP] にした場合

LDAPサーバを使用して認証を行います。

1. 以下の画面でLDAPサーバの設定を行います。

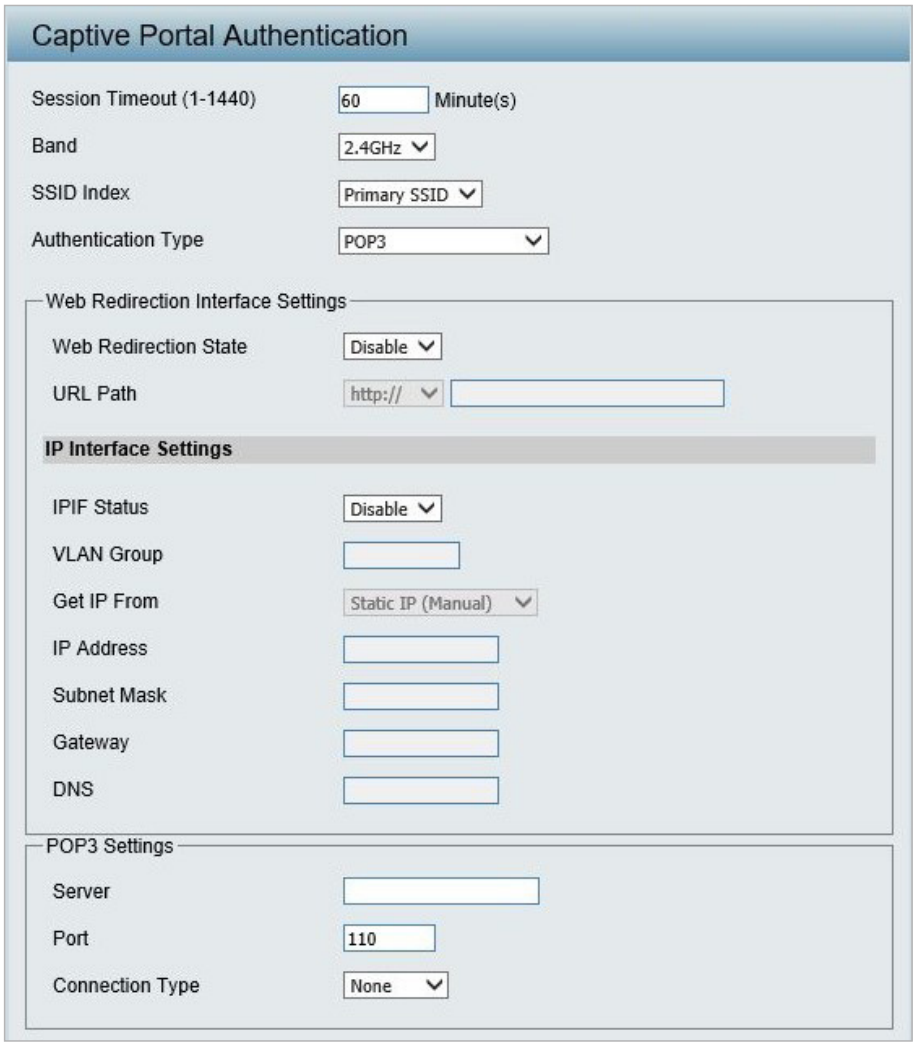


項目	説明
Server	LDAPサーバのIPアドレスまたはドメイン名を入力します。
Port	LDAPサーバのポートを入力します。 • 初期値：389
Authenticate Mode	認証モードを [Simple] または [TLS] から選択します。 • Simple：LDAPデータは暗号化されません。 • TLS：LDAPデータは暗号化されます。
User Name	LDAPサーバアカウントのユーザ名を入力します。
Password	LDAPサーバアカウントのパスワードを入力します。
Base DN	ベースDNを入力します。
Account Attribute	LDAPアカウントの属性値を入力します。 この文字列はクライアントの検索に使用されます。
Identity	アイデンティティのパス文字列全体を入力してください。 [Auto Copy] にチェックを入れると、自動的にパスが入力されます。

● 暗号化タイプを [POP3] にした場合

POP3サーバを使用して認証を行います。

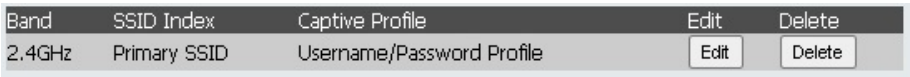
1. 以下の画面でPOP3サーバの設定を行います。



項目	説明
Server	POP3サーバのIPアドレスまたはドメイン名を入力します。
Port	POP3サーバのポート番号を入力します。 ・初期値:110
Connection Type	接続モードを選択します。 ・選択肢:[None][SSL/TLS]

3. 画面下部の [Save] をクリックして、手順 3 で設定した内容をキャプティブプロファイルに追加します。

設定した内容は以下のように表示されます。



◆ キャプティブプロファイル削除する場合：

1. [Delete] 欄の [Delete] をクリックします。

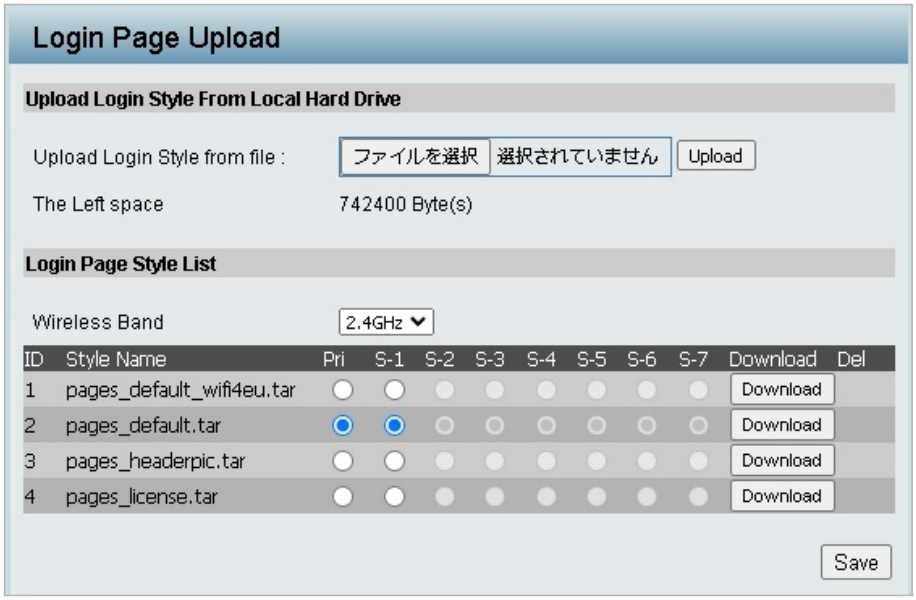
◆ キャプティブプロファイルを編集する場合：

1. [Edit] 欄の [Edit] をクリックします。
2. 設定を編集します。
3. [Save] をクリックして設定を保存します。

■Login Page Upload（ログイン画面アップロード）

キャプティブポータルのログイン画面のスタイルを変更したり、カスタムページをアップロードしたりすることができます。各スタイルのデザインはダウンロードしたHTMLファイルで確認することができます（実際の画面項目は、指定した認証設定により異なります）。

1. [Advanced Settings] > [Captive Portal] > [Login Page Upload] を選択します。
2. [参照 / ファイルを選択] をクリックし、アップロードする画像を選択します。



項目	説明
Upload Login Style From Local Hard Drive	アップロードするログイン画面のスタイルファイルを選択します。 [The Left space]は、デバイス上の利用可能なメモリ（Bytes）を示しています。
Login Page Style List	• [Wireless Band] 周波数帯を選択します。 選択肢：[2.4GHz][5GHz] • [ID Style Name] 各SSIDで使用するファイルを選択します。 ファイルをダウンロードする場合は [Download] 欄の [Download] ボタン、削除する場合は [Del] 欄の [Delete] ボタンを選択します。

3. [Upload] をクリックして画像をアップロードします。

◆ SSID に紐づけるスタイルを変更する場合：

1. [Wireless Band] 欄で周波数帯を選択し、設定を変更します。
2. 「Save」をクリックします。

■MAC Bypass（MAC Bypass 設定）

本項目では、MAC Bypassの設定方法について説明します。本機能により、キャプティブポータル認証を必要とせずに、ネットワーク内のクライアントがインターネットにアクセスできるようになります。

1. [Advanced Settings] > [Captive Portal] > [MAC Bypass Settings] を選択します。

2. 以下の画面で設定を行います。

項目	説明
Wireless Band	周波数帯を [2.4GHz] または [5GHz] に設定します。
SSID Index	SSIDを選択します。
MAC Address	以下の手順でMACアドレスを登録します。 1. MACアドレスを入力します。 2. [Add] をクリックします。 追加したMACアドレスは一覧に表示されます。追加したMACアドレスを削除する場合は [Delete] 欄の [Delete] をクリックします。
Upload MAC File	MACバイパスリストのファイルのアップロードを行います。 [参照/ファイルを選択] をクリックしてファイルを選択し [Upload] をクリックします。
Download MAC File	[Download] をクリックし、MACバイパスリストのファイルのダウンロードを行います。

3. [Save] をクリックして設定を保存します。

メモ

MAC Bypass機能において、登録可能なエントリはSSID毎 64個までとなります。

DHCP Server（DHCPサーバ設定）

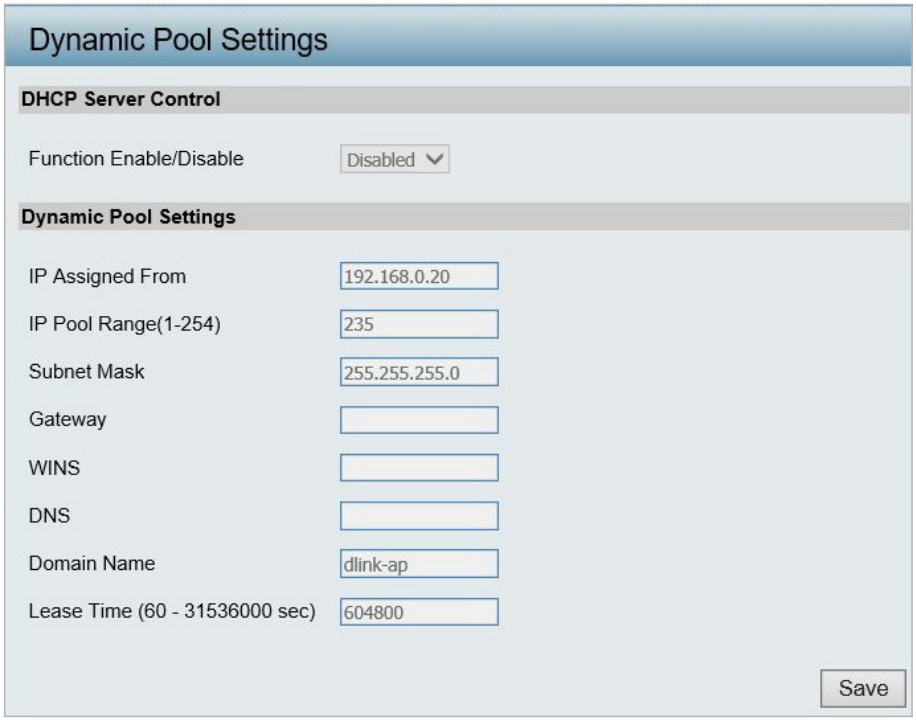
本製品のDHCP（Dynamic Host Configuration Protocol）サーバ機能の設定を行います。
DHCPサーバ機能により、IPアドレスなどネットワークに接続するために必要な情報を無線ステーションへ割り当てることができます。

■Dynamic Pool Settings（ダイナミックプール設定）

IPアドレスを自動的に無線ステーションへ割り当てるDHCPダイナミックプールの設定を行います。
DHCPアドレスプールは、ネットワークのステーションに割り当てるIPアドレスの範囲を定義します。
無線ステーションは、設定されたリース期間中、利用可能なIPアドレスを割り当てられます。

1. [Advanced Settings] > [DHCP Server] > [Dynamic Pool Settings] を選択します。

2. 以下の画面で設定を行います。



項目	説明
DHCP Server Control	[Function Enable/Disable] でDHCPサーバ機能を有効または無効にします。 • 選択肢：[Enable]（有効）[Disable]（無効）
Dynamic Pool Settings	DHCPサーバ機能を有効にした場合、以下の項目で設定を行います。 • IP Assigned From : 割り当てを開始するIPアドレスを入力します。 • The Pool Range (1-254)： 割り当てが可能なIPアドレスの数を入力します。[IP Assigned From] で指定したIPアドレスを起点とした範囲となります。 選択可能範囲：1-254 • Subnet Mask : 割り当てるIPアドレスのサブネットマスクを入力します。 • Gateway : ゲートウェイIPアドレスを入力します。 • WINS : Windows Internet Naming Service（WINS）サーバのアドレスを入力します。 • DNS : Domain Name System（DNS）サーバのアドレスを入力します。 • Domain Name : ネットワークのドメイン名を入力します。 • Lease Time (60-31536000 sec): IPアドレスをリースする期間を入力します。リース期間を超過すると新しいIPアドレスが無線ステーションに割り当てられます。 選択可能範囲：60-31536000 (秒)

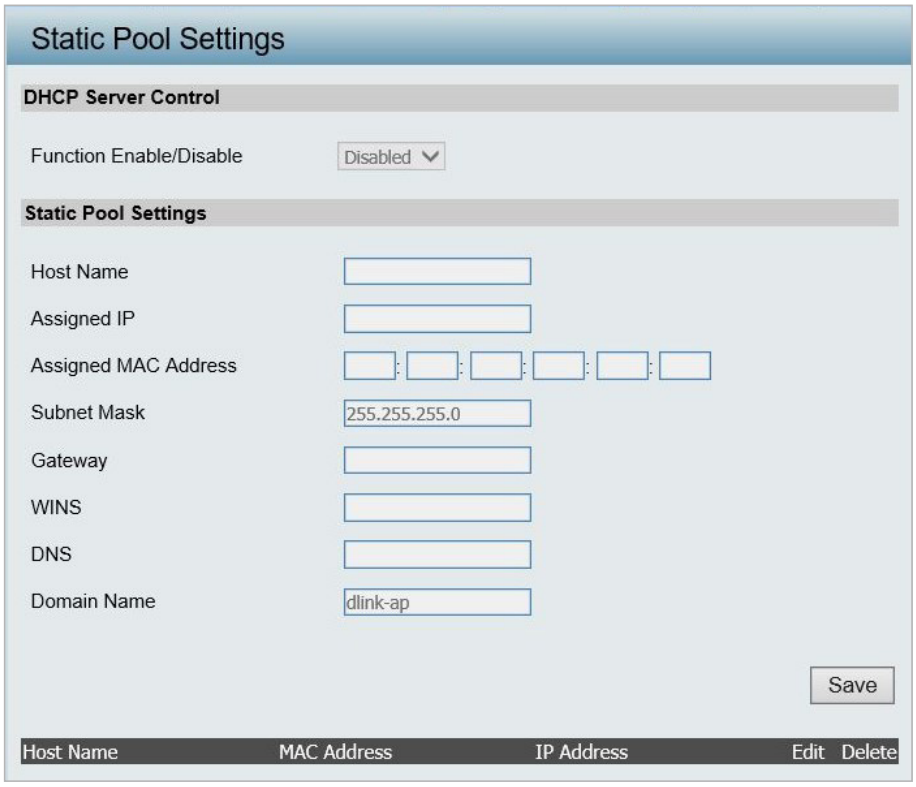
3. [Save] をクリックして設定を保存します。

■Static Pool Settings（スタティックプール設定）

固定のIPアドレスを無線ステーションへ割り当てるスタティックプールの設定を行います。

1. [Advanced Settings] > [DHCP Server] > [Static Pool Settings] を選択します。

2. 以下の画面で設定を行います。



項目	説明
DHCP Server Control	[Function Enable/Disable] でDHCPサーバ機能を有効または無効にします。 • 選択肢：[Enable]（有効）[Disable]（無効）
Static Pool Settings	DHCPサーバ機能を有効にした場合、以下の項目で設定を行います。 • Host Name : ホスト名を入力します。 • Assigned IP： 割り当てるIPアドレスを入力します。 • Assigned MAC Address : IPアドレスを割り当てる無線ステーションのMAC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。 • Gateway : ゲートウェイIPアドレスを入力します。 • WINS : Windows Internet Naming Service（WINS）サーバのアドレスを入力します。 • DNS : Domain Name System（DNS）サーバのアドレスを入力します。 • Domain Name : ネットワークのドメイン名を入力します。

