D-Link DWL-7620AP

Unified 802.11ac Tri-Band Unified Access Point

ユーザマニュアル

D-Link
Building Networks for People

目次

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、設置マニュアル、および同梱されている製品保証書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。

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、傷害または物損損害が発生するおそれがあります。

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

⚠危険

- 🚫 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。
- 🚫 ぬれた手でさわらない
  感電の原因となります。
- 🚫 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。
- 🚫 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。
- 🚫 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。
- 🚫 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。
- 🚫 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。
- 🚫 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。
- 🚫 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

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

⚠警告

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

⚠注意

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

電波障害自主規制について

本製品は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。
この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをしてください。

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。
- 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製品ラベルや認証ラベルをはがさないでください。はがしてしまうとサポートを受けられなくなります。

静電気障害を防止するために

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

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

バッテリの取り扱いについて

⚠警告

不適切なバッテリの使用により、爆発などの危険性が生じることがあります。バッテリの交換は、必ず同じものか、製造者が推奨する同等の仕様のものをご使用ください。バッテリの廃棄については、製造者の指示に従って行ってください。

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400Mbps 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。
WPA3は、無線LANの普及促進の業界団体であるWi-Fi Allianceによって2018年6月に策定された無線LANの暗号化技術の規格名称です。WPA2に代る次世代セキュリティ規格で、よりセキュアな通信を実現します。

「WPA-Personal」「WPA2-Personal」「WPA3-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」「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」「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、本製品の使用する上で、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。
  - 時期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/product-assurance-provision

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

設置と管理のしかた

2

本製品の設置方法と、Web GUIやCLIを使用した管理方法について説明します。

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
- RJ-45/DB9 変換ケーブル
- マウントキット
- GNU GPLライセンスノート
- PLシート
- クイックスタートガイド

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

ネットワーク接続前の準備

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。

● 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。一枚の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。

- 必ず付属のイーサネットケーブルをご使用ください。

⚠注意

本アクセスポイントは、IEEE 802.3at 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。

システム要件

Web インタフェースを使用、またはTelnet やSSH 経由でCLI を使用して統合アクセスポイントを管理するためには、アクセスポイントにIP アドレスが必要になります。また、ネットワーク上でVLAN や IEEE 802.1X 認証を使用している場合、ネットワークに接続する前に、アクセスポイントに追加の設定をする必要があります。

⚠注意

本製品は、インターネットのゲートウェイとして動作しません。ご使用の無線LAN を他のLAN またはインターネットに接続するためには、別途ゲートウェイが必要です。

■管理者用コンピュータ推奨環境

Web ベースのユーザインタフェースを使用して統合アクセスポイントの設定および管理を行うための管理者用コンピュータの最小必要環境を説明します。

- イーサネットへの接続
  本製品を最初に設定するためには、使用するコンピュータをシリアルケーブルまたはイーサネットケーブルで接続します。
- ネットワークへの無線接続
  新規の無線ネットワークで最初にアクセスポイントの初期設定および起動を行うと、内部ネットワークへの無線接続を使用して、管理者用 Web 画面で設定変更を行うことができます。
  本製品への無線接続には、管理者用機器に無線クライアントと同様の Wi-Fi 機能が必要になります。
  - 本製品が準拠する1つ以上の IEEE 802.11 モードをサポートする、ポータブルまたは内蔵型の Wi-Fi クライアントアダプタ。
  - 本製品と接続するよう設定した無線クライアントソフトウェア。
- Web ブラウザとオペレーティングシステム
  本製品の設定および管理は、本製品に実装された Web ベースユーザインタフェースを経由して行います。
  本製品の管理者用 Web 画面に接続するためには、以下のいずれかのブラウザを使用することをお勧めします。
  - Microsoft® Internet Explorer®
  - Mozilla® Firefox
  - Safari

  管理者用 Web ブラウザは、管理者インタフェースのインタラクティブ機能をサポートするため、必ず JavaScript を有効にしてください。
  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。
- セキュリティ設定
  本製品の初期設定に使用する無線クライアントのセキュリティが無効になっていることを確認してください。

■無線クライアントの必要環境

統合アクセスポイントは、アクセスポイントが動作している802.11 モードに対し、Wi-Fi クライアントアダプタが適切に設定されていれば、どんなクライアントにも無線接続を提供します。本製品は、複数のクライアントOSをサポートします。クライアントとは、Wi-Fi アダプタやサポートドライバが装備されているノートパソコンやデスクトップコンピュータ、PDA、その他の携帯型や据え置き型のデバイスを意味します。

アクセスポイントに接続するためには、無線クライアントに以下に示すソフトウェアおよびハードウェアが搭載されている必要があります。

- Wi-Fi クライアントアダプタ
  アクセスポイントが準拠する 1 つ以上の IEEE 802.11 モードをサポートする、ポータブルまたは内蔵型の Wi-Fi クライアントアダプタ。（IEEE 802.11a、802.11b、802.11g、802.11n 、802.11ac をサポート。）
- 無線クライアントソフトウェア
  本製品に接続するよう設定したクライアントソフトウェア（例：Microsoft Windows サプリカント）。
- クライアントセキュリティ設定
  本製品の初期設定を行うために、クライアントのセキュリティは必ず無効にしてください。

  本製品のセキュリティモードがテキスト以外で設定される場合、無線クライアントは本製品が使用する認証モードにプロファイルを設定して、有効なユーザ名、パスワード、証明書または同等のユーザ認証を提供する必要が生じます。セキュリティモードとして、IEEE 802.1X、RADIUS サーバを持つ WPA および WPA-PSK があります。

  本製品のセキュリティ設定に関する情報は、『VAP（仮想アクセスポイントの設定）：p.45 』を参照してください。

ダイナミック/スタティック IP アドレス設定

本製品の電源を入れると、実装されているDHCP クライアントは、IP アドレスおよびその他のネットワーク情報を取得するためにネットワーク上のDHCP サーバを検索します。

本製品がネットワーク上のDHCP サーバを検出しない場合は、DHCP サーバからネットワーク情報の受信に成功するまで、スタティック IP アドレスの初期値（10.90.90.91）を使用します。

メモ

CLI を使用して接続タイプの変更、およびスタティック IP アドレスの割り当てを行う場合は、『CLI を使用したイーサネット設定：p.24 』を参照してください。
Web GUIを使用する場合は、『Ethernet Settings（イーサネット設定）：p.35 』を参照してください。

■IPアドレスのリカバリ

本製品の接続に問題がある場合は、アクセスポイントの設定を工場出荷時の初期値にリセットしてスタティック IP アドレスを回復することができます 。(『工場出荷時設定に戻す：p.84 』を参照)。
または、DHCP サーバを持つネットワークにアクセスポイントを接続して、ダイナミックにアドレスを割り当てることもできます。

■ダイナミックに割り当てられたIP アドレスの検出

ご使用のネットワーク上のDHCP サーバに接続してアクセスポイントのIP アドレスを取得すると、アクセスポイントのMAC アドレスに紐づく新しい IP アドレスを参照することができます。
アクセスポイントに IP アドレスを割り当てるDHCP サーバに接続できない場合、またはアクセスポイントのMAC アドレスが不明な場合は、CLI を使用して新しい IP アドレスを確認する必要があるかもしれません。

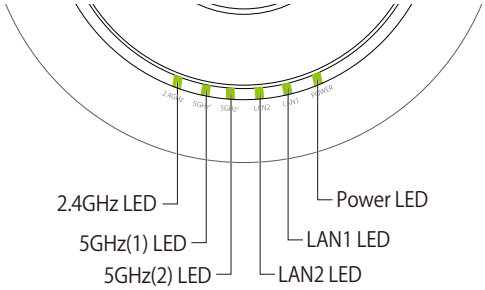
メモ

ダイナミックに割り当てられた IP アドレスの検出については、『CLI を使用した IP アドレスの参照：p.24 』を参照してください。

本体各部名称

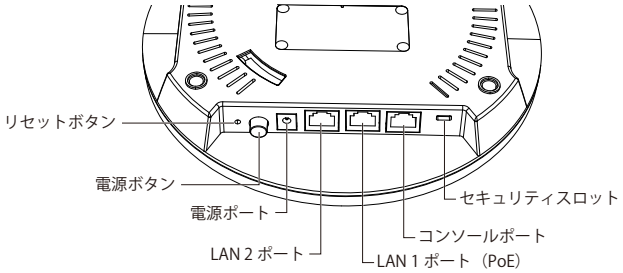
本製品の各部名称について説明します。

■上面



LED	色	状態	状況説明
Power LED	緑	点灯	電源が入っています。
	赤	点灯	システムが起動中です。
LAN1/LAN2 LED	緑	点灯	ネットワークのリンクが確立しています。
		点滅	ネットワーク上でデータを送受信しています。
2.4GHz LED	緑	点灯	2.4GHz帯域が有効になっています。
		点滅	2.4GHz帯域でデータを送受信しています。
5GHz[1]LED	緑	点灯	5GHz[1]帯域が有効になっています。
		点滅	5GHz[1]帯域でデータを送受信しています。
5GHz[2] LED	緑	点灯	5GHz[2]帯域が有効になっています。
		点滅	5GHz[2]帯域でデータを送受信しています。

■側面



名称	説明
リセットボタン	本製品を工場出荷時の設定にリセットします。
電源ボタン	本製品の電源ON/OFFスイッチです。
電源ポート	AC アダプタを接続します。 メモ ・本製品にACアダプタは同梱されていません。PoE接続でご利用になるか、別売りの「PSE-M12V25A-I」をご使用ください。
LAN1(PoE)ポート	RJ-45ケーブルを挿入し、ネットワークへの接続とPoE受電を行います。
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。
コンソールポート	コンソールケーブルを接続します。 CLI（コマンドラインインタフェース）にアクセスする際に使用します。
セキュリティスロット	市販のセキュリティワイヤを取り付けます。

製品の設置

■イーサネットケーブルの接続（LAN接続/PoE受電）

1. イーサネットケーブルを、本製品の側面にある RJ-45 コネクタ（「LAN1（PoE）」ポート）に接続します。
2. イーサネットケーブルのもう一端を、PoE スイッチ /PoE インジェクタに接続します。

メモ

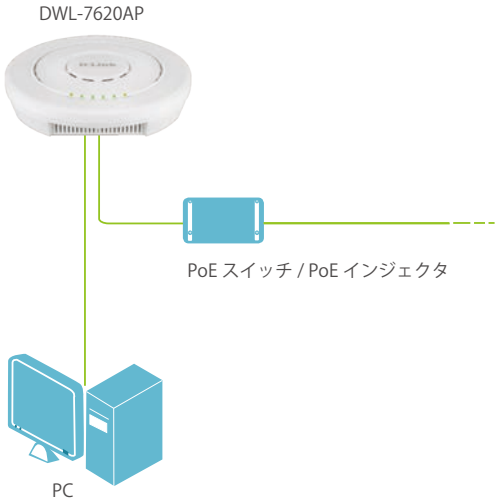
- 電源が供給されると、POWER LED が点灯します。
- 本製品にACアダプタは同梱されていません。PoE接続でご利用になるか、別売りの「PSE-M12V25A-I」をご使用ください。

■接続例

本製品の設定を行うには、管理用PCを使用して本製品のWeb GUIにアクセスする必要があります。

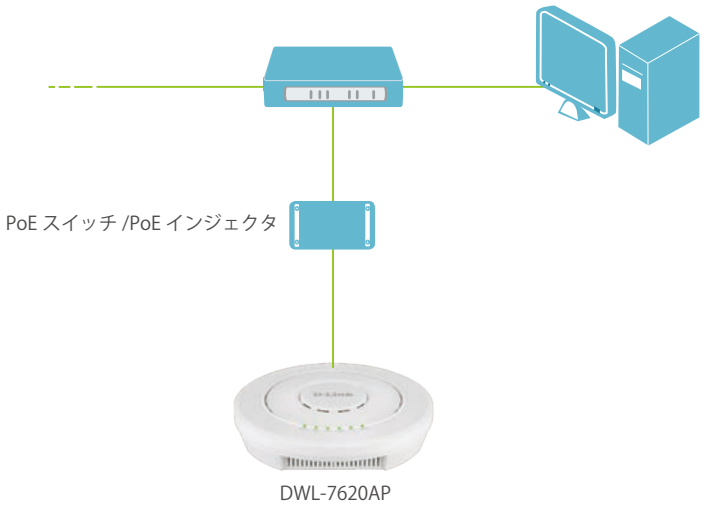
● 直接接続

本製品と管理用PCをイーサネットケーブルで直接接続します。



● スイッチ経由の接続

本製品を、管理用PCが接続しているハブに接続します。



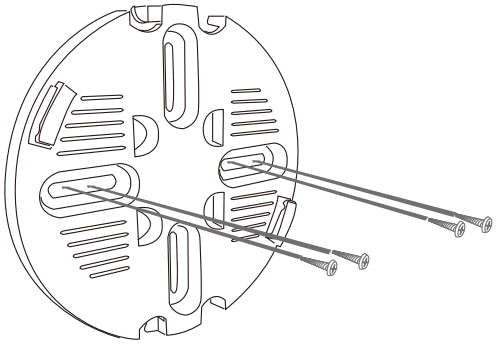
メモ

Web GUIへのアクセス、ログイン方法の詳細は『WEB GUI画面について：p.19 』を参照してください。

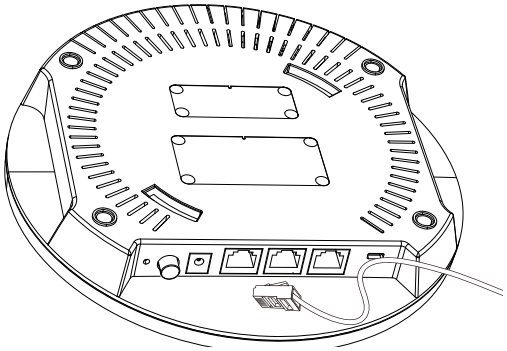
■マウントキットによる設置

本製品は、マウントキットを使用して壁面や天井に設置することができます。設置の際は以下の手順を参照してください。

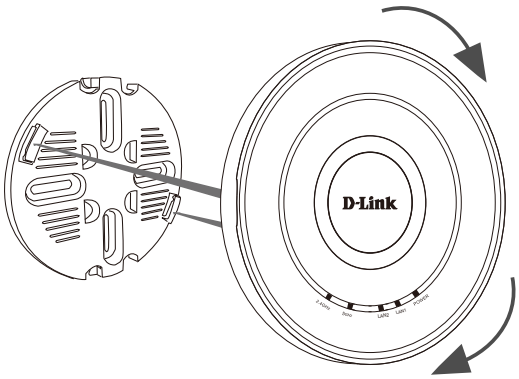
1. アクセスポイントを取り付ける壁または天井にマウントプレートを合わせます。
2. プラスティックアンカーをつける場所にマークをつけます。
3. マークした場所に穴をあけ、アンカーを挿入します。
4. アンカー用のネジを使用し、マウントプレートを壁面に取り付けます。



5. アクセスポイントの LAN ポートにイーサネットケーブルを挿入します。



6. アクセスポイントをマウントプレートに取り付けるには、まず、アクセスポイント右側のセキュリティロックのマークが書かれた箇所を、マウントプレートの「<<<OPEN LOCK>>>」と書かれている位置と合わせます。



7. アクセスポイントを時計回りにスライドさせ、マウントプレートに取り付けます。アクセスポイントのセキュリティロックのマークがマウントプレートの「CLOSE」に合わさるように固定してください。

WEB GUI画面について

■Web GUI画面へのログイン

メモ

- 本製品の設定は、イーサネットケーブルで接続したPCから行います。設定を始める前に、本製品とPCをイーサネットケーブルで接続してください。
- 本製品のIPアドレスとPCのIPアドレスは、同じサブネット内に設定してください。
  例）本製品のIPアドレス：10.90.90.91/8、PCのIPアドレス：10.90.90.100/8
- PCのプロキシサーバ機能は無効にしてください。

■手順：
Windowsの「スタート」＞「コントロールパネル」＞「インターネットオプション」＞「接続」タブ ＞「LANの設定」の順にクリックし、「LAN にプロキシサーバを使用する」のチェックを外します。

1. Web ブラウザを起動します。
2. Web ブラウザに本製品の IP アドレスを入力します。

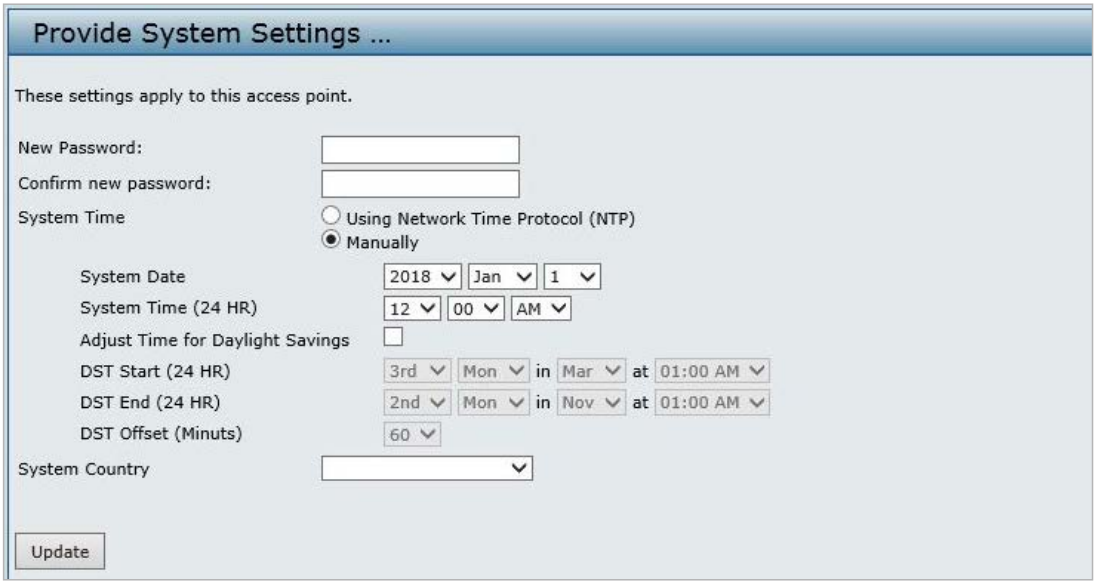
メモ

- IPアドレスの初期値は「10.90.90.91」です。
- ご使用のネットワークでDHCP サーバを使用していて自動的にネットワーク情報が設定される場合は、Web ブラウザに本製品の新しい IP アドレスを入力します。
  DHCPによって割り当てられた新しいIPアドレスがわからない場合は、以下の手順でIPアドレス情報を取得してください。
  - 管理者コンピュータとアクセスポイントをシリアルケーブルで接続し、端末エミュレーションソフトウェアを使用して CLI（ command-line-interface） に接続します。
    ターミナルソフトウェアの設定は下記の通りです。
    ・ボーレート：115200
    ・データビット：8
    ・パリティ：none
    ・ストップビット：1
    ・フロー制御：none
  - ログイン画面で、ユーザ名およびパスワードに「admin」と入力します。
    プロンプトが表示されたら、「get management」と入力します。
  - コマンド出力としてアクセスポイントの IP アドレスが表示されます。
    このアドレスをWeb ブラウザのアドレスに入力してください。
3. ログイン画面で [User Name] と [Password] を入力 [Logon] をクリックします。

工場出荷時の設定は以下です。
- User Name：admin
- Password：admin

■初回ログイン時のセットアップ

WEB GUI画面への初回ログイン後、以下の画面が表示されます。
管理者パスワードや時刻、国の設定を行ってください。

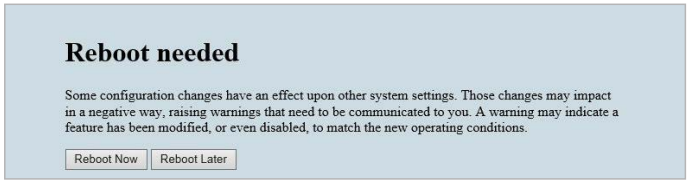


UI	説明
New Password	本製品の新しい管理者パスワードを入力します。 入力した文字は他人から見えないように「●●●」と表示されます。 ・入力可能文字数：最大32文字（半角英数字）
Confirm new password	確認のため、新しい管理者パスワードを再度入力します。
System Time	時間の設定方法を以下から選択します。 ・[Using Network Time Protocol（NTP）]：NTPサーバを使用して時間設定を行います。 ・[Manually]：手動で時間設定を行います。
NTP Server IPv4/ IPv6 Address/Name	NTPサー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。
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（24HR）	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。
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（NTP）]を選択した場合にのみ表示されます。 ・初期値：[Pacific Time（US/Canada）, Tijuana]
Adjust Time for Daylight Savings	チェックを入れ、Daylight Savings Time（サマータイム）の設定を行います。
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を選択します。
Update	設定を適用します。

メモ

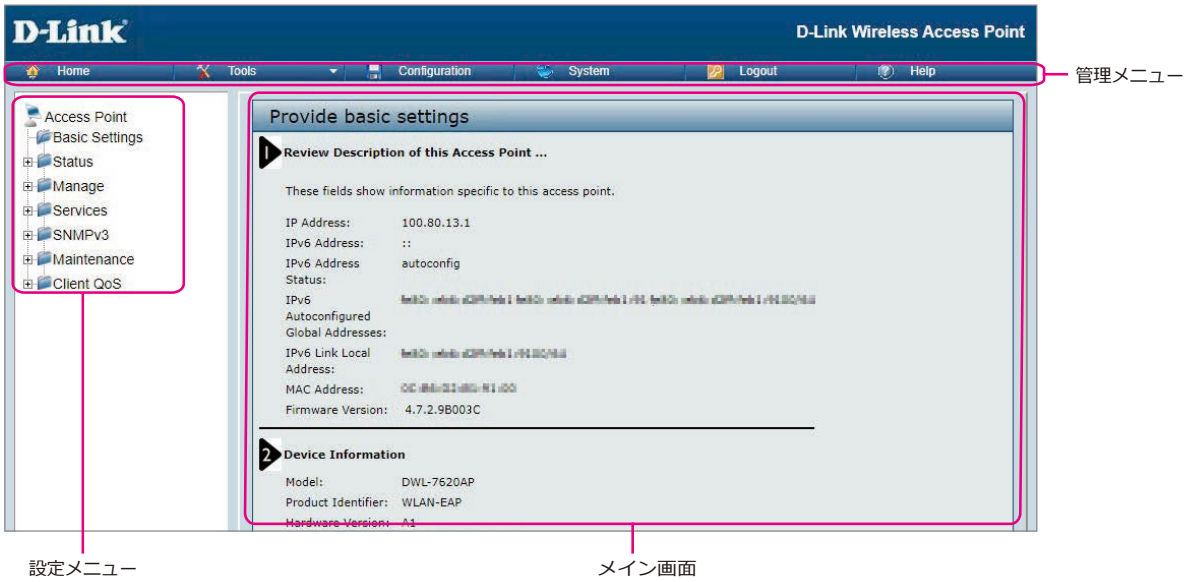
NTP Server IPv6アドレス設定は、現在のバージョンではサポートされません。