3. [Save] をクリックして設定を保存します。

◆ 設定を削除する場合：

1. [Delete] 欄の [Delete] をクリックします。

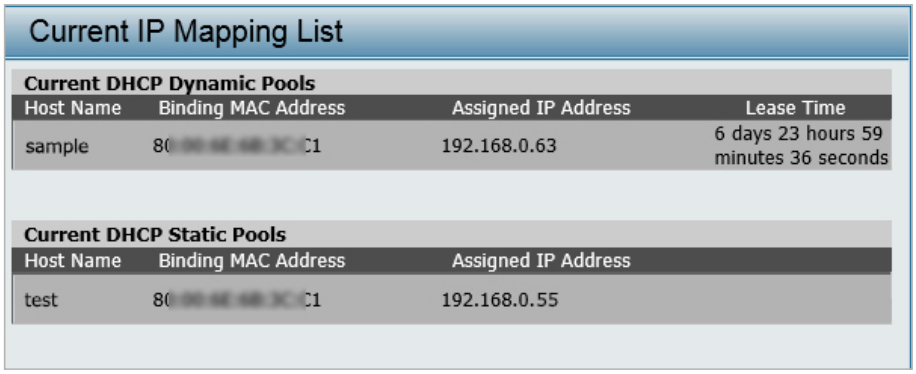
◆ 設定した内容を編集する場合：

1. [Edit] 欄の [Edit] をクリックします。
2. 設定を編集します。
3. [Save] をクリックして変更を保存します。

■Current IP Mapping List（IPマッピングリスト）

ダイナミックプール設定・スタティックプール設定によって割り当てられたIPアドレスのリストを表示します。

1. [Advanced Settings] > [DHCP Server] > [Static Pool Settings] を選択します。
2. 以下の画面で IP アドレスのリストを確認します。



項目	説明
Current DHCP Dynamic Pools	ダイナミックプールで割り当てたIPアドレスのリストが表示されます。 • Host Name : ホスト名が表示されます。 • Binding MAC Address : IPアドレスを使用している無線ステーションのMACアドレスが表示されます。 • Assigned IP Address : 割り当てたIPアドレスが表示されます。 • Lease Time : IPアドレスのリース期間が表示されます。
Current DHCP Static Pools	スタティックプールで割り当てたIPアドレスのリストが表示されます。 • Host Name : ホスト名が表示されます。 • Binding MAC Address : IPアドレスを使用している無線ステーションのMACアドレスが表示されます。 • Assigned IP Address : 割り当てたIPアドレスが表示されます。

Filters（フィルタ）

■Wireless MAC ACL Settings（ワイヤレスMAC ACL）

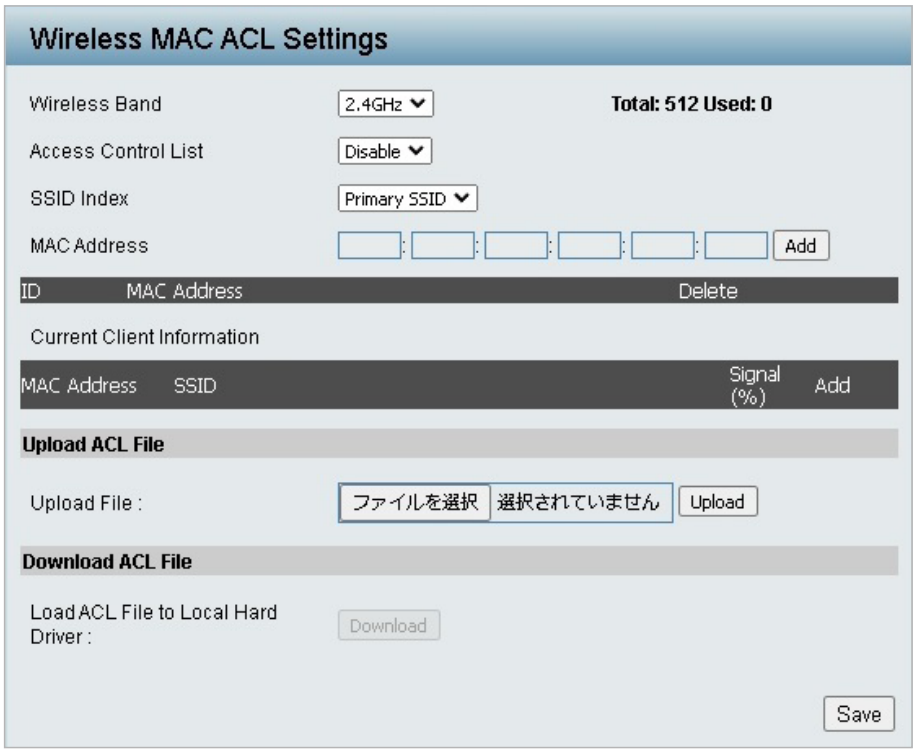
MACアドレスによるフィルタリングを行います。

メモ

MAC ACLはRadio単位で最大512までです。

1. [Advanced Settings] > [Filters] > [Wireless MAC ACL] を選択します。

2. 以下の画面で設定を行います。



項目	説明
Wireless Band	周波数帯を [2.4GHz] または [5GHz] から選択します。
Access Control List	ACL（Access Control List）の設定を無効/許可/拒否のいずれかに設定します。 • Disable : アクセスコントロールリストは無効となります。 • Allow : アクセスコントロールリストに登録されているMAC アドレスを持つデバイスのみ接続を許可します。 • Deny : アクセスコントロールリストに登録されているMAC アドレスを持つデバイスとの接続を拒否します。
SSID Index	SSIDを選択します。
MAC Address	以下の手順でMACアドレスを登録します。 1. MACアドレスを入力します。 2. [Add] をクリックします。 追加したMACアドレスは一覧に表示されます。
Current Client Information	本製品に接続しているクライアントの情報が表示されます。 [Add] にチェックをいれると、クライアントはアクセスコントロールリストに追加されます。
Upload ACL File	以下の手順でアクセスコントロールリストのファイルをアップロードします。 1. [参照/ファイルを選択] をクリックしてファイルを選択します。 2. [Upload] をクリックしてファイルをアップロードします。

項目	説明
Load ACL File to Local Hard Drive	[Download] をクリックして、アクセスコントロールリストのファイルをダウンロードします。

3. [Save] をクリックして設定を保存します。

◆ アクセスコントロールリストを削除する場合：

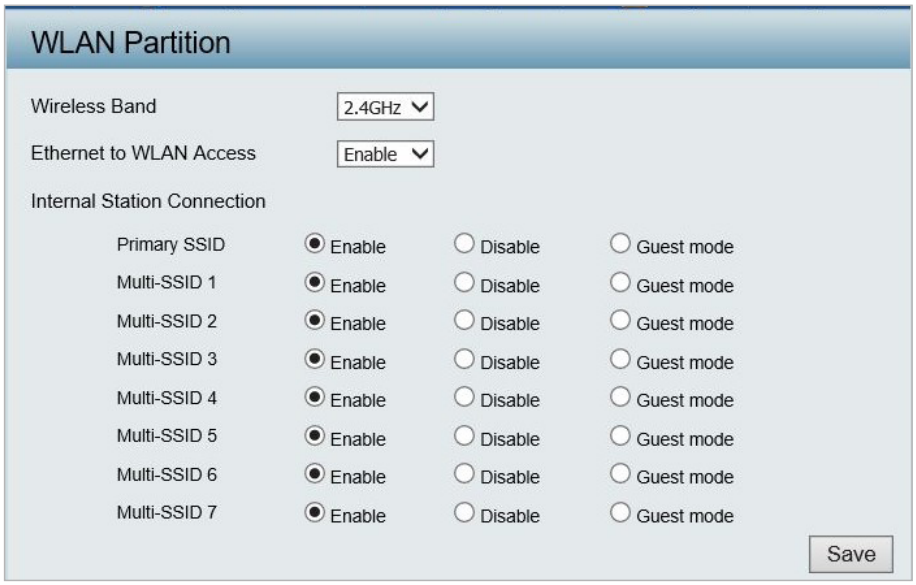
1. [Delete] 欄の [Delete] をクリックします。

■WLAN Partition（WLANパーティション）

WLANパーティションの設定を行います。

1. [Advanced Settings] > [Filters] > [WLAN Partition] を選択します。

2. 以下の画面で設定を行います。



項目	説明
Wireless Band	周波数帯を [2.4GHz] または [5GHz] から選択します。
Ethernet to WLAN Access	有線LANから無線LANへのデータ送信を有効または無効にします。 • 選択肢：[Enable]（有効）[Disable]（無効） • 初期値：[Enable]
Internal Station Connection	SSIDごとにステーションとの通信モードを設定します。 • Enable： 同じSSIDに接続しているワイヤレスクライアント間での通信、および異なるSSIDに接続しているワイヤレスクライアント間での通信が可能です。 • Disable： 同じSSIDに接続しているワイヤレスクライアント間での通信はできません。 異なるSSIDに接続しているワイヤレスクライアント間での通信は可能です。 • Guest mode： 同じSSIDに接続しているワイヤレスクライアント間での通信、および異なるSSIDに接続しているワイヤレスクライアント間での通信ができません。

3. [Save] をクリックして設定を保存します。

重要

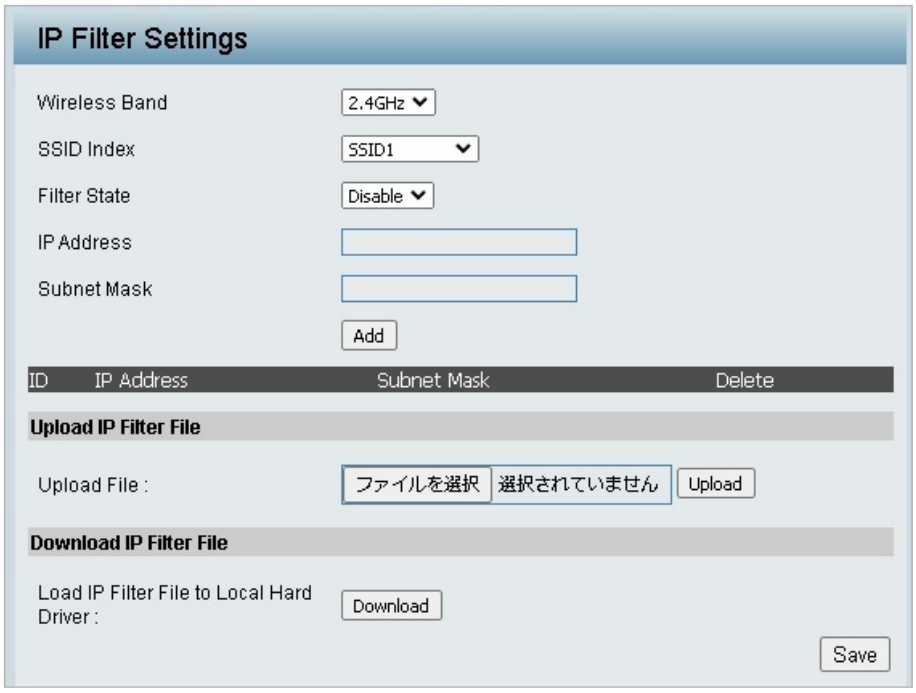
WLAN Partitionは、上位でVLAN間ルーティングされる構成では無効です。

■IP Filter Settings（IPフィルタ）

IPアドレス（192.168.70.66など）やネットワークアドレス（192.168.70.0など）を使用してフィルタリングを行います。
設定したアドレスはネットワークへのアクセスが無効になります。

1. [Advanced Settings] > [Filters] > [IP Filter Settings] を選択します。

2. 以下の画面で設定を行います。



項目	説明
Wireless Band	周波数帯を [2.4GHz] または [5GHz] に設定します。
SSID Index	SSIDを選択します。
Filter State	フィルタリングステータスを有効または無効にします。 ・選択肢：[Enable]（有効）[Disable]（無効） ・初期値：[Diable]
IP Address **Subnet Mask**	以下の手順でIPアドレスを登録します。 1. [IP Address] にIPアドレスまたはネットワークアドレスを入力します。 2. [Subnet Mask] にIPアドレスまたはネットワークアドレスのサブネットマスクを入力します。 3. [Add] をクリックします。 追加したIPアドレスは一覧に表示されます。
Upload IP Filter File	IPフィルタリストのファイルをアップロードします。 [参照/ファイルを選択] をクリックして、IPフィルタリストのファイルを選択し [Upload] をクリックします。
Download IP Filter File	[Download] をクリックして、IPフィルタリストのファイルをダウンロードします。

3. [Save] をクリックして設定を保存します。

◆ IP フィルタリストを削除する場合：

1. [Delete] 欄の [Delete] をクリックします。

重要

DAP-3666において、IPフィルタは対象宛ての全ての トラフィックを遮断します。

Traffic Control（トラフィックコントロール）

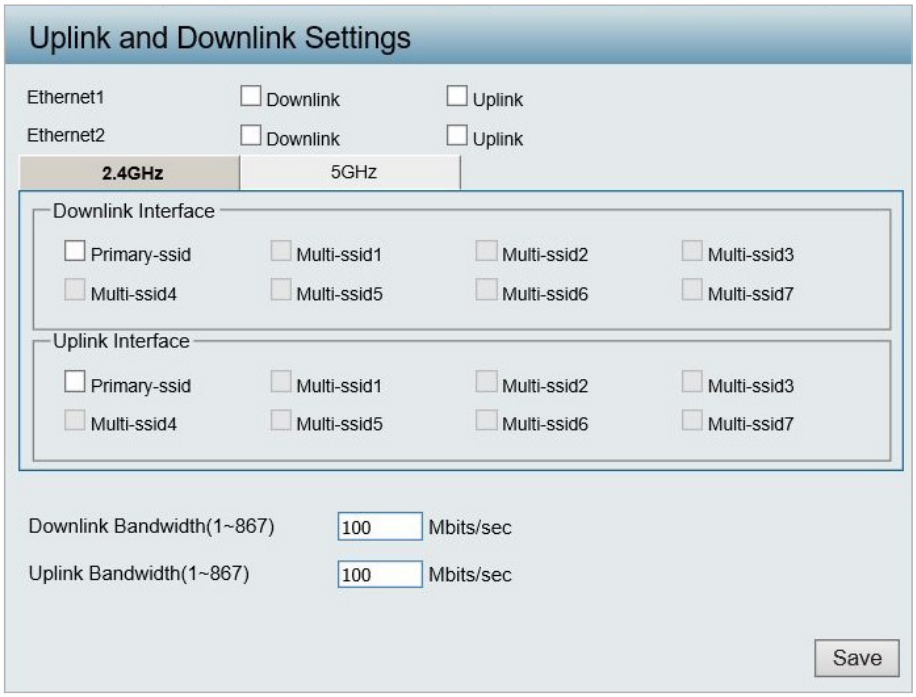
アップリンク/ダウンリンクの帯域幅設定、QoS設定などによりトラフィックをコントロールします。