再起動を促すメッセージが表示されます。
すぐに再起動を行う場合は[Reboot Now]、後で再起動を行う場合は[Reboot Later]をクリックしてください。



■Web GUI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**
  ホーム画面を表示します。ホーム画面では、IPアドレスやファームウェアバージョンなどの情報を確認できます。

- **Tools**
  ファームウェアのアップロードや、時刻設定を行います。詳しい設定内容については以下を参照してください。
  - Basic Settings:『ホーム画面:p.22 』
  - Upgrade:『Upgrade(ファームウェアアップグレード):p.77 』
  - Time Settings (NTP):『Time Settings(時間設定):p.68 』

- **Configuration**
  コンフィグレーションファイルのバックアップや、本製品の工場出荷時設定へのリセットを行います。詳しい設定内容については以下を参照してください。
  - 『Configuration(コンフィグレーションの保存・リストア):p.75 』

- **System**
  本製品の再起動/工場出荷時設定へのリセット/LEDの設定を行います。詳しい設定内容については以下を参照してください。
  - 『Maintenance:p.74 』

- **Logout**
  WEB GUIからのログアウトを行います。

- **Help**
  ヘルプ画面を表示します。

● 設定メニュー

設定メニューをクリックし、各機能の設定を行います。
詳しい設定内容についてはマニュアルの3章 - 9章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。

■ホーム画面

管理メニューの[Home]または設定メニューの[Basic Settings]をクリックすると、以下の画面が表示されます。
IPアドレスやファームウェアバージョンの確認のほか、システム名の変更やログインパスワードを変更することができます。

設定を変更した場合は、[Update]をクリックして設定を保存してください。

UI	説明
Review Description of this Access Point	本製品のIPアドレス、MACアドレス、ファームウェアバージョンを表示します。 • [IP Address]：本製品に割り当てられているIP アドレスです。 • [IPv6 Address]：本製品に割り当てられているIPv6アドレスです。 • [IPv6 Address Status]：本製品の管理インタフェースに設定されたスタティックIPv6 アドレスの状態を表示します。 • [IPv6 Autoconfigured Global Addresses]：本製品の管理インタフェースに自動的に設定されたグローバルIPv6 アドレスを表示します。 • [IPv6 Link Local Address]：ローカルの物理的なリンクによって使用されるIPv6 リンクローカルアドレスです。IPv6 Neighbor 探索プロセスを使用して割り当てられるため、変更はできません。 • [MAC Address]：本製品のMAC アドレスです。 • [Firmware Version]：現在のファームウェアバージョンです。
Device Information	本製品のハードウェアバージョンやシリアルナンバーなど、デバイス情報を表示します。 • [Model]：本製品のモデル番号です。 • [Product Identifier]：本製品のハードウェアモデルです。 • [Hardware Version]：本製品のハードウェアバージョンです。 • [Serial Number]：本製品のシリアルナンバーです。 • [Device Name]：本製品のデバイス名です。 • [Device Description]：本製品のハードウェア情報です。
Provide Network Settings	本製品のパスワードを設定します。 • [New Password]：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：最大32文字（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 Settings	本製品のシステム情報を設定します。 • [System Name]：本製品の名称を入力します。この名前は本画面およびCLIログインプロンプトに表示されるもので、管理者が本製品を識別するための名称です。64 文字までの半角英数字を入力します（例：My AP）。 • [System Contact]：本製品に関する連絡先として、名前、Eメールアドレス、電話番号などを入力します。 • [System Location]：本製品の物理的な設置場所を入力します（例：会議室A）。
Update	設定を適用します。

重要

無線ネットワークの安全性を高めるため、最初のセットアップ時に設定を初期値から変更することを推奨します。

コンソールポートを使用した管理

■CLI を使用した IP アドレスの参照

コンソールポートを使用し、CLIでネットワーク情報の設定を行う方法について説明します。

・本製品のDHCP クライアント機能は、初期設定で有効になっています。
DHCP クライアント機能が有効になっていると、本製品をDHCP サーバが存在するネットワークに接続した場合、自動的にIP アドレスを取得します。
Web GUIを使用して本製品を管理するためには、本製品のIP アドレスをWeb ブラウザに入力する必要があります。

1. 同梱の RJ-45/DB9 変換ケーブルを使用して、VT100/ANSI 端末かワークステーションをコンソール（シリアル）ポートに接続します。

   PCやApple、UNIX のワークステーションと接続する場合は、ハイパーターミナルなどの端末エミュレーションプログラムを起動してください。

2. 端末エミュレーションプログラムの設定を以下に合わせてください。

   - データ速度：115,200bps
   - データビット：8
   - パリティ：なし
   - ストップビット：1
   - フロー制御：なし

3. 「Enter」キーを押すとログインプロンプトが表示されます。
   ユーザ名とパスワードを入力してください。

   - 初期値/ユーザ名：「admin」、パスワード：「admin」

4. プロンプトが表示されたら、「get management」と入力し、IP アドレスを確認します。

```
DLINK-WLAN-AP# get management
Property        Value
---------------------------
vlan id: 1
interface: br-lan
static ip: 10.90.90.91
static mask: 255.0.0.0
ip: 10.90.90.91
mask: 255.0.0.0
mac: xx:xx:xx:xx:xx:xx
dhcp : up
DLINK-WLAN-AP#
```

■CLI を使用したイーサネット設定

以下の表のコマンドを使用してイーサネット（有線）インタフェースの値を参照および設定します。

コマンド	アクション
get management	イーサネット（有線）内部インタフェースの現在の設定を確認する
set management vlan-id <1-4094>	管理VLAN ID を設定する
get management dhcp-status	接続タイプを参照する
set management dhcp-status up	DHCP を接続タイプとして使用する
set management dhcp-status down	スタティック IP を接続タイプとして使用する
set management static-ip <ip_address> 例：set management static-ip 10.10.12.221	スタティック IP アドレスを設定する
set management static-mask <netmask> 例：set management static-mask 255.255.255.0	サブネットマスクを設定する

設定例:

管理用VLAN ID を「123」に設定し、すべてのトラフィックがタグ付けされてVLAN ID を持つように、タグなしVLAN を無効にします。

```
DLINK-WLAN-AP# set management vlan-id 123
dman: Restarting DHCPv6 client
DLINK-WLAN-AP# set untagged-vlan status down
dman: Restarting DHCPv6 client
DLINK-WLAN-AP# get management
Property                  Value
------------------------------------------
vlan-id                   123
interface                 brtrunk
static-ip                 10.90.90.91
static-mask               255.0.0.0
ip                        10.90.90.91
mask                      255.0.0.0
mac                       XX:XX:XX:XX:XX:XX
dhcp-status               down
static-ipv6               ::
static-ipv6-mask
ipv6
ipv6-mask
ipv6-status               up
ipv6-autoconfig-status    up
static-ipv6               ::
static-ipv6-prefix-length 0
dhcp6-status              up

DLINK-WLAN-AP#              get untagged-vlan
Property Value
---------------
vlan-id 1
status down
DLINK-WLAN-AP#
```

その他のコマンドは以下の通りです。

コマンド	アクション
get system	アクセスポイントのモデル名、ハードウェアバージョン、ファームウェアバージョン、MACアドレスなど、システム情報を表示します。
get managed-ap	アクセスポイントを検出・管理可能なスイッチの情報を表示します。
reboot	システムを再起動します。
firmware-upgrade <URL>	ファームウェアアップグレードを行います。
factory-reset	システムを工場出荷時の状態に戻します。
get system led	LEDの制御ステータスを表示します。 • 1: LEDが有効です。 • 0: LEDが無効です。
set system led on	システムLEDを有効にします。
set system led off	システムLEDを無効にします。
save-running	各種コマンドの実行後、save-running、rebootコマンドを実行して設定を適用します。

インストールの確認

本製品がLAN に接続し、ネットワークに無線クライアントが接続していることを確認してください。
無線ネットワークの基本設定を確認した後に詳細設定を行うことで、よりセキュリティ性の高い詳細な設定を行うことができるようになります。

1. 本製品を LAN に接続します。

   本製品および管理者用コンピュータを1 つのハブに接続している場合、本製品は既にLAN に接続しています。次に無線クライアントのテストを行います。
   本製品を直接ケーブルでご使用のコンピュータに接続している場合は、以下の手順で行います。
   - 本製品とコンピュータのケーブルを外します。
   - 本製品をイーサネットケーブルでLAN に接続します。
   - イーサネットケーブルまたは無線LAN カードを使用して、コンピュータをLAN に接続します。

2. 無線クライアントと LAN の接続を確認します。

   無線クライアントデバイスから、本製品を検出して接続することで本製品を確認します。

3. 詳細設定により、本製品にセキュリティ設定をします。

   無線ネットワークが動作し、本製品が無線クライアントに接続した後に、セキュリティレイヤの追加、複数のVAP の作成、および性能設定を行うことができます。

重要

- 本製品において、同時に複数の設定変更を行うことはできません。1 人以上の管理者が管理者用Web 画面にログインして設定変更を行う場合、複数のユーザによって指定された設定の変更が適用される保証はありません。
- 初期設定ではセキュリティ設定が行われていないため、どの無線クライアントからもアクセスポイントやご使用のネットワーク に接続することができます。『VAP（仮想アクセスポイントの設定）：p.45 』を参照し、セキュリティの設定を行ってください。

無線アクセスポイントのセキュリティ設定

有効な各仮想アクセスポイント（VAP）にセキュリティ設定を行い、セキュアな無線クライアントを設定します。周波数帯毎に最大16 個のVAP を設定して複数のアクセスポイントのように設定することができます。初期値では、有効なVAP は1 つです。各VAP に異なるセキュリティモードを設定して無線クライアントの接続を制御することができます。

各周波数帯には、VAP ID が0-15 の16 個のVAP があります。初期値ではVAP 0 のみ有効です。
VAP 0 の初期設定は以下の通りです。

- VLAN ID：1
- Broadcast SSID：有効
- SSID：dlink1
- Security：なし
- MAC Authentication Type：なし

他のすべてのVAP は初期値で無効です。VAP 1-15 のSSID の初期値 は、dlinkx（x はVAP ID）になります。

本製品への不正アクセスを防止するために、VAP の初期値および有効にした各VAP のセキュリティオプションで「None」以外を選択して変更を行うことをお勧めします。

重要

各VAP のセキュリティ設定方法に関する詳細は、『VAP（仮想アクセスポイントの設定）：p.45 』を参照してください。

Status

3

Statusメニューでは、アクセスポイントのステータスを参照することができます。

Interfaces（インタフェースステータスの参照）

設定画面：[Status] > [Interfaces]

イーサネットLAN および無線LAN（WLAN）設定を参照します。

UI	説明
Refresh	表示を更新します。
Wired Settings	有線設定（内部インタフェース）の情報です。 イーサネットMACアドレス、管理VLAN ID、IPアドレス、サブネットマスク、およびDNS情報が表示されます。 これらの設定を変更する場合は、[Edit]をクリックして設定画面を表示します。 有線設定の詳しい内容については、『Ethernet Settings（イーサネット設定）：p.35 』を参照してください。
Wireless Settings	無線設定の情報です。 各無線インタフェースに対応するMAC アドレス（参照のみ）も表示されます。 設定を変更する場合には、[Edit]をクリックして設定画面を表示します。 無線設定の詳しい内容については、『Wireless Settings（無線設定）：p.38 』および『Radio（無線詳細設定）：p.39 』を参照してください。

Events（イベントの参照）

設定画面：[Status] > [Events]

アクセスポイントへの無線クライアントの接続や認証など、アクセスポイントに発生するシステムイベントを表示します。
[Relay Options]エリアでログ保存の詳細設定を行うことができます。

重要

本アクセスポイントは、ネットワークタイムプロトコル（NTP）を使用して日付と時間情報を取得します。
このデータはUTC 形式（グリニッジ標準時）で通知されます。ログに出力された時間については、使用する場所の時間に変換する必要があります。ネットワークタイムプロトコルの設定については、『Time Settings（時間設定）：p.68 』を参照してください。

■Relay Options （カーネルメッセージ用のログリレーホストの設定）

カーネルログは、システムログ内に出力されるシステムイベントの包括的なリストであり、破棄されたフレームなどのエラー状態を含むカーネルメッセージです。

Web マネージャを使用して直接アクセスポイントのカーネルログメッセージを参照することはできません。まず始めに、Syslog処理を実行しSyslogリレーホストとして動作するリモートサーバを設定する必要があります。その後、リモートサーバにSyslog メッセージを送信するように本製品を設定することができます。
アクセスポイントのSyslog メッセージをリモートログサーバが収集することで、以下の機能を提供します。

- 複数のアクセスポイントからSyslog メッセージの収集を行うことができます。
- 単一のアクセスポイントで保持するメッセージよりも長期間の履歴を保存することができます。
- スクリプト化された管理操作およびアラートを起動することができます。

カーネルログリレーを使用するためには、リモートサーバがSyslog メッセージを受信するように設定する必要があります。
リモートログホストを設定する手順は、リモートホストなどご使用のシステムタイプによって異なります。

重要

Syslog プロセスは、ポート514 を初期値として使用します。このポート番号を使用することをお勧めします。
ログポートを再設定する場合には、Syslog ポートに割り当てるポート番号が別のプロセスに使用されていないことをご確認ください。

● ログリレーホストの有効／無効化

ログリレーの有効／無効化、および設定を行うためには、以下の表に示すログリレーオプションを設定して[Apply]をクリックします。

UI	説明
Relay Log	ログリレーを有効または無効にします。 • [Enabled]：リモートホストへのログメッセージの送信を有効にします。 • [Disabled]：すべてのログメッセージをローカルシステムに保持します。
Relay Host	リモートログサーバのIP アドレスまたはDNS 名を指定します。 指定できるIPアドレスはIPv4アドレスのみです。
Relay Port	リレーホストのSyslog プロセス用のポート番号を指定します。 • 初期値：514
Update	設定を適用します。

重要

設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。再起動が発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが少ない時にアクセスポイントの設定変更を行うことをお勧めします。

メモ

ログリレーホストを[Enabled]（有効）にして[Update]をクリックし、本製品を再起動すると、リモートログ出力がアクティブになります。
アクセスポイントは、ログリレーホストの設定内容に従って、リモートログサーバモニタ、定義したカーネルログファイル、または他のストレージに対して表示用のカーネルメッセージをリアルタイムに送信します。
ログリレーホストを[Disabled]（無効）にして[Update]ボタンをクリックし、本製品を再起動すると、リモートログ出力は無効になります。

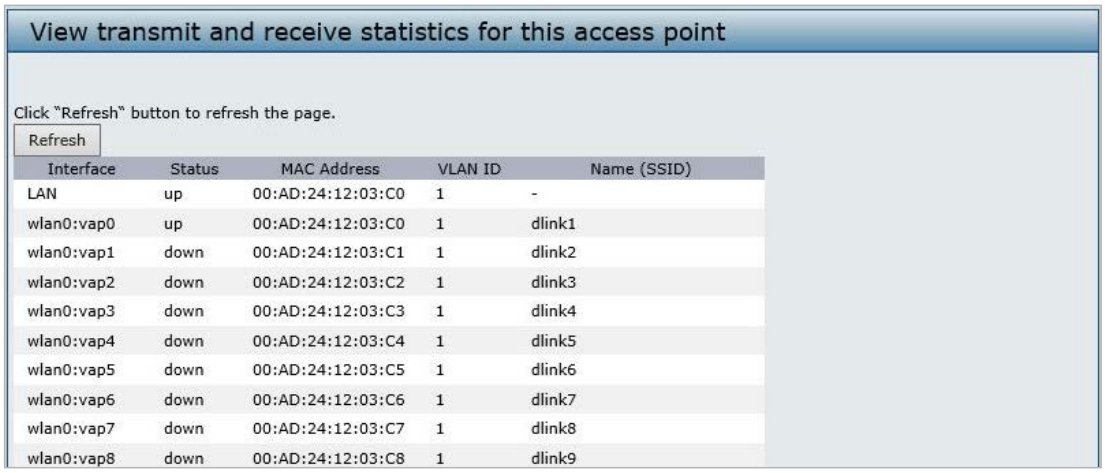
Transmit/Receive（送受信した統計情報の参照）

設定画面：[Status] > [Transmit/Receive]

各インタフェースのステータス情報と、アクセスポイント上のイーサネットインタフェースおよび無線インタフェース上のVAP で送受信したデータの統計情報を表示します。

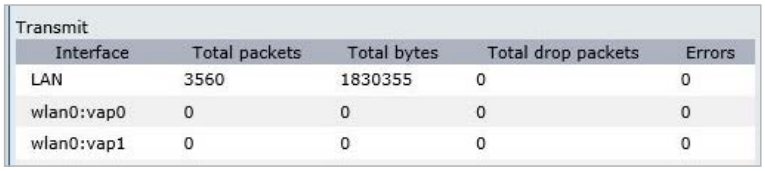
アクセスポイントが最後に起動してから現在までの統計情報が表示されます。
アクセスポイントを再起動した場合、再起動後の送受信データの合計が表示されます。

● 各インタフェースのステータス情報

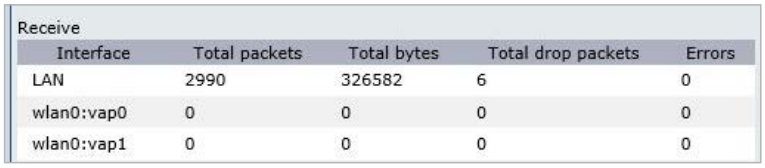


UI	説明
Interface	イーサネットまたはVAPインタフェース名が表示されます。
Status	各インタフェースのステータス（[up]（アクティブ）または[down]（ダウン））が表示されます。
MAC Address	各インタフェースのMACアドレスが表示されます。
VLAN ID	各インタフェースのVLAN IDが表示されます。 VLAN を使用して、同じアクセスポイントに複数の内部ネットワークおよびゲストネットワークを確立することができます。 VLAN IDの設定については、『VAP（仮想アクセスポイントの設定）：p.45 』を参照してください。
Name（SSID）	ワイヤレスネットワークの名称（SSID）が表示されます。SSIDの設定については、『VAP（仮想アクセスポイントの設定）：p.45 』を参照してください。
Refresh	表示を更新します。

● 送信したトラフィックの統計情報



● 受信したトラフィックの統計情報

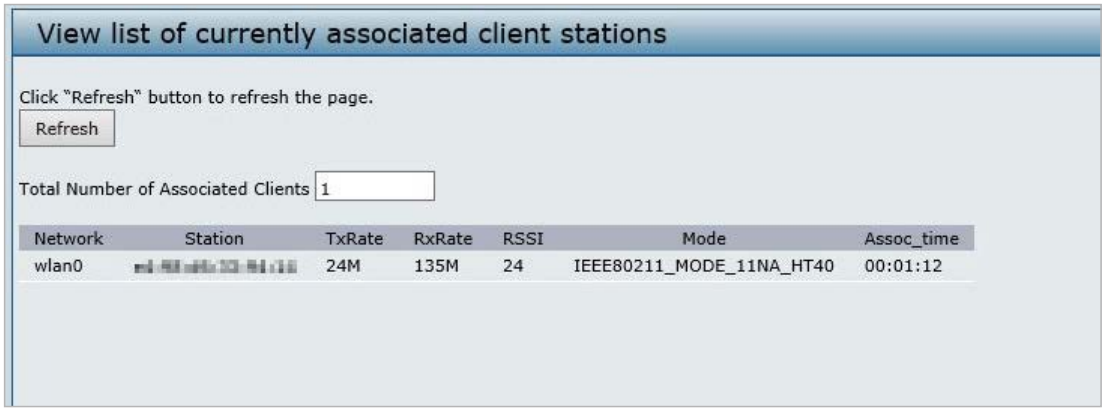


UI	説明
Interface	イーサネットまたはVAPインタフェース名が表示されます。
Total packets	送信/受信したパケットの合計が表示されます。
Total bytes	送信/受信したバイト数の合計が表示されます。
Total drop packets	送信/受信で破棄されたパケットの合計が表示されます。
Errors	送信/受信したデータに関連するエラーの合計が表示されます。

Client Associations（無線クライアント情報）

設定画面：[Status] > [Client Associations]

アクセスポイントに接続するクライアントの情報を参照します。



UI	説明
Refresh	表示を更新します。
Total Number of Associated Clients	接続中のクライアント数を表示します。
Network	クライアントが接続しているネットワークを表示します。
Station	無線クライアントのMAC アドレスを表示します。
TxRate	送信データレートを表示します。
RxRate	受信データレートを表示します。
RSSI	クライアントの最大RSSIを表示します。
Mode	802.11a/b/g/n/acモードを表示します。
Assoc_time	接続時間を表示します。

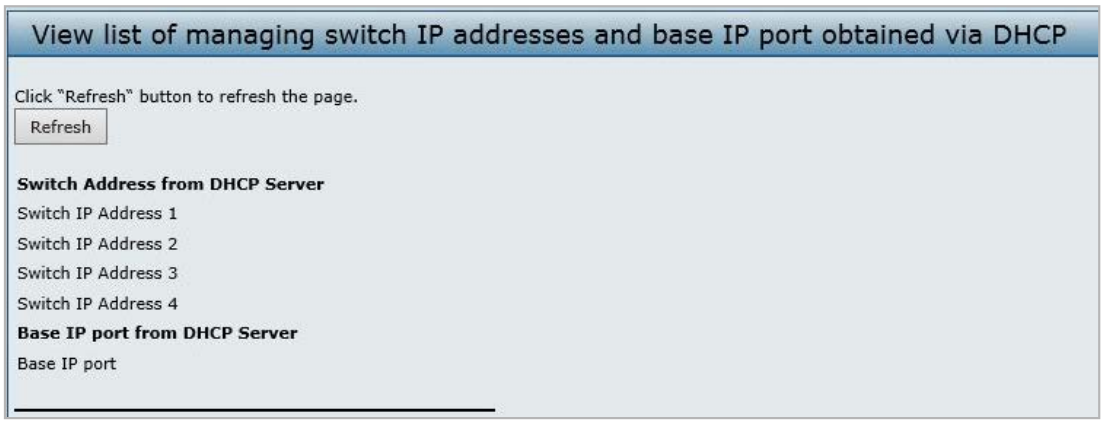
メモ

[Network]でwlan0vap2 と表示されている場合、クライアントがRadio 1上のVAP2 に接続していることを意味します。wlan0 と表示されている場合はRadio 1上のVAP0 、wlan1と表示されている場合はRadio 0 のVAP0 に接続していることを意味します。