■Uplink and Downlink Setting（アップリンク／ダウンリンク設定）

アップリンク/ダウンリンクの帯域幅を設定します。
本項目で設定した内容は、QoS及びTraffic Managerの設定内容にも反映されます。

1. [Advanced Settings] > [Traffic Control] > [Uplink/Downlink Settings] を選択します。

2. 以下の画面で設定を行います。



項目	説明
Ethernet 1/2	[Downlink] または [Uplink] を選択します。
2.4GHz / 5GHz	周波数帯を [2.4GHz] または [5GHz] から選択します。
Downlink Interface	ダウンリンクインタフェースを選択します。
Uplink Interface	アップリンクインタフェースを選択します。
Downlink Bandwidth (1-867)	ダウンリンクの帯域幅を入力します。 • 指定可能範囲：1-867（Mbps）
Uplink Bandwidth (1-867)	アップリンクの帯域幅を入力します。 • 指定可能範囲：1-867（Mbps）

3. [Save] をクリックして設定を保存します。

■QoS（QoS設定）

本項目ではQoSの設定を行います。

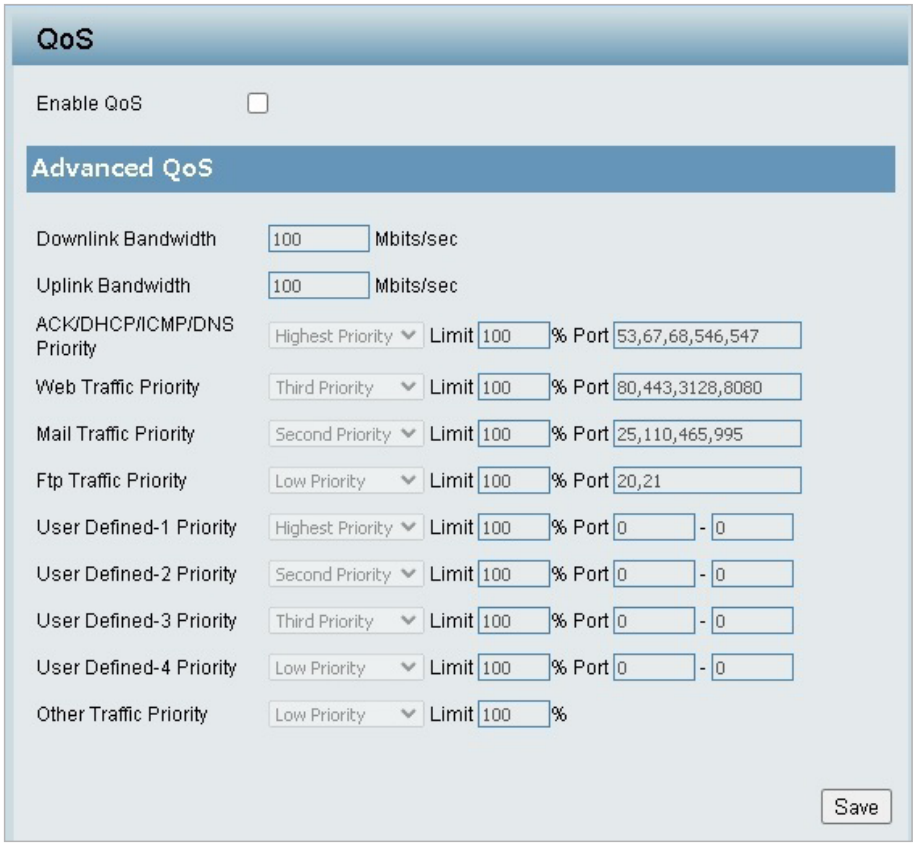
QoS (Quality of Service) とは、各アプリケーションのトラフィックに優先順位を付けることで、ネットワークの利用を効率化する機能です。優先度を高く設定されたトラフィックが優先的に処理されます。本製品は、4つのプライオリティレベルをサポートしています。

重要

QoS機能が有効化される場合、Bandwidth Optimization（帯域幅最適化）は無効となります。

1. [Advanced Settings] > [Traffic Control] > [QoS] を選択します。

2. 以下の画面で設定を行います。



項目	説明
Enable QoS	チェックを入れてQoSを有効にします。
Advanced QoS	QoSの詳細設定を行います。 • Downlink Bandwidth : [Uplink and Downlink Setting] で設定した帯域幅が表示されます。 →『Uplink and Downlink Setting（アップリンク／ダウンリンク設定）：p.86 』 • Uplink Bandwidth : [Uplink and Downlink Setting] で設定した帯域幅が表示されます。 →『Uplink and Downlink Setting（アップリンク／ダウンリンク設定）：p.86 』 • Priority : 各トラフィックの優先度を設定します。 - Highest Priority ：最も高い優先度です。 - Second Priority ：2番目に高い優先度です。 - Third Priority ：3番目に高い優先度です。 - Low Priority ：最も低い優先度です。 • Limit : [Downlink/Uplink Bandwidth] の設定値を元に、各トラフィックの最大帯域幅を設定します。 • Port : 対象ポートを指定します。

3. [Save] をクリックして設定を保存します。

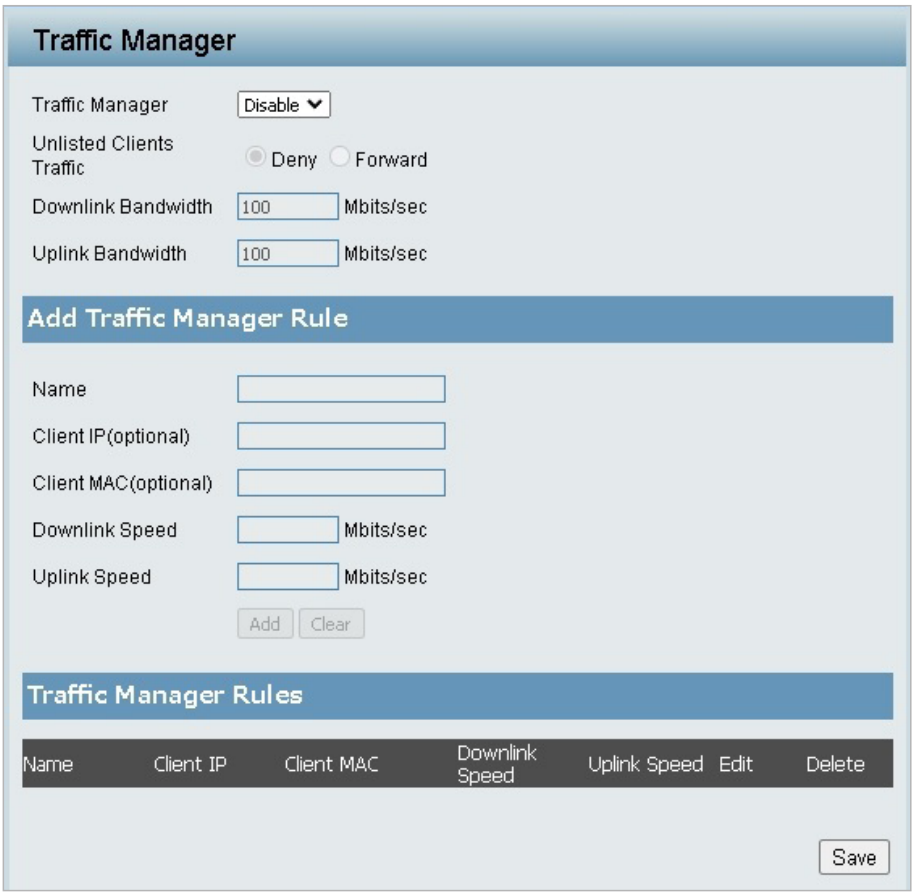
■Traffic Manager（トラフィックマネージャ）

トラフィックマネージャは、トラフィック管理ルールを作成し、クライアントのトラフィックとアップリンク／ダウンリンクのスピードを管理する機能です。

重要

QoS機能が有効化される場合、Bandwidth Optimization（帯域幅最適化）は無効となります。

1. [Advanced Settings] > [Traffic Control] > [Traffic Manager] を選択します。
2. 以下の画面で設定を行います。



項目	説明
Traffic Manager	トラフィックマネージャを有効または無効にします。 • 選択肢：[Enable]（有効）[Disable]（無効）
Unlisted Clients Traffic	リストに登録されていないクライアントのトラフィックに対する対応を選択します。 • 選択肢：[Deny]（拒否）[Forward]（転送）
Downlink Bandwidth	[Uplink and Downlink Setting] で設定した帯域幅が表示されます。 →『Uplink and Downlink Setting（アップリンク／ダウンリンク設定）：p.86 』
Uplink Bandwidth	[Uplink and Downlink Setting] で設定した帯域幅が表示されます。 →『Uplink and Downlink Setting（アップリンク／ダウンリンク設定）：p.86 』
Add Traffic Manager Rule	トラフィック管理ルールを作成します。 • Name：ルールの名前を入力します。 • Client IP (optional)：クライアントのIPアドレスを入力します。 • Client MAC (optional)：クライアントのMACアドレスを入力します • Downlink Speed：ダウンリンクの速度を入力します。（単位：Mbits/秒） • Uplink Speed：アップリンクの速度を入力します。（単位：Mbits/秒） • Add：設定した内容を追加します。 • Clear：入力した内容をクリアします。

項目	説明
Traffic Manager Rules	作成したトラフィック管理ルールが表示されます。

3. [Save] をクリックして設定を保存します。

◆ 設定を削除する場合：

1. [Delete] 欄の [Delete] をクリックします。
2. 確認メッセージが表示されるので、「OK」をクリックします。

◆ 設定した内容を編集する場合：

1. [Edit] 欄の [Edit] をクリックします。
2. 設定を編集します。
3. [Add] をクリックして設定を保存します。

Status（ステータス）

6

ファームウェアバージョンやクライアント情報、ログなど、アクセスポイントのステータスを確認できます。

■ Statusについて 90

■ Device Information（デバイス情報）..... 90

■ Client Information（クライアント情報）..... 92

■ WDS Information（WDS情報）..... 92

■ Statistics（統計情報）..... 93

Ethernet Traffic Statistics（イーサネットトラフィック統計情報）..... 93

WLAN Traffic Statistics（WLANトラフィック統計情報）..... 94

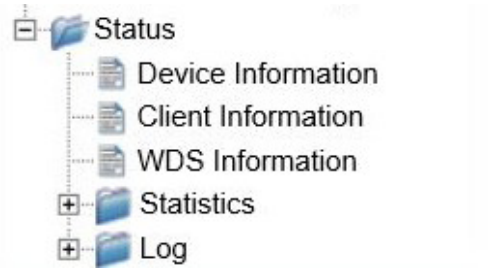
■ Log（ログ）..... 95

View Log（ログの表示）..... 95

Log Settings（ログ設定）..... 96

Statusについて

Status（ステータス）では、アクセスポイントのステータスを確認することができます。

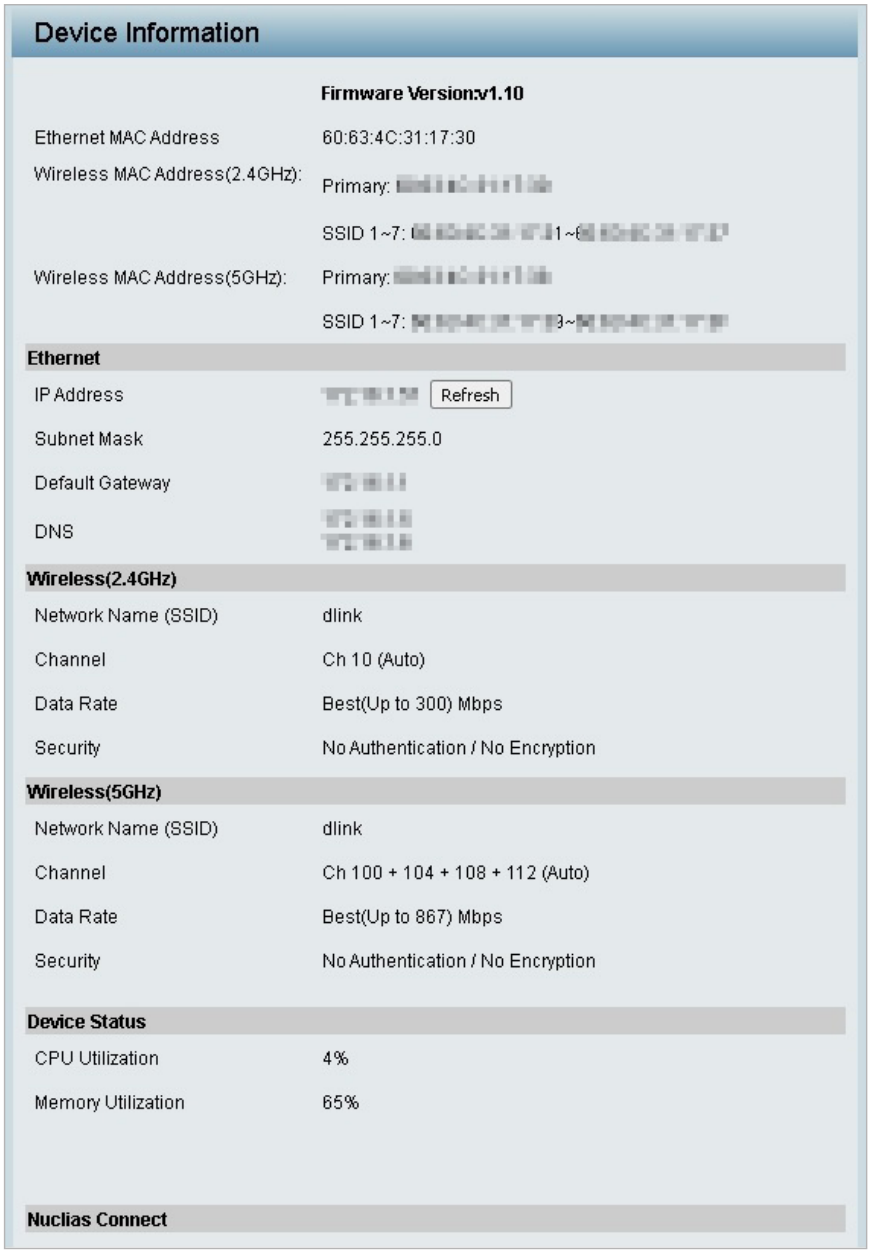


Device Information（デバイス情報）

本画面には、ファームウェアバージョン、IPアドレス、MAC アドレス、ワイヤレス設定などの情報と、CPUおよびメモリ使用率に関する情報が表示されます。

1. [Status] > [Device Information] を選択します。

2. 以下の画面で情報を確認します。



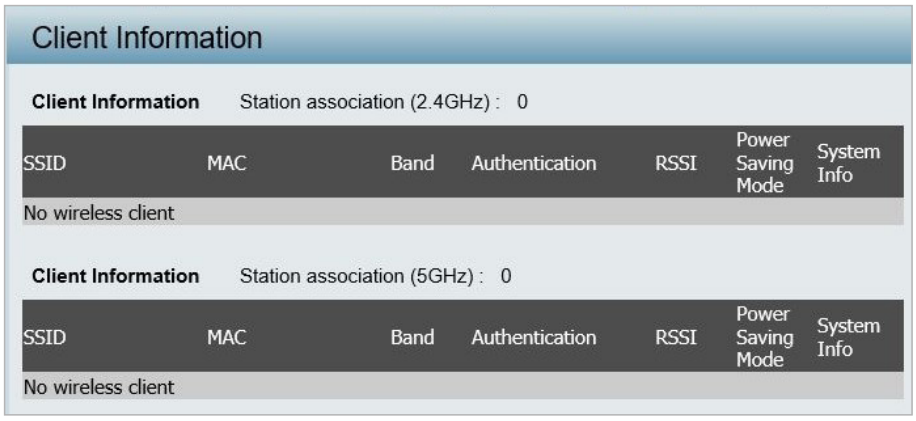
項目	説明
Ethernet MAC Address	イーサネットMACアドレスが表示されます。
Wireless MAC Address (2.4GHz)	2.4GHz無線MACアドレスが表示されます。
Wireless MAC Address (5GHz)	5GHz無線MACアドレスが表示されます。
Ethernet	
IP Address	割り当てられたIPアドレスが表示されます。
Subnet Mask	割り当てられたサブネットマスクが表示されます。
Default Gateway	割り当てられたゲートウェイが表示されます。
DNS	割り当てられたDNSが表示されます。
Wireless (2.4GHz)	
Network Name (SSID)	2.4GHzネットワークのSSIDが表示されます。
Channel	2.4GHzネットワークのチャネルが表示されます。
Data Rate	2.4GHzネットワークのデータレートが表示されます。
Security	2.4GHzネットワークのセキュリティが表示されます。
Wireless (5GHz)	
Network Name (SSID)	5GHzネットワークのSSIDが表示されます。
Channel	5GHzネットワークのチャネルが表示されます。
Data Rate	5GHzネットワークのデータレートが表示されます。
Security	5GHzネットワークのセキュリティが表示されます。
Device Status	
CPU Utilization	現在のCPU使用率が表示されます。
Memory Utilization	現在のメモリ使用率が表示されます。
Nuclias Connect	
Connection Status	現在の接続ステータスが表示されます。
Server IP	現在のサーバIPが表示されます。
Server Port	現在のポートが表示されます。

Client Information（クライアント情報）

本製品に接続しているクライアントの情報が、帯域ごとに表示されます。

1. [Status] > [Client Information] を選択します。

2. 以下の画面で情報を確認します。



項目	説明
SSID	クライアントのSSIDが表示されます。
MAC	クライアントのMACアドレスが表示されます。
Band	クライアントが接続している無線帯域が表示されます。
Authentication	使用している認証方式が表示されます。
RSSI	クライアントの受信信号強度（RSSI）が表示されます。
Power Saving Mode	省電力モードの状態が表示されます。
System Info	クライアントのシステム情報が表示されます。

WDS Information（WDS情報）

WDSネットワークの接続情報を表示します。

1. [Status] > [WDS Information] を選択します。

2. 以下の画面で情報を確認します。

項目	説明
Name	アクセスポイントのSSIDが表示されます。
MAC	アクセスポイントのMACアドレスが表示されます。
Authentication	ネットワークで使用している認証方式が表示されます。
Signal	アクセスポイントの信号強度が表示されます。
Status	アクセスポイントの状態が表示されます。

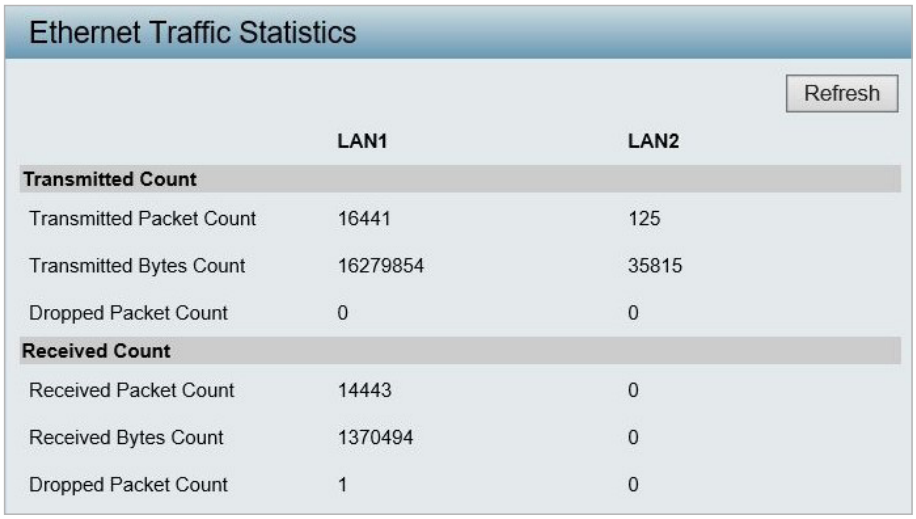
Statistics（統計情報）

■Ethernet Traffic Statistics （イーサネットトラフィック統計情報）

有線ネットワークで送受信されたパケットおよびバイトの統計情報を表示します。

1. [Status] > [Statistics] > [Ethernet] を選択します。

2. 以下の画面で情報を確認します。



Ethernet Traffic Statistics

Refresh

	LAN1	LAN2
Transmitted Count		
Transmitted Packet Count	16441	125
Transmitted Bytes Count	16279854	35815
Dropped Packet Count	0	0
Received Count		
Received Packet Count	14443	0
Received Bytes Count	1370494	0
Dropped Packet Count	1	0

項目	説明
Transmitted Count	
Transmitted Packet Count	送信パケット数が表示されます。
Transmitted Bytes Count	送信バイト数が表示されます。
Dropped Packet Count	破棄されたパケット数が表示されます。
Received Count	
Received Packet Count	受信パケット数が表示されます。
Received Bytes Count	受信バイト数が表示されます。
Dropped Packet Count	破棄されたパケット数が表示されます。

◆ 統計情報を更新する場合：

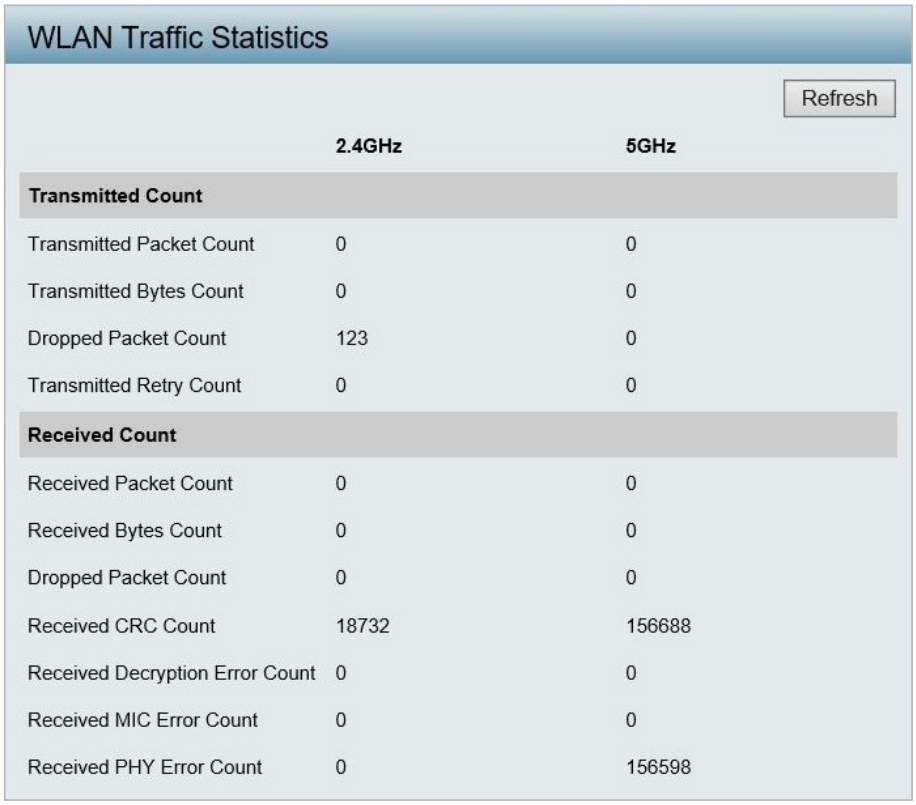
1. [Refresh] をクリックします。

■WLAN Traffic Statistics （WLANトラフィック統計情報）

無線ネットワークの送受信フレームおよびフレームエラーの統計情報を表示します。

1. [Status] > [Statistics] > [WLAN] を選択します。

2. 以下の画面で情報を確認します。



WLAN Traffic Statistics

Refresh

	2.4GHz	5GHz
Transmitted Count		
Transmitted Packet Count	0	0
Transmitted Bytes Count	0	0
Dropped Packet Count	123	0
Transmitted Retry Count	0	0
Received Count		
Received Packet Count	0	0
Received Bytes Count	0	0
Dropped Packet Count	0	0
Received CRC Count	18732	156688
Received Decryption Error Count	0	0
Received MIC Error Count	0	0
Received PHY Error Count	0	156598

項目	説明
Transmitted Count	
Transmitted Packet Count	送信パケット数が表示されます。
Transmitted Bytes Count	送信バイト数が表示されます。
Dropped Packet Count	破棄されたパケット数が表示されます。
Transmitted Retry Count	送信リトライ回数が表示されます。
Received Count	
Received Packet Count	受信パケット数が表示されます。
Received Bytes Count	受信バイト数が表示されます。
Dropped Packet Count	破棄されたパケット数が表示されます。
Received CRC Count	受信したCRC数が表示されます。
Received Decryption Error Count	受信した復号エラー数が表示されます。
Received MIC Error Count	受信したMICエラー数が表示されます。
Received PHY Error Count	受信したPHYエラー数が表示されます。

◆ 統計情報を更新する場合：

1. [Refresh] をクリックします。

Log（ログ）

■View Log（ログの表示）

アクセスポイントの動作や無線LANクライアントとの接続記録などのログを表示します。

重要

保存できるログの数は500個までです。

1. [Status] > [Log] > [View Log] を選択します。

2. 以下の画面で情報を確認します。

Date and Time	Message
Oct 20 09:51:59	Association Success, STA (MAC=[illegible]), APMAC=[illegible], Network=
Oct 20 09:51:59	5GHz, Received associate, STA (MAC=[illegible]), APMAC=[illegible], Network=
Oct 20 09:44:04	Web login success from IP=172.16.1.50 with HTTP
Oct 20 09:43:52	DHCP, Client (MAC=[illegible]) gets IP=[illegible]
Oct 20 09:43:50	DHCP, Client (MAC=[illegible]) receives ACK from server, IP=1[illegible], Lease time=259200
Oct 20 09:43:50	DHCP, Client (MAC=[illegible]) performs a DHCP renew
Oct 20 09:43:50	Ethernet eth1 LINK UP
Oct 20 09:43:48	DHCP, Client (MAC=[illegible]) gets IP=[illegible]
Oct 20 09:43:48	DHCP, Client (MAC=[illegible]) receives ACK from server, IP=1[illegible], Lease time=259200
Oct 20 09:43:46	DHCP, Client (MAC=[illegible]) performs a DHCP renew
Oct 20 09:43:44	Ethernet eth1 LINK DOWN
Oct 20 09:43:44	Web login failure from IP=[illegible] with HTTP
Oct 20 09:43:43	5GHz, Initiate wireless successfully
Oct 20 09:43:35	2.4GHz, Initiate wireless successfully
Oct 20 09:43:25	DHCP, Client (MAC=[illegible]) gets IP=[illegible]
Oct 20 09:43:23	DHCP, Client (MAC=[illegible]) receives ACK from server, IP=1[illegible], Lease time=259200
Oct 20 09:43:23	DHCP, Client (MAC=[illegible]) sends REQUEST, Request IP=[illegible] from server
Oct 20 09:43:23	DHCP, Client (MAC=[illegible]) receives OFFER from server
Oct 20 09:43:23	DHCP, Client (MAC=[illegible]) sends DISCOVER
Oct 20 09:43:23	Ethernet eth0 LINK DOWN

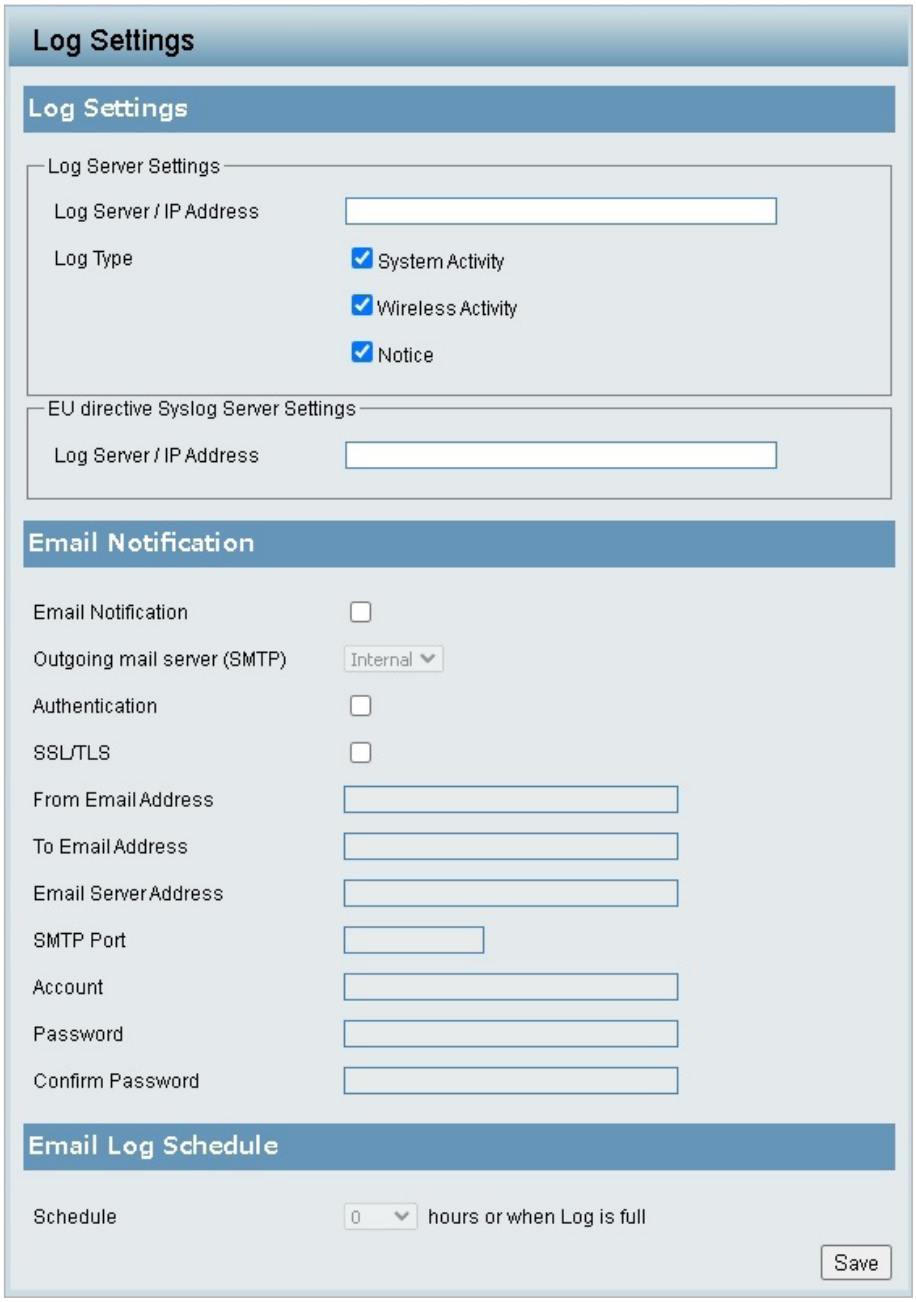
項目	説明
First Page **Last Page**	最初のページ／最後のページを表示します。
Previous **Next**	前のページ／次のページを表示します。
Clear	ログを削除します。

■Log Settings （ログ設定）

ログ取得に関する設定を行います。

1. [Status] > [Log] > [Log Settings] を選択します。

2. 以下の画面で設定を行います。



項目	説明
Log Server Settings	ログを送信するサーバと送信するログのタイプを設定します。 • Log Server / IP Address : ログサーバのIP アドレスを入力します。 • Log Type: 送信するログのタイプを選択します。 - [System Activity] : 本アクセスポイントのアクティビティに関するログを取得します。 - [Wireless Activity] : 無線LAN クライアントの接続情報などのログを取得します。 - [Notice] : その他の情報のログを取得します。
EU directive Syslog Server Settings	日本では使用しません。