Managed AP DHCP（管理アクセスポイントのDHCP情報）

設定画面：[Status] > [Managed AP DHCP]

DHCPサーバを利用して、ワイヤレスコントローラの情報を学習します。本画面では、DHCPサーバから学習した4つまでのワイヤレスコントローラについて、DNS名またはIPアドレスを確認することができます。



メモ

DHCP サーバが、アクセスポイントのDHCP 要求に対してコントローラのIPアドレスの情報で応答するように設定する方法については、ワイヤレスコントローラのマニュアルを参照してください。

Radio Statistics（無線統計情報）

設定画面：[Status] > [Radio Statistics]

本製品で送受信されたパケット/ バイトについて、詳しい情報を表示します。

UI	説明
Refresh	表示を更新します。
Radio Interface	[5GHz-1] [5GHz-2] [2.4GHz]のいずれかを選択し、参照する無線帯域を指定します。
WLAN Packets Received	無線インタフェース上でアクセスポイントが受信した総パケット数を表示します。
WLAN Packets Transmitted	無線インタフェース上でアクセスポイントが送信した総パケット数を表示します。
WLAN Packets Receive Dropped	無線インタフェース上でアクセスポイントが受信し、破棄されたパケット数を表示します。
WLAN Packets Transmit Dropped	無線インタフェース上でアクセスポイントが送信し、破棄されたパケット数を表示します。
WLAN Bytes Received	無線インタフェース上でアクセスポイントが受信した総バイト数を表示します。
WLAN Bytes Transmitted	無線インタフェース上でアクセスポイントが送信した総バイト数を表示します。
Multicast Frames Received	無線インタフェース上でアクセスポイントが受信したマルチキャストパケットの数を表示します。

Manage

4

イーサネット設定や無線設定など、本製品の管理方法について説明します。

Ethernet Settings（イーサネット設定）

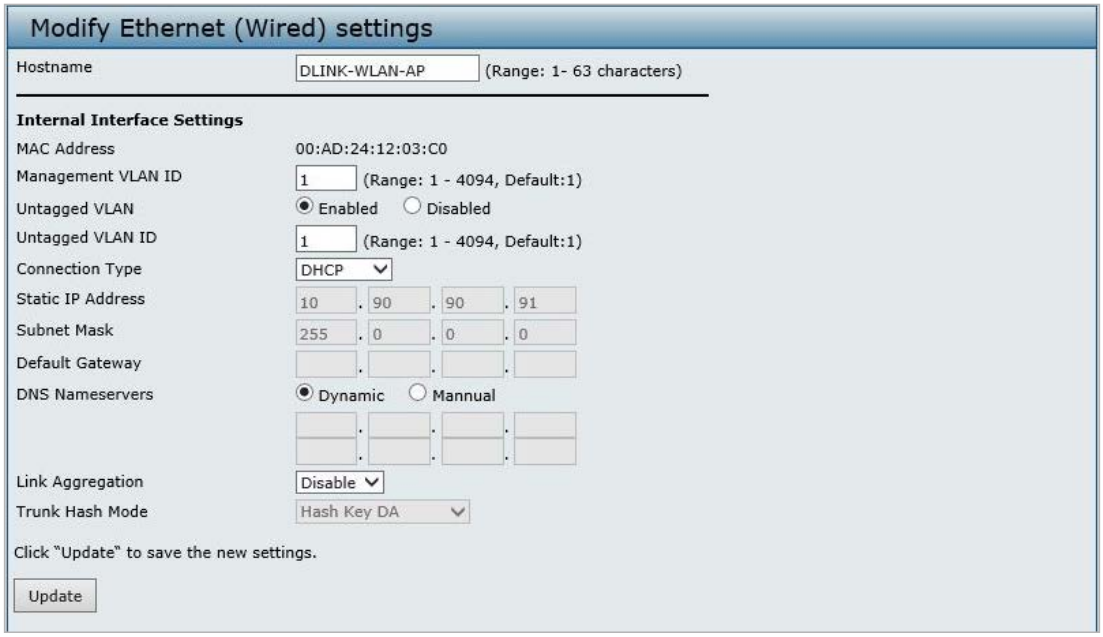
設定画面：[Manage] > [Ethernet Settings]

イーサネットの設定を行います。

初期設定では本製品上のDHCP クライアントは自動的にネットワーク情報に関する要求をブロードキャストします。
スタティックIP アドレスを使用する場合、DHCP クライアントを無効にして、手動でIP アドレスおよび他のネットワーク情報を設定する必要があります。
マネジメントVLAN は初期値でVLAN 1 のタグなしVLAN です。ネットワーク上に異なるVLAN ID を使用した管理用VLANが存在している場合は、アクセスポイントのマネジメントVLAN のVLAN ID を変更する必要があります。

重要

設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。
再起動が発生した場合、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが少ない時にアクセスポイントの設定変更を行うことをお勧めします。



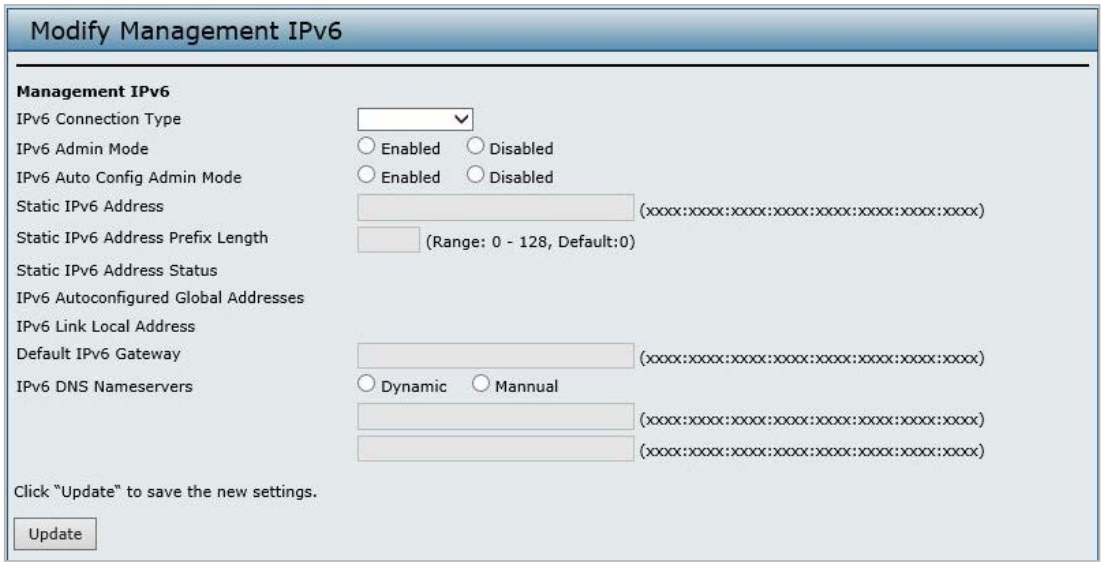
UI	説明
Hostname	アクセスポイントのホスト名を入力します。 ここで設定したホスト名はCLIのログインプロンプトで表示されます。 • 入力可能文字数：1-63 文字（半角英数字） • 入力可能な文字：英字（大文字小文字）、数字、および「-」（ダッシュ） • 条件：英字で開始し、英字または数字で終了する必要があります。
MAC Address	イーサネットポートのLAN インタフェースのMAC アドレスが表示されます。
Management VLAN ID	マネジメントVLANのIDを設定します。マネジメントVLANは、アクセスポイントへの接続に使用するIP アドレスに関連付けされているVLAN です。 • 初期値：1 • 設定可能範囲：1-4094
Untagged VLAN	タグなしVLANを有効または無効にします。 • [Enabled]：Untagged VLANを有効にします。 • [Disabled]：Untagged VLANを無効にします。すべてのトラフィックはVLAN ID でタグ付けされます。 デフォルトでは全てのトラフィックはタグなしのVLAN 1を使用します。 タグなしVLANを無効にして、トラフィックのタグなしVLAN IDを変更するか、RADIUSによるVAP/クライアントVLAN IDの変更が行われるまで、すべてのトラフィックはタグなしになります。

UI	説明
Untagged VLAN ID	タグなしVLANのIDを設定します。ここで設定するVLAN 上のトラフィックは、VLAN ID でタグ付けされません。 • 設定可能範囲：1-4094
Connection Type	接続タイプを設定します。 • [Static IP]：スタティック（固定）のIP アドレス、サブネットマスク、DNS、およびゲートウェイを使用します。 • [DHCP]：DHCP サーバから自動的にIP アドレス、サブネットマスク、DNS、およびゲートウェイ情報を取得します。
Static IP Address	IPアドレスを入力します。 接続タイプを[DHCP]に設定した場合は入力できません。
Subnet Mask	サブネットマスクを入力します。 接続タイプを[DHCP]に設定した場合は入力できません。
Default Gateway	デフォルトゲートウェイを入力します。 接続タイプを[DHCP]に設定した場合は入力できません。
DNS Nameservers	DNSのモードを選択します。 • [Manual]：固定のIP アドレスを使用します。 • [Dynamic]：DNS サーバのIP アドレスはDHCP を通じて自動的に割り当てられます。接続タイプを[Static IP]に設定した場合は選択できません。
Link Aggregation	リンクアグリゲーションを有効または無効にします。 • [Static]：スタティックリンクアグリゲーションを行います。 • [Disabled]：リンクアグリゲーションを無効にします。
Trunk Hash Mode	トランクハッシュモードを選択します。
Update	設定を適用します。

Management IPv6（IPv6設定）

設定画面：[Manage] > [Management IPv6]

IPv6アドレスの設定を行います。

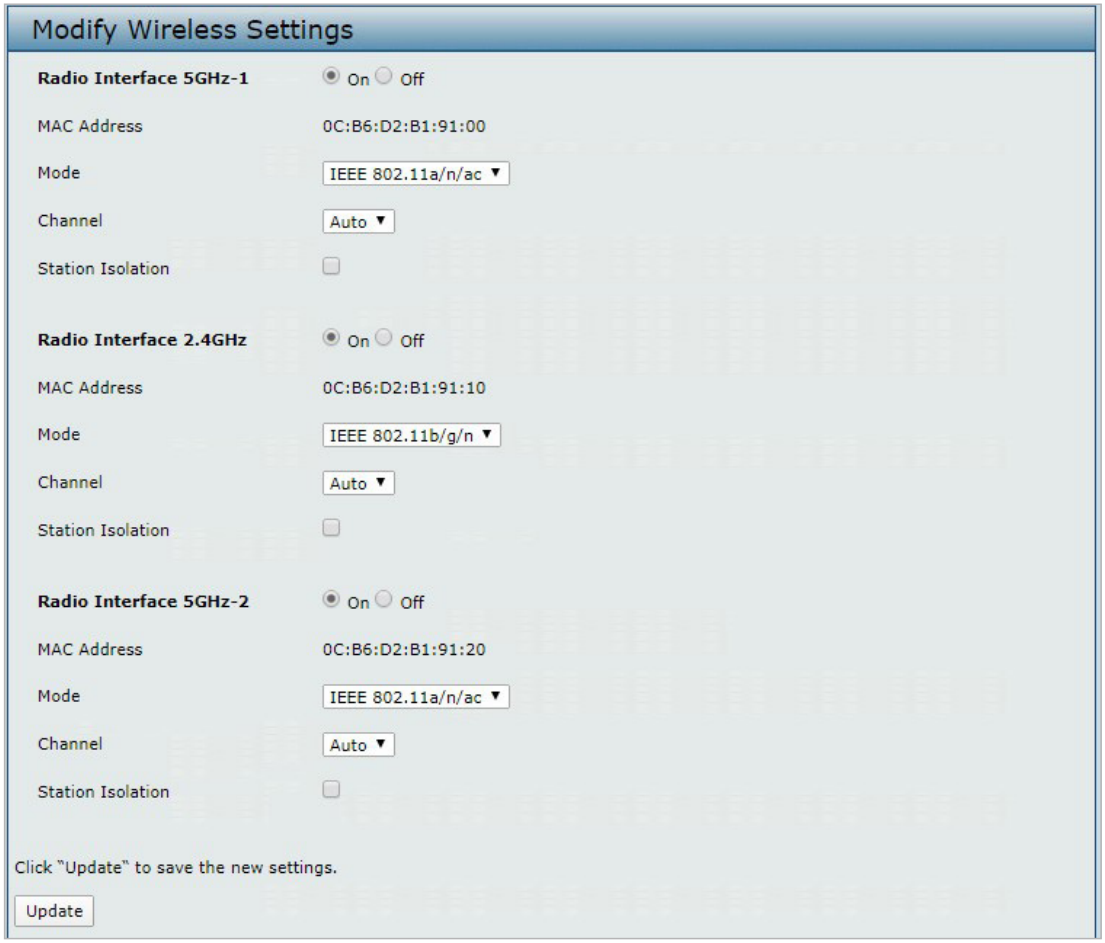


UI	説明
IPv6 Connection Type	接続タイプを設定します。 • [Static IPv6]：固定のIPv6 アドレスを使用します。 • [DHCPv6]：DHCPv6サーバから自動的にIPv6 アドレスを取得します。
IPv6 Admin Mode	アクセスポイントへのIPv6 管理アクセスを[Enabled]（有効）または[Disabled]（無効）にします。
IPv6 Auto Config Admin Mode	アクセスポイントへのIPv6 自動アドレス設定を[Enabled]（有効）または[Disabled]（無効）にします。 本設定を有効にした場合、LAN ポートで受信するルータ広告を処理することにより、自動IPv6 アドレス設定とゲートウェイ設定が行われます。アクセスポイントは、自動設定された複数のIPv6 アドレスを持つことができます。
Static IPv6 Address	スタティック（固定）のIPv6 アドレスを入力します。 接続タイプを[DHCPv6]に設定した場合は入力できません。
Static IPv6 Address Prefix Length	スタティックIPv6 のプレフィックス長を入力します。 接続タイプを[DHCPv6]に設定した場合は入力できません。 • 設定可能範囲：1-128
Static IPv6 Address Status	スタティックIPv6 アドレスのステータスが表示されます。
IPv6 Autoconfigured Global Addresses	自動的に1 つ以上のIPv6 アドレスをアクセスポイントに割り当てている場合に、アドレスが表示されます。
IPv6 Link Local Address	IPv6 Link Local アドレスを表示します。これは、ローカルな物理リンクによって使用されるIPv6 アドレスです。IPv6 Neighbor Discovery プロセスによって割り当てられるため、リンクローカルアドレスを設定することはできません。
Default IPv6 Gateway	デフォルトゲートウェイを入力します。 接続タイプを[DHCP]に設定した場合は入力できません。
IPv6 DNS Nameservers	DNS のモードを選択します。 • [Manual]：固定のIPv6アドレスを使用します。 • [Dynamic]：DNS サーバのIPv6 アドレスはDHCPv6 を通じて自動的に割り当てられます。 接続タイプを[Static IPv6]に設定した場合は選択できません。
Update	設定を適用します。

Wireless Settings（無線設定）

設定画面：[Manage] > [Wireless Settings]

無線の設定を行います。

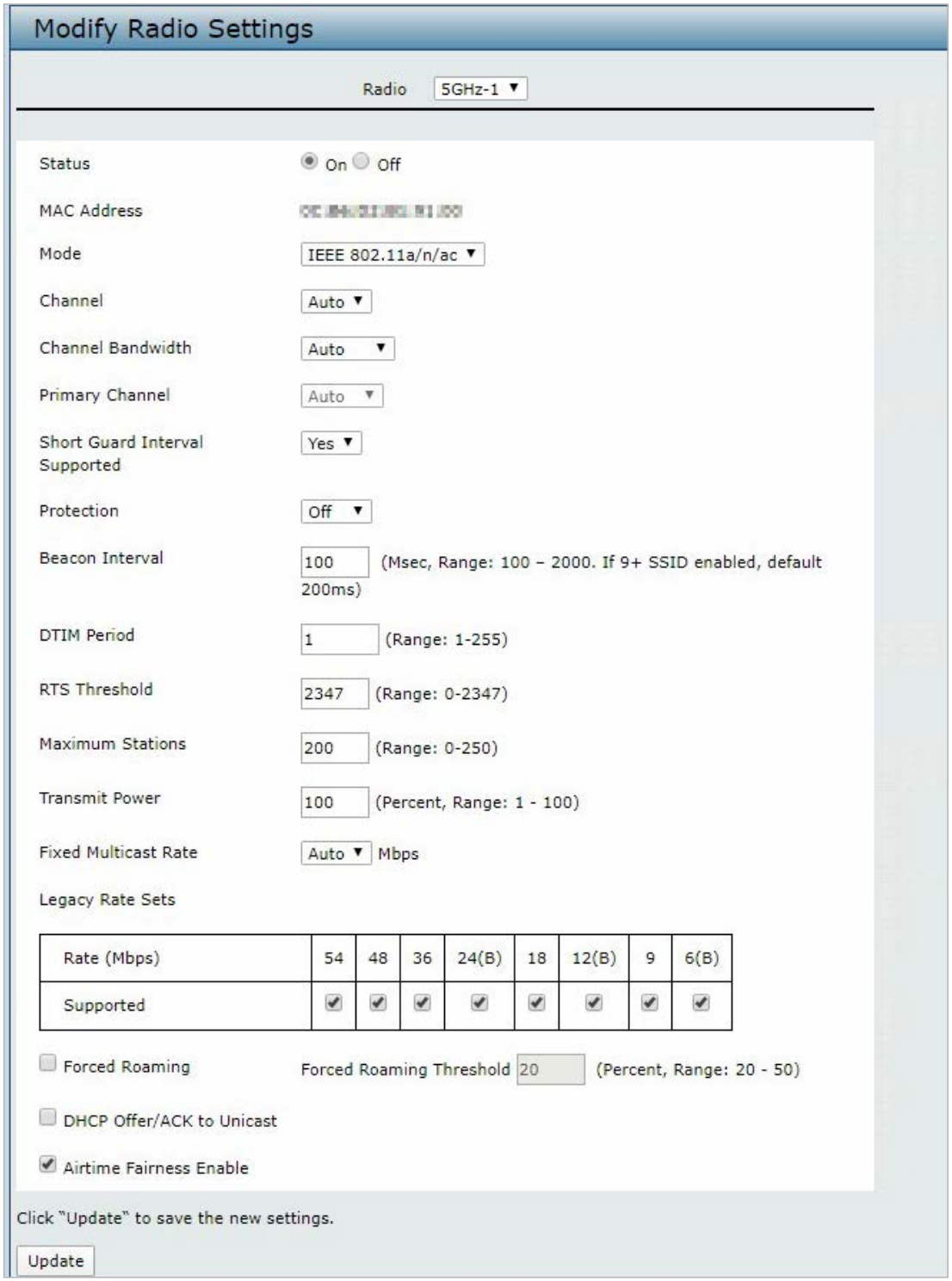


UI	説明
2.4GHz/ 5GHz-1/5GHz-2 Radio Interface	無線インタフェースを[On]（オン）または[Off]（オフ）にします。
MAC Address	無線インタフェースのMAC アドレスを表示します。周波数帯毎に固有のMACアドレスが設定されており、変更することはできません。
Mode	無線インタフェースのモードを選択します。 ここで選択したモードに対応しているクライアントのみが、無線インタフェースに接続できます。 •2.4GHz Radio Interface - 選択肢：[IEEE 802.11n] [IEEE 802.11b/g] [IEEE 802.11b/g/n] •5GHz-1/5GHz-2 Radio Interface - 選択肢：[IEEE 802.11a] [IEEE 802.11a/n] [IEEE 802.11n] [IEEE 802.11a/n/ac] [IEEE 802.11n/ac]
Channel	無線インタフェースのチャンネルを選択します。 利用可能なチャンネルの範囲は、無線インタフェースのモードによって異なります。 [Auto]を選択した場合、アクセスポイントは、チャンネルをスキャンして、利用可能なチャンネルを自動的に選択します。
Station Isolation	ステーションアイソレーションを有効または無効にします。チェックボックスにチェックを入れると有効になります。 • 無効にした場合： 無線クライアントは、通常通りアクセスポイントを経由してトラフィックを送信することで相互に通信できます。 • 有効にした場合： アクセスポイントは同じ周波数帯および同じVAPにある無線クライアント間の通信をブロックします。WDSリンクを経由した、異なるVAP上にあるクライアントとの通信についてはブロックしません。
Update	設定を適用します。

Radio（無線詳細設定）

設定画面：[Manage] > [Radio]

無線の詳細設定を行います。



UI	説明
Radio	設定する無線帯域を[5GHz-1] [5GHz-2] [2.4GHz]から選択します。
Status	無線インタフェースを[On]（オン）または[Off]（オフ）にします。
MAC Address	無線インタフェースのMAC アドレスを表示します。
Mode	無線インタフェースのモードを選択します。 ここで選択したモードに対応しているクライアントのみが、無線インタフェースに接続できます。 • 2.4GHz Radio Interface - 選択肢： [IEEE 802.11n] [IEEE 802.11b/g] [IEEE 802.11b/g/n] • 5GHz Radio Interface - 選択肢： [IEEE 802.11a] [IEEE 802.11a/n] [IEEE 802.11n] [IEEE 802.11a/n/ac] [IEEE 802.11n/ac]
Channel	無線インタフェースのチャンネルを選択します。 利用可能なチャンネルの範囲は、無線インタフェースのモードによって異なります。 [Auto]を選択した場合、アクセスポイントは、チャンネルをスキャンして、利用可能なチャンネルを自動的に選択します。
Channel Bandwidth	チャンネルの帯域幅を選択します。 802.11n規格では40MHz、802.11ac規格では80MHzまで利用可能ですが、その場合利用できるチャンネルは制限されます。
Primary Channel	プライマリチャンネルを選択します。 40MHzチャンネルは、周波数領域内で連続した2つの20MHzチャンネルから構成され、これらはプライマリ・セカンダリチャンネルとして扱われます。プライマリチャンネルは、20MHzのみサポートする802.11nクライアントやレガシークライアントで利用されます。 [Channel Bandwidth]を[40 MHz]に選択した場合のみ選択可能です。 • [Upper]：40MHz 帯域の上位20MHz のチャンネルとしてPrimary Channel を設定します。 • [Lower]：40MHz 帯域の下位20MHz のチャンネルとしてPrimary Channel を設定します。 • [Auto]：プライマリチャンネルを自動で設定します。
Short Guard Interval Supported	ショートガードインターバル機能を[Yes]（有効）または[No]（無効）にします。 ガードインターバルとは、送信されるシンボル（ビット）とシンボルの間に挿入される間隔のことであり、シンボル間干渉（ISI）やキャリア間干渉（ICI）を防止する機能です。 ショートガードインターバル機能を有効にすると、ガードインターバルを800ナノ秒から400ナノ秒へ短縮することができます。
Protection	保護機能を[Auto]（自動）または[Off]（オフ）にします。 保護が[Auto]の場合、アクセスポイントの適用範囲内にレガシーデバイスがあると、保護メカニズムが呼び出されます。保護を[Off]にすると、適用範囲内のレガシークライアントまたはアクセスポイントが802.11n 伝送によって影響を受けることがあります。 この設定はアクセスポイントに接続するクライアントの能力に影響しません。
Beacon Interval	ビーコンを送信する間隔を設定します。 ビーコンとは無線ネットワークを同期させるためにアクセスポイントから一定間隔で送信するパケットのことです。 • 選択可能範囲：100 - 2000（ミリ秒） • 初期値：100（ミリ秒） **⚠注意** • 100ms未満の値を入れた場合は無効になります。
DTIM Period	DTIM間隔を指定します。 DTIM（Delivery Traffic Information Map）メッセージは、ビーコンフレームに含まれる要素です。省電力モードの無線クライアントに対して、送信待ちのデータがあることを伝えます。 DTIM間隔を10に設定した場合は、10 回のビーコンフレーム送信に対して1 度DTIMメッセージが送信されます。 • 選択可能範囲：1-255