項目	説明
Email Notification	ログのE-Mail通知を設定します。 • Email Notification : チェックを入れるとE-Mail通知が有効になります。 • Outgoing mail server (SMTP) : 送信用のSMTP サーバを以下から選択します。 - [Internal] [Gmail] [Hotmail] • Authentication : チェックを入れると認証が有効になります。 • SSL/TLS : チェックを入れるとSSL/TLS 認証が有効になります。 • From Email Address : E-mail/SMTP 送信元のE-mail アドレスを入力します。 • To Email Address : E-mail/SMTP 送信先のE-mail アドレスを入力します。 • Email Server Address : E-mail/SMTP サーバのIP アドレスを入力します。 • SMTP Port : SMTP ポートの番号を入力します。 • Account : SMTP サーバのユーザ名を入力します。 • Password : SMTP サーバのパスワードを入力します。 • Confirm Password : 確認のためにSMTP サーバのパスワードを再度入力します。
Email Log Schedule	ログのE-Mail通知を行う間隔を設定します。(単位:時間) ログが上限に達した場合にも通知します。

3. [Save] をクリックして設定を保存します。

重要

- Cold StartのSyslog Trapは非対応です。
- SyslogのFacility、Levelは変更できません。

管理メニュー

7

ファームウェアアップデートや設定のリセットなど、本製品の管理を行う方法を説明します。

■ 管理メニューについて 99

■ Home (ホーム画面) 99

■ Maintenance（メンテナンス） 100

Administration Settings（管理設定） 100

Firmware and SSL Certification Upload（ファームウェアとSSL証明書のアップロード） 104

Configuration File Upload and Download
（コンフィグレーションファイルのアップロードとダウンロード） 106

Time and Date Settings（時刻と日付の設定） 107

■ Configuration（コンフィグレーション） 109

設定の保存と有効化 109

設定の破棄 109

■ System（システム設定） 110

本製品の再起動 110

工場出荷時設定へのリセット 110

Language Packの削除 111

■ Logout（ログアウト） 112

■ Help（ヘルプ） 112

管理メニューについて

ファームウェアアップデートや設定の保存、リセットなどを行うことができます。
管理メニューには以下の項目があります。

● Home
System Information(システム情報)画面を表示します。
『Home (ホーム画面)：p.100 』

● Maintenance
管理者設定やファームウェアアップグレードなど、本製品のメンテナンスを行います。
『Maintenance（メンテナンス）：p.101 』

● Configuration
設定の保存・有効化と、設定変更の取り消しを行います。
『Configuration（コンフィグレーション）：p.110 』

● System
本製品の再起動と、工場場出荷時状態へのリセットを行います。
『System （システム設定）：p.111 』

● Logout
WebGUI画面からログアウトします。
『Logout（ログアウト）：p.113 』

● Help
ヘルプ画面を表示します。
『Help（ヘルプ）：p.113 』

Home（ホーム画面）

System Information（システム情報）画面を表示します。

1. [Home] アイコンをクリックします。

2. 以下の画面で情報を確認します。

System Information

Model Name	DAP-3666
Firmware Version	v1.10 10:40:28 2022/10/07
System Name	dap3666
Location	
System Time	2022/10/17 14:57:57
Up Time	00:01:16
Operation Mode (2.4GHz)	Access Point
Operation Mode (5GHz)	Access Point
MAC Address (2.4GHz)	[illegible]
MAC Address (5GHz)	[illegible]
IP Address	[illegible]

Maintenance（メンテナンス）

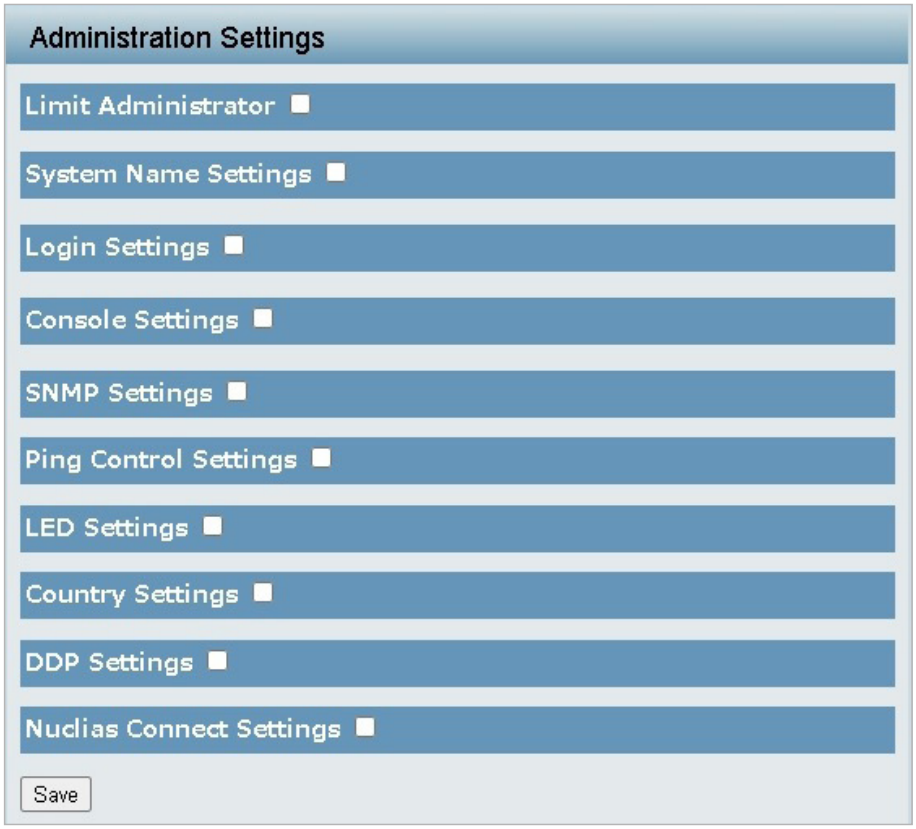
■Administration Settings （管理設定）

ログイン設定やコンソール設定など、管理設定を行います。
管理設定には以下の項目があります。

- Limit Administrator (管理者の制限)
  →『Limit Administrator：p.102 』を参照
- System Name Settings（システム名設定）
  →『System Name Settings：p.102 』を参照
- Login Settings（ログイン設定）
  →『Login Settings：p.102 』を参照
- Console Settings（コンソール設定）
  →『Console Settings：p.103 』を参照
- SNMP Settings（SNMP設定）
  →『SNMP Settings：p.103 』を参照
- Ping Control Settings（Pingコントロール設定）
  →『Ping Control Settings：p.104 』を参照
- LED Settings（LED設定）
  →『LED Settings：p.104 』を参照
- Country Settings（国設定）
  →『Country Settings：p.104 』を参照
- DDP Settings（DDP設定）
  →『DDP Setting：p.104 』を参照
- Nuclias Connect Setting（Nuclias Connect設定）
  →『Nuclias Connect Settings：p.104 』を参照

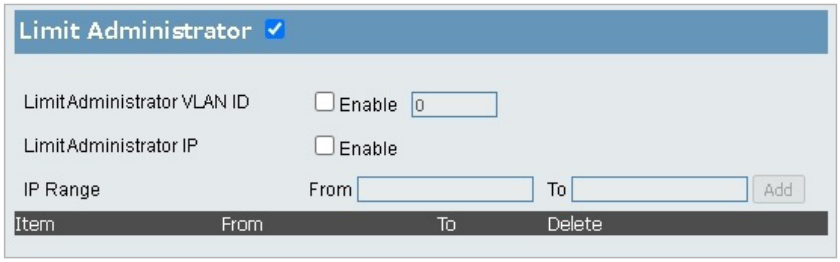
1. [Maintenance] アイコンをクリック → [Administration Settings] を選択します。

2. 以下の画面で項目を選択し、設定を行います。



● Limit Administrator

管理者の制限を行います。



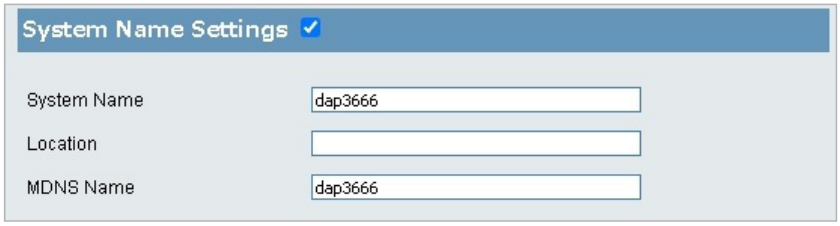
項目	説明
Limit Administrator VLAN ID	[Enable] をチェックし、管理者がログインを許可されるVLAN IDを入力します。
Limit Administrator IP	[Enable] をチェックし、管理者がログインを許可されるIPアドレスを入力します。
IP Range	[Limit Administrator IP] を有効にした場合、管理者がログインを許可されるIPアドレス範囲を入力します。
Add	設定したIPアドレス範囲を追加します。

◆ IP アドレス範囲を削除する場合：

1. [Delete] 欄の [Delete] をクリックします。

● System Name Settings

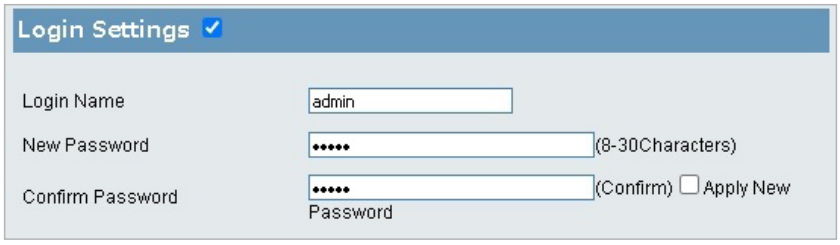
システム名を設定します。



項目	説明
System Name	本製品のシステム名を入力します。 ・初期値：dap3666
Location	本製品の設置場所を入力します。
MDNS Name	マルチキャストDNS名を入力します。 ・初期値：dap3666

● Login Settings

Web GUIにログインするためのログイン名とパスワードを設定します。



項目	説明
Login Name	ログイン名を入力します。 ・初期値：admin
New Password	新しいパスワードを入力します。 ・初期値：空欄

項目	説明
Confirm Password	確認のため、新しいパスワードを再度入力します。
Apply New Password	チェックをいれると新しいパスワードが有効になります。

重要

パスワードは大文字と小文字が区別されます。8～30文字で入力する必要があります。

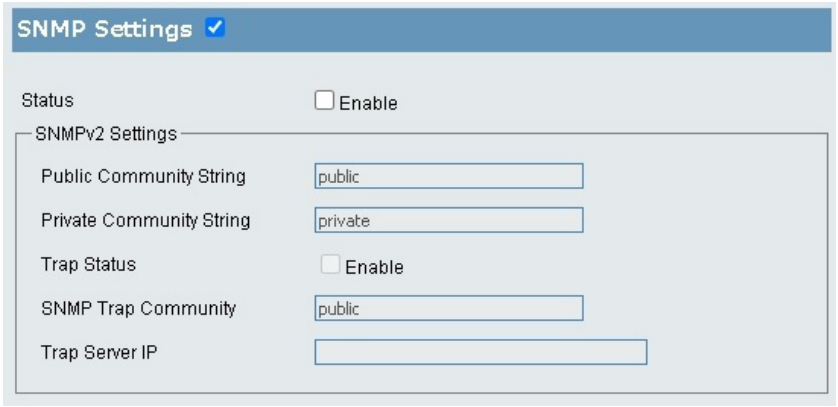
● Console Settings

コンソールセッションに関する設定を行います。

項目	説明
Status	[Enable] をチェックし、コンソール接続を有効にします。
Console Protocol	コンソール接続で使用するプロトコルを選択します。 ・初期値：TELNET ・選択肢：[TELNET][SSH]
Login Timeout	タイムアウトの設定を選択します。 ・選択肢：[1 Min][3 Mins][5 Mins][10 Mins][15 Mins][Never]

● SNMP Settings

SNMPの設定を行います。



項目	説明
Status	[Enable] をチェックし、SNMPを有効にします。
Public Community String	パブリックSNMP コミュニティ名を入力します。 ・初期値：public
Private Community String	プライベートSNMP コミュニティ名を入力します。 ・初期値：private
Trap Status	[Enable] をチェックし、トラップを有効にします。
SNMP Trap Community	SNMPトラップコミュニティ名を入力します。
Trap Server IP	トラップサーバのIP アドレスを入力します。

メモ

- STAのAssociation/Disassociation/Deauthentication、WebUI Loginに関するトラップは送信されません。
- SNMP Community Nameは5文字以上で入力する必要があります。
- 一部のMIBのみのサポートであるため、限定的な管理のみの対応となります。

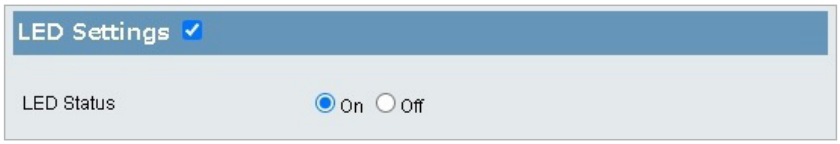
● Ping Control Settings

Pingを有効または無効にします。

項目	説明
Status	[Enable] をチェックし、Pingを有効にします。

● LED Settings

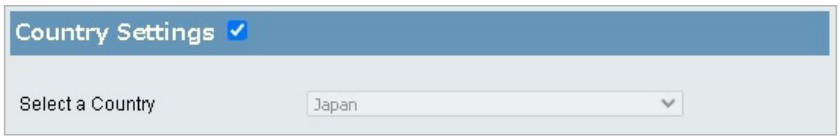
LEDの設定を行います。



項目	説明
LED Status	LEDの設定をします。 ・選択肢：[On] [Off] ・初期値：On

● Country Settings

国の設定を行います。



項目	説明
Select a Country	選択している国が表示されます。

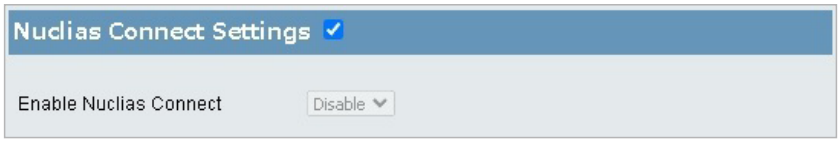
● DDP Setting

DDP設定を有効または無効にします。

項目	説明
Status	[Enable] をチェックし、DDP設定を有効にします。

● Nuclias Connect Settings

Nuclias Connectを利用すると、ネットワーク上のAPをまとめて管理することができます。



項目	説明
Enable Nuclias Connect	Nuclias Connectを有効または無効にします。 ・選択肢：[Enable]（有効）[Disable]（無効） ・初期値：[Disable]

※ Nuclias Connect の使用方法については、Nuclias Connect のマニュアルをご確認ください。

メモ

- スタンドアロンモードにおいて、「Nuclias Connect Setting」項目を有効化することはできません。Nuclias Connectのプロファイルが適用されると、本項目が有効（管理モード）になります。
- Nuclias Connectによる管理モードになると、ローカルWeb UIの表示項目は制限されます。

3. [Save] をクリックして設定を保存します。

■Firmware and SSL Certification Upload（ファームウェアとSSL証明書のアップロード）

ファームウェア、Language Pack、SSL証明書のアップロードを行います。

● ファームウェアのアップロード

1. [Maintenance] アイコンをクリック→ [Firmware and SSL Certification Upload] を選択します。

2. 以下の画面で [参照 / ファイルを選択] をクリックしてローカルに保存したファームウェアを指定します。

3. [Update] をクリックします。

⚠注意

アップロード中に電源を切らないでください。
アップデート中に電源を切ると、起動に失敗し、正常に起動できなくなることがあります。故障の原因となりますので、ご注意ください。

重要

「Online Check Firmware」の「Check」をクリックすると、ファームウェアステータスを確認できます。サポートされるファームウェアは弊社ホームページで公開される情報をご確認ください。