UI	説明
RTS Threshold	RTSしきい値を設定します。 送信データのサイズがRTSしきい値を上回る場合、RTS（Request To Send：送信要求）信号を送信します。RTSしきい値を低く設定すると、RTSパケットが高頻度で送信されネットワーク帯域を消費しますが、トラフィックの多いネットワークや電波障害の発生している状況においては、干渉や衝突を避けることができます。 • 選択可能範囲：0-2347
Maximum Stations	本アクセスポイントに一度にアクセスできるステーションの最大数を指定します。 • 選択可能範囲：0-250
Transmit Power	本アクセスポイントの送信電力レベルを設定します。 設定した数値が高いほど、アクセスポイントのブロードキャスト範囲が広くなります。 アクセスポイントの数や距離など、お使いの環境に適した値を指定してください。
Fixed Multicast Rate	アクセスポイントのマルチキャストトラフィック通信速度を選択します。
Legacy Rate Sets	APでサポートする送信レートセットにチェックを入れます。 • Rates：レート（Mbit/秒）を示します。 • Supported Rate Sets：APでサポートするレートを示します。複数のレートを指定することができます。チェックボックスをクリックして選択、または選択を解除します。APからのクライアント距離やエラーに基づいて、自動的に最も適切なレートが選択されています。 • （B）：ネットワーク上のクライアントステーションと通信を確立するために、APがネットワークにアドバタイズするレートを示します。通常、サポートされるレートセットのサブセットをブロードキャストすることが適切です。
Forced Roaming	本項目を有効にすると、クライアントRSSIに基づいて、無線クライアントを検出・切断します。クライアントRSSIがしきい値を下回ると、クライアントは切断されます。RSSIがしきい値を下回っている状態で接続の試行が継続された場合、4回目の試行後にアソシエーションが記録され接続されます。
DHCP Offer/ACK to Unicast	DHCP Offer/ACKのユニキャスト変換を[Enable]（有効）または[Disable]（無効）にします。
Airtime Fairness Enable	Airtime Fairness機能を有効化します。
Update	設定を適用します。

メモ

• Basic Rateの設定はできません。
• 同一周波数帯に 9つ以上の SSIDを設定すると Beacon Intervalの最小が200msになります。

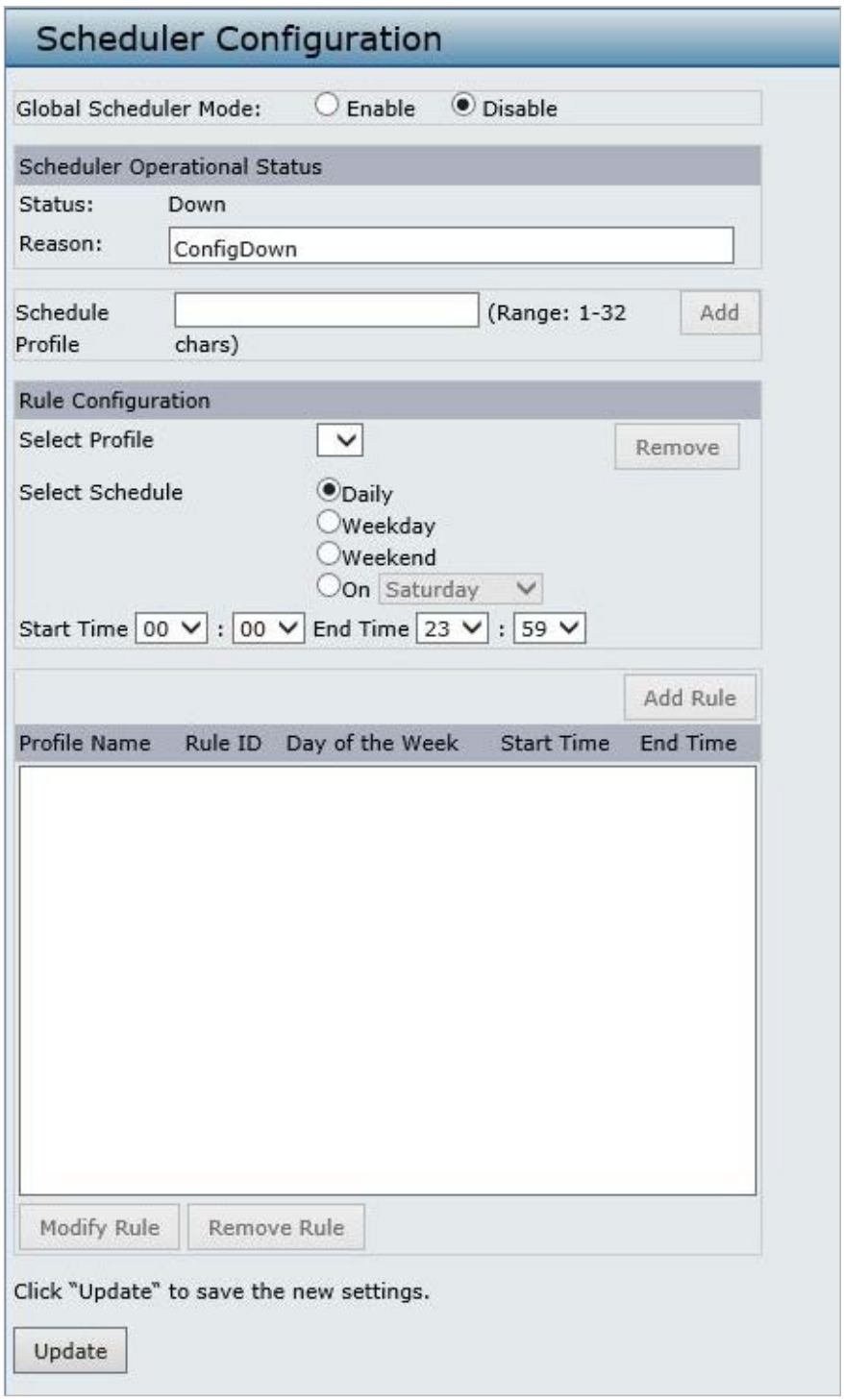
Scheduler Configuration（スケジューラの設定）

設定画面：[Manage] > [Scheduler]

スケジューラの設定を行います。
スケジューラはスタンドアロン使用時に利用できる機能です。無線を自動的に有効/無効にしたり、一日のうちの限られた時間のみ無線クライアントをVAP にアクセスさせたりすることができます。本機能により、セキュリティの向上や消費電力の抑制を実現します。

メモ

- プロファイルのルールで開始/終了時刻、曜日を設定します。このルールは定期的なスケジュールとして毎日あるいは毎週繰り返されます。
- 最大16個のプロファイルを作成することが可能です。



UI	説明
Global Scheduler Mode	スケジューラ設定を[Enable]（有効）または[Disable]（無効）にします。
Scheduler Operational Status	
Status	スケジューラ設定の状態（[Up]：有効、[Down]：無効）が表示されます。
Reason	ステータスの概要が表示されます。 • [IsActive]：スケジューラ設定が有効です。 • [ConfigDown]：スケジューラ設定が無効です。 • [TimeNotSet]：アクセスポイントの時刻が設定されていないため、スケジューラ設定は使用できません。 • [ManagedMode]：アクセスポイントが管理モードであるため、スケジューラ設定は使用できません。
Schedule Profile	プロファイル名を設定→[Add]をクリックして追加します。 プロファイルはVAPやRadioに紐付けることができます。最大16 個までのスケジューラプロファイル名を設定できます。 • 入力可能文字数：32 英数字
Rule Configuration	
プロファイルに適用するルールを設定します。 ルールを修正する場合は[Modify]、ルールを削除する場合は[Remove]をクリックします。	
Select Profile	プロファイルを選択します。[Remove]をクリックするとプロファイルを削除できます。
Select Schedule	日（曜日）を選択します。 • 選択肢： [Daily]（毎日）、[Weekday]（月～金）、[Weekend]（土日）、[On]（曜日を選択）
Start Time	無線/VAP が有効となる時間の開始時刻を選択します。 「時時：分分」の24 時間方式です。<00-23>：<00-59> から設定します。
End Time	無線/VAP が有効となる時間の終了時刻を選択します。 「時時：分分」の24 時間方式です。<00-23>：<00-59> から設定します。
Add Rule	設定した時間帯のルールをプロファイルに追加します。
Modify Rule	指定したルールを編集します。
Remove Rule	指定したルールをプロファイルから削除します。
Update	設定を適用します。

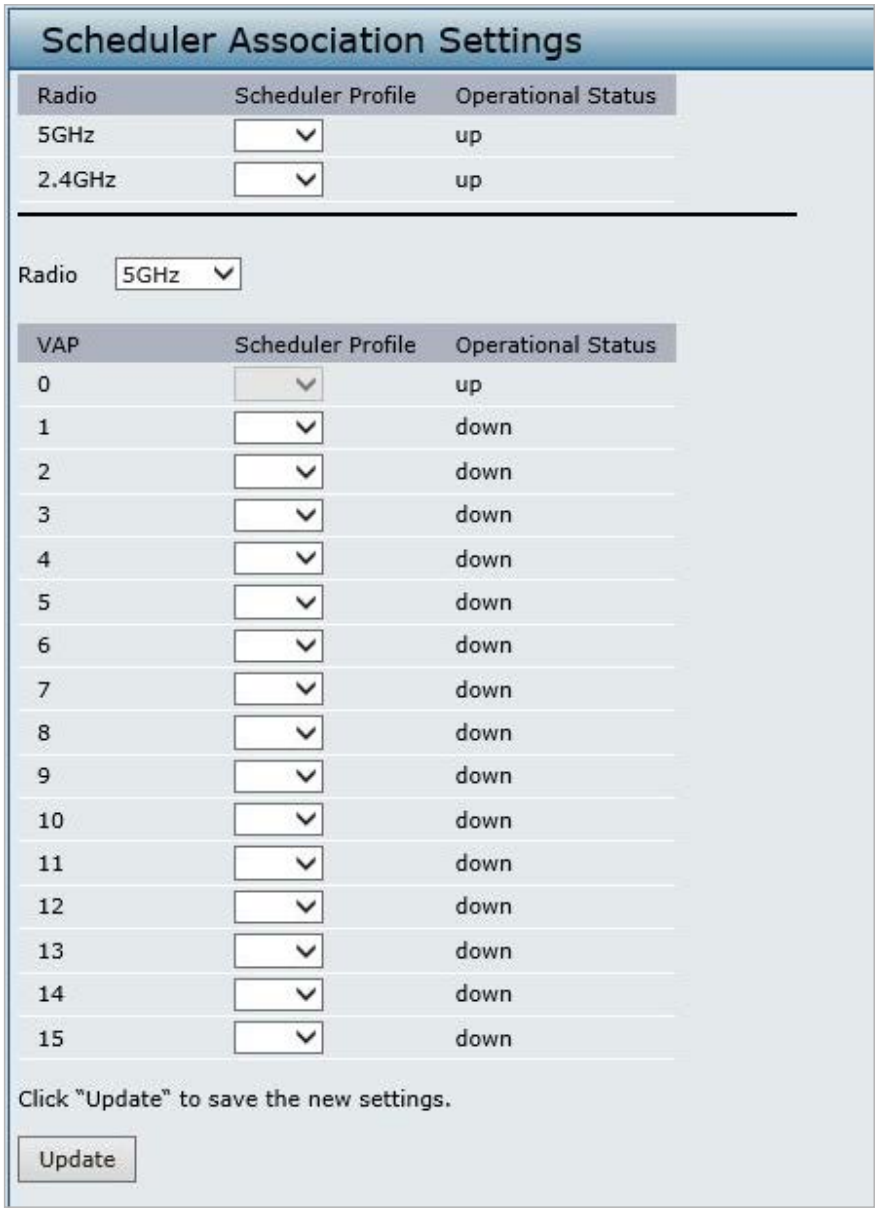
メモ

アクセスポイントの時間設定については、『Time Settings（時間設定）：p.68 』を参照してください。

Scheduler Association Settings（スケジューラ関連設定）

設定画面：[Manage] > [Scheduler Association]

スケジューラプロファイルを無線またはVAP と連携させます。



UI	説明
無線とスケジューラプロファイルを連携させます。	
Radio	2.4GHzまたは5GHzの帯域を設定します。
Scheduler Profile	無線と連携させるスケジューラプロファイルを選択します。
Operational Status	スケジューラ設定の状態（[up]：有効、[down]：無効）が表示されます。
VAPとスケジューラプロファイルを連携させます。	
2.4GHz /5GHz VAP	VAPが表示されます。
Scheduler Profile	VAPと連携させるスケジューラプロファイルを選択します。
Operational Status	スケジューラ設定の状態（[up]：有効、[down]：無効）が表示されます。
Update	設定を適用します。

VAP（仮想アクセスポイントの設定）

[Manage] > [VAP（SSID）]

VAP（仮想アクセスポイント）の設定を行います。

イーサネットのVLAN と同様に、無線LAN はVAP により複数のブロードキャストドメインに分割することができます。VAP は1 つの物理的なアクセスポイントに複数のアクセスポイントをシミュレートします。各無線帯域は最大16 個のVAP をサポートしています。

各VAP に対して、無線クライアントアクセスを制御するためにセキュリティモードをカスタマイズすることができます。また、各VAP は固有のSSID を持つことができます。個別にSSIDを設定することによって、ネットワーク上の他のシステムからは1台のアクセスポイントが2台以上のアクセスポイントから構成されているように見えます。

VAP を設定することで、ブロードキャストやマルチキャストのトラフィック管理が容易になり、ネットワークのパフォーマンスも向上します。

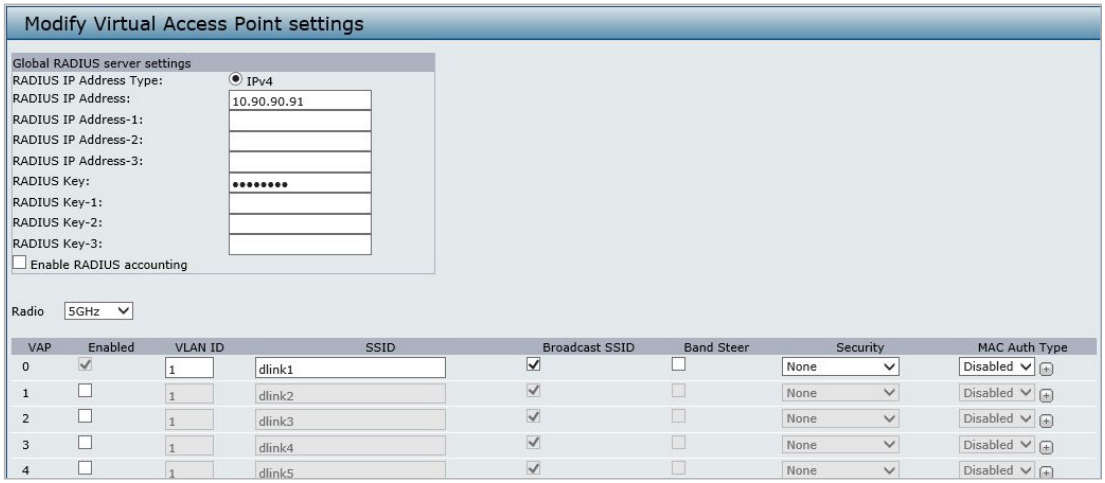
VLANの周波数帯に関わらず、各VAPで異なるVLANを使用したり、複数のVAPで同じVLANを使用したりすることが可能です。VAP0 は、デフォルトVLAN1 に割り当てられます。

アクセスポイントは、VAP画面で設定するVLAN ID に基づいて、または、RADIUS サーバの割り当てを使用して無線クライアントトラフィックにVLAN ID タグを追加します。外部のRADIUS サーバを使用する場合、各VAP で複数のVLAN を設定することができます。外部のRADIUS サーバは、無線クライアントが接続し認証を行う場合に、その無線クライアントをVLAN に割り当てます。

最大4 つのグローバルなRADIUS サーバを設定することができます。サーバの1 つはプライマリとして常に機能し、他のサーバはバックアップサーバとして機能します。ネットワークタイプ（IPv4）とアカウンティングモードは、すべての定義済みRADIUS サーバで共通です。各VAP でグローバルなRADIUS サーバを使用するように設定することができます。また、VAP毎に異なるRADIUS サーバ設定を行うことも可能です。
無線クライアントがRADIUS サーバと通信しないセキュリティモードを使用している場合、またはRADIUS サーバがVLAN情報を提供しない場合、各VAP にVLAN ID を割り当てることができます。アクセスポイントはそのVAP を通じてアクセスポイントに接続するすべての無線クライアントにVLAN を割り当てます。

重要

アクセスポイントにVLAN を設定する前に、アクセスポイントが使用するスイッチとDHCP サーバが、IEEE 802.1Q VLANのカプセル化をサポートしていることを必ず確認してください。



UI	説明
RADIUS IP Address Type	RADIUS サーバが使用するIP バージョンを指定します。
RADIUS IP Address	プライマリグローバルRADIUS サーバのIPアドレスを入力します。 初期値では、グローバルRADIUS 設定が各VAPで使用されます。
RADIUS IP Address 1-3	バックアップRADIUS サーバとして使用する最大3 個のIPアドレスを入力します。 プライマリサーバへの認証が失敗した場合、各バックアップサーバに対して順番に試行が行われます。
RADIUS Key	RADIUS キーを入力します。 RADIUS キーは、グローバルRADIUS サーバ用の共有秘密鍵です。63 文字以内の半角英数字および特殊文字を使用できます。キーは大文字と小文字を区別しており、アクセスポイントとRADIUS サーバに同じキーを設定する必要があります。入力した文字は「●●●」と表示されます。

UI	説明
RADIUS Key1-3	設定済みのバックアップRADIUS サーバに関連付けるRADIUS キーを入力します。 RADIUS IP Address-1 のキーはRADIUS Key-1、RADIUS IP Address-2 のキーはRADIUS Key-2 というように対応します。
Enable RADIUS accounting	RADIUS アカウンティングを有効にします。 有効にすると、システム時間、送受信したデータ量など、特定のユーザのリソース使用状況を追跡して測定します。プライマリRADIUSサーバとすべてのバックアップサーバに対して有効になります。
2.4GHz/5GHz	
VAP	各無線インタフェースに16 個までのVAP を設定できます。 VAP0 が物理的な無線インタフェースであるため、VAP0 を無効にするためには、無線インタフェースを無効にする必要があります。
Enabled	有効化するネットワークにチェックを入れます。特定のネットワークを無効にすると、入力したVLAN ID は失われます。
VLAN ID	VLAN IDを入力します。 • 設定可能範囲：1-4094 タグなしVLAN IDが設定されるか、RADIUSサーバによる無線クライアントのVLAN への割り当てが行われる場合を除き、無線クライアントがこのVAP を使用してアクセスポイントに接続する際に、無線クライアントの全てのトラフィックに対して、指定のVLAN ID をタグ付けします。 RADIUS認証を使用する場合、RADIUSまたはAAAサーバ上のファイルに次の属性を追加して、VLANを設定することも可能です。 • Tunnel-Type • Tunnel-Medium-Type • Tunnel-Private-Group-ID RADIUS によって割り当てられたVLAN ID は、「VAP」画面で設定するVLAN ID を上書きします。 Ethernet Settings画面でタグなし、管理VLAN ID を設定することも可能です。 詳細は『Ethernet Settings（イーサネット設定）：p.35 』を参照してください。
SSID	SSID（無線ネットワークの名称）を入力します。 • 入力可能文字数：最大32 文字（半角英数字） 複数のVAP に同じSSID を使用することができます。または、各VAP に固有のSSID を指定することもできます。 無線クライアントとして、管理しているアクセスポイントと同じアクセスポイントに接続する場合、SSID をリセットするとアクセスポイントへ接続性を失います。この新しい設定を保存した後に新しいSSID に再接続する必要があります。
Broadcast SSID	アクセスポイントがビーコンフレーム内のSSID をブロードキャストするかどうかを指定します。 初期値ではBroadcast SSID は有効です。VAP がSSID をブロードキャストしないと、クライアントステーション上の「使用可能ネットワークリスト」にネットワーク名が表示されなくなります。その場合、クライアントは接続前に、サプリカントに接続する相手の正しいネットワーク名を登録する必要があります。 ブロードキャストSSIDを無効にすると、クライアントが誤ってネットワークに接続してしまうことを避けることができますが、開かれたネットワーク（ゲストネットワークなど）に対するセキュリティ保護としては低いレベルのものです。
Band Steer	バンドステアリング（5GHz優先）機能を有効または無効にします。
Security	このVAP に対して以下のセキュリティモードから一つ選択します。 • [None] • [WPA Personal] • [WPA Enterprise] • [OWE] [None]以外のセキュリティモードを選択すると、新しい欄が表示されます。 詳細は『Security 設定について：p.47 』を参照してください。
MAC Auth Type	ネットワークへのアクセスを許可または拒否するMAC アドレスのグローバルなリストを設定することができます。プルダウンメニューで、使用するMAC 認証のタイプを選択します。 MAC認証については、『MAC Authentication（MAC 認証によるアクセス制御）：p.53 』を参照してください。 • [Disabled]：MAC 認証を行いません。 • [Local]：MAC Authentication画面で設定したMAC 認証リストを使用します。 • [Radius]：外部RADIUS サーバのMAC 認証リストを使用します。
Update	設定を適用します。

重要

設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。
再起動が発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが少ない時にアクセスポイントの設定変更を行うことをお勧めします。

メモ

OWEは本ファームウェアバージョン（4.7.2.9）ではサポートされません。

■Security 設定について

● NONE

[Security]で[None]を選択すると、そのアクセスポイントに対してそれ以上の設定は不要です。
本モードでは、アクセスポイントへの（からの）データ転送には暗号化が行われません。
本セキュリティモードは初期のネットワーク設定時、または問題解決時の使用に便利です。しかし、本モードの選択は、安全性が極めて低いため、内部用ネットワークでの通常使用にはお勧めできません。

● WPA Personal

WPA Personal はWi-Fi Alliance により発表されたIEEE 802.11i の規格で、AES-CCMP およびTKIP というメカニズムを採用しています。
WPA PersonalはWPA Enterprise で使用する「IEEE 802.1X」や「EAP」の代わりに、「Pre-shared Key」（事前共有鍵）を使用します。PSK は証明書の初期チェックだけに使用されます。
このセキュリティモードは、オリジナルのWPA をサポートする無線クライアントと下位互換性を持っています。

以下の画面で設定を行います。

UI	説明
WPA Versions	サポートするクライアントステーションのWPA タイプを選択します。 • [WPA-TKIP] • [WPA2-AES] • [WPA3]
Key	Pre-shared Key を入力します。 Pre-shared Key は、WPA パーソナルで使用する共有秘密鍵です。 • 入力可能文字数：8 -63文字（半角英数字） アルファベットの大文字、小文字、数字、および@# などの記号が入力できます。 HEX64文字は使用できません。
WPA3 Key	WPA3 Keyを入力します。 本項目は[WPA3]を選択した場合に表示されます。
Broadcast Key Refresh Rate	このVAP に接続するクライアントが使用するブロードキャスト（グループ）キーの更新間隔時間を入力します。0 に設定した場合、ブロードキャストキーは更新されません。 • 設定可能範囲：0-86400（秒） • 初期値：3600（秒）

メモ

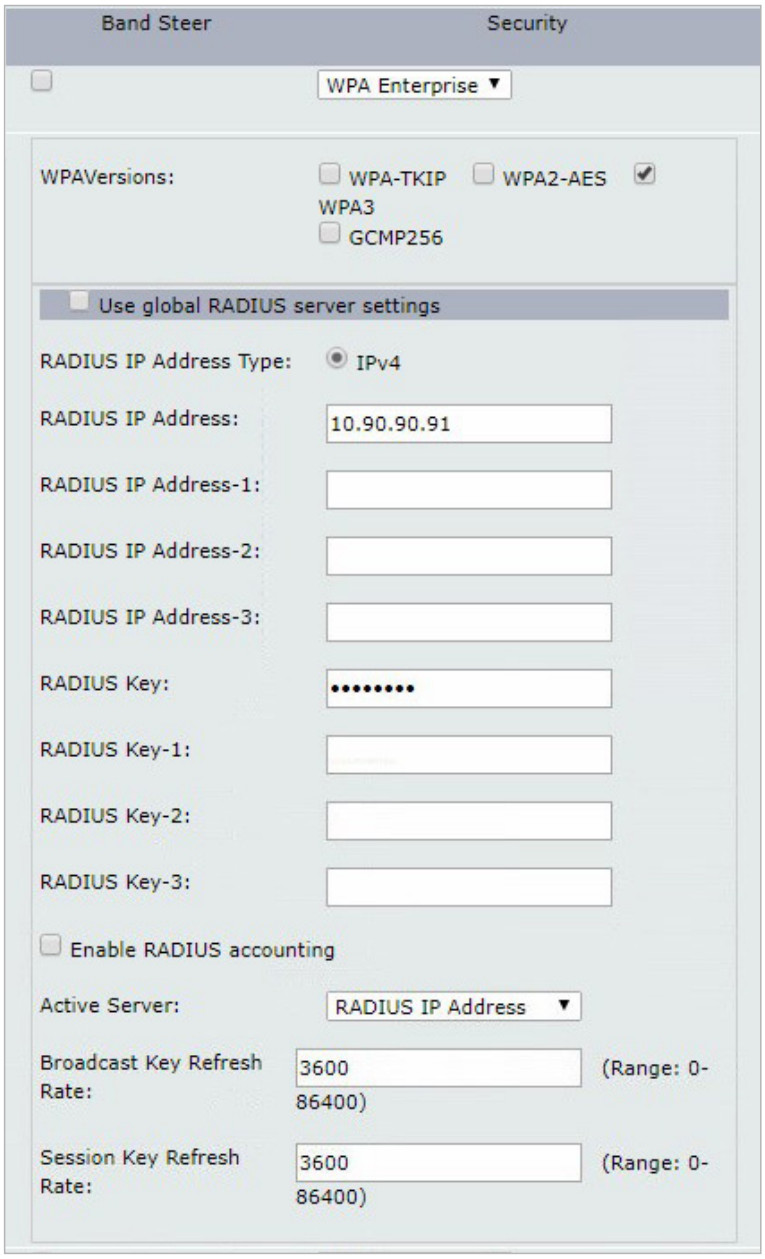
[WPA-TKIP]のみを選択して[WPA2-AES]を無効にすることはできません。

● WPA Enterprise

WPA EnterpriseはWi-Fi AllianceのIEEE 802.11i標準に準拠した規格です。
CCMP（AES）、TKIP、GCMP256（WPA3選択時のみ）というメカニズムを採用しています。

Enterprise モードでは、ユーザを認証するためにRADIUS サーバの使用を必要とします。
このセキュリティモードはオリジナルのWPA をサポートする無線クライアントと下位互換性があります。

以下の画面で設定を行います。



UI	説明
WPA Versions	サポートするクライアントステーションのWPA タイプを以下から選択します。 • [WPA-TKIP] • [WPA2-AES] • [WPA3] • [GCMP256] [GCMP256]は[WPA3]を選択した場合にのみ表示されます。
Use global radius server settings	チェックを入れるとグローバルRADIUSサーバ設定が有効になります。 グローバルRADIUSサーバ設定が有効である場合、各VAPは「VAP」画面（『VAP（仮想アクセスポイントの設定）：p.45 』）の1番目で定義するグローバルなRADIUS 設定を使用します。 各VAP で個別のRADIUS サーバを使用するには、チェックボックスのチェックを外し、RADIUS サーバのIP アドレスを設定してください。
RADIUS IP Address Type	RADIUS サーバが使用するIP バージョンを指定します。
RADIUS IP Address	プライマリグローバルRADIUS サーバのIPアドレスを入力します。 初期値では、グローバルRADIUS 設定が各VAPで使用されます。
RADIUS IP Address 1-3	バックアップRADIUS サーバとして使用する最大3 個のIPアドレスを入力します。 プライマリサーバへの認証が失敗した場合、各バックアップサーバに対して順番に試行が行われます。
RADIUS Key	RADIUS キーを入力します。 • 入力可能文字数：最大63文字（半角英数字および特殊文字） RADIUS キーは、グローバルRADIUS サーバ用の共有秘密鍵です。 キーは大文字と小文字を区別しており、アクセスポイントとRADIUS サーバに同じキーを設定する必要があります。入力した文字は「●●●」と表示されます。
RADIUS Key1-3	設定済みのバックアップRADIUS サーバに関連付けるRADIUS キーを入力します。 RADIUS IP Address-1 のキーはRADIUS Key-1、RADIUS IP Address-2 のキーはRADIUS Key-2 というように対応します。
Enable RADIUS accounting	RADIUS アカウンティングを有効にします。 有効にすると、システム時間、送受信したデータ量など、特定のユーザのリソース使用状況を追跡して測定します。また、プライマリRADIUSサーバとすべてのバックアップサーバに対して有効になります。
Active Server	アクティブにするRADIUS サーバ（Radius IP Address、Radius IP Address-1、Radius IP Address-2、Radius IP Address-3）を選択します。
Broadcast Key Refresh Rate	このVAP に接続するクライアントが使用するブロードキャスト（グループ）キーの更新間隔時間を入力します。0 に設定した場合、ブロードキャストキーは更新されません。 • 設定可能範囲：0-86400（秒） • 初期値：3600（秒）
Session Key Refresh Rate	このVAP に接続する各クライアントが使用するセッション（ユニキャスト）キーの更新間隔時間を入力します。0 に設定した場合、ブロードキャストキーは更新されません。 • 設定可能範囲：0-86400（秒） • 初期値：3600（秒）

メモ

- WEPはサポートされていません。DWC-2000にて管理する際は、staticWEPのみ設定可能です。（1xWEPは不可となります）。
- ［WPA-TKIP]のみを選択して［WPA2-AES]を無効にすることはできません。

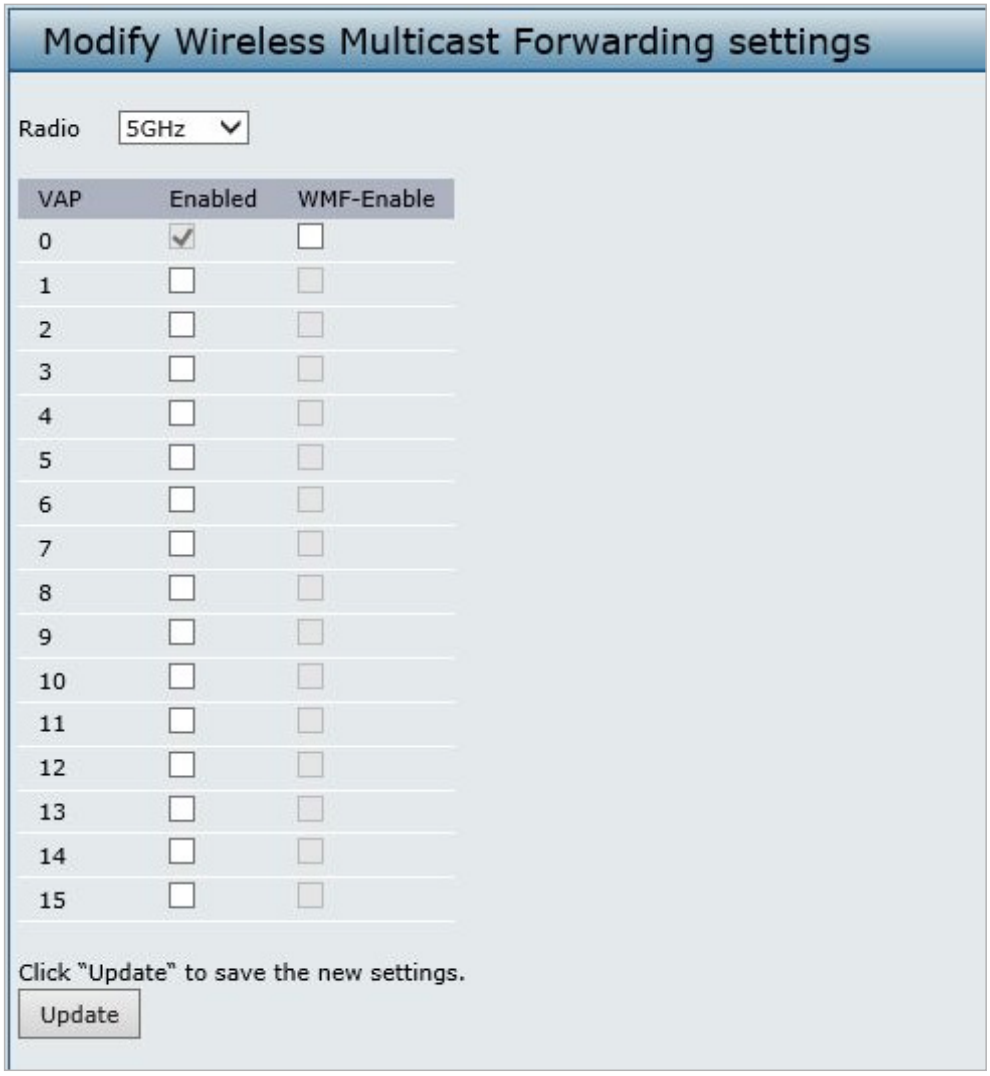
Wireless Multicast Forwarding（無線マルチキャストフォワーディング設定）

設定画面：[Manage] > [Wireless Multicast Forwarding]

無線マルチキャストフォワーディング（WMF）は、無線メディア上のマルチキャストトラフィックを転送する上で有用な機能です。マルチキャストフレームをユニキャストとして複数の送信先に転送することで、WLAN上のマルチキャスト転送時の問題を回避することができます。

本機能では、IGMPフレームによって参加グループメンバを把握し、ユニキャストMAC変換後、マルチキャストパケットが関連するメンバのみに対して転送されるようにします。

WMFを使用すると、フレームはユニキャストとして送信され、リンクエラーやノイズ状態に応じたステーション毎の動的なレート制御によってロバスト転送が可能になるため、データ転送の信頼性を高めることができます。
マルチキャストグループメンバはSTAエンドポイントとしても動作し、STAデバイス間のストリーミングもサポートされます。
マルチキャストストリーミングサーバはいずれのLANポートにも接続することができます。



UI	説明
Radio	設定する無線帯域を5GHzまたは2.4GHzから選択します。
Enabled	設定するネットワークを有効または無効にします。ネットワークを無効化した場合、有効化されたVLAN IDは利用不可となります。
WMF-Enable	各VAPのWMF機能を有効または無効にします。
Update	設定を適用します。

WDS（WDS の設定）

設定画面：[Manage] > [WDS]

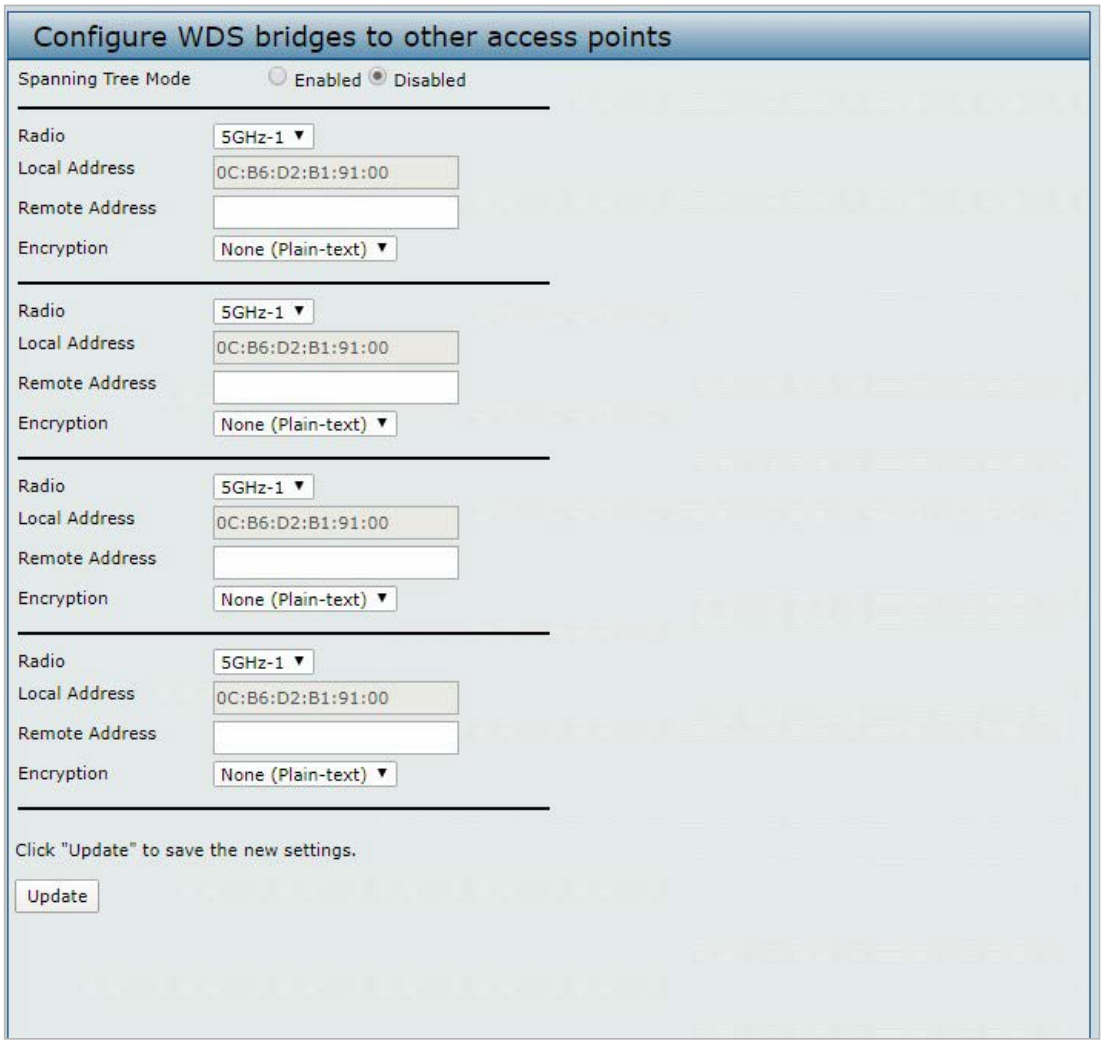
WDS（Wireless Distribution System）の設定を行います。
WDS を使用すると、標準化された方式により、ケーブルを使用せずにアクセスポイント同士で通信を行うことができます。この機能は、シームレスなクライアントのローミングや複数の無線ネットワーク管理を行うために重要です。
また、必要とされるケーブル接続数を削減することで、ネットワーク構造を簡素化することもできます。接続するリンク数に基づいて、ポイントツーポイントまたはポイントツーマルチポイントのブリッジモードでアクセスポイントを設定することができます。

ポイントツーポイントモードでは、アクセスポイントは、クライアントの接続を許可して無線クライアントや他のアクセスポイントと通信を行います。他のネットワークに向かうすべてのトラフィックは、アクセスポイント間で確立されるトンネルを経由して転送されます。

ポイントツーマルチポイントブリッジモードでは、1 つのアクセスポイントが複数のアクセスポイント間で通常のリンクとして機能します。このモードでは、中央のアクセスポイントは、クライアントの接続を許可して無線クライアントや他のアクセスポイントと通信を行います。それ以外のアクセスポイントは、ルーティングの目的のために適切な無線ブリッジにパケットを送信する中央のアクセスポイントとだけ接続します。

重要

- アクセスポイントをスタンドアロンモードから管理モードに移行させると、WDS は無効になります。
  管理モードでは、D-Link 統合コントローラを使用することによって、アクセスポイントを設定します。アクセスポイントが管理モードの場合、Web マネージャ、Telnet、SSH、およびSNMP アクセスは無効となります。
- 異機種間、異なるファームウェアバージョン間でWDS モードを使用することはできません。
- WDS利用時、有線側からの VLANタグ付きパケットはドロップされます。
- WDSをループ構成で使用することはできません。



アクセスポイントにWDS を設定する前に、以下のガイドラインに注意してください。

- WDS機能を使用する場合は、WDSリンクに参加する両方のアクセスポイントでWDS設定が行われていることを確認してください。
- アクセスポイントのペア間では1つのリンクのみ持つことができます。つまり、リモートMAC アドレスは特定のアクセスポイントのWDS 画面に一度だけ表示される可能性があります。
- WDS リンクに参加する両方のアクセスポイントが、同じ無線チャンネルにあり、同じIEEE 802.11 モードを使用する必要があります。(無線モードとチャンネルの設定に関する情報については、『Radio (無線詳細設定) : p.39 』を参照してください。)

UI	説明
Spanning Tree Mode	スパニングツリーを[Enabled] (有効) または[Disabled] (無効) にします。 スパニングツリープロトコル (STP) は、スイッチングのループを防ぎます。 WDS リンクを設定する場合は有効にすることをおすすめします。
Radio	２つの無線帯域を持つアクセスポイントにおける各WDS リンクに対して、[2.4G]または[5G]を選択します。無線帯域により、参照される[Local Address]は変わります。
Local Address	本アクセスポイントのMAC アドレスを示します。 ２つの無線帯域上の各WDSリンクについて、[Local Address]は選択された無線帯域上の内部インタフェースのMAC アドレスを反映します。
Remote Address	送信先アクセスポイントのMAC アドレスを指定します。 データの送信/ハンドオフ及び受信が行われる、WDSリンクの一端となるアクセスポイントを指します。
Encryption	WDS リンクで使用する暗号化のタイプを以下から選択します。 • [None (Plain-text)] : 暗号化を行いません。 • [WPA] : WPA2により、CCMPで暗号化を行います。
Update	設定を適用します。

重要

- WDSリンクを無効にするには、[Remote Address]欄に設定した値を削除する必要があります。
- 設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。
  これが発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが低い時にアクセスポイントの設定変更を行うことをお勧めします。

MAC Authentication（MAC 認証によるアクセス制御）

設定画面：[Manage] > [MAC Authentication]

本画面ではMACアドレス認証によるアクセス制御設定を行います。

MAC（Media Access Control）アドレスは、ネットワーク上の各ノードを特定するハードウェアアドレスです。通常、「:」（コロン）で区切られた12 個の16 進数（例00:DC:BA:09:87:65）として表されます。無線クライアントで使用される無線インタフェースカード（NIC）毎に固有のMACアドレスが付与されています。

無線クライアントのMAC アドレスに基づいてアクセスポイント経由でネットワークへのアクセスを制御するために、アクセスポイントのWeb マネージャを使用するか、または外部のRADIUS サーバを使用することができます。本機能は、MAC 認証またはMAC フィルタリングと呼ばれます。
アクセスを制御するためには、アクセスポイント上、または外部RADIUS サーバ上にMAC アドレスのステーションリストをに設定します。これらのMAC アドレスを持つクライアントネットワークへのアクセスを許可または拒否するかどうかを指定するフィルタを設定することができます。
無線クライアントがアクセスポイントへ接続しようとすると、アクセスポイントは"ローカル"または"RADIUS サーバ"上のステーションリストにあるクライアントのMAC アドレスを検索し、接続の許可または拒否を行います。