● Language Packのアップロード

1. [Maintenance] アイコンをクリック→ [Firmware and SSL Certification Upload] を選択します。

2. 以下の画面で [参照 / ファイルを選択] をクリックし、Language Pack ファイルを選択します。

3. [Update] をクリックします。

● SSL証明書のアップロード

1. [Maintenance] アイコンをクリック→ [Firmware and SSL Certification Upload] を選択します。

2. 以下の画面で [参照 / ファイルを選択] をクリックし、ファイルを選択します。

項目	説明
Upload Certificate From File	更新する証明書を指定します。
Upload Key From File	更新する認証キーを指定します。

3. [Update] をクリックします。

■Configuration File Upload and Download（コンフィグレーションファイルのアップロードとダウンロード）

コンフィグレーションファイルのアップロードとダウンロードを行います。アクセスポイントの設定をバックアップまたはリカバリすることができます。

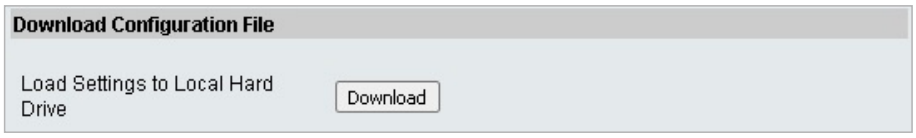
● コンフィグレーションのアップロード

1. [Maintenance] アイコンをクリック→ [Configuration File] を選択します。
2. 以下の画面で [参照 / ファイルを選択] をクリックしてファイルを選択 します。

3. [Upload] をクリックします。

● コンフィグレーションのダウンロード

1. [Maintenance] アイコンをクリック→ [Configuration File] を選択します。
2. 以下の画面で [Download] をクリックし、ファイルをダウンロードします。



● Nuclias Connectプロファイルのアップロード

Nuclias Connectでエクスポートしたプロファイルをアップロードすることで、アクセスポイントをNuclias Connectの管理対象として追加することができます。

1. [Maintenance] アイコンをクリック→ [Configuration File] を選択します。
2. 以下の画面で [参照 / ファイルを選択] をクリックしてファイルを選択 します。

3. [Upload] をクリックします。

メモ

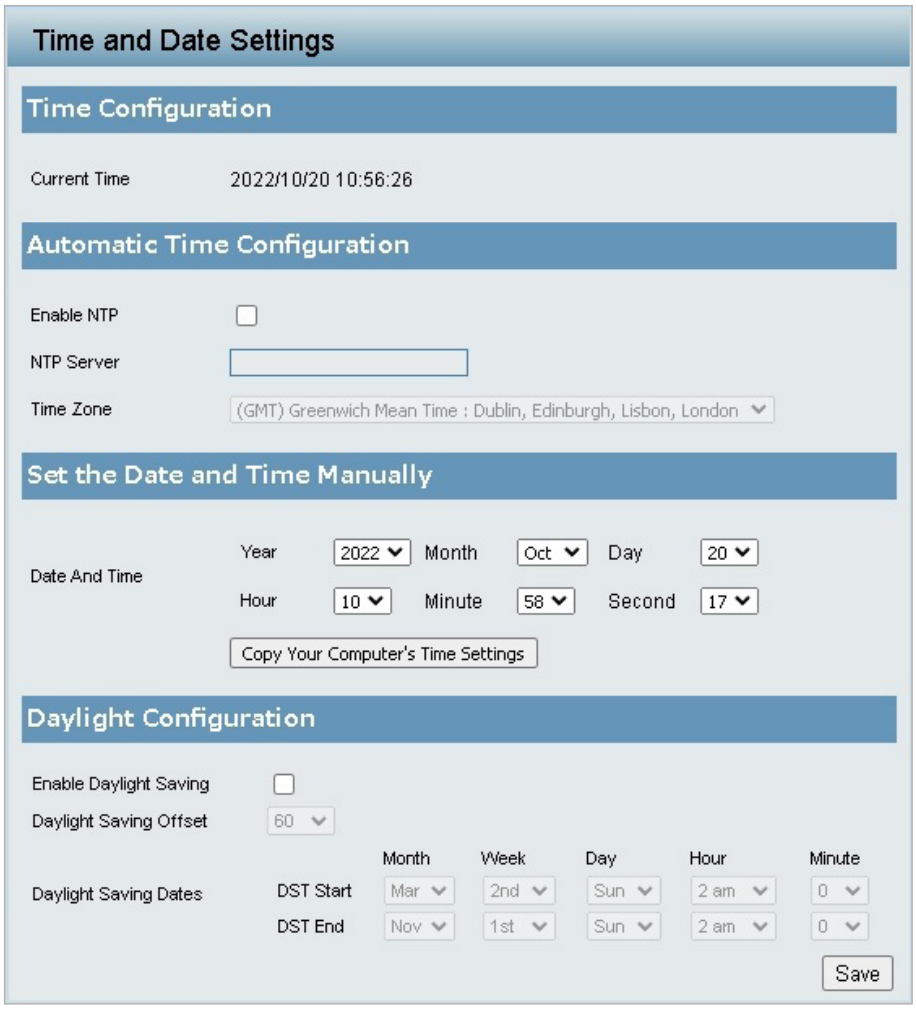
Nuclias Connectによる管理モードになると、ローカルWeb UIの表示項目は制限されます。

■Time and Date Settings（時刻と日付の設定）

本製品の時刻の設定を行います。
NTPサーバを使用して自動的に日時を設定、または手動で日時を設定することができます。

1. [Maintenance] アイコンをクリック→ [Time and Date] を選択します。

2. 以下の画面で設定を行います。



項目	説明
Time Configuration	[Current Time] に現在設定されている日時が表示されます。
Automatic Time Configuration	NTPサーバを使用して自動的に日時を設定します。 • Enable NTP : チェックを入れるとNTPサーバが有効になります。 • NTP Server : NTPサーバのIPアドレスを入力します。 • Time Zone : タイムゾーンを設定します。
Set the Date and Time Manually	日付と時刻を手動で設定します。 • Date And Time : 日付と時刻を指定します。 • Copy Your Computer's Time Settings : クリックすると、お使いのPCの日時をコピーできます。

項目	説明
Daylight Configuration	サマータイムを設定します。 • Enable Daylight Saving : チェックを入れ、Daylight Savings Time（DST/サマータイム）を有効化します。 • Daylight Saving Offset : Daylight Savings Time（サマータイム）のオフセット時間（単位：分）を設定します。 • Daylight Saving Dates : - DST Start : Daylight Savings Time（サマータイム）の開始日時を設定します。 - DST End : Daylight Savings Time（サマータイム）の終了日時を設定します。

3. [Save] をクリックして設定を保存します。

Configuration（コンフィグレーション）

■設定の保存と有効化

設定した内容を保存・有効化します。

1. [Configuration] アイコンをクリック→ [Save and Activate] を選択します。
2. 以下の画面が表示され、設定の保存と有効化が行われます。

⚠注意

再起動中は、電源を切らずにそのままお待ちください。

重要

本作業を行わない場合、各セクションで保存した設定は次のシステム再起動時に破棄されます。

■設定の破棄

設定した内容を破棄します。

1. [Configuration] アイコンをクリック→ [Discard Changes] を選択します。
2. 以下の画面が表示され、設定の破棄が行われます。

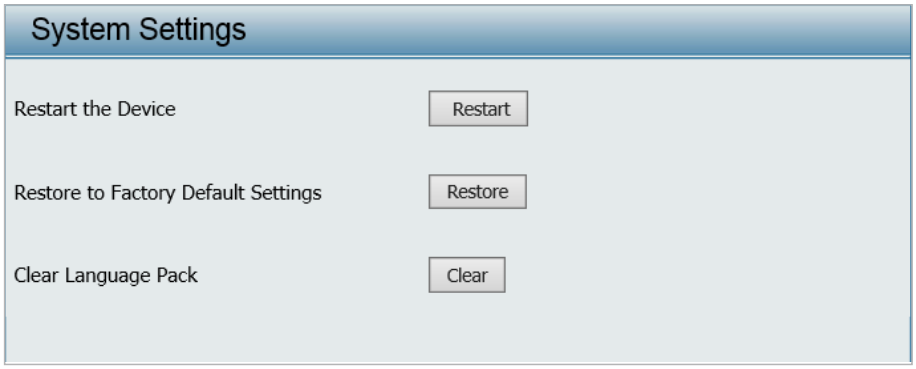
⚠注意

再起動中は、電源を切らずにそのままお待ちください。

System （システム設定）

■本製品の再起動

1. [System] アイコンをクリックします。
2. [Restart] をクリックします。



3. 確認画面が表示されるので、[OK] をクリックします。
4. 以下の画面が表示され、再起動が行われます。

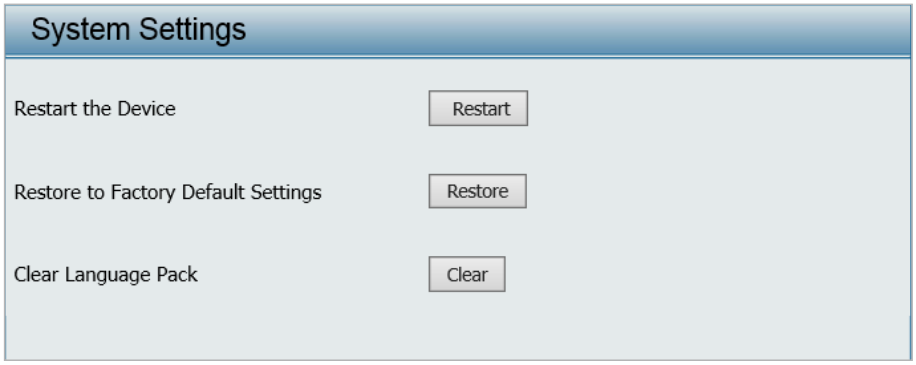
⚠注意

再起動中は、電源を切らずにそのままお待ちください。

■工場出荷時設定へのリセット

工場出荷時の状態へ設定をリセットします。

1. [System] アイコンをクリックします。
2. [Restore] をクリックします。



3. 確認画面が表示されるので、[OK] をクリックします。

4. 以下の画面が表示され、再起動が行われます。

⚠注意

再起動中は、電源を切らずにそのままお待ちください。

メモ

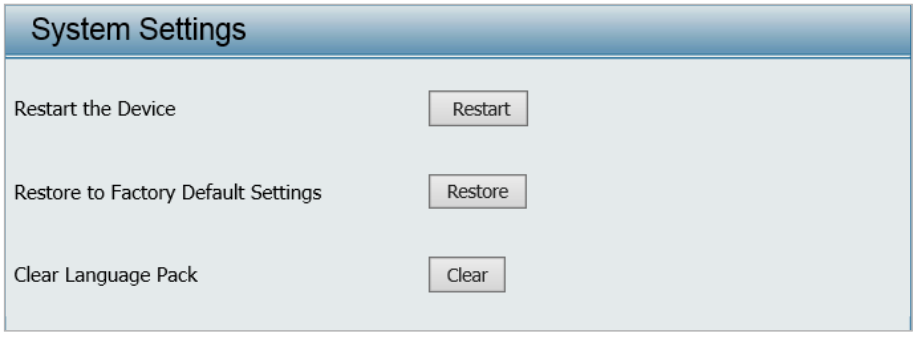
工場出荷時状態へのリセットは、本体のリセットボタンを押して行うこともできます。

■Language Packの削除

現在適用されているLanguage Packを削除します。

1. [System] アイコンをクリックします。

2. [Clear] をクリックします。

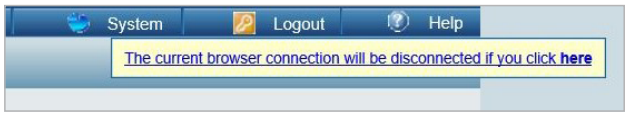


3. 確認画面が表示されるので、[OK] をクリックします。

Logout（ログアウト）

Web GUI画面からのログアウトを行います。

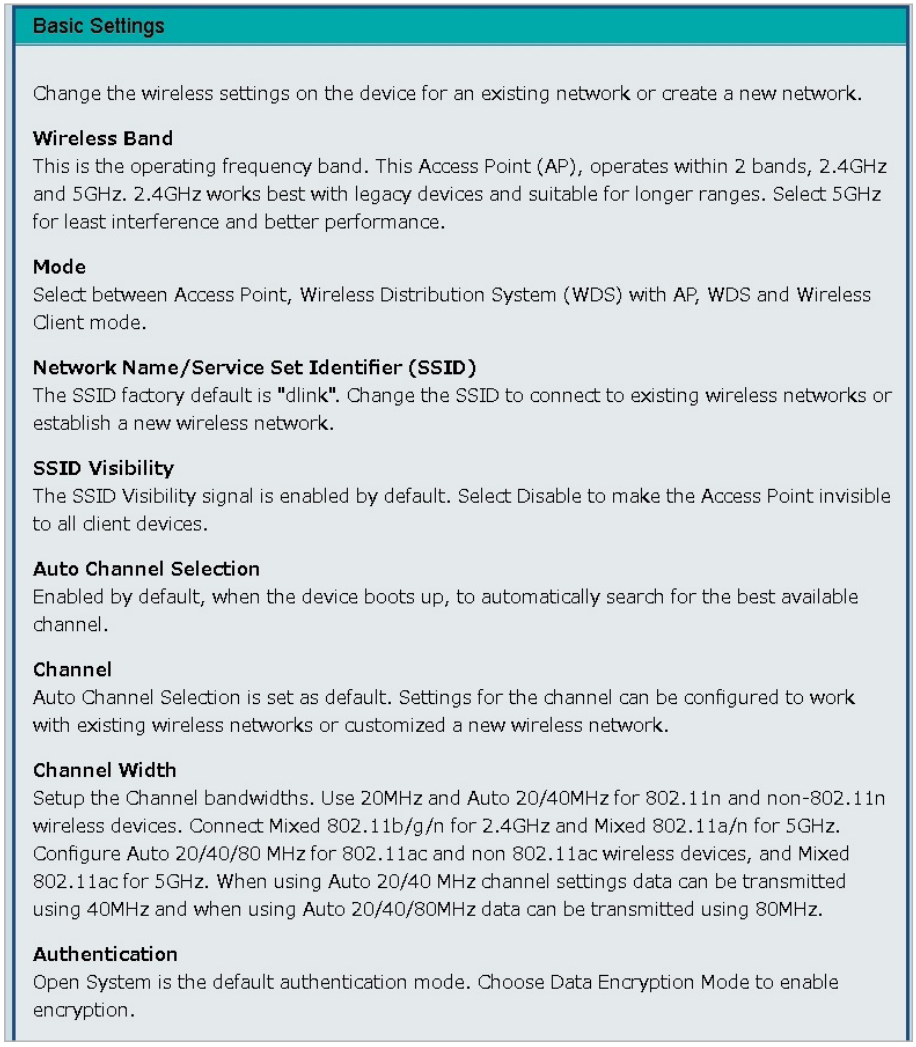
1. [Logout] アイコンをクリックします。
2. 以下のメッセージをクリックします。



Help（ヘルプ）

ヘルプ画面を表示します。

1. [Help] アイコンをクリックします。
2. 以下の画面でヘルプ情報を確認します。



付録

8

■ 工場出荷時設定に戻す 114
リセットボタンで設定リセット行う 114
Web GUIから設定リセットを行う 114
■ FAQ 115
■ 機能設定例 118
対象機器について 118
VLAN 118