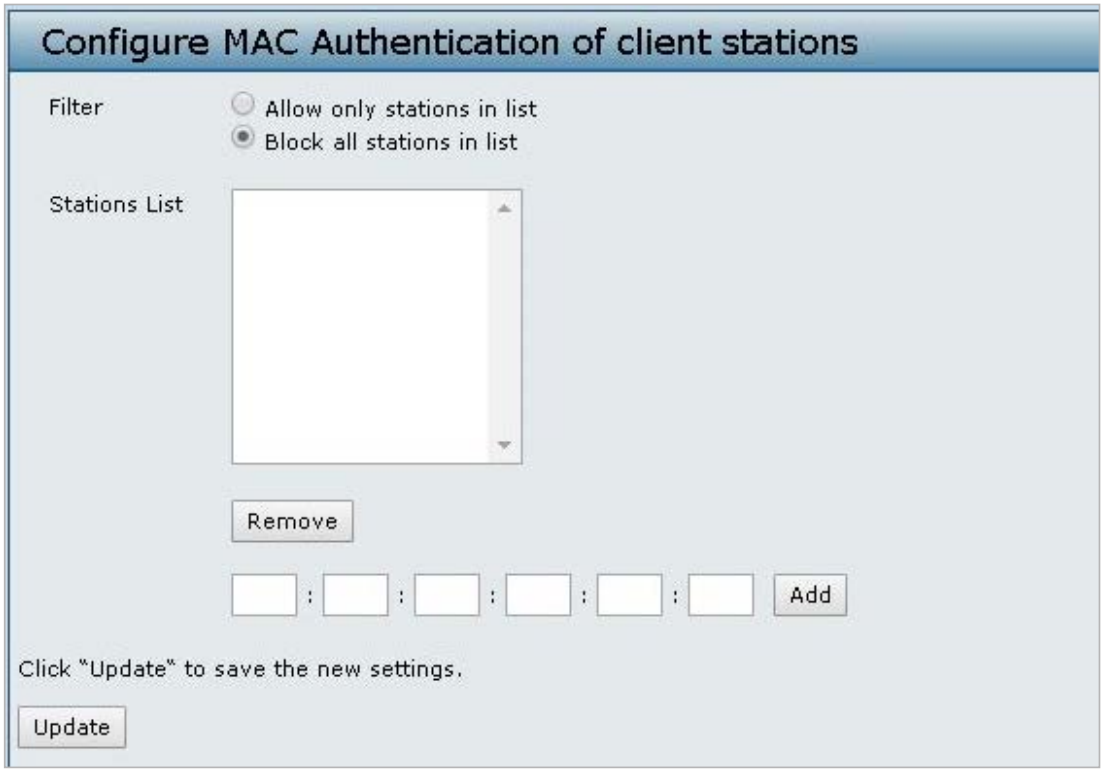
[VAP]画面の[MAC Auth Type]設定では、アクセスポイントが[MAC Authentication]画面で設定したステーションリストを使用するか、またはRADIUS サーバに設定されているステーションリストを使用するかを決定します。
MAC Authentication画面の[Allow/Block]設定は、ステーションリスト（localまたはRADIUS）内のクライアントがアクセスポイントを通じてネットワークにアクセスできるかどうかを決定します。
[VAP]画面のMAC 認証タイプの設定については『VAP（仮想アクセスポイントの設定）：p.45 』を参照してください。

■アクセスポイントにMAC フィルタとステーションを設定する

MAC アドレスに基づいたアクセスポイントへのアクセス制御を行います。フィルタの設定内容に基づいて、リストにあるMAC アドレスを持つクライアントステーションだけを許可するか、またはリストにあるステーションへのアクセスを拒否することができます。

重要

グローバルなMAC 認証設定はすべての無線帯域にあるすべてのVAP に適用されます。



UI	説明
Filter	フィルタリングの方式を以下から選択します。 • [Allow only stations in list]：ステーションリストにあるクライアントは、アクセスポイントを通じたネットワークへの接続を許可されます。 • [Block all stations in list]：ステーションリストにあるクライアントは、アクセスポイントを通じたネットワークへの接続を拒否されます。 本設定は、ローカル/RADIUSサーバ上いずれのステーションリストにも適用されます。
Stations List	ローカル上のステーションリストが表示されます。 VAP に対するMAC 認証タイプがLocalに設定されている場合、本リストを使用してクライアントのアクセスを許可/拒否します。VAP に対するMAC 認証タイプがRADIUS に設定されている場合、アクセスポイントは、このリストに設定されているMAC アドレスを無視して、RADIUS サーバに保存されているリストを使用します。
Remove	ステーションリストからクライアントを削除します。
Add	左の欄にMACアドレスを入力し、ステーションリストに追加します。
Update	設定を適用します。

重要

設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。
再起動が発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが少ない時にアクセスポイントの設定変更を行うことをお勧めします。

■RADIUS サーバにMAC 認証を設定する

MAC ベースのアクセス制御にRADIUS MAC 認証を使用する場合、RADIUS サーバにステーションリストを設定する必要があります。ステーションリストにはクライアントのMAC アドレスエントリが含まれます。

リストの形式について以下の表で説明します。

RADIUS サーバ属性	説明	値
User-Name（1）	クライアントステーションのMAC アドレス。	有効なイーサネットMACアドレス。
User-Password（2）	クライアントのMAC エントリ検索に使用する固定のグローバルパスワード。	NOPASSWORD

Load Balancing（ロードバランシングの設定）

設定画面：[Manage] > [Load Balancing]

ネットワーク利用率のしきい値を設定し、クライアントがアクセスポイントに接続または接続を解除する場合に無線ネットワークの速度と性能を維持することができます。
ロードバランシング設定は両方の無線帯域に適用されます。
ロードバランシングを設定し、アクセスポイントの定義済みの稼動率によって起動されるように制限と動作を設定します。

UI	説明
Load Balancing	ロードバランシングを[Enabled]（有効）または[Disabled]（無効）にします。
Utilization for No New Associations	無線帯域で許可されるネットワーク帯域幅利用率（%）を設定します。 この値を超えた場合、アクセスポイントは新しいクライアントの接続の受け入れを停止します。 0に設定した場合はロードバランシングが無効となります。
Update	設定を適用します。

重要

設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。
これが発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが低い時にアクセスポイントの設定変更を行うことをお勧めします。

Managed Access Point（管理アクセスポイントの設定）

設定画面：[Manage] > [Managed Access Points]

本アクセスポイントは、2 つのモード（スタンドアロンモードまたは管理モード）のいずれかで動作します。

◆ **スタンドアロンモード**
本製品はネットワークで個々のアクセスポイントとして動作します。
Web マネージャやCLI を使用することで管理します。

◆ **管理モード**
D-Link 統合アクセスシステムの一部となり、D-Link 統合ワイヤレスコントローラを使用して管理を行います。
アクセスポイントが本モードの場合、Web GUI、Telnet、SSHサービスはアクセスポイントで使用できなくなります。

● モードの移行について

D-Link 統合ワイヤレスコントローラは、管理するアクセスポイントのすべてに対し30 秒ごとにkeepalive メッセージを送信します。

各アクセスポイントは、SSL TCP 接続のkeepalive メッセージがないかどうかをチェックします。
アクセスポイントがkeepalive メッセージを通じてコントローラとの通信を維持する限り、管理モードが継続されます。
アクセスポイントが最後のkeepalive メッセージから45 秒以内にメッセージを受信しないと、アクセスポイントは、コントローラがエラーとなりコントローラへのTCP 接続を終了したものと見なして、スタンドアロンモードに入ります。

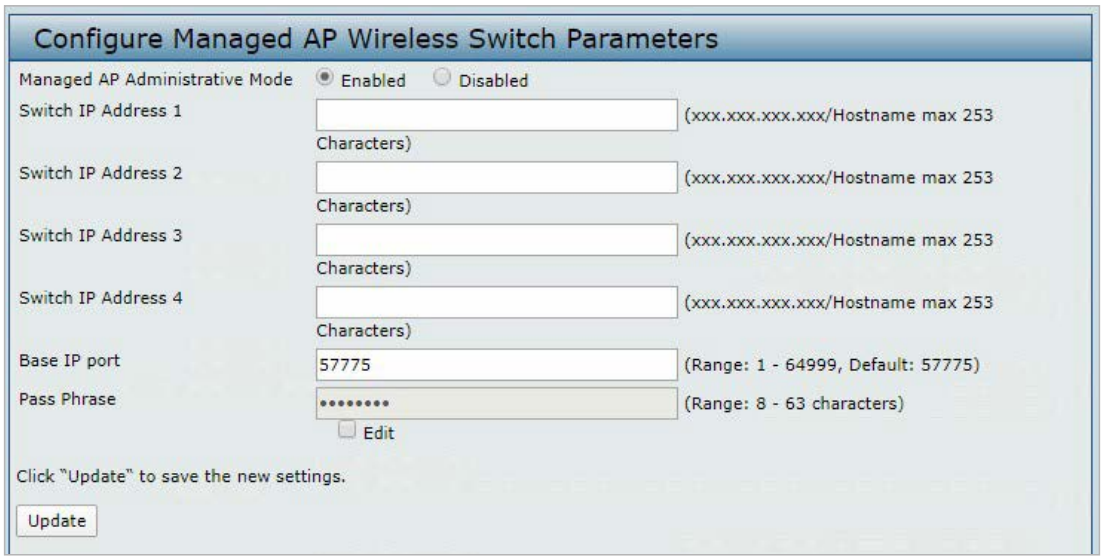
スタンドアロンモードに移行した後も、トラフィックの送信は損失することなく継続します。アクセスポイントは、VLAN Forwarding モード（標準の非トンネルモード）で設定されたVAP の設定を使用します。
アクセスポイントがスタンドアロンモードの場合、Web GUIまたはCLI（Telnet またはSSH 経由）を使用することで管理することができます。

アクセスポイントは、トンネルVAP を通じてアクセスポイントに接続するすべてのクライアントに対して、接続解除メッセージを送信し、トンネルVAP を無効にします。

[Managed AP Administrative Mode]が[Enabled]（有効）に設定されている間、アクセスポイントはディスカバリの手順を開始します。アクセスポイントが無線コントローラとの接続を確立すると、そのコントローラが以前に接続したものと同じであっても異なる場合でも、コントローラはアクセスポイントにコンフィグレーションを送信し、アクセスポイントは現在接続するすべてのクライアントに関する情報を無線コントローラに送信します。
コントローラから送信されたコンフィグレーションの適用後に、アクセスポイントの無線インタフェースは再起動します。
無線インタフェースが動作状態となり、クライアントが再接続するまで、クライアントのトラフィックは中断されます。

■管理アクセスポイントの設定

D-Link 統合コントローラのIP アドレスをアクセスポイントに追加します。



UI	説明
Managed AP Administrative Mode	管理アクセスポイントモードを[Enabled]（有効）または[Disabled]（無効）にします。 • [Enabled]：アクセスポイントとコントローラが相互にディスカバリを行うことを許可します。アクセスポイントが無線コントローラによる自身の認証に成功すると、Web GUIにアクセスできなくなります。 • [Disabled]：アクセスポイントは無線コントローラとコンタクトをとることができません。
Switch IP address 1-4	アクセスポイントの管理に使用できる4 台までの無線コントローラのIP アドレスを入力します。「.」（ドット）で区切った形式またはDNS 名でIP アドレスを入力します。 DHCP サーバを使用することで、ネットワーク上の無線コントローラの定義済みリストを参照することができます。アクセスポイントは、最初に[Switch IP Address 1]とコンタクトを試みます。
Base IP port	無線システムがIP トラフィックの送受信に使用するIP ポート番号の範囲の最初の値を指定します。指定したポート番号から始まる連続した10個のポート番号が設定されます。初期値では無線システムは「57775」から「57784」までのIP ポートを使用します。 [Base IP Port]を変更する場合、無線機能は自動的に無効となり、その後、再有効化されます。新しい設定値はクラスタ設定関連コマンドのグローバルコントローラ構成の一部として送信されないため、クラスタ内の全コントローラは個別に新しいIP 番号が設定される必要があります。 コントローラ側で無線IP ポート番号が初期値から変更された場合、AP 側も変更する必要があります。
Pass Phrase	[Edit]をクリックして、アクセスポイントが無線コントローラで認証されるためのパスフレーズを入力します。 • 入力可能文字数：8 - 63 文字 コントローラには同じパスフレーズを設定する必要があります。
Update	設定を適用します。

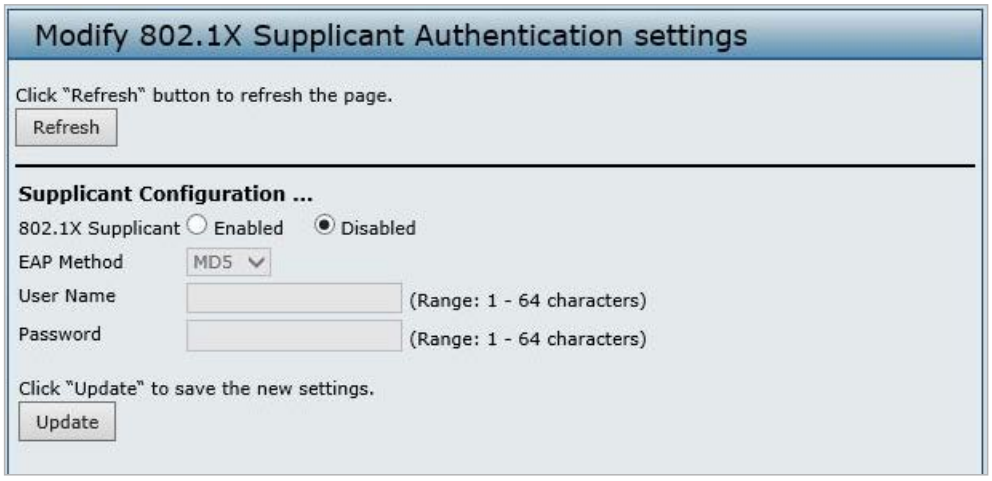
重要

設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。
再起動が発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが少ない時にアクセスポイントの設定変更を行うことをお勧めします。

Authentication（802.1X 認証の設定）

設定画面：[Manage] > [Authentication]

802.1X認証の設定を行います。
IEEE 802.1X のポートベースのネットワークアクセス制御を利用するネットワークでは、サプリカント（クライアント）は802.1X オーセンティケータにアクセスが許可されるまで、ネットワークへアクセスすることができません。
ネットワークで802.1X 認証が使用されている場合は、アクセスポイントに802.1X 認証情報を登録する必要があります。



UI	説明
Refresh	表示を更新します。
802.1X Supplicant	802.1Xサプリカントを[Enabled]（有効）または[Disabled]（無効）にします。
EAP Method	アクセスポイントとオーセンティケータが通信で使用するEAP方式を以下から選択します。 • [MD5] • [PEAP] • [TLS]
User Name	802.1X オーセンティケータからのリクエストに応じる場合にアクセスポイントが使用するMD5 ユーザ名を入力します。半角英数字64 文字以内で指定します。キータイプはASCII で、アルファベットの大文字、小文字、数字、および@# などの記号を含みます。
Password	802.1X オーセンティケータからのリクエストに応じる場合にアクセスポイントが使用するMD5 パスワードを入力します。 半角英数字64 文字以内で指定します。キータイプはASCII で、アルファベットの大文字、小文字、数字、および@# などの記号を含みます。
Update	設定を適用します。

メモ

本機能は現在のファームウェアバージョン（4.7.2.9）ではサポートされていません。

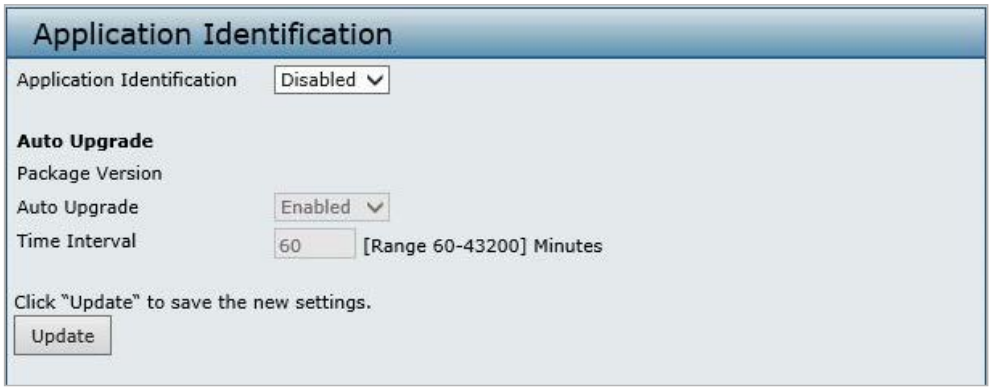
重要

設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。
再起動が発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが少ない時にアクセスポイントの設定変更を行うことをお勧めします。

Application Identification（アプリケーション識別）

設定画面：[Manage] > [Application Identification]

アクセスポイントからコントローラに対し、トラフィックのアプリケーション情報を送信します。



UI	説明
Application Identification	Application Identification機能を[Enabled]（有効）または[Disabled]（無効）にします。
Auto Upgrade	自動アップグレードを[Enabled]（有効）または[Disabled]（無効）にします。
Time Interval	送信間隔を設定します。 ・設定可能範囲：60-43200（分） ・初期値：60（分）
Update	設定を適用します。

メモ

- 本機能は管理モードのみで動作します。
- 本機能は現在のファームウェアバージョン（4.7.2.9）ではサポートされていません。

Service

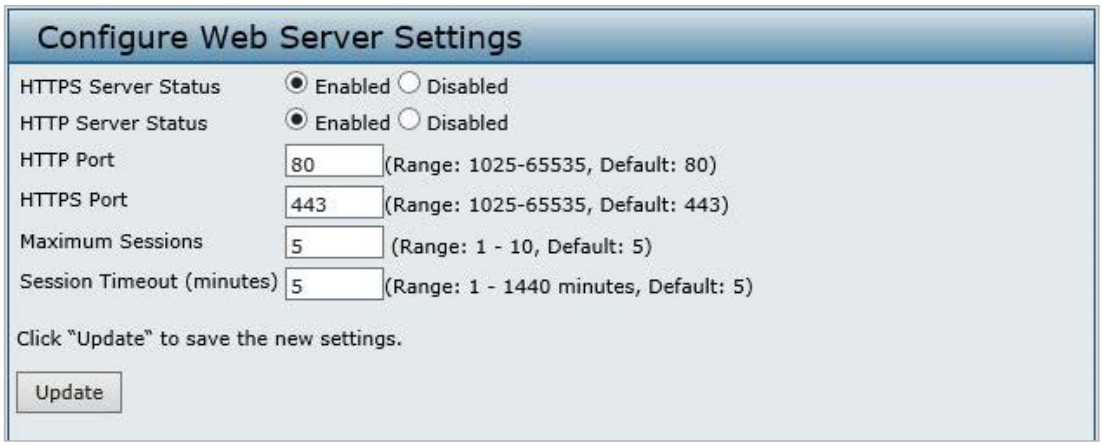
5

Webサーバ設定やSSH/Telnetの有効化/無効化、時間設定など、本製品のサービス設定について説明します。

Web Server（Web サーバの設定）

設定画面：[Service] > [Web Server]

アクセスポイントの管理を行うWebサーバ（HTTP またはHTTPS）の設定を行います。



UI	説明
HTTPS Server Status	HTTPS経由の通信を[Enabled]（有効）または[Disabled]（無効）にします。
HTTP Server Status	HTTP経由の通信を[Enabled]（有効）または[Disabled]（無効）にします。
HTTP Port	HTTPポートを指定します。 ・初期値：80
HTTPS Port	HTTPSポートを指定します。 ・初期値：443
Maximum Sessions	アクセスポイントのWebインタフェースにログインすると、セッションが確立します。このセッションは、ユーザがログオフするか、セッションの非アクティブ時のタイマが期限切れになるまで保持されます。HTTP/HTTPS両方を含む、最大セッション数を入力します。最大セッション数に達すると、Webインタフェースにログインを試みる新しいユーザにはエラーメッセージが表示されます。 ・初期値：5 ・設定可能範囲：1-10
Session Timeout（minutes）	Web GUI上で操作を行わずにログオン状態を継続できる時間を設定します。タイムアウト時間に達すると、ユーザは自動的にログアウトします。 ・設定可能範囲：1-1440（単位：分）
Update	設定を適用します。

重要

アクセスポイントの管理インタフェースにアクセスするために現在使用しているプロトコルを無効にすると、現在の接続は終了します。再度有効にするまで、そのプロトコルを使用したアクセスポイントへのアクセスはできなくなります。

SSH（SSHの設定）

設定画面：[Service] > [SSH]

Secure Shell（SSH）は、リモートホストから本製品のCLI へのアクセスを提供するプログラムです。
SSH は、保証されていないチャンネル上に強健な認証とセキュアな通信を供給するため、リモートアクセスにおいては Telnet より安全性が高くなっています。
システムへのSSH アクセスを有効、または無効にすることができます。

UI	説明
SSH Status	SSH経由の通信を[Enabled]（有効）または[Disabled]（無効）にします。
Update	設定を適用します。

Telnet（Telnetの設定）

設定画面：[Service] > [Telnet]

Telnet は、リモートホストから本製品のCLI へのアクセスを提供するプログラムです。
ここでは、システムへのTelnet アクセスを有効、または無効にします。

重要

Telnetの初期値は[Disabled]（無効）です。

UI	説明
Telnet Status	Telnet経由の通信を[Enabled]（有効）または[Disabled]（無効）にします。
Update	設定を適用します。

QoS（QoSの設定）

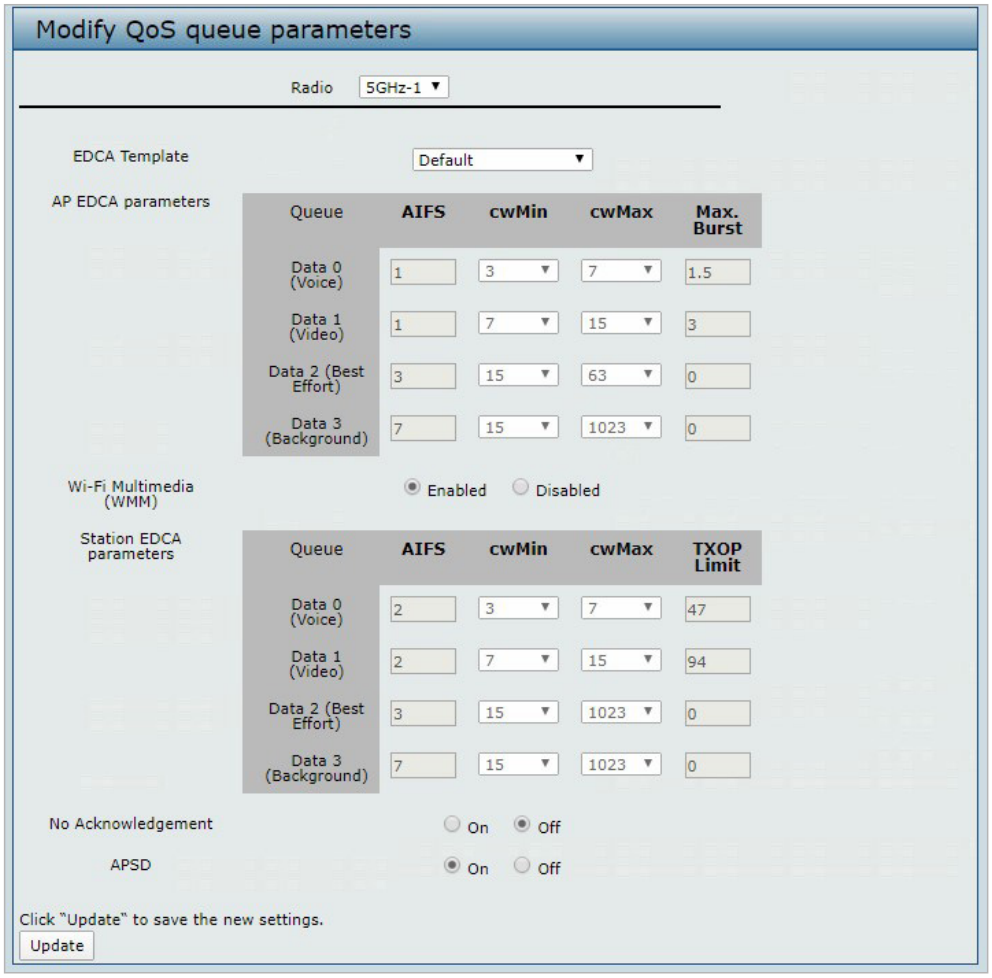
設定画面：[Service] > [QoS]

QoS（Quality of Service）機能は、複数のキューにパラメータを指定することで、本製品を通過する従来のIP データをはじめVoIP（Voice over IP）や音声、映像、ストリーミングメディアなどの多くの無線トラフィックのスループットとパフォーマンスの向上を可能にします。

本製品に設定するQoS は、さまざまな種類の無線トラフィック用のキューにパラメータから構成され、伝送時の最大/ 最小待ち時間を（コンテンション画面により）効果的に指定することができます。ここで説明された設定は、データ伝送動作をアクセスポイントにだけ適用し、クライアントステーションには適用されません。

Enhanced Distributed Channel Access（EDCA）パラメータは、APからクライアントステーションに送信されるトラフィックに適用されます。

アクセスポイントおよびステーションのEDCAパラメータの初期値は、WMM仕様におけるWi-Fi アライアンスによって示されているものです。通常の使用では、これらの値を変更する必要はありません。これらの値を変更すると、提供されるQoSに影響します。



UI	説明
Radio	設定する無線帯域を[5GHz-1] [5GHz-2] [2.4GHz]から選択します。
EDCA Template	EDCAのテンプレートを以下から選択します。[Custom]以外を選択した場合、EDCAのパラメータは自動的に決定されます。 • [Default]：初期設定のテンプレート使用します。 • [Optimize for Voice]：音声トラフィックに最適なテンプレートを使用します。 • [Custom]：テンプレートをカスタマイズします。
AP EDCA parameters	
Queue	[EDCA Template]で[Custom]を設定した場合、以下のキューに対してアクセスポイントのEDCAのパラメータを設定します。キューの優先度はData 0が最も高く、Data 3が最も低くなります。 • [Data 0（Voice）]：優先度「高」、最小限の遅延で送信されます。リアルタイム性が重視される音声トラフィックなどが本キューに送られます。 • [Data 1（Video）]優先度「高」、最小限の遅延で送信されます。リアルタイム性が重視される映像データが本キューに送られます。 • [Data 2（Best Effort）]：優先度「中」、通常のスループット、遅延で送信されます。一般的なIPデータは本キューに送られます。 • [Data 3（Background）]：優先度「低」、高いスループットで送信されます。最大限のスループットを必要とし、リアルタイム性が重要ではないBulkデータはこのキューに送信されます（例：FTP）。
AIFS（Inter-Frame Space）	Arbitration Inter-Frame Spacing（AIFS）は、データフレームの待機時間を指定します。待機時間はスロットで計測されます。 • 設定可能範囲：1-255
cwMin	CW（Contention Window）の最小値を指定します。送信の試行における最初のランダムなバックオフ待機時間（Window）は、0〜本値の間になります。データフレームが送信される前に最初のランダムなバックオフ待機時間が期限切れになると、リトライカウンタが増加し、ランダムバックオフ値（Window）が倍になります。ランダムバックオフ値のサイズがContention Windowの最大値（cwMax）に到達するまで、値は倍増します。cwMinの値はcwMaxの値より小さくする必要があります。
cwMax	CW（Contention Window）の最大値を指定します。データが送信されるか、この上限値（ミリ秒）に達するまで、試行の度にバックオフ値が2倍になります。バックオフ値が上限値に達すると、送信の試行が最大リトライ数に達するまで行われます。
Max.Burst	AP EDCA パラメータで、アクセスポイントからクライアントステーションへのトラフィックフローに対してのみ適用されます。本値は無線ネットワークでのパケットバーストに許可される最大バースト長です。パケットバーストとはヘッダ情報なしで送信される複数のフレームの集まりです。オーバヘッドを少なくすることにより、高スループットと高パフォーマンスを実現できます。 • 設定可能範囲：0-999
Wi-Fi Multimedia（WMM）	WMM（Wi-Fi Multimedia ）を[Enabled]（有効）または[Disabled]（無効）にします。（初期値：無効） WMMが有効の場合、無線メディアのQoS優先および調整が有効になります。UAPに対するQoS設定により、APからクライアントステーションへのダウンストリームトラフィック（AP EDCAパラメータ）、ステーションからAPへのアップストリームトラフィック（ステーションEDCAパラメータ）を制御します。 WMMが無効の場合、ステーションからAPへのアップストリームトラフィックに対するEDCAパラメータの制御が無効になります。この場合、APからクライアントステーションへのダウンストリームトラフィック（AP EDCAパラメータ）を設定することが可能です。

UI	説明
Station EDCA parameters	
AIFS	[EDCA Template]で[Custom]を設定した場合、以下のキューに対してアクセスポイントのEDCAのパラメータを設定します。キューの優先度はData 0が最も高く、Data 3が最も低くなります。 • [Data 0 (Voice)]: 優先度「高」、最小限の遅延で送信されます。リアルタイム性が重視される音声トラフィックなどが本キューに送られます。 • [Data 1 (Video)]: 優先度「高」、最小限の遅延で送信されます。リアルタイム性が重視される映像データが本キューに送られます。 • [Data 2 (Best Effort)]: 優先度「中」、通常のスループット、遅延で送信されます。一般的なIP データは本キューに送られます。 • [Data 3 (Background)]: 優先度「低」、高いスループットで送信されます。最大限のスループットを必要とし、リアルタイム性が重要ではないBulkデータはこのキューに送信されます (例:FTP)。
AIFS (Inter-Frame Space)	Arbitration Inter-Frame Spacing (AIFS) は、データフレームの待機時間を指定します。待機時間はスロットで計測されます。 • 設定可能範囲:1-255
cwMin	CW (Contention Window) の最小値を指定します。送信の試行における最初のランダムなバックオフ待機時間 (Window) は、0〜本値の間になります。データフレームが送信される前に最初のランダムなバックオフ待機時間が期限切れになると、リトライカウンタが増加し、ランダムバックオフ値 (Window) が倍になります。ランダムバックオフ値のサイズがContention Windowの最大値 (cwMax) に到達するまで、値は倍増します。cwMinの値はcwMaxの値より小さくする必要があります。
cwMax	CW (Contention Window) の最大値を指定します。データが送信されるか、この上限値 (ミリ秒) に達するまで、試行の度にバックオフ値が2倍になります。バックオフ値が上限値に達すると、送信の試行が最大リトライ数に達するまで行われます。
TXOP Limit	Station EDCA パラメータで、クライアントステーションからアクセスポイントへのトラフィックフローに対してのみ適用されます。 TXOP (Transmission Opportunity) は、チャンネル占有時間を意味します。 • 設定可能範囲:0-8192
その他のQoSパラメータ	
No Acknowledgement	[On]を選択すると、アクセスポイントがサービスクラス値としてQosNoAck を持つフレームを承認しません。
APSD	[On]を選択すると、電源管理方法である自動省電力機能 (APSD) が有効になります。APSD は、VoIP 電話がアクセスポイントを通じてネットワークにアクセスする場合にお勧めします。
Update	設定を適用します。

重要

設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。
これが発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが低い時にアクセスポイントの設定変更を行うことをお勧めします。

SNMP（SNMPの設定）

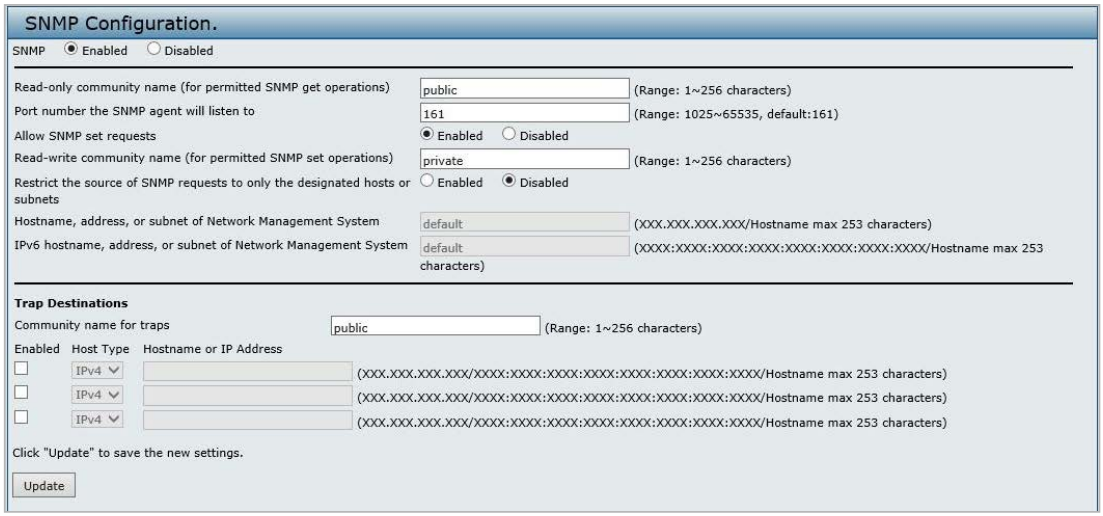
設定画面：[Service] > [SNMP]

SNMP（Simple Network Management Protocol）は、ネットワークデバイス情報の記録・格納・共有に関する標準規格です。SNMPを使用することにより、ネットワークの管理、トラブルシューティング、メンテナンスを容易に行うことができます。本製品では、SNMPv1v2v3をサポートしています。特に注釈がない限り、パラメータはSNMPv1とSNMPv2cのみに適用されます。

SNMP管理ネットワークの主要なコンポーネントは、管理デバイス、SNMPエージェント、管理システムです。SNMPエージェントのMIB（Management Information Bases）にはデバイス情報が含まれ、リクエストに応じてSNMPマネージャに送信されます。AP、ルータ、スイッチ、ブリッジ、ハブ、サーバ、プリンタなどのネットワークノードが管理デバイスとなります。
統合アクセスポイント（UAP）は、HP Openviewなどのネットワーク管理システムへのシームレスな統合の際にSNMP管理デバイスとして機能します。

本設定画面ではSNMPエージェントの有効化/無効化、コミュニティパスワードやアクセスMIB、トラップ送信先の設定を行うことができます。SNMPv3の設定画面ではSNMPv3ビュー、グループ、ユーザ、ターゲットを設定することができます。

詳細は『SNMPv3：p.69 』を参照してください。



UI	説明
SNMP	SNMPの管理モードを[Enabled]（有効）または[Disabled]（無効）にします。 ・初期値：[Enabled]（有効） SNMPを無効化した場合、他のパラメータは設定不可となります。 本設定は、SNMPv1v2cv3に適用されるグローバルSNMPパラメータです。
Read-only community name（for permitted SNMP get operations）	Read-Onlyコミュニティ名を入力します。SNMPv2cで定義されるコミュニティ名は、シンプルな認証メカニズムとして動作し、SNMPエージェントに対しリクエストを行うネットワークデバイスを制限します。本設定値はパスワードとして機能し、送信者がこのパスワードを知っている場合に認証が有効となります。コミュニティ名は英数字で設定可能です。 ・設定可能範囲：1-256文字
Port number the SNMP agent will listen to	初期値ではSNMPエージェントはポート161からのリクエストのみリッスンします。本設定により、このリッスンポートを変更することが可能です。本設定は、SNMPv1v2cv3に適用されるグローバルSNMPパラメータです。 ・設定可能範囲：1-65535
Allow SNMP set requests	SNMPのSetリクエストを[Enabled]（有効）または[Disabled]（無効）にします。 有効にした場合、ネットワーク上のデバイスはSNMPエージェント経由でD-Link System MIBに対して設定の変更が可能になります。
Read-write community name（for permitted SNMP set operations）	SNMPセットリクエストを有効にした場合、Read-Writeコミュニティ名を設定することができます。本設定値はパスワードとして機能し、送信者がこのパスワードを知っている場合に認証が有効となります。コミュニティ名は英数字で設定可能です。 ・設定可能範囲：1-256文字
Restrict the source of SNMP requests to only the designated hosts or subnets	SNMPリクエストの送信元の制限を[Enabled]（有効）または[Disabled]（無効）にします。送信元を制限する場合は[Enabled]、すべてのリクエストを許可する場合は[Disabled]に設定します。

UI	説明
Hostname, address or subnet of Network Management System	管理デバイスに対してGet/Setリクエストを実行できるデバイスのIPv4 DNSホスト名またはサブネットを指定します。 コミュニティ名と同じように、セキュリティレベルを設定することができます。SNMPエージェントはここで指定されたホスト名またはサブネットからのリクエストのみ受け付けます。 サブネットを指定する場合、<address>/<mask_length>で、1つ以上のサブネットワークアドレス範囲を入力します。 <address>にはIPアドレス、<mask_length>にはマスクビット数を指定します。 <address>/<mask>及び<address>/<mask_length>の形式がサポートされています。 IPアドレスやホスト名を指定して特定のホストを指定することもできます。 192.168.1.0/24という範囲を指定した場合、サブネットワーク192.168.1.0、サブネットマスク255.255.255.0の指定となります。 特定のNMSのサブネットを指定する場合、アドレス範囲で指定することが可能です。指定した範囲に含まれるIPアドレスのみがGet/Setリクエストを実行することができます。 上記の例の場合、192.168.1.1から192.168.1.254の範囲のデバイスがSNMPコマンドを実行することができます。（サブネットワーク範囲においてサフィックス「.0」で識別されたアドレスはサブネットアドレス、「.255」のアドレスはブロードキャストアドレスとなります。） もう1つの例として、10.10.1.128/25の範囲を指定した場合、10.10.1.129から10.10.1.254のIPアドレスでコマンドを実行できます。この例では、10.10.1.128がネットワークアドレスで10.10.1.255がブロードキャストアドレスです。126個のアドレスが指定のアドレスとなります。
IPv6 Hostname or IPv6 subnet of Network Management System	Get/Setリクエストを実行することができるIPv6 DNSホスト名またはサブネットを指定します。
Community name for traps	SNMPトラップに紐付けるグローバルコミュニティ文字列を入力します。トラップ送信時のコミュニティ名として使用されます。コミュニティ名は英数字で設定可能です。特殊文字を含めることはできません。 • 設定可能範囲：1-256文字
Host Type	有効化するホストの種類としてIPv4ホストまたはIPv6ホストを選択します。
Hostname or IP address	SNMPトラップ送信先のコンピュータのDNSホスト名を入力します（DNSホスト名の例：snmptraps.foo.com）。SNMPトラップはSNMPエージェントにランダムに送信されるため、トラップの送信先を明示的に指定する必要があります。最大3台のホスト名を設定することができます。「Enabled」チェックボックスにチェックを入れて、ホスト名を入力してください。 • 設定可能範囲：1-256文字
Update	設定を適用します。

重要

設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。
これが発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが低い時にアクセスポイントの設定変更を行うことをお勧めします。

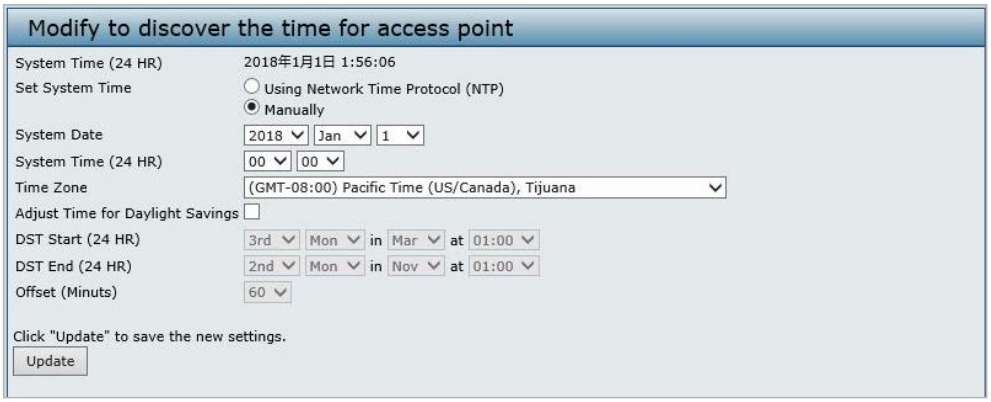
Time Settings（時間設定）

設定画面：[Service] > [Time Settings（NTP）]

本製品の時間設定を行います。
NTPサーバを使用するか、手動で時刻を設定するかを選択することができます。
また、サマータイムの設定を行うことも可能です。

メモ

- NTP（Network Time Protocol）は、ご使用のネットワークのコンピュータクロックタイムを同期させるインターネット標準プロトコルです。NTP サーバは協定世界時（また、グリニッジ標準時として知られている協定世界時）をそれらのクライアントシステムに送信します。NTP は定期的に時間の要求をサーバに送信し、返されたタイムスタンプを使用してクロックを調整します。タイムスタンプは、ログメッセージ内の各イベントの日時を示すために使用されます。



UI	説明
System Time（24 HR）	本製品に設定されている時刻が表示されます。
Set System Time	時間の設定方法を以下から選択します。 • [Using Network Time Protocol（NTP）]：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	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。
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（24HR）	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。
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。 • 初期値：[Pacific Time（US/Canada）, Tijuana]
Adjust Time for Daylight Savings	チェックを入れ、Daylight Savings Time（サマータイム）の設定を行います。
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。
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。
Update	設定を適用します。

重要

設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。
再起動が発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが少ない時にアクセスポイントの設定変更を行うことをお勧めします。

SNMPv3

6

SNMPv3の設定を行います。
SNMP（Simple Network Management Protocol ）とは、TCP/IPネットワークにおいて、ルータやコンピュータ、端末など様々な機器をネットワーク経由で監視・制御するためのプロトコルです。
SNMPでは、機器の状態に関する情報をMIB（Management Information Base）と呼ばれるデータモデルで管理しており、マネージャとエージェントが同じMIBに基いて情報をやりとりします。

SNMPv3 Views（SNMPv3ビューの設定）

設定画面：[SNMPv3] > [SNMPv3 Views]

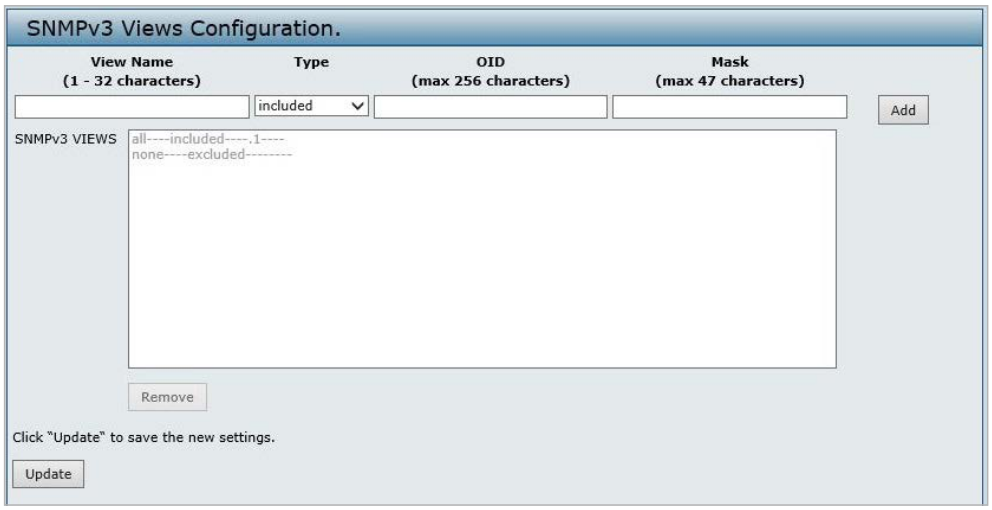
SNMPv3のMIBビュー設定を行います。

MIBビューは、1つまたは複数のサブツリーで構成されます。サブツリーは、OID（オブジェクト識別子）、OIDに対応するマスク、およびビュータイプの組み合わせで設定します。
SNMPv3ユーザがアクセスできるOID範囲をコントロールするために、MIBビューを作成します。

重要

- [all]のMIB ビューは、システムに初期値で作成されています。このビューはシステムによってサポートされるすべての管理オブジェクトを含んでいます。
- Excluded ビューのサブツリーを作成する場合、同じビュー名を持つIncluded エントリを作成して、Excluded サブツリーの外側のサブツリーをアクセス範囲として許可します。

例）サブツリー1.3.6.1.4 を除くビューを作成する場合：
OID 1.3.6.1.4 を持つExcluded エントリを作成します。その後、同じビュー名を持つOID.1 のIncluded エントリを作成します。



UI	説明
View Name	MIB ビューの名称を入力します。
Type	MIBビューのタイプを設定します。 • [included]：MIB ビューにビューサブツリーまたはサブツリーのファミリーを含めます。 • [excluded]：MIB ビューからビューサブツリーまたはサブツリーのファミリーを除外します。
OID	OID（オブジェクト識別子）を入力します。 例：システムサブツリーは、OID 文字列1.3.6.1.2.1.1 で指定されます。
Mask	OID マスクを設定します。 OID マスクの長さは47 文字です。OID マスクのフォーマットは、「xx.xx.xx...」であり、長さは16 オクテットです。各オクテットは「.」（ピリオド）または「:」（コロン）のどちらかによって区切られた2桁の16 進数です。 例：OID マスク「FA.80」は「11111010.10000000」です。
Add	MIBビューを追加します。
SNMPv3 VIEWS	MIBビューが表示されます。
Remove	MIBビューを削除します。
Update	設定を適用します。

SNMPv3 Groups（SNMPv3グループの設定）

設定画面：[SNMPv3] > [SNMPv3 Groups]