工場出荷時設定に戻す

本製品の設定を工場出荷時の状態に戻す方法について説明します。

重要

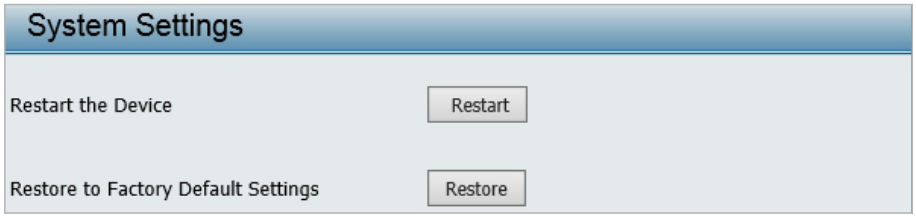
- 設定のリセットを行う前に、必要に応じて設定をバックアップしてください。
- リセット後のIPアドレスは「192.168.0.50」になります。

■リセットボタンで設定リセット行う

1. 本体の電源を入れた状態で、本体 LAN2 ポート横のリセットボタンを 10 秒以上押します。
2. ボタンを離すと、本体が再起動します。そのままお待ちください。

■Web GUIから設定リセットを行う

1. [System] アイコンをクリックします。
2. [Restore] をクリックします。



3. 確認画面が表示されるので、[OK] をクリックします。
4. 以下の画面が表示され、再起動が行われます。

⚠注意

電源を切らずにそのままお待ちください。

FAQ

よくお問い合わせいただく内容について記載しています。

メモ

・本製品の設定にはイーサネット接続を使用することをお勧めします。

Q 本製品の設定を行うコンピュータからWebベースの設定メニューにアクセスできません。

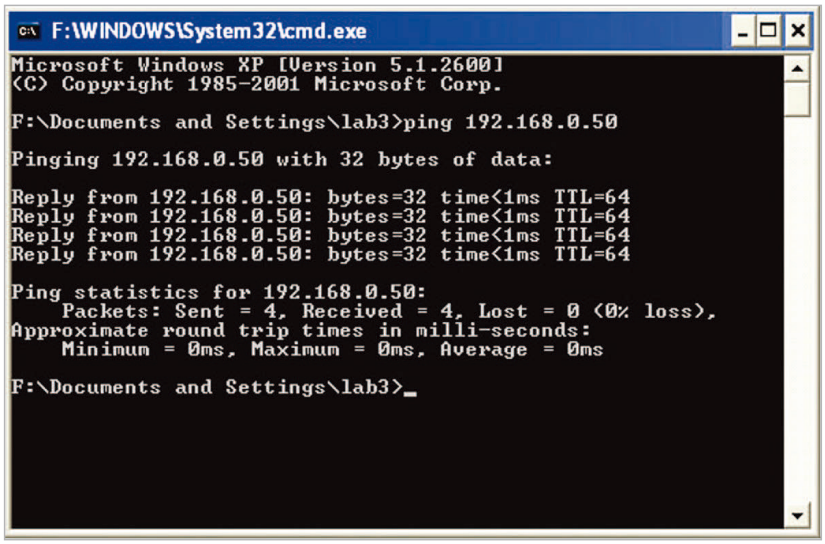
A ①本製品底面にあるPower LEDが点灯していることを確認してください。
LEDが点灯していない場合は、UTPケーブルが正しくポートに接続されているか確認してください。

メモ

本製品は初期値で「DHCP クライアント」として設定されています。有効なDHCP サーバからIP アドレスを割り振られる環境にある場合はホスト名を、DHCP サーバが無効な環境の場合はIPアドレスを使用してください。
工場出荷時の設定は以下の通りです。
・ホスト名 - http://dap3666.local
・IPアドレス - http://192.168.0.50

②本製品が応答していることを確認するには、Pingテストを実行します。

1. Windows で「スタート」＞「ファイル名を指定して実行」と選択し、「cmd」と入力して、Enter キーを押します。
2. DOS プロンプトで、ping 192.168.0.50 と入力します。
3. ping が成功すると、4 つの応答が表示されます。



メモ

・デフォルトのIPアドレスを変更した場合は、システムに割り当てられている正しいIPアドレスにpingを実行してください。

Q 無線クライアントがインフラストラクチャモード内でインターネットにアクセスできません。

A ①無線クライアントが正しいアクセスポイントに関連付けられ、参加していることを確認します。

1. タスクバーのローカルエリア接続アイコンをクリックし、利用可能なワイヤレスネットワークを表示します。
2. 使用可能な正しいネットワークが選択されていることを確認してください。

②無線アダプタに割り当てられたIPアドレスが、アクセスポイントおよびゲートウェイと同じIPアドレス範囲内にあることを確認してください。

- 本製品のIPアドレスは192.168.0.50（初期値）であるため、無線アダプタには同じ範囲のIPアドレス（192.168.0.xなど）が必要です。
- 各デバイスには一意のIPアドレスが必要です。
- サブネットマスクは、ネットワーク上のすべてのコンピュータで同じである必要があります。
- 無線アダプタに割り当てられたIPアドレスを確認するには、タスクバーのローカルエリア接続アイコンをクリックし、接続しているSSIDの「プロパティ」を選択すると、IPアドレスが表示されます。

③必要に応じて、無線アダプタに固定のIPアドレスを割り当てます。DNSサーバアドレスを入力する場合は、デフォルトゲートウェイアドレスも入力する必要があります。DHCP対応ルータがある場合は、固定IPアドレスを割り当てる必要はありません。

Q どのような要因によりワイヤレス製品の受信状態が悪くなる可能性がありますか。

A D-Link製品を使用すると、基本的にはどこからでもネットワークにアクセスできますが、使用環境における製品の配置はワイヤレス範囲に影響します。

Q ワイヤレス接続が途切れるのはなぜですか。

A ①2.4GHz帯デジタルコードレス電話、X10モジュールなどを使用したホームセキュリティシステム、シーリングファン/ライト、その他の無線製品電波などとの干渉により、通信品質が激しく低下して通信ができなくなる場合があります。干渉を避けるために、ルータ、アクセスポイント、およびワイヤレスアダプタのチャネルを別のチャネルに変更してみてください。

②本製品は、電子レンジやモニタ、電気モータなどのRFノイズを発生する電気機器から90~180cm以上離れた場所に設置してください。

Q ワイヤレス接続ができません。

A ①本製品で暗号化を有効にしている場合は、ワイヤレス接続を確立するために、すべてのワイヤレスクライアントでも暗号化を有効にする必要があります。

②アクセスポイントと無線クライアントのマルチSSIDが同じであることを確認してください。同じでない場合、ワイヤレス接続を確立できません。

③本製品と無線クライアントを同じ部屋に移動し、ワイヤレス接続をテストします。

④すべてのセキュリティ設定を無効にします。

⑤DAP-3666とクライアントの電源を切ります。DAP-3666の電源を入れ直してから、クライアントの電源を入れてください。

⑥すべてのデバイスがインフラストラクチャモードに設定されていることを確認してください。

⑦LED表示が正常な動作を示していることを確認します。そうでない場合は、AC電源ケーブルとイーサネットケーブルがしっかりと接続されていることを確認します。

⑧ネットワークのIPアドレス、サブネットマスク、ゲートウェイ、DNS設定が正しく入力されていることを確認します。

⑨2.4GHz帯デジタルコードレス電話、X10モジュールなどを使用したホームセキュリティシステム、シーリングファン/ライト、その他の無線製品電波などとの干渉により、通信品質が激しく低下して通信ができなくなる場合があります。干渉を避けるために、ルータ、アクセスポイント、およびワイヤレスアダプタのチャネルを別のチャネルに変更してみてください。

⑩本製品は、電子レンジやモニタ、電気モータなどのRFノイズを発生する電気機器から90~180cm以上離れた場所に設置してください。

Q パスワードを忘れた場合はどうすればよいでしょうか。

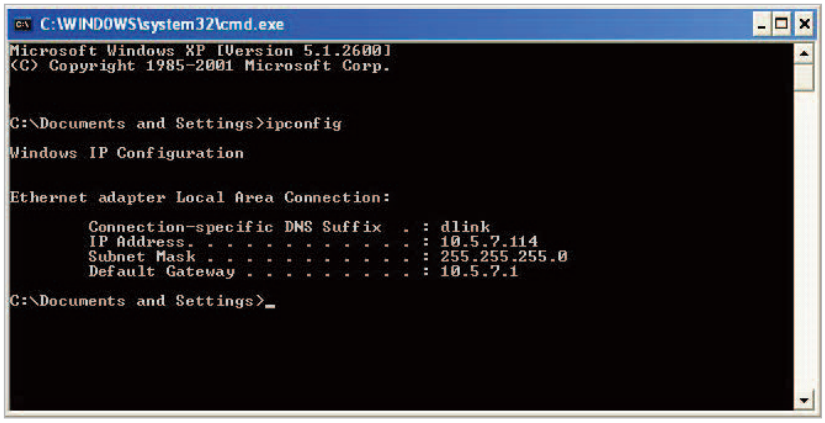
A 設定のリセットを行ってください。→『工場出荷時設定に戻す：p.115 』

Q IPアドレスを確認する方法は?

A ネットワークアダプタのインストール後、デフォルトでは、TCP/IP設定はDHCPサーバ（ワイヤレスルータ）からIPアドレスを自動的に取得するように設定されています。IPアドレスを確認するには、以下の手順に従ってください。

1. indows で「スタート」>「ファイル名を指定して実行」と選択し、「cmd」と入力して、Enter キーを押します。
2. DOS プロンプトで、「ipconfig」と入力し、Enter キーを押します。
3. アダプタの IP アドレス、サブネットマスク、およびデフォルトゲートウェイが表示されます。
4. アドレスが 0.0.0.0 の場合は、アダプタのインストール、セキュリティ設定、およびルータの設定を確認します。一部のファイアウォールソフトウェアプログラムでは、新しくインストールされたアダプタで DHCP 要求がブロックされる場合があります。

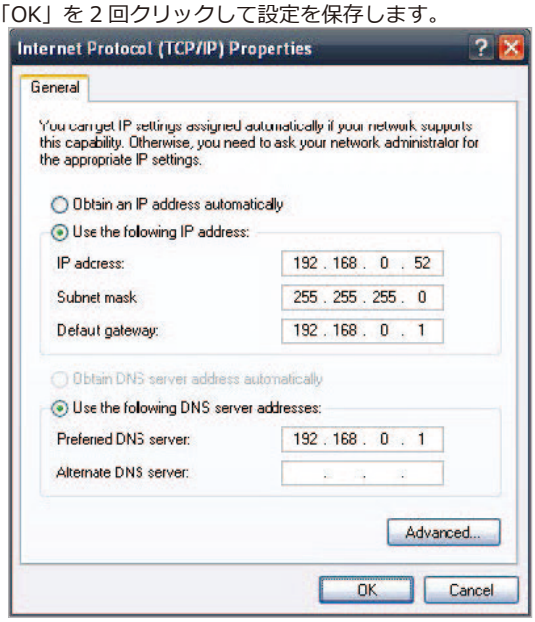
ホットスポット（ホテル、コーヒーショップ、空港など）で無線ネットワークに接続する場合は、従業員または管理者に連絡して、無線ネットワーク設定を確認してください。



Q 固定IPアドレスを割り当てる方法は?

A DHCP対応のゲートウェイ/ルータを使用していない場合、または固定IPアドレスを割り当てる必要がある場合は、以下の手順に従ってください。

1. Windows で「スタート」>「Windows システムツール」>「コントロールパネル」>「ネットワークと共有センター」の順にクリックします。
2. ネットワークアダプタを表すローカルエリア接続をクリックし、「プロパティ」を選択します。
3. 「ネットワーク」タブを開き、「インターネットプロトコル バージョン 4 (TCP/IPv4)」を選択した状態で「プロパティ」をクリックします。
4. 「次の IP アドレスを使う」をクリックし、ネットワークと同じサブネット上の IP アドレスまたはルータ上の LAN IP アドレスを入力します。
   例：ルータの LAN IP アドレスが 192.168.0.1 の場合、IP アドレス 192.168.0.X（X は 2~99 の数値）にします。ネットワークで使用されていない IP アドレスを設定してください。デフォルトゲートウェイ、Primary DNS をルータの LAN IP アドレス（192.168.0.1）と同じ IP アドレスに設定します。セカンダリ DNS は不要または ISP から DNS サーバを入力することもできます。
5. 「OK」を 2 回クリックして設定を保存します。



機能設定例

本項では、一般によく使う以下の機能について設定例を記載します。実際に設定を行う際の参考にしてください。

- 『VLAN：p.119』

■対象機器について

本コンフィグレーションサンプルは以下の製品に対して有効な設定となります。

- DAP-3666

■VLAN

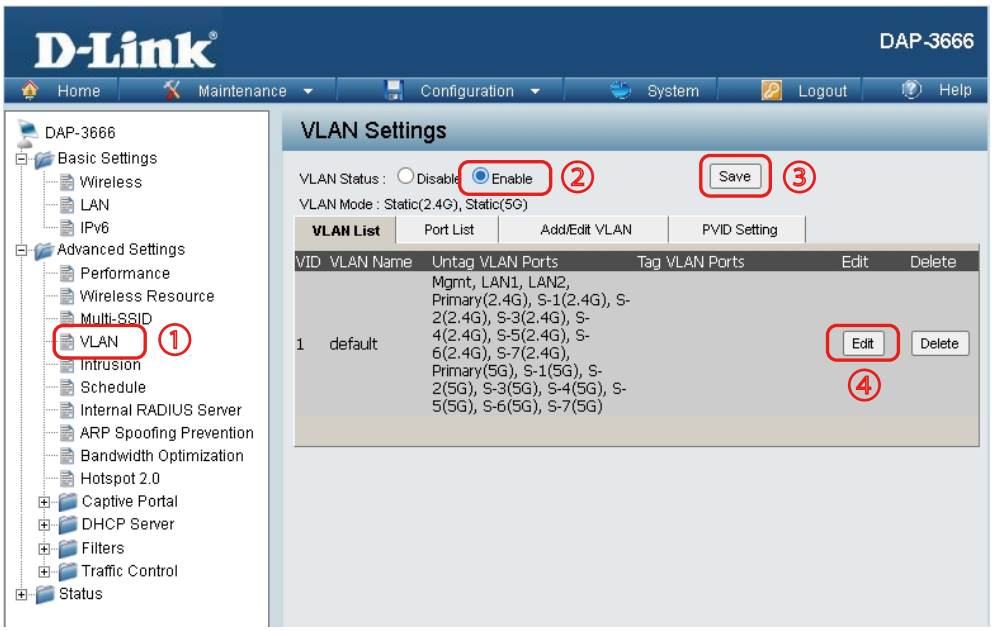
●概要

2.4GHz帯のすべてのSSIDに「VLAN10」、5GHz帯のすべてのSSIDに「VLAN20」を「Untag」で設定し、「Management VLAN」に「VLAN1」を「Untag」で設定します。

●設定手順

1. Advanced Settings > VLAN で「VLAN Settings」を表示します。

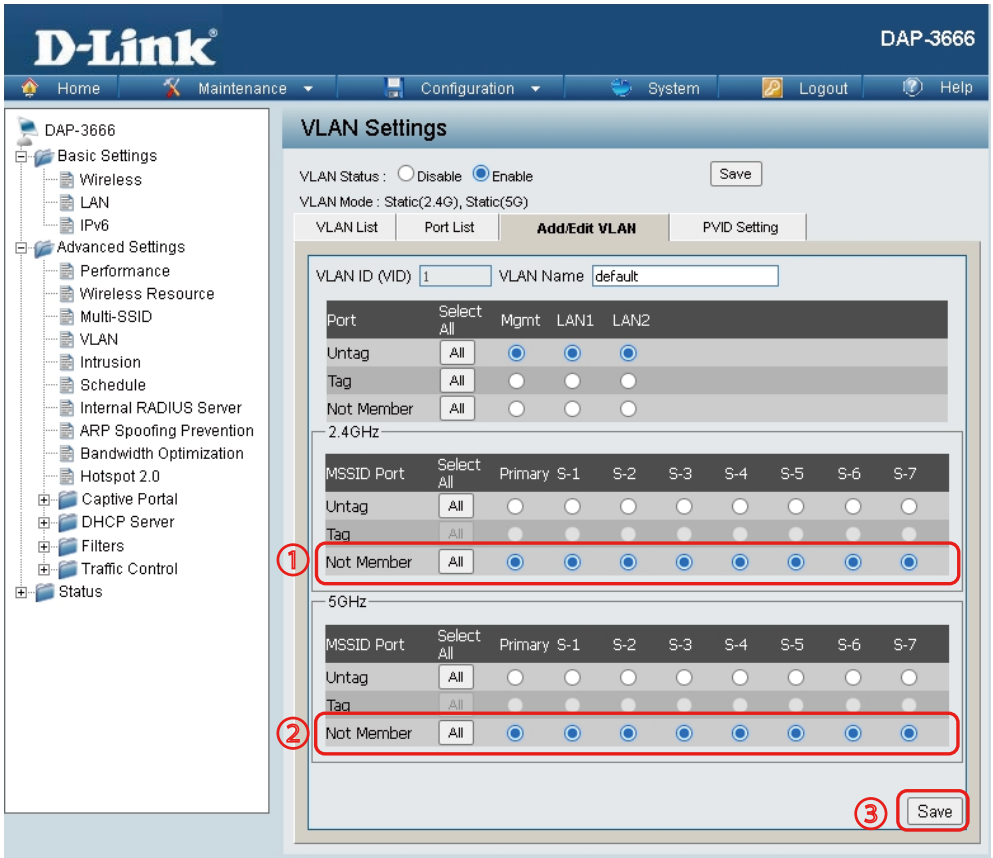
2. 「VLAN Status」で「Enable」を選択し「Save」をクリック、次に④の「Edit」をクリックします。



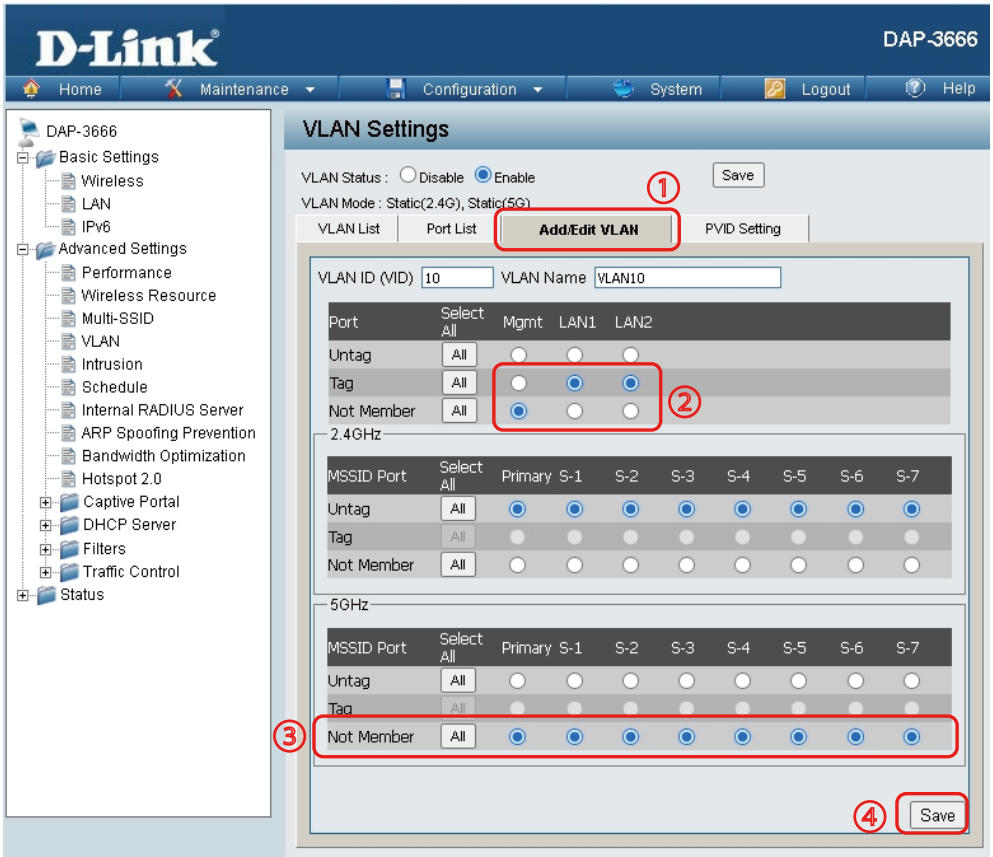
3. 「Add/Edit VLAN」タブが表示されます。

4. 「VLAN1」（VID1）の MSSID ポートで「Not Member」にチェックを入れて、無線ネットワークから「VLAN1」を削除します。

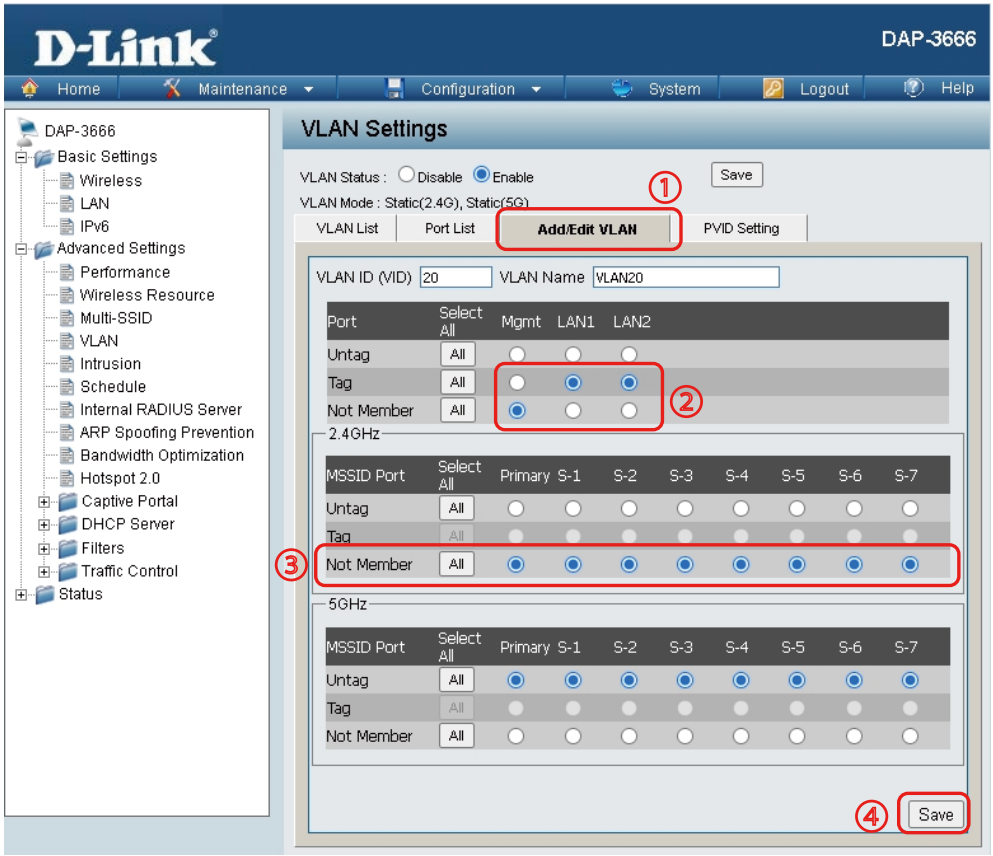
5. 「Save」をクリックします。



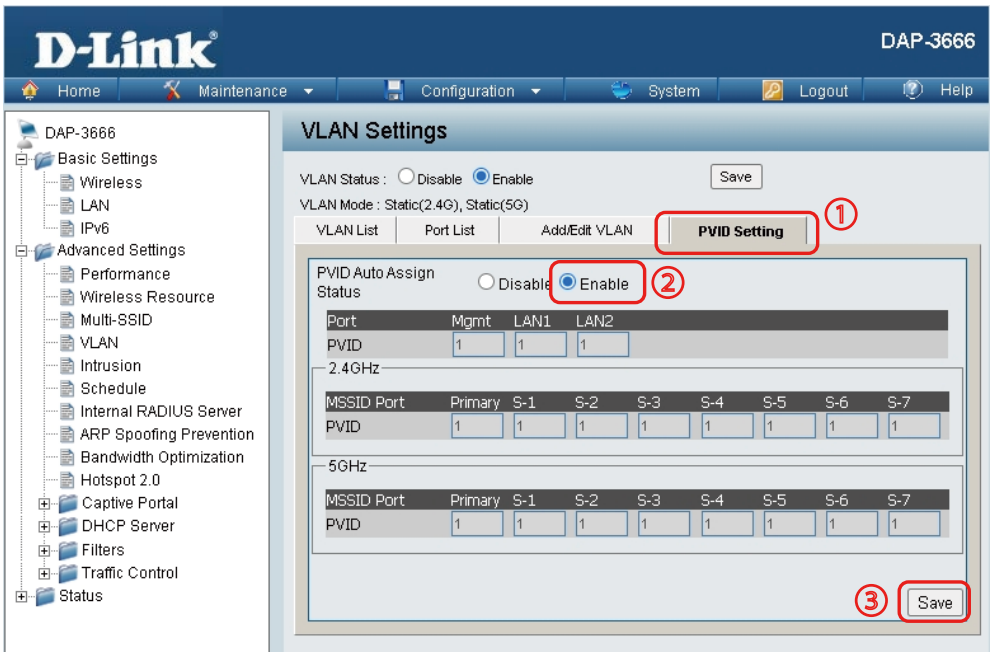
6. 「Add/Edit VLAN」タブを開き、「2.4GHz 帯」のすべての SSID に「VLAN10」を「Untag」で設定します。



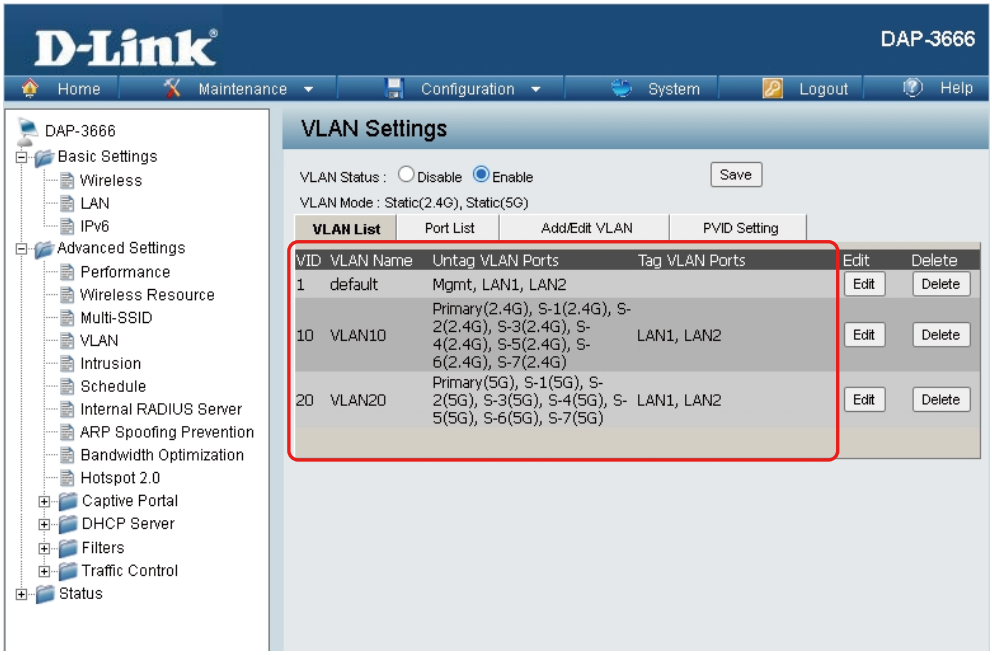
7. 下図のように「5GHz 帯」のすべての SSID に「VLAN20」を「Untag」で設定します。



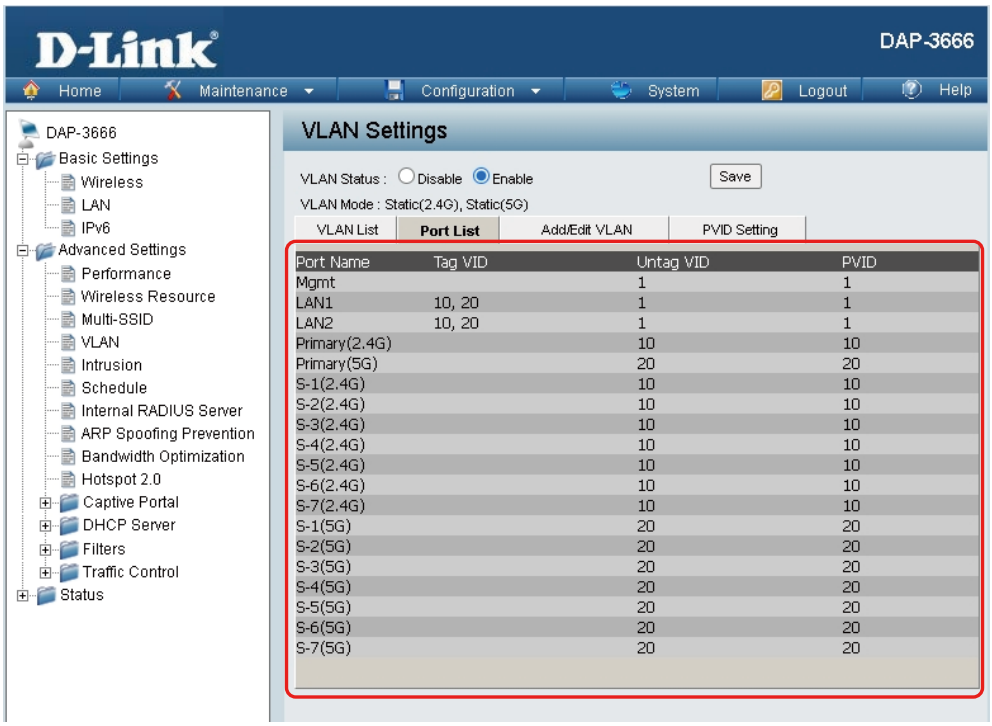
8. 「PVID Setting」タブを選択し、各ポートの VID を設定します。

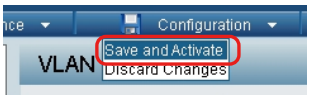
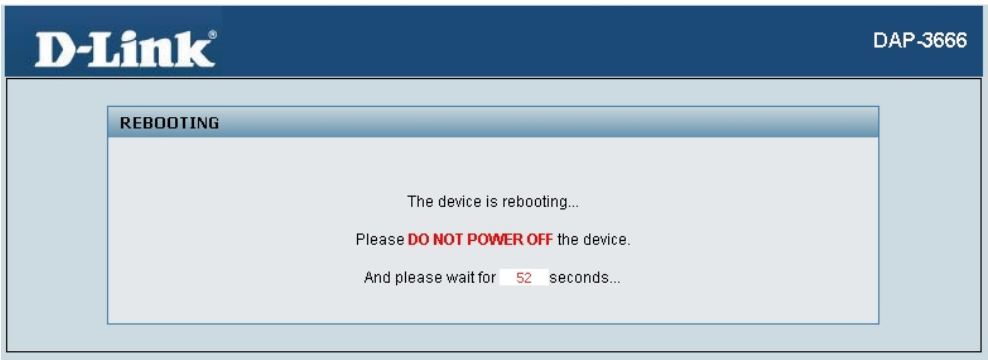


9. 「VLAN Settings」の「VLAN List」が下図の状態になっている事を確認します。



10. 「VLAN Settings」の「Port List」が下図の状態になっている事を確認します。



11. Configuration で「Save and Activate」をクリックし、設定内容を保存します。

下図のダイアログが表示され、しばらくの間設定の有効化を行います。
電源を落とさずにお待ちください。