SNMPv3グループの設定を行います。

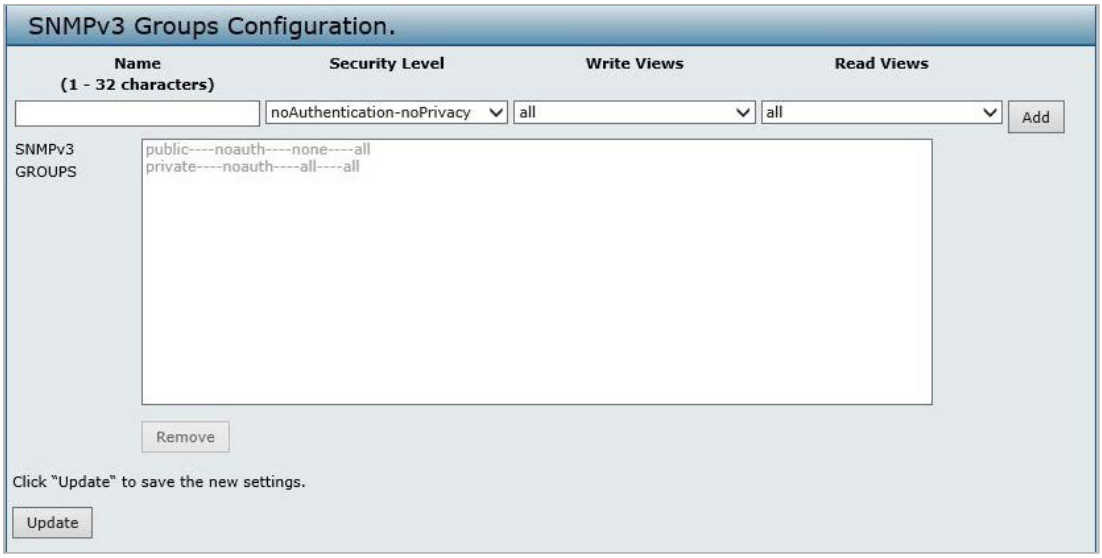
SNMPv3 グループにより、認証レベルとアクセス権限毎にユーザをまとめることができます。
初期値では以下のグループがあります。

- **public**
  認証とデータの暗号化のない読み取り専用グループ。本グループではセキュリティ認証を使用しません。初期値では、本グループのユーザは、ユーザが編集できるすべてのMIB ビューの初期値を参照することができます。
- **private**
  認証とデータの暗号化のないread/write（読み書き）グループ。本グループではセキュリティ認証を使用しません。初期値では、本グループのユーザは、ユーザが編集できるすべてのMIB ビューの初期値を読み書きすることができます。

メモ

最大8個のグループを設定することができます。

本画面では追加グループを定義することができます。



UI	説明
Name (1 - 32 characters)	グループの名称を入力します。 • 入力可能文字数：半角英数字32文字以内
Security Level	セキュリティレベルを以下から選択します。 • [noAuthentication-noPrivacy]： 認証とデータ暗号化の両方がありません。（セキュリティなし） • [Authentication-noPrivacy]： 認証を行いますが、データ暗号化は行いません。 ユーザは、認証にはMD5 キー/パスワードを使用するメッセージをSNMP に送信しますが、暗号化のためのDES キー/パスワードは送信しません。 • [Authentication-Privacy]： 認証とデータ暗号化を行います。 ユーザは、認証にはMD5 キー/パスワード、暗号化にはDES キー/パスワードを送信します。
Write Views	グループに管理オブジェクト（MIBs）に対するアクセス（書き込み）を選択します。 • [all]：グループは、MIBを作成、変更、および削除できます。 • [none]：グループは、MIBを作成、変更、または削除できません。
Read Views	グループに管理オブジェクト（MIBs）に対するアクセス（読み出し）を選択します。 • [all]：グループは、MIBの参照および読み出しができます。 • [none]：グループは、MIBの参照も読み出しもできません。
Add	グループを追加します。
SNMPv3 VIEWS	グループが表示されます。
Remove	グループを削除します。
Update	設定を適用します。

SNMPv3 Users（SNMPv3ユーザの設定）

設定画面：[SNMPv3] > [SNMPv3 Users]

SNMPv3ユーザの設定を行います。
複数のユーザを定義し、各ユーザに希望するセキュリティレベルの割り当て、セキュリティキーの設定を行うことができます。認証にはMD5 タイプ、暗号化にはDES タイプだけがサポートされています。

UI	説明
Name	SNMPv3ユーザの名称を入力します。 • 入力可能文字数：最大32文字（半角英数字）
Group	ユーザをグループにマップします。初期グループは[public]および[private] です。 [SNMPv3 Groups]画面で追加グループを定義することができます。
Authentication Type	ユーザからのSNMP リクエストに使用する認証タイプが表示されます。 • [MD5]： ユーザからのSNMPv3 リクエストにMD5認証を必要とします。 • [None]： ユーザからのSNMPv3 リクエストに対し認証を必要としません。
Authentication Key	認証タイプとしてMD5 が指定されている場合、パスワードを入力します。 • 入力可能文字数：8-32文字（半角英数字）
Encryption Type	ユーザからのSNMP リクエストに使用する暗号化のタイプが表示されます。 • [DES]： ユーザからのSNMPv3リクエストにDES暗号化を使用します。 • [None]： ユーザからのSNMPv3リクエストに対し暗号化を必要としません。
Encryption Key	暗号化タイプとしてDES が指定されている場合、SNMP要求を暗号化するためのキーを入力します。 • 入力可能文字数：8-32文字（半角英数字）
SNMPv3 USERS	アクセスポイントに定義したSNMPv3ユーザが表示されます。
Add	SNMPv3ユーザを追加します。
Remove	選択したSNMPv3ユーザを削除します。
Update	設定を適用します。

SNMPv3 Targets（SNMPv3ターゲットの設定）

設定画面：[SNMPv3] > [SNMPv3 Targets]

SNMPv3ターゲットの設定を行います。
SNMPv3ターゲットは、SNMP マネージャにトラップメッセージを送信します。
各ターゲットはターゲット名で識別され、ターゲットIP アドレス、UDP ポート、およびSNMP ユーザ名に関連付けられます。

UI	説明
IPv4/IPv6 Address	リモートのSNMP マネージャのIP アドレスを入力し、トラップメッセージを受信するターゲットホストを指定します。
Port	SNMPv3ターゲットを送信するために使用するUDP ポートを入力します。
Users	ターゲットに割り当てるSNMPv3ユーザ名を選択します。
SNMPv3 TARGETS	SNMPv3ターゲットを表示します。
Add	SNMPv3ターゲットを追加します。
Remove	選択したSNMPv3ターゲットを削除します。
Update	設定を適用します。

Maintenance

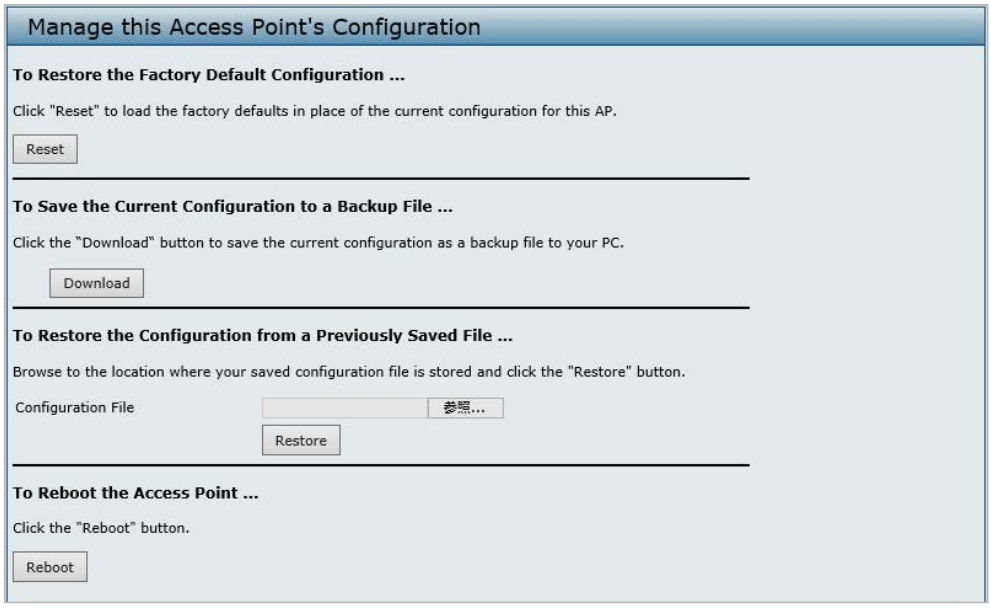
7

コンフィグレーションの保存/リストア、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。また、本製品のサポート情報をダウンロードして閲覧することも可能です。

Configuration（コンフィグレーションの保存・リストア）

設定画面：[Maintenance] > [Configuration]

コンフィグレーションファイルの保存、リストアを行います。
コンフィグレーションファイルはbin形式でダウンロードされます。また、本画面では設定の初期化やリブートを行うこともできます。

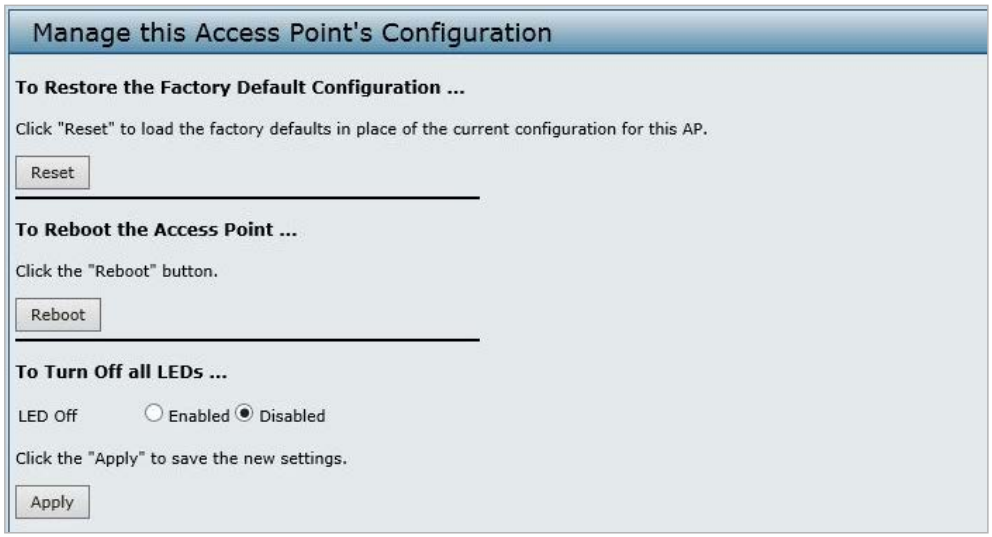


UI	説明
To Restore the Factory Default Configuration.....	
Reset	設定を工場出荷時の状態に戻します。 パスワードや無線設定などを含むすべての設定が工場出荷時の設定に戻ります。 本製品の側面にあるリセットボタンを押下して工場出荷時設定にリセットすることもできます。
To Save the Current Configuration to a Backup File	
Download	現在の設定をコンフィグレーションファイルとしてダウンロードします。[Download]をクリックし、HTTP経由でダウンロードを行います。
To Restore the Configuration from a Previously Saved File	
Restore	保存したコンフィグレーションファイルをリストアします。 [参照]をクリックしてファイルを選択 → [Restore]をクリックします。
To Reboot the Access Point.....	
Reboot	アクセスポイントを再起動します。

Maintenance（メンテナンス）

設定画面：[Maintenance] > [Maintenance]

設定の初期化、リブート、LEDの有効化/無効化を行います。



UI	説明
To Restore the Factory Default Configuration.....	
Reset	設定を工場出荷時の状態に戻します。 パスワードや無線設定などを含むすべての設定が工場出荷時の設定に戻ります。 本製品の側面にあるリセットボタンを押下して工場出荷時設定にリセットすることもできます。
To Reboot the Access Point.....	
Reboot	アクセスポイントを再起動します。
To Turn Off all LEDs ...	
LED Off	アクセスポイントのLEDを[Enabled]（有効）または[Disabled]（無効）にします。

Upgrade（ファームウェアアップグレード）

設定画面：[Maintenance] > [Upgrade]

ファームウェアのアップグレードを行います。

UI	説明
Model	モデル名が表示されます。
Platform	プラットフォーム名が表示されます。
Firmware Version	現在のファームウェアバージョンが表示されます。
New Firmware Image	[参照]をクリックしてファイルを選択→[Upgrade]をクリックします。

重要

- アップグレード中はWeb GUIに経過画面が表示されます。そのままお待ちください。
- アップグレードには数分かかることがあり、その間本製品は使用できなくなります。
- アップグレードを行っている間は、本製品の電源を切らないでください。アップグレード終了後、本製品は再起動します。
- FW：4.7.2.6からFW：4.7.2.9B003Cへのアップグレード後、本製品は以下の状態になります。
  - 設定が工場出荷時の状態にリセットされます。再度設定を行ってください。
    APがDWC-2000によって管理されている場合は、工場出荷時の状態にリセット後、APはDWC-2000から設定を自動的にダウンロードします。
  - FW：4.7.2.6およびそれ以前のファームウェアへのダウングレードはできません。
  - 古いバージョンで取得したコンフィグファイルは使用できません。

Support Information（サポート情報）

設定画面：[Maintenance] > [Support Information]

アクセスポイントのサポート情報をダウンロードできます。
サポート情報には、本製品の統計情報やトラブルシューティングに役立つ情報が含まれています。

UI	説明
Download	サポート情報をテキストファイルとしてダウンロードします。

Client QoS

8

無線クライアントからアクセスポイントへのトラフィックに作用するQoS の設定方法について説明します。統合アクセスポイントのクライアントQoS 機能を使用して、帯域制限を行うことができます。

VAP QoS Parameters（VAP QoS パラメータの設定）

設定画面：[Client QoS] > [VAP QoS Parameters]

クライアントQoS の管理モードを設定し、VAP のQoS 設定を行います。
本製品のクライアントQoS 機能を使用すると、ネットワークに接続する無線クライアントのQoS に対し、個々のクライアントで送受信を許可される帯域幅のコントロールといった、より詳細な制御を行うことができます。

UI	説明
Client QoS Global Admin Mode	アクセスポイントのクライアントQoS 機能を[Enabled](有効)または[DIsabled](無効)にします。 本設定を変更しても、QoS 画面で行ったWMM設定は変更されません。
VAP QoS Default Parameters	
Radio	設定する無線帯域を[5GHz-1] [5GHz-2] [2.4GHz]から選択します。
VAP	クライアントQoS 設定を行うVAP（VAP 0-15）を指定します。指定したVAP に設定したQoS は、他のVAP 経由でネットワークに接続しているクライアントには適用されません。
Client QoS Mode	VAPメニューから選択したVAP のQoS 機能を[Enabled]（有効）または[DIsabled]（無効）にします。 クライアントQoS 設定を無線クライアントに適用するには、[Client QoS Global Admin Mode]欄でクライアントQoS 機能を有効にし、さらに本欄のVAP を有効にする必要があります。
Bandwidth Limit Down	アクセスポイントから無線クライアントへの最大送信速度（bps）を入力します。 ・設定可能範囲：0-4294967295（bps） 0 は、最大帯域幅の制限が実施されないことを意味します。
Bandwidth Limit Up	無線クライアントからアクセスポイントへの最大送信速度（bps）を入力します。 ・設定可能範囲：0-4294967295（bps） 0 は、最大帯域幅の制限が実施されないことを意味します。
Update	設定を適用します。

付録

9

設定例

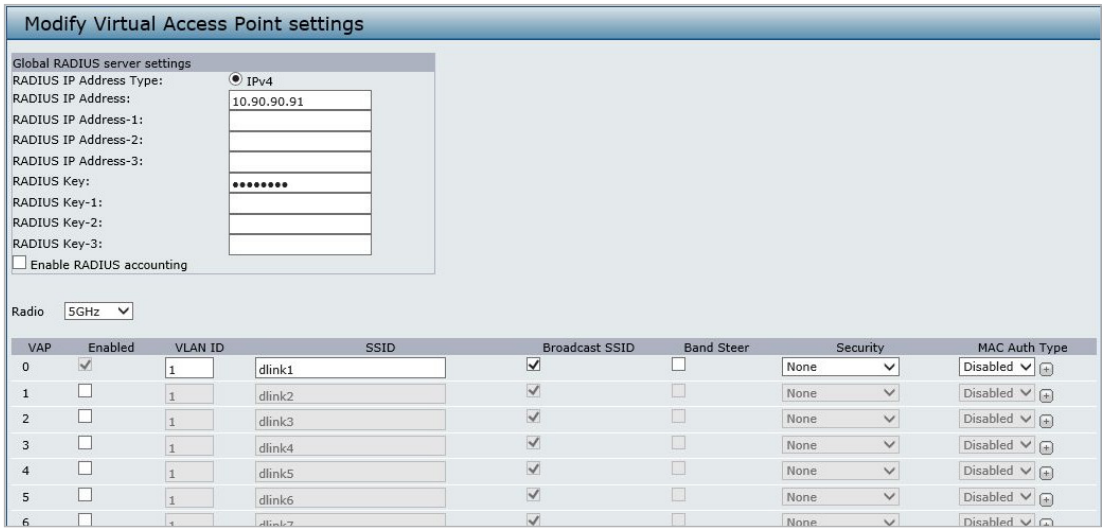
本製品で利用可能ないくつかの機能を設定する方法について説明します。

■VAPの設定

VAP 1 の設定を以下のとおりに設定します。
- VLAN ID：2
- SSID：Marketing
- Security：WPA Personal using WPA2 with CCMP（AES）

● Web GUIからのVAP設定

1. [Manage] > [VAP (SSID)] の順にメニューをクリックします。



2. VAP 1 の [Enabled] 欄のチェックボックスをチェックします。
3. [VLAN ID] 欄に [2] を入力します。
4. [SSID] 欄で既存の SSID を削除して [Marketing] と入力します。
5. [Security] 欄のプルダウンメニューから [WPA Personal] を選択します。

   以下の画面が表示されます。

6. [WPA-TKIP] のチェックを外します。
7. [Key] 欄に WPA 暗号キーを入力します。

   暗号キーには、半角英数字および記号を使用することができます。
   入力可能文字数：8 ～ 63 文字（大文字と小文字を区別）
8. [Update] をクリックし、設定を適用します。

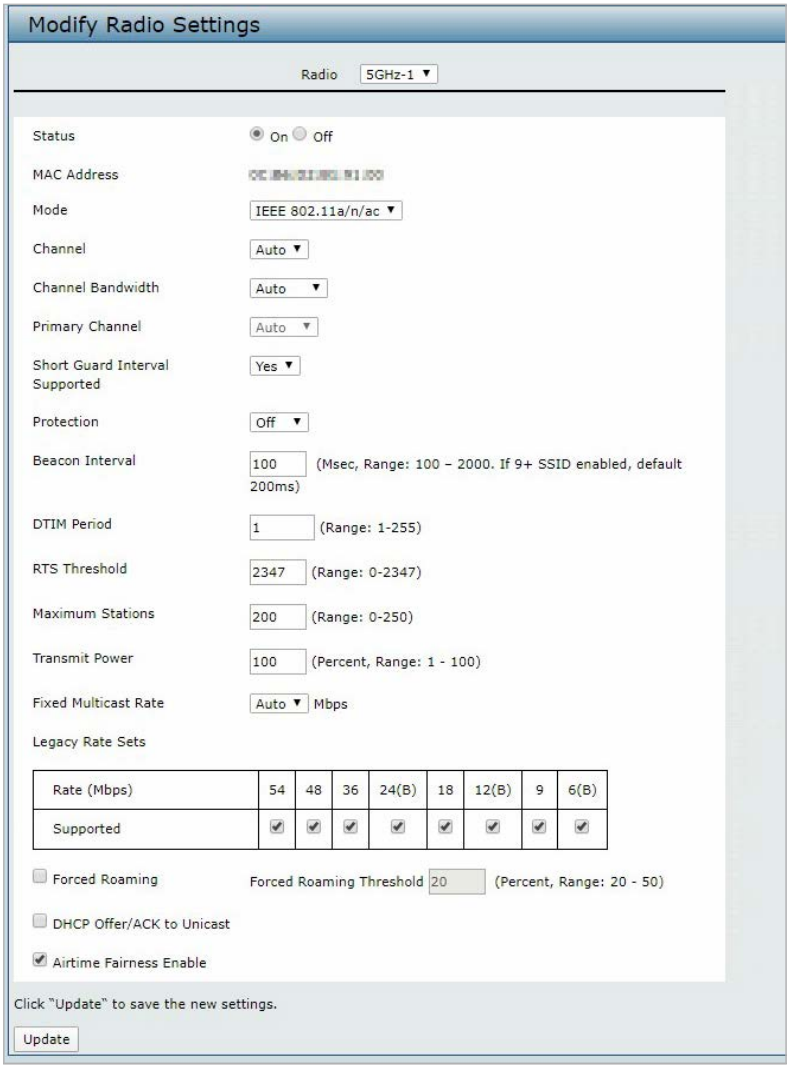
■無線インタフェースの設定

2.4GHz Radio Interfaceを以下の通りに設定します。

- モード - IEEE 802.11b/g/n
- チャンネル - 6
- チャンネル帯域幅 - 40MHz
- 接続ステーション最大数 - 100
- 送信電力 - 75%

●Web GUIからの無線インタフェース設定

1. [Manage] > [Radio] の順にメニューをクリックします。



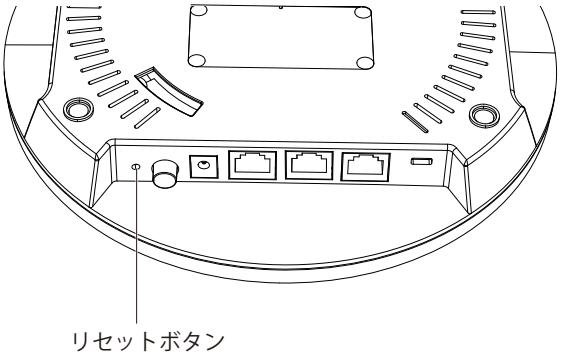
2. [Radio] で [2.4GHz] を選択し、[Status] が [On] であることを確認します。
3. [Mode] で [IEEE 802.11b/g/n] を選択します。
4. [Channel] で [6] を選択します。
5. [Channel Bandwidth] で [40MHz] を選択します。
6. [Maximum Station] の値を [100] に変更します。
7. [Transmit Power] の値を [75] に変更します。
8. [Update] をクリックし、設定を適用します。

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。

■リセットボタンで設定のリセットを行う

1. 本体の電源を入れた状態で、本体側面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、システムが再起動します。そのままお待ちください。

■Web GUIから設定のリセットを行う

1. Web GUI 上部にある管理メニューの [System] をクリックします。
2. [Reset] をクリックします。
3. システムが再起動します。そのままお待ちください。